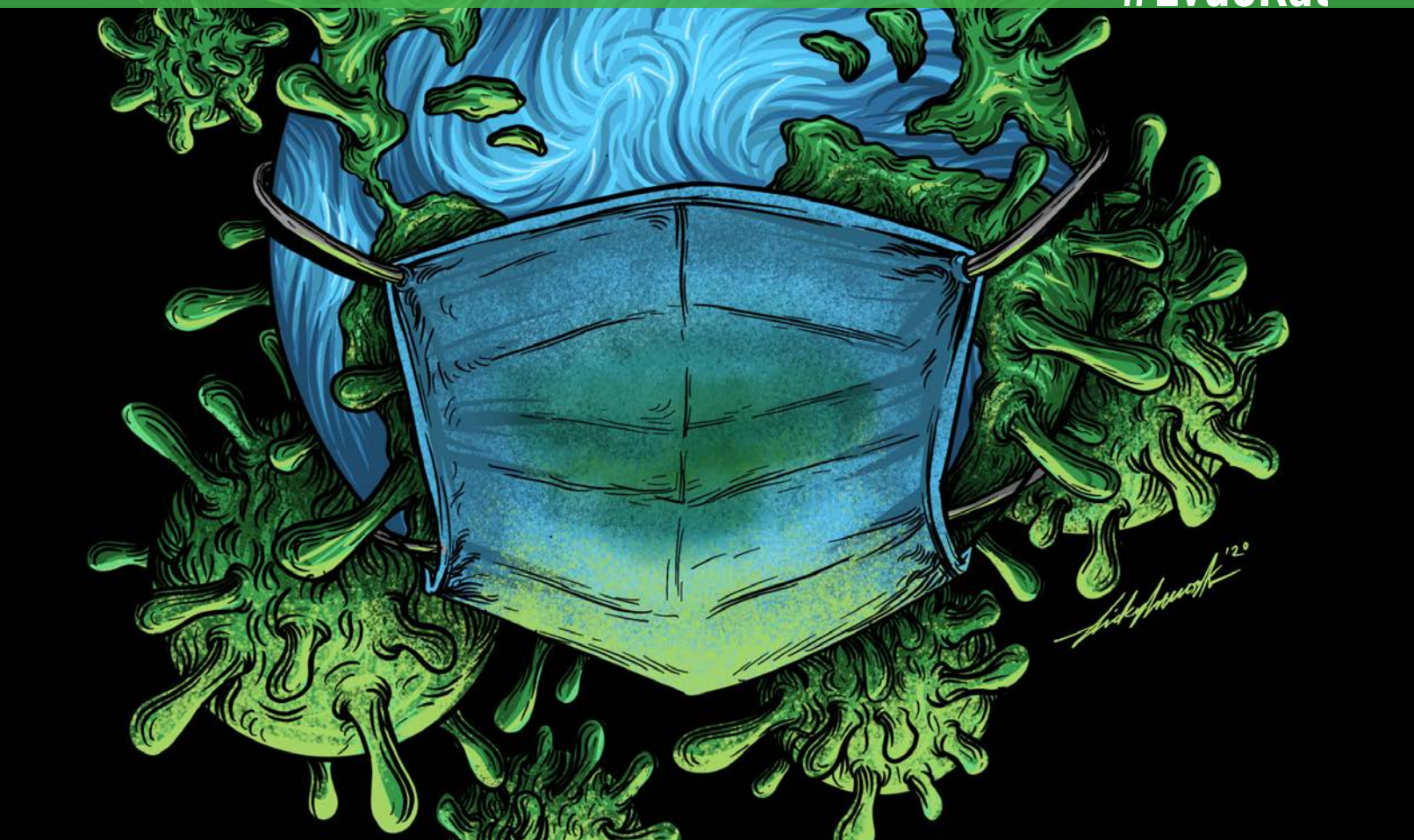
ARKAKAPI

SİBER GÜVENLİK DERGİSİ

www.arkakapidergi.com

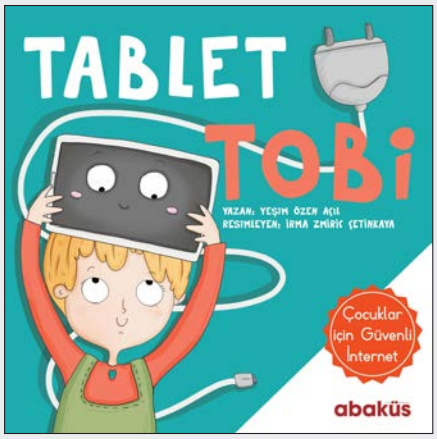
2 Aylık Siber Güvenlik Dergisi • 14 TL • 11. SAYI - 2020

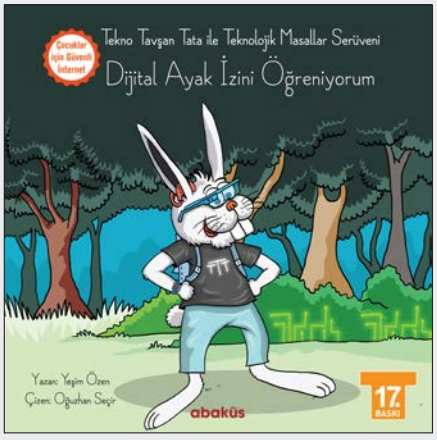
#EvdeKal



ÇOCUKLAR İÇİN GÜVENLİ İNTERNET SERİSİ

Çocuklar için Güvenli İnternet





abaküs

Türkiye'nin Bilişim Kaynağı

www.abakuskitap.com

KÜNYE

YIL: 2 Sayı: 11 - ISSN: 2618-6373

www.arkakapidergi.com

2 ayda bir yayımlanır.

Abaküs Kitap Yayın Eğitim Ltd. Şti.

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

Tel: 0212 514 68 61

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

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

Grafik Tasarım: Cem Demirezen - grafik@abakuskitap.com

Kapak: Ali Zahit Yavuz - alizahit@abakuskitap.com

Düzelti: Huriye Özdemir

Yayın Koordinatörü: Oğuz Aydınyılmaz

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

Hukuk Müşaviri: Avukat Mehmet Pehlivan - Pehlivan İlkakın Hukuk Bürosu

Sosyal Medya: Doğukan Turan, Görkem Güler ve Eren Uygun

Web: www.arkakapidergi.com

Twitter.com/arkakapidergi

abone@arkakapidergi.com

editor@arkakapidergi.com

etkinlik@arkakapidergi.com

Kapak Görseli: Dicktyartwork

EDİTÖRDEN

Dostlar merhaba!

Uzun bir ara oldu ve sizi çok özledik. Arayı biraz açtık ama kimin aklına gelirdi ki bir siber güvenlik dergisine biyolojik bir virüs konu olsun? Dijital virüslerden, biyolojik virüslere! Gerçi hoş, hayat da bu değil mi? … Şöyle bir oturup düşününce, insanoğlunun bilinen tarihine göre en yetkin olduğu bu dönemde, bir virüsün bu *koca yaşlı şişko dünyaya* resmen darbe yapmış olması? Binlerce can kaybının yaşanması? Sizce de garip değil mi? Bir arkadaşım bu durumu sosyal medyada güzel yorumlamıştı; müsadenizle o yorumu sizinle paylaşayım:

> *"14. yüzyılda basit bir bakterinin sebep olduğu kara veba salgını, çok basit bir antibiyotik ile tedavi edilebilecekken Avrupa'nın neredeyse yarısını öldürmüş. Şimdi düşününce hayret ediyor insan. 14. yüzyılda Antibiyotik nedir bakteri nedir bilen yoktu."*
>
> *Gelecek nesiller de bizim bu günlerde yaşadığımız trajediye hayret edecek. Çok basit bir virüs hayatı felç etmiş, şu kadar insan öldürmüş hatta Dünya ekonomisini çökertmiş, halbuki çok basit bir 'x' ile herkes kurtulabilirdi ama x'in ne olduğunu bile bilmiyorlardı diyecekler.*
>
> *Ama çok daha hayret edecekleri şey, insanoğlunun 2019 yılında birbirini öldürmek için harcadığı askeri bütçenin 2 Trilyon Dolardan fazla olması olacaktır. Dünya'daki tüm üniversiteler, enstitüler, laboratuvarlar ve tüm bilimsel çalışmalar bunun yarısını harcayamıyor."*

Neyse, canınızı daha fazla sıkmadan biz konumuza devam edelim iyisi mi. Yani biraz bizden biraz da malum, Koronavirüsünden dolayı bu sayı biraz geç ve sadece dijital bir sayı olarak yayımlandı. Takdir edersiniz ki bu süreç içerisinde matbaalar ve dağıtım derken basılı bir sayı çıkartmak doğru bir karar olmazdı zira pek mümkün de değil. Bu durumdan dolayı yine de affınıza sığınıyor ve bunu telafi edeceğimizin sözünü veriyoruz.

Unutmadan paylaşmam gereken bir husus daha var, bu süreçte biz de kolları sıvadık ve sizler için bir kampanya başlattık, derginin tüm sayılarını 1 ay boyunca halka açtık!

Kaç kişinin gündemine düştü bilmiyorum ama geçtiğimiz günlerde Cumhurbaşkanlığı Külliyesi'nde, Sosyal Medya Zirvesi gerçekleşti. Tasarının, yabancı sosyal medya şirketlerinden vergi alınması, Türkiye'de temsilci bulundurmaları gibi haklı tarafları olduğu gibi ifade özgürlüğünü risk altına alabilecek, korkutan yanları da var maalesef. İlginç olan şu ki bu tasarı, Koronavirüsle mücadele kapsamında hazırlanan tasarı ile birlikte sunuldu meclise? Neyse ki şimdilik telaşlanacak bir şey yok, nasıl oldu bilmiyorum ama bu tasarı meclisten geçmedi, 'şimdilik'. Eğer bu husus ile ilgili bilginiz yoksa bir bakmanızı rica ederim, zira hepimiz için oldukça önemli bir konu. Bu tasarıyı ve sürecini özellikle bizim gibi işin teknik tarafına daha yakın olan kimseler daha yakından takip etmeli ve kamuoyunu bilgilendirmeli. Belki de WhatsApp'ta elden ele dolaşan o garip mesajlar size de ulaşmıştır *("Önemli Duyuru! Yarından itibaren tüm dünyada Devletler anlaştı, bu yıl itibari ile WhatsApp, Facebook, Twitter, tüm yazışmalar, konuşmalar..dikkatli olun")*.

Gelelim 11. sayının içeriğine: Bir yandan yazı dizileri tüm hızıyla devam ederken diğer yandan yeni yazı dizileri geliyor, birbirinden habersiz iki yazarımız Big Brother'a selam çakarken, yeni yazarlarımız da kalemlerini konuşturuyor, yani dostlar yine dopdolu bir sayı ile huzurlarınızdayız! Başta yazarlarımız olmak üzere emeği geçen tüm dostların yüreğine sağlık. Konuşulacak çok şey birikti ama gelin görün ki bize ayrılan alanın sonuna geldik. :) İnşallah tez vakitte malum sorunlar çözülür de güzel bir meetup gerçekleştirir, bir güzel muhabbet eder, kurtlarımızı dökeriz! :)

Ayrıca bu zor günlerde başta sağlık çalışanları olmak üzere tüm emekçilere sonsuz teşekkürü bir borç biliriz. Bugün bu vesile ile birçok şeyin farkına vardığımız gibi, ilmin önemini de bir kez daha görmüş ve kabul etmiş olduk. Bir Anadolu ereni olan, Hacı Bektaş-i Veli der ki:

> *"İlimden gidilmeyen yolun sonu karanlıktır."*

İlim ve doğruluk yolunda buluşmak ümidi ile; yolunuz aydınlık olsun. Kalın sağlıcakla dostlar.

Şahin Solmaz - editor@arkakapidergi.com

İÇİNDEKİLER

Mayıs-Haziran 2020 Siber Güvenlik & Bilişim Etkinlikleri

<> Türkiye Açık Kaynak Platformu </> Turkey Open Source Platform

AçıkSeminer 10.Gün: Büyük Veri ve Açık Kaynaklı Veri Bilimi

28 Nisan 2020 | Çevrim İçi, 14:00

Türkiye Açık Kaynak Platformu'nun organize ettiği Açık Seminer etkinliklerinin 10. gününde büyük veri ve bankacılıkta açık kaynaklı veri bilimi konuları Hasan Basri Akırmak ve Çağlar Subaşı tarafından ele alınacaktır. Geçmiş seminerlere şu adresten erişebilirsiniz: https://bit.ly/2Y9AcXS

Bilgi: https://bit.ly/3cTGwqP

Ödül Avcılığı Dünyasına Giriş

29 Nisan 2020 | Çevrim İçi, 21:00

Mehmet İnce'nin moderatörlüğünde "Ödül avcılığı konusunda nasıl ilerlemeli, nelere dikkat etmeli?" gibi soruların cevaplarını bizzat Hackerone çalışanlarının (@umr4n6 ve @utkusen) vereceği bu yayın 29 Nisan saat 20:59'da gerçekleştirilecektir. Geçmiş yayınlara aynı Twitch kanalı üzerinden erişebilirsiniz.

Bilgi: https://www.twitch.tv/mdisec

HACKNIGHTS

Japonya'da Hacker Olmak

01 Mayıs 2020 | Çevrim İçi, 20:00

Hacknights'ın düzenlediği bu etkinlik 1 Mayıs'ta canlı yayın olarak gerçekleştirilecektir. Workshop eğitiminin toplamda 2 saat sürmesi planlanmaktadır.

Bilgi: twitch.tv/hacknightsorg

TÜRKİYE SİBER GÜVENLİK KÜMELENMESİ

Web Uygulama Güvenliği Eğitimi

05 Mayıs 2020 | Çevrim İçi, 14:00

Türk Telekom'dan Fatih COŞKUN tarafından verilecek "Web Uygulama Güvenliği 101" eğitimi 05 Mayıs saat 14:00'te Türkiye Siber Güvenlik Kümelenmesi YouTube kanalında canlı yayında gerçekleştirilecektir. Geçmiş eğitimlere yine aynı kanaldan erişebilirsiniz.

Bilgi: https://youtube.com/c/turkiyesiberguvenlikkumelenmesi

Yapay Zeka Çözümleri 2020

12 Mayıs 2020 | Çevrim İçi 12:00

BT vizyon

Gelişen teknoloji ile birlikte yapay zeka ve makine öğreniminin önemi de giderek artmaktadır. Etkinlikte yapay zeka çözümleri ele alınacaktır.

Bilgi: https://bit.ly/2yJVVeo

COVID-19 Pandemisinde Dikkat Edilmesi Gereken Siber Güvenlik Başlıkları

1 Haziran 2020 | Çevrim İçi 19:00

BARİKAT Siber Güvenlik

Birçok kötü niyetli yazılım ailesini dağıtan oltalama e-postalarında ve fidye yazılım kampanyalarında #coronavirus hikayeleri kullanılmaktadır.

Bu etkinlik, COVID-19 pandemisi süresince dikkat edilmesi gereken siber güvenlik başlıklarını içermektedir.

Bilgi: https://bit.ly/2xaZ1HU

CloudTalk Global 2020

11 Haziran 2020 | İstanbul Kongre Merkezi, 09:15

CloudTalk Global

3 farklı salonda eş zamanlı olarak devam edecek 30'dan fazla oturum, özel workshoplar ve ticari network toplantıları ile sektörün tüm paydaşları bu etkinlikte olacak.

Bilgi: https://bit.ly/3eW0eDR

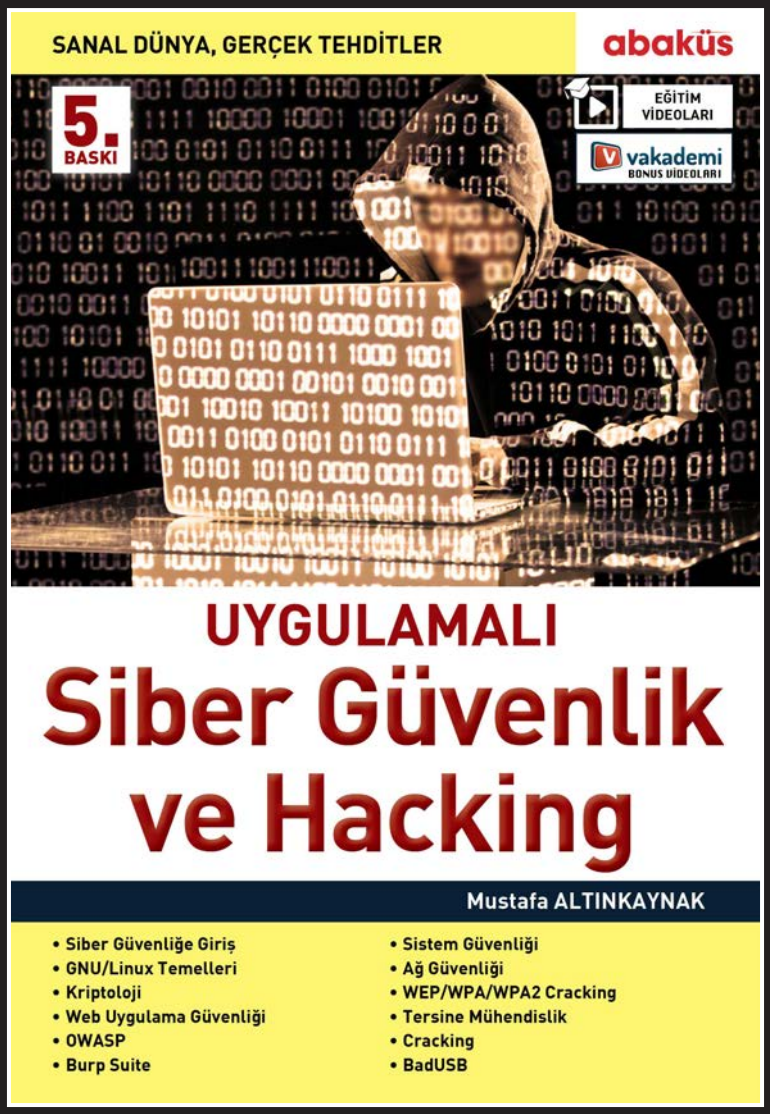
BTvizyon Konya 2020

18 Haziran 2020 | Konya, 09:00

BT vizyon

BTvizyon Anadolu Toplantıları, bilişim teknolojilerine ilişkin güncel ve gelecek vizyonların, deneyimlerin, bilgilerin, ürün ve çözümleriniz paylaşıldığı toplantı platformudur."BTvizyon Anadolu Toplantıları" etkinlikleri; önde gelen bilişim firmaları ile Anadolu'nun çeşitli illerindeki firmaların buluşturulmasını amaçlar.

Bilgi: https://bit.ly/2W01pd0



UYGULAMALI
SİBER GÜVENLİK VE HACKING

MUSTAFA ALTINKAYNAK

abaküs

Raportör: Cafer Uluç cafer@arkakapidergi.com

SÖYLEŞİLERLE SİBER GÜVENLİK UZMANLARINDAN

YENİ BAŞLAYANLAR İÇİN YOL HARİTASI II

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

Peki, Şahin Bayzan kimdir?

Yakın Doğu Üniversitesi'nden (Near East University – KKTC) 1998 yılında "Bilgisayar Mühendisliği" bölümünden mezun olan Şahin Bayzan, yüksek lisans öğrenimini 2005 yılında Pamukkale Üniversitesi'nde, doktorasını ise 2014 yılında Kocaeli Üniversitesi'nde tamamlar. Bu süreç içinde 2012 yılında Ankara Üniversitesi'nde "Adalet" programında ön lisansını Hukuk Fakültesinde aldıktan sonra eğitim serüvenine bir yenisini eklemek üzere 2014 yılında Kırıkkale Üniversitesi'nde "Siyaset Bilimi ve Kamu Yönetimi" öğrencisi olur ve 2018'de mezun olur.

2000-2008 yılları arasında ise mezunu olduğu Pamukkale Üniversitesi'nin "Bilgisayar Mühendisliği" bölümünde öğretim üyesi olarak çalışır. Aynı yıl şu anki aktif görev aldığı ve bizlerin daha çok BTK olarak bildiği Bilgi Teknolojileri ve İletişim Kurumu'nda çalışmaya başlar.

Bayzan'ın çalışma alanları ise oldukça geniş: Dijital vatandaşlık, siber zorbalık, sosyal medya, İnternet'te kişisel bilgi güvenliği, İnternet'in bilinçli ve güvenli kullanımı, İnternet'in çocuklara yönelik riskleri konularında akademik çalışmalar yapmakta ve sosyal medya, İnternet'te bilgi güvenliği ve İnternet'in bilinçli ve güvenli kullanımı, İnternet'te hak ve sorumluluklar konularında Türkiye genelinde 200'den fazla seminer eğitici eğitimleri verir, vermeye de devam etmektedir.

2014 yılında TRT Türkiye'nin Sesi Radyosu'nda yayımlanan ve her yönüyle İnternet'in irdelendiği "İnternet Dünyasından" adlı programın danışmanlığını yapan Bayzan'ın, "İnternet Bağımlılığı – Sorunlar ve Çözümler" adlı kitapta "İnternet'in Bilinçli ve Güvenli Kullanımı" başlıklı bölüm yazarlığı ve Hece dergisinin "Dijital Kültür" özel sayısında "Dijital Yerlilerin İnternet Macerası" adında makalesi de bulunmaktadır.

Halen, Bilgi Teknolojileri ve İletişim Kurumunun İnternet Daire Başkanlığı'nda Bilişim Uzmanı olarak görevini sürdürmekte olan Şahin Bey'in akademik çalışmalarına www.sahinbayzan.com.tr adresinden erişebilirsiniz.

ŞAHİN BAYZAN İLE SÖYLEŞİ

OCAK 2020

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

Şahin Bayzan: Aslında 1990'lı yıllarda "siber güvenlik" kavramı vardı ama popüler değildi. Olmaması da çok normaldi çünkü siber güvenlik, İnternet başta olmak üzere bilişim teknolojilerinin gelişmesiyle popülerlik kazandı. Çift taraflı bilgi alışverişinin yaygınlaşmasına imkân veren web 2.0 teknolojisinin hayatımıza girmesiyle daha anlamlı hale geldi. Gerçek hayatta olan birçok şeyin sanal ortama yani İnternet'e taşındığı bir dünyada yaşıyoruz. Halihazırda çoğu işimizi çevrim içi (online) olarak yapıyoruz. Çevrim içi bankacılık işlemleri, e-Devlet işlemleri, çevrim içi alışveriş, bilet satın alma ve benzeri birçok işlemi bunları yapabileceğimiz sistemlere, platformlara bağlanarak yapıyoruz.

Bu sistemlerin bir an için durması demek, birçok işlemin aksaması anlamına geliyor. Dolayısıyla bu sistemlerin durmaması ya da birileri tarafından durdurulmaması için korunması gerekiyor. Dışarıdan gelebilecek tehditlere karşı bu sistemlerin ayakta tutulması gerekiyor. Gerçek hayatta bir bankayı korumak için güvenlik görevlisi vardır, iş merkezlerini korumak için güvenlik vardır. Daha da güvenli olabilmesi için güvenlik kameraları vardır. İşte çevrim içi olarak bağlanarak işlem yaptığımız sistemlerin de güvenlik görevlisi, güvenlik kamerası olması gerekir.

Güvenlik kameraları, sistemlere giriş ve çıkışları gözetleyen, şüpheli işlemlerde uyarı veren uygulamalar, yazılımlardır. Sistemlere dışarıdan yapılan saldırıları bertaraf etmek için çalışanlar da sistemlerin verdikleri uyarılara karşı tedbir alanlar da bu sistemlerin bir anlamda güvenlik görevlisi olan "siber güvenlik uzmanları"dır. Aslında bu alanın çok dikkat isteyen, ilgi ve bilgi isteyen bir alan olduğunu net olarak ifade etmemiz gerekiyor. Bir hevesle başlanabilir fakat bu heves dikkat ve bilgi ile desteklenmezse pek fazla bir anlam ifade etmeyebilir. Bu yöndeki hevesinizi, bilgi ile destekleyerek hedef haline getirmeniz gerekiyor. Onun için hevesi olmayan yapmasın, hevesi olan da bu alanda en iyi olma hedefine ulaşmak için bilinmesi gerekenler konusunda kendisini çok iyi yetiştirsin.

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

Ş. B.: Öncelikle adayın bu alana ilgi duyması gerekiyor. İlgi duymak tek başına yeterli değil elbette. İlginizi, bilgi ile desteklemeniz gerekiyor. Bilgi ile desteklenmeyen ilgiler genellikle kişiyi ileriye taşıyamıyor maalesef. Öncelikle bu alanın olmazsa olmazlarını bilmeniz gerekiyor. Bu alandaki temel kavramları, bunların ne anlama geldiklerin araştırıp öğrenmekle işe başlayabilirler. Bilgisayar sistemlerini, işletim sistemlerini, ağ sistemlerini ve bunların işleyişini öğrenmesi gerekiyor. Sistemlerin birbiriyle nasıl konuştuklarına yani nasıl haberleştiklerine vakıf olması gerekiyor.

Şöyle düşünün: Her insan bir kişilik barındırır ve her insanın zayıf ve güçlü yanları vardır. O kişiyi kontrol edebilmeniz için kişiliğini, zayıf ve güçlü yönlerini çok iyi bilmeniz gerekir. Bilmeniz gerekir ki ona hükmetmeniz kolay olabilsin. Bilgisayar sistemleri de buna benzer. Bu sistemlerin de tıpkı insanda olduğu gibi güçlü ve zayıf yönlerini çok iyi bilmek zorundasınız. Onun için de önce temel bilgilerden başlanarak adım adım ilerlenmesi, öğrenilenlerin de uygulamalarla desteklenmesi gerektiğini düşünüyorum.

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

Ş. B.: Ben 1993 yılında okumak istediğim bölüm tercihini yaparken hiç kimse beni yönlendirmedi. Zaten bizim zamanımızda yani 90'lı yılların başında bu yönde bize rehberlik yapacak kimse de yoktu. O günün kısıtlı imkânlarıyla, mesleklerle ilgili araştırmayı ben kendim yapmıştım. Hatta tercihlerimi kendim yapmıştım, kimseyi de tercihlerime karıştırmamıştım. İnternet yoktu. Öyle şimdiki gibi anında bilgiye ulaşmanız mümkün değildi. İlk bilgisayar mühendisliği bölümü 1977 yılında ODTÜ ve Hacettepe'de açılmıştı. Sonrasında bunu 1980 yılında İTÜ, 1982 yılında Ege ve Yıldız Teknik Üniversitesi takip etmişti. 90'lı yılların başından itibaren de bilgisayar mühendisliği daha da popüler olmaya başladı. Sonraki yıllarda da daha bilinir oldu. Sadece bilgisayar mühendisliği bölümünü bitirenler siber güvenlik uzmanı olabilir gibi bir yanlış anlaşılma olmasın lütfen. İlgisi alakası olan fakat daha çok mühendislik bölümlerinden mezun olanlar bu alana daha yatkın oluyorlar diyebilirim. İstisnalar kaideyi bozmaz. Elbette diğer bölümlerden mezun olanlar da pekâlâ siber güvenlik uzmanı olabilir. Zaten siber güvenlik alanı, spesifik olarak tek alan değil birçok alanla iç içe. Gelelim bana: 1993'te 530 matematik puanı almıştım, %2'lik dilimdeydim ve ilk 5 tercihim şu şekildeydi:

1. Yakın Doğu Üniversitesi Bilgisayar Mühendisliği (İngilizce-Burslu)
2. Yakın Doğu Üniversitesi Elektrik-Elektronik Mühendisliği (İngilizce-Burslu)
3. Doğu Akdeniz Üniversitesi Bilgisayar Mühendisliği (İngilizce-Burslu)
4. Doğu Akdeniz Üniversitesi Elektrik-Elektronik Mühendisliği (İngilizce-Burslu)
5. Uludağ Üniversitesi Tıp Fakültesi – Tıp

Aslında bugün bir tıp doktoru da olabilirdim. Tıp doktoru olsaydım siber güvenlik alanına ilgi duyar mıydın diye sorarsanız, "Neden olmasın?" derim.

C. U.: İlgi duyduğunuz anı hatırlıyor musunuz? Sizi bu alana çeken "şey" ne oldu?
Ş. B.: İlgi duymak çok farklı bir şey. Eğer bilişim teknolojilerinin içindeyseniz bir noktadan sonra merak edip ilgi duymaya başlıyorsunuz. Bugün hemen hemen hepimiz sistemlere bağlanıyoruz. Sistem derken bu banka sistemi de olabiliyor, e-Devlet sistemi veya sosyal medyayı kullanırken bağlandığımız sistemler de. Bu sistemler milyonlarca kullanıcı bilgisi barındırır. Belki de o sistemlerde tanımlanmış kişiye ait kredi kartı ve hesap bilgileri de var. Bu sisteme yetkisi olmadığı halde giren ve milyonlarca kişinin bilgisine erişen, hatta bilgileri çalarak kötü amaçla kullananlar olduğunu düşününce hem korkuyorsunuz, hem de nasıl olur böyle bir şey diyorsunuz. Neden olmasın ki? Bunun evimize hırsız girmesinden mekân dışında hiçbir farkı yok ki. Ama ilgi ve merak uyandırıyor değil mi?

Evimizi korumak için tedbirler alıyoruz. Örneğin, sitede kalıyoruz. Site güvenli olsun diye güvenlik görevlisi alıyoruz, çalıştırıyoruz. Kameralar koyuyoruz ve izlenmesi gereken alanları takip ettiriyoruz. Büyük bir sitede yaşayan binlerce kişi var ama bugün bizim kullandığımız elektronik sistemlerde ise milyonlarca kişi var. Sosyal medyada kullanıcı bilgileri, bankalarda müşteri bilgileri, e-Devlet sisteminde vatandaş bilgileri, sağlık sisteminde kişilere ait sağlık bilgileri. Dolayısıyla bu kadar değerli bilginin korunması da şart oluyor. Tüm bunları düşününce ister istemez sizi bu alana çeken bir şeyler oluyor.

Adını vermeyeyim, ben 2014 yılında bir bankadan aldığım kredi kartı bilgilerimi çaldırmıştım. Artık alışveriş yaptığım ve farkına varamadığım güvensiz bir İnternet sitesi mi kullandım ya da birileri farklı yollarla mı ele geçirdi bilemiyorum ama bir şekilde bu bilgilerimi çaldılar. Öncesinde kredi kartını aldığım bankayı defalarca uyarmıştım. "Yaptığım her alışverişte bana bilgilendirme mesajı gönderin. Benim istemim dışında yapılacak yüklü alışveriş olursa kartı bloke edin." diye. Bunların hiç birini yapmadılar. Sonuçta kartımdan yurt dışı kaynaklı 6500 dolar alışveriş yapıldı. Hatta unutmuyorum, bu olayın olduğu gün radyoda İnternet'te kredi kartı dolandırıcılığı diye bir radyo programı yapacaktık. Benim için unutulmaz bir durum olmuştu. Sonuçta banka zararımı karşılasa da böyle bir olumsuz durum yaşamıştım. Şimdi düşünün benim gibi kart kullanan milyonlarca kişi var ve bu kart bilgilerini girdikleri sistemler var. Bu sistemlere izinsiz nasıl girilebildiği, nerede güvenlik açığı olduğu ister istemez insanın ilgisini çekiyor.

C. U.: Vazgeçmeyi düşündüğünüz an oldu mu? Oldu ise sizi yeniden devam etmeye iten motivasyonunuz ne idi?
Ş. B.: Önemli bir şey yaptığınızı hissetmiyorsanız vazgeçebilirsiniz. "Binlerce kişinin verisinin bulunduğu sistemleri koruyan ve izinsiz erişimleri önleyecek çözümler üreten birisi olarak ben pek de önemli bir şey yapmıyorum." diye nasıl düşünebilir açıkçası anlamak zor. Bu iş, sadece bir sistemin güvenliğini sağlamak değil ki. Belki birileri bu sisteme giremeyecek ama bu sistemi durdurmaya çalışacaktır. Dolayısıyla sistemi durdurma girişimlerini de savuşturmak gerekiyor. Bugün e-Devlet sisteminde vatandaşlarımızın bilgisi bulunuyor, sağlıkla ilgili verileri bulunuyor. Bu verilerin güvenliğini sağlamakla vatanın güvenliğini sağlamak arasında sadece mekân farkı var. Birisi gerçek hayatta oluyor, diğeri sanal ortamda gerçekleşiyor. Bunun, vatanı sanal ortamda savunmak olduğunu düşünerek bile kişi kendisini motive edebilir. Bağlandığınız sistemlerin, siber bir saldırı sebebiyle belirli bir süre işlev yapamaz olduğunu düşünün. Çoğu işlem aksayacaktır. Bunların yaşanmaması için vazgeçmeyen ve bu alana ilgi duyan liyakatli uzmanlara ihtiyaç var.

C. U.: Dünyada ve özelde ülkemiz için -günümüzde ve gelecekte olmak üzere- kariyer noktasındaki öngörünüz nedir?
Ş. B.: Bugün bana en büyük güç nedir diye sorsanız, ben "VERİ" derim çünkü hemen hemen her şeyimiz sanal ortamda. Dijital olarak bıraktığımız izler devasa büyüklükte bir VERİ kitlesi oluşturmuş durumda. Hemen hemen bugün kullandığımız sistemlerde binlerce kişinin verisi bulunuyor. Bankacılık sisteminde milyonlarca müşteri bilgisi, e-ticaret sitelerinde milyonlarca kişinin kişisel bilgisi, sosyal medya platformlarında milyarlarca kişinin bilgisi bulunuyor.

Bugün bağlandığımız hemen hemen her sistem bizden üyelik istiyor. Bazı bilgileri onlarla paylaşmamız talep ediliyor. Kendi sistemlerini kullandırma şartları bu. Bilginizi verirseniz kullanırsınız, vermezseniz güle güle! "Eğer bir şey bedava ise muhtemelen ürün sizsiniz." diye bir yaklaşımı hepimiz biliyoruzdur. Size bedava ürün sunanlar, sizin hakkınızda bazı şeyleri bilmesi gerekir ki ona göre sizden faydalansın. En azından ilgi alanına göre sana reklam göstersin.

Tüm bunları yaparken senden elde ettiği verilerin korunması noktasında da sana garanti veren sistemlerin elinde bulundurduğu devasa verinin korunmaya ihtiyacı var. Verinin bulunduğu sistemlerin ayakta ve çalışır halde tutulmasına gereksinim var. Dolayısıyla bunu yapacak uzmanlara da ihtiyaç var. Bu açıdan siber güvenliğin gelecekte önü açık istisnai bir meslek ve alan olacağını düşünüyorum. Bu alanda iyi olanlar, kendilerini iyi yetiştirenler de hep bir adım önde olacaklardır. Hatta tıp gibi çok havalı olmasa da ona yakın havalı bir meslek olacağını söyleyebilirim.

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

Ş. B.: Siber güvenlik alanında gözlem ve dikkat oldukça önemlidir. En küçük ayrıntılara dikkat etmek zorundasınız. Zaman gelir küçük bir karakter bile çok belirleyici hatta yıkıcı olabilir. Elinizde tuttuğunuz bir merminin zararı olmayabilir ama onu namluya verdiğiniz ve tetiğe bastığınız zaman öldürücü olabilir. Tek başına kullanılmayan bir komut da böyledir. Bu komutu bir sisteme saldırı amaçlı kullanırsanız sistem için öldürücü olabilir. Aynı komutu binlerce kişinin aynı sisteme saldırı amaçlı kullandığını düşünürseniz ne kadar öldürücü ve susturucu olduğunu anlayabilirsiniz.

Onun için saldıranın kullandığı araçların da saldırılan sistemlerin de çok iyi bilinmesi gerekiyor. Bu noktada bahsettiğiniz başlıkların hepsi ayrı ayrı önem taşıyor. Yazılımı bilmelisiniz, yazılımdan önce yazılımın mantığını bilmelisiniz. Bu mantığı bilmek için de algoritmayı bilmek zorundasınız. Algoritma, bir işin yapılışının sözlü olarak anlatılması işidir. Yazılım ile algoritmada söylediklerimizi, o yazılım dilindeki komutlarla elektronik ortamda ortaya koyuyoruz.

Bu arada her komutun arkasında bir yazılım dilinin olduğunu, bir programlamanın olduğunu unutmamak gerekiyor. Temel bilgileri öğrendikten sonra, işletim sistemlerini, ağ sistemlerini, web teknolojilerini, güvenlik amaçlı kullanılan yazılımların kabiliyetlerini bilmek gerekiyor. Ben temelden özele doğru bir sıra takip edilmesini öneriyorum. Elbette bunları yaparken uygulamayı da ihmal etmemek gerekiyor.

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

Ş. B.: Bir şeyi en iyi şekilde veya daha iyi öğrenmek istiyorsanız onu başkalarına da anlatın. Evet, bir şeyi daha iyi öğrenmenin yolu, başkalarına anlatmaktır. Bazıları maalesef bu konuda cimri davranabiliyor. "Benden öne geçmesin, benden daha iyi olmasın, zirvede ben kalayım." mantığında hareket edenler oluyor. Bana çok saçma geliyor bu. Biliyorsan, bilginden bir başkasını faydalandırman gerekir. Ben, bilgisinde

cimrilik yapanların bir müddet sonra körelmeye başlayacağını düşünüyorum.

Bazen çok iyi bildiğimiz şeylerde bile yeni şeyler öğrenebiliyoruz. "Vaay!" diyoruz "Bu da varmış.". "Bu zamana kadar nasıl öğrenememişim?" diye de hayıflandıklarımız oluyor. Bu böyle bir şey. İnsan öğrenmeye açık olduğu müddetçe mutlaka bir şeyler öğrenir. Yeter ki alıcıları her daim açık olsun. Merak etsin ve araştırsın. Hatta hiç çekinmeden, bilmediğine "Bilmiyorum." desin ve bunun peşine düşsün. Çok şey kazandığını zamanla fark edecektir.

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

Ş. B.: Mesela hızlı karar verebilme çok önemlidir. Örneğin, bir futbol maçını kazanmak istiyorsunuz ama gol yemişsiniz. Gol atmanız lazım ki kazanabilesiniz. İşte tam bu noktada teknik direktörün oyuna müdahale etmesi lazım. Kazanmak adına bir şeyler yapması lazım. Hücuma dayalı mı yoksa savunmaya dayalı mı oynayacak buna karar vermesi ve buna göre oyuncu değişikliği yapması lazım. Bir sistemden sorumlu siber güvenlik uzmanı da herhangi bir siber saldırı durumunda hızlı karar verip savunma yapmak mı yoksa hücum etmek mi buna hızlı harar verebilmeli. Pratik düşünme, hızlı karar verme, insan eğilimlerini, davranışlarını analiz edebilme gibi özellikler adayları bir adım öne çıkaracaktır. Tabii siber güvenlik alanının hukuk, sosyal bilimler gibi birçok alanla iç içe olduğunu unutmamak gerekiyor.

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

Ş. B.: Bilmesi gereken teknik bilgileri bildiğini varsayarak çok yönlü düşünüp hızlı karar verebilmeli ve bu kararını hızlıca uygulamaya geçirebilmedir. Bunu desteklemesi açısından da dikkat ve ince ayrıntıları kaçırmama gibi özellikleri sayabilirim.

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

Ş. B.: En az 1-2 yazılım diline hâkim olma, sistemlerin ha-

berleştiği ağ sistemlerini bilme, siber güvenlikte kullanılan güvenlik uygulamalarına hâkim olma, işletim sistemleri ve sunucu sistemlerine hâkim olma gibi birçok yetkinliği bir arada taşımanız gerekiyor. Zaten bu alanda çalışırken zamanla çok şeyi öğreniyorsunuz, leb demeden leblebiyi anlayacak noktaya geliyorsunuz.

C. U.: Ulusal ve uluslararası sertifika programlarında nasıl bir yol izlenmelidir?
Ş. B.: Evet, bu alanda yetkin olduğunuzu ispat etmenin önemli göstergelerinden birisi ulusal ve uluslararası sertifikalar. Şunu da özellikle ifade etmem gerekiyor: Sertifikayla orantılı olacak pratik bilgiye sahip olmak zorundasınız. Sınavını geçerek sertifikayı aldığınızda, bu sertifikanın hakkını uygulamada yaptığınız çalışmalarla verebiliyor olmanız gerekiyor. Bu tür programlarda özellikle öğrenilenlerin uygulamaları olarak gösterildiği, teorik bilginin pratiğe döküldüğü programların tercih edilmesini öneriyorum. Pratik bilgilerin verildikten sonra hiçbir uygulama yapılmadan yapılan sınavlarla alınan sertifikaların benim için bir soru işareti olduğunu söylemem gerekir. Bir taraftan da bu tür programların çok sıkı, çantada keklik olmadığını da belirtmeliyim.

C. U.: Ve diploma konusu! İlgili ön lisans veya lisans bölümlerinden mezun olmamak bir eksiklik midir?
Ş. B.: Sertifika konusunda herhangi bir mezuniyet şartı aranmadan siber güvenlik kursları alınabildiğini biliyorum. Bununla birlikte belirli bir altyapı olmadan bunun olabileceğine de ihtimal vermiyorum. Onun için de bu tür programlara başvuranların belirli bir altyapısı olduğunu düşünüyorum ya da olması gerektiğine inanıyorum. Bir eksiklik olduğunu söyleyemem ama temel bilgileri bilme noktasında, bireyin bir alt yapısı olması noktasında bunların olması gerektiğini de ifade etmek isterim.

C. U.: Bilimsel düşünce ve güvenlik yaklaşımında ufuk açtığını düşündüğünüz kitap, film öneriniz neler olurdu?
Ş. B.: Zor Ölüm 4, Ratter, Open Windows, Friend Request, Eagle Eye, Nerve, Disconnect, Algorithm, Blackhat, The Net, Hackers, The Fifth Estate, Transcendence, Signal, Anonymous, Swordfish, Sneakers, WarGames, 23, Snowden, We Are Legion: The Story of the Hacktivists, Enemy Of State, Who Am I, Enigma, Track Down, The Matrix, The Score, The Italian Job, Untraceable, Mr. Robot, Watch Dogs 1 ve 2.

C. U.: E-bültenlerle birlikte portal, blog, forum sitesi gibi web platformlarından hangilerinin takip edilmesini önerirsiniz?
Ş. B.: Bu dergiyi (Arka Kapı'yı) takip etsinler. E-Dergi Turk Hack Team, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, CyberMagOnline.

C. U.: Ülkemizde ortaokul seviyesinden üniversiteye değin siber güvenlik yarışmaları düzenlenmektedir. Adayların, bu gibi yarışmalara katılmalarında ne gibi fayda görüyorsunuz?
Ş. B.: Bu alandaki uzmanlarla tanışma noktasında çok olumlu olacağını düşünüyorum. Bu konuda ne kadar çevreniz olursa o kadar şanslısınızdır. Bilgisi olanlarla etkileşimde olmak her zaman kazandırır. Hem bilgi noktasında hem de kariyer noktasında.

C. U.: Sektörel bazlı çevre oluşturmak adına çevrim içi sosyal ağlar nasıl etkin kullanılabilir? Yanı sıra topluluklarca düzenlenen etkinlikler, buluşmalar gibi organizasyonların adaya sağlayacağı katkıları nasıl yorumluyorsunuz?
Ş. B.: Sosyal ağlar farklı alanlardaki uzmanlara ulaşmanın ve soru sormanın en kolay ve pratik yolu. Özellikle bu alanda çalışan kişileri takip etmeyi tavsiye ediyorum çünkü güncel gelişmeleri ve bu alanda yapılacak etkinlik, eğitim programları vb. duyurulara bu vesileyle ulaşabilirsiniz. Ayrıca sosyal medyada bu alanda bilgi paylaşımında, ilişkisi olduğunu ifade etmiştim. Bu alanlardan biri de bilişim hukuku. Sistemlere saldırmanın, sistemleri bozmanın, sistemlerdeki verileri ele geçirmenin bir bilişim suçu olduğunu çoğumuz biliyoruz. Siber güvelik uzmanının bilişim hukuk alanındaki mevzuatı bilmesi gerektiğini düşünüyorum. Aday öğrenciler, sistemleri hacklemenin cazibesine kapılıp yasa dışı olarak bir sisteme girmenin suç olduğunu bilip ona göre davranması gerekiyor. Örneğin, beyaz şapkalı hacker olabilirler. Sistemlerin güvenlik açıklarını, sistem zafiyetlerini tespit edip ilgili kurumlara bildirmeleri onlara itibar kazandıracaktır. Belki de bu yaptıklarıyla kullanıcılar için büyük bir tehlikenin önlenmesini sağlayacaklardır.

bulunan, etkileşimli sosyal medya gruplarına, forumlara katılmanın faydalı olacağına inanıyorum.

C. U.: Hatırlatmakta fayda var: Yasaların iyileştirilmesiyle birlikte, Türk Ceza Kanununca, işlenen bilişim suçları cezai yaptırıma tabi tutulmaktadır. Bu husus da göz önüne alındığında, aday, öğrendiklerini uygulama safhasında nelere dikkat etmelidir?
Ş. B.: Siber güvenliğin farklı disiplinlerle, alanlarla iç içe olduğunu

C. U.: Son olarak, bu okumayı bitirdikten hemen sonra ne yapmalarını önerirsiniz?
Ş. B.: İlginiz varsa "harekete geçin". Konuyla ilgili temel bilgileri öğrenin. Bulabiliyorsanız bu alanla ilgili kitapları okuyun. Bu alanla ilgili İnternet'te araştırma yapın. Bu alan uzmanlarını sosyal medyada takip etmeye başlayın. Konuyla ilgi forumları inceleyin. Faydalı olacağına inandığınız sosyal medya gruplarına katılın. Tavsiye ettiğim filmleri de izlemeyi ihmal etmeyin. Filmlerin yaşa uygunluğunu https://www.commonsensemedia.org/ adresinden sorgulamayı da unutmayın lütfen.

cyberthint

siber tehditlere karşı
erken tanı

Cyberthint, siber uzayda, şirketinizin ve çalışanlarınızın etkilenebileceği **siber tehdilere karşı önceden önlem alınmasını sağlayan** gelişmiş bir siber tehdit istihbarat platformudur.

Cyberthint hakkında daha fazla ayrıntı ve ücretsiz demo talebi için **https://seccops.com/cyberthint/** sayfamızı ziyaret edebilirsiniz.

seccops

www.seccops.com – info@seccops.com

seccops seccops seccops

Serhan W. Bahar / w.serhanbahar@protonmail.com

Gizlilik Aşkına!

Gizlilik Yazı Dizisi - I

İnternet. Sekiz harflik bu kelime insanoğlunun yaşamını hiç olmadığı kadar değiştirdi. Emekleme döneminden bu yana İnternet, insanların birbirleriyle 7/24 iletişim halinde kalması için çabaladı. 2020'li yıllara gelmişken bu amacına ulaşan "İnternet" beraberinde de birçok sorunu hayatımıza sokmuş oldu. Temel sorunumuz olan "gizlilik" ile tanışın.

Akşam evde eşinizle oturduğunuzu hayal edin. Derin bir sohbet var. Bir yandan flörtleşiyor bir yandan özel konular konuşuyorsunuz. Kendi evinizde olduğunuz için çok rahatsınız. Nasılsa kimse sizi duyamaz. Ertesi gün işe gittiniz ve sohbete e-posta veya mesajlaşma uygulamasından devam etmek istediniz. Peki sizi izleyenlerin farkında mısınız? Tüm konuşmalarınızın, yazışmalarınızın ve tüm hareketlerinizin (loglar) kaydedildiğini ve incelenebileceğini biliyor musunuz?

İşte şimdi olay rahatsız edici bir hal almaya başladı. Peki "İnternet" bunu bilerek mi yapıyor? Elbette hayır. İnternet, doğası gereği makinelerin birbirleriyle iletişim kurabilmesi için bazı protokollerle çalışır. Ve tüm bu protokoller insan elinden çıkma olduğu için insanoğlunun gözlemleri sonucu insan iletişimine en benzer şekilde oluşturulmuştur.

Bu yazı dizisinde tamamen gizliliğe odaklanacağız. Gizliliğin tüm yönlerini A-Z'ye masaya yatırırken kendimizi gözetlenmelerden nasıl koruyacağımıza dair teknikleri tek tek inceleyeceğiz.

Yazımızın son bölümünde ise uçtan uca nasıl anonim kalacağımızı örnek bir senaryo ile sizlere sunacağız.

Bölüm 1: İnternet'in Gizlilik Karşıtı Evrimi

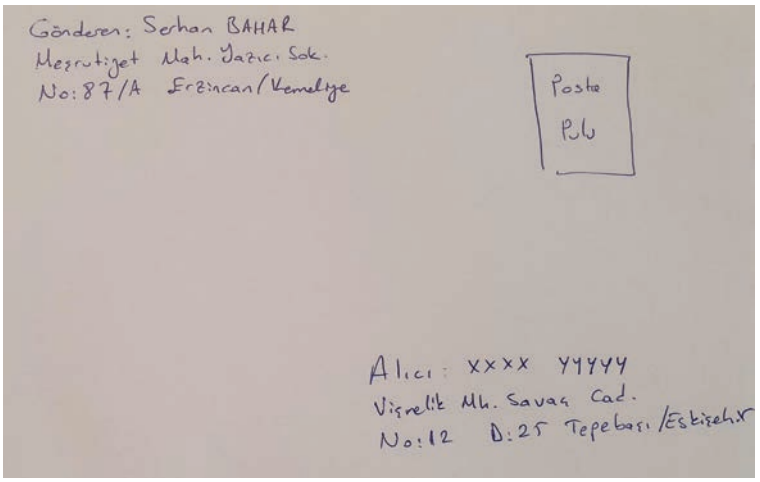
İnternet'in nasıl çalıştığını anlamak onu daha verimli ve doğru şekilde kullanabilmek için çok önemlidir. Eğer İnternet'te gizli kalmak istiyorsanız öncelikle İnternet'in bunun için yapılmadığını bilmeniz gerekir.

Eğer "İnternet'te gizliliğim önemli değil" diyenlerdenseniz hemen sayfayı çevirip daha ilgi çekici yazıları okuyabilirsiniz ancak bu dergiyi okuduğunuza göre gizliliğin sizin için değerli ve önemli olduğunu düşünüyorum.

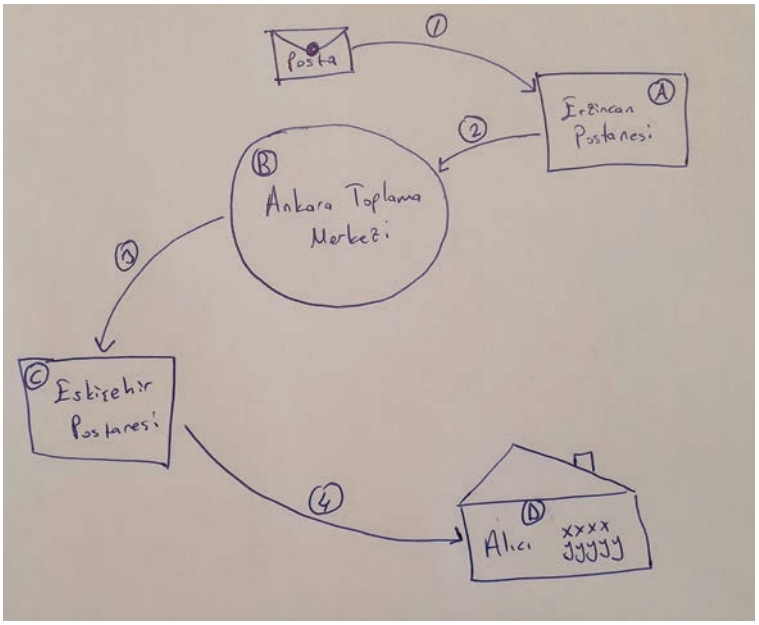
Derinlere doğru gidecek olan yolculuğumuza başlamadan önce İnternet nasıl çalışır kısaca anlamaya çalışalım.

Yazının başında da belirttiğimiz gibi İnternet aslında bildiğimiz insan iletişimine çok benzer. Bunu bir metaforla pekiştirmeye çalışalım.

Yıl 1980. Erzincan'da askerlik yapıyorsunuz. Nişanlınız ile 3 aydır iletişim kuramadınız. Heyecanla ona olan özleminizi bir mektup yazarak belirtmek istediniz. Bir yandan inanılmaz bir soğuk var ve yazdığınız mektubu postaneye götürene kadar iliklerinize kadar üşüdünüz. Postaneye vardığınızda aşağıdaki gibi bir zarf içinde mektubunuzu teslim ettiniz.



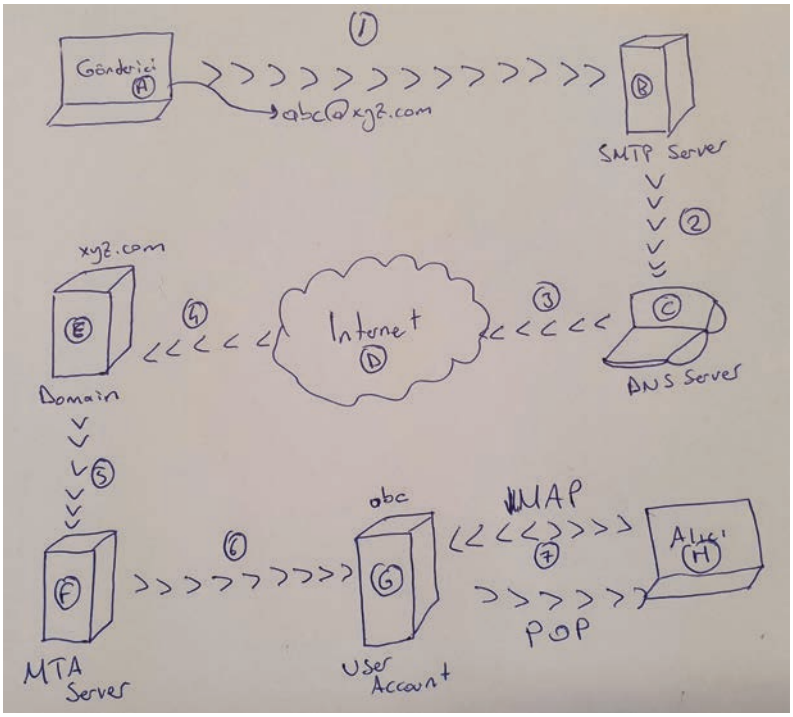
Bu mektubu teslim ettiğiniz yer Erzincan'da bir postane. Gideceği yer ise Eskişehir'deki postane. Şimdi bu akışı bir inceleyelim. Erzincan'dan gece yola çıkan mektubunuz önce Ankara'da bulunan toplama merkezine ulaşıyor. Daha sonra oradan da yola çıkıp Eskişehir'deki postaneye ulaşıyor. Postanede postacıya verildikten sonra alıcımız olan xxxx yyyy'ye ulaşacak. Bunu bir de çizerek görelim.



Bu görseli incelersek eğer, ellerimizle özene bezene yazdığımız ve içerisinde çok özel şeyler içeren aşk mektubumuz 4 farklı yolculuğa çıkıyor ve 3 farklı duraktan geçerek alıcımıza ulaşıyor. Postamız 1 numaralı yolculuğunda güvenli çünkü henüz biz taşıyoruz. Ancak A noktasına postamızı teslim ettiğimizde artık bizden çıkmış oluyor.

A, B ve C noktalarında kötü niyetli birinin olması halinde postamız okunabilir. Hadi oralarda güvenlik mükemmel seviyede olsun ve okunması engellendi diyelim. 2,3 ve 4 numaralı taşıma esnasında mektubumuz yine okunabilir. Doğal olarak burada bir gizlilik beklemek mümkün değildir. Bu şekli görüp de yok hala benim postam okunmaz diyorsanız büyük bir hayal kırıklığı sizi bekliyor çünkü bu konuda resmi bir açıklama olmasa da birçok devletin zamanında savaş ve benzeri durumlarda mektupları tek tek okuduğuna dair söylentiler vardı. Sonuç olarak burada postamızın okunabilir şekilde olması bir zafiyettir ve okunmayacağı anlamına hiçbir zaman gelmemektedir.

İşte İnternet de buna benzer şekilde çalışır. Sıcacık evinizde kapınız kilitli ve güvenli bir şekilde otururken bir iş ortağınıza çok gizli projeniz ile ilgili bir e-posta attığınızı varsayalım. Bu e-posta okunabilir mi? Başkaları tarafından ele geçirilebilir mi? Veya yaşadığınız ülkedeki ISP, hükümet veya size hizmet veren e-posta servis sağlayıcınız bu e-postayı okuyabilir mi? Hadi bunu da çizerek kontrol edelim. Örnek olması açısından en standart şekliyle inceliyoruz:



Bu görsele yakından baktığımızda tıpkı posta gönderdiğimizde olduğu gibi bir çok yolculuktan ve duraktan geçiyor. Şimdi burayı yorumlama işini size bırakıyorum. Göndermiş olduğumuz e-posta (PGP gibi özel teknikler kullanılmadığı takdirde) 7 farklı yolculuk ve 7 farklı durakta sizce okunabilir mi?

İşte tam olarak bu yüzden gizliliğin ne demek olduğunu öğrenmemiz gerekiyor. Bunun için de ilk bakmamız gereken şey IP adresleri olacak.

Ancak henüz o kısma girmeden önce gizlilik konseptimizin üzerinden bir geçmemiz gerekiyor. Birlikte aşağıdaki senaryomuzu inceleyelim:

"Bir çevre aktivisti olan Ayşe son zamanlarda devletin almış olduğu kararlara karşı bir bildiri yayımlamak istiyor. Ancak bunu yaparken hukuki anlamda sorun yaşamak istemediği için de İnternet'te anonim kalmak istiyor. Hemen cüzdanını çıkartıp kredi kartını eline alıyor ve en iyi VPN hizmet sağlayıcılarından birine aylık 5$ ödeyerek abone oluyor. Daha sonra yine en iyi denilen ve çok güvenli mail sağlayıcılarından birine 5$ daha ödeyerek ona da abone oluyor. Daha sonra evinden bu VPN'e bağlanıp arkadaşının Gmail'ine yayımlamayı düşündüğü manifestoyu ultra güvenli mail olarak gönderiyor. Daha sonra şahsi Twitter hesabına tam tamına 5$'a satın aldığı ve asla log tutmadığı iddia edilen VPN ile bağlanıp manifestoyu yayımlıyor."

Ne kadar güvenli değil mi? Peki aşağıdaki sorulara cevap vermeye çalışarak anonim olup olmadığımızı kontrol edelim.

1. Manifesto kimin Twitter adresinden yayımlandı?

2. VPN'e giden bağlantı kimin IP adresiydi?

3. Mail gönderen kimdi?

Apaçık ortada. İnternet gizli kalmak üzerine tasarlanmamıştır. Bu yüzden de tam anlamıyla gizli kalmak hiçbir zaman mümkün değildir. Ancak gizli kalmak yerine bir başkası olmak mümkündür. Bu yüzden gizlilik yazı dizisinde konseptimizi tamamen bir başkası olmak üzerine kurguladım. Eğer anonim kalmak istiyorsanız sizden tamamen bağımsız, sizinle hiçbir şekilde bağlantısı kurulamayacak hayali bir karakter yaratmanız gerekiyor. Bu karakteri nasıl yaratacağınızı yazı dizimizin son bölümünde her şeyi birleştirerek açıklayacağız. Bunu yapmadan önce temelde anlamamız gereken şeylerin üzerinden geçmemiz gerekiyor.

Bu bölümde göz atacağımız konular:

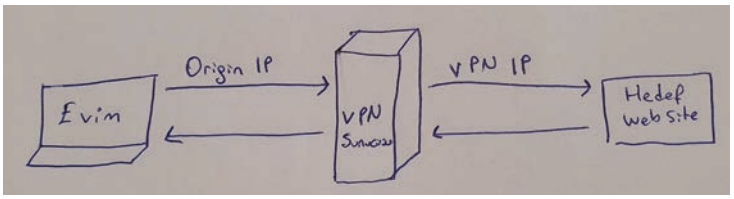
1. VPN Hizmetleri
2. Tor Project
3. İnternet'te Gezinme
4. Anonim Hesaplar
5. Sosyal Mühendislik
6. Fiziksel Yaşam
7. Sonuç

1. VPN Hizmetleri

VPN'in açılımı Virtual Private Network yani Sanal Özel Ağ'dır. Daha önce örneğini verdiğimiz mektup yollama hikayemizi düşünün. Tıpkı onun gibi çalışır aslında. Mesela evinizden www.serhanbahar.com'a bağlandığınızda eğer VPN kullanmıyorsanız direkt olarak benim websitemin loglarına kendi origin IP adresinizi bırakmış olursunuz. Ancak VPN kullandığınızda www.serhanbahar.com'a bağlanmadan önce bu VPN sunucusuna bağlanırsınız ve VPN üzerinden benim websiteme ulaşırsınız. Bu sayede websitemin loglarında sizin origin IP adresinizi değil VPN sunucusunun IP adresini görmüş olurum.

Çok güvenli görünse de bunun da bazı sorunları var. Mesela VPN sağlayıcınız log tutuyor mu? Her ne kadar tutmadıklarını iddia etselerde 5-10 dolara satın aldığınız VPN hizmetleri ne kadar güvenilir olacaktır? Log tutmalarını geçtim (ki bunu geçmemek lazım en önemli kısım burasıydı) direkt olarak origin IP'nizden VPN'e bağlandığınız için VPN sağlayıcınız sizin verilerinizi başkaları ile paylaşırsa gizlilikten eser kalmamış demektir.

Hadi VPN nasıl çalışır kısaca çizim üzerinden de bakalım.



VPN sayesinde origin IP adresimizi bağlandığımız yerlerden saklayabiliyoruz. Çoğu senaryoda VPN güçlü bir seçenektir. Ancak tamamen gizlilik ve koruma sağlamaz.

VPN'i hazır hizmet olarak sunan birçok firma mevcut. Aylık çok cüzi miktarda para ödeyerek bunları kullanabilirsiniz veya daha güvenli ancak daha pahalı (ayda sadece 5$'dan başlayan fiyatlarla) bir seçenek olarak kendinize bir sunucu kiralayarak kendi VPN'ininizi kendiniz kurabilirsiniz. Her iki seçeneği yapacak da olsanız dikkat etmemiz gerekenlere hızlıca bir göz atalım.

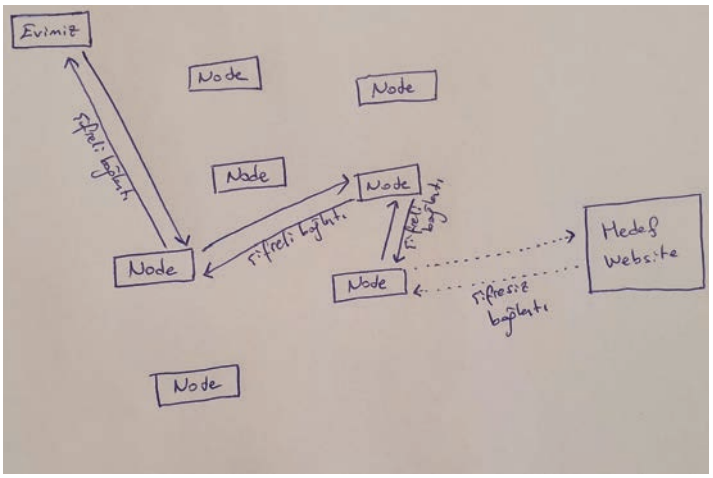
- VPN sunucusu her hareketimizi loglayabilir. Loglarımızın tutulup tutulmadığını biliyor muyuz? Bundan emin miyiz? Bu loglarımız kimlerle paylaşılıyor?

Yukarıdaki soruların cevabından hiçbir zaman %100 emin olamayacağımız için VPN tek başına mükemmel bir çözüm olmayacaktır. VPN tüm gizlilik sürecimizdeki bir adım olacak.

Son olarak VPN'in gizlilik için değil güvenlik için tasarlandığını unutmamak gerekir. VPN'de temel amaç verilerimizin başkaları tarafından okunmasını, müdahale veya manipüle edilmesini engellemektir.

2. Tor Project

Efsanelerin toplandığı nokta. Kimisi "Dark Net" der kimisi "Deep Web". Ancak Tor projesi eşit değildir dark/deep web. Tor, VPN'e çok benzemekle birlikte ondan gizlilik için tasarlanmış olmasıyla ayrılır. Hadi kısaca Tor nasıl çalışır muhteşem çizimlerimizden biriyle inceleyelim.



Daha kolay anlaşılması açısından bağlantımız hedef websitesine giderken 3 farklı VPN sunucusundan geçiyormuş gibi hayal edebilirsiniz. Çok güvenli gibi gözükse de teoride bağlandığınız node'ların kontrolü ele geçirildiğinde veya ilk node'a gidişiniz ile son node'dan çıkışınızı yakalayabilirlerse trafiğiniz ifşa olacaktır. O nedenle Tor'da tek başına %100 güvenlik ve gizlilik sağlayan bir seçenek değildir. Ancak buradaki güzellik de şu: Her bağlandığınız websitede bu 3 node her seferinde değişmektedir. Bu nedenle takip etmesi çok zordur. Her seferinde değişen 3 farklı node kullanmanın adı da "onion routing"dir. Bu bilgi de ekstra olarak burada dursun.

Peki Tor bu kadar mükemmel mi? Elbette hayır. Gizlilik arttırılmaya çalışıldıkça maalesef bağlantı hızı düşüyor. O nedenle Tor bağlantısı genellikle yavaş çalışır. Sabırsız davranıp Tor bağlantınızı yarıda keser ve trafiğe origin IP'niz ile devam ederseniz rahatlıkla ifşa olabilirsiniz.

Şimdi burada bir tercih söz konusu olacak. Güvenlik ve gizlilik katmanlarını artırabilmek amacıyla genellikle Tor ile VPN birlikte kullanılır ancak bunun da bir sıralaması vardır. Örneğin önce VPN'e bağlanıp sonra Tor'a bağlanabilir veya önce Tor'a bağlanıp sonra VPN'e bağlanabilirsiniz. Ancak her ikisinin de kendince artı ve eksileri söz konusu.

VPN'e bağandıktan sonra Tor'a bağlanırsak:

Burada amaç Tor'a bağlandığımızı gizlemektir.

Artılar:

- Kurulması kolaydır, ileri seviye teknik bilgi gerektirmez.
- İnternet servis sağlayıcınız Tor Network'e bağlandığınızı göremez. Bu nedenle Tor ile sizi ilişkilendiremez.
- VPN sağlayıcınız Tor Node'larına gönderdiğiniz verinin içeriğini okuyamaz sadece node'lara bağlandığınızı görebilir.
- Tor Node'ları sizin origin IP'nizi bilmez bunun yerine VPN IP adresinizi bilir.
- Tor'un gizli servislerine (.onion uzantılı) erişim sağlayabilirsiniz.
- Güvenlik için daha iyi denilebilir(!)

Eksiler:

- Tor'un çıkış node'u ile gittiğiniz web site arasındaki trafik şifresizdir ve okunabilir.
- Tor'un çıkış node'ları genellikle çoğu web sitesi tarafından bloklanmaktadır. Bağlanmak zor olabilir.
- VPN sağlayıcınız güvenilir değilse Tor node'larına giden trafiğiniz ifşa olabilir.

Tor'a bağlandıktan sonra VPN'e bağlanmak

Burada amaç VPN sağlayıcısından origin IP adresimizi gizlemektir.

Artılar:

- VPN sağlayıcınız origin IP adresinizi göremez.
- İnternet Servis Sağlayıcınız VPN'e bağlandığınızı göremez.
- Tor'un bloklanan çıkış node'larından etkilenmezsiniz.
- Lokasyon tespitinin engellenmesi için daha iyidir.
- Gizlilik için daha iyi denilebilir(!)

Eksiler:

- Tor'un gizli servislerine (.onion uzantılı) erişim sağlayamazsınız.
- İnternet Servis Sağlayıcımız Tor ağına bağlandığımızı bilir.
- VPN Tor'a göre daha sömürülebilir bir yapıdır.
- VPN'i nasıl satın aldığınıza bağlı olarak ifşa olabilirsiniz.

Kısaca VPN ve Tor'dan bahsettiğimize göre parçaları birleştirmeden önce diğer konulara da bir göz atalım.

3. İnternette Gezinme

En iyi VPN'i de kullansanız, bunu Tor ile en mükemmel senaryoda da birleştirseniz eğer bu adımları yaptıktan sonra kendiniz ile bağlantı kurabilecek şeyler yapıyorsanız gizlilikten bahsetmenize gerek kalmaz. Örneğin tüm önlemleri aldıktan sonra bir e-ticaret sitesine gidip kendinize ait kredi kartınız ile sipariş verirseniz ifşa olursunuz. Yine tüm önlemleri aldıktan sonra kendinize ait bir hesaba (Twitter, e-mail vb.) login olursanız yine ifşa olursunuz. Gizlilik, sizinle hiçbir şart ve koşulda bağlantı kurulamaması sayesinde var olabilir. Bu nedenle sizinle ilgisi olan hiçbir şeyi bu bağlantılar esnasında kullanmamanız gerekir ve yine bu nedenle bir "hayali karakter" yaratmanız gerekiyor. Gizli kalmak istiyorsanız şahsi İnternet kimliğiniz ile hayali karakterinizin İnternet kimliğini birbirinden tamamen ayırmanız gerekiyor.

4. Anonim Hesaplar

Anonim hesap kime ait olduğu hiçbir şart ve koşulda bilinmeyen hesaptır. Bunu oluşturabilmek biraz sancılı ancak dikkat edildiğinde ve adımlar atlanmadığında yapılması mümkündür.

Kural 1: Asla kendi IP adresinle anonim hesabına giriş yapma!

Kural 2: Anonim hesaplarda asla kendine ait gerçek bilgi kullanma!

Bu iki kurala dikkat ederseniz anonim olma konusunda çok büyük bir adım atmış olursunuz. Bazen telefonuma bir bildirim geliyor. Instagram'da telefon rehberimde kayıtlı olan yaşlı başlı bir tanıdığım fake hesap açmış. Bildirimde de şu yazıyor: Kişi listende bulunan A.... Y… crazyboy_34 kullanıcı adı ile İnstagramda! Ne demek istediğimi anladınız. :)

Kendi telefon numaranızı, e-posta adreslerinizi, banka/kredi kartlarınızı, sosyal medya hesaplarınızı vb. aklınıza gelebilecek ve sizinle bağlantı kurulabilecek hiçbir şeyi anonim hesaplarda kullanmamanız gerekiyor. Yoksa yukarıdaki amcamız gibi 60 yaşından sonra kadın peşine düştüğünüz belli olup rezil olabilirsiniz. :)

Anonim hesap oluşturmanın zorluğu son dönemde popüler olan kyc (know-your-customer) yüzünden arttı. Birçok hizmet sağlayıcı artık sizin cep telefonu numaranız veya sizi tanımlayabilecek bir bilgi olmadan hesap açılmasına müsaade etmek istemiyor. Bu nedenle en önemli 2 kuralımıza geri dönüyoruz. Eğer bir hizmet sağlayıcısı sizin "hayali karakter" için açmak istediğiniz hesaba dair telefon numaranızı veya tanınmanıza sebep olacak bir bilgi istiyorsa o hizmeti kullanmayın. Bu konuda risk almak isteyeceğinizi zannetmiyorum.

5. Sosyal Mühendislik

Her şeyi doğru yapsanız bile ifşa olabilirsiniz. Neden? İnsanın doğası olan hata yapma özelliği yüzünden. Son yıllarda teknik konularda hata yapmayan insanlar genellikle insan ilişkileri sırasında yaptıkları hatalar nedeniyle ifşa oldular. Bu yüzden sizi ifşa etmek isteyen kişiler muhtemelen size karşı sosyal mühendislik saldırıları düzenleyerek sizi ifşa etmeye çalışacaklardır. Bu yüzden "hayali karakter" ile yaptığınız tüm aktiviteler sırasında sizinle etkileşime geçen kişilere dikkat etmenizi öneririm.

Ayrıca sosyal mühendislik dışında korelasyon kurulması sonucu da ifşa olabilirsiniz. Bu nedenle aşağıdaki sorulara yanıt verip bunların sizin alışkanlıklarınızdan tamamen farklı olmasını sağlamanız gerekiyor.

1. Hangi web sitelerini sıklıkla ziyaret edersiniz?
2. Ne kadar hızlı yazarsınız?
3. Kullandığınız dil nasıl? Ne tarz espriler yaparsınız?
4. İnternet'te genel davranış stiliniz nedir?
5. Neleri seversiniz ve bunların hangilerini yansıtma eğilimindesinizdir?

Bu ve buna benzer sizin profilinizi çıkarmaya yarayacak soruları cevaplayarak bunlardan tamamen uzak durmanız gizliliğinizi koruması açısından çok önemlidir.

6. Fiziksel Yaşam

İnternet söz konusu olunca görünmez olduğumuzu zannediyoruz. Birçok insan İnternet sırasındaki bazı aktivitelerini public Wi-Fi'lara bağlanarak yapmayı tercih ediyor. Ancak burada atlanan bir şey var: Tüm önlemleri alsanız da oturduğunuz bir kafedeki güvenlik kameraları sizi ifşa edebilir. 24 Aralık akşamı saat 20.00'da ABC isimli kafeden gönderilen bir mail takip edilmeye başlandığında birkaç şüpheliden biri olmanız işten (bile) değil! Bu nedenle yazıda sürekli vurguladığımız "hayali karakter" yaratma olayını sadece sanal alemde değil fiziki hayatta da çok ciddiye almak gerekiyor.

7. Sonuç

Yeni yazı dizimizin ilk bölümünde temel fikirleri vermeye çalıştık. Amacımız tamamen anonim bir "hayali karakter" yaratarak İnternet'teki gizlilik ve güvenliğimizi sağlamak. Ancak bunu yapabilmek için her adım dikkatlice planlanmalı ve hiçbir adım hiçbir zaman atlanmamalı.

Bir sonraki bölümde işletim sistemlerinin tamamını inceleyerek gizlilik/güvenlik için en ideal senaryoyu oluşturmaya çalışacağız. Bu esnada ifşa olmamaya gayret gösterin çünkü serüvenimiz henüz yeni başladı :)

E.D:

Makalede bahsi geçen kendi VPN sunucunuzu kurma ve TOR ile ilgili iki rehber:

https://arkakapidergi.com/kendi-baglantim-ile-kendi-vpn-sunucunuzu-kurun/

https://arkakapidergi.com/internette-gizli-kalin-the-onion-router/

Sadullah Ali Aslan - ali@hackpress.org

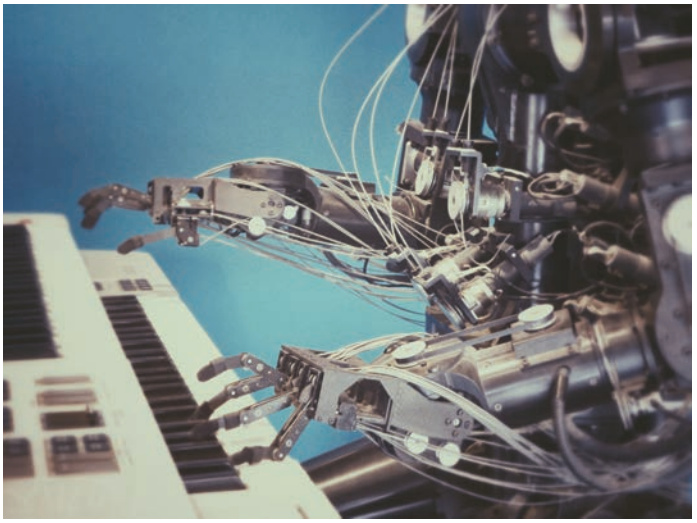
Devletlerin Gözleri: Yapay Zekâ

Zekâ nedir? Hayatta kalmamızı sağlayan bir özelliğimiz mi, canlıların birbirleri üzerinde üstünlük kurmak için kullandığı bir silah mı ya da hayatımızı kolaylaştıran becerilerimizin toplamı mı?

Zekâ nedir? sorusuna cevap vermek elbette ki şahsımı aşan bir durum ancak standart olarak tanımlarsak *"Zihnin öğrenme, öğrenilenden yararlanabilme, yeni durumlara uyabilme ve yeni çözüm yolları bulabilme yeteneğidir[1]"* diyebiliriz. Ancak yazıma başlarken söylediğim *"Zekâ, canlıların birbirleri üzerinde üstünlük kurmak için kullandığı bir silah mı?"* sorusu, bize zekânın farklı odalarının kapısını aralayacaktır. Aralanan kapılardan girdiğimizde ise insanlığın, zekâsını birbirlerine üstünlük kurmak için kullandığını gösteren tablolarla karşılaşacağız. Günümüze kadar yaşanmış tüm savaşların, siyasi ve politik olayların birer zekâ ürünü olduğunu görebiliriz. İnsanlar, zekâlarını diğer insanları alt etmek, onlara üstünlük kurmak için kullanmıştır ve kullanmaya da devam etmektedir.

Günümüzde ise insanlar zekâlarını, bilgisayar sistemlerini geliştirmek ve onları insan gibi düşünen yeni varlıklara dönüştürmek için kullanıyor. Bunun nedeni insan gibi zeki olan, kendi kendine karar verebilen ve diğer insanları geçmeye veya alt etmeye yarayan bir varlığın ortaya çıkartılmasının istenmesidir. Bu varlık, insanlığın geleceğini çok farklı yerlere getirebilecek bir keşif olan "yapay zekâdır". Yapay zekâ, bir bilgisayarın, robotun veya yazılımın zeki varlıklara benzer şekilde davranışlar sergilemesini sağlayan yetenektir. Adından da anlaşılabileceği üzere yapay zekâ, "yapay" bir üründür.

Yapay zekâ, son yıllarda oldukça fazla ilerleme kaydetmiş bir buluştur ancak bu ilerleme medyaya yansıyan haberlerde olduğu gibi bizi "iyi ve güzel bir dünyaya" mı götürecek yoksa, insanlığın "sınırsızca kontrol edilebildiği" bir dünyaya mı? Şimdi kafamızı kaldırdığımızda her tarafta kameraları görüyoruz ve bunlar bizim için bir şey ifade etmiyor değil mi?



Ancak gelecekte o kameraların bizi kontrol etmek için orada olduğunu bilerek yaşadığımızı düşünmek bizim için şimdiden bir şeyler ifade etmeli. O kameraların kimler tarafından konulduğu da şu an bizim için bir şey ifade etmiyor ama gelecekte onun da bir şeyler ifade etmesi gerekecek.

Şimdi bizim, devletlerin insanları yapay zekâyı kullanarak sosyal medyada, sokakta, çalıştığımız şirkette, evimizde ve aklınıza gelebilecek her yerde bizi kontrol etme çabasında olduğunu anlamamız gerekiyor çünkü devletler, bunu yapmanın yollarını aramaya çoktan başladılar ve oldukça iyi mesafe kaydettiler. Bu devletlerden biri olan Çin, ülkenin yönetim biçiminin doğal gerekliliği yüzünden kurulduğu yıllardan itibaren halkını kontrol etmeye çalışıyor. Bunu ilk başlarda geleneksel kontrol mekanizmalarıyla gerçekleştiren Çin, teknolojinin gelişmesi sayesinde bunu yapay zekâ ile yapmaya başladı.

Çin, uyguladığı devlet politikaları sayesinde birçok ülkeyi geride bıraktı ve şu an GSYİH'ye göre dünyanın en büyük

2. Ekonomisi konumunda. Elbette ki bunu başarmak sadece uygulanan ekonomi politikalarının sonucu olmadı. Bunu yapmak için halkın da kontrol edilmesi ve koordineli bir şekilde yönetilmesi gerekliydi. Çin, halkı kontrol etmek için çok kapsamlı yöntemler kullanıyor ve bu yöntemler yapay zekânın yardımıyla gerçekleşiyor. Örneğin "sosyal kredi sistemi" adı verilen bir yapı sayesinde vatandaşlarını "beyaz listedekiler" ve "kara listedekiler" olmak üzere ikiye ayırıyor. Beyaz listedeki vatandaşlar, toplumsal kurallara uyan insanlardan oluşurken, kara listedekiler ise toplumsal kurallara uymayan insanlardan oluşuyor. Beyaz listedekiler, hastane gibi devlet kurumlarında daha az bekleme süresine sahip olabilme, daha fazla iş teklifi alma gibi olanaklardan yararlanabilirken, kara listedeki vatandaşlar uçak bileti alamama, çocuklarını özel okullara hatta üniversitelere gönderememe gibi uygulamalarla karşılaşıyor.

Sosyal kredi sisteminde kullanılan teknolojiler ise son derece gelişmiş sistemler olarak karşımıza çıkıyor zira Çin hükümeti, vatandaşlarını sınıflandırdığı bu sistemde yapay zekânın bir ürünü olan yüz tanıma teknolojisini kullanıyor. Yüz tanıma teknolojisi, akıllı telefonlar gibi çeşitli ürünlerde güvenliği arttırmak için kullanılan yöntemlerden biri olsa da kitleleri takip etmek ve onları sınıflandırmak gibi amaçlar için de biçilmiş bir kaftan olduğundan Çin hükümeti, bu teknolojiyi kullanıyor. Hatta yüz tanıma sistemleri Çin'de öyle yaygınlaşıyor ki ülkede bulunan kameraların sayısı diğer ülkeleri geride bıraktı ve 2022'ye gelindiğinde Çin'deki her iki kişiye bir kamera (CCTV kamerası) düşeceği tahmin ediliyor.[2] Bu kameralar sayesinde Çin hükümeti, sosyal kredi sistemini yönetebiliyor ve yapay zekâdan faydalanmış oluyor.

Çin'in sahip olduğu kitlesel gözetim teknolojileri yalnızca bunları kapsamıyor. Hükümet, "Great Firewall" ile interneti ve sosyal medyayı kontrol edebiliyor. Great Firewall, Çin hükümeti tarafından çeşitli internet sitelerine ve uygulamalara (Google, Twitter, Facebook…) erişimi engellemek için kullanılıyor. Bu siteleri engelleyen yetkililer, onların alternatifleri-ni piyasaya sürüyor. Bu, Çin vatandaşlarının eğer VPN kullanmazlarsa zorunlu olarak hükümet tarafından desteklenen sitelere, uygulamalara veya yazılımlara erişmesini sağlıyor ve böylelikle kullanıcı verileri Çin sınırları içerisinde kalıyor ve veriler hükümetin kitlesel gözetim teknolojilerinin kullandığı big data'yı oluşturuyor. Zaten aslında Çin'in yapay zekâ teknolojilerini kullanmasındaki amaç vatandaşların tüm verilerini kitle gözetim araçlarıyla bir araya toplamak ve bunları halkı kontrol etmek için kullanmak çünkü halkı kontrol etmek, devletin ideallerinin gerçekleştirilebilmesi için gereken iş gücünün ve fikirlerin kontrol edilebilmesine olanak tanır. Çin hükümetinin yapay zekâya dayalı olarak kullandığı bu sistemlerin hepsi Çin'in çok da uzak olmayan bir gelecekte ne kadar büyük ve hiç görmediğimiz bir dünyayı oluşturduğunu gösteriyor. Bu dünya, devletin halkı "sınırsızca kontrol ettiği" bir dünya ve burası öyle tahmin edilemez bir yer ki insanlar kontrol edildiklerinin farkında bile değil. Bahsettiğim dünyanın bileşeni elbette ki sadece Çin'den ibaret değil, Rusya ve ABD gibi büyük devletler de bu dünyanın bir parçası.

Rusya, kitlesel gözetim teknolojilerini kullanan ülkelerden birisi olarak karşımıza çıkıyor ve o da aynı Çin gibi yapay zekâdan yararlanıyor. Rusya'nın sahip olduğu en bilinen sistem SORM (System for Operative Investigative Activities) olarak adlandırılan dinleme sistemidir. SORM ilk olarak 1995 yılında uygulamaya konulmuş ve SORM-1 olarak adlandırılmıştır. SORM-1, mobil ve sabit telefonları dinlemek için kullanılmaktadır. 1999 yılında kullanıma sunulan SORM-2 ise internet trafiğini izlemek için kullanılırken, son yıllarda sosyal medya siteleri de dahil olmak üzere internet ortamındaki her yerde dinleme yapabilen SORM-3 kullanılmaktadır. Rusya hükümeti, bu sistemin uygulanması için ülkedeki ISP'lere çeşitli zorunluluklar getirmektedir ve bu sistem için gereken ekipmanları kurmayan ISP'lere ceza uygulanmaktadır.

Ayrıca Rusya'da dünyadaki bazı ülkelerde de uygulanan "kara liste" tekniği uygulanmaktadır. Bu yöntem ile hükümet, başta pornografi olmak üzere, uyuşturucu ve aşırılık olarak adlandırılan şeylerin bulunduğu internet sitelerini erişime kapatabilmektedir ve bu siteler "kara listeye" alınmaktadır ancak ne yazık ki "kara listeye" alınan siteler sadece topluma gerçekten zararı olan veya olabilecek sitelerden oluşmuyor! Dünya'nın hemen hemen her yerinde olduğu gibi gücü elinde barındıran kişi veya kişiler imkanlar dahilinde kendi güçlerini ve geleceklerini sarsacak fikirlerin yayıldığı internet sitelerini engelleyerek varlığını korumaya çalışıyor ve işte Rusya'da da olan bundan ibaret. Aslında ilk açıdan baktığımızda yani kendimizi bir devlet yerine koyduğumuzda, halkın gerçekten etkilenebileceği kötü içerikleri barındıran internet sitelerini yasaklamak biraz mantıklı bir yöntem gibi gelebilir ancak ikinci açıdan baktığımızda, bir şeyi yasaklamanın kişiler üzerinde o yasağı

delme psikolojisini oluşturduğunu görebiliriz. Bu durumda kişilerin zihni, yasaklı internet sitelerine girmek ve yasağı delmek için bir arzuyla kaplanır zira kilitli ve içerisinde bir şeylerin olduğunu bildiğiniz bir kapıyı açmak her zaman merak uyandıran bir aktivite olmuştur.

Çin ve Rusya'nın ardından belki de popüler kültürde "kitlesel gözetim" denince akla ilk gelen ülke olan ABD'den bahsetmek gerek. ABD için dünyanın askeri, ekonomik ve siyasi güç bakımından en güçlü ülkesi desek herhalde yanılmış olmayız. Dünyadaki hemen hemen her alanda lokomotif olmayı başaran ABD elbette bunu bir talih kuşu sayesinde başarmadı. Bu başarının sırlarından birisi ileri teknolojileri üretmekti. İleri teknolojileri üretmenin sonucu ise hayatın kolaylaşmasının, ülke gelirinin artmasının yanı sıra hükümetin halkı kontrol ve takip etme dürtüsünü arttırdı. Çünkü belirli bir güce sahip olan kişi veya kişiler her zaman ellerindeki imkânları mümkün mertebe kullanmak ister. İşte ABD'de olan da buydu; halkı kontrol etme dürtüsü.

Bu dürtünün sonucu olarak ABD, daha bilgisayarlar keşfedilmeden önce toplumu izlemeye yönelik adımlar atmıştı ancak asıl izleme çalışmaları bilgisayarların ve internetin ortaya çıkmasıyla gerçekleşmişti. ABD'nin kullandığı "kitlesel gözetim" teknolojilerinin birçoğunun varlığı eski CIA ve NSA personeli olan Edward Snowden'ın sızdırdığı belgelerle ortaya çıkmıştı. Snowden'ın sızdırdığı belgeler oldukça kritik öneme sahipti ve belgeler çeşitli medya organlarıyla yayınlandıkça, insanlar ABD'nin tüm dünyayı "sınırsızca dinleyebildiğini" anlamış ve gündem uzun süre bu konu olmuştu. Tabii ki daha sonra bu konular unutulmuş hayat "normale" dönmüştü ancak ABD, NSA ile tüm dünyayı dinlemeye devam etmektedir.

Bu dinlemelerin yapılması için kullanılan teknolojilerin nasıl çalıştığı ayrıntılı olarak bilinmiyor ancak söz konusu teknolojilerin çoğunun yapay zekâyı kapsadığını tahmin etmek oldukça kolay zira tüm dünyayı dinlemek için elinizde böyle teknolojiler olmak zorunda. ABD'nin insanları veya devletleri dinlemek için kullandığı teknolojilerden biri PRISM projesiydi. Bu proje, NSA'in çeşitli ABD şirketleri üzerinden internet trafiğinin dinlenmesini kapsıyordu. PRISM sisteminin varlığı Edward Snowden tarafından basına sızdırılan belgeler ile ortaya çıkmıştı. PRISM, 2007 yılında başlatıldığında amaç ABD'nin güvenliğini tehdit eden unsurların takip edilmesiydi ancak Snowden'ın sızdırdığı belgelerde ve daha sonra ortaya çıkan bazı bilgilerde, NSA'in keyfi dinleme yaptığı ortaya çıktı. Google, Microsoft ve Facebook gibi dev şirketlerin habersizce dinlendiği bu sistemin son derece gelişmiş olduğunu söyleyebiliriz zira sistem, topladığı milyonlarca veriyi (e-posta, video, ses vb.) analiz edebiliyor ve bunu ilgili NSA personeline sunuyordu. Snowden'a göre PRISM, NSA'in analitik raporları için kullanılan bir numaralı zekâ kaynağıydı.

ABD'nin kullandığı bir diğer kitlesel gözetim sistemi yine PRISM gibi internetteki verileri toplayan MUSCULAR sistemiydi. MUSCULAR, GCHQ (Government Communications Headquarters) yani İngiltere'nin siber dünyadaki güvenliğini sağlayan istihbarat kurumu ile NSA'in ortak bir projesiydi. Proje sayesinde Yahoo! ve Google'ın veri merkezleri dinlenerek her gün milyonlarca kullanıcı verisi NSA ve GCHQ'nun eline geçiyordu. Bu işlem, iki şirketin kendilerine ait olan fiber hatlarına, telekomünikasyon şirketinin iş birliği ile açılan bir erişim noktası üzerinden gerçekleştiriliyordu.

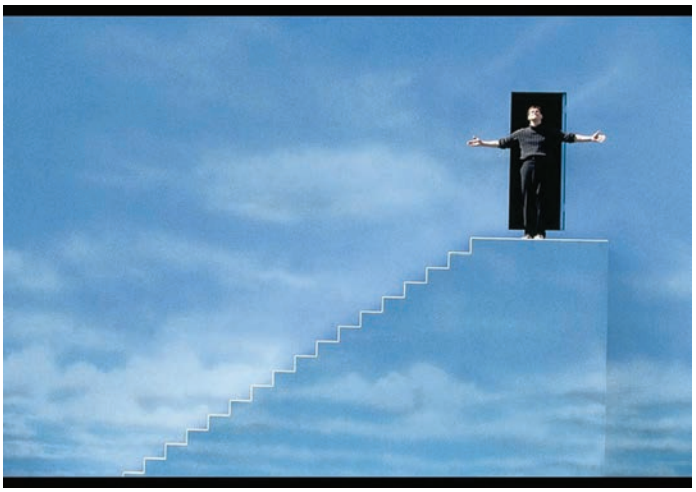
Sizlere ABD'nin yine son derece gelişmiş bir "kitlesel gözetim" sisteminden daha bahsetmek istiyorum ve yine bahsettiğim diğer sistemler gibi bunun da varlığı Edward Snowden'ın sızdırdığı belgelerle ortaya çıktı. Bu sistemin adı "XKeyscore". XKeyscore, internetteki verileri toplayan ve analiz eden bir sistemdir. Snowden'a göre bu sistem oldukça sofistikte bir yapıya sahip ve dünyanın herhangi bir yerindeki kişi hakkında birçok bilgiyi toplayabiliyor. Örneğin hedef kişinin e-posta iletişimi, ziyaret ettiği web siteleri, kullandığı bilgisayarlar hakkında detaylı bilgiler gibi verileri topluyor ve böylelikle hedef kişi etiketleniyor. Daha sonra ise toplanan tüm veriler analiz edilerek NSA'in istihbarat operasyonları gibi görevlerde kullanılıyor. Ayrıca NSA'in bu sistemi, Avustralya, Yeni Zelanda, İngiltere, Kanada, Almanya ve Japonya'nın istihbarat servisleriyle paylaştığı biliniyor.

XKeyscore hakkındaki belgeler ortaya çıktığında ABD'li Avukat Glenn Greenwald, "Amerikalıları nasıl gözetleyebileceğiniz konusunda yasal kısıtlamalar var. FISA mahkemesine gitmeden onları hedefleyemezsiniz. Ancak bu sistemler analistlerin istedikleri e-postaları, telefon görüşmelerini, tarama geçmişlerini, Microsoft Word belgelerini dinlemelerine izin veriyor" diyerek XKeyscore'un NSA personeli tarafından mahkeme emri olmaksızın kullanıldığını söylemişti[3].

Bahsettiğim bu sistemler dışında NSA'in farklı kitlesel gözetim teknikleri veya araçları bulunuyor ancak benim bahsettiklerim bunlar arasında yapay zekânın en çok kullanıldığı sistemler ve en sofistike olanları. Ayrıca hem ABD'nin hem de Rusya ve Çin'in belki şimdi varlığını bilemediğimiz yüksek teknoloji ürünü olan kitlesel gözetim sistemleri mevcut olabilir ancak bu yazıda sadece internete veya basına sızmış veriler ışığında bazı bilgiler verdim. Örneğin, Türkiye'nin herhangi bir kitlesel gözetim sisteminin varlığından şu an için bahsedemiyoruz çünkü; bununla ilgili bir veri şu an için internete veya başka bir platforma sızmış değil. Zaten bu yazıda asıl anlatmak istediğim hangi devletin daha çok kitlesel gözetim yaptığından bahsetmek değildir.

Burada anlatılmak istenen devletlerin/hükümetlerin, kendi vatandaşlarını veya tüm insanları "sınırsızca kontrol" etme isteği ve çalışmalarıdır. Devletlerin, insanları sınırsızca kontrol etme davranışları bilgisayar ve internetin icadıyla çok hızlı bir şekilde artmış, günümüzde ve gelecekte yapay zekânın aklımızın hayal edemediği sınırlara ulaşmasıyla bu davranışlar tahmin bile edilemez boyutlara ulaşmıştır. Devletlerin, halkını kontrol etme çabasının bir numaralı yardımcısı yapay zekâ, medyadaki birçok haber veya içerikte geleceği değiştirmesi beklenen ve son derece yararlı bir teknoloji olarak lanse ediliyor ki aslında sadece madalyonun ön yüzüne baktığımızda bu son derece doğru gözüküyor. Ancak madalyonun arka yüzüne baktığımızda ise yazımda da bahsettiğim gibi devletlerin bu teknolojiyi insanları gözetlemek için kullandığını görebiliyoruz. Yapay zekâ kullanılırken ortaya çıkan ince çizgi üzerindeki sorular işte tam olarak burada beliriyor; Devletler neden yapay zekâyı insanları kontrol etmek için kullanmak istiyor? İnsanları kontrol etmek hangi içgüdünün bir ürünü? Peki ya insanlar, devletlerin onları izlediğinin farkında mı?

İnsanlar, büyük gözler tarafından izlendiklerinin farkına varmak zorunda! çünkü; eğer insanlar bu gözlerin farkına varmazsa gelecekteki dünya her şeyin "sınırsızca kontrol edilebildiği" bir dünya olabilir. Şimdi bizim, ya *The Truman Show'daki Truman Burbank* gibi izlendiğimizin farkına varmamız gerekiyor ya da onun gibi yapmayıp sonsuza kadar izlenmeyi ve kontrol edilmeyi kabullenmemiz gerekiyor. Tercih bizim: ya *Truman Burbank* gibi yapacağız ya da *Christof'un* bizi izlemesine ve kontrol etmesine izin vereceğiz.



E.N.:
Bu makalede bahsi geçen XKeyscore, bu sayımızda Nuri Çilengir tarafından, ***XKeyscore: Büyük Birader'in Gölgesinde Yaşamak*** *adlı makalede detaylıca ele alınmıştır,* ***31.*** *sayfada sizleri bekliyor.*

Ayrıca bakınız: ***Türkiye Çin'den Dijital Distopya mı İthal Ediyor?*** *- Utku Şen Arka Kapı Dergi, 10. Sayı Sf. 9 - 12*

1: https://tr.wikipedia.org/wiki/Zek%C3%A2

2: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

3: https://abcnews.go.com/blogs/politics/2013/07/glenn-greenwald-low-level-nsa-analysts-have-powerful-and-invasive-search-tool/

Saniye Nur Çintimur / saadetsaniye33@gmail.com

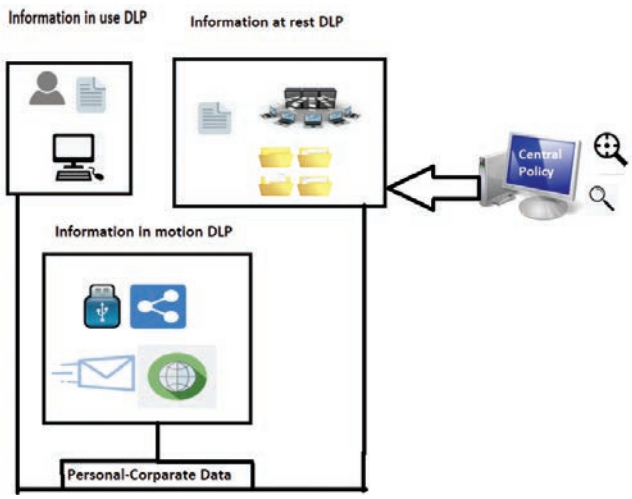
Veri Sızıntısı Önleme Popülaritesi Arttıkça Daha da Önemli Hale Gelen DLP

Merhaba Kıymetli Arka Kapı Okuyucuları, Bilgi Güvenliği Araştırmacısı olarak çalıştığım kurumda; bilgi güvenliği stratejilerinin belirlenmesi, politika ve standartların oluşturulması ve uygulanmasında kurum içi gereken kurallar veya kontrol edilmesi gereken riskler konusunda ilgili bölümler ile çalışarak gerekli düzenlemenin yapılması ve performanslarının takip edilmesinde aktif rol alıyorum. Bu süreçte edindiğim bilgilerle size DLP hakkında bir şeyler yazmak istedim. İyi okumalar.

Veri kaybını önleme veya DLP'yi, somut ve yalın bir şekilde açıklayacak olursak, hassas verilerin kaybolmasını, yanlış kullanılmasını veya yetkisi olmayan kullanıcılar tarafından erişilmesini önlemek amacıyla tasarlanmış bir dizi araç, teknoloji, ürün ve tekniktir. Yönetilen bir uç nokta cihazında kullanım esnasında, ağ üzerinden hareket halinde, e-posta ve anlık mesajlaşma, web sitesi formları, dosya aktarımları veya diğer yollarla gönderilen veriler yanlış ellerde olabilir. Bu bağlamda, uygulamalar yoluyla gönderilen verilerin hem içerik denetimini hem de bağlamsal analizini gerçekleştiren, yetkisiz bilgi akışını izleyen, tespit eden ve engelleyen teknolojiler olarak tanımlanabilir.

DLP yazılımı, düzenlenmiş, gizli ve işle ilgili kritik verileri sınıflandırır ve genellikle HIPAA, PCI-DSS (Veri güvenliği standardı) veya GDPR (Avrupa Birliği Genel Veri Koruma Yönetmeliği) gibi (ve şu an ülkemizde KVKK gibi) yasal uyumluluktan kaynaklanan kuruluşlar tarafından veya önceden tanımlanmış bir politika paketi içinde tanımlanan politikaların ihlallerini tanımlar. Bu ihlaller tespit edildikten sonra DLP, son kullanıcıların, kuruluşu risk altına sokabilecek verileri bilmeden farkında olmadan veya bilinçli olarak paylaşmasını önlemek için uyarılar, şifrelemeler ve diğer koruyucu işlemlerle düzeltmesini sağlar ve bu kurallar tek tek yazılır.

DLP 3 Ana Kullanım Alanı



Şekil 1

Üç temel durumu korumak için DLP çözümleri üç DLP işlevsel türü uygular: "Kullanımda Veri" (DIU) DLP, "Hareket Halinde Veri" (DIM) DLP ve "Beklemede Veri" (DAR) DLP.

"Kullanımda Veri" DLP, yerel kanallarda, çevre birimlerde ve çıkarılabilir, sabit ve yeniden yönlendirilmiş depolama, yazdırma, ekran görüntüsü yakalamaları vb. Dahil olmak üzere uç nokta bilgisayarlarındaki uygulamalara veri erişimi ve aktarım işlemlerini kontrol eder.

"Hareketli Veri" DLP, ağ iletişimi yoluyla veri sızıntısını önler. Örneğin e-posta, web posta, Anlık Mesajlaşma, sosyal medya, bulut tabanlı ve P2P dosya paylaşımı, HTTP / HTTPS, FTP / FTPS, SSL / TLS protokolleri vb.

"Beklemede Olan Veriler" DLP, dosya paylaşımları ve Ağa Bağlı Depolama (NAS), uç nokta dosya sistemleri, veritabanları, belge depoları ve bulut tabanlı depolama gibi kurumsal BT varlıklarında depolanan verilerde açıkta kalan gizli içeriği keşfeder. Korunmayan veriler yanlış bir yerde bulunursa, DAR DLP bu verilerin kontrolsüz potansiyel erişimini, kullanımını

ve iletimini önlemek için otomatik olarak çeşitli iyileştirme eylemleri başlatabilir.

Farklı DLP fonksiyonel türleri, çeşitli tipte uygulayıcı maddeler kullanır. DIU DLP'yi zorunlu kılmak için yalnızca uç noktada yerleşik aracılar kullanılabilirken, DIM DLP'yi zorlamak için son nokta aracıları ve ağda yerleşik donanım, yazılım veya sanal cihazlar birbirini tamamlayabilir. Sırasıyla, DAR DLP yerel dosya sistemlerini taramak için (geçici veya yerleşik) uç nokta aracıları kullanır ve ağda bulunan keşif sunucuları dosya paylaşımlarını, NAS'ı, veritabanlarını, belge depolarını ve bulut depolamayı uzaktan taramak için kullanılabilir.

DLP, ağ çıkışında, bilgisayar bağlantı noktalarında bulunan ve neyi terk etmeye çalıştığını ve ağ çevresinden kimin çıkarmaya çalıştığını kontrol eden bir "polis" gibidir. Ayrıca, bir tür kurumsal kuralı ihlal eden hassas veriler için ağ depolarını da izler.

Şirketler, politikaların ve sınıflandırmanın rafine bir yönetimini gerektirerek, bir "engelleme" aşamasına geçmeden önce, ağda ne tür verilerin ayrıldığını tespit etmek için genellikle bir "izleme" aşaması ile başlar. Politika iyileştirilirse, giden verilerin kontrolü verimli olur ve engelleme süreçleri *yanlış pozitif (false positive)* üretmez. Aksi takdirde, erişilebilir olması veya gönderilmesi gereken verilerin engellenmesi nedeniyle kuruluşta üretilen risk önemli olabilir.

Özetlemek gerekirse, DLP araçları çok güçlüdür ve hassas verilerin ağdan çıkışını sınıflandırabilir, izleyebilir ve engelleyebilir; bunları uygulamak, bunları iyileştirmek ve yanlış pozitiflerden kaçınmak için çabalar.

DLP teknolojileri genel olarak iki kategoriye ayrılır - Kurumsal DLP ve Entegre DLP. Enterprise DLP çözümleri kapsamlı ve masaüstü ve sunucular için ajan yazılımları, ağları ve e-posta trafiğini izlemek için fiziksel ve sanal cihazlar veya veri keşfi için basit cihazlar olarak paketlenirken, Entegre DLP güvenli web ağ geçitleri (SWG'ler), güvenli e-posta ağ geçitleri (SEG'ler), e-posta şifreleme ürünleri, kurumsal içerik yönetimi (ECM) platformları, veri sınıflandırma araçları, veri keşif araçları ve bulut erişimi güvenlik aracıları (CASB'ler) olarak paketlenir.

DLP KULLANIMINI ARTTIRAN 7 TREND

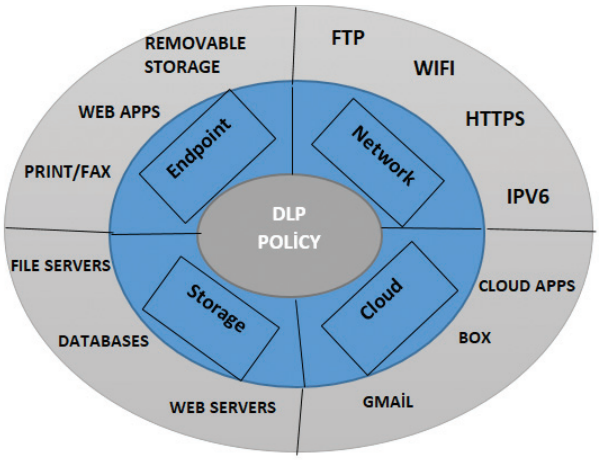
Gartner DLP pazarının yeni gelişen bir pazar olmadığını 2020 yılında 1.3 milyar Dolara ulaşacağını tahmin ediyor, tabii buna yönetilen hizmetler, bulut işlevselliği ve aralarında gelişmiş tehdit koruması içerecek diğer uygulamalar, dev veri ihlallerindeki artış eğilimi ile birleştiğinde, hassas verileri korumanın bir aracı olarak DLP'nin benimsenmesinde büyük bir artış gördü. DLP kullanımını arttıran 7 trendi inceleyelim:

1. **CISO'nun büyümesi:** Daha fazla şirket, genellikle CEO'ya rapor veren Baş Bilgi Güvenliği Görevlilerini (CISO) işe aldı ve alıyor. CEO'lar veri sızıntılarını önlemek için planı bilmek istiyor. DLP bu konuda net iş değeri sağlar ve CISO'lara CEO'ya düzenli güncellemeler sağlamak için gerekli raporlamalar verir.
2. **Gelişen uyumluluk zorunlulukları:** Global veri koruma düzenlemeleri sürekli olarak değişmektedir ve kuruluşunuzun uyarlanabilir ve hazır olması gerekmektedir. Son birkaç yıl içinde, AB ve New York Eyaleti, veri koruma gereksinimlerini sıkılaştırılmış olan GDPR ve NYDFS Siber Güvenlik Yönetmeliğine geçirdi. DLP çözümleri, kuruluşlara değişen küresel düzenlemelerle evrimleşme esnekliği sağlar ve sürekli günceldir.
3. **Karmaşık veri zincirleri:** Bulut üzerinde artan kullanım, karmaşık tedarik zinciri ağları ve artık üzerinde tam kontrole sahip olmadığınız diğer hizmetler verilerinizi korumayı daha karmaşık hale getirdi. Bu karmaşıklığı aşmak, düzene sokmak amacıyla DLP kullanımı artmış ve artmaya devam etmektedir.
4. **Veri ihlalleri sık ve büyüktür:** Kötü niyetli içeride olan rakipler, hassas verilerinizi kurumsal casusluk, kişisel finansal kazanç ve siyasi avantaj gibi çeşitli nedenlerle hedefliyor olabilir. DLP kötü niyetli olsun veya olmasın her türlü düşmana karşı koruma sağlayabilir. Sadece son birkaç yıl içinde binlerce veri ihlali ve daha birçok güvenlik olayı yaşandı. Dev veri ihlallerinde milyarlarca kayıt kayboldu: 2015'te yaklaşık 200 milyon ABD seçmen kaydına sızan veritabanının yanlış yapılandırılması, büyümeye devam eden Equifax veri ihlali ve Yahoo ihlali 3 milyar kullanıcıyı etkiledi. Bunlar, kuruluşunuzun verilerini koruma ihtiyacını vurgulayan pek çok örnekten yalnızca birkaçıdır.
5. **Kuruluşunuzun çalınan verileri daha değerlidir:** Çalınan veriler genellikle bireylerin ve grupların kendi yararları için satın alıp kullanabileceği Dark Web'te satılabilir. Birkaç bin Dolara kadar satış yapan belirli veri türlerinde, veri hırsızlığı için açık bir mali teşvik vardır. Önemli olan kuruluşunuzun güvenliğidir ve bu risk göz ardı edilemeyecek kadar büyüktür.
6. **Çalınacak daha fazla veri var:** Hassas verilerin tanımı yıllar içinde genişledi. Öznitelikli kişisel veri katagorisi genişledikçe tanımda genişledi ve hassas veriler artık fiyatlandırma modelleri ve işletme yöntemleri gibi maddi olmayan varlıkları da içermektedir. Ocean Tomo'nun Maddi Olmayan Duran Varlık Piyasası Değer Çalışmasına (Intangible Asset Market Value Study) göre, 1975'ten 2015'e kadar maddi olmayan duran varlıkların miktarı S&P 500 piyasa değerinin %17'sinden %84'e yükseldi. Bu oranlar, kuruluşunuzun korunacak ne kadar fazla veriye sahip oldugunun göstergesidir.
7. **Kurum içinde çalışanların güvenlik farkındalıkları-yete-**

nekleri eksik: Buna sanırım güvenlik yeteneği kıtlığı diyebiliriz ve bu durum uzun zamandır var olan bir durum ve muhtemelen kendi kuruluşunuz üzerindeki etkisini zaten hissediyorsunuz. 2017 yılında yapılan bir ESG ve ISSA anketinde, katılımcıların %43'ü kuruluşlarının bu sıkıntıdan etkilendiğini söyledi. Yönetilen DLP hizmetleri, personel boşluğunu doldurmak için ekibinizin uzaktan bağlantısı olarak işlev görür.

VERİ KAYBINI ÖNLEME SÜRECİ

İlk olarak veri koruma hedefinizi belirleyin. Fikri mülkiyetinizi korumaya, verilerinizde daha fazla görünürlük elde etmeye veya mevzuata uygunluğu karşılamaya mı çalışıyorsunuz? Temel bir hedef olduğunda, en uygun DLP dağıtım mimarisini belirlemek daha kolaydır. Dört ana DLP dağıtım mimarisi şunlardır: Endpoint DLP, Network DLP, Storage ve Cloud.



Şekil 2

DLP yalnızca güvenlikle ilgili bir karar değildir. DLP'nin bunlara nasıl hitap edebileceğini göstermek için farklı iş birimlerinin risk noktalarından yararlanın. Örneğin, CFO'nun risk puanları varlıkların verimli kullanımını ve kârlı büyümeyi içerir. Yönetilen DLP hizmetleri, ek personel ve CapEx'in bir DLP programı dağıtma ve sürdürme ihtiyacını ortadan kaldırarak bu risk noktalarını giderir.

DLP satıcılarını araştırırken değerlendirme kriterlerinizi belirleyin:

- Ne tür dağıtım mimarileri sunulmaktadır?
- Windows, Linux ve OS X'i destekliyorlar mı?
- Hangi dağıtım seçeneklerini sunuyorlar? Yönetilen hizmetleri sunuyorlar mı?
- Esas olarak iç veya dış tehditlere karşı savunmanız gerekiyor mu ya da her ikisi de mi?
- İçeriğe dayalı inceleme ve sınıflandırma gerçekleştirmeniz gerekiyor mu?
- Kullanıcılarınız belgeleri kendi kendine sınıflandırabilecek mi? Birden çok yöntem kullanmaya ihtiyacınız var mı?
- Politikalara, olaylara veya kullanıcılara dayalı veri hareketini görmeyi planlıyor musunuz ya da kurum içinde buna ihtiyaç var mı?
- Kurum hangi uyumluluk düzenlemelerine tabidir?
- DLP'nizle hangi teknolojileri entegre etmek istersiniz?
- DLP programınızı ne kadar hızlı dağıtmanız gerekiyor?
- DLP programınızı yönetmek için ek personele ihtiyacınız olacak mı?

Kuruluşunuzun DLP programında yer alan kişilerin rollerini ve sorumluluklarını açıkça tanımlayın. Role dayalı haklar ve görevler oluşturmak, kontrolü ve dengeyi sağlayacaktır. İş yüklerini azaltacaktır.

Kuruluşunuzun verilerini yönetecek DLP politikalarını tanımlamak için iş birimi başkanlarıyla birlikte çalışın. Bu, farklı iş birimlerinin yürürlükteki politikalar ve bu politikalardan nasıl etkilenebilecekleri konusunda bilgi sahibi olmalarını sağlayacaktır. DLP politikalarını geliştirmenin tek bir doğru yolu olmadığını unutmayın. Genellikle, DLP stratejisi kurum kültürünüze uygun olacaktır. Yani kurum içi tutumunuzla eşdeğer ilerleyecektir.

Süreçlerinizi dikkatlice belgeleyin. Bu, politikaların tutarlı bir şekilde uygulanmasında size yardımcı olacak, incelemeler gerektiğinde size bir kayıt belgesi verecek ve yeni ekip üyelerini veya çalışanlarını işe alırken de yardımcı olacaktır.

Başarı metriklerini tanımlayın ve raporları iş liderleriyle paylaşın. DLP programınızın başarısını ve iyileştirme alanlarını belirlemek için ölçmeniz ve izlemeniz gereken temel performans göstergelerini (KPI'lar) belirleyin. DLP'nin ve işletme değerinin olumlu etkisini göstermek için bu metrikleri kuruluşunuzun liderleriyle paylaşın.

DLP bir programdır, ürün değildir. DLP aracının yüklenmesi, Veri kaybını önlemenin sadece ilk adımıdır. Hızlı kazançlar elde etmenize rağmen, DLP'nin sürekli üzerinde çalışılacak bir program olduğunu anlamak kalıcı başarıya ulaşmanıza yardımcı olacaktır. DLP, verilerinizi ve kullanıcıların, sistemlerin ve olayların verileri daha iyi korumak için bu verilerle nasıl etkileşime girdiğini anlamak için sürekli bir süreçtir.

Kaynaklar:

https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention

https://www.cisco.com/c/en/us/products/security/email-security-appliance/data-loss-prevention-dlp.html

https://www.skyhighnetworks.com/cloud-security-blog/how-data-loss-prevention-dlp-technology-works/

https://www.sealpath.com/dlp-irm-which-one-should-i-choose-to-protect-my-sensitive-data/

Eren Talha Altun / erenaltun@protonmail.com

Gazeteciler için Açık Kaynak İstihbaratı II

LinkedIn:

Sosyal Medya İstihbaratı [SOCMINT] 'de olmazsa olmazlardan Linkedin birçok istihbarat servisinin gözde platformu olmuştur.

Özellikle de Çin istihbarat örgütleri Linkedin gibi ağları etkin olarak kullanmaktadır . Bu gibi ağlar vasıtasıyla istihbarat edinmeye çalışıyorlar. Ayrıca kullanıcıların alışkanlıkları, hobileri ve siyasi yönelimleri hakkında da veri topladıkları da bilinmektedir. Bu konu daha önce haberlere de konu olmuştur.

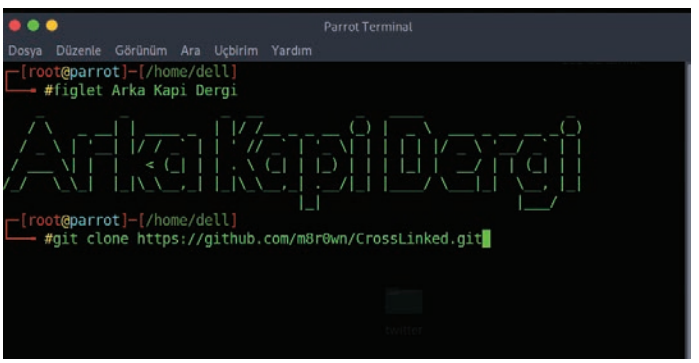
Örnek Bir Haberde, "Çin sosyal medya platformlarında yapılan ajanlık faaliyetlerini anlattı. Çin ajanlarının, LinkedIn'de aynı anda binlerce kişiyle irtibat kurduğunu belirten Evanina, 'Tek bir hedef için ABD'ye casuslar göndermek yerine, Çin'deki bir bilgisayarın arkasında oturmak ve sahte profillerle binlerce kişiye arkadaşlık isteği göndermek çok daha etkili oluyor.' diye konuştu. Özel sektörde önemli konumdaki kişilerin yanı sıra akademisyenlerin de hedef alındığını kaydeden Evanina, Çin istihbaratının faaliyetlerinde geçen yıllara göre bir azalma görülmediğini söyledi." [1]

Her platformda olduğu gibi Linkedin'de de yarı otomatik, araştırmacıların işine yarayacak, açık kaynak istihbarat araçları mevcut. Linkedin için kullanabileceğimiz Crosslinked aracı bünyesinde birçok özellik barındırmaktadır.

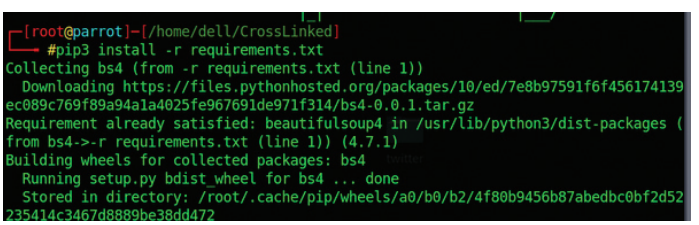
Araştırmalarınızda size vakit kazandıracak CrossLinked Uygulaması sayesinde araştırmasını yaptığınız şirketin çalışanları hakkında otomatize bilgi toplayabileceksiniz. Çıkan sonuçlar .txt formatında dışa aktarılacaktır. Linkedin için kullanacağımız CrossLinked uygulaması her ne kadar çok bilinmese de oldukça kullanışlı bir araçtır.

CrossLinked Kurulumu:

$ git clone https://github.com/m8r0wn/crosslinked



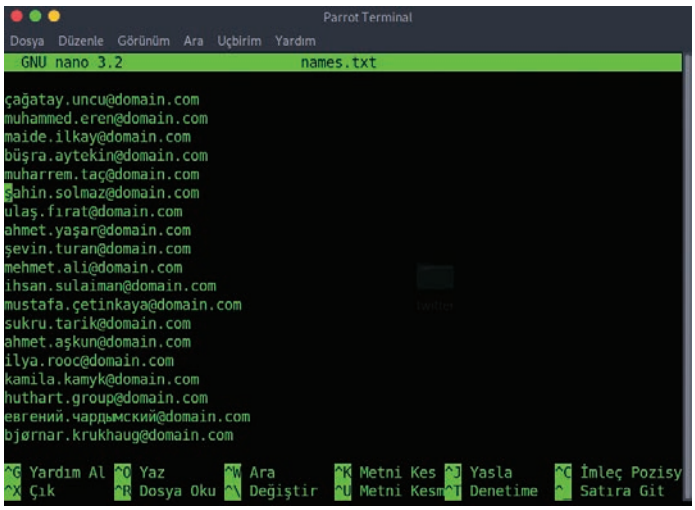
$ pip3 install -r requirements.txt



$ python3 crosslinked.py -f '{first}.{last}@domain.com' company_name

$ python3 crosslinked.py -f 'domain\{f}{last}' -t 45 -j 0.5 company_name

```
┌─[root@parrot]─[/home/dell/CrossLinked]
└──╼ #python3 crosslinked.py -f '{first}.{last}@domain.com' company_name
[*] Searching google for valid employee names at company_name
[*] 0 : https://www.google.com/search?q=site:linkedin.com/in+"company_name"&num=1
00&start=0
[*] 79 : https://www.google.com/search?q=site:linkedin.com/in+"company_name"&num=
100&start=135
[*] 156 : https://www.google.com/search?q=site:linkedin.com/in+"company_name"&num
=100&start=276
[*] Searching bing for valid employee names at company_name
[*] 0 : https://www.bing.com/search?q=site:linkedin.com/in+"company_name"&first=0
[*] 8 : https://www.bing.com/search?q=site:linkedin.com/in+"company_name"&first=2
8
```



Yukarıda da gördüğümüz gibi özellikle şirket araştırmalarında bu şekilde şirketin çalışanlarının bilgilerinin çıktısını bize txt formatında sunmaktadır.

Tarih boyunca hep ateş çemberinde olan coğrafyamızda bugün de yüksek tehdit ve risk ortamı devam etmektedir. Bu ortamda ülkemizin bekasına en fazla katkı sağlayacak kuvvet çarpanı güvenilir kaynaklar ve istihbarattır. Açık kaynak istihbaratının da bu çarpanda önemli bir değişken olduğu her zaman göz önünde bulundurulmalıdır.

Günümüz teknolojik imkânları ve gelişen iletişim yetenekleri, eski usul istihbarat toplama yöntemleri yanında yeni imkânlar ve kolaylıklar getirmiş durumdadır.

Önceleri açık kaynak istihbaratı kapsamında sınırlı sayıdaki yazılı ve görsel medya takip edilerek bilgi toplanmaya çalışılmıştır. ABD Merkezi İstihbarat Teşkilatı CIA'in Soğuk Savaş döneminden itibaren açık kaynak istihbaratı birimine sahip olduğu, bilinmektedir. 1953-1961 yılları arasında CIA başkanlığını yapmış olan Allen W. Dulles CIA'in elde ettiği istihbaratın %80'inin açık kaynak istihbaratından elde edildiğini ifade etmiştir.

O dönemin iletişim imkânları göz önüne alındığında bu oranın hayli yüksek olduğu düşünülebilir. O dönemde bile bu kadar yüksek oranda istihbarat sağlayan bu kaynağın günümüzde daha yüksek oranlarda bilgi sağlaması kaçınılmazdır.

2000'li yılların başlarından itibaren siber dünyanın büyüklüğü ve internet kullanımı her geçen gün inanılmaz bir hızla artmıştır. Twitter sosyal ağı üzerinden örnekleyecek olursak 2006 yılında faaliyetine başlayan sosyal ağın 2018 yılı ortasına göre aylık 326 milyon aktif kullanıcısının gönderdiği mesaj sayısı günlük 500 milyon mesaja ulaşmıştır.

2018, Ocak ayında yapılan ve grafiği üstte yer alan araştırmaya göre yaklaşık yaklaşık 7 milyar 500 milyon olan dünya nüfusunun 4 milyarı internet, 5 milyarı cep telefonu kullanıcısıdır. Bu 4 milyar kişi, sosyal medyayı da aktif olarak kullanmaktadır.

Uzmanlar daha önce , hızla gelişen krizlerle ilgili istihbarat toplamak için Facebook ve Twitter'in en önemli kaynaklardan biri haline geldiğini belirtmişler.

Başta da belirttiğimiz gibi medya organları ve gazeteciler, daima istihbarat örgütlerinin gözde alanları olagelmiştir. Gazeteci kimliği ile yürütülen bir çok iş, normalde istihbarat örgütlerinin kolaylıkla elde edemeyecekleri değerli bilgi veya gözlemleri bu örgütlerin ayağına getirebiliyor.

Haber bültenlerine yansıdığına göre CIA, Facebook ve Twitter gibi sosyal medya mesajlarının dünya genelindeki trafiğini izlemeye alan bir çalışma başlatarak günde beş milyona yakın mesajı didik didik okuyarak önemli bir istihbarat kaynağı oluşturmuş durumda.

Haberlere göre CIA'in Virginia'daki Açık Kaynak Merkezi'nde yüzlerce uzman, Arapça'dan Mandarin Çincesine kadar birçok dilde sosyal medya yazışmasını izliyor.

Bilinen basın organları üzerinden yürütülen istihbarat çalışmaları bu denli kapsamlı iken sosyal medya denen ve herkese açık olan platformların oluşturduğu muazzam kaynak, her gazeteci tarafından kullanılmalıdır!

OSINT'in amacı internet ortamında yayınlanan verilerin ya da bilgilerin toplanmasıdır. Bu bilgilerin toplanması yasaldır. Hedef ile etkileşim yaratacak iletişim olmaması önemlidir. Toplanan verilerin analizi yapılarak, sonraki aşama için kullanılabilir hale getirilmesi gerekir. Yine günümüzde açık kaynak istihbaratın önemine dair birçok olay mevcut bunlara örnek vermek gerekirse [2]:

HDP, Güvenlik ve İstihbarat Komisyonu raporuna şerh koydu: 'Çok gizli' ibareli bilgilere açık kaynaklardan ulaşılabilir

2014 yılında kurulan komisyonun görüşmeleri kapalı oturumla yapılıyor

"Çok Gizli" Seviyesindeki Bilgiyi Deşifre Eden Alman Gazeteci:

Geçmişte Alman gazetelerinden birinde bir haber çıkar. Haberi kaleme alan gazetecinin iddiasına göre Alman genelkurmayı yeniden yapılanmayı ve kurmay kademesinde çok önemli değişiklikler yapmayı planlamaktadır. Bu haber ülkede çok ilgi görmez ancak haberin yayınlandığı o akşam, yazar, Alman İstihbarat Teşkilatı tarafından bir operasyonla derdest edilir ve teşkilatın merkezinde kapsamlı bir sorguya alınır!

Gazeteci, Alman istihbaratı tarafından casusluk ile suçlanmaktadır. Ajanların amaçları gazetecinin genelkurmaydaki bağlantısını ortaya çıkarmaktır. Çünkü çok gizli olan bu bilgi ancak Genelkurmaydan sızmış olabilirdi. Bir başka ekip de gazetecinin evini aramaktadır. Casusluk ile suçlanan gazeteci ise suçlamaları reddetmekte, bilgiyi yalnızca Alman Genelkurmayı ile alakalı gazetelerde çıkan haberlerden ve bürokratların beyanatlarından analizle kaleme aldığını iddia etmektedir.

Uzun bir sorgunun ardından gazetecinin evini arayan istihbarat ekibi klasörler dolusu doküman ile merkeze gelirler. Onlarca klasör, yıllar boyu Alman Genelkurmayı hakkında çıkmış tüm haberlerin gazete küpürlerini ve beyanatların metinlerini ihtiva etmektedir. Sonuç olarak gazetecinin casus olmadığına, bu "top secret" seviyesindeki bilgiyi "açık kaynak istihbaratı" sonucu ürettiğine kanaat getirilir ve gazeteci serbest bırakılır. [3]

Farklı bir hikayeye örnek vermek gerekirse:

İkinci Dünya Savaşı sırasında ABD ve Japonya arasında geçen bu hikâye, bence açık kaynak istihbaratının önemini bugüne kadar konuyla alakalı okuduğum tezlerden ve makalelerden çok daha iyi anlatmaktadır.

Japonya'yı her yönden köşeye sıkıştırmak isteyen ABD, Japon halkının yiyecek kaynaklarını da hedef almaktadır. Bir ada ülkesi olmasından dolayı zaten kısıtlı tarım imkânı olan Japonya'nın tarımını bitirmek için tüm önlemleri alan ABD bir türlü Japonları açlığa mahkûm edememiştir. Tarım yapamamaları için tüm gübre kaynaklarına dahi ulaşımı engellemiş ancak tarımın önüne geçememiştir.

Japonların tarım yapabilmek için gerekli gübreyi nereden bulduğunu araştırmak için özel bir istihbarat ekibi kurulur. İstihbaratın bilinen tüm yöntemlerini uygulayan Amerikalı ajanlar bir türlü istedikleri bilgiye ulaşamamaktadır. Japonlar üretime devam etmekte, Amerikalıların umutları tükenmektedir.

Özel istihbarat ekibinin başında olan albay neredeyse başarısızlığını kabul etmek üzeredir. Ancak Japon adalarının coğrafi özelliklerinin bulunduğu bir ansiklopediyi karıştırırken okuduğu bir cümle tüm operasyonun kaderini değiştirmiştir. Cümle şudur; "..adasında geniş fosfat yatakları vardır."

Bu bilgiyi okuyan albay derhal hava kuvvetlerine emir verir ve bahsi geçen bölgeyi savaş uçaklarına bombalatır. Bu bombalamadan sonra Japonların zar zor ayakta duran tarımının sonu gelir ve operasyon bir ansiklopedi sayesinde başarıya ulaşır. İşte bu, başarılı bir "açık kaynak istihbaratı" operasyonudur. [4]

OSINT AŞAMALARI:

Öncelikle istihbarat ihtiyacının ne olduğuna karar verilmelidir, hedef kişi ile ilgili bir profil oluşturulmalı, hobileri, görüştüğü kişiler, hangi mekanlarda takıldığı, hangi sosyal medya hesaplarını daha etkin kullandığı, ne tarz hobilere sahip olduğu gibi unutmayın bulabileceğimiz en ufak ayrıntı bile bizim için önemli! Örneğin şahsın genelde gittiği mekanları Swarm uygulamasına sahip ise Swarm üzerinden de tespit etmek mümkün, birçok alternatif olmasına rağmen Swarm diğerlerine göre daha kullanışlıdır.

Hedefle yönelik yapılan basit internet taramaları, Google, Bing, Yandex, DuckDuckGo, LinkedIn, Facebook, Twitter.. ve bir çok arama motorları ve sosyal medya hesaplarının araştırılması, Hedefe ait e-posta adreslerinin tespit edilmesi, Kullanılan uygulamaların geçmiş kayıtlarının tespit edilmesi önemlidir, Hassas verilerin tespit edilmesi (Metadata Analizi), Fotoğraf, video, lokasyon bilgileri gibi başlıca temel bilgilerin elde edilmesi gerekir. Bu bilgiler elde edildikten sonra profile uygun çalışmaya devam edilmelidir.

Terörizm Açık Kaynak İstihbarat Araştırma Kaynakları:

Siber terörizm potansiyelinin abartıldığı düşünülebilir ancak böyle bir tehdidi inkar etmek ya da görmezlikten gelmek yanlıştır. Terörle mücadelede elde edilen başarı teröristleri siber terörizm gibi olağan dışı yöntemlere yöneltebilir..Istihbarat araştırmacıları sahada araştırma yaptığı kadar siber uzayda da bu araştırmaları yürütmektedir. Gelişmiş askeri donanım araçlarının yanı sıra, siber uzay üzerinden açık kaynak istihbaratı sayesinde de hedef hakkında birçok delil ve ayrıntı elde edebilmekteyiz. Bunlardan birkaçına örnek vereceğiz.

Uluslar ve Uluslararasi Terör Faaliyetlerinin Toplandiği Veritabanı:

https://www.start.umd.edu/gtd/NewUser.aspx

Uluslarası Terörle Mücadele Ensitüsü:

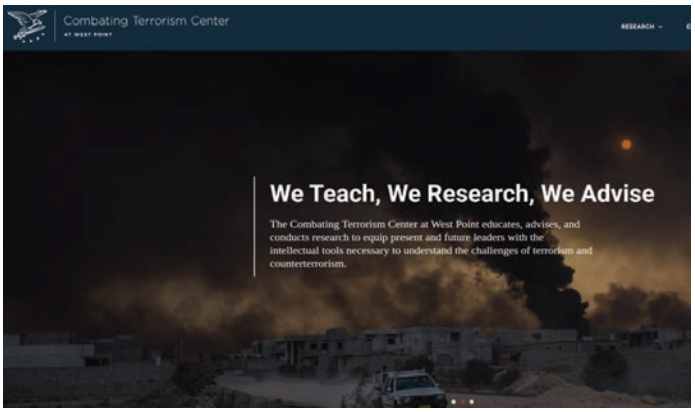
Terörle mücadele, iç güvenlik, tehdit açığı, risk değerlendirmesi, istihbarat analizi, ulusal güvenlik ve savunma politikası konularında uzmanlık sağlayan bağımsız bir düşünce kuruluşudur.

İstatistiksel raporlara ek olarak küresel terörist saldırıları, terör örgütleri ve aktivistlerini kapsayan İnternet üzerindeki en büyük kamuya açık araştırma veritabanını mevcuttur.

Terörle Mücadele Araştırma Merkezi:

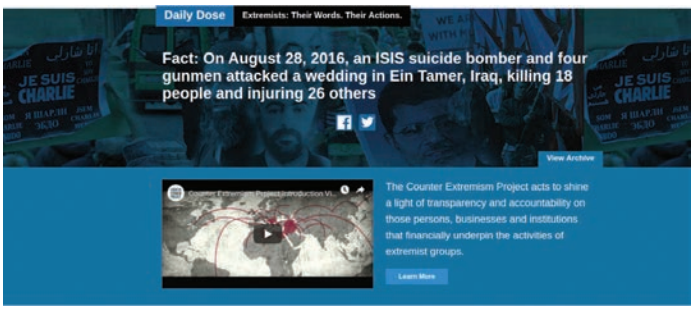
https://ctc.usma.edu/

Terörle Mücadele Merkezi, mevcut ve gelecekteki liderleri terör ve terörle mücadelenin zorluklarını anlamak için gerekli entelektüel araçlarla donatmak için araştırma yapan web sitesidir.



Teröristler Veri Tabanı:

https://www.counterextremism.com/ - https://www.counterextremism.com/extremists



Küresel Terörle Mücadele Forumu:

thegctf.org - Küresel Terörle Mücadele Forumu (GCTF), terör eylemlerini önleme, mücadele etme ve kovuşturma eylemlerini önleyerek, bunlarla mücadele ederek ve kovuşturma yoluyla terörist eylemleri önleyerek, savaşarak ve kovuşturma yoluyla, dünya çapında teröristlere karşı savunmasızlığı azaltma misyonunun yer aldığı 29 ülke ve Avrupa Birliği uluslararası bir forumudur.

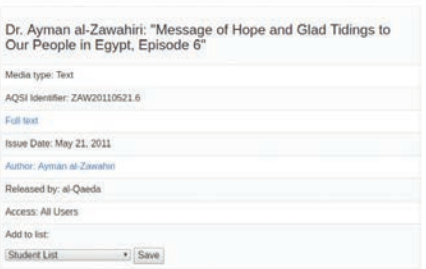
Araştirma topluluğu , dünyadaki ülkelerden ve bölgelerden uzmanları ve pratisyenleri deneyimlerini ve uzmanlıklarını paylaşmak ve gelişen terör tehdidine karşı koyma konusunda araçlar ve stratejiler geliştirmek için bir araya getiriyor.

GCTF
GLOBAL COUNTERTERRORISM FORUM

Küresel Terörizm Araştırma Projesi:

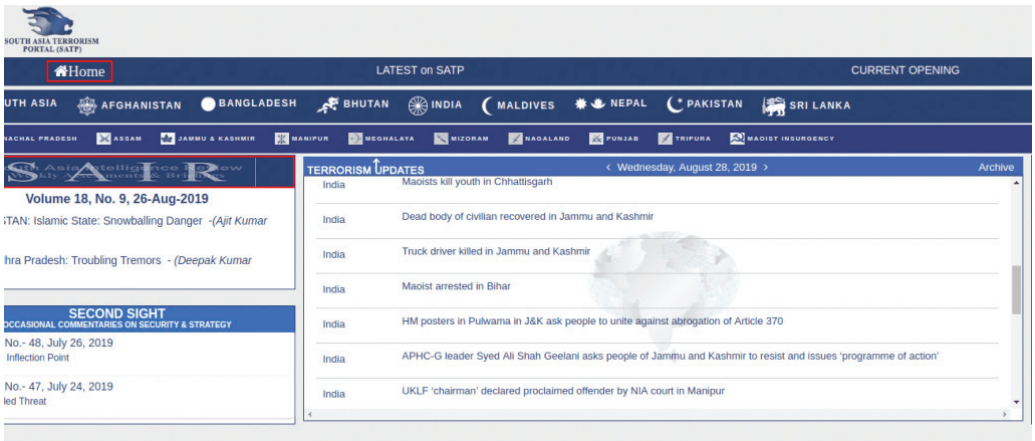
http://gtrp.haverford.edu sitesi iki bölümden oluşuyor. Web sitesinde kaynaklar bölümünde, terörizm ve uluslararası güvenlik hakkında bilgi veren diğer çeşitli faydalı web sitelerine bağlantılar derlenmektedir.

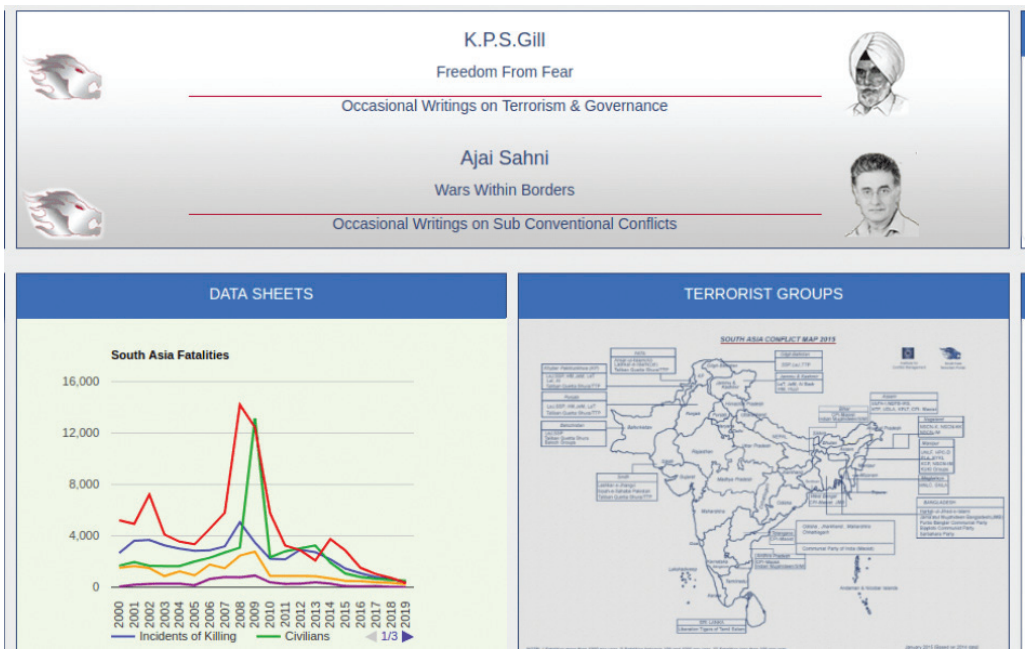
Web sitesinin bu bölümü, kitaplar, birincil kaynaklar, veri kaynakları, dergiler, haberler, bloglar, araştırma siteleri, araştırma portalları ve öğrenciler için kaynaklar içermektedir.



Asya Terör Araştırma Merkezi:

https://www.satp.org/

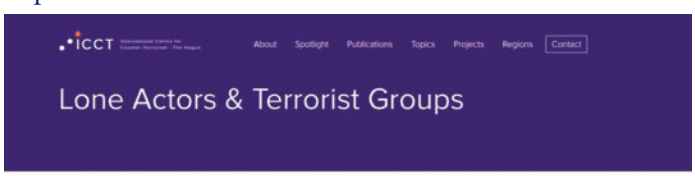




Uluslararası güvenlik ve uluslararası terörizm ile ilgili verilen paylaşıldığı platformdur.

Terörle Mücadele Uluslararası Merkezi:

https://icct.nl/

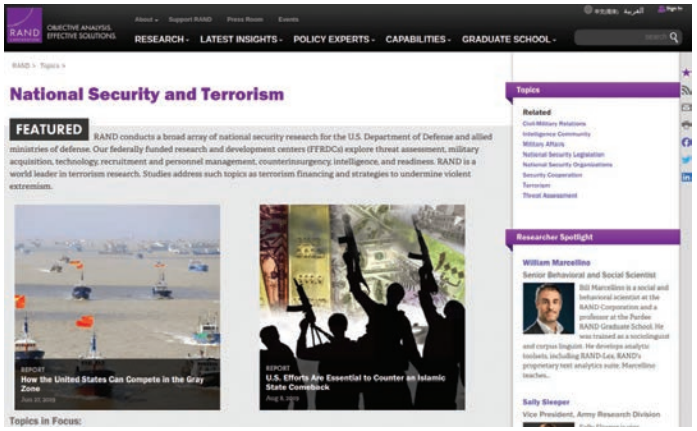


Terörle mücadelenin insan haklarıyla ilgili yönlerinin kesiştiği temalara odaklanmaktadır. Başlıca proje alanları şiddetli aşırılıkçılıkla mücadele, hukukun üstünlüğü, yabancı savaşçılar, ülke ve bölgesel analizlerdir. Terörle Mücadele Araştırma ve Analizi Akademisyenler ile çalışmak ve eğilimlerin analizi de dahil olmak üzere, terörle mücadeleye yönelik hukuk temelli yaklaşımların önlenmesi ve yönetimi konusunda politika ile ilgili bilgiler geliştirmektedir.

Ulusal Güvenlik ve Terörizm:

https://www.rand.org/

RAND Corporation, dünyadaki toplulukları daha güvenli ve daha sağlıklı hale getirmek için kamu politikası zorluklarına çözümler geliştiren bir araştırma kuruluşudur.



Terörle Mücadele Eğilimleri ve Analizleri & Diğer Kaynaklar:

https://en.wikipedia.org/wiki/Global_Terrorism_Index#20

https://www.rsis.edu.sg/wp-content/uploads/2018/06/CTTA-June

https://www.rsis.edu.sg/rsis-publication/icpvtr/counter-terrorist-trends-and-analyses

https://onlinejihad.net/

http://www.jihadica.com/

Bahsedilenler:

[1] https://www.aa.com.tr/tr/dunya/cinin-linkedini-istihbarat-faaliyetleri-icin-kullandigi-iddiasi/1568877

[2] https://t24.com.tr/haber/hdp-guvenlik-ve-istihbarat-komisyonu-raporuna-serh-koydu-cok-gizli-ibareli-bilgilere-acik-kaynaklardan-ulasilabilir,532460

[3] https://www.stratejikortak.com/2018/03/gercek-istihbarat-operasyonlari-ile-acik-kaynak-istihbarati.html

[4] https://www.stratejikortak.com/2018/03/gercek-istihbarat-operasyonlari-ile-acik-kaynak-istihbarati.html

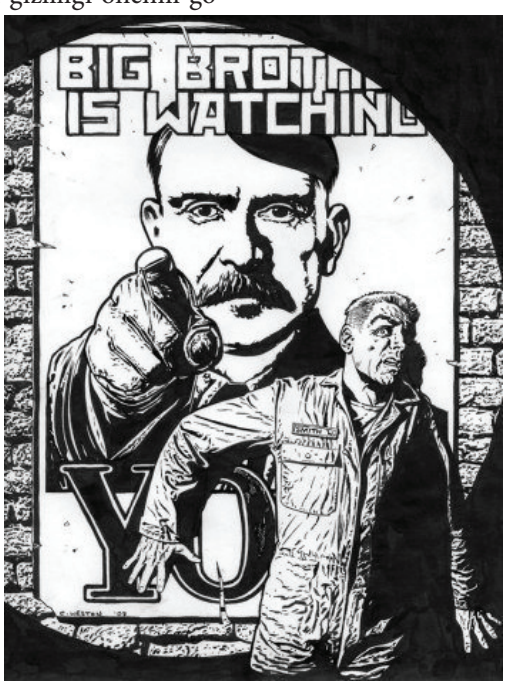
Nuri Çilengir - nuriilengir@protonmail.com

XKeyscore: Büyük Birader'in Gölgesinde Yaşamak

"Gizlenecek hiçbir şeyin olmadığı için gizlilik hakkıyla ilgilenmediğinizi iddia etmek, özgür konuşma hakkıyla ilgilenmediğinizi söylemekten farklı değildir çünkü söyleyecek bir şeyiniz yoktur."
Edward Snowden

Mahremiyetin insanlığın başlangıcına kadar uzanan bir hikayesi vardır ve insanın özgür bir birey olabilmesinin ön şartlarından biridir. Dolayısıyla mahremiyet ihtiyacı, en temel insan ihtiyaçlarından biri olmalıdır. Durum böyleyken, günümüz bilgi çağında insanlar mahremiyet haklarından bir takım yanılsamalar ya da farklı amaçlar uğruna bilinçli veya bilinçsiz vazgeçmektedirler. Bilginin önemin arttığı ve her kesimden insanın bilgi alışverişi ile yaşayabildiği çağımızda, kişisel bilgilerin gizliliği önemli görülmemekte. Bu yüzden makale boyunca mahremiyet kavramından yola çıkarak, insanların global çapta devlet ya da şirketler tarafından mahremiyetleri hiçe sayılarak nasıl manipüle edildiğini gösteren XKeyscore'a değineceğiz.

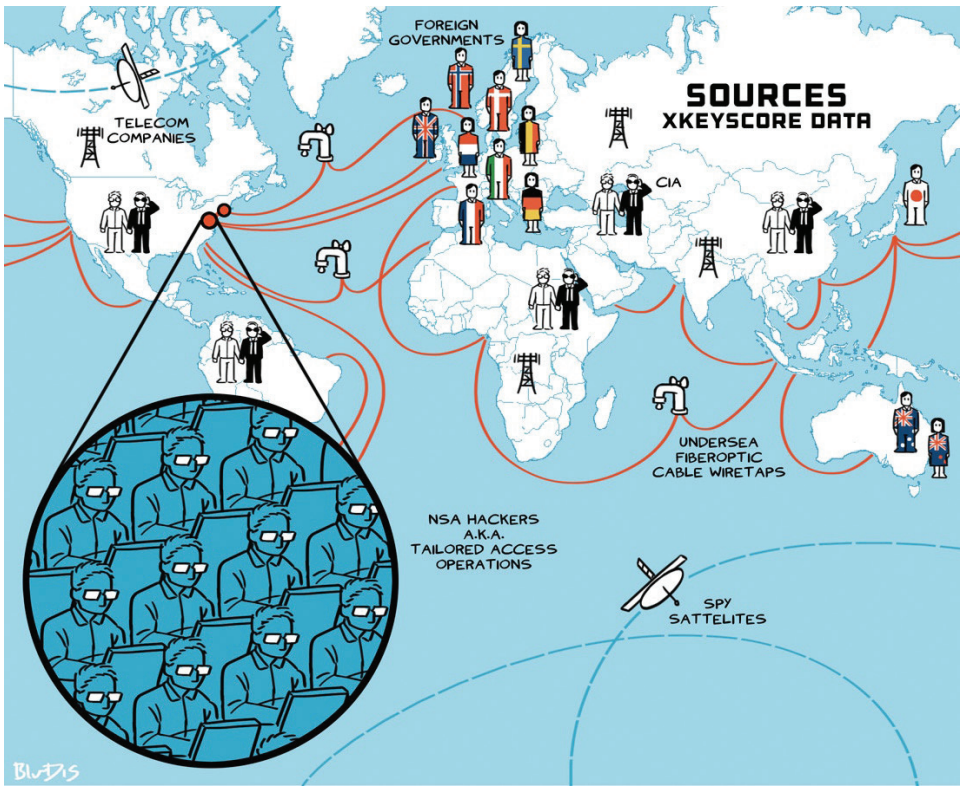
Bir düşünelim. En sevdiğiniz müzisyenin doğum gününü mü unuttuğunuzda ne yapıyorsunuz? Tabii ki Google'a bakıyorsunuz! Yediğiniz efsane yemeği dünyayla mı paylaşmak istiyorsunuz? Fotoğrafını çekip Instagram'a atın ki herkes beğensin! Eski arkadaşlarla hasret mi gidermek istiyorsun? Facebook'tan yazıyorsun! Toplantın var ve uzakta mısın? Skype'tan bağlan! Bunlar hemen hemen birçoğumuzun günlük yaptığı aktiviteler. Peki, tüm bu aktiviteler sırasında aslında biri bizi gözetliyor olsa ve kötüsü bu ihtimale rağmen şunun varsayımlarla kendimizi avutmayı denesek; *"Beni, kim neden izlesin? Ki izlese de benim saklayacak bir şeyim yok..."*



Mahremiyet Nedir?

Mahremiyet, literatürde ilk kez 1890 yılında Amerikalı yargıç Brandeis tarafından "*Yalnız bırakılma hakkı; hakların en kapsamlısı ve özgür insanlar tarafından en çok değer verileni.*" olarak özgürlük ve birey olma kavramları ile mahremiyet kavramını ilişkilendirerek tanımlanmıştır. Ancak daha güncel bir tanımlamaya başvurmak istersek James Rachels'in *"...Sadece saklanacak şeyi ifade etmek için değil, yaşam niteliğini artırmak için bir gereksinim, kendini gerçekleştirme, özerkliğini koruma yollarından biri olarak ele alınmalıdır. Sonuç olarak mahremiyet, toplumdan soyutlanma değil, ben ile öteki sınırının belirlenmesi, kontrol edilmesi olarak özetlenebilir."* şeklindeki tanımını da aktarmakta fayda var.

XKeyscore Nedir?



XKeyscore, adını ilk kez 2013 yılında Guardian'ın yayınladığı Snowden belgelerinde ortaya çıkan bir NSA projesi olarak biliyoruz. Bu projenin amacı, internette istihbarat amacıyla kullanılabilecek her türlü bilgiyi toplayan, organize eden ve analistlerin gerek duyduklarında bu araç üzerinden arama yaparak sayısız kişinin internet aramalarını, e-postalarını, belgelerini, kullanıcı adlarını ve parolalarını ve diğer özel iletişimleri gibi bilgilere ulaşabilecekleri bir altyapı oluşturmak. 2013 yılında yayımlanan bu belgeler bize NSA'in amaçladıklarını büyük derecede başarabildiğini gösteriyor.

XKeyscore 2008'de, Amerika Birleşik Devletleri, Meksika, Brezilya, Birleşik Krallık, İspanya, Rusya, Nijerya, Somali, Pakistan, Japonya, Avustralya ve diğer birçok ülkede bulunan 700'den fazla sunucudan oluşan yaklaşık 150 saha alanına sahip. Bu sunucuların çoğu CIA kontrolünde backbone üzerinden topladıkları verileri istenilen herhangi bir zamanda NSA analistlerine iletiyorlar. Çeşitli bölgelerdeki sunucular tüm trafiği dinliyor ve dinledikleri trafiğin içeriğini 3-5 gün, metadalarını ise 30-45 gün aralığında depoluyorlar. Kaldı ki, Snowden tarafından sızdırılan NSA dökümanları milyarlarca kaydın veritabanlarında tutulduğunu da gösteriyor.

NSA kendi sunumlarında XKeyscore'u "Dünyanın dört bir yanındaki makinelerde çalışan, tamamen dağıtık bir veri işleme ve sorgulama sistemidir." şeklinde açıklanıyor. Bu açıklamadaki sorgulama kısmı aslında her birimizin verilerinin bir arama butonu kadar uzak olduğunu gösteriyor. Peki toplanan ve işlenen veriler neler ve bu veriler nasıl kullanılmakta?

Belgelerden XKeyscore'un, internet üzerinden her türlü veriyi toplama amacıyla tasarlamış olduğu görülüyor. Toplanan verileri işleyip kişiler ve kurumlar hakkında profilleme yapmakta. Sistem, sosyal medya uygulamaları gibi işlenen tüm veriyi tıbkı Facebook, Twitter ve Google gibi büyük şirketlerin yaptığı gibi profilize ediyor. Oluşturulacak profil için sunucuların topladığı veri sadece normal internet trafiği, e-posta yazışmaları ve mesajlaşmalarınızla sınırlı değil. Tüm bunların haricinde VoIP görüşmeleri, cep telefonlarında taşınabilecek ve sızdırılabilecek her türlü içeriği/veriyi, telefon aramalarınızı, webcam erişimi, özel fotoğraflar ve videoları, web sitelerinin analiz amacıyla topladığı çerezler ve analytics verilerini, sosyal medya trafiği, botnet trafiği, log dosyaları, CNE hedeflerini, ele geçirilmiş ya da sızdırılmış kullanıcı adı ve parola kaynaklarını, çevrimiçi servislere yüklenmiş dosyaları, Skype oturumları ve daha fazlasını toplayabilme ve tüm bu verileri profilleme yetisine sahip.

Öte yandan XKEYSCORE, şüpheli davranışlar algıladığı durumları modelleyerek, insanları inanılmaz derecede geniş gözetime tabi tutuyor. Örneğin, insanların konumlarını, uyruklarını ve ziyaret edilen web sitelerini temel alarak faaliyetlerini göstermek için sistemde arama yapmak mümkün. Yani bu, Pakistan'da almanca içerikler üretseniz de sizi takip edebildiği anlamına geliyor. Facebook, Twitter, Amazon, YouTube, Netflix ve daha birçok ünlü uygulamalar aslında bizleri bu çerezler ile çok güzel özetliyor. Bu yüzden, ziyaret ettiğiniz her web sitesinde bıraktığımız izler ve tutulan çerezler XKeyscore için en büyük hazinelerden biri. Dolayısıyla ben VPN kullanıyorum ya da internete şöyle erişiyorum demenin de çerezlerinizi silemedikçe bir önemi kalmıyor.

XKEYSCORE'un kapasitesi ve yöntemleri yalnızca bilgileri toplama ve arşivleme ile sınırlı değil. Tüm bunların yanında bunları kullanarak kolayca istedikleri sistemleri de hackleyebildikleri ve erişim sağlayabildikleri belgelerde öne çıkıyor. Bu yüzden NSA analistlerinin popüler hedeflerinden biri de sistem yöneticileri. Sistem yöneticilerinin bilgilerine erişmek krallığın anahtarını elinde bulundurmak demek. Dolayısıyla analistler, sistem yöneticilerini hedef alarak bir çok sisteme erişim sağlayabiliyor. Ayrıca, sistem sürekli olarak Hacker fo-

rumlarını, sızdırılmış veri ve diğer hack araçlarını satan veya kullanan kişileri ve web sayfalarını da takip ediyor. NSA, rakipleri tarafından geliştirilen araçları anlamak için izlerken, aynı zamanda bu tür yeteneklerin satın alınabileceği yerleri de izliyor.

XKeyscore Nasıl Çalışır?

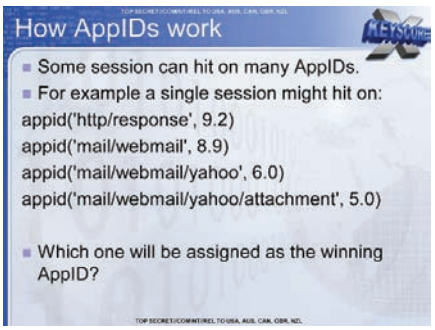
Dünyanın herhangi bir yerinde, bir kişi çevrimiçi olduğunda -ister e-postalarını okumak için, ister sosyal medyada gezmek için, ister oyun oynamak için- yaptığı eylemden bağımsız bir şekilde gönderdiği ve aldığı tüm internet trafiğinin toplanması ve işlenmesi XKeyscore'un bu dağıtık yapısının nasıl çalıştığı hakkında oldukça merak uyandırıyor. Bu kadar büyük ve istikrarlı bir bilgi akışını anlamak için, NSA analistleri, farklı trafik türlerini tespit etmek ve her türden yararlı bilgileri ayıklamak için binlerce script yazdılar.

Sistemin çalışma mantığı aslında uzaktan baktığımızda o kadar da komplike olmadığı görünüyor. Daha net anlamak için bir belgelerdeki bir örneği ele alalım. Örneğin, bir arkadaşınıza mail gönderiyorsunuz. XKeyscore oluşan bu trafiğin mail olduğunu tespit ediyor. Daha sonra, hangi servisi -Google, Yandex, Yahoo vs- kullandığınıza bakıyor ve buna göre bir etiketleme yapıyor. Eğer gönderdiğiniz e-posta PGP ile şifrelenmiş ise veya gönderilen dil Fransızca olarak ayarlanmışsa bunları alt etiket mantığı ile etiketliyor.

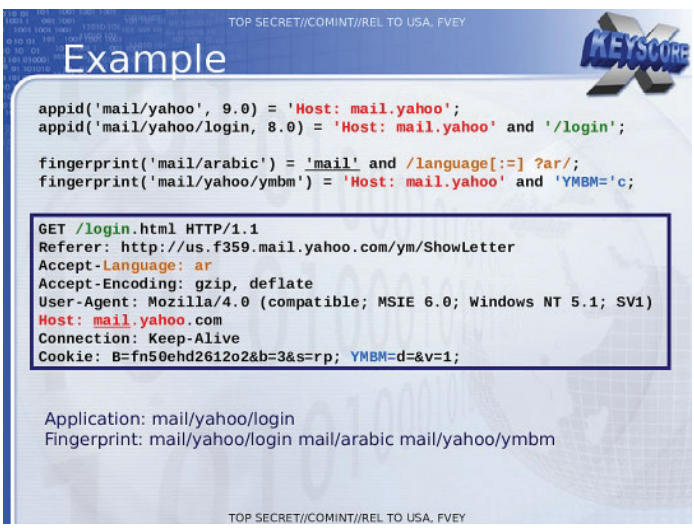
XKeyscore, Linux sunucuları -genellikle Red Hat sunucuları- üzerinde çalışan bir sistemlerden oluştuğu bilmekte. Apache web sunucusunu -XKeyscore web tabanlı bir sistem- kullanıyor ve toplanan verileri MySQL veritabanlarında depoluyor. Sunuculardaki dosya sistemleri NFS ve Autofs servisleri tarafından gideriliyor ve tabi ki zamanlanmış görevler için CRON scriptler kullanılıyor. Bu kadar büyük verileri işleyen ve saklayan sistem aslında herkesin az çok aşina olduğu servisler ile yönetiliyor.

Sistemin ne olduğunu gördük. Aslında baktığımızda bu kadar büyük veri akışının olduğu sistem için oldukça mütevazi ve basit bir konfigürasyona sahip. Dolayısıyla, bu sistemi daha efektif kullanmak gerekiyor ki toplanan onca ham veri kolayca işlenebilsin. Bunun için toplanan veriler, GENESIS adında özel bir dil ile appID, fingerprint ve microplugin adı verilen kurallara uygun bir şekilde kaydediliyor. AppID'ler, yakalanan trafik protokolünü tanımlamak için kullanılırken, fingerprintler belirli bir içerik türünü algılıyorlar. Her yakalanan trafik akışı bir appID'ye ve herhangi bir fingerprint'e atanıyor. AppID'leri kategoriler, fingerprint'leri etiketler olarak düşünebiliriz. Örneğin; Windows Update isteklerini "update_service/windows" appID altında, normal web istekleri "http/get" appID altında işleniyor. Öte yandan, THY'den bir bilet aldınız bu trafik XKeyscore tarafından "travel/turkishairlines" fingerprint ile ya da iPhone'nunuzda bulunan bir tarayıcıda gezinirken oluşturduğunuz trafik "browser/cellphone/iphone" ile tespit edilip etiketleniyor.

Yeni trafik bir XKeyscore sunucularına geldiğinde, sistem gelen verileri bu kuralların her birine karşı test ediyor ve trafiğin var olan patternlerle ile eşleşip eşleşmediğine bakıp depolıyor. Öte yandan, birden fazla appID tek bir trafik akışıyla eşleşiyorsa, en düşük "düzey" olan appID seçiliyor. Örneğin, XKeyscore, Yahoo postasından bir dosya ekini değerlendirirken, görselde olan tüm appID'ler eşleşiyor, ancak bu trafik akışıyla yalnızca "mail/webmail /yahoo/attachment" ilişkilendiriliyor.

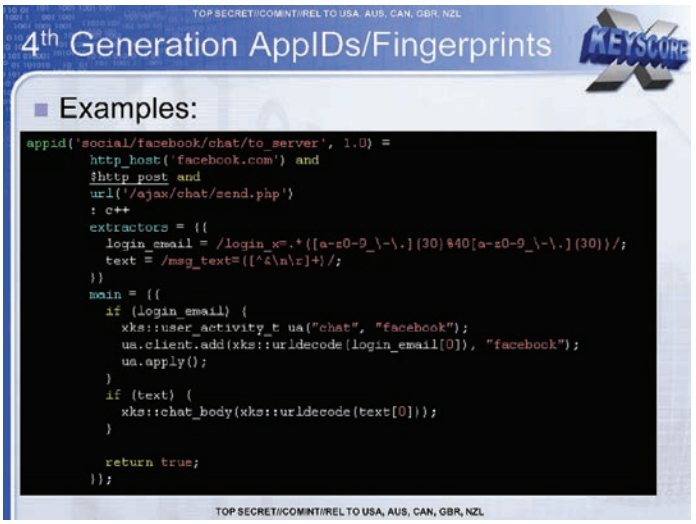


Daha net anlamak için, Arapça iletişim kuran kimse bir Yahoo e-posta adresine girdiğinde bu trafik "mail/yahoo/login" appID ile saklanacaktır. Öte yandan bu trafik akışı, "mail/arabic" parmak iziyle (dil ayarları) ve "mail/yahoo/ymbm" parmak iziyle (Yahoo tarayıcı çerezleri) eşleşip etkileniyor.



Belgeler, 2010 yılında XKeyscore'un yaklaşık 10000 appID ve fingerprint'e sahip olduğunu gösteriyor. Günümüzde bu sayının ne olduğu gerçekten merak edilesi.

Genesis adı verilen özel dil, bazı karmaşık pattern barındıran trafik türlerininin eşleşmesini yapacak kadar güçlü değildir. Bu durumlarda, dökümanlarda gözüktüğü kadarıyla Micropluginler devre girmete. Micropluginler, C/C++ ile yazılmış appID ve fingerprintlerdir.



Örnek olarak burada, yakalanan Facebook sohbet mesajlarını incelemek ve ilişkili e-posta adresi ve sohbet mesajının gövdesi gibi ayrıntıları almak için C++ kullanan bir microplugin görmekteyiz.

Sonuç: "Benim saklayacak bir şeyim yok"

Gözetimin çok eskilere dayanan bir kavram olduğunu biliyoruz fakat 1980'ler itibaren enformasyon teknolojileri sayesinde daha da arttığını ve zamanın düşünürleri, gözetim toplumlarını anlatan ve irdeleyen Karl Marx, Michel Foucault ve daha nicelerinin ne kadar haklı olduklarını görüyoruz. Eğer çevrimiçi iseniz sizi devletler, şirketler ve diğerleri izliyor. Öte yandan çevrimdışıyken de kayıt altına alınıyorsunuz. Kim olduğunuzdan ziyade ürettiğiniz verilere bakılıyor! Onlar için önemli olan ürettiğiniz veri ve yaptığınız eylemler. Kısacası, kimse sizin Muhittin Topalak olmanız ile ilgilenmiyor. 2013 yılında Snowden dosyalarının ancak ufak bir kısımdan görebildiğimiz kadarıyla, bize demokratik bir ortam olarak sunulan internetin aslında tüm mahremiyetimizi nasıl yok ettiğini gösterdi. Masumca kullandığımız servislerin ve ürünlerin aslında bize karşı kullanılan bir silah olduğunu bir daha gördük. Tüm bunları kanıtlarıyla birlikte daha yüzümüze vuran Edward Snowden'e saygılarla.

"-Neden kör olduk,
-Bilmiyorum, bunun nedeni belki bir gün keşfedilir,
-Ne düşündüğümü söylememi ister misin?
-Söyle,
-Sonradan kör olmadığımızı düşünüyorum, biz zaten kördük,
-Gören körler mi?
-Gördüğü halde görmeyen körler."
Körlük / Jose Saramago

Kaynaklar

https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/

https://theintercept.com/2015/07/02/look-under-hood-xkeyscore/

https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

https://en.wikipedia.org/wiki/XKeyscore

Halit İnce / halit.ince@infinitumit.com.tr

AÇIK KAYNAK İSTİHBARAT YAZI DİZİSİ BÖLÜM II: ORGANİZASYONLAR

İlk yazımızda da bahsettiğimiz üzere, açık kaynak istihbaratın arkasındaki temel prensip, verilerint "açık kaynak" olarak nitelendirdiğimiz kaynaklardan elde edilmiş olmasıydı. Aynı zamanda bu yazımızın üzerinde duracağı başlık olan, bir kurum veya kuruluş üzerinde istihbarat analizi yapmak istediğimizde de metodolojimiz bu tanıma uygun ve aynı zamanda gerçekleştirilebilir olmalıdır. Arayışımızın kapsamı, detayları ve elde edilmek istenen sonuca göre her hedef için gerçekleştirilmesi gereken analiz farklı olsa da serimizin bu yazısında bir organizasyon üzerinde yapılabilecek araştırma sonucunda hangi bilgiler elde edilebilir gibi genel bir konu üzerinde durmaya çalışacağız.

Yazımızın ilerleyen kısımlarında teknoloji keşfi, geçmişe dönük bilgi edinme, gün yüzünde tutulan sırlar ve organizasyonların korkulu rüyası, yer altındaki topluluklardan bahsedeceğiz ve risk teşkil etmemesi açısından bir hedef örneği koymak yerine platformların ekran görüntüleri ile bu yapıları açıklamaya çalışacağız.

İlk İzlenim ve Teknoloji Keşfi:

Serimizin ilk yazısında; *Whois*, *Wappalyzer* araçlarından bahsetmiştik. Hedef organizasyonumuzun web sitesinde kullandığı teknolojilerden bu şekilde haberdar olmanın mümkün olduğunu da söylemiştik. Organizasyonlar için teknoloji keşfinde önemli olan bir diğer nokta ise iş ilanları ve bu platformlarda oluşturdukları şirket profilleridir. İş ilanlarında firmaların kullandığı teknolojilerini, altyapı hizmeti aldığı şirketleri ve/veya kullandıkları marka ürününü spesifik olarak belirtmesi, aradığı çalışanı daha kısa sürede bulma umuduyla başlayıp istenmeyen sonuçlara yol açabilir. Örneğin A şirketi, kullandığı programlama dili çatısında ve web sunucusunda tecrübe aradığını belirtmek isterken saldırganlar tarafından en çok aranan bilgileri ifşa etmiş oluyor. Bu sebeple Linkedin gibi önemli profesyonel kullanıcı platformlarında bulunan ilanlar ile yapılabilecek teknoloji keşfi, organizasyonların genel olarak farkında olmadığı önemli bir kaynak niteliğindedir.

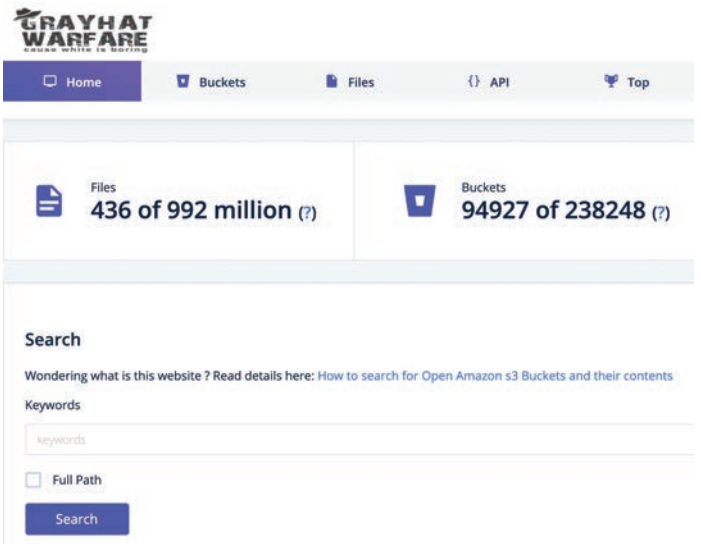
Geçmişe Dönük Bilgi Edinme:

Bir organizasyonun yıllarla kazanılan eklentiler ve içerikler ile biriken, oldukça nitelikli istihbaratlar elde edilebilecek bir web sitesinin olduğunu ve alınan bir kararla yakın bir geçmiş zamanda tamamen yenilendiğini düşünelim. Bir web sitesi sıfırdan kurulmuş bir altyapı ile bilgi sızıntısı gerçekleştirmeyecek şekilde yeniden dizayn edilse, eski yapıda sızdırdığı bilgilerinin üzerini örtmüş kabul edebilir miyiz? Archive.org, belirli zamanlarda geçmişten günümüze web sitelerin anlık durum görüntülerini kaydeden ve bir veri tabanında uzun süreler boyunca tutabilen, kendi tabirleri ile "internet arşivi" bir platformdur. Bu platform sayesinde istenilen alan adının, bir organizasyona ait olduğunu varsayarak ilerliyoruz, geçmişe dönük durum kayıtları üzerinde inceleme yapabiliriz. Kronolojik bir istihbarat örüntüsü oluşturma, gelecek tahminleme gibi durumlarda kullanmak için vazgeçilmez bir araç olduğunu söyleyebiliriz.

Depolama Servisleri Can Yakabiliyor:

Yanlış yapılandırılan depolama servisleri sebebiyle yetkisiz erişime açık birçok veritabanı, Amazon S3 Buckets ve/veya DigitalOCean Spaces gibi veri depoları tahmin edilemeyecek

seviyede veri ihlaline yol açabiliyor. Proje kaynak kodları, parolalar, log dosyaları ve daha birçok türde dosyanın ihlali birkaç kolay anahtar kelime uzağımızda bulunuyor. Bu ihlallerin yanı sıra, saldırı vektörlerine ve sosyal mühendislik saldırılarına yardımcı olabilecek, hedef organizasyonun çalışanlarına ait kişisel bilgilerin (kimlik numarası, adres, telefon, mail adresleri vb.) ifşası da istihbarat analizlerinde dikkat edilmesi gereken noktalardan biridir. Bu açıdan bakıldığında erişime açık bu depoların keşfi ve keşfedilmiş depolar üzerinde sorgu gerçekleştirebilmek zor gibi gözükse de bu amaç için gerçekleştirilmiş araçlardan birini örnekleyerek gerçekleştirimin ispatını yapabiliriz.



buckets[.]grayhatwarfare[.]com adresinde erişime açık milyonlarca Amazon S3 deposunda bulunan birçok farklı türde dosya üzerinde anahtar kelimeler ile arama yapabiliyoruz. Bu aramalar ile geliştiricilerin ve sistem yöneticilerinin farkında olmadığı erişime açık birçok dosyaya ulaşabiliyoruz. Örneğin sadece ".log" diyerek genel bir arama yaparak log dosyası barındıran s3 depolarını birlike görelim:

Filename	Size
Backups/Daily_Log_20171231_[redacted].log	1.44MB
Backups/Daily_Log_20180228_[redacted].log	1.28MB
Backups/Daily_Log_20180331_[redacted].log	1.41MB
Backups/Daily_Log_20180430_[redacted].log	1.37MB
Backups/Daily_Log_20180531_[redacted].log	1.41MB

Şekil 1: URL kısmı gizlenmiş örnek sorgu

Mailler, Kullanıcı adları, Parolalar ve Daha Fazlası...

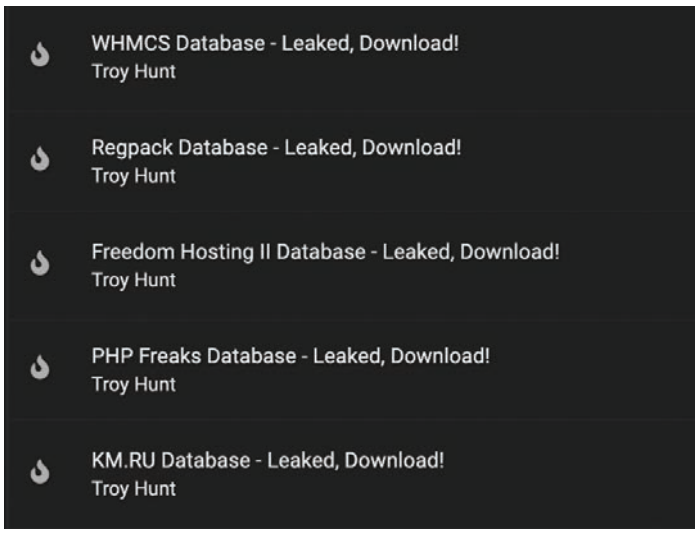
2000'li yılların başında kaba kuvvet saldırıları sıkça kullanılan yöntemlerden biriydi. Geçerli bir kullanıcı hesabı bulunan bir servis veya uygulama üzerine bir "wordlist" aracılığıyla art arda denemeler gerçekleştirip başarılı sonuçlar elde edilebiliyordu. Fakat organizasyonlar artık kaba kuvvet saldırılarına günümüzde bu kadar kolay geçit vermiyorlar. Hatalı oturum açma işlemlerini anlıyorlar, kayıtlarını tutuyorlar ve en önemlisi anladıkları kaba kuvvet saldırılarını rahatça engelleyebiliyorlar. Geçen zamanda zorlaşan diğer noktalar da; parolaların nispeten daha karmaşıklaşmış olması ve yaygınlaşan organizasyonlara özgü parola karmaşıklık politikaları denebilir. Geçmişten günümüze bu süreçte varmak istediğimiz en önemli nokta: sızıntı veri tabanları. Kaba kuvvet saldırıları, aktif kullanım alanlarındaki önceliğini gün geçtikçe yerini sızdırılmış veri tabanlarından elde edilen parolalarla yapılan denemelere bırakıyor gibi görünüyor.

Sızdırılmış veri tabanları konusunda önemli olan nokta, dünyanın en güvenli parola politikasını kullanmış olsanız dahi üye olduğunuz platformdan veri sızdırılırsa parolanızın kuvvetinin neredeyse hiçbir anlamı kalmıyor. Bir sızıntı sonrası, üye olduğunuz platformun parolanızı kendi veri tabanlarında özeti alınmış şekilde tutup tutmamasına göre iki olası durum gerçekleşecektir diyebiliriz. Eğer parolanızı, özet algoritmalarından geçirmeden saklıyorlarsa bir sızıntı halinde parolanızın gerçek haline direkt erişim mevcut olacaktır. Diğer durumda, yani bir özet algoritmasından geçirilerek saklanması durumunda, ise bu özetin gerçek karşılığını bulmaları gerekecek ve eğer siz yeterince "özgün" bir parola kullanmadıysanız, parolanıza erişim yine rahatça sağlanacaktır.

Organizasyonlara yönelik e-mail adresleri, kullanıcı adları gibi önemli bilgileri parolaları ile birlikte elde edebildiğimiz en önemli kaynaklar, yukarıda da bahsettiğimiz sızıntı veritabanları. Sızıntı veri tabanları, parola yönetim politikaları olmayan veya belirli aralıklarla parolalarını yenilemeyen bilinçsiz organizasyon çalışanları yüzünden organizasyonlar için tehlike çanlarıyla eş anlama gelebilecek bir kelime oldu artık günümüzde. Gerçek senaryolarda sıkça karşılaştığımız durumlar arasında sızıntı veri tabanlarından elde edilen bilgiler ile gerçekleşen başarılı oturum açma işlemleri önemli bir yere sahip. Yetkili, yetkisiz veya az yetkili fakat her durumda parolalarının sızdırıldığından haberleri olmayan ve aynı parolayı tüm hesaplarında kullanan organizasyon çalışanları, kendilerine zarar vermekle kalmıyor beraberinde çalıştıkları organizasyonlar için de büyük tehlikeler oluşturuyorlar.

Sızıntı veri tabanları bazen ücretsiz, bazen satılık ve bazen de kredi sistemleri ile çalışan takas usulü ile rahatça ele geçirilebiliyor. Dark veya yüzey web'deki forumlar, IRC kanalları, Telegram grupları ve diğer mesajlaşma uygulamalarında bulunan odalar adeta internetin karanlık yüzünün birer amatör tasviri gibi varlıklarını sürdürmeye devam ediyorlar. Bu toplulukların aktif olanları takip edildiğinde, birçok güncel hacking vakasının kokusu alınabiliyor ve bir adım önde olmak isteyen organizasyonlar için savunma puanı ve alınabilecek aksiyonlar nispeten artabiliyor.

Örneğin aşağıdaki görselde kredi sistemiyle alışveriş/takas yapılan bir yeraltı forumunda, haveibeenpwned platformunun kurucusu Troy Hunt'ın, sızdırılmış güncel ve kıymetli veritabanlarını elde etmek için paylaştığı "nispeten" daha az kıymetli(!) veri tabanlarını paylaştığını görebilirsiniz:



Sızıntı veri tabanlarının sorgulama, araştırma ve elde etme kaynak/metodolojilerine kötüye kullanım risklerinden dolayı bu yazımızda yer vermeyeceğiz fakat bunları elde etmek için herhangi bir teknik bilgi gerekmediğinin de tehlikenin boyutunu anlamak için altını çizmekte fayda var. Naçizane, organizasyonların bu konuda bilinçlendirilmeleri ve gerekirse hizmet almaları gerektiği kanaatindeyim.

Toparlayalım:

Açık kaynak istihbarat toplama üzerine konuştuğumuz ikinci yazımızda, günümüzün en olası kurban adayları olan organizasyonlar üzerinde durmaya çalıştık. Bu organizasyonlar bir saldırganın hedefi olurken sızıntı veri tabanlarının, yani organizasyona ve çalışanlarına ait oturum açma bilgilerinin nasıl internette kolayca erişilebildiğinden bahsetmeye çalıştık. Organizasyon odaklı açık kaynak istihbarat analizi incelemesi yapmaya çalıştığımız, serimizin ikinci yazısını okuduğunuz için teşekküler, devam yazılarımızda görüşmek üzere.

ÖzgürKon

16-17 Mayıs 2020
Çevrimiçi!

ÖzgürKon 2020, özgürlük üzerine çevrimiçi ve uluslararası bir konferanstır.

Eğer özgürlük üzerine bir sözünüz var ise ÖzgürKon sizi bekliyor!

www.ozgurkon.org
@OzgurKonorg

Artist
Eylül Doğruel
Istanbul, Turkey

Small Tech Foundation
Aral Balkan
Cork, Ireland

FSFE
Alexander Sander
Berlin, Germany

Bilgi University
Chris Stephenson
Istanbul, Turkey

İskele47
Bager Akbay
Istanbul, Turkey

Özgür Yazılım Derneği

hs.ist hackerspace istanbul

Small Technology FOUNDATION

FREE SOFTWARE FOUNDATION

ARKAKAPI SİBER GÜVENLİK DERGİSİ

OMEGA HUKUK BÜROSU

MADE4SENSE

monobilişim

Siber Savaş ve DDoS

İnternetin hayatımıza girmesiyle birlikte büyük bir kolaylık sağladığı aşikârdır. Artık, para transferi veya yatırım yapmak için bankaya, alışveriş yapmak için mağazaya hatta eğitim almak için kursa gitmeye dahi gerek yok. Tek bir tuşla istenilen tüm bilgilere erişebildiğimiz internet üzerinden yapabildiklerimiz bugün artık neredeyse sınırsız durumda. GSM operatörlerinin her geçen gün daha ucuza internet paketleri sunmasıyla birlikte bugün Türkiye'nin hatta dünyanın neresinde olunursa olunsun internete erişmek mümkün. Dolayısıyla da artık her yanımızın internetle kaplı olduğu yeniçağda, bir o kadar da tehdit altındayız demektir.

Bilgi savaşlarının yaşandığı bu yıllarda artık devreye bir başka önemli aktör girmiştir: "**Siber Savaş**"

Günümüzde, konvansiyonel savaşın uzağında olduğumuzu söylemek mümkün. Her ne kadar halen dahi konvansiyonel savaşlar son yıllarda özellikle Ortadoğu'da yaşanıyor olsa da siber savaşlar arka planda devam etmektedir. Üstelik bu siber saldırılar, belli bölgede değil, ucu bucağı olmayan neredeyse sınırsız diyebileceğimiz bir ortamda gerçekleşiyor yani siber uzayda...

Siber savaş; bir devletin başka bir devlete ait siber uzayda yer alan varlıklarına zarar vermek, manipüle etmek, çıkarları çerçevesinde kullanmak, istihbari faaliyetler gerçekleştirmek (siber istihbarat), kesinti oluşturmak, tamamen hizmet veremez duruma getirmek üzere gerçekleştirilen saldırı faaliyetlerinin tümüdür. Siber savaş sadece devletler arasında değil şirketler/kişiler/gruplar arasında da olabilmektedir. Siber savaşın en önemli özelliklerinden birisi de *sessiz* gerçekleşir ancak etkisi oldukça ses getirmektedir. (Hizmet kesintileri, kritik alt yapı sistemlerinin çalışmaması, ekonomik zarar, hassas bilgilerin çalınması, bilgi manipülasyonu/kirliliği, sistemlerin tahribatı vb...)

Bir Siber Savaş Silahı: DDoS

2019 Ekim ayının son haftasında ülkemizde, özellikle en önemli bankalardan birine ve büyük internet servis sağlayıcılarından birinin etkilendiği/hedeflendiği bir **DDoS** saldırısıyla karşı karşıya kaldık. (Disributed Denial-of-Service, internete bağlı bir sistemin hizmetlerini geçici veya süresiz olarak aksatarak, bir makinenin veya ağ kaynaklarının asıl kullanıcılar tarafından ulaşılamamasını hedefleyen bir siber saldırıdır.)

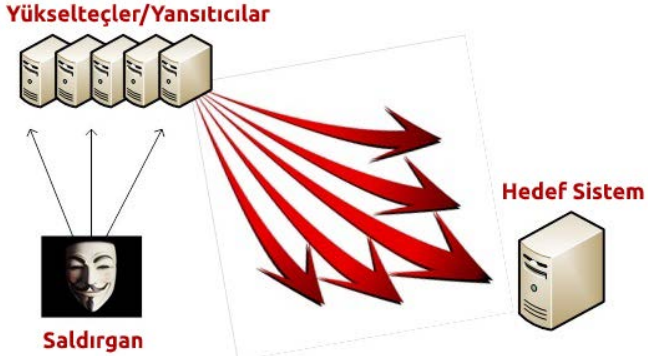
Öncelikle ilgili banka kurumuna, herhangi bir sızma olayının gerçekleşmediğinin altını çizmekte fayda var.

DDoS saldırısının sonucunda, ilgili bankanın internet sayfası, mobil uygulaması, ATM ve POS cihazları vatandaşa hizmet veremez hale geldi. Yanı sıra, bankanın hizmet aldığı ilgili internet sağlayıcısı da saldırıdan etkilendiği için bazı diğer müşterilerde de servis kesintileri yaşandı.

Düşünün ki, ülkemizin birçok bankasına ve internet servis sağlayıcılarına yüklü miktarlarda ve daha uzun süren bir DDoS saldırısı yapılsa durum ne olurdu? Söyleyelim; POS cihazları çalışmayacağından kredi kartıyla alışveriş yapamazdınız (örneğin; market, yakıt ve çeşitli ödemeler...), ATM'ler çalışmayacağından para çekemezdiniz, internet servis sağlayıcılarında hizmet kesintisi olduğundan web sitelerinize erişim sağlanamazdı, sosyal medyaya erişim sağlanamazdı. Bunlar maalesef hikâye değil ve bu örnekler çoğaltılabilir.

DDoS Saldırısının Perde Arkası

Yapılan teknik incelemeler sonucunda, "**yükselteç/yansıtıcı**" protokoller (bir bağlantı isteği yapıp 10-50-100… daha fazla cevap almak) kullanıldığı için ülkemizdeki ilgili kurumları etkileyen DDoS saldırısının türü "**DrDoS**" (Distributed Reflected Denial-of-Service) olarak kayıtlara geçmiştir.



Yukarıdaki şema, DrDoS saldırısının sürecini anlatmaktadır. Konu bağlamında şemayı özetle açıklamak gerekirse;

Saldırganlar, hem IP adreslerini gizlemek maksadıyla hem de saldırının etkisini arttırmak için "IP Spoofing" yöntemiyle saldırı paketinin kaynak IP adresini hedeflerindeki sistemin IP adresi olarak tanımlayıp yükselteç/yansıtıcı protokoller barındıran açık sunuculara "TCP SYN-ACK" isteği gönderirler, yansıtıcı sunucular da isteğin nerden geldiğine bakarak boyutu daha büyük olan cevabı ise saldırganların hedefindeki adrese iletir.

Böylece, yoğun ağ trafiğinden dolayı hedef sistemin kaynakları tükeneceğinden kullanıcıları tarafından ulaşılamaz hale gelmektedir.

DDoS koruma konusunda dünyaca bilinen **Radware** şirketinin araştırmacıları, geçtiğimiz haftalarda **Amazon**, **SoftLayer** ve bazı telekom altyapı şirketlerine büyük boyutlarda "TCP SYN-ACK Reflection DDoS" saldırıları gerçekleştirildiğini bildirdiler.

Araştırmacıların analizlerinde, "*Radware şirketi olarak son 30 gün içerisinde büyük şirketlere TCP reflection saldırısı kullanılarak yapılan suç girişimleri tespit ettik. Saldırılar yalnızca hedeflenen ağları etkilemekle kalmadı, kullanılan yansımalar dünyadaki ağları da bozdu ve birçok işletme tarafından şüpheli olarak tanımlanan SYN-flood saldırıları tespit edildi.*

… Bu saldırılardaki sahte kaynaklar, hedeflenen IP adreslerinin aralıklarını bildiriyor ve hedeflenen yansıtıcılar RST paketleri almadığı sürece 'carpet bombing' saldırısına maruz kalarak SYN-ACK paketlerini tekrar tekrar iletmek zorunda kalıyor." ifadelerine yer verildi.

"**Carpet Bombing**" terimi, kelime manasına düz olarak bakıldığında "halı bombardımanı" demek ancak teknik olarak buradaki kullanım amacı, hedeflenen IP aralığına karşı yapılan DrDoS saldırısıyla geniş yüzeyi aynı anda bombalama anlamı taşımaktadır.

Küresel olarak, kötüye kullanıma açık olan sistemlerdeki **etki arttırma faktörleri**, yansıtma IP adresinde çalışan servis tarafından yeniden iletilen SYN-ACK sayısına bağlı olarak değişir. Servis ne kadar güçlüyse iletilen paket de o kadar artar. Bağımsız bir araştırmaya göre dünya üzerinde inanılmaz bir saldırı gücü oluşturabilecek, bir saldırı vektörünün gücünü ortalama **112 kat artırabilen 4.8 milyondan fazla** cihaz bulunuyor. Saldırının gücünü **80.000** katlık bir faktöre yükseltebilecek binlerce sistem bulunması da saldırganlara büyük bir saldırı gücü kazandırıyor.

Ülkemiz kurumlarına karşı yapılan bu DDoS saldırısının arkasında kimin olduğu belli değil ama bu saldırılar, 5G teknolojisinin gelişmiş bant genişliği ve daha yüksek hızları ile DDoS saldırılarının etkisini ve getireceği riskleri büyük ölçüde arttıracaktır.

Kurumların Sürekli Karşılaşacağı Siber Tehditler

DDoS saldırılarının yanı sıra, yıllar içerisinde birbirleri arasındaki rekabet oranları ne kadar değişkenlik gösterse de aşağıda bahsedilecek siber tehditlerle sürekli karşılaşacağız…

Phishing (Oltalama)

E-posta ortamı, web sitesi veya sosyal medya aracılığıyla yasadışı yollarla bir kişinin parolasını ya da kredi kartı detaylarını öğrenmeyi amaçlayan saldırı türüdür.

En az 4 yıllık istatistikleri incelediğimizde, özellikle kurumlara karşı yapılan hedef odaklı siber saldırılarda, sistemlere ilk giriş noktası olarak iyi kurgulanmış bir senaryoya sahip phishing saldırılarının yapıldığını görmekteyiz.

Ransomware

Fidye yazılımı, şantaj yazılımı veya fidye virüsü olarak bahsedilen yazılımlar "ransomware" olarak adlandırılan fidye yazılımlarına verilen genel bir isimdir. Fidye virüsleri, bulaştığı bilişim sistemleri üzerinde dosyalara erişimi engelleyerek (şifreleyerek) kullanıcılardan Bitcoin yoluyla fidye talep eden zararlı yazılımlardır.

Veri kaybı ve kesinti süresi, fidye yazılımının en büyük sonuçlarıdır. Çoğu şirket, bir fidye yazılımı saldırısı sonucu veri kaybı ve büyük kesinti yaşadıklarını söylüyor. Bu sonuçların her ikisi de, özellikle yüzlerce çalışanı olan büyük işletmeler için son derece maliyetlidir. Önemli kesinti süreleri milyonlarca dolar gelir kaybına ve tüketici güveninin azalmasına neden olabilir.

İstatistiklerle Fidye Yazılımı

- SafetyDetectives'in araştırmalarına göre, uzmanlar, fidye yazılımı saldırılarının, işletmelere yaklaşık 11 milyar dolara mal olacağını tahmin ediyor. Bu da 2015 yılında rapor edilen 325 milyon dolardan önemli bir artış.
- Küçük ve orta ölçekli işletmeler için ortalama fidye ödemesi genellikle $500 ila $2.000 arasındadır. Bu miktar daha büyük işletmeler için önemsiz gibi görünse de, verilerini kaybetmeyi göze alamayan küçük işletmeler için daha kritik olabiliyor.
- Birçok hizmet sağlayıcısının %99'u, Windows (%88) işletim sistemlerinin en sık fidye yazılımı saldırıları tarafından hedeflendiğini söylüyor. Ancak bu, OS X (%2), Linux (%2) ve Android'in (%8) bağışık olduğu anlamına gelmez. Herhangi bir işletim sistemi bir fidye yazılımı saldırısına kurban gidebilir.

- Fidye yazılımı saldırılarının yaklaşık %60'ı yerleşik URL'ler olarak e-posta yoluyla gönderilmektedir.
- Fidye yazılımı, popülerliğini artırmaya devam ederek Verizon'da ilk beş tehdit arasına girmeyi başardı.
- 2017-2018 verilerine göre, fidye yazılımı saldırılarından en çok etkilenen ilk 10 ülke arasında 10. sırada Türkiye bulunmaktadır.
- 2015 yılından bu yana, 2017 yılı fidye yazılımlarının en etkin olduğu yıldır.

BEC Saldırıları (Business E-mail Compromise)

Banka havalesi yapan ve yurtdışında tedarikçileri olan şirketleri hedef alan bir tür dolandırıcılıktır. Finansmanla ilgili veya banka havalesi ödemeleriyle ilgilenen yöneticilerin veya üst düzey çalışanların kurumsal veya kamuya açık e-posta hesapları ele geçirilerek ifşa olmuş veri tabanları, tuş kaydediciler (keylogger) veya phishing saldırıları yoluyla ele geçiriliyor. Sonrasında ise e-posta mesajlarının arasında istek, ödeme, transfer ve acil gibi kelimeler içeren konular tespit edilerek ava çıkılıyor...

BEC saldırganları, çalışan ve yöneticileri kandırmak için sosyal mühendislik yöntemlerini kullanarak genellikle, CEO ya da banka havalesi yapmak için yetkili herhangi bir yöneticiyi taklit ederler. Potansiyel hedef mağdurlarını ve organizasyonlarını dikkatlice araştırmakta ve yakından takip etmektedir.

BEC saldırıları, 2016 yılında, dünya genelinde şirketler için ortalama 140.000 Dolar zarara yol açmıştır.

Siber Saldırılardan Korunmak için Kurumsal Önlemler

- Şimdiki zamanın ve geleceğin konusunu olan **siber güvenliğe yatırım yapın!**
- Savunma amaçlı kullanılan ürünlerin (yazılımsal, donanımsal, bulut tabanlı…), ihtiyaçlar doğrultusundaki dinamiklere göre doğru bir şekilde yapılandırılması gerekmektedir.
- Yılda bir defa mutlaka kurum sistemlerinize karşı içeriden ve dışarında olmak üzere tabir-i caizse uçtan-uca **penetrasyon testleri**nin yaptırılması gereklidir.
- Penetrasyon testinin yapılmadığı zaman aralıklarında sistemler düzenli olarak güvenlik taramalarından geçirilerek çıkan **zafiyetlerin yönetimi** sağlanmalıdır.
- Eğer kurum içinde SOME gibi bir güvenlik birimi varsa sistemlerinizin efektif bir şekilde izlendiğinden emin olun, eğer siber güvenliğe ekip ayıracak bütçeye sahip değilseniz bu işi dışarıdan sağlayacağınız bir SOC (Security Operation Center) hizmetiyle çözebilirsiniz. Böylece sistemleriniz güvenlik bakış açısıyla sürekli izlenecek ve SOC'nin diğer yan bileşenleriyle de kurumunuzun siber güvenlik olgunluk seviyesini arttırmış olacaksınız.
- **Siber tatbikatlar**ın, düzenli zaman aralıklarında, doğru kişilerce ve en önemlisi; yaşadığımız DDoS saldırısı örnek alınarak *gerçek senaryolarla* yapılması gerekmektedir.
- Kurumların, siber saldırısı esnasında ve sonrasında uygulayabilecekleri **A, B, C… planları** olmalıdır.
- Personellerinizin bilgi güvenliği farkındalığını arttıracağı eğitimler organize etmelisiniz.

Konuda geçen bu tür büyük kurumlarımızın, bu gibi DDoS saldırısı esnasında, ilk andan itibaren sosyal medya üzerinden **objektif** olarak bilgilendirmelerin yapılması gerekmektedir. Böylece, kullanıcıların yargılamalarıyla değil büyük ölçüde destekleyici paylaşımlarıyla yanıt alacaksınız.

Oğuz Aydınyılmaz - aydinyilmazoguz@gmail.com

HTTP/3 ile TCP Tarih mi Oluyor?

Yıllar geçtikçe web sayfaları daha fazla komplike olmaya ve bunun sonucunda protokol olarak bir takım değişimlere kaçınılmaz olarak maruz kaldı. Veri dilinde konuşmak gerekirse: 2010 - 2020 yılı arasında bir URL'e yapılan istek sonucunda transfer edilen veri boyutu %320 olarak artarak, 2020, Ocak ayında 10 milyon URL örnek havuzunda ortalama değeri yaklaşık olarak 2 MB civarındadır. [1]

Bu yazımda üst tarafta rakamlarla belirttiğim değişimin etkilerini gördüğümüz HTTP protokolünün yolculuğundan ve HTTP/3'ün bizlere ne getireceğinden bahsedeceğim.

TCP/IP protokollerinden biri olan HTTP (HyperText Transfer Protocol), geçen sene 30. yılını kutladığımız World Wide Web'in altındaki temel iletişim protokolüdür ve Hypertext dökümanlara ulaşmak için kullandığımız hyperlink'lere tıkladığımızda, sunucu ve istemci arasındaki mesaj formatlarının nasıl olacağını ve bu aradaki bağlantının nasıl gerçekleşeceğini belirlenmiş olan kurallar bütünüdür. Bu standart IETF[2] (Internet Engineering Task Force) ve W3C (World Wide Web Consortium) tarafından geliştirilmiş ve RFC (Requests for Comments) dökümanları altında toplanmaktadır. 1969 yılından beri geliştirilen ve devam eden RFC index'ine buradan erişebilirsiniz: https://tools.ietf.org/rfc/index

HTTP protokolünün şu ana kadar 5 versiyonu bulunmaktadır:

Bunlar: HTTP/0.9, HTTP/1.0, HTTP/1.1, HTTP/2, HTTP/3

Haydi hep birlikte bu 5 versiyona göz atalım.

HTTP Versiyonları:

1-) HTTP/0.9

HTTP protokolünün başlangıç versiyonu olarak tanımlanan bu versiyonda ilk başlarda herhangi bir numaralandırma yoktu. Daha sonraları ayırım yapmak için 0.9 olarak numaralandırılmıştır. Çok basit ve sade bir protokol olarak karşımıza çıkan bu versiyon 1991 yılında yayınlandı.

- **Desteklenen metodlar:** Sadece GET
- **İstek Davranışı:** Sadece GET Metodu + Dosya Yolu
- **Yanıt Tipi:** Sadece HTML
- **Bağlantı Yapısı:** Yanıttan sonra hemen bağlantı kapanmaktadır. Yani her bir istek için yeniden TCP bağlantısı açmamız gerekmektedir.
- HTTP Header/Başlıkları bulunmamaktadır. Ne HTTP durum ne de hata mesajı yer almaktadır. Kısacası aşağıdaki örnekte de görüleceği üzere şu anki kullandığımız versiyona göre kabiliyeti oldukça sınırlıdır.
- HTTP başlığı bulunmadığından dolayı sadece HTML dosyaları işlenebilmekteydi ve cookie, content-type, host header'ı vs gibi şu an kullandığımız olmazsa olmaz başlıklar bulunmuyordu.

İstek:

```
GET /arkakapi.html
```

Yanıt:

```
<HTML>
Arka Kapi Dergi
</HTML>
```

1 https://httparchive.org/reports/state-of-the-web

2 https://ietf.org/

2-) HTTP 1.0

HTTP/0.9 çok kısıtlı olması, Netscape tarayıcısının 1994 yılında kullanılmaya başlaması ve 90'ların ortalarına doğru internet'in artık daha da yaygınlaşması ile birlikte daha geniş çaplı bir ihtiyaç doğmuştu. Artık HTML'den fazlasını sunabilecek, istek ve yanıtta daha zengin meta veriler sağlayabilecek bir protokol lazımdı. Bütün bu gelişmelere nazaran Mayıs 1996 yılında HTTP çalışma grubu olarak adlandırılan (HTTP-WG) grubu, HTTP/1.0 uygulamalarını belgeleyen RFC 1945'i paylaştı.

Peki bu yeni protokol bizlere ne getiriyordu?

- **Desteklenen metodlar:** GET, HEAD, POST
- **Bağlantı Yapısı:** Yanıttan sonra hemen bağlantı kapanmaktadır.
- **Yanıt Tipi:** Content-Type HTTP başlığıyla birlikte HTML dosyalarından ziyade diğer dosyalar da işlenebilmekteydi. Örneğin; script, image (gif,jpg etc)
- Versiyon bilgisi her isteğin sonuna eklenmişti. `(GET / foo.html HTTP/1.0)`

İstek:

```
GET /arkakapi.html HTTP/1.0
User-Agent: NCSA_Mosaic/2.0 (Windows 3.1)
```

Yanıt:

```
HTTP/1.0 200 OK
Content-Type: text/html
Content-Length: 137582
Expires: Thu, 01 Dec 1997 16:00:00 GMT
Last-Modified: Wed, 1 May 1996 12:45:26 GMT
Server: Apache 0.84

<HTML>
A page with an image
 <IMG SRC="/myimage.gif">
</HTML>
```

3-) HTTP/1.1

HTTP/0.9 ve HTTP/1.0 versiyonlarında her bir istek için yeni bir bağlantı açmak ve yanıt gönderildiğinde de bu bağlantıyı kapatmak gerekiyordu. Tabii her bağlantı kurulduğu zaman "TCP three-way handshake" de oluşmaktaydı. Daha iyi bir performans için sunucu ve istemci arasında bu gidip gelmeyi düşürmek oldukça önem arz ediyordu.

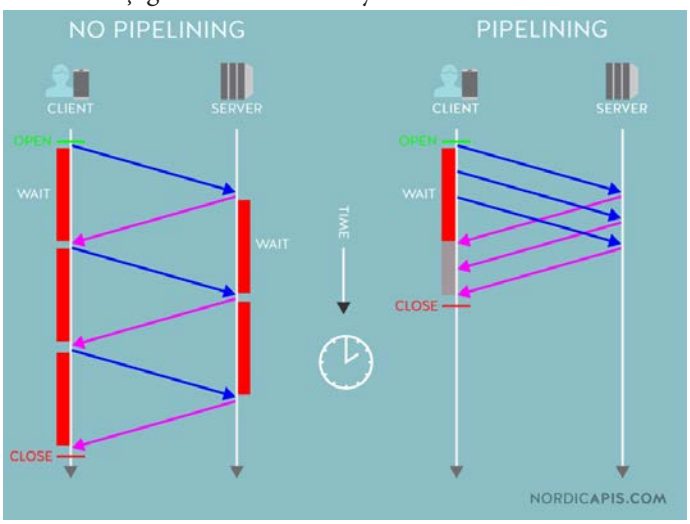
HTTP/1.1'in doğuşu yakındı ve HTTP'in ilk ana versiyonu olarak RFC 2068 içerisinde Ocak, 1997 yılında yayımlandı. Bu da aşağı yukarı HTTP/1.0'dan 6 ay sonrasına tekabül etmekteydi.

- Şu an genel olarak kullanılan versiyondur.
- **Desteklenen metodlar:** GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
- **Bağlantı Yapısı:** Uzun bağlantı (long-lived)
- "Host" header'ı sayesinde birden fazla domaini aynı IP addresinde barındırılması sağlandı.

HTTP/1.1'in gelmesiyle birlikte önceki versiyonlarda olan birçok kritik performans sorunları; *keep-alive* bağlantı yapısı, *chunked encoding* transferleri, gelişmiş cache mekanizması ve *request pipelining* gibi yeni özelliklerle çözüldü.

Kalıcı Bağlantılar (**keepalive connections**) bağlantının tekrar kullanılmasını,

Chunked Transfer Encoding ile veri stream etmeyi ve Request pipelining ile paralel istek gönderebilmeyi başardık. Yani toparlarsak sürekli bağlantı açıp kapatmak yerine tek bir TCP bağlantısı içerisinde Pipelining ile birlikte önceki isteğin yanıtının, geri dönmesini beklemeden hemen yapılabilir. Yanıtlar aynı sırayla ilk giren ilk çıkar mantığıyla (FIFO) istemciye dönecektir. Aşağıdaki örnekte inceyelebiliriz.



4-) HTTP/2.0

"Neden versiyon 2'ye ihtiyaç duyduk?" sorusunu sorduğunuzu duyar gibiyim. Zaten HTTP/1.1 ile de pipelining geldi ve birden fazla isteği yanıt beklemeden gönderebiliyorduk değil mi?

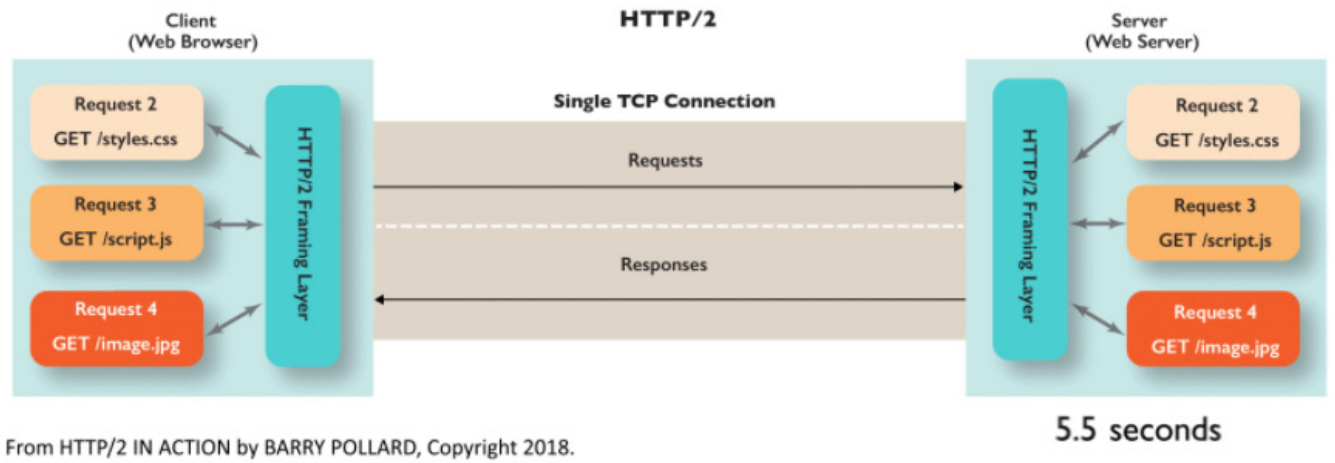
HTTP/1.1 pipelining'i sunucu tarafında uygulaması pratik değil hem de HTTP Request Smuggling[3] zafiyetine sebep veriyordu. Eğer pipeling kullanırken herhangi bir istek veya yanıtta paket kaybı oluşursa, bu istek ve yanıtın iletişim kurduğu TCP bağlantısındaki her şey bloklanmış oluyordu. Buna da "head-of-line blocking" denmektedir.

HTTP/1.1 97 yılında yayımlandığından bugüne kadar internetin yaygınlaşması ve websitelerin daha fazla dinamik & komplike hale gelmesiyle birlikte bu versiyonda iyileştirme yapma kaçınılmaz hale gelmişti.

3 https://portswigger.net/web-security/request-smuggling

Her bir statik dosyaya tek tek istek yapmak yerine bir frame layer içerisinde, istek yapılan sayfaya ait bütün dosyaları çağırmak üzere tasarlanmış yeni bir versiyon 2015 yılında RFC 7540 altında yayımlandı. Bir TCP bağlantısı içerisinde birden fazla paket göndererek iletişim gerçekleştirilen işleme Multiplexing denmekte ve bu HTTP/2'nin en önemli özelliğidir. HTTP 2.0 öncesinde bu özellik olmadığı için cdn1. cdn2. cdn3 gibi subdomain'ler kurarak, bir web sayfasındaki dosyaların daha hızlı yüklenmesi hedeflenirdi.

Aşağıda bir HTTP/2 isteğinin şemasını görüntüleyebilrsiniz:



From HTTP/2 IN ACTION by BARRY POLLARD, Copyright 2018.

HTTP/2 içerisinde bulunan push özelliğini ve HTTP/1.1 ile detaylı karşılaştırmaları içeren şu makeleye de göz atabilirsiniz. [4]

Peki H2'yi nasıl uygulayabiliriz?

Sunucu tarafında HTTP/2'ye geçmeniz için yapmanız gereken tek şey H/2 konuşabilen bir web server'a yükseltme işlemi veya sizin için konuşmasını isteyebileceğiniz bir CDN servisi kullanmanız gerekmektedir. Peki "biz H/2'ye geçtik, ya istemciler ne yapacak? Buradaki kaybımız ne şekilde ve trafiğimiz azalır mı?" diye sorarsanız eğer son iki yıl içerisinde yayımlanmış herhangi bir browser kullanılıyorsa HTTP/2 desteği bulunmaktadır[5]. (Kullanan kaldıysa IE, hala tam olarak destek vermemektedir.) *HTTP/2 için TLS gerekli midir?* sorusuna ise *-hayır-* yanıtını vermek teknik olarak doğru kabul edilebilir fakat bütün modern tarayıcılar H2'yi TLS harici desteklememektedir. Bu yüzden istemcilerinizin, sunucunuzda H2 versiyonu ile faydalanması için en azından TLS 1.2 desteğini vermeniz gerekmektedir.

HTTP/1.1 ve HTTP/1.2 arasındaki hız farkını buradan test edebilirsiniz:
https://http2.akamai.com/demo

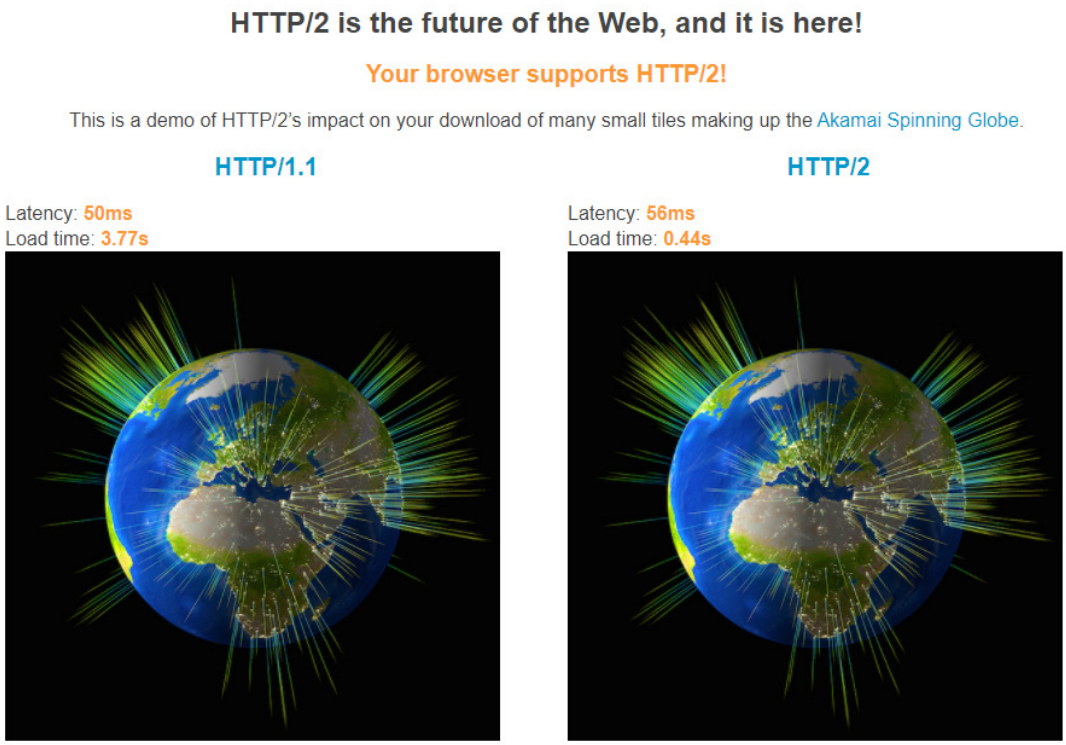
HTTP/2 Tarayıcı Desteği

Tarayıcı	Version >	
Chrome	41	
Firefox	36	
Edge	12	
Safari	9	OSX 10.11 >
Internet Explorer	11	Windows 10
Opera	28	
Safari - iOS	9.2	
Android Browser	51	
Chrome - Android	51	

4 https://medium.com/@factoryhr/http-2-the-difference-between-http-1-1-benefits-and-how-to-use-it-38094fa0e95b

5 https://caniuse.com/#search=http2

Brave tarayıcı üzerinden yaptığım testin ekran görüntüsü:



HTTP/2 destekleyen siteleri buradan test edebilirsiniz **https://tools.keycdn.com/http2-test**

5-) HTTP/3

Aslında bu yazının amacı sadece HTTP/3 üzerine olacaktı fakat HTTP versiyonlar arasında karşılaştırma yaparak ve gelişim sürecini gözlemleyerek daha iyi bir kanıya varılması açısından böyle bir yol izleme gereği duydum.

Bir Google çalışanı 2013 yılında daha hızlı bir protokol amacıyla QUIC (Quick UDP Internet Connections) adı altında yeni bir network taşıma protokolünü taslak olarak duyurdu. Daha sonra bu taslaktan IETF çalışma grubu tarafından evrimleştirilerek 2016 yılında HTTP/3 uygulama protokolü olarak tanıtıldı. QUIC, TCP + TLS + HTTP/2'ye çok benzemektedir. Bu versiyonun en büyük farkı TCP yerine UDP kullanılıyor olması ve aşağıdaki resimde göründüğü üzere QUIC, TLS 1.3'ü içerisinde bulundurarak veriyi taşımaktadır. Kısacası QUIC protokolü içerisinde her şey default olarak şifrelenmektedir.

QUIC'in TCP + TLS + HTTP2'ye göre en önemli avantajları şunlardır:

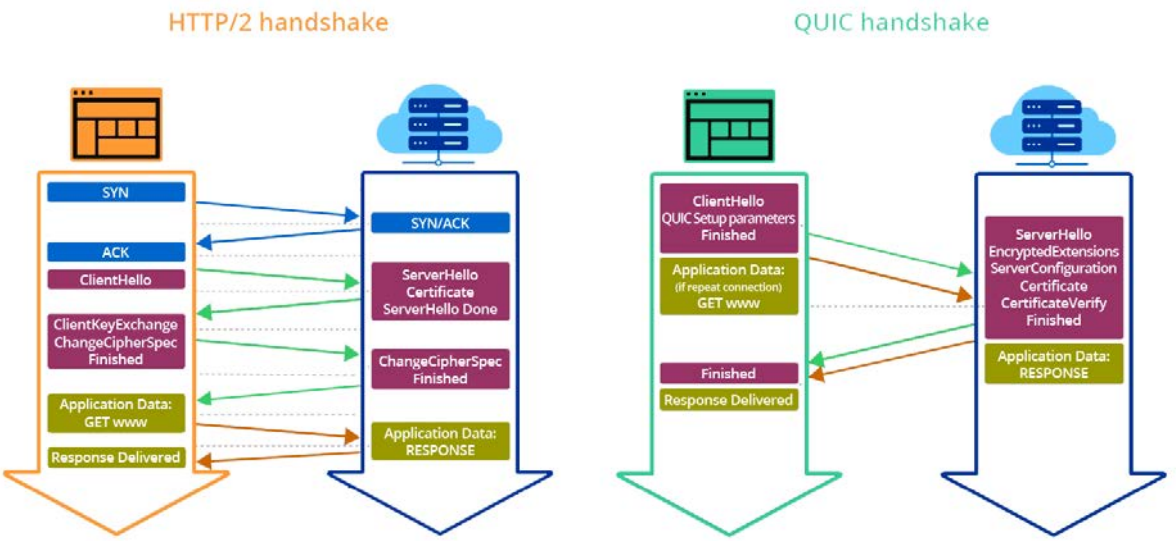
- Bağlantı kurma sürecindeki gecikmenin çok düşük olması
- Bağlantı Geçişi (Connection Migration)
- Multiplexing işleminde Head-of-line blocking sorunu olmaması
- Built-in TLS 1.3

Şimdi bunları hep beraber inceleyelim:

1-) Bağlantı kurma sürecindeki gecikmenin çok düşük olması

QUIC hand shakeler, TCP + TLS'de 1-3 arasında gidiş dönüşlere karşılaştırıldığında tek gidiş dönüş ile handshake'i tamamlamaktadır.

Yani; bir QUIC üzerinden işlem yapan istemci, sunucuya ilk kez bağlandığında handshake işlemini tamamlamak için istemcinin bir gidiş-dönüş yapması yeterlidir. İstemci CHLO (client hello) gönderir daha sonra sunucu, kaynak adres belirteci ve sunucunun sertifikaları da dahil olmak üzere istemcinin işleme devam etmesi için gereken bilgileri içeren bir REJ (rejection) gönderir. İstemci bir sonraki CHLO gönderdiğinde, sunucuya anında şifrelenmiş istekler göndermek için önceki bağlantıdan önbelleğe alınmış kimlik bilgilerini kullanabilir. [6] Aşağıdaki örnekte daha anlaşılır biçimde izah edilmiştir.



2-) Bağlantı Geçişi (Connection Migra1tion)

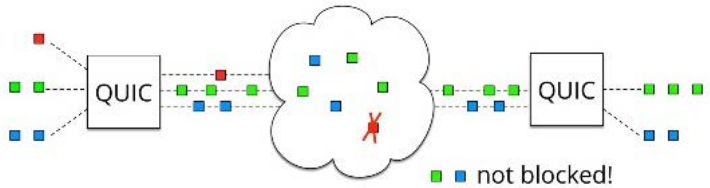
QUIC bağlantıları, istemci tarafından rastgele oluşturulan 64 bit connection ID ile tanımlanır. TCP bağlantıları ise 4 adımlı kaynak adresi, kaynak bağlantı noktası, hedef adres ve hedef bağlantı noktası ile tanımlanır. Bu şu anlama gelmektedir. Eğer bir istemci IP adresini (örneğin, Wi-Fi aralığından çıkıp hücresel ağa geçerse) veya portunu değiştirirse, artık aktif TCP bağlantısı geçerli olmaz . Bir QUIC istemcisi IP adresini değiştirdiğinde, kesinti sırasındaki istekleri kesmeden, yeni IP adresindeki eski bağlantı kimliğini kullanmaya devam edebilir. Yani burada IP adresi değiştiği esnada QUIC ile bir veri kaybı yaşamıyoruz. Ne kadar hoş değil mi?

3-) Multiplexing işleminde Head-of-line blocking sorunu olmaması

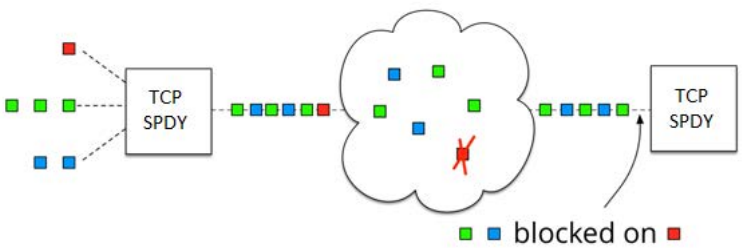
HTTP/2 içerisinde anlattığımız Multiplexing yani tek bir TCP bağlantısı üzerinden birden fazla paket göndererek daha hızlı bir iletişimi sağlamaktadır fakat bu iletişim sırasında tek bir paket kaybı oluştuğunda bu paket tekrar gönderilir ve TCP bağlantısı durmaktadır.

QUIC protokolünde ise UDP ile sunucu ve istemci arasında birçok bağımsız akış (stream) kurar. Eğer bu akışlardan birinde problem olursa veya bağlantı koparsa, tek bir akış için veri taşıyan kayıp paketler genellikle yalnızca belirli akışı etkiler. Diğer akışlar işlemine devam eder ve genel akışta bir problem olmaz.

6 https://docs.google.com/document/d/1g5nIXAIkN_Y-7XJW5K45IblHd_L2f5LTaDUDwvZ5L6g/edit



QUIC

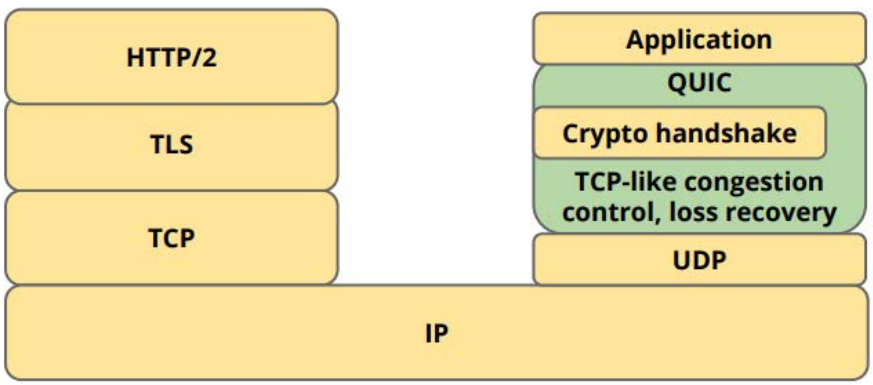


HTTP/2

4-) Built-in TLS 1.3

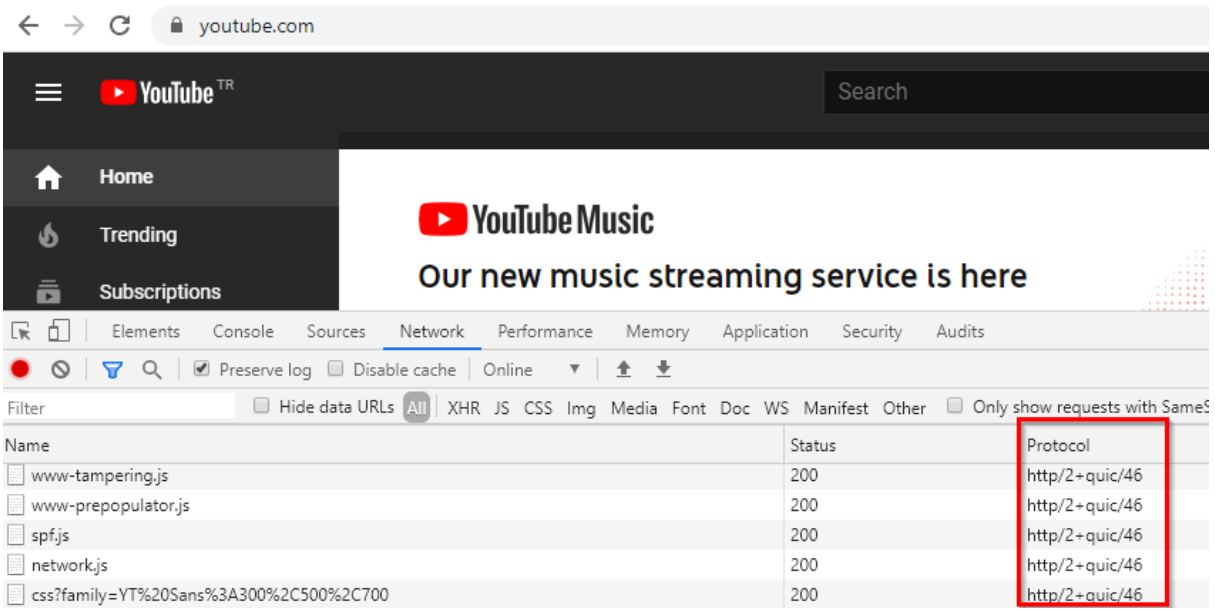
QUIC, HTTP/2'nin aksine TLS 1.3'ü default olarak barındırır ve clear text kullanımına izin vermez. Peki QUIC neden taşıma katmanı şifrelenmiş bir şekilde çalışmaktadır?

QUIC'in temel amaçlarından birisi de şifrelenmeyi her yerde default olarak getirip, MITM (Man-in-the-middle) ataklara karşı korunmayı amaçlamaktadır. Bu sayede QUIC akışlarının analiz edilmesi de çok zordur.



Peki HTTP/3'ü istemci olarak nasıl test edebiliriz ve kullanabiliriz?

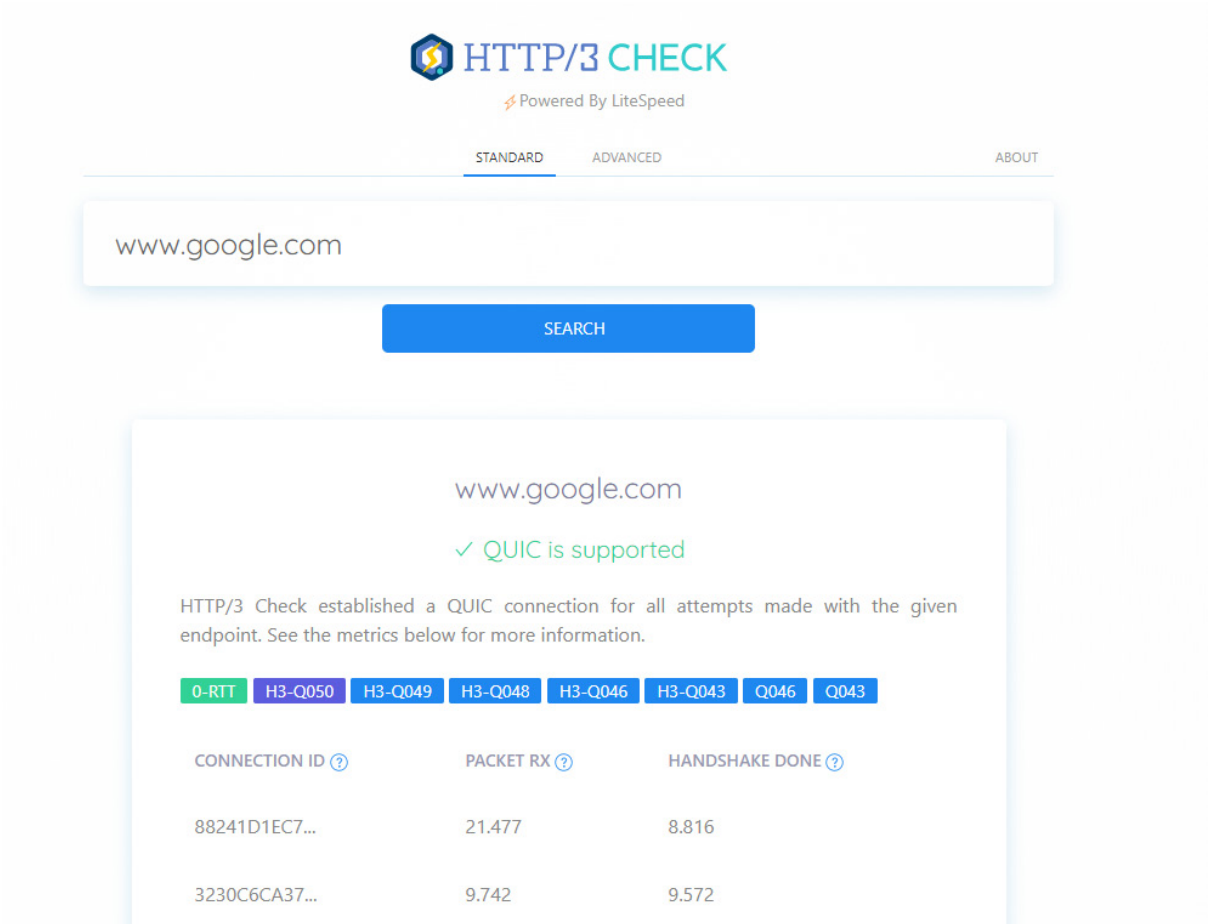
Şu an Chrome dışında hiç bir popüler browser HTTP/3'ü desteklememektedir. QUIC'i istemci olarak test etmek için Google Chrome'un şuanki son versiyonu olan Chrome 80 ile developer tool -> Network tabından direk test edebilirsiniz. Chrome 79+ versiyonlarında quic built-in bir şekilde gelmektedir. Protocol kolonunu açılması lazım tabii ki.



Ayrıca Google Canary ve Firefox Nightly versiyonlarını da kurup test yapılabilir.

CLI üzerinden `--enable-quic --quic-version=h3-24` komutlarıyla çalıştırmanız gerekmektedir.

Bir websitenin HTTP/3 desteğini buradan kontrol edebilrsiniz: https://www.http3check.net/



Sunucu tarafında HTTP/3'ü aktif etmek

Şu an HTTP/3 hala test aşamasında ve tam olarak bir standart olarak kabul görmediği için bu konuda araçlar biraz kısıtlı.

Denemek için Docker[7] üzerinde Caddy[8] kullanabilirsiniz.

Eğer Cloudflare'den CDN hizmeti alıyorsanız kolaylıkla QUIC'i aktif hale getirebilirsiniz. (Bunu yaptığınız takdirde sunucunuz üzerinde direk olarak herhangi bir ekstra işlem yapmanıza gerek kalmaz.) Dashboard -> Network tabından aşağıdaki şekilde aktif edebilirsiniz. Sizi sıraya aldıktan sonra bilgilendirme emaili alacaksınız. [9]

https://github.com/quicwg/base-drafts/wiki/Implementations

Hangi webserver'lar QUIC destekliyor?

- Nginx 1.6.1 + CloudFlare quiche patch -> Nginx geçtiğimiz günlerde Cloudflare'den HTTP / 3'ün desteklemesini sağlayan bir yama güncellemesi aldı.
- Litespeed Web Server
- Diğer web serverlar için docker üzerinde reverse proxy ayarlayabilirsiniz. [10]

Daha fazla bilgi için: https://github.com/quicwg/base-drafts/wiki/Implementations

Hangi CDN'ler desteklemektedir?

- QUIC.cloud
- Cloudflare

HTTP/2'i geçişi daha tam olarak yapılmamışken (Şu an bütün websitelerin %43.1'i desteklemektedir)[11], neredeyse her gün kullandığımız protokolün en yeni versiyonun getirilerinden bahsetmek istedim.

Sonuç olarak HTTP/3'ün yaygınlaşmasıyla TCP protokolüne bağımlılığımız daha da azalacak görünüyor. Bekleyip göreceğiz. Hep beraber güvenli günlere!

Referanslar:

Bahsi geçen tüm RFC dökümanlarına buradan sorgu yaparak ulaşabilirsiniz: **https://tools.ietf.org/html/**

https://blog.cloudflare.com/http3-the-past-present-and-future/

https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/Evolution_of_HTTP

https://tools.ietf.org/html/draft-ietf-quic-http-23

7 https://docs.docker.com/

8 https://github.com/caddyserver/caddy/wiki/QUIC

9 https://blog.cloudflare.com/http3-the-past-present-and-future/

10 https://hub.docker.com/r/devsisters/quic-reverse-proxy/

11 https://w3techs.com/technologies/details/ce-http2

Bilal Teke / m.bilalteke@gmail.com

Nedir bu Bug Bounty?

Bug Bounty, Türkçesi ile "Hata Avcılığı" anlamına geliyor. Şirketlerin yazılımlarının, web güvenlik açıklarının bulunması amacıyla açılan programların genel adıdır. Şirketler bu programı insanlara duyurarak yazılımlarına güvenlik testleri yapılmasına izin verir ve bu güvenlik açıklarını bildiren kişiye belli başlı ödüller verir.

Zafiyet bildiren hacker'ların kazançları değişkenlik göstermektedir. Bounty programlarına ve şirketlere bağlı olarak değişim göstermekle birlikte olası ödüller: Para, Sertifika, Hall Of Fame'dir. Bazen ise swag paketleri (t-shirt, çanta, usb, kalem, bardak vs.) hediye edilmektedir.

Herkes Bug Bounty Yapabilir mi?

Öncelikle bug hunter (hata avcısı) olmanız için, "ilerleyeceğiniz konseptin zafiyetleri nedir?", "nasıl ortaya çıkar?", "ben nasıl yararlanırım?" gibi sorulara cevap bulmanız gerekir. Kendimden örnek vererek anlatmam gerekirse, web üzerinden ilerlemeye karar verdim ve ilk olarak web pentesting alanında ilk zafiyetleri bulmayı öğrendim. Sonra bu işlemin ne işe yaradığını ve son olarak nasıl çalıştığını öğrenerek giriştim bu işe. Mesela siz network pentesting yapacaksanız network pentesting hakkında bilgi sahibi olmalısınız.

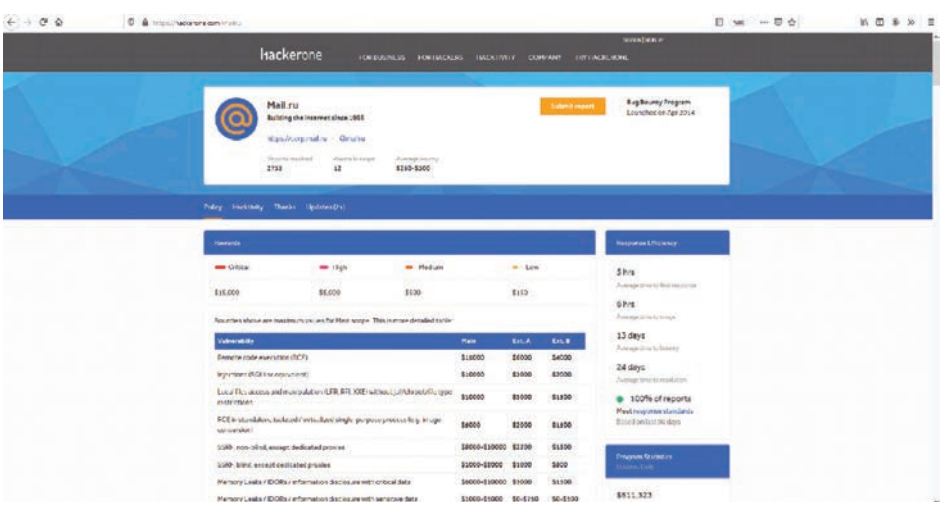
Kısacası yazılımcı ve ethical hacker olan herkes bu alanda iş yapabilir anlamına geliyor. Her şey sadece biraz merakla başlıyor.

Süreç Nasıl İşliyor ?

1.) Hedef Bulma

Öncelikle tabii ki de ilk yapacağımız iş kendimize bir hedef bulmak olacak. Peki gelelim asıl soruya: Hedefi nasıl bulacağız? Öncelikle önümüzde birkaç şık var ya şirketlerle anlaşmalı bir bug bounty platform kullanacağız ya da şirketlerin kendi bug bounty programı üzerinden hedef seçeceğiz.

Bu platformları daha ayrıntılı anlatacağım merak etmeyin ama önce süreci işleyelim. Hedefimimiz Mail.Ru olsun. (https://hackerone.com/mailru Mailru bug bounty program url'i.)

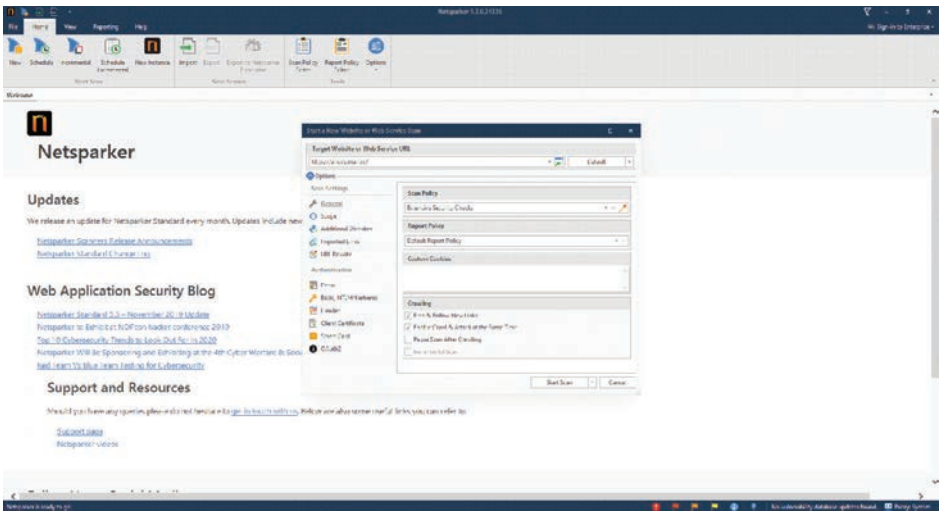


Sonra yapacağımız programı okuyarak kabul olan ve olmayan açık tiplerine bakmalıyız. Araştırmacının yapması ve yapmaması gerekenleri ve taranması istenilen domain'leri incelemeliyiz. Eğer domain kapsam dışı ise zafiyet bulsak bile bizi ödüllendiremeyebilirler.

2.) Hedefi Tarama

Şimdiki adımımız ise bug programındaki kapsamlara göre zafiyet aramaya başlamak ve bulduğumuz zafiyeti test edip raporlamak.

Öncelikle şunu söylemek isterim: Hem manuel hem de tools ile tarama yapan biriyim. Hedefimizi önce Netsparker'a atacağım. Sonra manuel olarak tarama yapacağım. Öncelikle Netsparker ayarlarımızı yapıyorum:

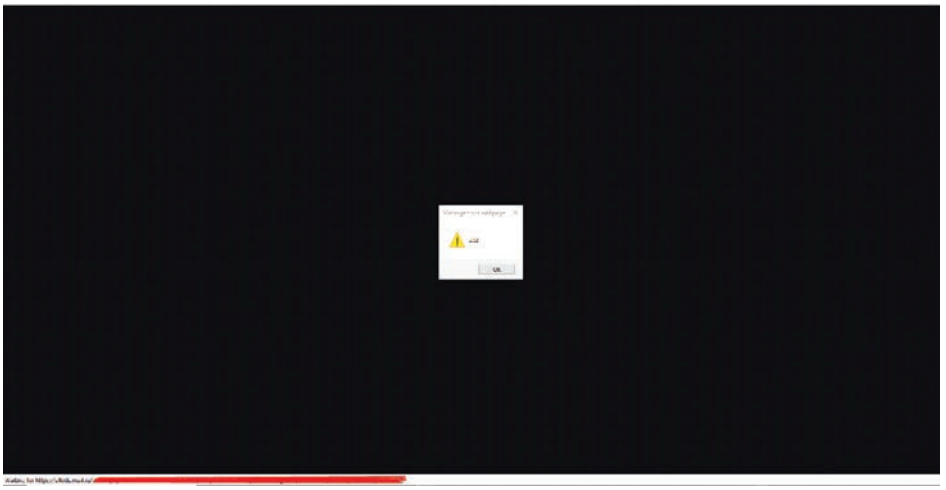


Bu arada şunu söylemek isterim ki bazı bug programları scanner'ları yasaklar. Bu kural yasaklar bölümünde yazılır. Eğer scanner'larla tarama yaparsanız büyük ihtimalle tarama yaptığınız site veya server sizi engeller. Genelde scanner'lar için koruma script'i vardır. Script yoksa bile emin olun zafiyetin log'larına bakılınca scanner kullanıp kullanmadığınız belli olur. Bu yüzden scanner kullanmayın deniliyorsa kullanmayın.

Şimdi Netsparker bir taraftan yavaş yavaş tararken ben de bir yandan portları tarayacağım ve manuel şekilde zafiyetleri araştıracağım. Bu arada şunu demeden geçmek istemiyorum: HTTPS ve HTTP olarak 2 farklı zafiyet olabiliyor. Yani demek istediğim https://x.com'da zafiyet yokken http://x.com'da zafiyet bazen olabiliyor. Bazı bug hunter'lar bunu atlasa da aslında önemli bir konudur aklınızda bulunsun.

Manuel olarak pek bir şey bulmasam da Netsparker, olası bir XSS zafiyeti bulmuş. Bunu şimdi deneyeceğim. Eğer çalışıyorsa rapor edeceğim.

Sürümü eski olan bir tarayıcıda çalıştığı için büyük ihtimalle bulduğum zafiyet ya önceden bildirilmiş olacak ya da büyük ihtimalle sadece HoF verecekler (Hall of Fame - onur/teşekkür listesinde isminizin yayımlanması).

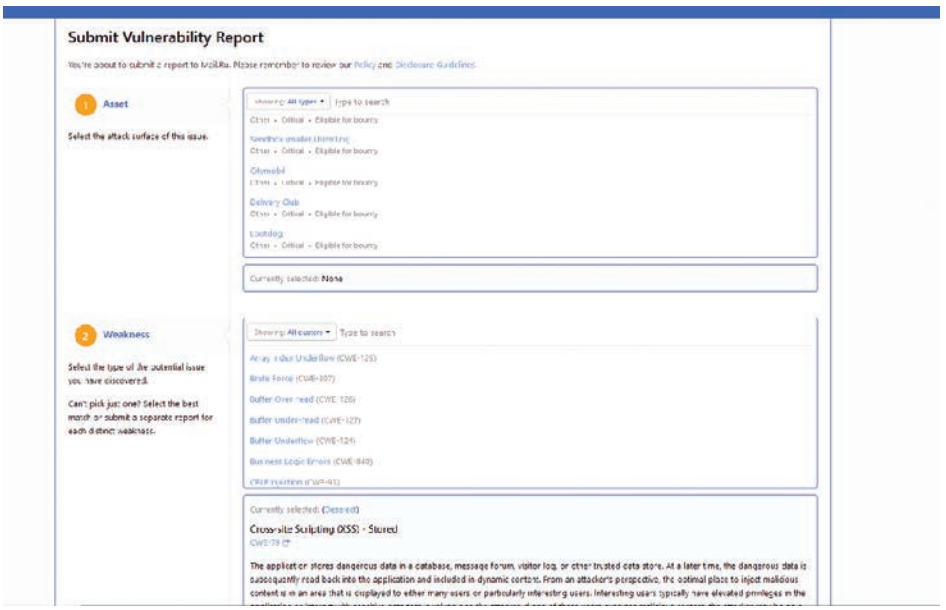


XSS zafiyeti hakkında bilmeyenler için biraz bilgi vereyim: Açılımı "Cross Site Scripting"'tir. Bilgisayar güvenlik açığı. HTML kodlarının arasına istemci tabanlı kod gömülmesi yoluyla kullanıcının tarayıcısında istenen istemci tabanlı kodun çalıştırılabilmesine olarak tanır. Cross-Site Scripting (XSS), OWASP Top 10 listesinde bulunmaktadır ve üç çeşidi vardır demek yeterli olacaktır zira ana konumuz bug bounty. Şimdi rapor yollama adımına geçelim:

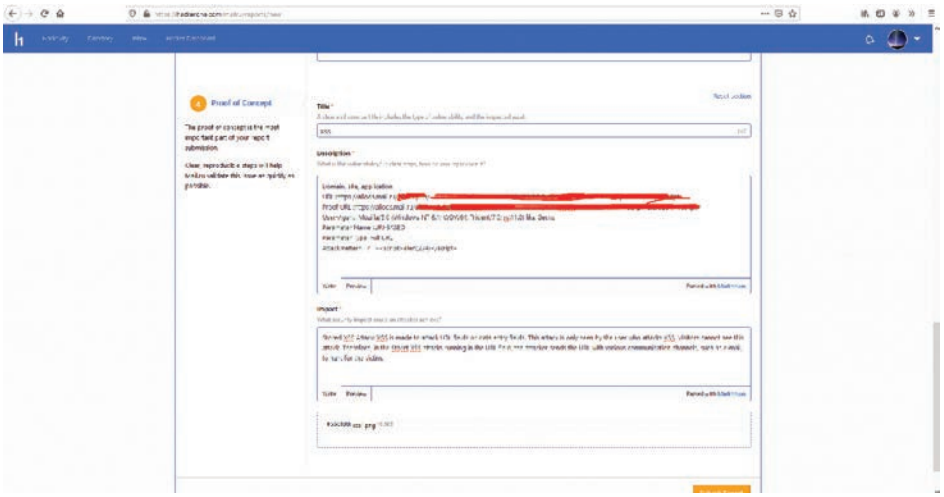
3.) Rapor Yollama:

Öncelikle şunu unutmayın raporlar her zamana İngilizce şekilde yollanır ve bol bol ayrıntı verilir. Böylelikle ayrıntılarla birlikte problem daha iyi anlatılabilir.

Şimdi benim ilk yapacağım işlem HackerOne üzerinden rapor yollamak olacak.



Bilgileri doldurup devam ediyoruz



Bilgileri gönderdiğimizde otomatik olarak HackerOne, Mail.Ru ekibine bunu yolluyor. Şimdi raporlarınızda görebileceğiniz durumlara bakalım:

Raporlarınızda Görebileceğiniz Durumlar:

1. Triaged:

Raporunuzun firma tarafından onaylandı demektir.

2. Needs More Information:

Bu güvenlik açığı hakkında daha fazla bilgi gerekmektedir. Hemen telaşlanmayın, bundan sonra durumun triaged olma şansı da vardır. Video vs çekerek açık hakkında daha fazla bilgi vermeyi deneyin.

3. Duplicate:

Firma, gönderdiğiniz güvenlik açığını zaten biliyor demektir. Muhtemelen sizden önce birileri açığı bulmuş ve şirkete yollamıştır.

4. Resolved:

Güvenlik açığı başarıyla düzeltilmiştir.

Bug Bounty Platformları:

HackerOne

Bug bounty programları arasında HackerOne, bilgisayar korsanlarına erişme, bug bounty programları oluşturma, sözcüğü yayma ve katkıları değerlendirme konusunda liderdir.

HackerOne'ı kullanmak için iki yol var: Birincisi, güvenlik zafiyeti raporları toplamak ve bunlar üzerinde kendi kendine çalışmak. İkincisi ise HackerOne uzmanlarına bu zor işi bırakmak. Yani triaging adını verdiğimiz işlem. Triaging, güvenlik açığı raporlarını derleme, doğrulama ve bilgisayar korsanlarıyla iletişim kurma işlemine verilen addır.

HackerOne, Google Play, PayPal, GitHub, Starbucks v.b gibi büyük markalar tarafından kullanılır yani ciddi bug'ları olan markalar için.

Bugcrowd

Bugcrowd, güvenlik değerlendirmeleri için çeşitli çözümler sunan bir platform. Bunlardan bir tanesi de bug bounty. Bugcrowd size, yaşam döngünüze kolayca uyum sağlayan ve başarılı bir bug bounty programı ve çalıştırmayı kolaylaştıran bir SaaS çözümü sunar.

Seçilmiş birkaç hacker içeren özel bir bug bounty programlarını veya binlerce kişinin ulaşabileceği public kaynak programlarını seçebilirsiniz.

SafeHats

Eğer bir girişimci iseniz ve bug bounty programınızı public yapma konusunda tereddütleriniz varsa güvenliğe tipik bir bug bounty programının sağladığından çok daha fazla dikkat etmeniz gerekiyor. SafeHats bu amaç için güvenli platform.

SafeHats özel güvenlik danışmanı, derinlemesine hacker profilleri, gereksinimlerinize ve güvenlik modelinizin vadesine bağlı olarak sağlanır.

Intigriti

Intigriti, özel veya public bir program yürütmek istediğinizde sizi beyaz şapkalı hacker'lara bağlayan kapsamlı bir bug bounty programıdır.

Hacker'lar için kazanılacak çok fazla ödül var. Şirketin büyüklüğüne ve endüstrisine bağlı olarak 1.000 ile 20.000 € arasında değişen bug ödülleri mevcut.

Synack

Synack, piyasadaki kalıpları kıran istisnalarından biri. Onların güvenlik programı Hack the Pentagon, önemli kritik noktaların keşfedilmesini sağladı.

Yani, sadece bug bounty değil, aynı zamanda da üst düzey güvenlik rehberliği ve eğitimi arıyorsanız, Synack tam size göre!

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

abaküs

Hacking Seti

Yazılım Güvenliği ve Siber Güvenliğe Giriş

Muhammed Eren Uygun / erenn.uygun@gmail.com

Google Hacking for Penetration Testing

Hepimiz mutlaka Google üzerinden bir arama yapmışızdır. Fakat bunlar genellikle aramak istediğimiz bilginin direkt olarak anahtar kelimelerini kullanarak yaptığımız aramalardı. Örneğin bir kitabın PDF uzantılı halini istiyorsak, basitçe kitabın ismini yazarak PDF halini tek tek arıyorduk. Fakat bu gibi spesifik aramalarımızda Google bizim için operatörleri(dork) aktif etmiş. Bu operatörleri kullanarak istediğimiz bilgiye kısa sürede erişebiliyoruz.

Bu durum "Hacking" konusunda ise bizlere çok yardımcı olmaktadır. Çünkü biliyorsunuz ki bir sisteme penetrasyon testleri yapılırken hacker arkadaşlarımız bazı aşamalardan geçmektedir. Bu aşamaların başında ise aktif ve pasif bilgi toplama gelmektedir. Tabii ki oturup arama motorları üzerinden tek tek inceleyerek belki günlerce belki haftalarca zamanınızı ayırarak pasif bilgi toplama işlemlerinizi yapabilirsiniz fakat Google kullanıcıları için arama operatörlerini yapmış. Böylelikle bu durumu lehimize çevirerek aramak istediğimiz bilgiye direkt olarak ulaşabiliriz.

Bir örnek senaryo üzerinden Google Hacking'in önemine değinelim daha sonrasında ise bu operatörleri örnekler ile inceleyelim.

Bir hacker, pentest yapacağı websitesi için pasif bilgi toplamaya başlar. Google operatörlerini kullanarak o site altında bulunan ve içeriğinde "config" adı geçen yerleri getirmesini isteyebilir. Böylelikle eğer ki "config" adı geçen yerler üzerinde kritik bilgiler içeren dosya bulabildiyse, saldırgan belkide haftalarca sürecek olan çalışmasını sadece 5 dakikaya indirmiş olacaktır.

İşte biz de bu yazımızda Google'ın bize vermiş olduğu operatörleri nasıl kullanacağımıza ve bunlar ile neler yapabileceğimize değindik. Keyifli okumalar dileriz.

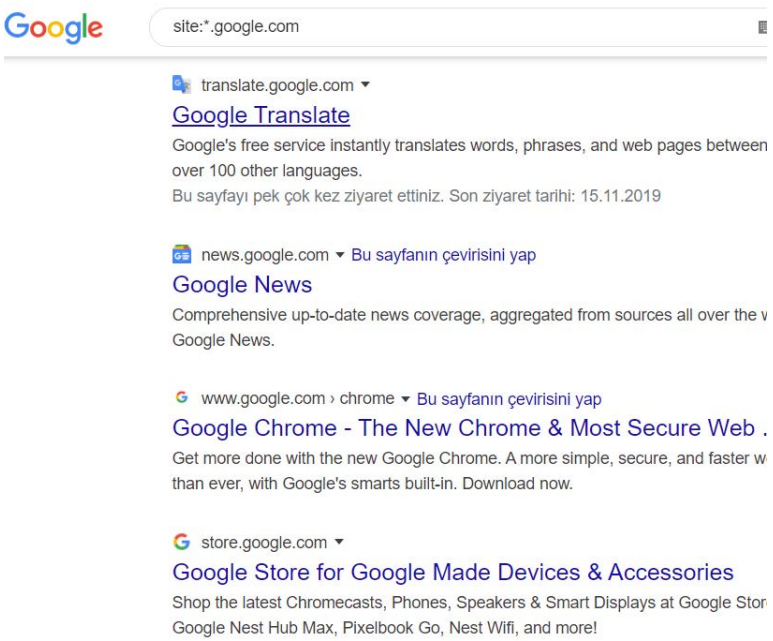
Google operatörlerini sırasıyla incelemeye başlayalım.

site: Spesifik olarak belirlediğiniz web sitesi içerisinde aramak istenildiğinde kullanılan sorgu operatörüdür.

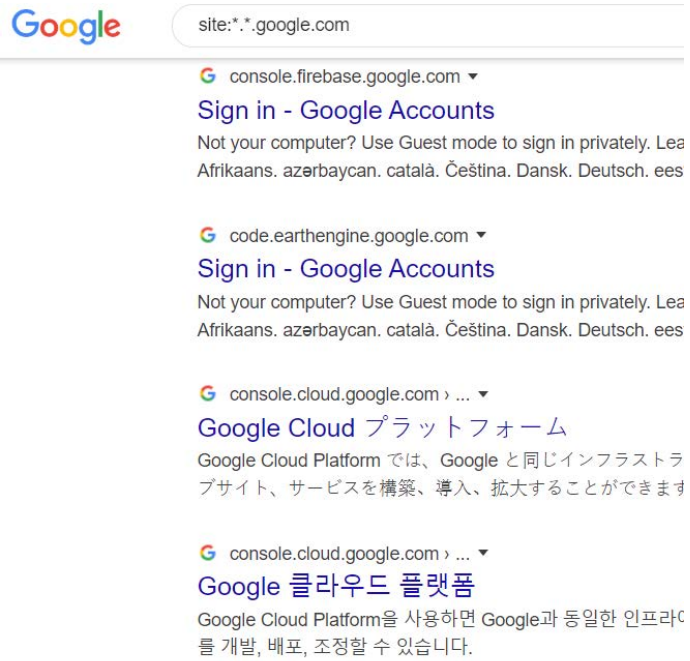
- site:arkakapidergi. com

Bu operatörü regex kullanımı ile birleştirdiğimizde ise hayatımıza çok güzel kolaylıklar gelecektir. Örneğin bir web sitesinin subdomain bilgilerini öğrenmek istiyorsunuz. Bunun için elbette araçlar var fakat Google operatörleriyle de web sitelerin subdomain bilgilerini elde edebiliyorsunuz.

- site: *. example. com -> subdomain bulgusu.

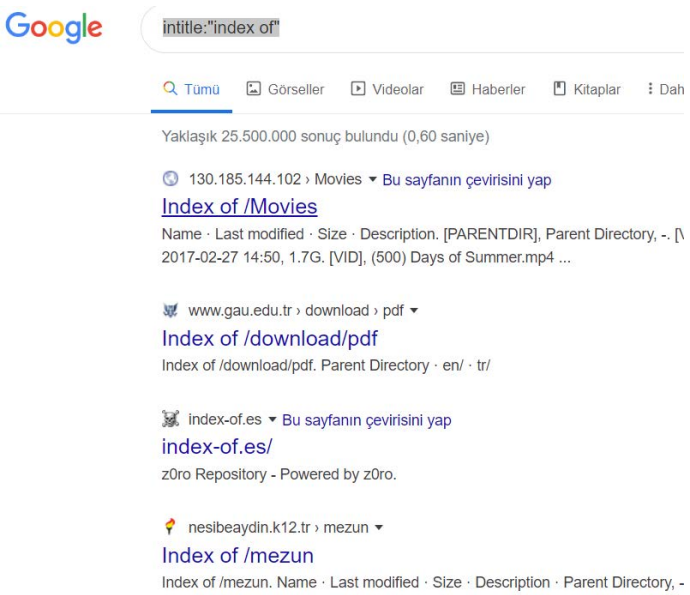


- site: *. *. example. com -> subdomain'in subdomaini.



intitle: Sayfa başlığında bulunan yazılar üzerinde bir arama yapmak için kullanılır. Bu operatörü örneğin "index of" başlığı bulunan sayfaları getirmek için kullanabiliriz. Çünkü "index of" başlığı web sunucularında bulunan bir dizinin kaybolması sonucunda dizin içeriklerinin listelenmesini sağlayan bir özelliktir. Böylelikle sunucuda bulunan kritik dosyaları keşfedebiliriz.

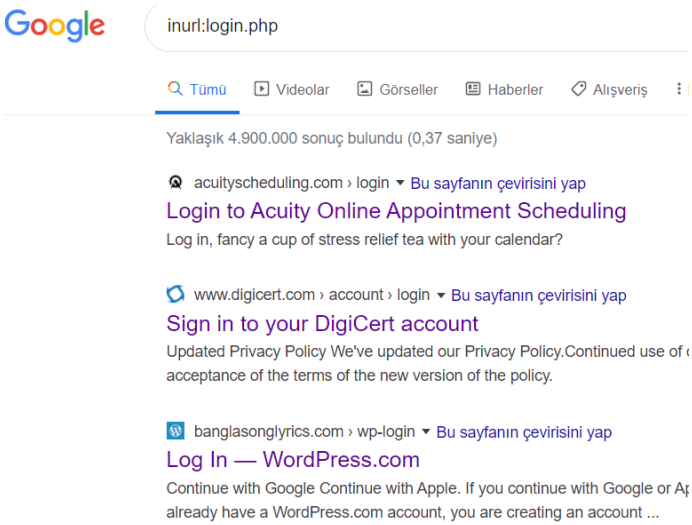
- intitle:"index of"



Yukarıda ekran görüntüsünde gördüğünüz üzere ilk çıkan sayfada olduğu gibi normal sitelerde bulamadığınız yeni çıkan filmleri, dizileri de böylelikle bulabilirsiniz.

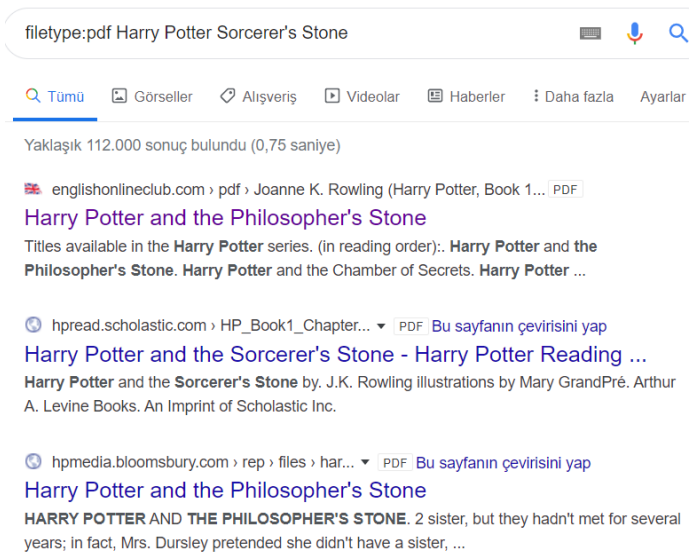
inurl: Sayfa URL'inde aramak istediğimiz dizinleri bulmak için kullandığımız bir operatördür. Bu operatörü örneğin sayfaların admin panellerini bulmak için kullanabilirsiniz.

- inurl:admin.php



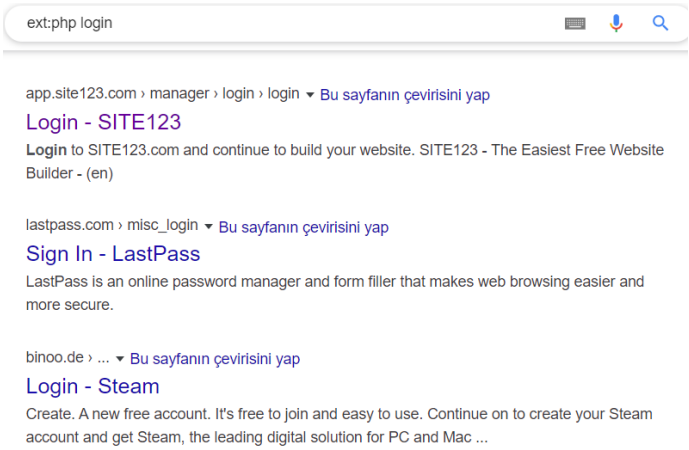
filetype: Bu operatörü kullanırken yanına bir dosya uzantısı belirtiyoruz. Böylelikle yazımızın başında vermiş olduğumuz örnekteki gibi aramak istediğimiz bir kitabı bulmak için PDF uzantısını belirterek daha kısa sürede sonuca varmış oluyoruz.

- filetype:pdf Harry Potter Sorcerer's Stone



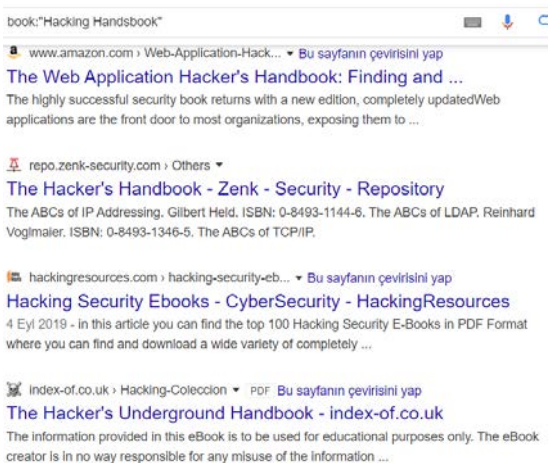
ext: Filetype operatörü ile aynı sonucu vermektedir.

- ext:php login



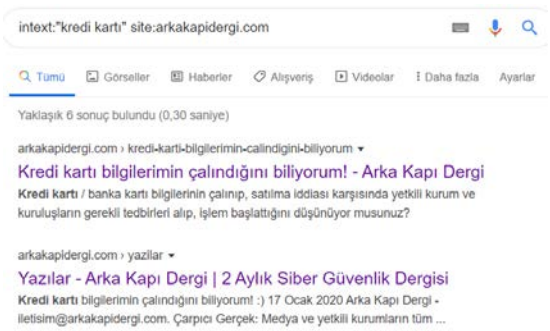
book: Aradığınız kitap hakkında bilgi edinmek için kullanılan bir operatördür.

- book:"Hacking Handsbook"



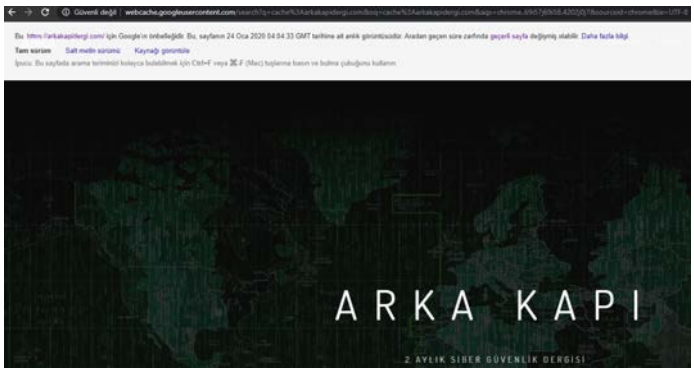
intext: Yazdığımız ifadeyi belirttiğimiz web sitesi içerisinde bulup getiren operatördür. Bu operatör bir web sitesi içerisinde aramak istediğimiz kelimeyi saatlerce aramaktansa, spesifik olarak karşımıza getirdiği için bizlere çok kolaylık sağlar.

- intext:"kredi kartı" site:arkakapidergi. com



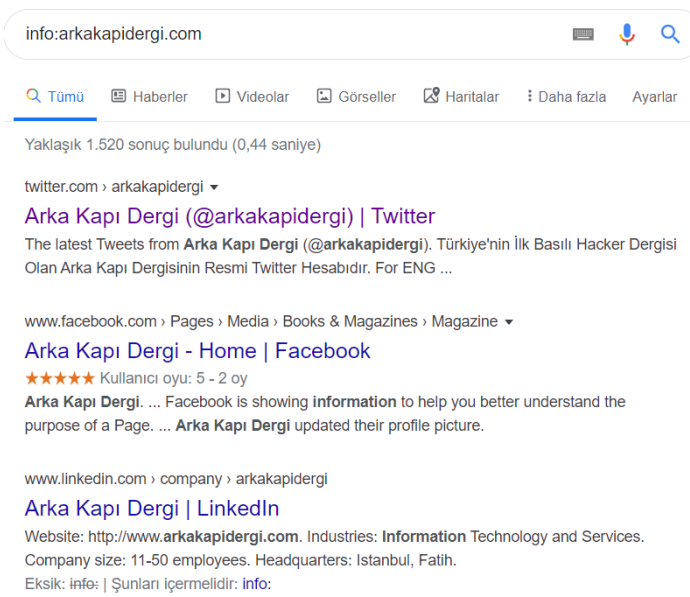
cache: Cache, adından anlaşılacağı üzere yanına yazmış olduğunuz sayfaların Google önbelleğindeki son halini görüntülemeye yarayan bir operatördür. Bu operatörü kullanma amacımız ise bazen ihtiyacımız olan bir web sitesi kapanabiliyor veya çökebiliyor. Fakat cache operatörü ile Google önbelleği sayesinde web sitesinin eski halini görebiliyoruz.

- cache:arkakapidergi. com



info: Yazacağımız web sitesi ile alakalı diğer web sitelerini listeleyen operatördür.

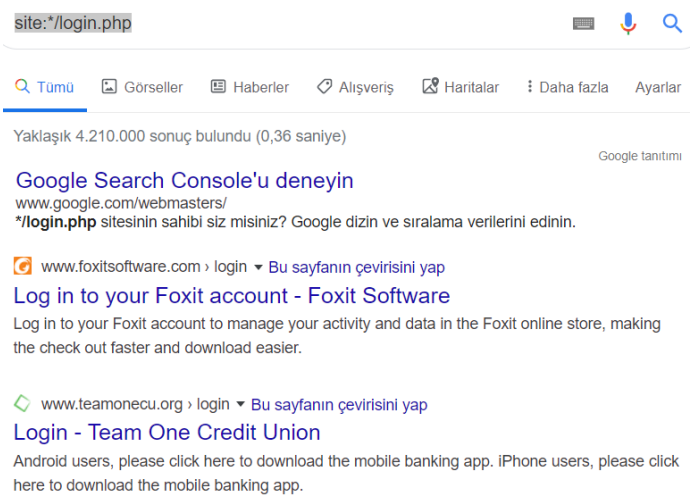
- info:arkakapidergi. com



İşimize yarayacak olan çoğu operatörü inceledik. Şimdi ise bu operatörlerin yanı sıra kullanmamız gereken bazı **Regex (Regular Expressions)** ifadelerinin kullanımını inceleyelim.

Yıldız(*): İlk örnekte yıldız (*) regex ifadesinden kısaca bahsetmiştik. Fakat başka kullanımlarını görmemiştik bu yüzden tekrardan inceleyelim. Yıldız (*) ifadesi, regex bilmiyorsanız eğer her şey anlamına gelir. Yani bir değerin önüne veya arkasına bu ifadeyi koyduğunuz zaman, o tarafa her şeyin gelebileceği manasına gelmektedir. Örnekle inceleyelim;

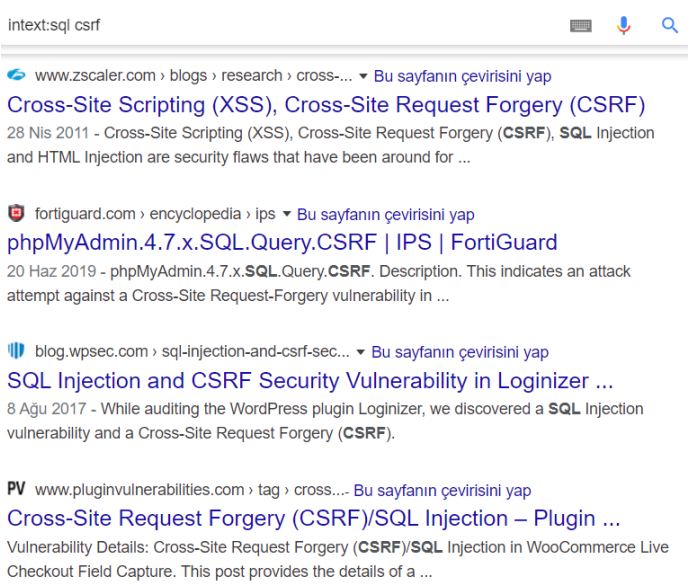
- site:*/login.php



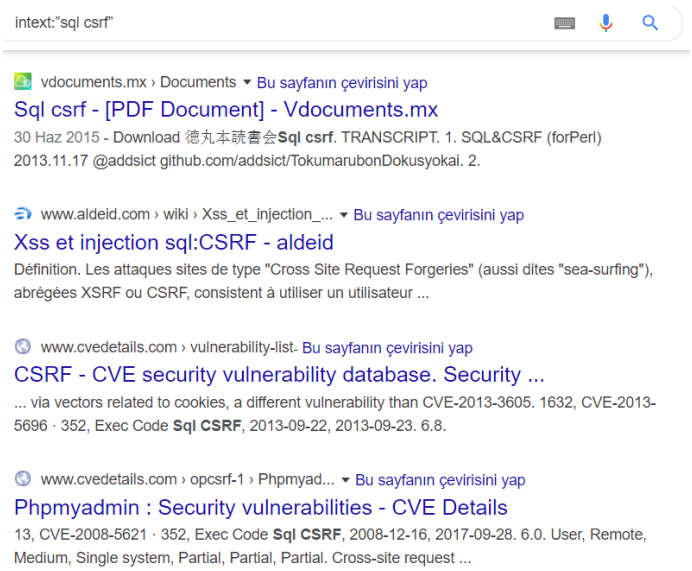
Ekran görüntüsünde gördüğünüz gibi "/login.php" başına ne gelirse gelsin biz login.php bulunan dizinleri getirmek istediğimiz için "*/login.php" yazarak **Yıldız (*)** ifadesini kullanmış olduk. Bu ifade ilk örnekte belirttiğimiz gibi genellikle subdomain tespiti için kullanılır.

Çift Tırnak (" "): Boşluklu ifadeler ile arama yapıldığında Google boşluk öncesi ve sonrasını farklı şekilde değerlendirir. Örneğin root toor şeklinde çift tırnak olmaksızın arama yaptığınızda root içeriklerini ve toor içeriklerini getirir. Ancak "root toor" şeklinde tırnak işaretlerini kullanarak arama yapıldığında root toor ifadesini spesifik olarak beraber bir şekilde kelime sırasına dikkat ederek arar ve o şekilde getirir.

- intext:sql csrf

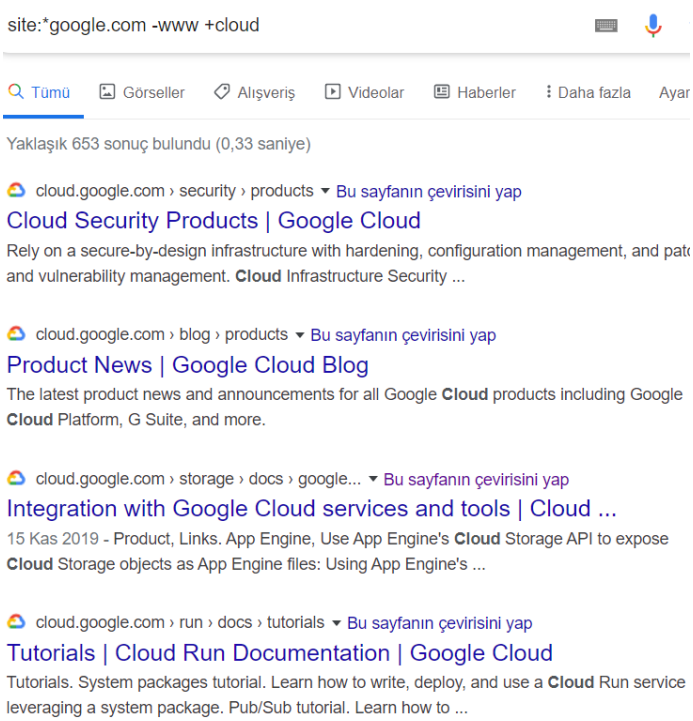


- intext:"sql csrf"



Boolean Arama: AND, OR ve NOT ifadeleri ile birden fazla sorguyu mantıksal olarak gruplayabilirsiniz. Bu ifadelerin sorgu içerisinde büyük yazılması önemlidir. Bunlar içerisinde AND operatörü aramalarda varsayılan arama yöntemidir. AND yerine + simgesi de kullanılabilir. AND işleminin tam tersi işlem – işareti yani NOT 'dır. Aramada bu olmasın demektir. OR(\) ise bilindiği üzere veya anlamında kullanılır.

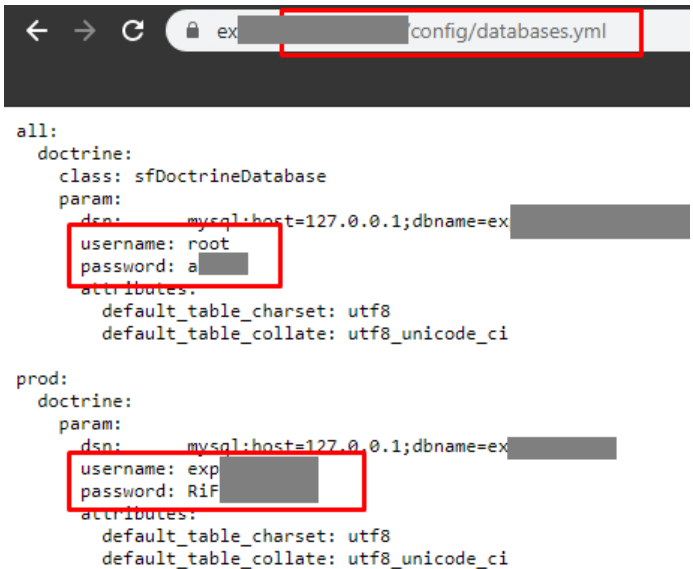
- site:*google. com -www +cloud



Google Operatörlerinden bazılarını inceledik. Şimdi ise yazımızın başında belirtmiş olduğumuz senaryoyu bir hacker gözünden inceleyelim.

Hacker Google operatörlerinden ikisini kullanarak senaryoda da belirttiğimiz gibi sadece test yaptığı sitenin title bilgisinde "Index Of/config" geçenleri getirmesini istemiştir. Böylelikle belki test yapacağı sitenin kritik bilgilerine erişim sağlayabileceğini düşünmektedir.

Belirtilen Google operatörlerini yazan hacker'ın karşısına görüldüğü gibi bir sonuç gelmiştir. Sonucun içeriğine girdiği zaman bir veritabanı config dosyası bulunmaktadır. Dosya içeriğinde ise veritabanına ait kritik bilgiler bulunmaktadır.



Böylelikle hacker çok hızlı bir şekilde test yapmış olduğu web-sitenin kritik bilgilerini elde etmiştir.

- Google Hacking Database (GHDB)

Google Hacking Database

Show 15

Date Added	Dork
2020-01-23	site:*/AdminPanel.php
2020-01-23	inurl:memberlogin.php
2020-01-23	intitle:"Sign in" site:*/idaas/
2020-01-23	"key" OR key.jar intitle:"index of" webstart
2020-01-23	intitle:"index of" "server at"
2020-01-23	"fetchmailrc" intitle:"index of" -linux
2020-01-21	intitle:rsview32 ext:asp

GHDB, kullanıcıların Google'daki operatörleri kullanarak yaratıcı dorklarının bulunmuş olduğu bir nevi veri tabanıdır. En çok bilineni ise **exploit-db**'dir. Bu adrese ise buradan (http://bit. ly/392QDYs) erişebilirsiniz. Siz de Google üzerinde denemeler yaparak bulmuş olduğunuz yaratıcı dorkları **exploit-db** sitesine gönderebilirsiniz.

Ayrıca Google Operatörlerini aşağıda belirtmiş olduğum kendi sayfası üzerinden inceleyebilirsiniz.

https://www. google. com. tr/intl/tr/help/operators. html

Yazımızı okuduğunuz için teşekkür ederiz. Diğer yazılarımızda görüşmek üzere. Güvenli günler dileriz!

Ayşenur Burak / nurayse47@gmail.com

Docker-Konteyner Güvenliği - Part II

Docker Güvenliği serisinin ilk bölümünde "Docker nedir?", "Neden Docker'ın güvenli olmasını sağlamalıyız?", "Docker kurulumu ve örnek proje oluşturulması" gibi konulara giriş yapmıştık. İzninizle bu bölümde "Docker'ı nasıl daha güvenli yapabiliriz?" sorusuna yanıt vermeye çalışalım.

Hatırlarsanız size Cilium adlı konteyner güvenliğini sağlayan bir araçtan bahsetmiştik. Yazının devamında Kubernetes'e kısaca bir giriş yapıp Cilium'un kurulumuna geçelim.

1. Docker Güvenliğini Sağlamak için İpuçları:

- Her konteyner için kullanacağı bellek ve CPU miktarı sınırlandırılmalıdır. Güvenli olmayan kapsayıcıların kötü amaçlı işlem gerçekleştirmek için büyük miktarda kaynak tüketmesini önleyerek güvenliği artırır.
- Konteynerleri root olarak çalıştırmayın. Root olarak çalıştırmak, saldırganın, hassas bilgilere ve çekirdeğe çok daha kolay bir erişebilmesine neden olur. Build ederken --user ya da -u parametresi ile root dışında bir kullanıcı kimliği belirleyebilirsiniz:

  docker run -u 1000 my_image

1000 parametresi, ayrıcalıklı olmayan bir kullanıcı id'sini belirtir. Linux'ta 0 ile 499 arasındaki kullanıcı id'leri genelde ayrılmıştır. Varsayılan sistem kullanıcısı olarak çalışmaktan kaçınmak için id'si 500'den fazla olan kullanıcı kimliklerini seçin. Bunun yerine Dockerfile içerisinde paket yükleme komutlarından sonra USER 1000 komutunu ekleyerek de ayıcalıklı olmayan bir kullanıcıyı ayarlayabilirsiniz. Bu konuda daha fazla bilgi için şu adresi ziyaret ediniz: http://bit.ly/2TurL7d.

- Konteyner kayıt defterinin kullanımında ihlal riskini azaltmak için Docker Hub yerine kendi güvenlik duvarınızın arkasına kurulabilen Docker Trusted Registry'yi kullanın.
- Güvenilir ve resmi Docker imajları kullanın. Güvenilir depolar dışındaki genel konteyner kayıtlarını kara listeye alabilirsiniz. Docker imajlarındaki bilinen bazı güvenlik açıklarını tanımlamaya yardımcı olması için imaj tarama aracı kullanabilirsiniz.
- Kodunuzun kaynağını belirleyin. Docker imajlarınızdaki tüm paketleri indirerek ve kaynağını belirlemek için tarayarak imajlara eklenen kodların bilinen güvenlik açıklarını içerip içermediğini belirleyebilirsiniz.
- API ve ağlarınızın güvenliğini sağlayın.
- Ana sunucu yazılımınızı, Docker sürümünüzü, imajlarınızı, imajlarınızdaki dilleri ve kütüphaneleri güncel tutun.
- Bir kuruluşunuz varsa Docker Community yerine Docker Enterprise kullanabilirsiniz. (Docker Trusted Registry, sadece Docker Enterprise için geçerlidir.)
- Ağ bağlantılı tek ana bilgisayarlı bir uygulama kullanıyorsanız, varsayılan köprü ağını kullanmayın. Teknik eksiklikleri vardır ve üretim kullanımı için önerilmez. Bir bağlantı noktası yayınlarsanız, köprü ağındaki tüm kapsayıcılar erişilebilir hale gelir.
- Dockerfile dosyasında, ADD yerine COPY'yi kullanın. ADD, sıkıştırılmış dosyaları otomatik olarak ayıklar ve URL'lerden dosya kopyalayabilir.
- Hassas verileri sadece volume'lerde saklayın. Asla konteynerlerde saklamayın.
- Bir REST API'ı ile çalışıyorsanız, API uç noktalarını HTTPS veya SSH ile güvenli hale getirin.
- Aynı sunucuda başka işlemler yapıyorsanız, bunları Docker kapsayıcılarında çalıştırın.

2. Kubernetes Nedir?

Kubernetes, containerize edilmiş uygulamaların dağıtımını, ölçeklendirmesini ve yönetimini otomatikleştirmek için kullanılan açık kaynak kodlu bir konteyner yönetme aracıdır. Kubernetes, servisleri izler, yük dengelemesi (load balancing) yapar ve depolama alanınızı yönetir.

Pod (kapsül), bir veya daha fazla konteynerin çalıştığı alandır. Paylaşılan depolama ve ağ alanları, konteynerlerin nasıl çalıştırılacağı ile ilgili tanımlamalar yer alır.

Minikube, Kubernetes üzerinde testler ve geliştirmeler yapmak için yerel bilgisayarlarda kullanılan mini kubernetes kümesidir. Minikube; master, node ve docker bileşenlerinden oluşmaktadır. Kubectl, Kubernetes'in komut satırı aracıdır. Cluster (küme) oluşturmak, bunları yönetmek, deployment (dağıtım) yapmak, uygulamaları incelemek, log kayıtlarına erişmek vb. işlemleri bu komut sayesinde yaparız.

3. Minikube ve Kubectl Kullanarak Cilium Kurulumu

Başlamadan önce; terminal ekranınızda root olduğunuzdan ve sanal makinenizin Ayarlar -> Sistem -> İşlemci ayarlarında en az iki CPU ayarladığınıza emin olun.

1. Minikube'ü indirin ve user/local/bin klasörüne kurun:

curl -LO https://storage.googleapis.com/minikube/releases/latest/minikube-linux-amd64

install minikube-linux-amd64 /usr/local/bin/minikube

```
root@ubuntu:/home/ayse_cybersec# curl -LO https://storage.googleapis.com/kubernet
es-release/release/`curl -s https://storage.googleapis.com/kubernetes-release/rel
ease/stable.txt`/bin/linux/amd64/kubectl
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 41.4M  100 41.4M    0     0   601k      0  0:01:10  0:01:10 --:--:--  779k
```

2. Eğer benim gibi bir sanal makine içerisinde çalışıyorsanız hipervizörünüz iç içe sanallaştırmaya izin vermez. Bu durumda None sürücüsünü kullanarak ek bir sanal makine katmanı oluşturulması işlemini atlayabilirsiniz:

minikube start --vm-driver=none

```
root@ubuntu:/home/ayse_cybersec# sudo minikube start --vm-driver=none
😄  minikube v1.6.2 on Ubuntu 18.04 (vbox/amd64)
✨  Selecting 'none' driver from user configuration (alternates: [])
🤹  Running on localhost (CPUs=2, Memory=2532MB, Disk=48436MB) ...
ℹ️  OS release is Ubuntu 18.04.3 LTS
🐳  Preparing Kubernetes v1.17.0 on Docker '19.03.5' ...
    ▪ kubelet.resolv-conf=/run/systemd/resolve/resolv.conf
💾  Downloading kubeadm v1.17.0
💾  Downloading kubelet v1.17.0
🚜  Pulling images ...
🚀  Launching Kubernetes ...
🤹  Configuring local host environment ...

⚠️  The 'none' driver provides limited isolation and may reduce system security an
d reliability.
⚠️  For more information, see:
👉  https://minikube.sigs.k8s.io/docs/reference/drivers/none/

⚠️  kubectl and minikube configuration will be stored in /root
⚠️  To use kubectl or minikube commands as your own user, you may need to relocate
 them. For example, to overwrite your own settings, run:

    ▪ sudo mv /root/.kube /root/.minikube $HOME
    ▪ sudo chown -R $USER $HOME/.kube $HOME/.minikube

💡  This can also be done automatically by setting the env var CHANGE_MINIKUBE_NO
NE_USER=true
⌛  Waiting for cluster to come online ...
🏄  Done! kubectl is now configured to use "minikube"
💡  For best results, install kubectl: https://kubernetes.io/docs/tasks/tools/ins
tall-kubectl/
```

3. Kümenin durumunu kontrol etmek için aşağıdaki komutu kullanın:

minikube status

```
root@ubuntu:/home/ayse_cybersec# minikube status
host: Running
kubelet: Running
apiserver: Running
kubeconfig: Configured
```

4. Minikube sürümünü kontrol edin (Cilium kurmak için v1.3.1'den büyük olmalıdır).

minikube version

```
root@ubuntu:/home/ayse_cybersec# minikube version
minikube version: v1.6.2
commit: 54f28ac5d3a815d1196cd5d57d707439ee4bb392
```

5. Kubectl'i indirin:

curl -LO https://storage.googleapis.com/kubernetes-release/release/`curl -s https://storage.googleapis.com/kubernetes-release/release/stable.txt`/bin/linux/amd64/kubectl

```
root@ubuntu:/home/ayse_cybersec# curl -LO https://storage.googleapis.com/kubernet
es-release/release/`curl -s https://storage.googleapis.com/kubernetes-release/rel
ease/stable.txt`/bin/linux/amd64/kubectl
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 41.4M  100 41.4M    0     0   601k      0  0:01:10  0:01:10 --:--:--  779k
```

6. Kubectl dosyasını yürütülebilir yapın:

chmod +x ./kubectl

7. Dosyayı usr/local/bin/ klasörüne taşıyın:

mv ./kubectl /usr/local/bin/kubectl

8. Sürüm bilgisini kontrol edin (Cilium kurmak için v1.10'dan büyük olmalıdır):

kubectl version

```
root@ubuntu:/home/ayse_cybersec# chmod +x ./kubectl
root@ubuntu:/home/ayse_cybersec# sudo mv ./kubectl /usr/local/bin/kubectl
root@ubuntu:/home/ayse_cybersec# kubectl version
Client Version: version.Info{Major:"1", Minor:"17", GitVersion:"v1.17.0", GitComm
it:"70132b0f130acc0bed193d9ba59dd186f0e634cf", GitTreeState:"clean", BuildDate:"2
019-12-07T21:20:10Z", GoVersion:"go1.13.4", Compiler:"gc", Platform:"linux/amd64"
}
Server Version: version.Info{Major:"1", Minor:"17", GitVersion:"v1.17.0", GitComm
it:"70132b0f130acc0bed193d9ba59dd186f0e634cf", GitTreeState:"clean", BuildDate:"2
019-12-07T21:12:17Z", GoVersion:"go1.13.4", Compiler:"gc", Platform:"linux/amd64"
}
```

9. Kubectl'in doğru yapılandırıldığını kontrol etmek için aşağıdaki komutu yazın. Eğer cevap olarak bir bağlantı dönerse kümeniz doğru bir şekilde yapılandırılmıştır:

kubectl cluster-info

```
root@ubuntu:/home/ayse_cybersec# kubectl cluster-info
Kubernetes master is running at https://192.168.1.13:8443
KubeDNS is running at https://192.168.1.13:8443/api/v1/namespaces/kube-system/ser
vices/kube-dns:dns/proxy

To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.
```

10. Yeni Kubernetes kümenize Cilium'u yükleyin:

kubectl create -f https://raw.githubusercontent.com/cilium/cilium/v1.6/install/kubernetes/quick-install.yaml

```
root@ubuntu:/home/ayse_cybersec# kubectl create -f https://raw.githubusercontent.
com/cilium/cilium/v1.6/install/kubernetes/quick-install.yaml
configmap/cilium-config created
serviceaccount/cilium created
serviceaccount/cilium-operator created
clusterrole.rbac.authorization.k8s.io/cilium created
clusterrole.rbac.authorization.k8s.io/cilium-operator created
clusterrolebinding.rbac.authorization.k8s.io/cilium created
clusterrolebinding.rbac.authorization.k8s.io/cilium-operator created
daemonset.apps/cilium created
deployment.apps/cilium-operator created
```

11. Gerekli bileşenlerin kurulumunu aşağıdaki komut ile izleyebilirsiniz: (kurulumların tamamlanması uzun sürebilir.)

kubectl -n kube-system get pods --watch

```
root@ubuntu:/home/ayse_cybersec# kubectl -n kube-system get pods --watch
NAME                               READY   STATUS              RESTARTS   AGE
cilium-279gq                       1/1     Running             1          51m
cilium-operator-55658fb5c4-tzjj5   1/1     Running             1          51m
etcd-minikube                      1/1     Running             1          95m
kube-addon-manager-minikube        1/1     Running             0          95m
kube-apiserver-minikube            1/1     Running             4          95m
kube-controller-manager-minikube   1/1     Running             11         95m
kube-proxy-qqwhm                   1/1     Running             0          95m
kube-scheduler-minikube            1/1     Running             8          95m
storage-provisioner                1/1     Running             0          88m
coredns-6955765f44-8bfqg           0/1     Pending             0          0s
coredns-6955765f44-8bfqg           0/1     Pending             0          0s
coredns-6955765f44-f8mxv           0/1     Pending             0          0s
coredns-6955765f44-f8mxv           0/1     Pending             0          0s
coredns-6955765f44-8bfqg           0/1     ContainerCreating   0          1s
coredns-6955765f44-f8mxv           0/1     ContainerCreating   0          2s
coredns-6955765f44-8bfqg           0/1     Running             0          9s
coredns-6955765f44-f8mxv           0/1     Running             0          9s
coredns-6955765f44-f8mxv           1/1     Running             0          11s
coredns-6955765f44-8bfqg           1/1     Running             0          12s
coredns-6955765f44-8bfqg           1/1     Terminating         0          37s
```

12. Kapsüller arasındaki bağlantıyı test etmek için bağlantı kontrolü uygulayın:

kubectl apply -f https://raw.githubusercontent.com/cilium/cilium/v1.6/examples/kubernetes/connectivity-check/connectivity-check.yaml

```
root@ubuntu:/home/ayse_cybersec# kubectl apply -f https://raw.githubusercontent.
com/cilium/cilium/v1.6/examples/kubernetes/connectivity-check/connectivity-check
.yaml
deployment.apps/probe created
service/echo created
deployment.apps/echo created
```

13. Mevcut pod'ları görüntülemek için aşağıdaki komutu kullanın: (Siz ilk çalıştırdığınızda çıktı henüz bu şekilde olmayabilir. Biraz bekledikten sonra tekrar deneyin.)

kubectl get pods

```
root@ubuntu:/home/ayse_cybersec# kubectl get pods
NAME                    READY   STATUS    RESTARTS   AGE
echo-5659cf6c69-47wzf   1/1     Running   0          10m
echo-5659cf6c69-82dr8   1/1     Running   0          10m
echo-5659cf6c69-lfxdk   1/1     Running   0          10m
echo-5659cf6c69-nbwdl   1/1     Running   0          10m
```

Evet, Cilium'u kurduk. *minikube stop* komutu ile şimdilik kümenizi durdurabilirsiniz. Bir sonraki bölümde Cilium'un nasıl kullanılacağı, Cilium ile HTTP/REST API çağrısı yetkilendirme, DNS tabanlı ilkelerde harici erişimi kilitleme, Kafka kümesinin güvenliğini sağlama gibi işlemleri gerçekleştirmeye çalışacağız.

Kaynaklar:

Önceki yazıda kaynakları yazmayı unutmuşuz. Bunun için özür dilerim.

https://cilium.readthedocs.io

https://medium.com/@WhiteSourceSoft/docker-container-security-challenges-and-best-practices-70707b84eb36

https://towardsdatascience.com/top-20-docker-security-tips-81c41dd06f57

https://minikube.sigs.k8s.io/docs/start/linux/

https://kubernetes.io/docs/tutorials

İbrahim Baloğlu / ibrahimbaloglu@yahoo.com

YaaniMail UYGULAMASININ ADLİ BİLİŞİM İNCELEMESİ

Merhaba değerli Arka Kapı okuyucuları, önceki sayılarda olduğu gibi bu sayıda da Adli Bilişim alanıyla ilgili bir yazı ele aldım. Bu yazımda, geçtiğimiz aylarda Turkcell tarafından duyurulan *Yaani Mail* isimli mail uygulamasının manuel yöntemler kullanarak Adli Bilişim açısından incelenmesinin nasıl yapılabileceğinden bahsediyor olacağım.

Yaani Mail Turkcell tarafından oluşturulmuş, e-posta okumak ve cevaplamak, internet olmadan da önceden gelmiş olan maillerin görüntülenebildiği ve cevaplanabildiği, daha sonrasında da internet bağlantısının kurulması ile tüm işlemlerin otomatik olarak gerçekleştirildiği bir mail hizmetidir.

Yaani Mail servisine Ad-Soyad, kulllanıcı adı, parola ve güvenlik sorusu belirleme, cep telefonu tanımlaması yapılarak kayıt olunmaktadır. Ayrıca hızlı giriş seçeneği de bulunmaktadır. Hızlı giriş, kullanıcılarının kişisel bilgilerini paylaşmadan, yalnızca cep telefon numarası aracılığıyla sağlanabilen müşteri doğrulama servisidir.

Günümüzde e-posta hizmetleri oldukça yaygın olarak kullanılmaktadır. Bu durum e-posta hesapları ile işlenen suçların veya kişinin e-posta aktivitelerinin incelenmesinin önemini arttırmaktadır. Bu bölümde, henüz hiçbir lisanslı adli bilişim yazılımına eklenmemiş olan Yaani Mail'in bir cep telefonu içerisinde hangi kalıntıları bıraktığını inceleyeceğiz. İncelerken kullanmış olduğum araçlar ve yazılımlar aşağıda yer alan tabloda sunulmuştur:

Adı	Açıklama
Geny Motion (3.0.3)	Sanal Android Platformu
Samsung Galaxy S8 (8.0)	Sanal Android Cihaz
ADB Tool	Cep telefonu ile bilgisayar arasındaki bağlantıyı sağlayan araç.
SQLite DB Browser	SQLite formatındaki veritabanı dosyalarını görütüleyen araç.
SublimeText	Metin Editörü

Cep Telefonu İçerisinde Yer Alan Yaani Mail Verilerini Elde Etme

Uygulama kurulduktan sonra verileri kök dizinde yer alan *com.turkcell.yaaniemail* isimli klasör içerisinde depolanmaktadır. Klasör içerisinde kullanıcı bilgilerinin tutulduğu önbellek, veritabanı, uygulama üzerinden paylaşılan dosyalar, uygulama logları, uygulamaya ait ayarların *ve verilerin* yer *aldığı XML dosyaları* olduğu görülmüştür. Kök dizinde yer alan *com.turkcell.yaaniemail* klasörü içerisinde yer alan klasörler aşağıdaki şekilde sunulmuştur:

```
C:\Windows\System32\cmd.exe - adb.exe shell
vbox86p:/data/data/com.turkcell.yaaniemail # ls -l
total 32
drwxrwx--x 2 u0_a68 u0_a68       4096 2020-01-05 21:02 app_textures
drwxrwx--x 3 u0_a68 u0_a68       4096 2020-01-05 21:02 app_webview
drwxrws--x 5 u0_a68 u0_a68_cache 4096 2020-01-05 21:02 cache
drwxrws--x 2 u0_a68 u0_a68_cache 4096 2020-01-05 21:01 code_cache
drwxrwx--x 2 u0_a68 u0_a68       4096 2020-01-05 21:03 databases
drwxrwx--x 6 u0_a68 u0_a68       4096 2020-01-06 11:57 files
drwxrwx--x 2 u0_a68 u0_a68       4096 2020-01-05 21:02 no_backup
drwxrwx--x 2 u0_a68 u0_a68       4096 2020-01-14 11:45 shared_prefs
vbox86p:/data/data/com.turkcell.yaaniemail #
```

Adli inceleme açısından kullanıcının aktivitelerine erişebilmek için bu bilgilerin analiz edilmesi oldukça önemlidir. Cep telefonu içerisindeki uygulama verilerini almak için sırasıyla aşağıdaki adımlar uygulanmıştır:

- Cep telefonunun bilgisayara bağlanması,
- **Bağlantı sonrası ADB aracı ile *adb shell* komutunu kullanarak cep telefonuna bağlanılması,**
- **Bağlantı sonrası dizinindeki uygulama verilerinin bulunduğu *data/data/* dizinine gidilmesi ve uygulama verilerinin var olup olmadığının kontrol edilmesi,**
- **Uygulama verileri kontrol edildikten sonra, *adb pull com.turkcell.yaaniemail HedefAdresYolu* yazılarak uygulama verilerinin cep telefonu içerisinden bilgisayara kopyalanması.**

data/data dizininde yer *alan com.turkcell.yaaniemail* isimli klasör içerisinde yer alan dosyalar aşağıdaki şekilde sunulmuştur.

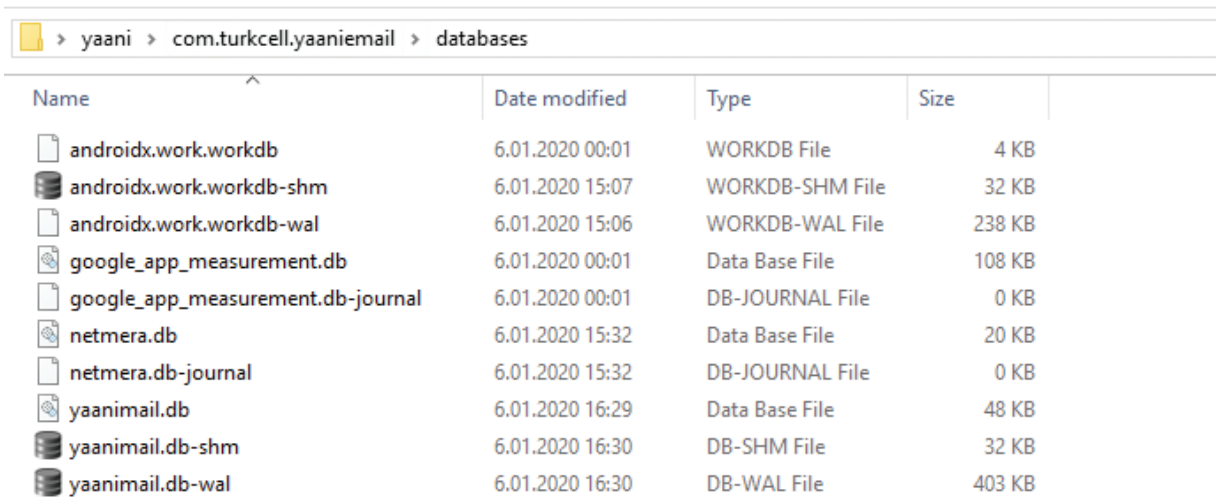
Yaani Mail Veritabanı Bilgileri ve Analizi

Yaani Mail gönderilen ve alınan mailleri kullanılan telefon üzerinde de depolamaktadır. Veritabanı bilgilerine ancak telefon üzerinden ulaşmamız mümkündür, veritabanı dosyalarına ulaşabilmek için Android telefonlarda ROOT işlemi yapılmalıdır.

Yaani Mail uygulamasının veritabanı dosyaları */data/data/com.turkcell.yaaniemail/databases* dizini içerisinde yer almaktadır. Bu dizin altındaki veriler kullanılarak kullanıcı aktivitelerine ulaşılabilmektedir. */data/data/com.turkcell.yaaniemail/databases* dizini altındaki veritabanı dosyalarının analizi için aşağıdaki adımlar izlenir:

- **Dışarıya aktırmış olduğumuz *com.turkcell.yaaniemail* verileri içerisinde yer alan *databases* klasörü içerisine girilir.**
- **Databases klasörü içerisinde yer alan veri tabanı dosyaları *SQLite DB Browser* ile görüntülenir.**

data/data/com.turkcell.yaaniemail/databases dizini içerisinde yer alan dosyaları aşağıdaki şekilde sunulmuştur.



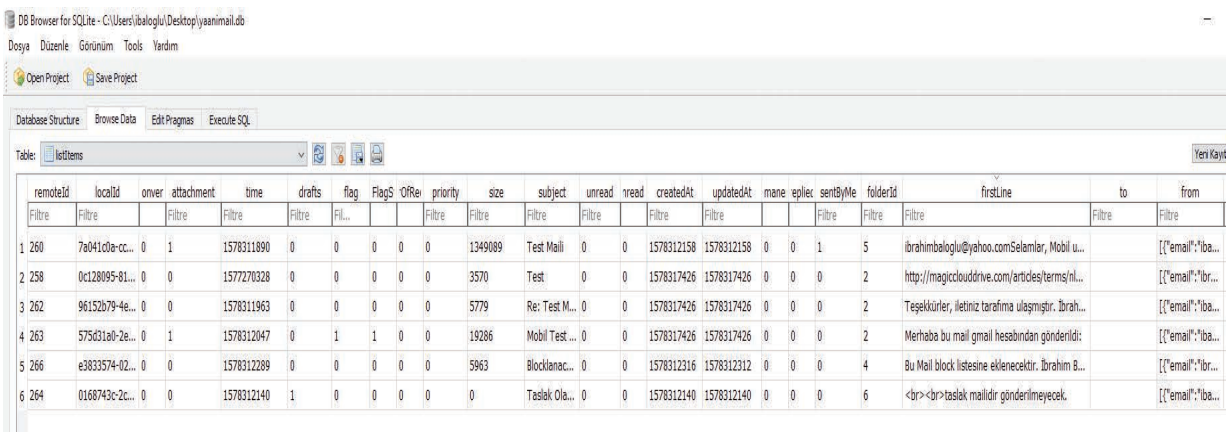
Android cihazlarda, Yaani Mail uygulaması içerisinde adli veri niteliği taşıyan iki veritabanı dosyasına rastladım. Bunlar ***yaanimail.db*** ve ***yaanimail.db-wal*** veritabanlarıdır. **yaanimail.db** bir kullanıcı ve kişiler arasındaki mail görüşmeleri hakkında ayrıntılı bilgi içerir. **yaanimail.db-wal** dosyası geçici verilerin tutulmuş olduğu bir veritabanı dosyasıdır ve uygulama içerisinde silinen maillere ait kalıntılar yer almaktadır. (*Not: .db-wal, .db-shm gibi dosyalar, geçici veritabanı dosyalarını temsil etmektedir.*) yaanimail.db isimli veritabanı içerisinde yer alan tablolara ilişkin bilgiler aşağıda yer alan tabloda sunulmuştur:

Adı	Açıklama
android_metadata	Android bilgisi yer almaktadır.
folderSyncOptions	Dosya id'lerini ve dosyaların son güncellenme tarihleri yer almaktadır.
folders	Gelen, giden, taslak, gereksiz ve kullanıcı tarafından oluşturulan dosyaların isimlerini ve içerisinde barındırdıkları mail sayıları yer almaktadır.
listItems	Kullanıcı aktivitelerinin detaylı bilgileri yer almaktadır.
messageDetails	Kullanıcı aktivitelerinin detaylı bilgileri yer almaktadır.
pendingComposeActions	İçerik kaydına rastlanmadı.
room_master_table	İçerik kaydına rastlanmadı.

yaanimail.db veritabanı içerisinde yer alan messageDetails ve listItems tabloları bir kullanıcının gönderdiği veya aldığı tüm iletilerin detaylı bilgilerini içerir. **Bu bilgilere ek olarak:**

- **Mail içeriği,**
- **Mailin API servisi üzerindeki URL adresi,**
- **Mailin bağlı olduğu dosya ID numarası,**
- **Mailin oluşturulma ve güncellenme tarihi,**
- **Mailin okunup okunmadığı bilgisi,**
- **Taslak mail olup olamadığı bilgisi,**
- **Maile herhangi bayrak bilgisinin eklenip eklenmediği bilgisi,**
- **Mailin kaplamış olduğu toplam büyüklüğün bilgisi,**
- **Mail eklerinin olup olmadığı varsa mail ekinin tipi ve ismi gibi temel bilgilere ulaşılabilmektedir.**

yaanimail.db isimli veritabanı içerisinde yer alan *messageDetails* ve *listItems* tablolarına ilişkin detaylar aşağıda yer alan şekillerde sunulmuştur.

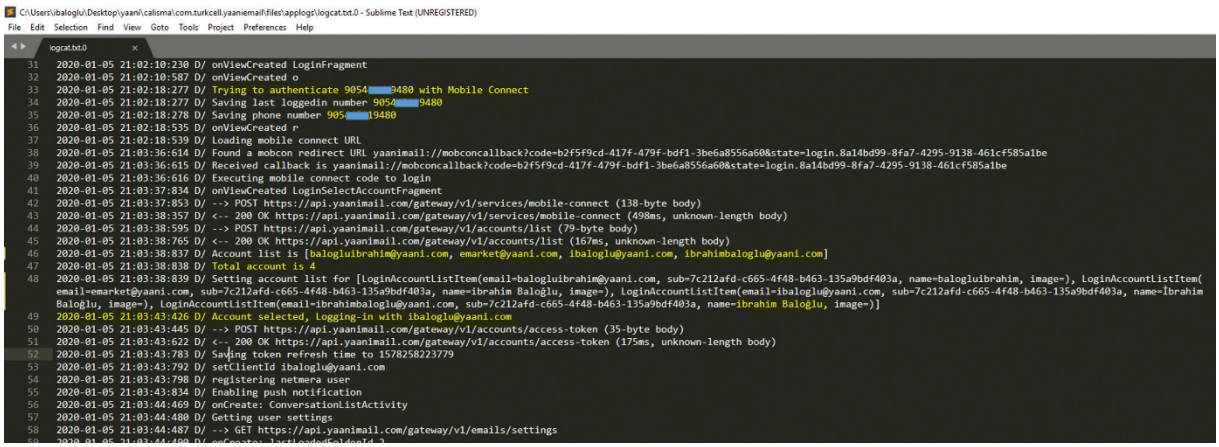


Yaani Mail Log Dosyası ve Analizi

Log dosyaları *com.turkcell.yaaniemail\files\applogs* klasörü altında yer alan ***logcat.txt.0*** isimli dosya içerisinde tutulmaktadır. Uygulama kullanıcı ve uygulama hareketleri ile ilgili yapılan işlemleri log dosyalarında saklamaktadır. Log dosyaları incelenerek adli bilişim açısından çeşitli veriler elde edilebilmektedir. logcat.txt.0 isimli log dosyasının içeriği Sublime Tex metin editörü ile incelendiğinde;

- **Maile servisine yapılan giriş tipi (hızlı giriş veya kullanıcıAdı/parola)**
- **Giriş yapılan telefon numarası bilgisi,**
- **Telefon numarasının bağlı olduğu yaani mail adreslerinin tümüne ait bilgiler (bu husus kişinin diğer yaani mail adreslerinin de öğrenilmesinde fayda sağlamaktadır.)**
- **Telefon numarasına bağlı olunan e-posta adreslerinden hangisi ile ne zaman giriş yaptığı gibi bilgiler elde edilebilmektedir.**

Mail servisinin kullanmış olduğu api servislerine ait url adresleri olduğu görülmüştür. logcat.txt.0 isimli log dosyasının içeriğine ilişkin ekran görüntüsü aşağıda yer alan şekilde sunulmuştur.



Umarım sizler için keyifli ve faydalı bir yazı olmuştur. Bir sonraki sayıda tekrar görüşebilmek ümidiyle… Esenle kalın.

Mertcan Coşkuner / mcan.coskuner@protonmail.com

Android'de Frida Öğreniyorum #1

Merhaba, uzun zamandır planladığım Frida serisini sonunda yazmaya karar verdim. Bu seride Android platformunda sızma testi ya da zararlı yazılım analizi gerçekleştirirken çoğu zaman hayatınızı kurtaran bu framework'ü ele alacağız. İlk etapta:

1. Nedir?

2. Nasıl kurulur?

3. Nasıl kullanılır?

Konularından bahsedeceğim. Frida kurulumu ve kullanımını gördükten sonra, Frida ile ne yapılabilir görmek adına her seride farklı bir kullanım örneğini ele alacağım.

Nedir?

Uygulamalara dinamik olarak müdahale edebilmenize olanak sağlayan bir toolkit'tir. Windows, MacOS, Linux, iOS, Android ve QNX ortamlarında çalışan uygulamalara JavaScript snippet'leri ya da kendi kütüphanenizi injection etmenizi sağlar. Halihazırda toolkit içerisinde basit araçlar barındırsa da (örn. frida-trace), Frida, API üzerinden kendi araçlarınızı geliştirmenize de olanak sağlıyor.

Neden Kullanayım?

Frida ile yapabileceklerinize bazı kullanım örnekleri üzerinden bakalım:

1. Elinize incelemek için bir Android uygulaması aldınız. Uygulamayı açıp, debuggable anahtar ekleyip, tekrar paketlemek gibi işlerle uğraşmak istemiyorsunuz. Hızlıca bir Frida script'i yazarak ya da frida-trace kullanarak uygulamanın davranışını inceleyebilirsiniz.
2. Android zararlı uygulaması keşfettiniz ve incelemek istiyorsunuz. Wireshark'ı aradan çıkarıp şifrelenmiş protokolleri destekleyen sniffer yazabilir, uygulamanın çalışması için gereken bazı durumları ilgili fonksiyonları tetikleyerek oluşturabilirsiniz.
3. Bir uygulamaya black-box sızma testi yapmak için gerekli tüm ihtiyaçlarınızı Frida script'leri ile giderebilirsiniz!

Frida Core

C ile yazılmıştır. Hedef process'e Google V8 Engine inject eder ve yazılan JavaScript'i çalıştırır. Process'e inject olduğu için full memory erişimi, fonksiyon hook'lama ve native fonksiyonların çağırılması/manipülasyonu mümkün oluyor. Python ve JavaScript'in birlikte kullanımı ile Frida scriptl'eri yazılabilir. Python yanında Node.js, Swift, .NET, Qml gibi dillerde de Frida geliştirmeleri yapılabilir.

Kurulum

Kurulum yapmak için Python 3.x ve Windows/MacOS/Linux bir işletim sistemi gerekiyor. Gereksinimleri sağladıktan sonra '*pip install frida-tools*' ile Frida araçlarını kuruyoruz.

Android telefonlarda Frida kullanabilmek için 'frida-server' kurmak gerekiyor. Frida'nın Github sayfasında yer alan frida-server executable dosyaları içerisinden kullandığınız gerçek/sanal telefona uygun x86 ya da ARM mimarisindeki frida-server dosyasını indirip telefonunuzda bir dizine koyup çalıştırabilirsiniz. Bu sayede yazdığınız script'leri inject edebileceğiniz ya da Frida araçlarını kullanabileceğiniz bir analiz ortamına sahip olursunuz.

Ya da üstte yazdıklarımı 'frida-server böyle çalışıyor demek' şeklinde değerlendirip '*pip install frida-push*' ile frida-push kurabilirsiniz. Kurulum sonrası '*frida-push -d <telefon/emulator-ismi>*' komutuyla direkt olarak telefonunuza uygun mimaride frida-server dosyasını telefonunuza atıp, gerekli izinlerle çalıştırıp, hızlıca analize odaklanabilirsiniz.

Kurulumunuzu doğrulamak adına '*frida-ps -U*' (-U: USB) komutuyla kullandığınız telefonun içerisindeki aktif process'leri listeleyebilirsiniz.

Frida Araçları

Frida-tools ile gelen araçlara biraz göz atalım:

1. Yukarıda kurulum doğrulama için kullandığımız '*frida-ps -U*' komutu ile aktif processleri görebilirsiniz.
2. Takip etmek istediğiniz fonksiyon çağrılarını '*frida-trace*' komutu ile gerçekleştirebilirsiniz. Örn. *frida-trace -U -i open -i strcmp -f <uygulama>* komutuyla uygulamada kullanılan open ve strcmp fonksiyonlarının takibini yapabilirsiniz.
3. *frida -U (opsiyonel: --no-pause) -f <uygulama>* komutu ile direkt ilgili uygulamaya inject olabilir ve Frida CLI ile JavaScript yazarak uygulamayı çalışırken manipüle edebilirsiniz. Eğer komutu --no-pause opsiyonunu koymadan çalıştırırsanız Frida size JavaScript kodunuzu inject etmek için zaman tanımak adına uygulamayı direkt olarak başlatmaz. --no-pause olmadan çalıştırdığınız durumlarda CLI ekranında '%resume' yazarak uygulama akışını başlatabilirsiniz.

Frida API

Frida API örneklerini, eğer direkt JavaScript değil de bir wrapper kullanacaksak, hızlıca yazabilmek adına desteklenen diller arasında en uygunu olan Python ile yazacağım. Aşağıda örnek iki adet iskelet kod bulabilirsiniz.

Frida ile çalışan bir uygulamaya inject olmak için

```
import frida, sys
script = """
Java.perform(function () {
…
…
});
"""
device = frida.get_device_manager().enumerate_devices()[-1]
session = device.attach("<uygulama>")
script = session.create_script(script)
script.load()
sys.stdin.read()
```

Frida ile bir uygulamayı yazdığımız JavaScript kodunu inject ederek açmak için

```
import frida, sys
script = """
Java.perform(function () {
…
…
});
"""
device = frida.get_usb_device()
pid = device.spawn(["<uygulama>"])
session = device.attach(pid)
script = session.create_script(script)
script.load()
device.resume(pid)
sys.stdin.read()
```

Çalışan bir uygulamaya inject olmak ile bir uygulamayı inject olarak açmak arasında bir fark yok gibi görünse de bir uygulamanın başlarken yapacağı kontrolleri atlatmak için ikinci seçenek hayat kurtaracaktır. Örneğin uygulama açıldığı esnada (MainActivity içerisinde) bir root detection ya da anti-emulator kontrolü yapıyorsa, bu kontrolü script'imizi enjekte ederek açtığımız bir senaryoda bypass edebiliriz. İroniktir ki, anti-hooking kontrolü içeren uygulamaların kontrollerini de yine Frida ile hook'layarak bypass edebilirsiniz.

İskelet kodda yer alan script alanındaki 'Java.perform(function() { });' kalıbı, uygulamayı manipüle etmek için yazacağımız kodları içerecek. Bu kodlar JavaScript ile yazılacağından, syntax olarak JavaScript kullanacağız. Örnek bir script'i aşağıda görebilirsiniz:

```
Java.perform(function () {
      const System = Java.use('java.lang.System'); // Java sistem kütüphanesi
      const Log = Java.use("android.util.Log"); // Android log kütüphanesi
      const Exception = Java.use("java.lang.Exception"); // Java exception kütüphanesi

// Java sistem kütüphanesinde yer alan exit fonksiyonunun implementasyonu
// manipüle ediliyor ve alınan exception logu direkt ekrana basılıyor
      System.exit.implementation = function() {
       console.log(Log.getStackTraceString(Exception.$new()));
      };
});
```

Bir sonraki yazımızda görüşmek üzere!

Utku Yıldırım / utku.yildirim@beamteknoloji.com

Siber Güvenlik Alanında Lisansüstü Eğitim

Merhaba değerli Arka Kapı okuyucuları. TOBB ETÜ Bilgi Güvenliği Yüksek Lisansı eğitimime devam ederken sizlere yazdığım bu makalede siber güvenlik alanında lisansüstü eğitimin ne olduğundan, ders içeriklerinden, öğrenci profilinin kimlerden oluştuğundan ve eğitimin çıktılarının bireysel kazançlarından bahsediyor olacağım. Paylaşacağım tecrübeler ve süreçler bireysel olup, üniversiteme ve bana bağlıdır. Yazıya alacaklarım, kişi ve kurumlara göre farklılık gösterebilir.

Türkiye'de Siber Güvenlik Eğitimleri

İnternet ile birlikte hızla gelişen konulardan biri güvenliktir. Yeni teknolojiler ve bu teknolojiler ile gelişen yeni donanımlar, yazılımlar ve servisler için güvenlik ihtiyacı her geçen gün artmaktadır. Bazı üniversitelerde siber güvenlik alanında seçmeli dersler açılmasına rağmen, henüz Türkiye'de siber güvenlik alanında lisans eğitimi mevcut olmadığı için bireyler, bu alan üzerine yönelimlerini bireysel çalışmalar veya bu alanda düzenlenen eğitimler, konferanslar ve etkinlikler aracılığı ile geliştirebilmektedir.

Özellikle son yıllarda bu eğitimlerin, konferansların ve etkinliklerin sayısının hızla artması ülkemizde siber güvenlik alanında nitelikli personel yetiştirilmesi için güzel gelişmeler olmakla beraber, alana ilgi duyan daha fazla insana ulaşabilmeyi sağlamaktadır. Özellikle son dönemde yapılan bu organizasyonların Türkiye'nin her yerine ulaşmasının hedeflenmesi ve bu hedef üzerine çalışılması ülkemiz adına bu alanda attığımız güzel adımlardandır.

Lisansüstü Eğitimin Amacı

Lisansüstü eğitimin temel amacı lisans eğitimi sonrası kişiye özel bir alanda uzmanlaşma sağlıyor olmasıdır. Lisansüstü eğitim çoğu zaman bireylerin bakış açısını ve bilgi birikimini genişletmektedir fakat sadece bireyin bakış açısının ve araştırmalarının yansıması olarak değil aynı zamanda toplumsal gelişimin adımları olarak da değerlendirilmelidir. Lisansüstü eğitimin kişisel bir kariyer olarak düşünülmesi hatalı olacaktır. Zira böyle bir düşünce, bilginin değersizleştirilmesine ve beraberinde akademik yetersizliğe sebebiyet verebilecektir.

Türkiye'de Siber Güvenlik Alanında Lisansüstü Eğitim

Üniversiteden üniversiteye, programdan programa göre değişmekle beraber lisansüstü programlar için belirli başvuru ve kabul şartları bulunmaktadır. Genel olarak tezli programlar için 4 yıllık lisans mezuniyeti, ALES puanı, yabancı dil puanı ve lisans diploma notu için belirlenen taban puanlar ve zorunluluklar mevcut bulunmaktadır. Başvuru koşullarına ve kabul şartlarına ilgili üniversitelerin ilgili enstitü sayfalarından ulaşabilirsiniz.

Türkiye'de siber güvenlik yüksek lisansı açan eğitim kurumlarının listesine ve haritada konumlandırmasına alttaki görselden ulaşabilirsiniz.

Şekil 1

Lisansüstü Eğitimde Dersler

Daha önce belirttiğim gibi her üniversitenin kendine ait ders listesi ve müfredatı bulunmakla beraber, örnek olması açısından eğitimim boyunca şu ana kadar aldığım dersleri ve içeriklerini özetleyeceğim. Derslerin neredeyse tamamında (özellikle teknik alandaki derslerde) eğitim süreci sektörden gelen eğitimciler ile birlikte yürütülüyor. Dersler genellikle öğrenci

profiline uygun olacak şekilde (çalışan) haftada 8 saat akademik izni engellemeyecek şekilde gerçekleştiriliyor, böylece yüksek lisans yaparken çalışma imkanı sunuluyor.

Bilişim Hukuku

Teknolojinin gelişmesi ve ilerlemesi ile birlikte ortaya çıkan hukuksal süreçlerde düzenlemelerin, yeniliklerin iki farklı bakış açısından değerlendirilebilmesini (teknik ve hukuki) mümkün kılan bu dersin eğitmenliğini, hem elektrik elektronik mühendisi hem de avukat olan Fatih Öğmen hocamız yürütmüştü. Kişisel verilerin korunması kanunu, 5651 sayılı *"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"* gibi popüler konuları içeren bu derste Türk Ceza Kanunu rehberliğinde örnek bilişim suçu senaryolarını değerlendirerek, teknik olarak bu senaryolarda alınması gereken önlemler ve teknik sorumluluklar ile süreçleri ilişkilendirerek hem gündelik hayatımızda hem de iş hayatımızda yaşayabileceğimiz süreçlerin simülasyonlarını gerçekleştirdik.

Ağ Adli Analizi

"Network Forensic" olarak bilinen bu derste yine sektörden alanında uzman hocamız Alparslan AKYILDIZ ile birlikte yürüttüğümüz derslerde, temel ağ bilgisi ile başlayarak ileri ağ bilgisi, ağ dinleme araçları, saldırılar ve saldırıların ağ üzerinde bıraktığı izler, bunların analizi ve snort - suricata gibi ortamlarda bunların tespiti için kural oluşturma üzerine tamamen uygulamalı bir eğitim aldık. Dönem sonunda proje gruplarına ayrılarak yine popüler konulardan APT atak simülasyonu, bu atakların ağ kaydı analizleri ve uç nokta trafik analizi üzerine proje gerçekleştirdik.

Sızma Testleri ve Güvenlik Denetimleri

Dersin tamamı, alanlarında uzman ve tanınmış olan hocalarımız Kürşat Oğuzhan Akıncı ve Şeref Can ÖZKAYA ile yürütüldü. "Penetration Test" olarak bilinen bu derste ise sızma testi metodolojisi, sızma testi kapsam belirleme, sızma testi adımları, sızma testi basamaklarından bilgi toplama, ağ tarama, versiyon tespiti, zafiyet keşfi ve atakları gördük. Dersin amacı, daha önce hiç sızma testi yapmamış olan birine TSE standartlarına uygun, baştan sona bir sızma testi tecrübesi yaşatmaktı. Mesleğim gereği sürekli sızma testi yapıyor olmama rağmen, bu ders farklı bakış açıları kazanmamı sağladı. Dersler, tamamen uygulamalı ve zafiyetli makineler ile hazırlanmış laboratuvar ortamında gerçekleştirildi. Sınavlar, TSE tarafından düzenlenen Sızma Testi Uzmanı Sertifika Sınavı benzerliğinde birbirlerine bağlı zafiyetli sistemler, makineler üzerinde gerçekleştirildi.

İnternet Güvenlik Protokolleri

Okulumuzdaki kıymetli bir akademisyenimiz olan Prof.Dr.Ali Aydın Selçuk tarafından verilen bu ders internet güvenlik protokollerinin teorileri üzerine bir dersti. Gündelik yaşamda kullanılan protokollerin teorik olarak incelenmesi ve detaylarının öğrenilmesi hedeflenen bu ders hem genel kültür hem tez yazım aşaması için teorik bakış açısı katmaktadır.

İstismar Programlama

"Exploit Development" olarak bilinen bu ders sektörden, kendini alanında kanıtlamış değerli hocamız Kaan EZDER tarafından verildi. Türkiye'de bu alanda eğitim bulmak gerçekten çok zor. Dönem boyunca istismar programlama üzerine uygulamalı eğitim alarak, haftalık olarak gerçekleştirdiğimiz çalışmalar ve ödevlerde CTF formatında uygulamaların istismar edilmesi üzerine çalışmalar gerçekleştirdik. Sınavlarımız yine uygulamalı olarak CTF formatında gerçekleştirildi.

Beklentiler, Gerçekleşenler

Lisansüstü eğitime başlamadan önce yaptığım araştırmalarda gördüğüm ve bu konuyla ilgili konuştuğum kişilerin sürekli olarak söylediği, akademisyen olma hayali olmayan bir kişi için yüksek lisansın boğucu olabileceği yönündeydi. Başlamadan önceki en büyük çekincem bu idi. *Akademisyen olmak istiyor muyum, istemiyor isem yüksek lisans benim için zaman kaybı mı olacak* gibi soruların cevaplarını arıyordum. "Çalışırken yüksek lisans çok yıpratır hem o kadar zamanı sertifikalara ayırsan sektörde yüksek lisanstan daha değerli çalışmalar yapmış olursun" gibi cümleleri de o kadar çok duyuyor ve endişeleniyorsunuz, ta ki yüksek lisansa başlayana kadar! Yüksek lisans esnasında yoruluyorsunuz bu doğru, hatta aynı zamanda çalışıyor iseniz daha çok yoruluyorsunuz bu da doğru ama her dönem sonunda edindiğiniz bilgi ve tecrübelere bakarak *buna değer* diyebiliyorsunuz.

Siber Güvenlik Alanında Lisansüstü Eğitimin Katkıları

Siber güvenliğe ilgim lisans hayatımda katıldığım bir Capture The Flag yarışmasında başlamıştı. Sonrasında alana dair araştırmalar yapmama rağmen, nereden nasıl başlayacağım konusunda kendime yol haritası çizmek konusunda zorluk yaşamıştım. Düzenlenen birkaç eğitime katıldıktan sonra bu eğitimlerden birine ev sahipliği yapan TOBB ETÜ'nün siber güvenlik yüksek lisansı mevcut olduğunu öğrendim ve yol haritamı belirleyebildim. Lisans eğitimimi bitirerek sonrasında yüksek lisans eğitimimi siber güvenlik alanında yaparak uzmanlık alanıma bu vasıtayla yöneldim.

Şu an hem eğitimim devam etmekte hem de siber güvenlik alanında bir firmada "Penetration Tester" olarak çalışmaktayım. Lisansüstü eğitim süreci, kırmızı takım alanında çalışma-

ma rağmen alanım dışındaki farklı perspektifleri göstermektedir. Hatta öyle ki alanımla ilgili farklı bakış açıları, pratik yöntemler ve yeni sistemlerde tecrübeler kazanmama olanak sağlamaktadır. Saldıran tarafta olmanın yanı sıra savunan taraftın inceliklerini, bakış açılarını görmek benim hem günlük yaşamımda hem de iş yaşamında farklı tecrübeler edinmemi sağlamaktadır.

Alanında uzman insanlardan eğitim almanın haricinde siber güvenlik alanında yüksek lisans yapmanın en büyük katkısı, farklı uzmanlık alanlarından ve farklı firmalardan insanlar ile birlikte aynı ortamı paylaşmak, onlarla bilgi alışverişinde bulunmak ve tecrübelerini dinleyerek kendini geliştirmektir. Neredeyse siber güvenlik alanında faaliyet gösteren her firmadan her alandan insan ile etkileşime geçebileceğiniz bir sınıf ortamı mevcut bulunmaktadır. Birlikte oluşturduğumuz proje grupları ile mesleki bilgi birikimlerimizi ortak paydada toplayarak ortaya geniş kapsamlı ürün fikirleri çıkartabilmekteyiz. Şu ana kadar yaşadığım bütün süreçten, elde ettiğim tecrübelerden ve harcadığım emekten memnunum. Bilginin paylaşıldıkça çoğaldığı bu devirde, paylaşılabilecek insanlarla iç içe olmak insanı hem motive hem de mutlu ediyor.

Türkiye'de bu sektörün gelişmesi ve büyümesi için eğitim ihtiyacı bulunmakla beraber uzman akademisyen ihtiyacı da bulunmaktadır. Siber güvenlik alanında lisansüstü eğitimin bir diğer çıktısı ise lisans düzeyinde uygulanmasını umut ettiğimiz eğitimlerin verilmesini sağlayacak, siber güvenlik alanında uzman akademisyenler yetiştirilmesidir. Özellikle siber güvenlik alanında tabiri caizse usta-çırak yapısını değiştirecek olan nesil bizleriz. Sektörde bilgileri çok değerli, tecrübelerine saygımız sonsuz gerçekten çok kıymetli "alaylı" insanlarımız mevcut olsa da bu sektörün "mektepli" grubuna artık çok net şekilde ihtiyacı olduğunun farkındayız.

Bu makaleyi, siber güvenlik alanında lisansüstü eğitim konusunda elde etmiş olduğum deneyimlerimi sizlerle paylaşmak ve lisansüstü eğitimine siber güvenlik alanında başlamak isteyenler için fikir ve yol gösterici olması ümidiyle yazdım. Bu alanda da lisansüstü eğitim veren kurumların artmasını ve bu alanda Türkiye'nin ihtiyaç duyduğu yüksek nitelikli insan gücünün elde edilmesini temenni etmekteyim.

Kaynaklar:

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'in-tarih%C3%A7esi

https://www.savunmasanayiidergilik.com/tr/HaberDergilik/Turkiye-deki-siber-guvenlik-yuksek-lisans-programlari

https://www.etu.edu.tr/tr/bolum/bilgisayar-muhendisligi/lisans-ustu-programlar/17

Are You Safe?

We protect your company from attackers.

+90 (850) 885 32 16
info@strixcs.com
Buyukdere St. No:107 Esentepe

strix
cyber security

Muhammed Hilmi Koca - mhkoca60@gmail.com

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.

Şol Kuantum Bilgisayar Dedikleri

Kuantum Bilgisayar son dönemin "hype"larından. Ama ismi ne kadar bilinse de ne olduğunu gerçekten bilen kişi sayısı çok az. Ne olduğunu bilenler arasında da muhtemelen gerçekten nasıl çalıştığını bilen sayısı daha da az. Ki aslında bu pek anormal bir durum değil. Çünkü konu fizik, kuantum fizik, matematik ve bilgisayar bilimlerini aynı anda içeriyor.

Konu hakkında nitelikli Türkçe içerik üretenlerden Kutlu Kutluer, uzun uzadıya ve elden geldiğince anlayacağımız seviyeye indirgeyerek Kuantum Bilgisayarlarını, çalışma prensibini ve nasıl inşa edildiklerini detaylıca anlatmış. (Daha önce dediğim gibi beynimde yer yer kızarıklıklar oluşsa da baya anladığımı sanıyorum.)

Diğer yandan Yavuz Selim Yıldız da Kuantum Bilgisayarlar'ın çalışma prensibini anlatarak başladığı yazısında, bu bilgisayarların Bitcoin ve Sha256 şifreleme algoritmasının güvenliği için bir tehdit olup olmadığını irdelemiş.

Google vs Rekabet Kurulu

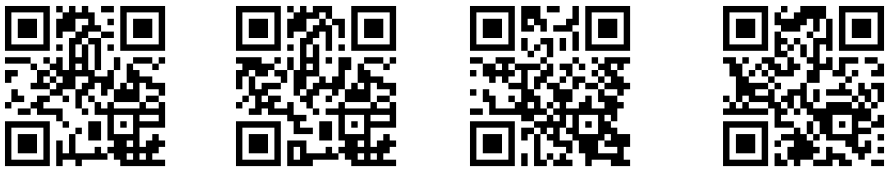
Geçen haftanın flaş gelişmelerinden biri Rekabet Kurulu'nun Google kestiği ceza ve akabinde Google'ın misilleme olarak Android uygulamalarının(Google Play, Gmail vb.) lisanslarını Türkiye'ye kapatması oldu. Bu konuda pek çok yazı, haber çıktı.

Hadi Tok, konunun geliştiricilere bakan yönünü anlatan 2 yazı yayımlamış. İlkinde genel durumdan ikincisinde ise teknik detaylardan ve problemin çözülememesi halinde uygulanabilecek alternatiflerden bahsetmiş. Ayrıca durumun ciddiyetine binaen yazılımcıları seslerini duyurmaya çağırarak bir imza kampanyası başlatmış.

Kullanıcı Deneyimi

Bir yazılım ürünün başarısı pek çok farklı etkene kritik seviyede bağlı. İlk olarak yazılımın ihtiyaçları karşılayabilmesi, sonra kullanımı kolay bir arayüz ve tamamen farklı bir disiplin olan pazarlama kısmı. Biz yazılımcılar doğal olarak ilk kısımla ilgileniyoruz. Ama ister istemez UX nam kullanıcı deneyimi kavramı ile de muhatap oluyoruz. Takip ettiğim bloggerlardan Arda Aksoy, son dönemde bu alanda yoğun ve nitelikli içerikler üretiyor. Bunların ikisinde vazgeçmesi zor bir ürün ve kullanıcıların seveceği bir ürün inşa etmekten, bir diğerinde MVP yerine MLP(Minimum Lovable Product) çıkarmaktan, bir başkasında ürüne gereksiz özellikler ekleme hastalığından(feature creep), diğer bir yazıda ise kullanıcı araştırmalarından bahsetmiş. Ayrıca Medium profilinde görebileceğiniz üzere günlük hayatta kullandığı dijital ürünlerin/servislerin "kullanıcı gözünden" deneyim incelemesini yazıyor.

Burak Çevik de bekleme (yükleniyor…) ekranlarının kullanıcı deneyimi doğrultusunda tasarımını anlatmış.



Yapay Zeka ve Yazılımcılar

Yapay Zeka pek çok sektörü etkilemeye hazırlanırken muhtemelen biz yazılım geliştiricileri de boş geçmeyecek. Deniz Kılınç, Yapay Zeka'nın biz yazılım geliştiricilere ve geliştirme süreçlerine muhtemel etkilerini somut örneklerle anlatmış.

Yapay Zeka demişken;

Profesör Cem Balçıkanlı Yapay Zeka'nın yabancı dil çevirisi konusunda ne kadar başarılı olduğunu ve iyi çeviri için karşılaşabileceği zorlukları irdelemiş.

Rahime Yeşil, veri mahremiyeti odaklı makine öğrenimi algoritması "federe öğrenim"den bahsetmiş.

Şevket Ay, makine öğrenmesinde topluluk öğrenimi kavramından ve bunun için kullanılan algoritmalardan bahsetmiş.

Burak Yılmaz, Karar Ağacı algoritması oluşturmayı anlatmış.

İbrahim Baran, R dilinde Makine öğrenimi kullanmayı kolaylaştıran H2O kütüphanesinden bahsetmiş.

Bugün Ne Öğrendik

Recep İnanç, güzel bir motivasyonla yazılım hakkında günlük öğrendiği şeyleri blog olarak paylaşmaya karar vermiş. Serinin başlığını TIL(Today I Learned) olarak belirlemiş. Büyük oranda hedefini yakalayarak devam ediyor: 1 ayda 25 yazı. Konularda yok yok: mesaj kuyrukları, String kullanımının ideal yöntemi, çöp toplayıcıların(garbage collector) çalışma prensibi, yazılım prensipleri; kısa kısa eşzamanlılık, paralel programlama, mikroservis mimarisi ve dahası. Takipte kalıp istifade etmek gerek.

İşlemcinin İşleyişi

Burada münasebeti geldikçe ifade ettiğim gibi yüksek seviyeli dillere ve frameworklere daldıkça temellere yabancılaşıyoruz. Halbuki temelleri, bilgisayarın mimarisini, işlemcileri, derleyicileri… bilmek hem ufuk açıyor hem de bizleri daha iyi yazılımcı yapıyor. Bu kapsamda geçtiğimiz haftalarda 2 yazıya denk geldim. Bunlardan ilkinde Barış Ekin Yıldırım, modern CPU'ların çalışma prensibini anlatmış. Ömer Savaş ise oldukça anlaşılır bir örnekle işlemcinin aritmetik işlemleri yapan birimi ALU'nun(Arithmetic Logic Unit) işleyişini anlatmış.

Ayrıca Prisync ekibi hazırladıkları video içerikte derleyicilerin(compiler) çalışma prensibini anlatmış. Konuyla alakalı tavsiye edeceğim bir diğer video ise Frame of Essence kanalından.

Bir E-Ticaret Sitesinde Kampanya Dönemi

Kasım ayı e-ticaret siteleri için adeta 2 aşamalı bir sınav ayı. İlk aşama 9-11 Kasım indirimleri, ikinci aşama ise Black Friday haftası. Geçtiğimiz sene olduğu gibi bu sene de sınavlar zorlu geçti. Dönem dönem patlamalar meydana geldi. Ben de o dönem bu sıkıntılar için vaka çalışması niteliğinde içerikler görmeyi ummuştum. Denk geldiğim ilk içerik Trendyol ekibinden geldi. Onur Destanoğlu, kampanya dönemin öncesi aldıkları önlemlerden başlayarak 9-11 kampanya döneminde yaşananları, iyi yaptıkları ve sıkıntı çektikleri konuları, bunlar için yaptıkları düzenlemeleri, Black Friday dönemi tecrübelerini ve çıkardıkları dersleri kaleme almış.

Bu arada Trendyol Tech ekibi, son dönemlerde çok yoğun ve nitelikli içerikler üretiyor. Bunlardan birkaçı ;

Hüseyin Demir, birbirinden farklı 4 veritabanı kullandıkları

yapıda provision işlemlerini nasıl kolaylaştırdıklarını anlatmış.

Onur Mat, ElasticSearch'te ileri seviye performans iyileştirme yöntemlerinden bahsetmiş.

Emre Savcı ise Golang'de struct kullanımında nasıl memory optimizasyonu yapılabileceğini anlatmış.




Bir Emülatör Yazmak

Rust, son zamanların en çok övülen dili olabilir. Benim de zaman bulabilirsem öğrenmeyi istediğim bir dil. Onur Aslan, bizler için Rust ile oldukça ilginç ve kapsamlı bir proje geliştirmiş ve geliştirilmesini e-kitap olarak yayımlamış. Konu: Rust ile bir CHIP-8 dili emülatörü yazmak. Proje, ayrıca emülatörlerin ve aynı zamanda modern CPU'ların çalışma prensibini anlamak için de önemli.

Kitap Okumak

Okumanın, hassaten kitap okumanın saymakla bitmeyecek kadar çok faydası var. Bir şeyler öğrenme, yeni bakış açıları/perspektifler kazanma, kendini ifade etme yetisinin gelişmesi, farklı dünyaları tanıma, insan psikolojisini anlama, anlayışın genişlemesi… Biz yazılımcılar genelde blog veya teknik kitaplar okuyoruz ama diğer kitaplara pek eğilmiyoruz. Halbuki mesleğimizle ilgili de alacağımız nice feyiz, teknik olmayan kitaplarda saklanmış bekliyor.

Bu noktada Hüseyin Polat Yürük, biz yazılımcıların neden ve nasıl kitap okuma alışkanlığı kazanabileceğimizi anlatmış.

Bir başka yazısında ise önde gelen hobilerimizden "yazılımı sıfırdan yazmak" konusundaki notlarını kaleme almış.


Veri Bilimine Dalış

Deniz Kılınç, "Python ile veri bilimi" yazılarının üçüncüsünü yayımlamış. Bu kez Python ile veri ön işlemeye dalmış.

Bekir Arslan, veri analitiği ve iş zekası konularında faydalandığım video kaynakları derlemiş.

Ezel Merin Nalbantoğlu, yapay zeka ve büyük verinin pazarlama süreçlerine etkilerinden bahsetmiş.

Veri demişken Mert Çobanov, detaylı bir örnek üzerinden veri görselleştirmeyi anlatmış.




Kapsamlı Bir Proje

En üretken yazılımcı bloggerlarımızdan Bora Kaşmer, bir kez daha spesifik bir konuyu alıp detaylıca anlatmış. Bu kez normalden de detaylı bir proje/makale yazmış ve 3 parça olarak yayımlamış. İlk yazıda NodeJS ve Angular üzerinden yetkilendirme(authentication) ve güvenlikten(security) bahsetmiş. İkinci yazıda NodeJS'te Redis kullanımını göstermiş ve örnek projede refactoring yapmış. Üçüncü yazıda ise projeye Socket.io ekleyerek sunucudan gerçek zamanlı veri iletimini anlatmış.



Mikro Startup

Küçük ek projelerle pasif gelir sağlayabilmek mesleğimizin en güzel yönlerinden biri olabilir. Hüseyin Mert, bu projelerin anı yakalayan, ürün ya da ürüncük olanlarını "micro startups" olarak nitelemiş.

Geçtiğimiz haftalarda yayımladığı diğer bir yazıda hype aşamasını aşmış NodeJS ve Golang'den, başka bir yazısında ise sistematik hale getirdiği yazılım problemi çözme adımlarından bahsetmiş.

Javascript'i Anlamak

Javascript frontend, backend, mobil derken her tarafımızı sarmaya devam ediyor. Direkt Javascript geliştirici olmasak da ucundan bucağından bir şekilde bulaşıyoruz. Böyle bulaşınca da çoğu zaman gerçekten öğrenmeden, ihtiyacımız olan şeyleri StackoverFlow'dan bulup devam ediyoruz. Sonuç olarak da x fonksiyonu nasıl çalışıyor, y keywordü neden şurada farklı, burada farklı davranıyor vb sorular kafamızı kurcalıyor(*yaşanmış olaylardan esinlenilmiştir*). Onur Dayıbaşı, bu durumda olanlara deva olabilecek güzel bir seriye başlamış. İlk etapta Javascript'in tarihçesini anlatarak sırasıyla önemli kavramları neden ve nasıl kullandığımızı anlatmış. An itibariyle seri, 9 yazıya ulaşmış.

Yine Tahir Kardak, Javascript'te bolca kafa karıştıran this ifadesini anlatmış.

Halil İbrahim Özdoğan, Javascript'te daha performanslı uygulamalar geliştirmek için kullanılabilecek memoization yöntemini anlatmış.

Derek Austin, Javascript'te Infinity kavramını anlatmış.

Kaan Bayram ise Javascript'te Object.freeze() fonksiyonunun kullanım nedenini, mutable ve immutable kavramlarını anlatmış.

Diğer yandan Zafer Ayan, Javascript ES6 üzerinden detaylıca fonksiyonel programlamayı anlatmış. Hem fonksiyonel programlamayı öğreniyorsunuz hem de Javascript'i daha iyi anlıyorsunuz.

Tertemiz Mimari

Clean Architecture, literatüre Robert C. Martin tarafından sokulan bir konsept. Ve bu konsepti/deseni implemente eden, hayatımızı kolaylaştıran Hexogonal ve Onion gibi mimariler var.

Gökhan Gökalp, yine detaylı bir anlatımla AspNet Core'da Clean Archtitecture ile tasarlanmış bir uygulama geliştirmeyi anlatan bir seriye başlamış.

Yunus Emre Kaş ise Clean Architecture'ın ne olduğunu ve sahip olması gereken katmanları anlatmış.

Mimari demişken Bahadır Taşdemir, "event driven" mikroservis mimarisini anlatmış.

Gökhan Ayrancıoğlu, mikroservis mimarisi serisinde bu kez bir yazılımı mikroservis mimarisinde nasıl tasarlayabileceğimizi yazmış.

Hüseyin Kutluca, yazılım mimarileri serisinde dağıtık servislerde veri iletimini sağlayan DDS arakatmanından bahsetmiş.

Çin'in Blockchain Seferberliği

Geçen haftaların ilgi çekici gündemlerinden biri Çin'in Blockchain seferberliği idi. Devletin öncelikli teknoloji olarak belirlediği Blockchain, gazete manşetlerine ve sayfalarca bilgilendirme yazısına konu olmuş.

İsmail Hakkı Polat, Çin'in bu hamlelerle ne yapmak ve nereye varmak istediğini irdelemiş. Diğer bir yazısında ise 2020 Cumhurbaşkanlığı Yıllık Planı'nda yer alan Türkiye'nin dijital parasından bahsetmiş.

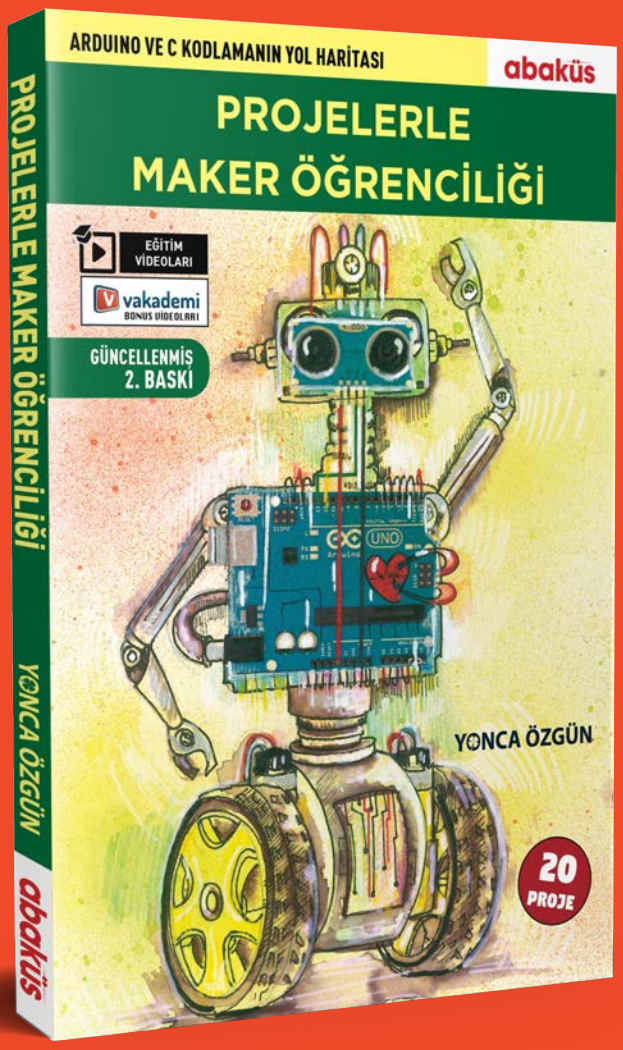
Enes Türk ise Çin'in bu teknolojiyi benimseme yolundaki 7 adımından bahsetmiş. Bir diğer yazısında ise Libra'nın mutabakat algoritması LibraBFT'yi anlatmış.

Blockchain'den bahis açılmışken Selim Önengüt, Blockchain teknolojisinin hukuk büroları için kullanımını inceleyen ve verimli olup olmayacağını sorgulayan bir çalışmayı anlatmış.

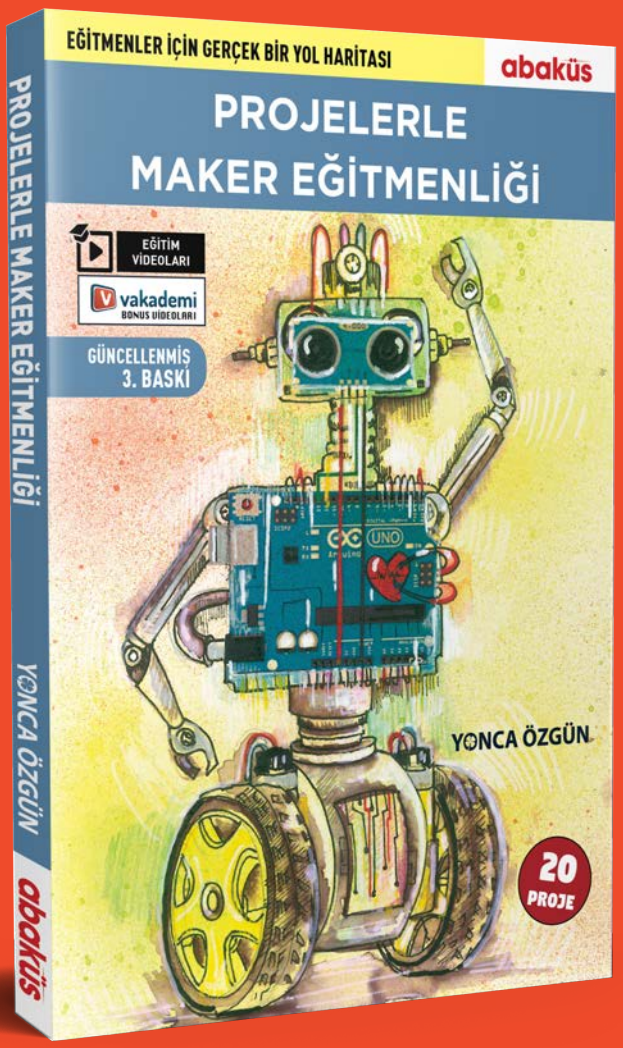
Devrim Danyal, özellikle Blockchain uygulamalarında kullanılan konsensüs algoritmalarından ve bunlara neden ihtiyaç duyulduğundan bahsetmiş.

Kanunlarımız

Yasa, ortaokuldan hatırladığım kadarıyla "bilimsel olarak doğruluğu kesin teorem"ler olsa da bizim hayatımızdaki kanunlar, yasalar(Murphy, Moore) daha ziyade genellemeleri ifade ediyor. Github'da Hacker Laws diye bir doküman oluşturulmuş. Yazılım ve bilgisayar bilimi ile ilgili yasalar ve yazılım prensipleri güzelce derlenmiş. Umut Işık, amme hizmeti olarak bu dokümanı Türkçeye çevirmiş.



PROJELERLE MAKER ÖĞRENCİLİĞİ

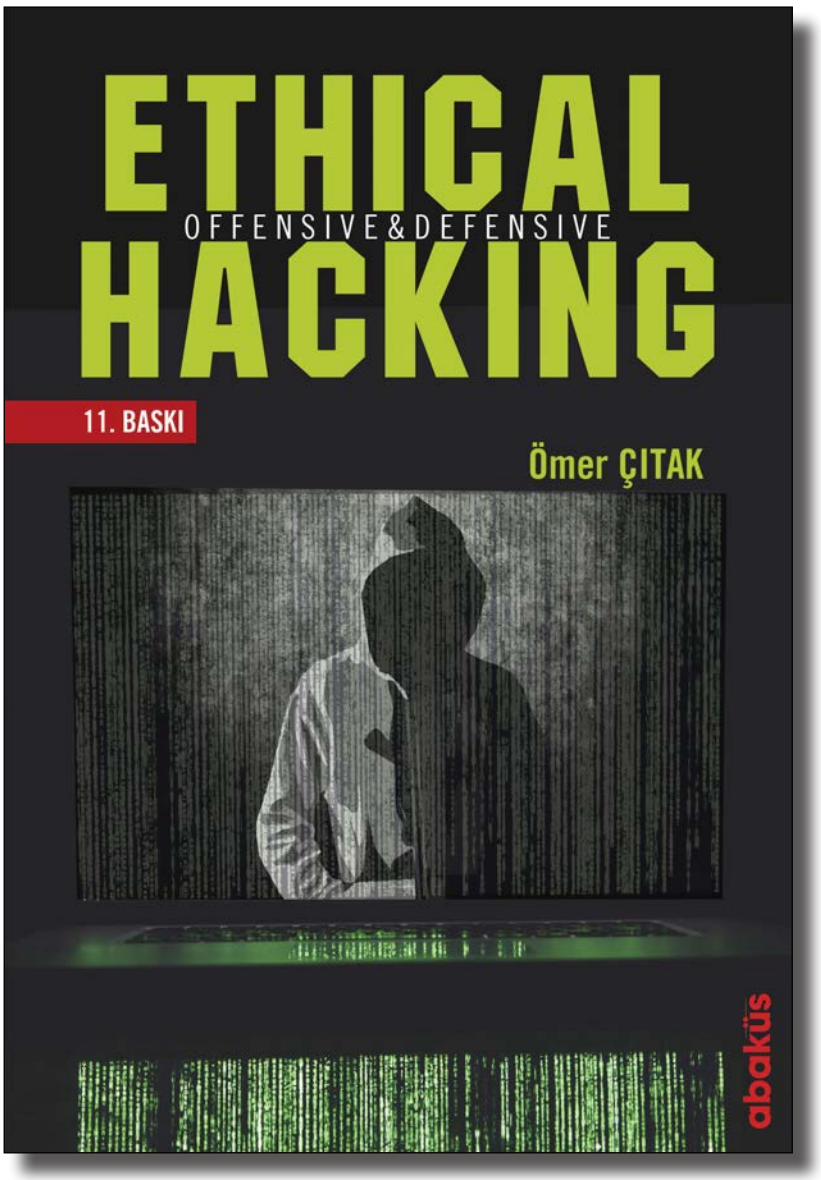


PROJELERLE MAKER EĞİTMENLİĞİ

www.abakuskitap.com

ETHICAL HACKING

ÖMER ÇITAK



abaküs

...
Kendi kendimizle yarışmadayız, gülüm.
Ya ölü yıldızlara hayatı götüreceğiz,
Ya dünyamıza inecek ölüm.
Nâzım Hikmet

Cemil Taşçıoğlu
1952-2020