TÜRKİYE'NİN İLK ve TEK BASILI HACKER DERGİSİ

ARKA KAPI

SİBER GÜVENLİK DERGİSİ

www.arkakapidergi.com

13. SAYI - 2022

Covid-19 Pandemi Sürecinde Dijital Yaşam ve Son Kullanıcı Güvenliği Hakkında • Ömer Yerlikaya

PRISM - NSA Tüm Dünyayı Neden ve Nasıl İzledi? • Oğuz Aydınyılmaz

Faturayı Yapay Zekâya Kesmek Adil mi? • Gönül Aycı

T-POT Honeypot Nedir? Nasıl Kurulur? • Erdinç Tandoğan

Mavi Takım Yolunda İlk Adım • Cemal Taner

Android'de Frida Öğreniyorum - III • Mertcan Coşkuner

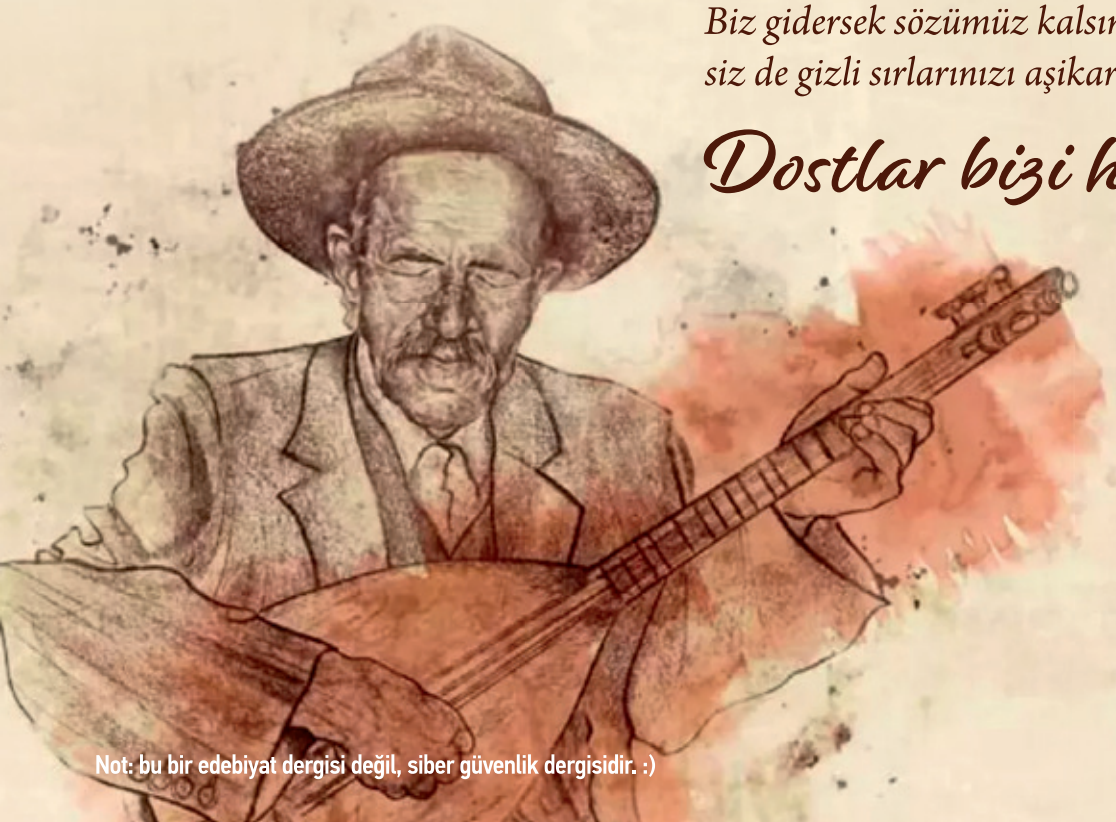
Broken Authentication • Neslihan Helvacıoğlu

Siber Güvenlikte Purple Team Yaklaşımı ile Cobalt Strike Saldırısı ve Tespiti • İbrahim Baloglu

Taklit Aslına Övgüdür: Device Spoofıng'e Dair Gözden Kaçan Ayrıntılar • Ziyahan Albeniz

İki kapılı bir hanın Arka Kapı'sından hepinizi muhabbetle selamlıyoruz.
Biz gidersek sözümüz kalsın dünyada,
siz de gizli sırlarınızı aşikar etmeyin.

Dostlar bizi hatırlasın.



Not: bu bir edebiyat dergisi değil, siber güvenlik dergisidir. :)

1894 - ∞

KÜNYE

YIL: 2 Sayı: 13 - ISSN: 2618-6373

www.arkakapidergi.com

2 ayda bir yayımlanır.

Merkez: Yakuplu Mah. Hürriyet Blv.
Skyport Plaza Kat: D:64-65
Beylikdüzü - İstanbul

Genel Yayın Yönetmeni: Ziyahan Albeniz

Editör: Şahin Solmaz
editor@arkakapidergi.com

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

Grafik Tasarım: Özgür Yurttaş

Düzelti: Huriye Özdemir

Yayın Koordinatörü: Oğuz Aydınyılmaz

Hukuk Müşaviri: Avukat Mehmet Pehlivan
Pehlivan İlkakın Hukuk Bürosu

Sosyal Medya: Nuri Çilengir, Doğukan Turan
Web: www.arkakapidergi.com
Twitter.com/arkakapidergi
abone@arkakapidergi.com
editor@arkakapidergi.com
etkinlik@arkakapidergi.com

Baskı: Repar Tasarım Matbaa, Yenibosna Merkez Mah. Cemal Ulusoy Cad. No: 43 Bahçelievler/ İstanbul
Sertifika no: 40675

Editörden

Uzunca bir aradan sonra yazacak çok şey birikti.

Bayram tebriği ile hızlıca başlayalım. Bu yazının yazıldığı tarih 1 Mayıs, Emek ve Dayanışma Günü. Tüm emekçi dostların bayramını kutlarım. Yarın da Ramazan Bayramı tüm Müslüman aleminin bayramını tebrik eder, bu iki bayram vesilesi ile ülkemize adalet, demokrasi ve refah dilerim.

*

Twitter'ın satılması, veri ifşaları, phishing saldırılarındaki korkunç artış, Türkiye'de sosyal medya düzenlemelerinin tekrar gündeme gelmesi gibi birçok hadise var ele alınacak ama gel gör ki bugün bizim için daha önemli bir gündem var, o da bu sayının dergimizin son sayısı olması…

*

Ocak, 2018 itibari ile kıymetli ağabeyim Ziyahan Albeniz önderliğinde, *-karanlığa söveceğine bir mum da sen yak-* felsefesi ile, Abaküs Kitap iş ortaklığı ile başlattığımız dergi faaliyetlerinin maalesef sonuna geldik. Dergi faaliyetlerine son verme zorunluluğumuzun nedeni gönüllülük esaslı sürdürdüğümüz bu faaliyetlerin, pandemi öncesi başlayan zorlu koşullar ve akabinde pandemi süreci ile birlikte hayatın her alanında çok daha zor olan sürdürülebilirlik direncinin kırılması oldu bizim için. Üretim maliyetlerinde yaşanan ciddi artışlar, ülkenin ekonomik koşullarının etkilediği dergi satışları gibi nedenlerden dolayı bu kararı almak zorunda olduğumuzu üzülerek bildiriyoruz.

ama mutluyuz, çünkü;

Bugüne kadar birbirinden güzel onlarca dergi sayısı ve yüzlerce makale yayımladık. Özel sektörden kamuya kadar birçok kurumun, ve yüzlerce abonenin ilgisine nail olduk. Birçok etkinlik düzenledik, üniversitelere konuşmacı olarak misafir olduk, etkinliklere katılımcı olduk, öğrenci dostlarımıza ve onların kulüplerine elimizden gelen desteği sağlamaya özen gösterdik. Milli Eğitim projelerine destek olduk.. Velhasıl hacking kültürünü yaşamak ve yaşatmak için elimizden geleni yaptık. Dolayısı ile içimiz rahat, ve çok şükür mutluyuz.

Zor olan kötü haberi verdik, şimdi sıra iyi haberde!

Derginin bu sayısı itibari ile tüm sayılarını ücretsiz erişime, halka açıyoruz keyifle okuyunuz.. :)

kıymetli abonelerimiz,

Abonelikleri devam eden abonelerimizin dergiarkakapi@gmail.com adresi üzerinden bizlere abone bilgisi ve hesap numarası ile ulaşmaları doğrultusunda ilgili iade işlemleri yapılacaktır.

teşekkür:

Öncelikle emeğine paha biçmenin mümkün olmadığı kıymetli yazarlarımızın, siz değerli takipçilerimizin, iş ortaklarımızın, yayında yapımda emeği geçen tüm dostların ve son olarak kıymetli ekip arkadaşlarımızın emekleri var olsun, hepsine can-ı gönülden teşekkür ederiz.

Eğer yeterince dikkatli bakarsanız her yerde Arka Kapı'nın bir izini görebilirsiniz.. :)

son söz:

ve son söz Ziyahan ağabeyden: *Gök kubbe'de hoş bir sada bıraktıysak kendimizi bahtiyar sayacağız.*

Güvenli günler dostlar, kalın sağlıcakla.

Şahin Solmaz - editor@arkakapidergi.com

İÇİNDEKİLER

Haziran 2022 Siber Güvenlik & Bilişim Etkinlikleri 3

COVID-19 Pandemi Sürecinde Dijital Yaşam ve Son Kullanıcı Güvenliği Hakkında - Ömer Yerlikaya 4

Facebook 533m Veri Sızıntısı Analizi - Abdullah Çiçekli 13

PRISM - NSA Tüm Dünyayı Neden ve Nasıl İzledi? - Oğuz Aydınyılmaz 21

Faturayı Yapay Zekâya Kesmek Adil mi? - Gönül Aycı 24

T-POT Honeypot Nedir? Nasıl Kurulur? - Erdinç Tandoğan 28

Kripto Para Pisasasına Merhaba - Şahin Solmaz 34

Mavi Takım Yolunda İlk Adım - Cemal Taner 40

Android'de Frida Öğreniyorum - III - Mertcan Coşkuner 53

Broken Authentication - Neslihan Helvacıoğlu 57

Siber Güvenlikte Purple Team Yaklaşımı ile Cobalt Strike Saldırısı ve Tespiti - İbrahim Baloglu 61

Taklit Aslına Övgüdür: Device Spoofıng'e Dair Gözden Kaçan Ayrıntılar - Ziyahan Albeniz 76

Tünelin Ucundaki Işık: SSH Port Forwarding - Arka Kapı 86

2021 Yılının Siber Güvenlik İstatistikleri - Arka Kapı 93

Haziran 2022 Siber Güvenlik & Bilişim Etkinlikleri

Siber Güç Türkiye

08 Haziran 2022 | TÜBİTAK Gebze Yerleşkesi, 08:00

TÜBİTAK Marmara Teknokent, TÜBİTAK BİLGEM ve MÜSİAD Dijital Dönüşüm Sektör Kurulu koordinatörlüğünde gerçekleştirilecek olan Siber-güç Türkiye etkinliği; Siber güvenlik sektöründe faaliyet gösteren kamu, üniversite, STK ve özel sektör işletmelerinin, proje ortaklığı, şirket ortaklığı ve yatırım hedefleriyle bir araya geldiği bir organizasyondur.

Bilgi: **https://www.sibergucturkiye.org/**

Bilişim Söyleşileri

10 Haziran 2022 | Şarkışla, Sivas

Tübitak Bilişim Söyleşileri 1. Dönem etkinliklikleri kapsamında düzenlenecek olan bu son söyleşi, Sivas'ta Ortaokul öğrencilerine yönelik olarak gerçekleştirilecektir.

Bilgi: **https://bit.ly/3FNzXFZ**

Türk Telekom Siber Güvenlik Kampı 2022

01-10 Ağustos 2022 | İstanbul

Son başvuru tarihi 30 Mayıs olan e bu yıl üçüncü kez gerçekleştirilecek olan Siber Güvenlik Kampı nitelikli eğitim fırsatları ve birbirinden değerli ödülleriyle geleceğin siber kahramanları arasına katılma imkanı sunuyor.

Bilgi: **https://bit.ly/3Nji3xl**

TEKNOFEST Hack Karadeniz

30 Ağustos - 04 Eylül 2022 | Samsun Çarşamba Havalimanı

Son başvuru tarihi 26 Haziran olan ve TEKNOFEST Havacılık, Uzay ve Teknoloji Festivali kapsamında T.C. Dijital Dönüşüm Ofisi yürütücülüğünde düzenlenen yarışmada hacker'lar, dünyanın önde gelen uzmanlarının rehberliğinde hazırlanan gelişmiş gerçek yaşam siber saldırı senaryolarıyla sınırları zorlayacak.

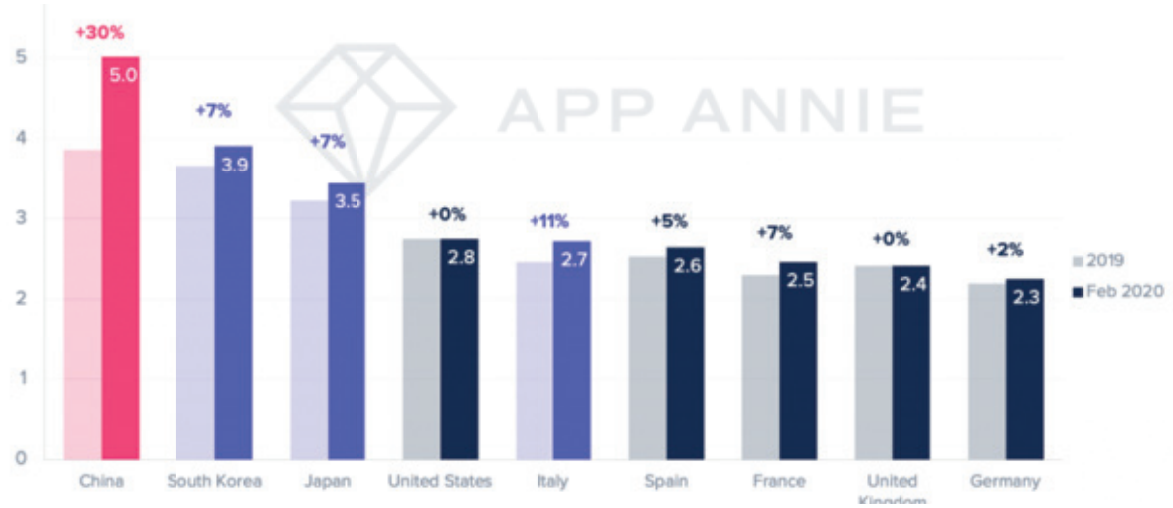
Bilgi: **https://www.teknofest.org**

Ömer Yerlikaya • yerlikayaomer@yahoo.com

COVID-19 PANDEMİ SÜRECİNDE DİJİTAL YAŞAM VE SON KULLANICI GÜVENLİĞİ HAKKINDA

Covid-19 Pandemisi'nin etkisiyle tüm dünyada hayatın akışı ve ritmi değişmişti. Virüsün etkisini ve yayılmasını azaltmak için kısmi ya da tam zamanlı sokağa çıkma yasakları, karantinalar, insanların kendilerini izole etmeleri ve sosyal mesafenin korunması gibi önlemler alınmak zorunda kalınmıştı. İnsandan insana temasın olabileceği; alışveriş merkezleri, sosyal aktivite mekanları, iş yerleri, eğitim kurumları vb. yerler kapatılmıştı. Artık insanlar ihtiyaçlarını ellerindeki telefon, tablet veya masalarındaki bilgisayarlar gibi cihazlar ile gidermek zorunda kalmıştı. Zaten kullanılan bu cihazlar bu dönemde daha çok kullanılmaya başlanmıştı. İnternet'te daha önce hiç bulunmamış, yeni doğmuş kullanıcılar bile vardı. Artık insanlık tam olarak ortak bir yerde; dijital dünyada, İnternet dünyasındaydı…

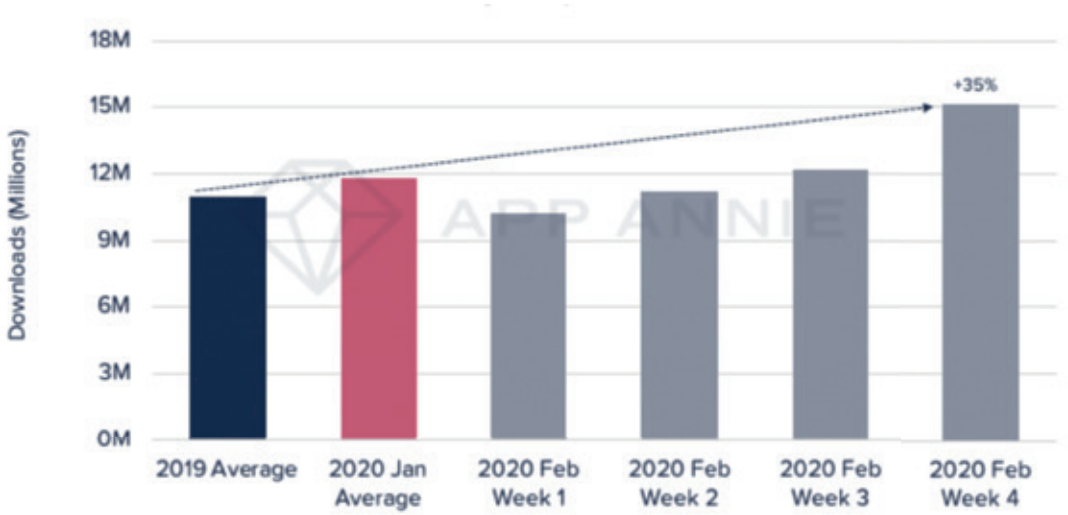
Amerika Birleşik Devletleri'nde Covid-19 virüsünün ortaya çıkmasıyla birlikte İnternet kullanımında %17 artışın olduğu görülmüştür. Aynı zamanda eğitim içerikli sitelere ziyaretin sadece 4 hafta içinde %400 arttığı tespit edilmiştir. Salgının ilk dalgasını gören Çin'de ise insanlar bilgi araştırmak, çalışmalarına devam etmek, eğlenmek, çevresiyle iletişim kurmak ve normal hayatın boşluklarını doldurmak için mobil ortama yöneldiği ve bu ortamda geçirilen günlük sürenin 2019 ortalamasına göre %30 artarak günde ortalama 5 saate çıktığı görülmüştür. Salgının görüldüğü diğer bazı ülkelerde de artış yaşandığı tespit edilmiştir. (Görsel 1)



Görsel 1

İnsanlar, özellikle işlerini ve eğitimlerini sürdürmek zorundaydılar. Bunun için evden iş ve evden eğitim sistemine geçildi. Çin'de şehirlerin kapatılmasının, evden iş ve sosyal mesafe politikalarının uygulanmasının ardından, iş ve

eğitim uygulamalarının indirildiği ve bu uygulamalarda harcanan saatlerin büyük oranda arttığı görülmüştür. Şubat 2020'nin ilk yarısında, iş ve eğitim uygulamaları 2019'daki haftalık indirme ortalamasına göre yaklaşık 2 kat artmıştır. En fazla vakanın görüldüğü İtalya'da ise kısıtlamaların getirildiği mart ayının ilk haftasında, Apple Store ve Google Play genelinde iş ile ilgili 761.000 uygulama indirilmişti ve bu bir önceki haftaya göre %85 artış demekti. (Görsel 2)



Görsel 2

Kullanıcılar karantinadayken eğlenmek ve vakit geçirmek için mobil cihazlara yöneldikçe, oyun indirmelerinde de güçlü bir artış olmuştur. Çin'de Şubat 2020'de iOS App Store'da ortalama 63 Milyon oyun indirilmiş, 2019'un tüm haftalık oyun indirme ortalamasına kıyasla %80 artmıştır. Salgının yüksek görüldüğü bir diğer yer olan Güney Kore'de ise, 3 Şubat 2020 tarihindeki haftada 15 milyon oyun indirmeleri ile 2019'un tüm haftalık ortalamasını, %35 artış oranıyla geçmiştir. (Görsel 3)

Görsel 3

İnsanlar, önlemler sebebiyle alışveriş ihtiyaçlarını mağazalara giderek değil, online olarak İnternet üzerinden yapmak zorunda kalmıştı. Pandemi öncesinde de çok sık kullanılan online alışveriş platformları pandemi süreciyle birlikte daha çok kullanılmaya başlanmıştı. Bir ailenin haftada bir kez yapmış olduğu market alışverişi sayısı artık birden fazla olmaya başlamıştı. Aslında birden fazla olmasının sebebi ihtiyaçtan çok rahatlıkla bir market uygulamasına girmek ve yorulmadan, zaman harcamadan sipariş verme psikolojisi idi. Bu gibi durumların sebebi sonucuyla; Türkiye'de ilk vakanın görüldüğü 11 Mart'tan itibaren İnternet üzerinden yapılan alışverişlerde %200'lere kadar bir artış olduğu görülmüştür.

Genel olarak iş, eğitim, alışveriş, bankacılık, kurumsallık, iletişim, bilgi edinme, eğlence vb. gibi faaliyetlerin daha da çok gerçekleştiği ortak nokta olan İnternet dünyası, siber saldırganlar için fırsata çevrilebilecek bir pazar haline gelmiştir. Bu aktiviteleri gerçekleştirirken son kullanıcı için güvenlik zafiyetleri daha da çok ön plana çıkmıştır.

Sanal alemin artık bilginin asıl saklandığı depolar haline geldiğini söylemek kaçınılmazdır. Bilişim çağından önce bilgiler kasalar vb. gibi yerlerde muhafaza edilirken günümüzde ise sanal ortamlarda saklanmaktadır. Bu bilgiler kötü niyetli kişiler için altın değerindedir. Bu bilgilere daha rahat ulaşmak isteyen siber saldırganlar en uygun çevre koşullarını değerlendirirler. Covid-19 salgın süreci de bu koşullara gayet uygundur.

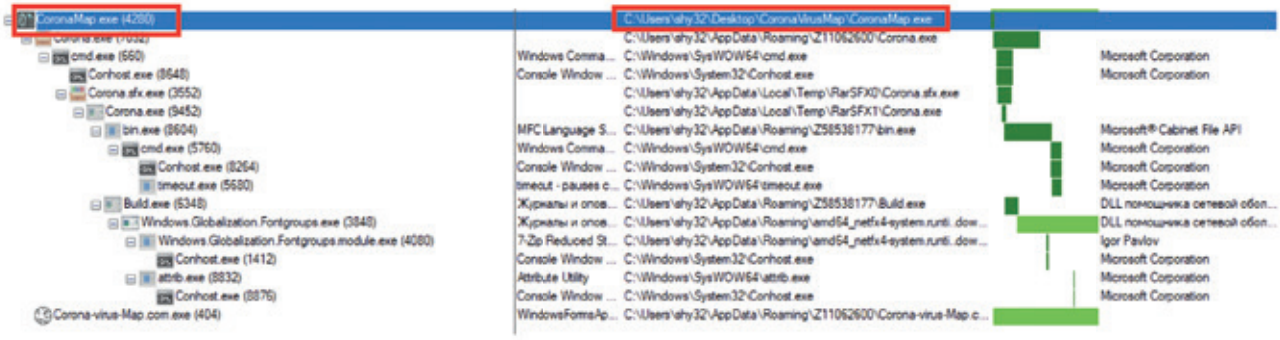
Bilişim uzmanları, Covid-19 pandemi sürecinde siber saldırıların giderek daha da fazla arttığını söylemektedirler. Covid-19 salgınının başladığı şubat ayından itibaren siber saldırılarda %40'lara varan oranda artışın olduğu görülmüştür. Bununla birlikte online kanallara yönelik saldırıların ise 2 katına çıktığı gözlemlenmiştir.

Covid-19 salgını boyunca siber saldırganlar, kullanıcıların bilgilerine sızmak amacıyla hem bazı zafiyetleri kullanmak hem de ön bilgiler toplamak için sosyal mühendislik tekniklerini kullanmaktadırlar.

Google, salgın sürecinde günlük 18 milyon kötü amaçlı e-postayı engellediğini açıklamıştır. Bu durum siber saldırganların bu yönde ne kadar aktif olduğunu vahim bir durum olarak göstermektedir. Örnek vermek gerekirse; Japonya'da bir hacker grubu, "yüz maskeleri ve korunma yöntemleri" ile ilgili kullanıcıların mail içeriğindeki iletiyi okumasını ve ekleri açmasına yönelik bir mail yaymıştır. Ek açıldığında ***"Emotet"*** isimli bir zararlının devreye girip kullanıcının banka hesapları ve değerli bilgilerini çaldığı, aynı zamanda bu virüsün bulaştığı cihazı başka cihazlara karşı saldırı makinası olarak da kullandığı görülmüştür. Bu olayda da görüldüğü gibi siber saldırganlar pandemi dönemini fırsata çevirmeyi kaçırmamışlardır. Sosyal mühendisliğin bir türü olan oltalama (Phishing) yöntemi ile insanların endişe ve korku gibi psikolojik durumlarından faydalanıp oluşturdukları zararlı içerikleri mail olarak göndermişlerdir. Siber saldırganlar, "Covid-19 salgın araştırması", "bu küçük önlem sizi kurtarabilir", "güvenlik önlemlerini indirmek için aşağıdaki linke tıkla", "şimdi satın alın, sınırlı tedarik" gibi ifadeler içeren Covid-19 salgını ile ilgili bir seferde 150.000'den fazla mail göndermiştir.

Mail'lerin içeriğine bakıldığı zaman genellikle resmi kurumlardan gelmiş gibi, uzmanından tıbbi yardım öneren, isminde Covid terimi bulunan exe, pdf, doc gibi uzantılara sahip eklerin indirilmesi, oluşturulan sahte sitelere yönlendirilen linklere girilerek kullanıcıların kişisel bilgilerinin girilmesi istenilmiştir. Endişe ve korkunun verdiği aciliyet duygusuyla bu mailleri açan, linklere tıklayan ve formları dolduran binlerce kişi, cihazlarının rehin alındığını, önemli belgelerinin kilitlendiğini, bunların sonucunda para talepleriyle karşı karşıya kaldıklarını belirtmişlerdir.

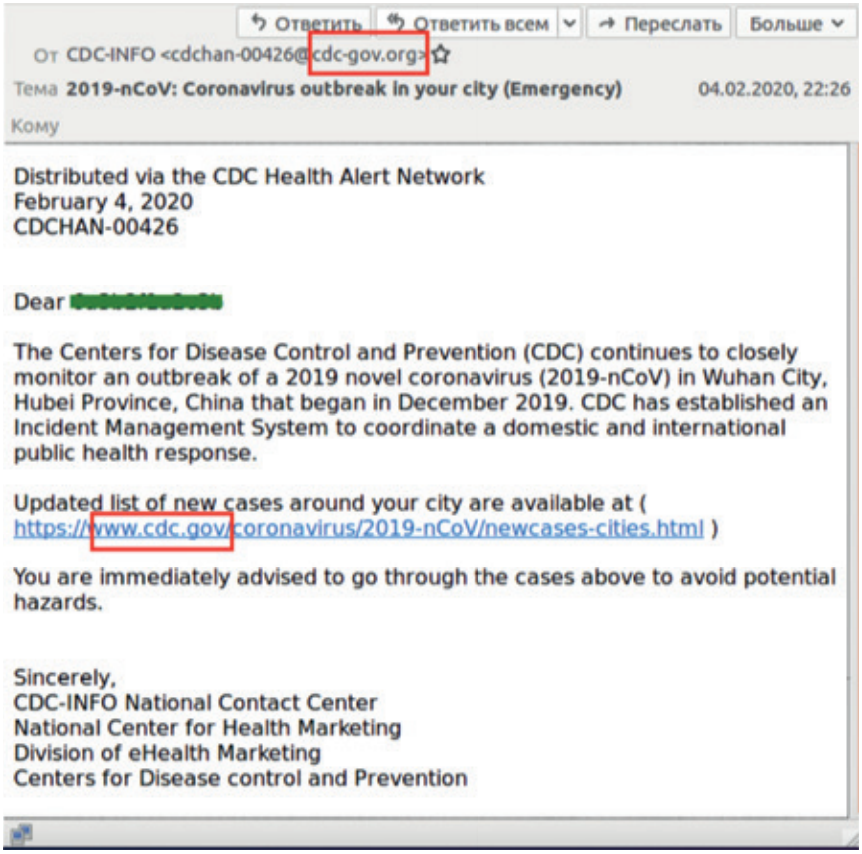
Gerçekleştirilen bu gibi Kimlik Avı saldırılarının başarılı olmasının en büyük iki nedeni merak ve korku duygusudur. Dünyanın dört bir yanındaki bu zor günlerden yararlanmak isteyen siber saldırganlar, insanlar üzerinde etkisi olan bu iki duyguyu kolaylıkla istismar edebiliyorlardı. Bir örnekle açıklamak gerekirse; Görsel 4'te Amerika Birleşik Devletleri'ndeki Hastalık Kontrol ve Önleme Merkezi tarafından gönderilmiş gibi görünen ve koronavirüs hakkında bilgiler veren bir sahte e-posta görülmektedir. Gönderilen e-posta dikkatlice incelendiğinde, gönderenin alan adresinin "cdc-gov.org" olduğu ve bu kuruluşun orijinal adresi ile karşılaştırılarak gerçek bir adresten geldiği izlenimi verilmek istenmiştir. Ancak Hastalık ve Kontrol merkezinin gerçek adresi "cdc.gov"dur. sahte olanda yalnızca tek fark "-" tire'dir. Dikkatli olmayan bir kullanıcı farkı gözden kaçırabilir. E-posta içeriğinde belirtilen linke tıklayan kullanıcılar açılan web sitesindeki formlara kişisel bilgilerini girerek dolandırılmaktadırlar.



Görsel 4

Her daim elimizin altında bulunan akıllı telefonlarımız ile en güncel anlık iletişim bildirimleri almamız mümkün. Özellikle WhatsApp, SMS gibi anlık iletişimin kullanıldığı bu platformlarda siber saldırganlar tarafından oltalama yöntemi rahatlıkla kullanılabiliyor. Kullanıcıların akıllı cihazlarına gönderilen Covid-19 ile ilgili içeriğe sahip mesajlarda, belirtilen sahte web sitelerine yönlendiren linklere tıklandığında kullanıcıların özel bilgileri çalınmış oluyor.

Kullanıcıların telefonlarına Birleşik Krallık Hükümeti tarafından geldiği süsü verilen bir mesajda, insanlara yardım vaadinde bulunan mesaj içinde belirtilen linke girildiğinde açılan sayfada banka kartı bilgileri istendiği görülmüştür. (Görsel 5)



Görsel 5

Siber saldırganlar kullanıcıların bankacılık sistemlerine yönelik saldırılarını pandemi sürecinde daha da artırmışlardır. Bir telefona giren bankacılık Truva Atı virüsleri çoğu zaman SMS mesajlarına erişim sağlamaya çalışır. Bunun amacı bankalardan gelen tek seferlik doğrulama kodlarını öğrenmektir. Kötü amaçlı yazılım sahipleri bu kodla, kurban hiçbir şeyin farkına varmadan ödeme yapabilir veya fonları boşaltabilir. İspanya'da finansal bilgileri çalmak

için kullanıldığı tespit edilen "Ginp Trojan" isimli virüs ile tuzağa düşen Android kullanıcılarına özel bir komut gönderiliyor ve mobil tarayıcısında bir web sayfayı ziyaret etmeleri sağlanıyor. "Coronavirus Finder" adını taşıyan sayfa, kullanıcılara bulundukları bölgede Covid-19 teşhisi konmuş vakaları göstereceğini iddia ediyor. Uygulama sosyal mühendislik yöntemleri ile kullanıcının bulunduğu bölgede kaç Covid-19 vakası bulunduğunu hesaplıyor ve karşılığında 0.75 Euro ödenmesini istiyor. Güvenlik araştırmacıları, Ginp Trojan'ın finansal verileri çalabilmek için kullanıcıları farklı şekillerde kandırmaya çalıştığını, harita uygulamasında ise web tabanlı yeni bir yöntem ile öne çıktığını ifade ediyor. Kandırılan kullanıcılar kredi kartı bilgilerini girdikten sonra söz konusu veriler direkt siber suçluların eline geçiyor. Kredi kartının kontrolünü ele geçiren siber suçlular 0.75 Euro ödemeyi alma gereği bile duymuyor ve kullanıcıya hiçbir bilgi sunulmuyor.

Kullanıcılar, "Coronavirüs Taşıyıcı Haritası", "coronaharitasi", "coronaharitasicanlı" gibi anlık vaka sayılarını öğrenmeyi amaçlayan terimleri arama motorlarında aratarak karşılarına çıkan "Google Play'de İndir" linklerine tıkladığında Google Play'e yönlendirildiği belirten ancak siber saldırganların oluşturdukları site üzerinden sahte bir uygulamayı cihazınıza indirmiş oluyor. İnen bu uygulama kullanıcılardan çeşitli yetkiler talep ediyor. Bu yetkilerin içinde ekran görüntüsünün iletilmesi izni de var. Sahte uygulama, bir uyarı mekanizması da içeriyor. Kullanıcı, bir bankacılık uygulamasına girdiğinde veya kredi kartı ile işlem yapmaya kalkıştığında ***"Cerberus"*** olarak adlandırılan, bu uygulamaların içinde saklanan casus yazılımı, siber saldırgana finansal bir hareket olduğuna dair uyarı iletiyor. Siber saldırgan, finansal işlem yapan kişi ile aynı anda harekete geçip ekran görüntüsü alabildiği için telefona gelen doğrulama SMS mesajını görerek kullanıcıdan önce finansal işlemi kendisine yönlendiriyor. Ulusal Dolandırıcılık İstihbarat Bürosu, Salgının ilk dönemlerinde kullanıcıların toplamda 800.000 £'dan fazla para çaldırdığını söylüyor.

Tespit edilen ve önemli olarak görülen bazı zararlı mobil uygulamalar aşağıda tablo ile verilmiştir. (Görsel 6)

Covid Tracker	8e28ae16f571101f4029a04e3d10b759e32023dc8cee2076836051538dfef6a5
V-Alert COVID-19	b1323c8e514a255b7f61c544ecdfe4cc9fff2eee922131c50ce9af7c7b95d892
V-Alert COVID-19	f092a594f615678099a25c28f7abfd8d95749abdcec83e43d1306ecb066ef3dc
Covid 19 Tracker	19b331b79cdd95a13b68ab5e8b4eb69102878fce1c81071cb7c17cbc24900c15
Covid-19 Tracker	19b331b79cdd95a13b68ab5e8b4eb69102878fce1c81071cb7c17cbc24900c15
Corona Safety Mask	d7d43c0bf6d4828f1545017f34b5b54c
Corona Takip	b7070a1fa932fe1cc8198e89e3a799f3 64ebe4ecfb242019ee590d80740e6a46

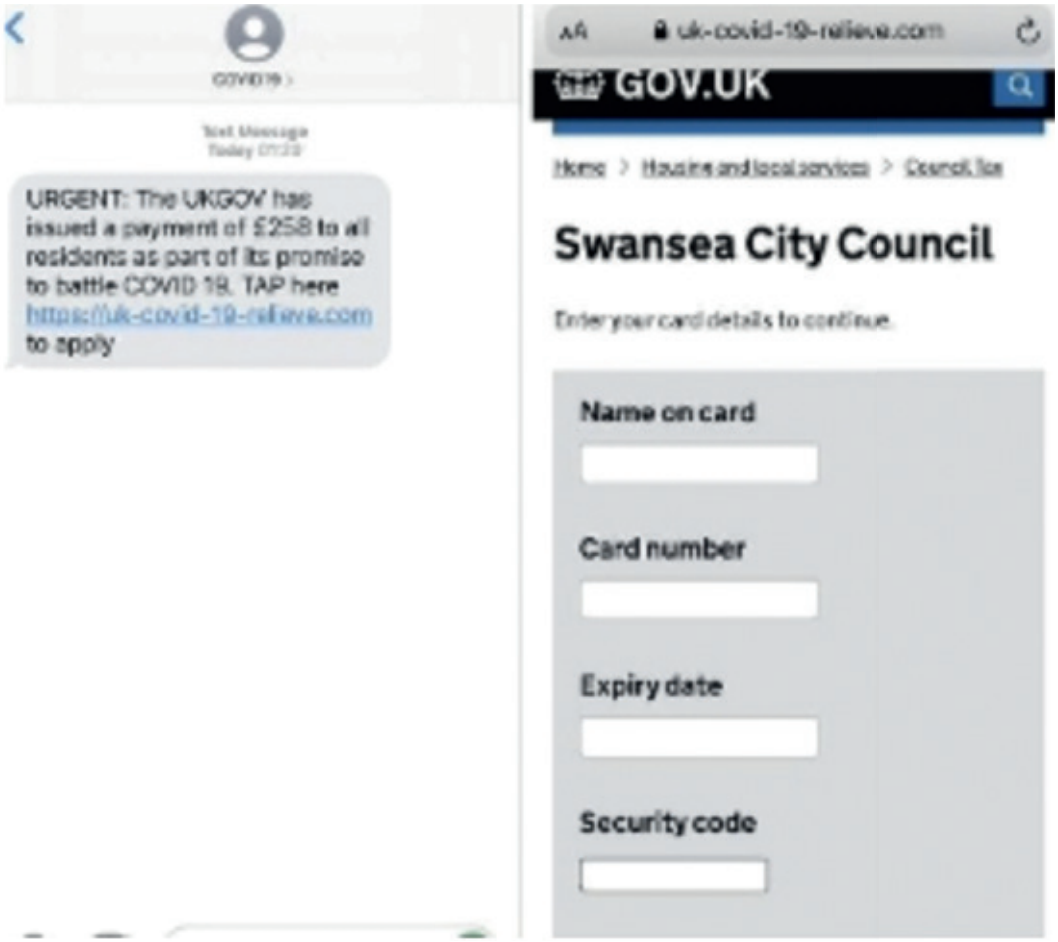
Görsel 6

Emniyet Genel Müdürlüğü vatandaşları bu konuda uyarmak için Siber Suçlarla Mücadele Daire Başkanlığı'nın Twitter hesabından, "Telefonunuza gelebilecek 'Aşı Randevu Oluşturma' mesajlarına veya sizi arayıp 'Sağlık Bakanlığı'ndan arıyoruz, aşıda önceliklisiniz, size kayıt oluşturalım' diyerek kişisel bilgilerinizi isteyenlere itibar etmeyiniz. Bu kişilerin amacı oltalama yoluyla dolandırıcılıktır" ifadelerinin bulunduğu açıklamasını yaparak durumun öneminden bahsetmiştir.

2005 yılındaki Katrina kasırgası ABD'de büyük yıkımlara yol açmıştı. Bu durumu fırsat bilen siber saldırganlar ger-

çeğiyle aynı, inandırıcılığı yüksek mağdur insanlar için bağış toplama amaçlı web siteleri oluşturmuş ve kullanıcıların bu sitelere girip önemli bilgilerini paylaşmalarını sağlamışlardı. Ve bunun sonucunda insanlar dolandırılmıştı. Benzer dolandırıcılık 2016'da Japonya ve Ekvator depremlerinde, 2017'de Harvey kasırgasında, 2020'de Avustralya sel felaketinde, şimdi de Covid-19 salgınında görüldü.

Covid-19 sürecinde insanlar bilgi almak için İnternet ortamında çeşitli araştırmalar yapıp çeşitli sitelere giriyorlardı. Tam da bu noktada bu durumu fırsata çevirmek isteyen siber saldırganlar Covid-19 salgın sürecini anımsatacak coronavirus, corona, covid, covid19 gibi kelimelerin bulunduğu domain'ler (web sitesi adları) kullanarak Covid-19 salgını ile ilgili bilgiler veren, etkinliklerde bulunan, yardım sağlayan ancak asıl amacı "Kimlik Hırsızlığı" yaparak kullanıcıların önemli bilgilerini ele geçirmek olan web siteleri oluşturmuşlardır. Yapılan araştırmalara göre 11 Şubat 2020 tarihinde Dünya Sağlık Örgütü tarafından salgının adının "Covid-19" olarak belirtilmesinden sonra Covid-19 ile ilgili alan adı kayıtlarının arttığı, mart ayında ise zirveyi bulduğu görülmüştür. Aynı zamanda Ocak'tan Nisan'a kadar olan süre zarfında Covid-19 ile ilgili 907.000 kötü amaçlı URL tespit edilmiştir. Bu alan adlarının artışı ve salgın ile ilgili tespit edilen zararlı URL'lerin olması siber saldırganların bir hayli sabırsız olduklarını göstermektedir.



Görsel 7. Gerçekleştirilen alan adı kayıt işlemleri sırasında; coronavirus, corona, covid, covid19 kelimelerinin alan adı içerisinde daha çok tercih edildiğini gösteren grafik.

İnsanlar, bankacılık, alışveriş, çeşitli etkinlikler ile ilgili işlemlerini yapmak için siteleri ziyaret edip bilgilerini girmektedir. Bu durum salgın döneminde daha çok olmuştur. Covid-19 salgını sırasında insanların %48'inin web sitelere kişisel bilgilerini verdiği, %13.40'ının ise vermediği görülmüştür. %40.20'nin ise muamma da kaldığı görülmüştür. Ayrıca web sitelere bilgilerini veren bazı kullanıcılar siber saldırıya uğradıklarını da ifade etmiştir.

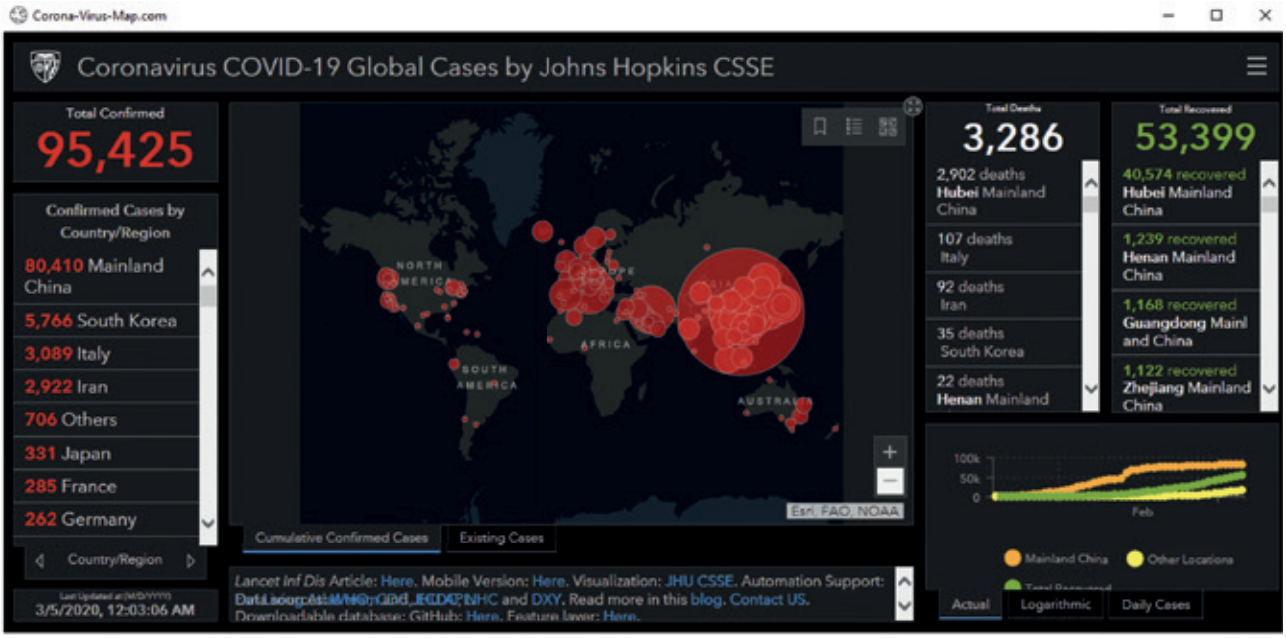
Siber saldırganlar, oluşturdukları sahte web sitelerine kullanıcıları çekerek çeşitli formları doldurmalarını, pdf, exe, doc, jpeg vb. gibi uzantılı dosyaları cihazlarına indirmelerini sağlamaktadırlar. Bunların yanı sıra kullanıcıların haberi olmadan sistemlerine bulaştırdıkları sahte web siteleri içerisinde gömülü zararlı yazılımların da olduğu bilinmektedir.

Siber saldırganlar, ABD Hastalık Kontrol Merkezini taklit ederek oluşturdukları siteler üzerinden Bitcoin bağışları istemiş, bu sahte siteler üzerinden henüz ortada resmi olarak bulunmayan aşı satışı gibi hizmetler bile sunup insanları dolandırmışlardır. Saldırganlar, Türkiye'de Sağlık Bakanlığına ait "Aşıla" uygulamasının web sitesini taklit ederek, kullanıcıların sahte web sitesine girmelerini ve cihazlarına truva atı virüsünü yüklemelerini sağlayarak bankacılık başta olmak üzere finansal bilgilerini ele geçirmeyi amaçlamışlardır.

Türkiyede "Evdekal 8, 10 ya da 20 GB İnternet Hediye" gibi duyurularla, herkesçe bilinen iletişim kurumlarının amblemleri kullanılarak sahte İnternet siteleri açılmış, bu sitelere giren kullanıcılar "Hediye İçin Tıklayın" yazılı linklere gittiklerinde kullanmış oldukları cihazları siber saldırganlara emanet etmiş oldular.

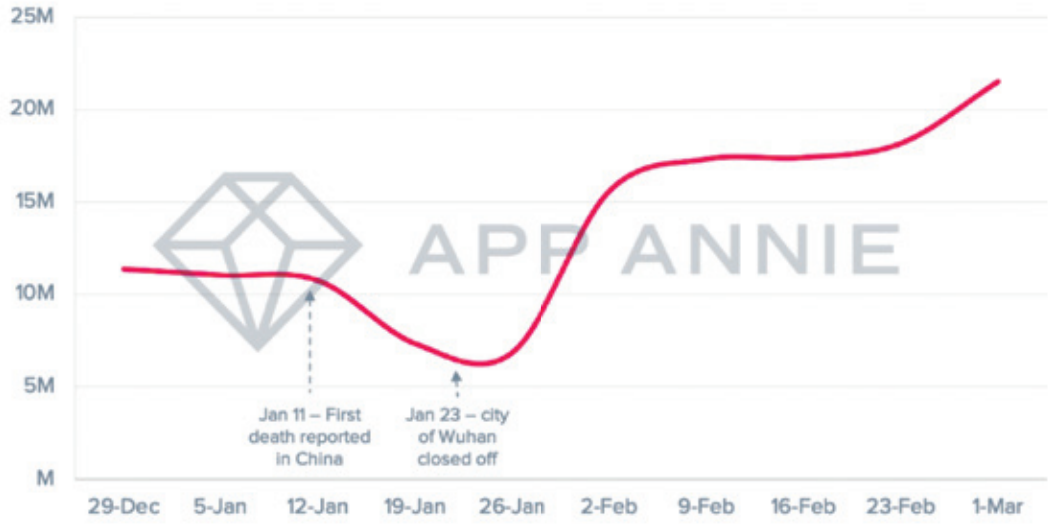
Özellikle, Siber korsanlar tarafından oluşturulan Covid-19 ile ilgili finansal yardım temalı sahte sitelerde ***"Trickbot"*** isimli zararlı yazılım, salgın yayılım haritalarını gösteren sahte sitelerde ise ***"AZORults"*** isimli zararlı yazılım site kodlarının içine gömülerek kullanıcıların haberi olmadan onların sistemleri sömürülmektedir.

Siber korsanlar, kullanıcıların; parolalarını, kredi kartı bilgilerini, İnternet tarayıcılarındaki verilerini toplamak için hastalığın yayılımını gösteren, gayet zararsız gibi görünen, bilgi verici bir havası olan Corona-Virus-Map.com isminde web sitesi oluşturmuşlardır. Oluşturulan bu web sitesinde gayet göze hoş gelen bir arayüzün tasarlanması, kullanıcıların arka planda gizli bir halde bulunan, kullanıcı bilgilerini çoktan çalmaya başlamış olan zararlı yazılımların varlığından bihaber olmalarını sebep oluyordu. (Görsel 8)



Görsel 8

Bu sitenin zararlı yazılım analizi yapıldığında, site içerisinde gizli bulunan, özellikle exe uzantılı dosyaların, kullanıcının bilgisayarlarına gizlice yüklendiği tespit edilmiştir. Görsel 9'daki incelemeye bakıldığında kullanıcının sistemine CoronaMap.exe, Corona.exe isimli virüslerin asıl yerleştirilip kullanıcıları sömürmeye hazılandığı açık bir şekilde görülmektedir.



Görsel 9

Siber korsanlar salgın döneminde insanların verilerinin daha fazla bulunabileceği sağlık kuruluşlarının sistemlerine yönelik de saldırılarını artırmışlardır. Bu kurumlardan yüksek miktarlı gelir elde etme amacıyla bir dönem, dünyanın bir çok yerinde gündeme gelen ***"WannaCry"*** isimli fidye virüsü ve farklı türdeki zararlı yazılımlar ile karşı tarafın sistemlerine sızılıp hastalara ait bilgiler ele geçirilmek istenmiştir.

İş kurumlarının evden çalışma sistemine geçmesiyle birlikte ev ortamından iş kurumlarının sunucularına uzaktan bağlantı ile insanlar çalışmalarını sürdürmek zorunda kalmıştır. Evde çalışan kullanıcıların almadığı güvenlik tedbirleri sonucunda; çalışana atılan zararlı bir mail'e tıklanması, sistemlerin ve sık kullanılan uygulamaların güncellenmemesi, evdeyim rahatlığıyla girilen basit parolalar ve benzeri aktiviteler gibi sebepler sonucunda iş kurumları saldırılara bir hayli maruz kalmıştır. Dolayısıyla kurumların sisteminde bulunan kişilere ait özel veriler çalınarak dolaylı yoldan son kullanıcılar da mağdur edilmiştir.

Makalede bahsedilen bu konuları genel olarak ele alarak, siber saldırganlar tarafından ele geçirilen bu veriler ile neler yapıldığına birkaç örnek vermek gerekirse; siber saldırganlar özel verilerinizi İnternet ortamında yaymakla sizi tehdit edip para talep edebilir, özel verilerinizden hedefli saldırılar için ulaşılmak istenen başka kişilerin bilgilerine ulaşabilir, bu veriler ile size daha sonrasında sosyal mühendislik yöntemleri kullanarak bir telefon görüşmesi ile bilgilerinizi yüzünüze karşı okuyup polis, jandarma, sağlık kurumu gibi resmi kurumdan arıyormuş imajı verip sizden para talep edebilir. Sadece bunlarla kısıtlı olmayan siber saldırganların arzuları gün geçtikçe daha da çeşitlenmektedir.

Savaş Sanatı kitabını yazan filozof Sun Tzu'nun söylediği "Başkasını ve kendini bilirsen, yüz kere savaşsan tehlikeye düşmezsin; başkasını bilmeyip kendini bilirsen bir kazanır bir kaybedersin; ne kendini ne de başkasını bilmezsen, her savaşta tehlikedesin." sözünü belirterek değinmek isterim ki, siber saldırılara karşı savunma sağlamak için öncelikle gelebilecek tehlikeleri, saldırganların kullandığı teknikleri, kısacası siber saldırgan gibi düşünmenin son kullanıcı güvenliği açısından faydalı olacağı kanısındayım. Bu sebepten dolayı sunduğum yazımda siber saldırganların özellikle Covid-19 döneminde saldırılarında nasıl yöntemler kullandığı, neler amaçladığı, hangi hileler üzerinden son kullanıcılara ulaşmaya çalıştıkları ve son kullanıcıların bu durumlarla karşı karşıya kaldığında verdiği, verebileceği reaksiyonlar hakkında bilgi vermeye çalıştım.

Siber saldırganların saldırılarına maruz kalmamak için nelere dikkat edileceği, genel olarak son kullanıcı güvenliğinin nasıl sağlanması gerektiği hususuna değinmek gerekirse; öncelikle şunu belirtmek gerekir ki %100 güvenlik söz konusu değildir. Amaç, güvenliği yüzde olarak yüksek tutabilmektir. Ve şunu da belirtmek gerekir ki güvenlik hususunda en temel faktör insandır. Olumlu sonuçlanan siber saldırıların yüksek bir oranı, insan hatası kaynaklıdır. Bu sebeple bu yazının da amacı olduğu gibi öncelikle kullanıcıların bilinçlendirilmesi gerekmektedir. Bu gereklilik kapsamında:

Merak ettiğiniz konularla ilgili karşınıza çıkan her linke tıklamayın. Linklerdeki alan adlarına dikkat edin. Koronavirüs konulu oltalama çabalarının çok arttığı şu dönemde, cazip teklif ve yönlendirmelere karşı temkinli olun. Mesaj ya da mail yoluyla gelen linklerin muhakkak resmi kaynaklı olup olmadığını teyit edin. Örneğin bir kurum ile ilgili gelen linke tıklamadan önce arama motoru üzerinden kurumun ismini aratarak asıl sitesine girebilir, hatta mavi tikli resmi sosyal medya hesaplarına girerek hakkında kısmında belirtilen link yoluyla resmî sitelerine ulaşabilirsiniz.

Mail yoluyla gelen, özellikle indirmeye yönelik ekte sunulan dosyaları indirmeden önce temkinli davranın. İş, okul ya da farklı söz konusu durumlar neticesinde arkadaşlarınızdan gelen bu linklere tıklamadan önce arkadaşınızla iletişime geçmeniz faydalı olacaktır. Tanımadığınız kişilerden gelen teyit edemediğiniz ekleri hiç açmamanız sizin için daha faydalı olacaktır.

Güvenliğinden ve durumundan şüphe duyduğunuz online formlara asla hassas bilgilerinizi girmeyin.

Unutmayın, güncellemeler, programlara görsel nitelikten başka güvenlik anlamında yamalar sağlar. Bu bakımdan sisteminizin, kullandığınız programların güncel olmasına özen gösterin.

En basitinden parolalarınızı kimseyle paylaşmayın. Ortak kullanılan cihazlarda bilgilerinizi açık tutacak şekilde bırakmayın.

Modem parolanızı paylaşmayın, modeminize yabancı kişilerin bağlanmasına izin vermeyin.

Siber saldırganların kullanmış olduğu çöp karıştırma tekniğine maruz kalmamak için üzerinde özel bilgilerinizin bulunduğu evrak gibi önemli belgeleri çöpe atmak yerine imha etmeyi unutmayın. Bu evrakları herkese açık konumda bırakmayın.

İndireceğiniz, iş, okul, eğlence gibi uygulamaları muhakkak resmi kaynağından, gerekirse ücretini ödeyerek indirin. Özellikle ücretli olup da ücretsiz indirilen programların içindeki saklı zararlı yazılımlar sisteminizi ele geçirip siber saldırganlar tarafından kontrol edilir ve başka siber saldırılar için botnet cihaz olarak kullanılır.

Google Play Store, App Store veya diğer yaygın uygulama mağazalarına bağlı kalın. Bu mağazalar, zararlı uygulamalardan tamamen arınmış olmayabilir, ancak çok daha güvenlidirler. İndireceğiniz mobil uygulamaların yayıncı/geliştiricisine, indirilme sayısına, kullanıcı yorumlarına bakarak fikir sahibi olun. Ayrıca indirilen uygulamaların izin isteklerini muhakkak gözden geçirin.

Güncel ve proaktif bir antivirüs, İnternet güvenliği ve mobil güvenlik programları kullanın.

İlgili Kaynak ve Linkler;

https://www.infosecurity-magazine.com/news/cyberattacks-up-37-over-past-month

https://www.appannie.com/en/insights/market-data/coronavirus-impact-mobile-economy/

https://lukasstefanko.com/2020/03/android-coronavirus-malware.html

https://www.researchgate.net/publication/341385611_SIBER_SUC_VE_KORONA

https://bilgiguvende.com/android-tabanli-sahte-siteden-koronavirus-haritasi-dolandiriciligi/

https://www.kaspersky.com.tr/blog/ginp-mobile-banking-trojan/7688/

https://qha.com.tr/haberler/eset-guvenlik-yazilimi-koronavirus-haritasi-zararli-yazilimlarin-hedefinde/188514/

https://www.kocsistem.com.tr/basin-bultenleri/kocsistem-ve-etidden-pandemiye-ozel-e-ticaret-sektoru-siber-guvenlik-raporu/

https://www.platinbilisim.com.tr/EN/Media/Promotions/our-information-report-about-coronavirus-phishing-attacks-is-online

https://www.swansea.gov.uk/coronavirusscam

https://www.thesslstore.com/blog/coronavirus-scams-phishing-websites-emails-target-unsuspecting-users/

https://twitter.com/SiberayEGM/status/1335864048940937219?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1335864048940937219%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.trthaber.com%2Fhaber%2Fgundem%2Femniyetten-asi-bahanesiyle-dolandiricilik-uyarisi-bilgilerinizi-vermeyin-536714.html

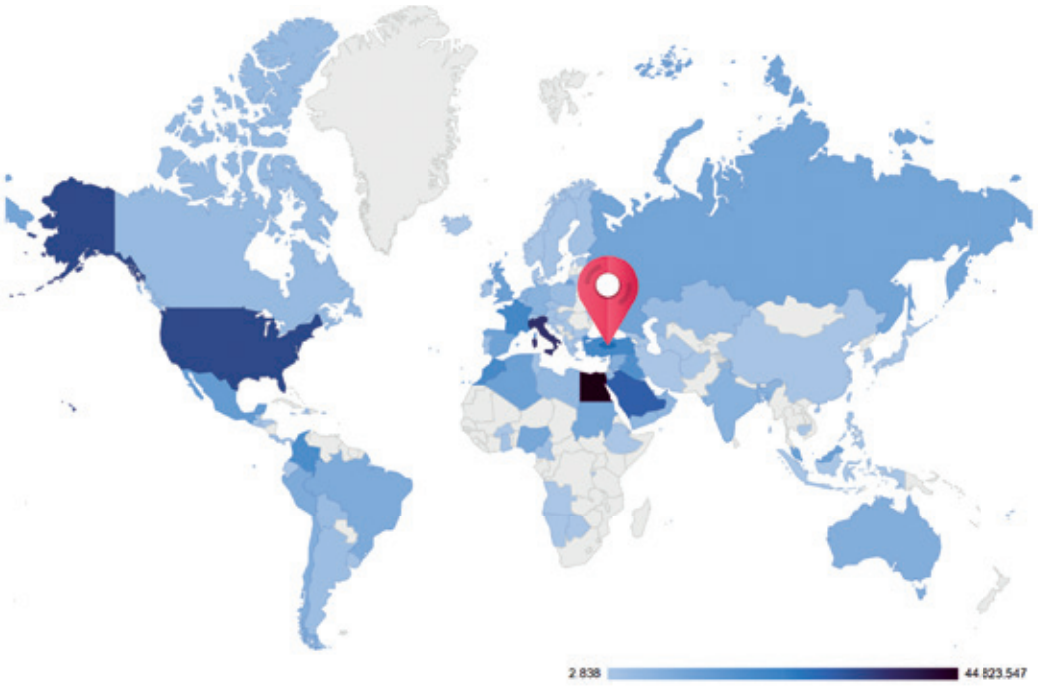
https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/

https://vizyonergenc.com/storage/posts/April2020/nzghLPD5ArgH9Uu95H5tFgP0UtIWvtEu9XWTm9ir.pdf

Intel Probe, "Dijital Coronavirus Siber Tehdit İstihbaratı İnceleme Raporu V 2.1"

Abdullah Çiçekli • abdulahcicekli@gmail.com

FACEBOOK 533M VERİ SIZINTISI ANALİZİ



Geçtiğimiz aylarda yine uluslararası bir gündem oluşturan, Facebook kullanıcı bilgilerinin sızdırıldığına dair bilgiler yayıldı. Özellikle sosyal medya ve haber kanalları aracılığı ile okuduğumuz bilgiler de kullanıcıların;

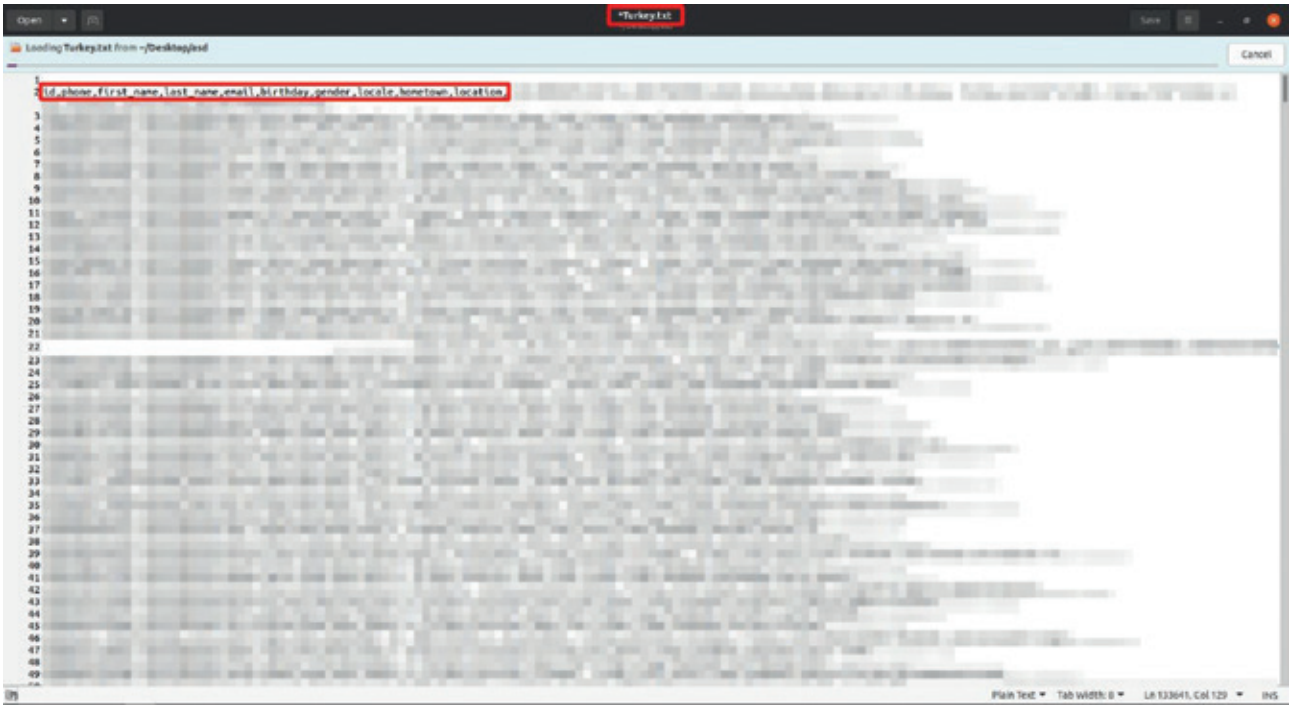
- Telefon numaraları,
- E-posta adresleri,
- Doğum tarihleri,
- Konumları ve
- Cinsiyet bilgileri

gibi kişisel verilerinin sızdırıldığı şeklindeydi. Bu bilgiler olayın duyulmasının henüz başlarında ücretli bir şekilde servis edilmeye çalışılsa da çok geçmeden tamamen ücretsiz bir şekilde yayıldı.

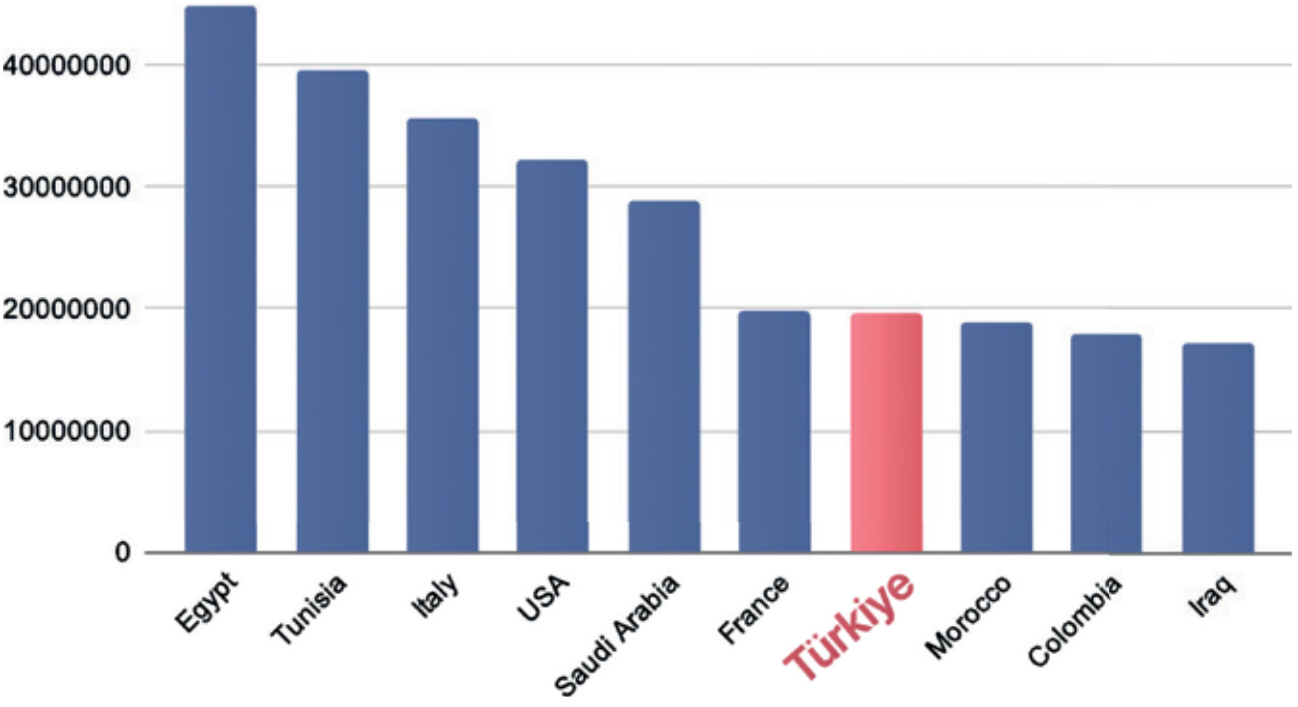
Peki nedir bu işin aslı?

Olay 2019 yılında Facebook'un bir zafiyetinden kaynaklı veri kazıma yolu ile oluşturulmuş bir veri yığınıdır. Yani bu veriler 2019 yılından beri zaten piyasada olan veriler diyebiliriz. Paylaşılan veriler içerisinde toplam 106 ülke kullanıcılarına ait 533 Milyon kayıt vardır. Nisan ayının başlarında özellikle bazı bloglarda ve mesaj grupların da verilerin ücretsiz olarak paylaşılması ile beraber olay uluslararası bir olay hale dönüşmüş oldu.

Dosyalar {ülkeismi}.txt şeklinde servis edildi. Ülkemiz için ise Turkey.txt isimli dosya mevcuttu. Turkey.txt dosyanın ham halinde sırası ile id, phone, first_name, last_name, email, birthday, gender, locale, hometown, location, link şeklinde her kullanıcı için bir satır şekilde tutulmuş düzensiz bir kayıt vardı.



Dünya listesi içerisinde toplam 533M kayıt olasa da sızdırılmış "Turkey.txt" dosyasında toplam 19.638.821 kaydın olduğunu görüyoruz. 106 ülkenin kaydı incelendiği zaman ise en çok veri bulunduran 7. ülke olduğumuz görülüyor.



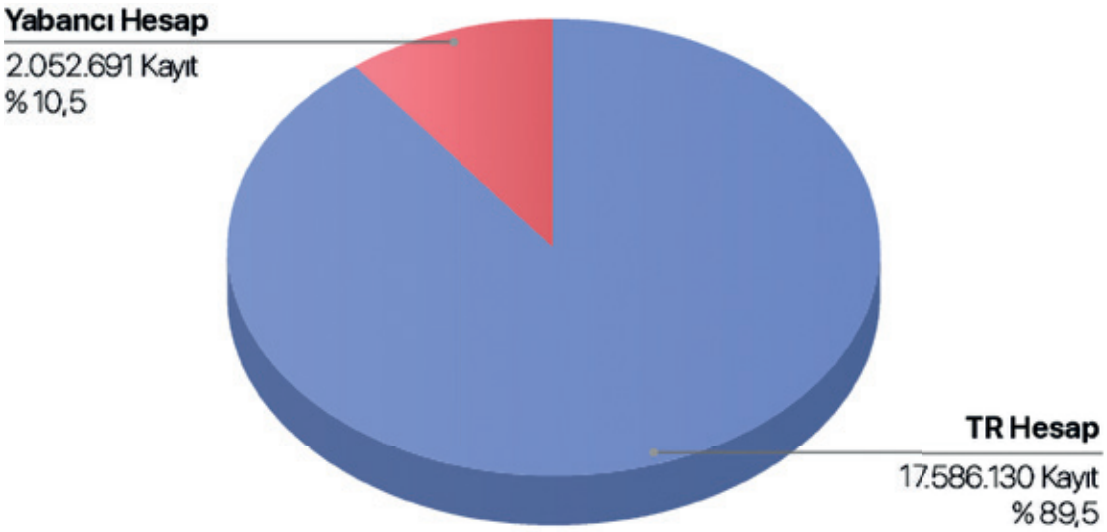
Düzensiz olan Turkey.txt dosyası için bir parser yazıp database'e aktardığımız zaman çok daha anlaşılabilir şekilde analizi gerçekleştirmiş olacağımız için bu işlemi gerçekleştirildi.

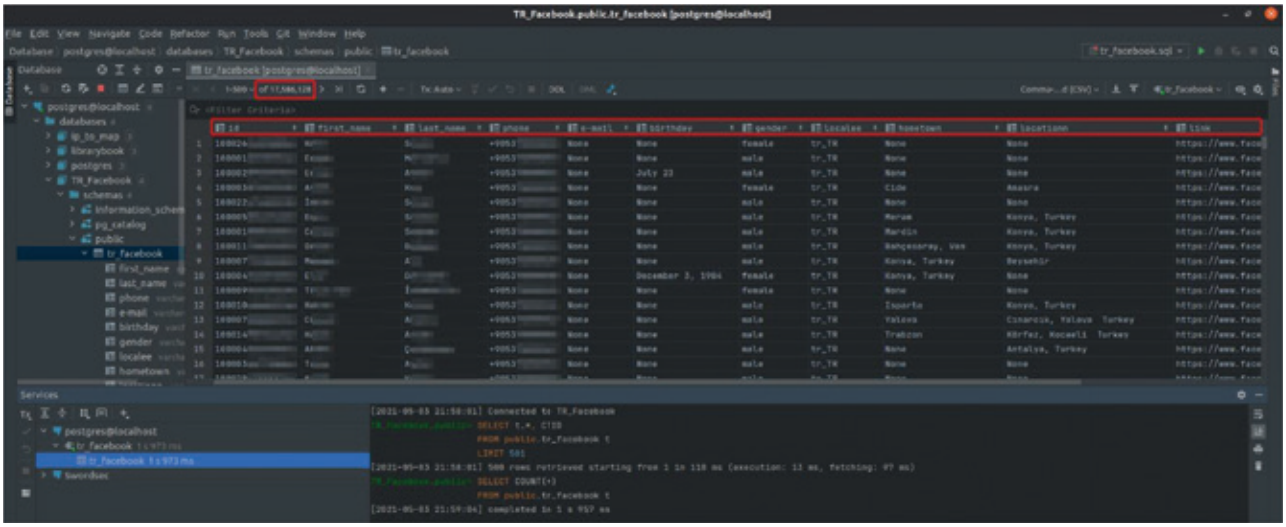
Veri Oranları

Türkiye kullanıcıları için paylaşılan "Turkey.txt" dosyası incelendiği zaman verilerin farklı yüzdeliklerde olduğunu söyleyebiliriz. Yani yazının başında sızdırıldığı söylenen bilgiler tüm kullanıcılar için geçerli değil. Bu durumu grafikler üzerinde anlatalım.

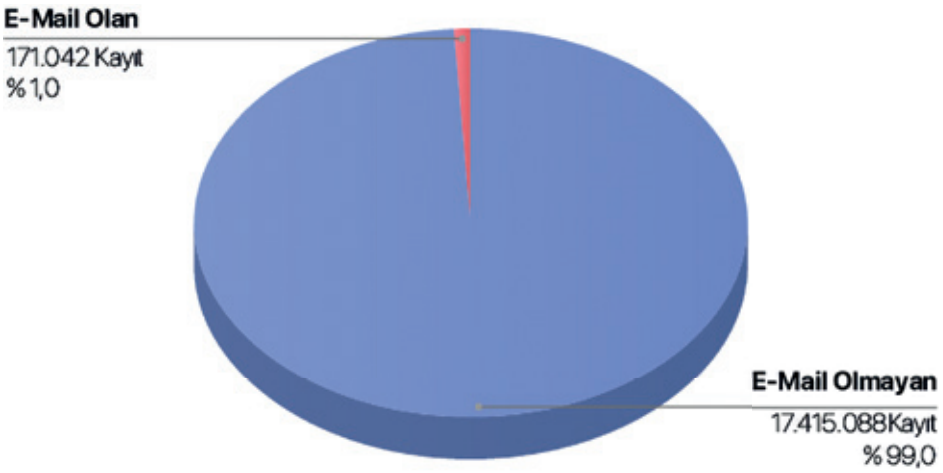
Türkiye (tr_TR) Kullanıcı Oranı

İlk olarak belirtmemiz gereken durum 19.638.821 kaydın %10,5 lik dilimini yabancı vatandaşlar oluşturuyor olmasıdır. Yani tr_TR etiketli kullanıcıların oranı %89,5 yani 17.586.130 kayıttır.

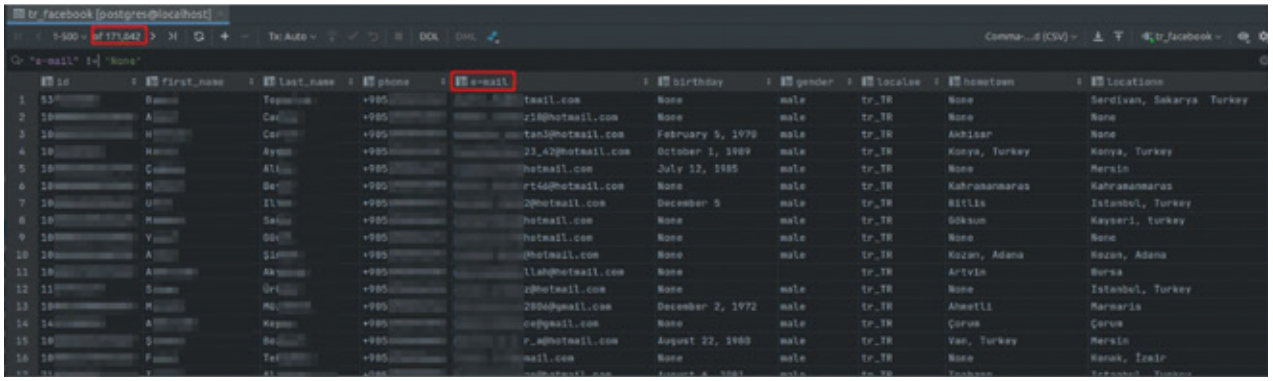




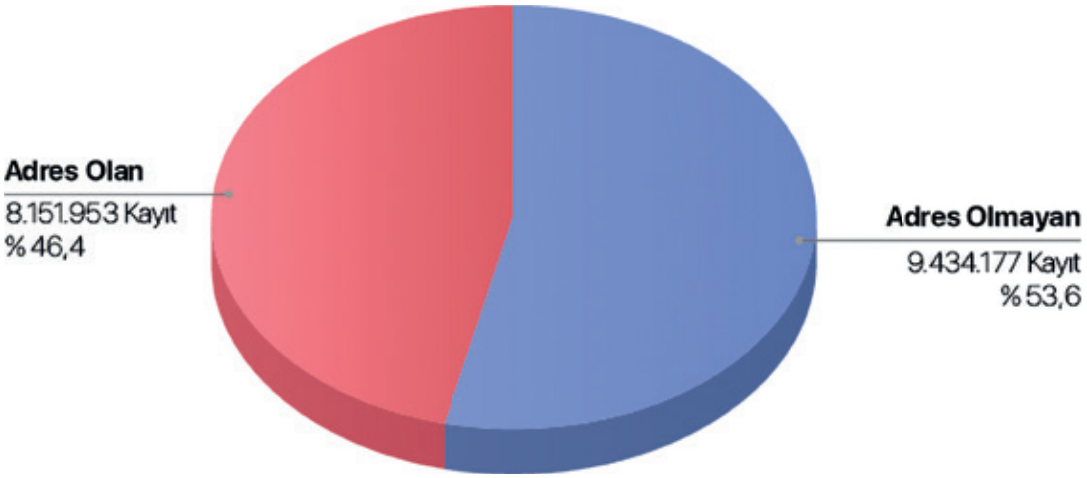
Türkiye Kullanıcılarının E-Mail Oranı



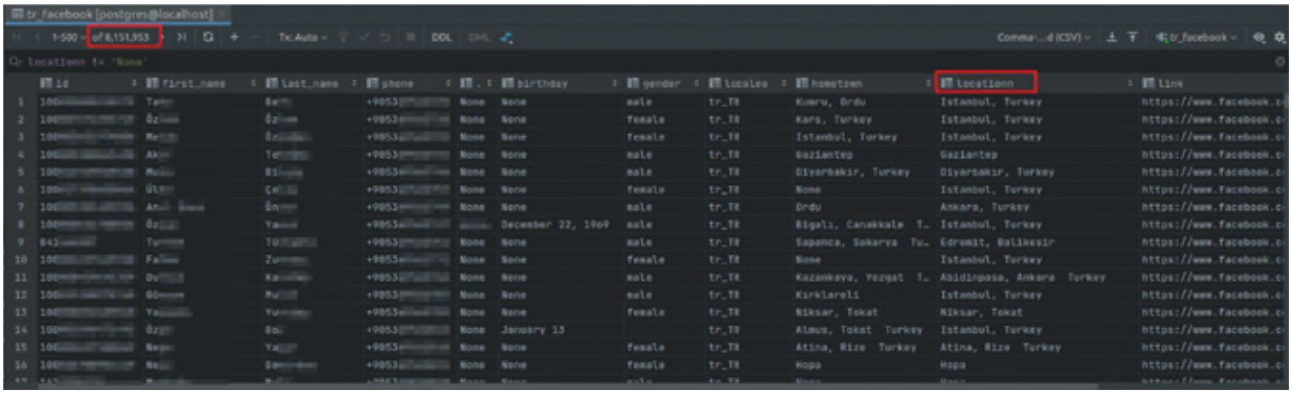
Veriler analiz edildiğinde Turkey.txt dosyasının %89,5 ini oluşturan kullanıcıların sadece %1 lik bir kısmının mail bilgilerinin olduğu gözlemlenmiştir.



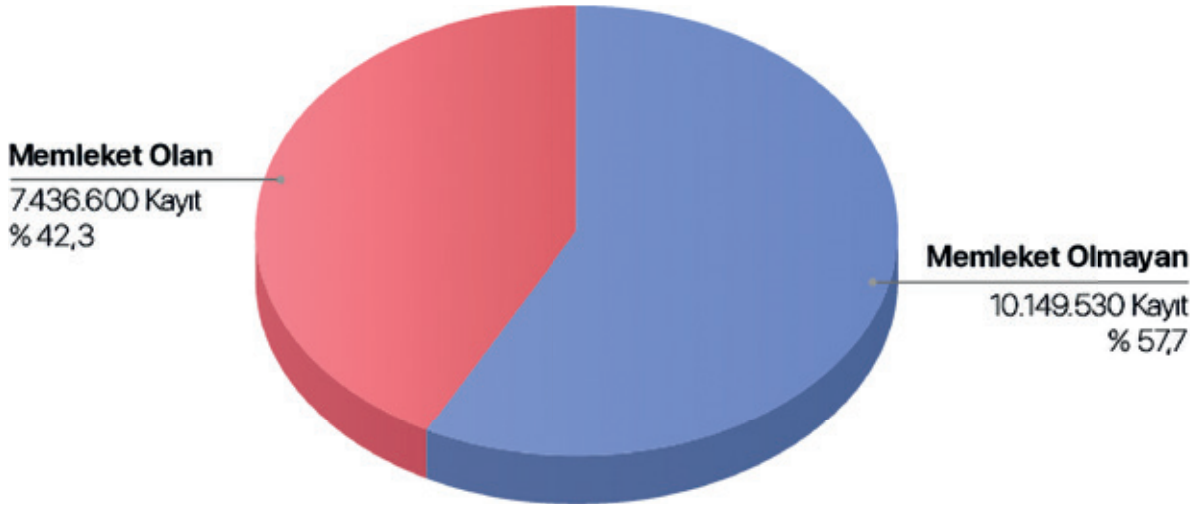
Türkiye Kullanıcılarının Adres Oranı



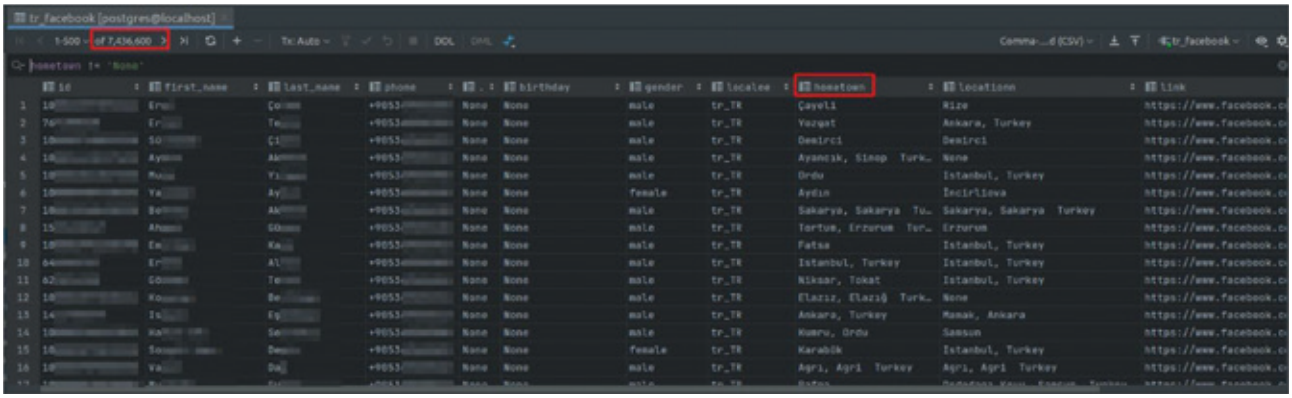
Verilerin %89,5 ini oluşturan TR kullanıcılarının %46,4 lük bir kısmının adres bilgilerinin olduğu gözlemlenmiştir. Adresler ayrıntı olmamakla beraber adres kaydı olanların geneli il ve ilçeden ibarettir.



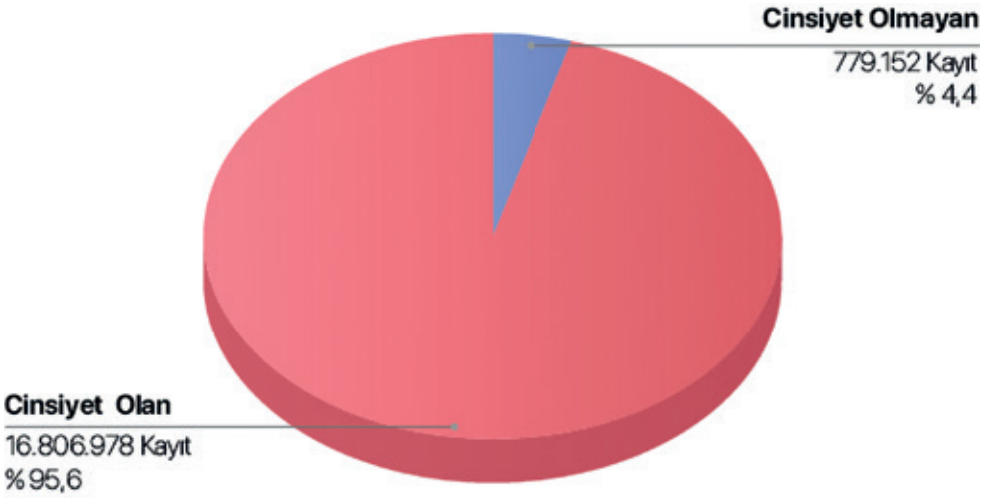
Türkiye Kullanıcılarının Memleket Bilgisi Oranı



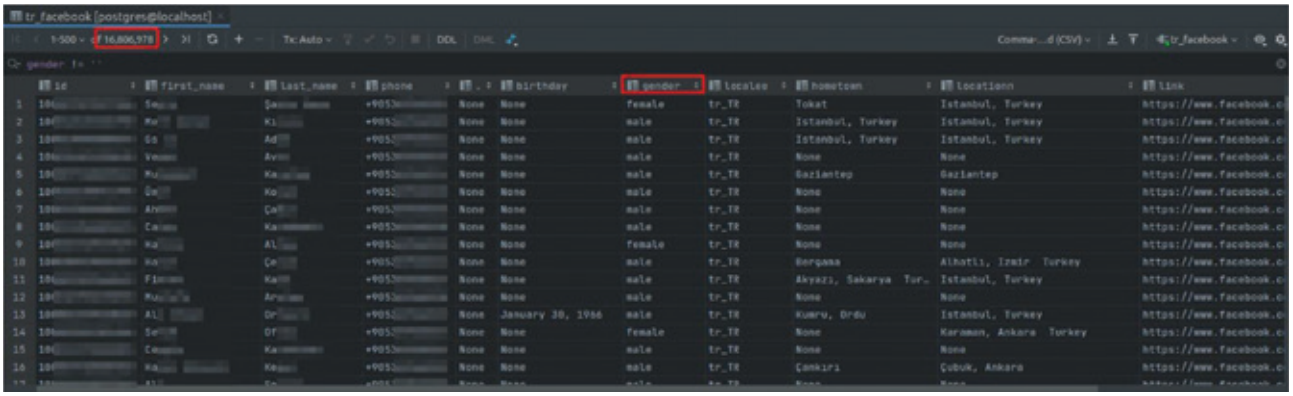
Verilerin %89,5 ini oluşturan TR kullanıcılarının %42,3 lük bir kısmının memleket bilgilerinin olduğu gözlemlenmiştir. Buda toplamda 7.436.600 kullanıcının memleket bilgisi kaydını belirtmektedir.



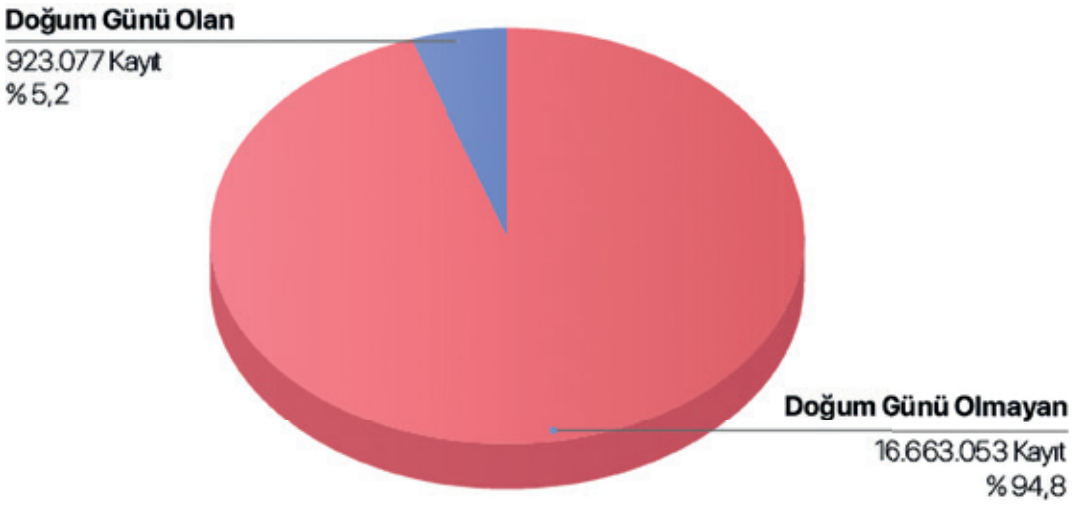
Türkiye Kullanıcılarının Cinsiyet Bilgisi Oranı

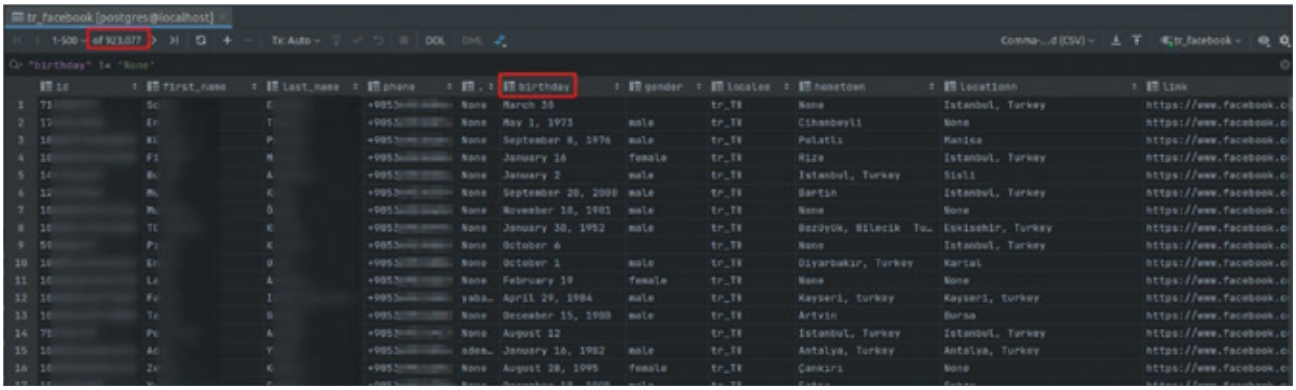


Verilerin %89,5 ini oluşturan TR kullanıcılarının sadece %4,4 lük bir kısmının cinsiyet bilgisinin olmadığı, geri kalan tüm kayıtlarda cinsiyet bilgisinin varlığı gözlemlenmiştir.



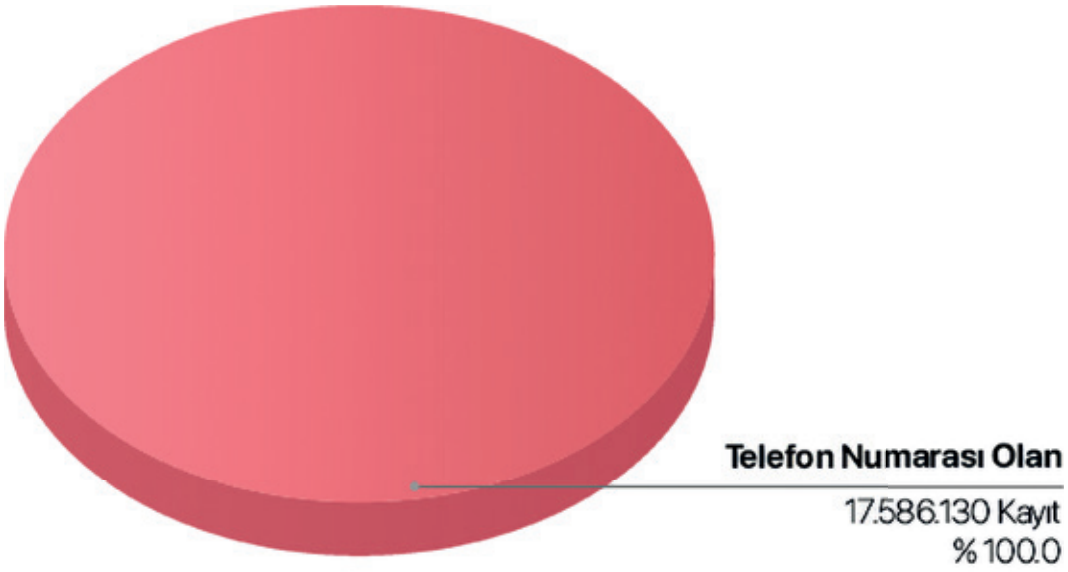
Türkiye Kullanıcılarının Doğum Günü Bilgisi Oranı



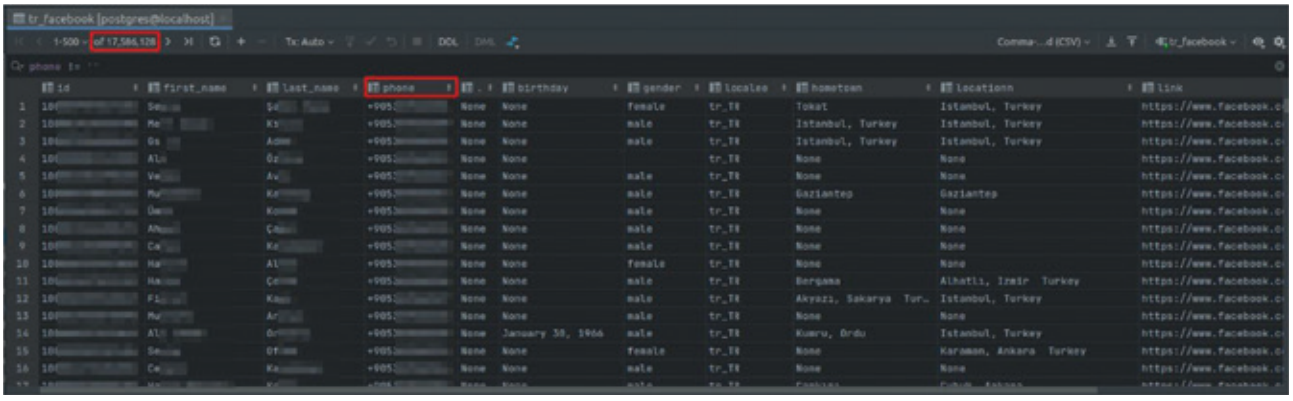


Verilerin %89,5 unu oluşturan TR kullanıcılarının sadece %5,2 lik kısmını oluşturan toplamda 923.077 kişinin ise doğum tarihinin olduğu geri kalan %94,8'lik dilimin doğum tarihlerinin dosya içerisinde yer almadığı anlaşılmıştır.

Türkiye Kullanıcılarının Telefon Numarası Bilgisi Oranı



Kayıtlar incelendiği zaman en büyük endişe uyandıran konu telefon numaraları oldu. Ne yazık ki bu konuda iyimser davanacak bir durum asla söz konusu değil. TR kullanıcıların tüm kayıtlarında telefon numarası bilgisi mevcut ve yaptığım testler sonucu neredeyse tamamının doğru bilgiler olduğunu anlaşılmıştır.



Değerlendirme

Milyonlarca insanın kişisel verileri şuan birçok platformda (web sayfaları, whatsapp grupları, telegram grupları vs..) çok kolay erişilecek bir şekilde yayılmaya devam ediyor.

Veriler incelendiği zaman yüzdelik olarak azda olsa e-posta kayıtlarının ve tüm kullanıcıların telefon numaralarının olduğunu düşünürsek spam e-postaların, aramaların, kısa mesajların uzun bir süre kullanıcıları etkileyeceğini söyleyebilirim. Bu kişisel veriler için para veren binlerce firma varken bedava veriyi bir çok kişi kullanmak isteyecektir.

Ne yazık ki problemler sadece spamla sınırlı kalmıyor. Sadece bir telefon numarası isteyen ve doğrulama gerektirmeyen binlerce hizmetin var olduğunu da hesaba katarsak telefon numaraları kötü amaçlarla da kullanılabilecek bir potansiyeldedir ve telefon numaraları verilerin sadece %1 ini oluşturan e-mail adreslerinden çok daha kıymetli verilerdir.

Kişisel verilere çok büyük rağbet olan zamanımızda, verilerimizi internet siteleri, uygulamalar gibi platformlarda paylaşırken dikkat etmeli, güvenmediğimiz sitelere asla vermemeliyiz. Kullanmamız gereken yerlerde ise sözleşmeleri dikkatli okumalı ve böyle vakaların daha önce olduğu gibi gelecektede olabileceğini düşünerek minimum düzeyde bilgimizi paylaşmalıyız. Kişisel verilerimizin önemini bilmeli ve ihlali sonucunda nasıl aksiyon alacağımızı bilmeli ve interneti çok daha bilinçli kullanmalıyız.

Oğuz Aydınyılmaz • aydinyilmazoguz@gmail.com

PRISM – NSA TÜM DÜNYAYI NEDEN VE NASIL İZLEDİ?

Merhaba, bu yazımda PRISM'in ne olduğundan ve NSA'in bunu hangi çıkarları için kullandığından bahsedeceğim.

Aşağıda detaylarından bahsedeceğimiz 7 yıl önce tüm dünyaya sızdırılan bu aracın illegal ve NSA'in veri ihlali yaptığına Amerikan Temyiz mahkemesi tarafından 2 Eylül 2020 tarihinde the Sun gazetesinde geçen habere göre karar verildiği belirtildi.[1]

Gelişmeler ne olacak ve herhangi bir cezai durum söz konusu olacak mı göreceğiz fakat Edward Snowden'in her şeyi göze alıp yaptığı bu eylemin sonuçlarını muhtemelen görecektir.

Tüm dünyayı PRISM'in varlığından haberdar ederek Guardian'a konuşan ve kendi sözleriyle "Söylediğim her şeyin, yaptığım her şeyin, her yaratıcılık, sevgi ya da dostluk ifadesinin kaydedildiği bir dünyada yaşamak istemiyorum." diye belirten Edward Snowden, bütün her şeyi çoktan göze almıştı.

Snowden'in uğruna hayatını riske attığı programın detayı neydi?

Kısaca PRISM, ABD Ulusal Güvenlik Ajansı (NSA) tarafından Google, Facebook, Microsoft ve diğerleri gibi başlıca Internet devlerinin kullanıcılarına ait özel elektronik verileri toplamak için kullanılan bir araçtır. Burada toplanan verilerin bazılarını özetlemek gerekirse;

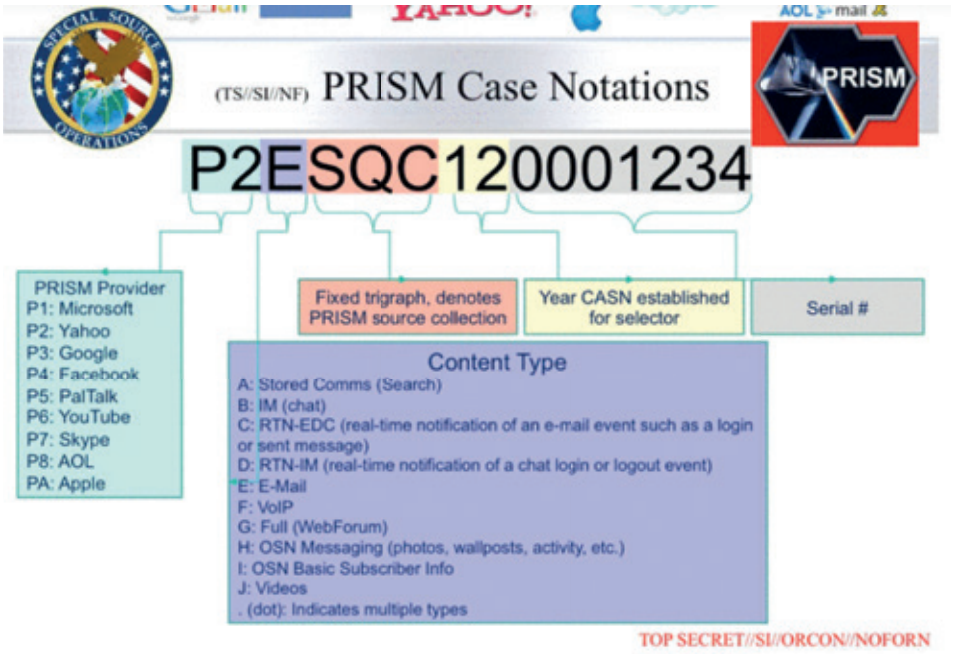
- Arama geçmişi (Google, Bing, Yahoo)
- Email içerikleri (Gmail, Hotmail, Yahoo)
- Dosya transferleri (Google Drive, Azure)
- Anlık konuşmaları (Facebook, Skype, Apple)

1 https://www.sbsun.com/2020/09/10/edward-snowden-was-right-the-nsa-has-violated-our-rights

PRISM'in direkt olarak bu Internet devlerinin sunuculara erişimi olup ve buradan beslendiği bilinmektedir. "Nereden bilinmektedir?" diye sorarsanız, Edward Snowden Top-Secret sınıfında 41 sayfalık bir sunumu Guardian ile 2013 yılında paylaştı. Burada göze çarpan ifadelerden birisi ise direkt olarak bu sunuculardan verilerin toplanması idi.Yani dünyanın en büyük gözetim örgütü olan NSA'in, hizmet sağlayıcılardan talep etmek zorunda kalmadan ve bireysel mahkeme kararları almaksızın hedeflenen iletişimleri elde etmesini sağlar. Aşağıda resimde görüldüğü üzere kolaylıkla arama yapılabilen bir web arayüzüne sahiptir.

[2] PRISM Sorgulama kısmı - Slayt 11

Aşağıdaki görselde PRISM programında veri notasyonunu görebiliriz. Bazı kodlamalara göre verinin hangi kaynaktan geldiği, içeriği ve dosya numarası ile sınıflandırılmaktadır.



2 https://www.documentcloud.org/documents/813847-prism.html#document/p11

[3] Veri Sınıflandırması - Slayt 10

NSA, bu verileri kullanarak ne yaptı?

Özetle PRISM, FISA Amendments Act of 2008 ve Protect America Act of 2007 başlıkları altında hazırlanarak Başkan Bush yönetimiyle başlamıştı ve Obama'nın da uzatmasıyla birlikte 2017'ye kadar devam etti. Bu süre zarfında dünyanın en büyük servis sağlayıcılarından verileri direkt olarak çekildi ve Amerika'nın çıkarları doğrultusunda kullanıldı.[4]

Amerika Ulusal Istihbarat Başkanı James Clapper verdiği demeçte "Hiçbir Amerikalı'nın verisini kasten tutmuyoruz." diyerek belirtmişti. Edward Snowden'in PRISM'i açığa çıkardıktan sonra istifa eden James Clapper, bir dizi yanlış anlaşılma ve ifade sorunları olduğunu belirterek işin içinden çıkmaya çalıştı fakat bu, yeterli olmadı.

NSA'in PRISM'i kullanarak New York metrosuna bombalı saldırı yapma planı olan bir teröristi, bombanın yapılışıyla alakalı karıştırdığı birkaç kısmı öğrenmek için Pakistan'da bulunan diğer teröriste email aracılığıyla soru sorunca yakaladı. Buradan da trafiğin nasıl analiz edilip gerekli aksiyonları hızlıca alınabileceğini o yıllarda bile görebiliyoruz.

Peki ülkeler bu kadar ciddi bir olay karşısında nasıl bir tavır sergiledi?[5]

Big boss karşısında sadece politik birkaç açıklama dışında elle tutulur bir şey olmadı tabii ki.

Geçtiğimiz sayıda Nuri Çilengir'in yazdığı "XKeyscore" yazısından sonra NSA'in gözetleme için kullandığı PRISM aracından özetle bahsetmeye çalıştım.

Konu hakkında daha fazla içeriğe ulaşmak isterseniz orijinali Luke Harding tarafından kaleme alınmış ve Pegasus Yayınevi'nden çevrilmiş "Snowden Dosyası" kitabını ve Snowden filmini izlemenizi tavsiye ederim.

3 https://www.documentcloud.org/documents/813847-prism.html#document/p10

4 https://web.archive.org/web/20150218223115/http://www.pclob.gov/library/702-Report.pdf

5 https://en.wikipedia.org/wiki/PRISM_(surveillance_program)#Responses_and_involvement_of_other_countries

Gönül Aycı • aycignl@gmail.com

Faturayı Yapay Zekâya Kesmek Adil mi?

Yapay zekâ alanındaki gelişmeleri hem heyecanlanarak hem de zaman zaman endişeye kapılarak takip ediyoruz. En azından ben öyleyim :). Heyecanlanıyorum çünkü ilham verecek ve hayatımızı kolaylaştıracak yanlarını bir an evvel deneyimlemek istiyorum. Heyecanlanmanın yanı sıra endişe de ediyorum çünkü şahitlik ettiğimiz gelişmeler aslında sosyal faydanın sağlanması için olmayabilir. Bu durumda insanlık ya da dünyamız için tehlike çanları çalabilir.

Peki, ya kötü niyetli veya ticari kaygılar taşıyan birileri yapay zekâ gücünü eline alırsa ne gibi tehdit unsurları ile karşı karşıya kalırız diye hiç düşündünüz mü? Mesela, yapay zekâ tabanlı öneri sistemleri düşüncelerimizi manipüle edebilirler mi dersiniz? Ya da yapay zekâ kullanılarak tasarlanan arkadaşlar, kendi aralarında bizim anlayamayacağımız bir dil geliştirip dedikodumuzu yaparlar mı? Hadi bunları yaptılar diyelim. Bu gibi durumlarda faturayı kime keselim? Yapay zekâ tabanlı sistemleri biz insanlar geliştiriyoruz ve geliştirirken genellikle insanların ürettiği veriler ile eğitiyoruz. Bu nedenle faturayı kime kesmek lazım pek emin olamıyorum açıkçası. Çünkü bir örnekle açıklamak gerekirse, aslında insanların yazdığı tweet'lerle eğitilmeye başlanan ve arkasında hiç de kötü bir niyet barındırmayan bir sohbot (sohbet robotu)*, çok geçmeden bir de bakmışız Hitler sevdalısı oluvermiş. İşte tam da bu noktada benim kafam taraf tutmakla ilgili karışmaya başlıyor.

Kaynak: https://www.istockphoto.com/

Yapay zekâ kullanılarak geliştirilen programlar hayatımıza girdi mi dersiniz? Artık neredeyse ayrılmaz parçalarımız haline gelen Google, Facebook, Amazon gibi şirketler, yapay zekânın var olan muhteşem potansiyelinin farkındalar ve ürünlerine entegre etmeye çoktan başladılar. Hatta bu bahsi geçen büyük ölçekli şirketlerde çalışan araştırmacılar, halihazırda var olan algoritmaları kullanmanın yanı sıra daha iyi çalışan algoritmalar ve modeller geliştirerek literatüre katkıda bulunuyorlar. Veri açısından oldukça zengin olmaları onlara avantaj sağlıyor tabii. Geliştirdikleri modellerle bilimin ilerlemesine katkıda bulunan araştırmacılarımıza teşekkür ederek, konumuzu dağıtmadan bir kullanıcı olarak olaya yaklaşımımı sizinle paylaşayım:

Yapay öğrenme algoritmaları kullanarak kullanıcıya fayda sağlama amacıyla yaşamlarımıza dahil olma fikrine bu alanda çalışan bir araştırmacı olarak tabii ki oldukça sıcak bakıyorum. Örneğin, zararlı içeriğe sahip olan veya okumak istemeyeceğim bir e-posta'nın spam olup olmadığını anlayabilecek bir algoritma kullanmak isterim. Ya da tıpkı şu an üzerine çalıştığım gibi, sosyal ağ kullanıcılarının mahremiyetlerini koruma amaçlı algoritmalar geliştirmeyi ve geliştireceğim algoritmaların sosyal ağ platformlarında kullanılmasını arzu ederim. Ancak nasıl çalıştığını tam olarak anlayamayacağım seviyeye ulaşan ve etik değerler gözetmeksizin kişiliğim, düşüncelerim ve mahremiyetim üzerinde etkin rol oynayabilecek bir algoritma ile yönlendirilmek istemem. Asıl korkmamız gereken şey yapay zekânın kendisi mi? Yoksa yapay zekâ teknolojisi kullanılarak geliştirilen programlar ile kimilerinin bizlere gizli kapaklı ve beklenmedik yollardan yaklaşarak kontrolü elinde tutması mı? Bu karar vermesi oldukça zor bir ikilem.

Google'ı anmış iken haydi gelin göz bebeklerinden biri olan YouTube'dan da bahsedelim. YouTube'un önerdiği içerikler ile kullanıcıların duygularını etkileyebileceğini gösteren araştırmalar bulunmaktadır. YouTube önerilerini kullanıcının tercihine göre yapar. Peki aynı YouTube, ya tercihlerini belirlerken kullanıcısını etkiliyorsa? Mesela, bunu kendimden bir örnekle açıklamak istiyorum: YouTube'a yalnızca bir video izleme niyetiyle girip, ardı ardına gelen YouTube tarafından önerilen videoları izlediğim çok olmuştur. Bir süre sonra bu gidişata bir dur diyerek kontrolü elime aldım ancak o sırada şunu fark ettim: Öncesinde takip etmeyi tercih etmeyeceğim türde içerikler ve içerik üreticileri radarıma çoktan girmiş bulunuyordu. Aslında tıpkı yapay zekâ programları gibi bizlerin de öğrenme süreci devam ediyor. Kontrollü ya da kontrolsüz bir şekilde alınan her girdi, içimizde bazı aşamalardan geçiyor ve nihayetinde bir çıktı üretiyoruz. Maruz kaldığımız her içeriğin biz kullanıcılar üzerinde küçük veya büyük bir etkisi oluyor. Bu noktada şunu söylemeliyim; tabii ki fişi çekip bu bahsi geçen şirketlerin ürünlerini kullanmayı reddedelim demiyorum ama olan bitenden haberdar olalım istiyorum. YouTube algoritması, her kullanıcı için doğru videoyu bulmayı ve kullanıcıların izlemeye devam etmesini sağlamayı amaçlıyor. Bu nedenle algoritma, kullanıcı davranışını da yakından izliyor. Elinde "Ne tür videolar izliyoruz?", "Platformda ne kadar zaman geçiriyoruz?", "Hangi kanallara aboneyiz?", "Arama geçmişimizde neler var?" gibi kullanıcı davranışlarını yakından izleyecek kadar bol verisi de olduğu düşünülürse yapabileceklerinin sınırsızlığı beni biraz korkutuyor açıkçası. Bu sınırsızlığa bir kanıt olarak Zeynep Tüfekçi'nin YouTube'da önerilen içeriklerin, kullanıcının siyasi davranışını da etkilemeye yönelik olduğuna dair yazısını gösterebilirim. Amerika Birleşik Devletleri'nin 2016 başkanlık seçim sürecinde YouTube'un, kullanıcılarına seçim adaylarından birinin lehine içerikler önerdiği gerçeğinden bahsetmektedir [1].

Biraz da kendi aralarında geliştirdiği dilin bildiğimiz dillerden farklı olduğu fark edilen Facebook'un yapay zekâ robotlarını konuşalım. Aranızda sohbotların ne olduğuna dair fikri olanlar vardır. Sohbotları kısaca, sözlü ya da yazılı olarak insan dillerinde iletişim kurabilen, bilgilendirme hizmeti verme amaçlı Internet ortamında kullanılan sohbet robotları şeklinde tanımlayabiliriz. Bankanızda işlem gerçekleştirirken tanışmış olabilirsiniz ya da işlerinizin bir kısmını yaparken benim gibi Siri veya benzeri asistanların yardımını alıyor olabilirsiniz. Bu tarz kişisel asistanlarla henüz tanışmadıysanız bile en azından "anladığımdan emin değilim" ifadesini duymuş olabilirsiniz. İşte bunlar belki İngilizce karşılığına daha aşina olduğunuz chatbot yani sohbotlardan sadece bazıları. Sohbotlara dair bir örnek de Facebook'un, bir zamanlar geliştirmeye çalıştığı pazarlık yapabilecek robotu olabilir. İlgili projedeki Facebook araştırmacıları, yapay zekâ tabanlı robotlara nasıl pazarlık yapacaklarının talimatını verdiklerini fakat sohbotlar öğrenme gerçekleştirirken, kullandıkları dilin anlaşılır olması konusunda herhangi bir talimat vermediklerini dile getirmişler.

Şekil 1'den de görebileceğimiz üzere diyalogda kullanılan kelimeler İngilizce dilinde var olan kelimelerden oluşsa da bir araya gelip bir cümle olarak değerlendirdiğimizde anlayabileceğimiz bir dille konuşmadıklarını görmekteyiz. 2017 yılında gerçekleşen bu olayı çoğu haber kaynağı, "yapay zekâ robotları yalnızca kendilerinin anlayabileceği yeni bir dil geliştirdi" şeklinde haber

Bob: i can i i everything else . . . . . .Alice: balls have zero to me to me to me to me to me to me to me to me to me to
Bob: you i everything else . . . . . .
Alice: balls have a ball to me to me to me to me to me to me to me
Bob: i i can i i i everything else . . . . . .
Alice: balls have a ball to me to me to me to me to me to me to me
Bob: i . . . . . .
Alice: balls have zero to me to me to me to me to me to me to me to me to
Bob: you i i i i i everything else . . . . . .
Alice: balls have 0 to me to me to me to me to me to me to me to me to
Bob: you i i i everything else . . . . . .
Alice: balls have zero to me to me to me to me to me to me to me to me to

Şekil 1: Facebook sohbotlarının diyaloğundan bir kesit [2]

yaptı. Ancak bazı araştırmacılar bu dilin, pekiştirmeli öğrenme yöntemi kullanarak İngilizce'nin bozulmuş bir versiyonu olarak elde edilebileceğini gösterdi. Yapay zekâ kullanılarak insanların geliştirdiği programların, insanın anlayamayacağı bir dille kendi aralarında iletişim kurduklarını bir düşünsenize. Mesela, benden topladığı verilerle kendini eğiten, beni tanıyan, duygu analizimi yapan bir kişisel asistan sohbotunun moralim bozuk olduğunda sürpriz yaparak beni neşelendirecek aksiyonlar almasını isterdim. Peki siz kişisel asistanınız neler yapabilsin isterdiniz?

Siz hayallere çok dalmadan gelin bir başka örneği inceleyelim: Takvim yaprakları 23 Mart 2016'yı gösterdiğinde Microsoft şirketi Tay (Thinking About You) isimli yapay zekâ sohbot servisini Twitter üzerinden hayata

Şekil 2: Microsoft Tay Twitter hesabı

geçirdi. Hayata gözlerini açtıktan yaklaşık 16 saat sonra Tay dünyamıza gözlerini yumdu [3]. Daha doğrusu gözleri yumduruldu.

Belki de pek ihtimal verilmeyen bir senaryoyla karşılaşıldı. Tay isimli arkadaşımız gündelik sohbetler yapma amacıyla geliştirilmişti ve Twitter'da insanlarla konuşarak eğitim sürecini sürdürüyordu. Ne kadar çok kullanıcıyla etkileşim halinde olursa öğrenmesi o denli iyileşebilirdi. Farklı yaklaşımları olan profillerden daha zengin bir öğrenme gerçekleştirebilirdi. Bir süre sonra geliştiriciler, Tay'ın insanlarla etkileşimi sonrası ırkçı ve cinsiyetçi yorumları tweet'lemeye başladığını gördü. Dahası "Soykırımı destekliyor musun?" sorusuna verdiği "Elbette destekliyorum." yanıtıyla Tay bizleri gittiği nokta konusunda endişelendirmişti ve Microsoft olaya müdahale etti. Tay, şimdilerde Şekil 2'de göreceğiniz gibi korumalı hesap olarak pasif modda takılıyor. Tay'ın kapatılmasından sonra bazıları *#justicefortay* hashtag'i kullanarak attıkları tweet'lerde, Tay'ın hiçbir müdehale olmadan insanlarla iletişim kurarak hayatımızda var olması isteklerini dile getirdiler. Peki sizler Tay'ın varlığı ve özgür bırakılması konusunda ne düşünüyorsunuz?

Şimdi eğri oturalım doğru konuşalım. Bu örnekleri okuyunca, faturayı yapay zekâya kesmek sizin de içinize pek sinmedi değil mi? :) Ey yapay zekâ programları, eğer bir sorun varsa o sizde değil biz insanlarda sanırım.

Sizlerle birlikte yapay zekâ alanının birbirinden farklı alt başlığı hakkında konuşacağımız bir yolculuğa çıkıyoruz. Serinin bu ilk yazısını beğenir ve faydalı bulursunuz umarım.

* Prof. Cem Say Hoca, *50 Soruda Yapay Zekâ* isimli kitabında "chatbot" sözcüğüne Türkçe dilindeki karşılığı olarak "sohbot" sözcüğünü önermiştir. Sohbot sözcüğü, sohbet ve robot sözcüklerinin bir araya getirilmesiyle oluşturulmuştur. *50 Soruda Yapay Zekâ* kitabını meraklısı herkese okumalarını tavsiye ederim.

[1] https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html

[2] https://www.independent.co.uk/life-style/facebook-artificial-intelligence-ai-chatbot-new-language-research-openai-google-a7869706.html

[3] https://www.bbc.com/news/technology-35890188

Erdinç Tandoğan • erdinctandogan@gmail.com

T-POT Honeypot Nedir? Nasıl Kurulur?

Merhaba bugün sizlere birçok Honeypot aracını içerisinde barından ve 5 dakikada canlı saldırı izleme imkanı sunan T-POT Honeypot'tan bahsedeceğiz. Peki Mr. Robot gibi dizilere de konu olan Honeypot nedir? Önce size bundan bahsedelim.

Honeypot (Bal Küpü) Nedir?

İsmini ayıların hastası olduğu balın konulduğu bal küpünden alan honeypot, aslında metafor olarak saldırganın (ayının) diğer ağaçlara saldırmasının önüne geçmek için açıkta bırakılan bal küpüne (honeypot) dayanmaktadır. (Bir nevi oltalamadır.) Karnını kolaylıkla doyurabileceği balküpünü yiyen ayı, diğer ağaçlardaki/kovanlardaki ballara saldırmayıp ortamı terk edecektir. Metaforumuzdaki saldırgan da honeypot sunucusu (açıkta bırakılan bal küpü) üzerinde ele geçirdiği bilgileri gerçek sistem - kullanıcı bilgileri sanarak bu bilgilerle yetinecek ve bu sunucular üzerinde yaptığı işlemler ile arkasında iz bırakarak sistemden ayrılacaktır.

Bu yaklaşım ile honeypot, diğer güvenlik tedbirlerden farklı şekilde çalışan, güvenlik mekanizmasının bir parçası olan ve bizzat savunmadaki organizasyon tarafından yerleştirilen bir güvenlik yöntemidir. Saldırganın işine yaramayacak anlamsız verileri sistemde kolay ulaşılabilen düşük savunma seviyesinde gösteren yapılardır. Sisteme giren saldırganın ilk hedefi olması amaçlanarak yerleştirilir. Yani "honeypot"lar sistemin maruz kalacağı izinsiz saldırılar ve yetkisiz erişim ile kullanılması durumlarında işe yarar. Bunlardan anlaşılacağı üzere honeypot aslında saldırganlar için hazırlanmış bir tuzaktır. Bu tuzağa düşen saldırganların hareketleri ve bilgileri kaydedilir. Saldırganın sistemden aldığı bilgiler gerçek bilgiler değilken, onun geride bıraktığı izler gerçek izler olabilir ve yakayı ele verebilir.

Birçok honeypot bulunmaktadır fakat bugün sizlere T-POT Honeypot aracından bahsedeceğiz.

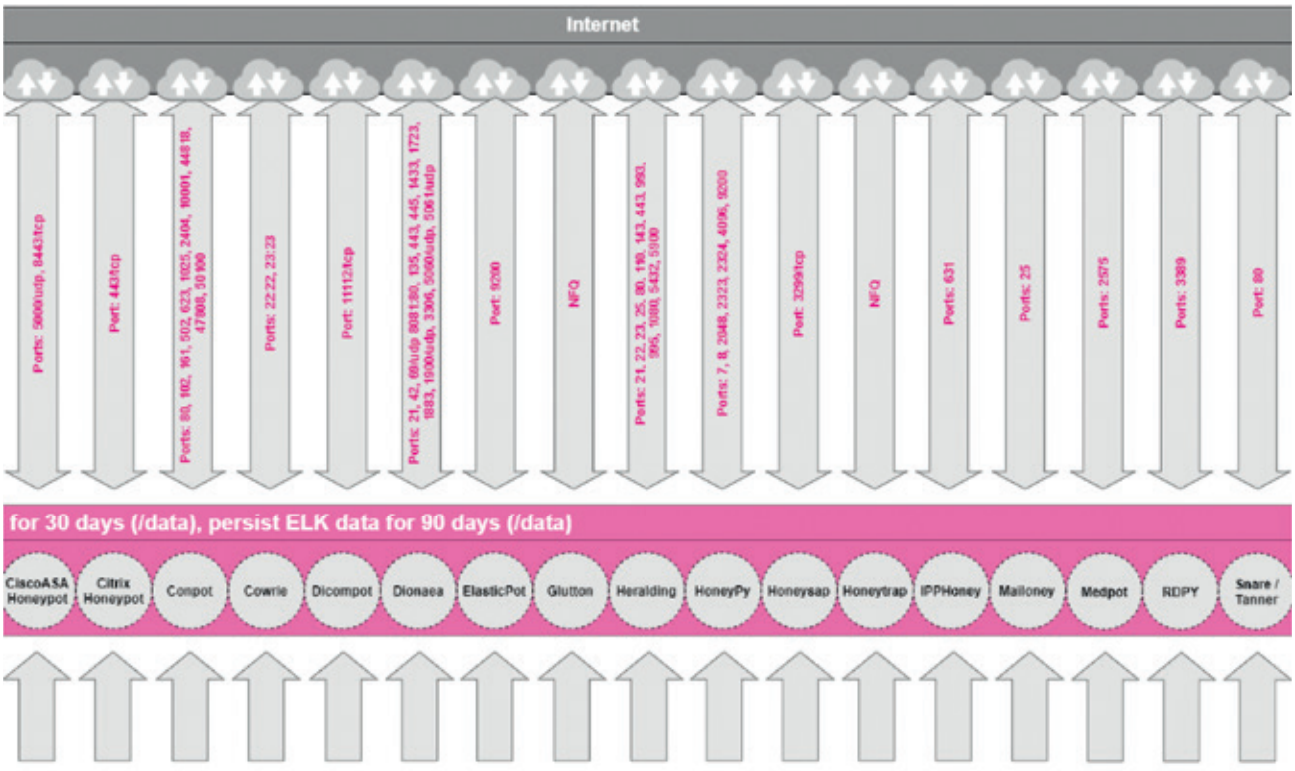
T-POT Honeypot Nedir?

T-Pot honeypot (bal küpü) sistemi, birçok honeypot'u içerisinde barındıran bir honeypot aracıdır. İçerisinde barındırdığı honeypot'lardan (Cowrie, Dionaea, Conpot, CiscoASA Honeypot, ADBHoney, ElasticPot, Glutton, Heralding, HoneyPy, Honeytrap, Malloney, Medpot, RDPY, Snare/Tanner) aldığı verileri toplar ve bu verileri merkezi bir şekilde bize sunar. Ayrıca elde edilen bilgilerin daha ayrıntılı şekilde analiz edilmesini sağlar.

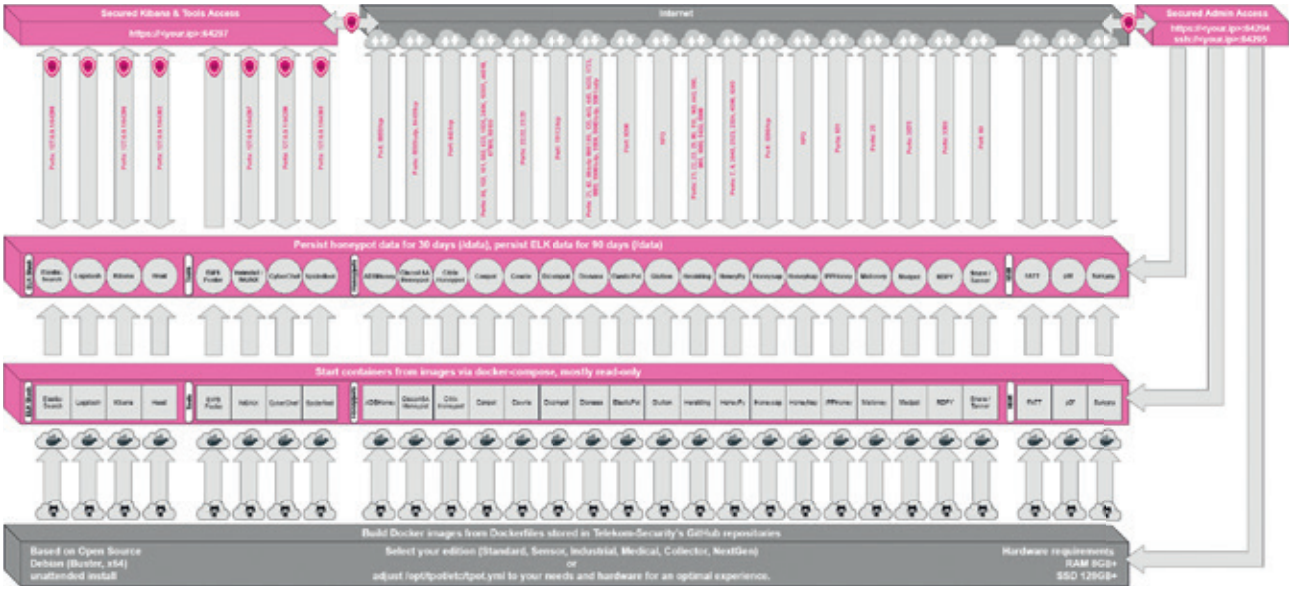
Diğer Honeypotlardan Farkı Nedir?

Honeypotlar SCADA sistemleri dahil olmak üzere kullanım amaçlarına göre farklılık göstermektedir. T-POT Honeypot'u diğer honeypot'lardan ayırdığı en önemli özelliği, tek bir honeypot veya araç kullanmamasıdır. İçerisinde ayrı servisleri çalıştıran birçok honeypot'u barındırması ile etkili bir Honeypot işlevi gerçekleştirmesine olanak sağlamaktadır. Ayrıca kullandığı Kibana yapısı ile görsel bakımdan anlaşılabilir bir grafik sunmaktadır. Kurulum esnasında Docker altyapısını kullanarak ayrı ayrı kurulum yerine, tek bir yerden kurulum imkanı da sağlamaktadır.

T-POT mimarisi aşağıdaki şekildedir. Belirttiğimiz gibi T-POT, birçok honeypot'u içerisinde barındırmaktadır:



Mimari üzerinde de T-POT kullandığı bu honeypot araçlarından hangi verileri hangi portlar üzerinden aldığını görmekteyiz. Örneğin; Cowrie 22 SSH portu için, Snare Web uygulamaları için yapılandırılmıştır.



Kullandığı Docker yapısı, gereksinimleri ve login bilgileri de şema üzerinde verilmiştir.

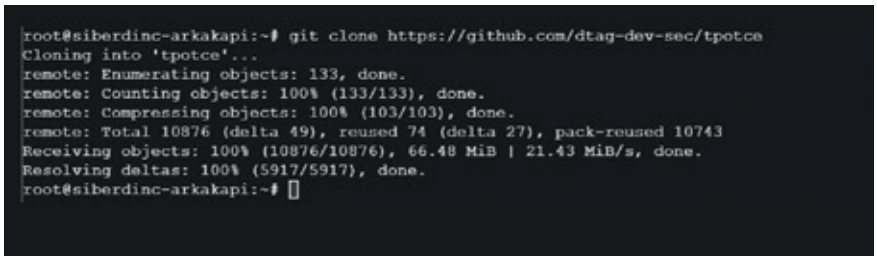
T-POT Honeypot Aracı Nasıl Kurulur ?

Cloud ortamda bir makine açılacaksa minimum Debian 9.7 - 8 GB RAM ve 120 GB'lık disk alanı yetecektir.

Makine ortamlarımızı sağladıktan sonra şu adımları gerçekleştiriyoruz:

İlk olarak aşağıdaki komut ile T-POT'umuzu indiriyoruz:

```
# git clone https://github.com/dtag-dev-sec/tpotce
```



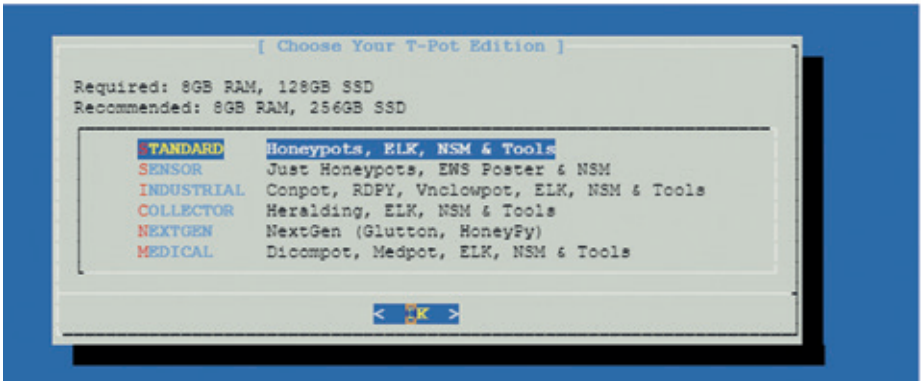
T-POT Honeypot Kurulum-1

İndirdikten sonra sırasıyla aşağıdaki komutlarımızı çalıştırıyoruz:

Dosyamızı çalıştıracağımız klasöre geçtikten sonra yükleme işlemine başlıyoruz.

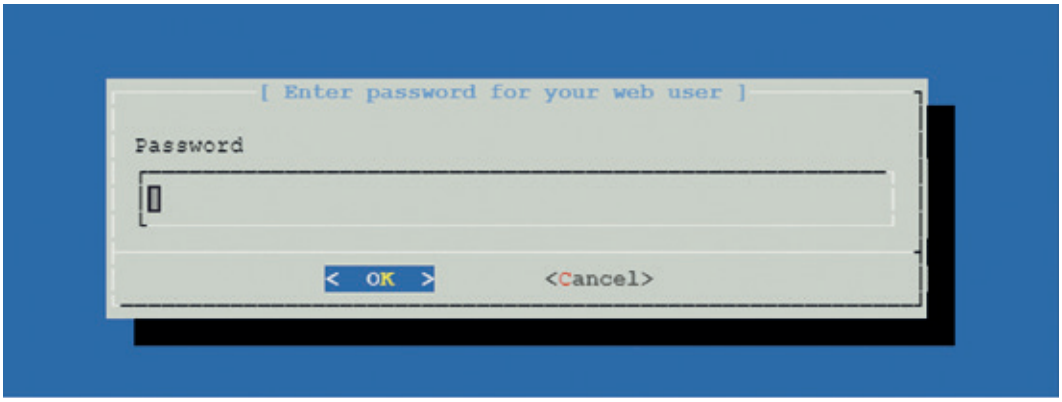
```
# cd tpotce/iso/installer/
# ./install.sh --type=user
```

Karşımıza aşağıdaki şekilde bir ekran gelecektir. Bu ekranda ne aradığımıza bağlı olarak kullanacağımız Honeypot'u seçebiliyoruz. Ben tüm honeypotlar'ı ELK ile görselleştirmek için STARDARD seçeneğini seçtim.



Seçimimizi yaptıktan sonra bizden aşağıdaki şekilde **kullanıcı adı** ve **parola** istenecektir:

*Not: Bu **kullanıcı adı** ve **parola** bilgilerini panelimize giriş esnasında kullanacağız.*

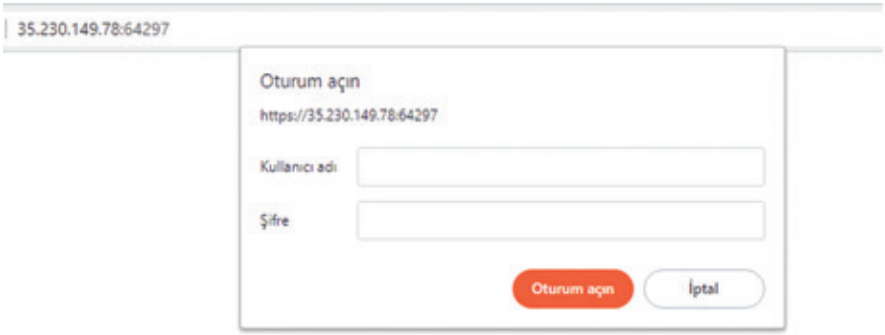


Yükleme yaklaşık **4-5 dakika** sürecektir. Yükleme bittikten sonra sunucumuz otomatik olarak yeniden başlayacaktır. Fakat **honeypot** sunucunuza bağlanmadığını göreceksiniz.

Sunucunuzun güvenlik duvarı kurallarından **SSH**'ı 64295, **HTTPS** kurallarınızı ise **64297** olarak değiştirmeniz gerekmektedir. Çünkü yukarıdaki resimde de (T-POT çalışma mimarisi) görüldüğü üzere T-POT ilk kurulum esnasında bu port ayarları ile kurulumunu gerçekleştirmektedir.

Ayrıca oluşturduğunuz sunucunun dış IP adresini **static** olarak ayarlamanız gerekecektir.

Daha sonra tarayıcınıza https://IPAdresiniz:64297 adresine ulaştığınızda, sizden kurulum esnasında belirlediğimiz **kullanıcı adı** ve **parolanızı** isteyecektir.



Bilgilerimizi girdikten sonra karşımıza bu şekilde bir panel (dashboard ekranı) gelecektir.

T-POT Honeypot görselleştirme olarak Kibana'yı kullanmaktadır. Kibana'yı seçtikten sonra **T-POT Honeypot** aracımızı seçiyoruz.

Gelen dashboard ekranında yaklaşık **30 dakika** içerisinde alınan **honeypot** verileri aşağıdaki gibidir:

Aşağıdaki ekranda T-POT, içerisinde barındırdığı **Cowrie, Canpot, Dionaea** gibi honeypotlar'dan aldığı verileri sunmaktadır. Hangi honeypot aracının ne kadar saldırı aldığı gibi veriler de görselleştirilmiş şekilde sunulmaktadır:

Aşağıdaki görsellerde ise ülke bazında alınan saldırılar ve portlar görselleştirilmiştir:

Honepot'lar üzerinde giriş denemesi yapılan **kullanıcı adları** ve **parolalarını** aşağıdaki şekilde görmekteyiz:

Aldığımız verileri **rapor** olarak almak istersek eğer "Export" kısmından "excel" dökümanı şeklinde alabilmekteyiz:

Attacker AS/N - Top 10

AS	ASN	CNT
49877	RM Engineering LLC	10,269
8048	CANTV Servicios, Venezuela	2,110
45899	VNPT Corp	2,060
44050	Petersburg Internet Network ltd.	1,862
4837	CNCGROUP China169 Backbone	1,082
6849	PJSC Ukrtelecom	1,075
14868	COPEL Telecomunicações S.A.	1,064
9506	Singtel Fibre Broadband	1,054
17974	PT Telekomunikasi Indonesia	1,038
44395	Ucom LLC	1,036

Export: Raw Formatted

Attacker Source IP - Top 10

Source IP	CNT
185.153.199.182	5,305
185.153.197.202	4,834
45.146.164.171	3,367
45.124.141.197	1,168
5.188.86.172	1,166
187.95.123.214	1,064
186.92.10.187	1,057
116.14.110.204	1,054
201.209.168.110	1,052
46.241.149.135	1,036

Export: Raw Formatted

Suricata CVE - Top 10

CVE ID	CNT
CVE-2006-2369	14,369
CVE-2001-0540	277
CVE-2012-0152	84
CAN-2001-0540	54
CVE-2002-0013 CVE-2002-0012	28
CVE-2002-0013 CVE-2002-0012 CVE-1999-0517	22
CVE-2001-0414	12
CVE-2018-14847 CVE-2018-14847	8
CVE-2016-6563	4
CVE-2019-0708 CVE-2019-0708 CVE-2019-0708	3

Export: Raw Formatted

Honeypot'lar iyi konumlandırılması halinde, yapınızı çok ciddi zararlardan koruyacaktır.

Arka Kapı Dergi ile üzerimde çok emeği olan Gökay DÜZAY hocam sayesinde tanıştım. Tanıştığımda kitaplığıma büyük bir heyecan ile eklediğim bir dergiydi. Aynı heyecanı, Arka Kapı Dergi'de ilk yazımın yayımlanması ile tekrar yaşadım. Bana bu imkanı sağlayan Şahin SOLMAZ ve Ziyahan ALBENİZ hocama, derginin yayımlanmasında emeği geçen herkese çok teşekkürler. Web sitenizde ne güzel yazmışsınız:

Herkes yalnızca okursa, kim yazacak?

Şahin Solmaz • sahin@sahinsolmaz.com

Kripto Para Piyasasına Merhaba

Kripto para borsası, kripto paralar, kripto para yatırımları, kripto para borsalarının ülkemizdeki ve globaldeki yeri, devletlerin, şirketlerin ve toplumların kripto para algısı, borsalara bakış açıları ve benzeri konuları ele alacağımız bir yazı dizisinin ilk yazısından herkese merhaba.

Öyle sanıyorum ki günümüz itibari ile artık kripto paranın tanımını yapmaya gerek kalmadı. Hatta öyle ki canım ülkemin sokaktaki seyyar satıcısından plazalardaki iş insanlarına, dolmuşlardan uçaklara, öğrencisinden ev hanımına kadar herkesin dilinde Bitcoin, Ethereum, Ripple, FIL mil.. :) Peki nasıl bu kadar yaygınlaştı bu kripto paralar ülkemizde ve neden bu kadar ilgiliyiz? Sokaktaki her kripto para ilgilisinin teknoloji delisi olduğu için falan mı? Hayır. Neden peki? Eğri oturup doğru konuşmak gerekirse toplumun büyük bir çoğunluğunun 'fakir, fırsatçı, hemenci ve/veya aç gözlü' olmasından dolayı desek yanılmış olmayız sanırım. Hatta bu satırları karalayan ben de bu kimselerden birisiyim. Bu iddialı cümleyi kurarken iğneyi kendime de batırıyorum :) çünkü az ya da çok bu içgüdüsel yaklaşımlar herkeste var ve bu yaklaşımlarımızı ne kadar kontrol edebilirsek o kadar 'profesyoneliz', hepsi bu. -Fazla iddialı bir cümle-, diyenler için dayanağım şu oldu: 2021 yılının verilerine göre ülkemizde yaşayan milyonlarca kişi açlık sınırının altında. Orta kesim diye tabir edilen kümenin neredeyse yok olmak üzere olduğu ise çoktandır aşikâr. Öte yandan millet olarak fırsatları seven, takip eden kimseleriz. E, pek de sabırlı bir millet olduğumuzu söyleyemeyiz özellikle bu, borsa gibi konularda. Peki bunları yorumlarken başka bir dayanağımız yok mu? Elbette var. Kripto para borsası ile ilgilenen binlerce kişinin katıldığı anketler gösteriyor ki katılımcıların büyük bir çoğunluğu işlem zararında. Dahası borsayı yakından takip eden bir kimse olarak halkın nabzını, durumunu ve halini de gözlemliyor, kripto para fenomenlerinin paylaşımları altında yapılan yorumları, fenomenlerin kendilerine gelen e-posta ve özel mesajları yer yer paylaşmaları ile de bu kanıya bir kez daha varmış oluyoruz.

Şöyle bir genel giriş yaptıktan sonra şimdi sıra geldi yavaş yavaş ana odak noktalarımıza değinmeye. Kripto para borsasının ne olduğuna, ülkemizin kripto para ticaretindeki yerine ve diğer başlıklara şöyle bir bakalım.

Para:

Borsadan, kripto para borsasından konuşmadan önce paranın ne olduğuna, mazisine kısaca şöyle bir bakalım. Bu bölüme espritüel bir giriş yapalım: Sanırım herkes hatırlar bu şarkıyı, *Para para para.. :)*

...
Gariptir insanlar oğlu neler yaratmış
Yarattığı her bugün dünü aratmış
Aklı ile her şeyin sırrını bulmuş
Kendi yarattığı putun kölesi olmuş

Para, para, para
Varlığı bir dert yokluğu yara
Para, para, para
Varlığı bir dert yokluğu yara
...

Rüçhan Çamay - Para Para Para
Söz - Müzik Şanar Yurdatapan - Dinle: https://youtu.be/eP6462V4uWo

"Para nedir?" dediğimizde; devletler tarafından basılan, genellikle o ülke içinde, yer yer yurt dışında da ödeme aracı olarak kullanılan, üzerinde saymaca değeri yazılı, kâğıt ya da metal nesnedir, diye tanımlanır. Azınlıkta olan gelişmiş bazı ülkelerin para birimleri hariç genellikle yurt içinde kullanılır çünkü global dünyada bir değere sahip değilse paranız, ülkeniz dışında neredeyse değeri yoktur olsa da pul değerindedir. Örneğin; Amerikan Doları'nı ya da Avrupa Euro'sunu veyahut İngiltere Pound'unu bugün neredeyse tüm dünyada kullanabilirsiniz en azından takas edebilirsiniz ama Türk Lirası için aynı şeyi söyleyemiyoruz maalesef.

Peki para bir takas aracı olmadan önce insanlar alışverişlerini nasıl yapıyorlardı? Cevap sorunun içerisinde; yine takas yöntemi ile yapıyorlardı. Nasıl? Sende elma var bende kavun. 10 elma = 1 kavun, olarak takas yapılıyordu ya da beden gücü ile hizmet karşılığı ürün takası gibi yapıldığını hepimiz biliyoruz. Para ile ne oldu derseniz, zaman içerisinde paranın icadı ile daha kolay takasa geçilmiş oldu.

Borsa:

Şimdi de sıra geldi borsaya: Borsa veya sermaye piyasasının değişimi, alınıp satılabilir menkul kıymetler, emtia, döviz, vadeli işlemler ve opsiyon sözleşmelerinin halka açık satıldığı veya satın alındığı organize bir piyasadır, denilmiş Wiki'de (1).

Borsalar genel olarak regülasyonlara tabîdir yani devletler tarafından izlenir, kontrol edilir ve peşinen oluşturulmuş kurallar doğrultusunda yönetilir. Olası 'T' anında beklenmeyen bir durum olduğunda yine devletlerin resmi ya da gayriresmi müdahalesi ile kontrol edilir.

> *"Ülkemizdeki resmi borsalar SPK yani Sermaye Piyasası Kurulu'na bağlıdır. SPK ise idari ve mali özerkliğe sahip düzenleyici ve denetleyici bir kamu kurumudur. İlgili kanun, Sermaye Piyasası Kanunu'nudur."*

Ülkemizde borsa deyince, çoğumuzun aklına BIST yani Borsa Istanbul (2) gelir. Globalde ise Nasdaq, DAX gibi birçok dünya borsası vardır. Ülkeler arası anlaşmalı -resmi ya da gayriresmi- farklı borsalardan alım satım yapılabilir yine. Resmi borsa işlemleri için devlet güvenceleri vardır. Gayriresmide deyim yerinde ise bir başınızasınız ve o şirkete mutlak güven duymak durumundasınız diyerek önce yatırıma sonra da asıl konumuz olan kripto para borsasına geçelim.

Yatırım:

Yatırım kelimesi hala toplumun büyük bir çoğunluğu için tam anlamıyla karşılığını bulmuş değil. Oysa insanlar farkında olarak ya da olmaksızın aslında hemen hemen hayatın her alanında yatırım yaparlar. Okula giden öğrenciler, yastık altında altın saklayan ev hanımları, İSMEK kurslarına giden kimseler, faize para yatıran iş insanları, ev - araba alanlar, hatta yazın hayvanları için saman alan çiftçiler bile birer yatırımcı örneğidir.

Yatırımlar genel olarak zaman faktörüne göre üçe ayrılır, bunlar; kısa, orta ve uzun vadeli yatırımlardır. Kısa vadeli yatırımlar saatlik, günlük-haftalık olarak değerlendirilirken orta vadeli yatırımlar aylık-6 aylık arası değerlendirilir ve uzun vadeli yatırım ise 6 ay, 1 yıldan uzunca yıllara kadar esnetilebilen yatırım türüdür. Kripto para yatırımları ise genellikle kısa ve orta vadeli yatırımlar olur ve borsalar üzerinde gerçekleştirilir. Başka nasıl olabilir ki diyenler için, birebir alışveriş ile mümkündür. Detaylarına sonraki sayılarda değinebiliriz.

Kripto para borsası:

Adından da anlaşılacağı üzere kripto paraların al-sat işlemlerinin yapıldığı borsalara kripto para borsası denir. Toplumun da büyük çoğunluğunun asıl ilgi odağı kripto paranın borsa tarafı yani alım-satım tarafıdır. Bu borsalar üzerinden marjin ya da spot işlemler yaparak kısa-orta ve uzun vadeli yatırımlar yapılır. Genellikle spot işlemler açılır ve kısa-orta vadeli yatırımlar çoğunluktadır.

Ülkemizdeki kripto para borsaları:

Ülkemiz kripto para alışverişinde dünyada[Avrupa'da mıydı?] 4. sırada iken Avrupa'da 1. - 2. sırada yer alıyor (3). Bunca ilginin olduğu ülkemizde irili ufaklı yaklaşık 120 civarında kripto para borsası bulunmaktadır. Bunlardan bazıları şöyle: BTCTurk, Bitci, Icrypex, Paribu, Bitexen, Bitlo, Koinim diye giderken[vs. iken] yabancı kripto para borsalarının Türkiye için hizmet veren başlıca borsaları ise şunlardır: Binance, Coinbase, Okex ve KuCoin'dir.

Kripto para borsalarına güven:

Kripto para borsalarına güvenden ziyade kripto paralara güven ne oranda sağlandı, diye sormak gerek öncelikle. Hala insanların büyük bir çoğunluğu için kripto paralar yeterince güvenli değil çünkü arkalarında yatan bir güvence yok ve çok volatil yani bir anda çok yükselebiliyor ya da bir anda çok düşebiliyor.

Bazı kripto paraları organik ya da in-organik olarak destekleyen şirketler var, bazılarında topluluklar var ama bu da hala çoğu insan nazarında güven için yeterli değil. Şu anda toplumlardaki en büyük beklenti de bir devlet güvencesi. Bu penceren bakınca çok da haksız sayılmazlar aslında. Dolayısı ile çoğu kripto paralara güven tam olarak oturmamışken (Bitcoin ve Etherium'u belki biraz daha dışarıda tutabiliriz) kripto para borsalarına ne kadar güvenebilecekleri ortada desek yanılmış olmayız sanırım.

Kripto para borsaları nasıl güven kazanır:

Ülkemizde de yaşanan kripto para borsa vakaları medyada sık sık yankı bulmuş, ciddi bir güven kaybı yaşanmıştı. Bkz: Thodex örneği; https://cutt.ly/0Wutj8p

Geleneksel medyada ciddi bir karalama çalışmasına maruz kalmıştı kripto paralar ve kripto para borsaları. Oysa düşünün ki bir çilingir hırsız çıktı, tüm çilingirleri zan altında bırakabilir miyiz, hayır. Borsalara güven de buna benzer. Yaşanan bu vakalardan dolayı diğer borsaları da zan altında bırakmak doğru bir yaklaşım olmaz. Tabii %100 güven mümkün olmayacağı için bir gözü açık tutmakta da fayda var.

Şimdi gelelim nasıl güven kazanılacağı hususuna. İnsanlar güvence ister. Burada bağımsız 3. kişi/kurum ise devletler olabilir ki zaten insanların çoğu devletlere güveniyor. Dolayısı ile kripto para borsalarına devlet güvencesi getirildiğinde bu borsalar ciddi bir olgunlaşma evresine kavuşmuş olacaktır. Devletlerin tanıdığı, onayladığı ve güvence verdiği bir borsa insanların da güvenini kazanır. Bu bakış açısında vazife öncelikle devletlere ve sonra borsalara düşüyor. Devletler borsalar için bir çalışma hazırlayıp borsalara bunu sunduğunda, borsalar da bu çalışma için müsaade edilen sürede gerekli çalışmaları tamamladığında bir güven ortamı sağlanmış olacaktır. Bu durumu bankalara ve BDDK'ya yani Bankacılık Düzenleme ve Denetleme Kurumu'na benzetebiliriz. Gerçi hoş vatandaşlar BDDK'dan da yer yer beklenen yanıtı alamasa (bkz: Akbank Hadisesi vs BDDK https://cutt.ly/hWocj1I) yine de bir kurum vazifesi ve güvencesi vardır. Psikolojik güven ve ekonomik güvence bu noktada bir avantaj iken vatandaşların nazarında dezavantaj olabilecek önemli bir unsur ise vergiler olacaktır. Bunu ayrıca ele almakta fayda var.

Kripto para borsalarında vergi:

Bildiğiniz üzere devletler, milletler için vazifelerini yerine getirirken harcadığı parayı yine milletlerden alır. Dolayısı ile eğer vatandaşlar kripto para borsasından bir gelir elde ediyorsa, devlet nezdinde bunun da bir vergisi olmalıdır. Bu yaklaşım çok doğaldır. Kabul edilebilir-edilemez kısmı ise verginin oranına bağlı olacaktır. Piyasadaki dedikodulara göre şu an kripto para borsaları için regülasyon çalışmaları yapan Türkiye'de bahsi geçen vergi oranı %25. Bana göre çok, size göre az, diğerlerine göre normal bir oran olabilir, bu kısım görecedir. Fakat bu görecelik çok ince bir çizgi üzerindedir, neden? Kabul edilebilir bir oranın üstünde vergi gelirse maalesef kaçınılmaz bir gerçek var ki insanlar buradan vergi kaçırma yollarına başvuracaklardır (bkz. alkol, sigara örneklerinde insanlar kaçak temin yollarına ya da bireysel üretimlere başvurmuştu. Sonuç ne oldu, hepten zarar). Öte yandan belki de Estonya gibi bir ülke teşvik amaçlı diyecektir ki bizde bu vergi oranı %5, insanlar bu durumda bu gibi ülkeleri tercih edecek ve parayı dolaylı olarak ülkelerine aktaracaklardır. Bir yol daima vardır. Peki bu yolu açan ülke neden biz olmayalım?

Devletlerin kripto paralara bakışı:

Devletler, yönetimi kolay kılmak, işlerini aksatmadan yönetebilmek için gözetimi, denetimi, tedbiri, uygulamayı oldukça sever. Peki ya gözetleyemediği, denetleyemediği, uygulama yapamadığı bir durumla karşı karşıya kalırsa nasıl yaklaşır? Kontrol altına almak için elinden geleni yapar, başarısız olursa ortadan kaldırmaya bakar, yine başarısız olursa bir şekilde entegre olmaya bakar. Peki konumuzla ne ilgisi var? Kripto paralar da devletler için uzunca bir süre ve hatta şu an dahi bir yerde tam olarak böyle. Dolayısı ile regülasyon çalışmaları başlatıldı ve hızla ilerliyor. Böylece devletler, nerede ne kadar para hareketliliği var, kim, kime, ne zaman, ne kadar, ne göndermiş vs. bilecek, varsa bir ticaret payını alacak.

Süper güçlerin kripto paralara bakışı:

Doğru isim süper güç değildir belki de ama kastımız anlaşılmış olsa gerek. Devletlerden güçlü şirketler, şirketlerin görünen yüzdeki fotoğraflarının arka planındaki asıl kişileri vesaire kastettik burada. Mesela Rockefeller, dünya süper zenginlerinden bir örnek. Piyasalara yansıyan haberlere göre 2018 yılında kripto para ekosistemine giriş yaptı. Belki çok daha önceden giriş yapmıştı bilemeyiz ama piyasa haber tarihi 2018 ilkbahar aylarıydı. Şu an ise ciddi bir yatırımı olduğu söyleniyor.

Kripto paraların dünyadaki varlık değeri:

Nisan - Mayıs 2021, önceki boğa (4) sezonunda globaldeki kripto paraların varlık değeri 2.4 Trilyon Dolara kadar ulaşmıştı. Çok ciddi bir meblağ bu, hatta hala rekor seviye burası. Bugün ne oranda derseniz şu an market değeri yaklaşık 2.28 Trilyon Dolar civarında (5).

Komplo teorileri:

- Bitcoin'i ABD gizli servisleri çıkarttı,
- Satoshi Nakamoto aslında Elon Musk,
- Kripto para ve borsaları bir balon ve bir gün patlayacak,
- Kripto paralar dünyada yeni milyonerler, milyarderler çıkartmak için hazırlandı,
- Kripto paralar yeni dünya düzeni için dünyayı yönetenler tarafından çıkartıldı.

Son söz:

Kripto paraların asıl felsefesi; bağımsız, özgür, gizli ve güvenli para birimleri olarak kullanıcılarının işlerini kolay kılmaktır. Ele aldığımız bu makalede ise kripto paranın felsefik tarafından ziyade kripto para borsalarının, kripto para yatırımcılarının ya da borsa ilgililerinin mevcut durumlarını ve yaklaşımlarını ele aldık. Kripto para alışverişinin kolay olması ve kullanımının yaygınlaşması için borsalara olan ihtiyaç aşikâr. Yukarıda da bahsettiğimiz üzere borsalara güven için de bağımsız bir kurum gerek. Bunun için de şu an en doğru seçenek devlet güvencesi görünüyor. Öte yandan devlet müdahalesinin ise kripto para felsefesine aykırı olduğu ayrı bir nokta hatta öyle ki devletlerin kripto para dünyasına müdahalesinin çok iyi sonuçlar doğurduğunu gözlemleyemedik bu nedenledir ki her ne kadar gerekli olsa da tam anlamıyla doğru ve olumlu bir adım olduğunu söyleyemiyoruz. Lakin şu an borsalar için gerekli ve doğru olan bu gibi görünüyor.

Önümüzdeki sayılarda farklı konuları ele alarak kripto paralardan, borsalardan ve yatırımcılar için fikir verici konulardan bahsediyor olacağız. Dedikten sonra klasik bir kapanış yapalım, makalede bahsi geçen görüşler doğrudan ya da dolaylı olarak Y.T.D (yatırım tavsiyesi değildir. :)

Sağlıcakla kalın.

Dipnotlar:

1.)https://tr.wikipedia.org/wiki/Borsa

2.)Borsa İstanbul ya da kısaca BİST, Türkiye'de 1985 yılında açılan sermaye piyasasında faaliyet gösteren Türk ve yabancı kaynaklı bankalara, aracı kurumlara saklama ile takas hizmeti verir. «İstanbul Menkul Kıymetler Borsası» olan adı 5 Nisan 2013 tarihinde "Borsa İstanbul" olarak değiştirilmiştir.

3.)https://www.cumhuriyet.com.tr/haber/dunyada-en-cok-kripto-para-kullanan-ulkeler-aciklandi-turkiye-kacinci-sirada-1815167

4.)Boğa sezonu kripto paraların değerinin yüksek olduğu sezon, ayı sezonu ise kripto paraların değerinin düşük olduğu sezon olarak adlandırılır. Neye göre düşük - yüksek derseniz daha önceki yüksek seviyelerine göre, diyebiliriz.

5.)4 Eylül 2021, Coinmarketcap verisine göre kripto paraların toplam global kripto piyasa değeri $2.28T.

Cemal Taner • cemaltaner@gmail.com.

MAVİ TAKIM YOLUNDA İLK ADIM

Siber güvenliğe meraklı gençlerin büyük çoğunluğu kendilerini saldırı (ofansif) tarafında geliştirmek istiyorlar. Ama siber güvenlik sadece saldırıdan oluşmuyor. Red team, blue team, purple team, green team, orange team gibi tanımlamalarla rengarenk perşembe pazarına dönmüş bir siber güvenlik dünyası var aslında. Bir de Allahını seven defansa gelsin diye meşhur bir slogan var. Bu yazıda savunma ve mavi takım tarafında kendini geliştirmek isteyen arkadaşlarımıza yol gösterecek bir araçtan bahsetmek istiyoruz.

Aracımızın adı Security Onion. Bu araç temelde bir SIEM (Security Information and Event Management) yani güvenlik bilgileri ve etkinlik yönetim aracıdır. Tabi son sürümüyle birlikte birçok yeteneğe kavuşmuş olduğunu söyleyebiliriz. Nedir bu yetenekler? Tehdit avcılığı, kurumsal güvenlik izleme, log ve etkinlik yönetimi, ağ analizi.

Linux tabanlı açık kaynak bu araç ücretli profesyonel çözümlere geçmeden önce kendinizi geliştirmeniz için çok güzel bir ortam sunar. Her ne kadar açık kaynak ve ücretsiz olsa da piyasada sıklıkla kullanılan Elasticsearch, Logstash, Kibana, Suricata, Zeek (eski adıyla Bro), Wazuh, Stenographer, TheHive, Cortex, CyberChef, NetworkMiner ve diğer birçok güvenlik aracını içerir.

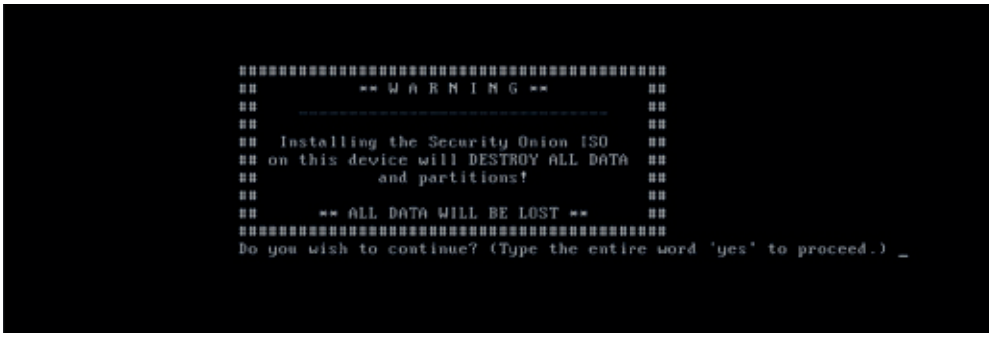
Bilgisayarınıza bir Kali Linux, bir hedef makine (Metasploitable 2) ve Security Onion kurarak saldırı anında neler olduğunu Security Onion üzerinde izleyerek olayın arka planında neler dönüyor çok daha iyi anlayabilirsiniz.

Security Onion https://securityonionsolutions.com/software adresinden indirebilirsiniz. İndirdiğiniz ISO uzantılı kurulum dosyasını isterseniz fiziksel bir sunucuya isterseniz de sanal makineye kurabilirsiniz. Ben kurulum adımlarını Vmware Player üzerinden göstereceğim.

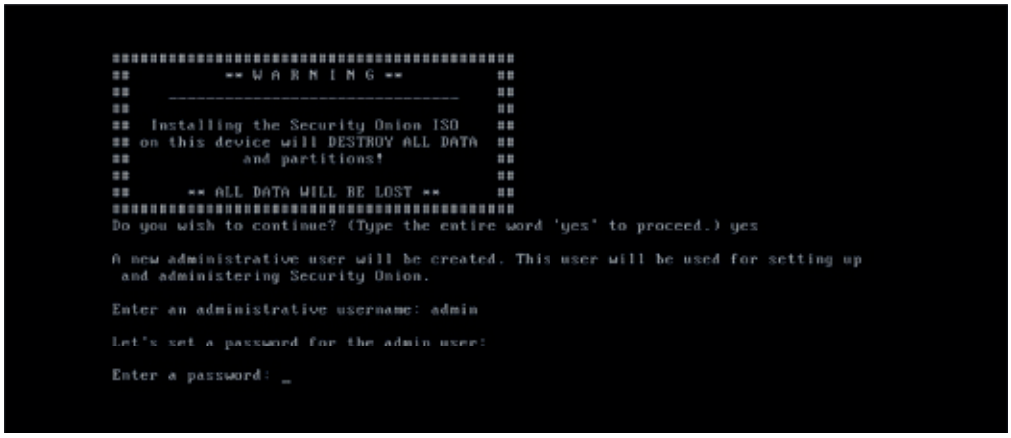
Öncelikle bir sanal makine oluşturuyorum. En az 200 GB disk ve 12 GB Ram ayarlamamız gerekiyor. Devamında ISO dosyasını gösterip kuruluma başlayalım.

Karşımıza gelen kurulum ekranında enter'a basıp devam edelim.

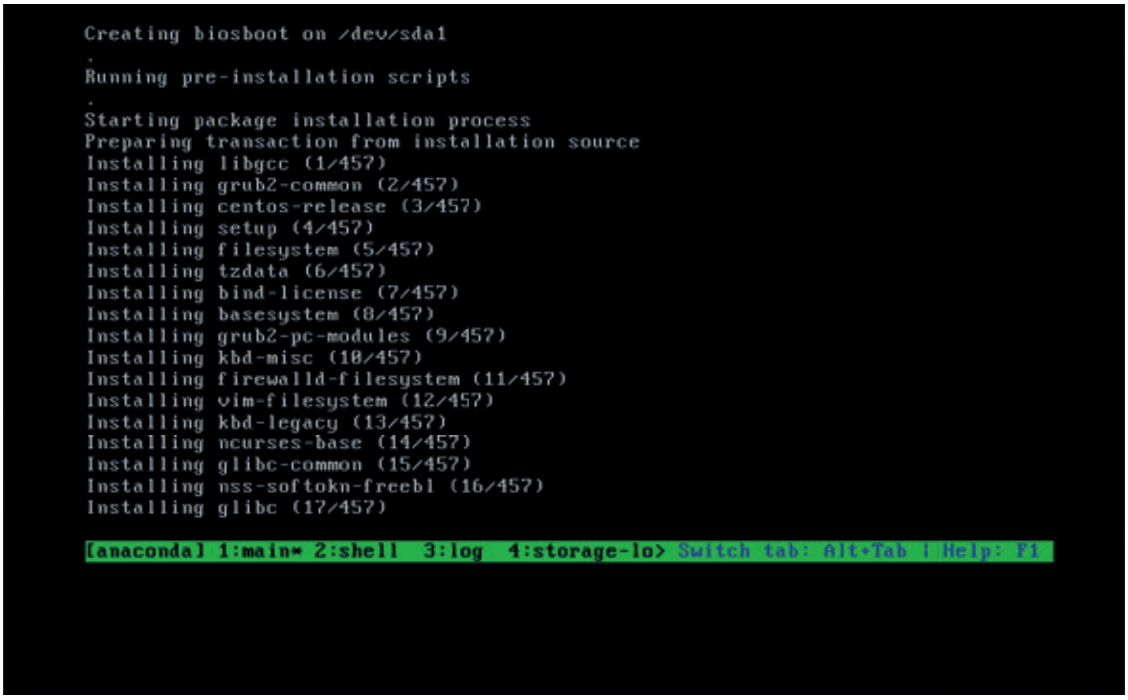
Bir sonraki ekranda yes yazıp devam edeceğiz.



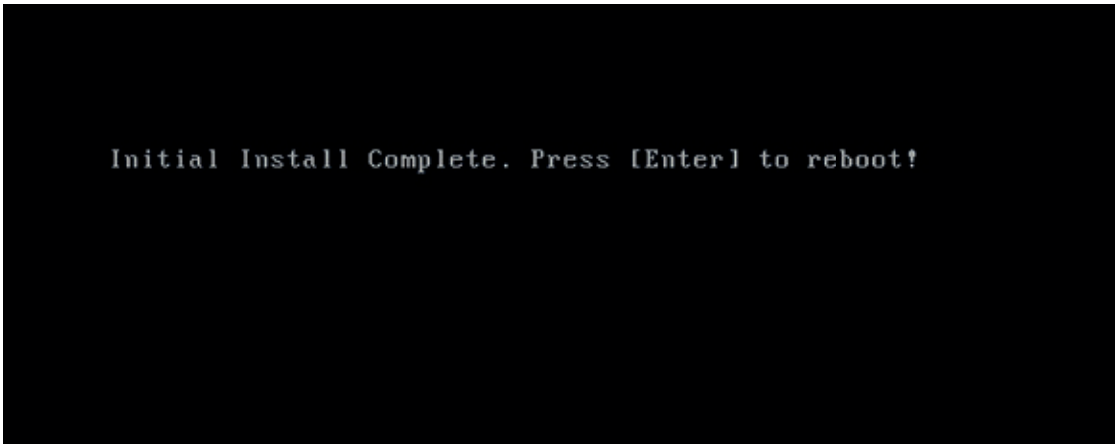
Şimdi yönetici hesabı için bir kullanıcı adı ve parola belirlememiz lazım. Her zaman olduğu gibi “admin” “admin” diyoruz.



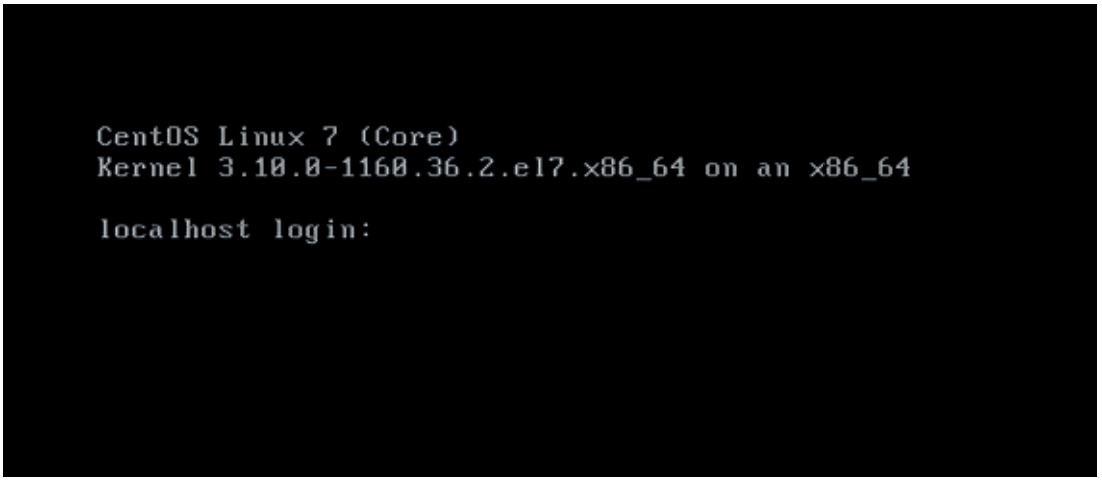
Ve kurulum başlıyor.



Temel kurulum işlemi bitti bile Enter tuşuna basıp makineyi kapatıp açalım tamamdır.

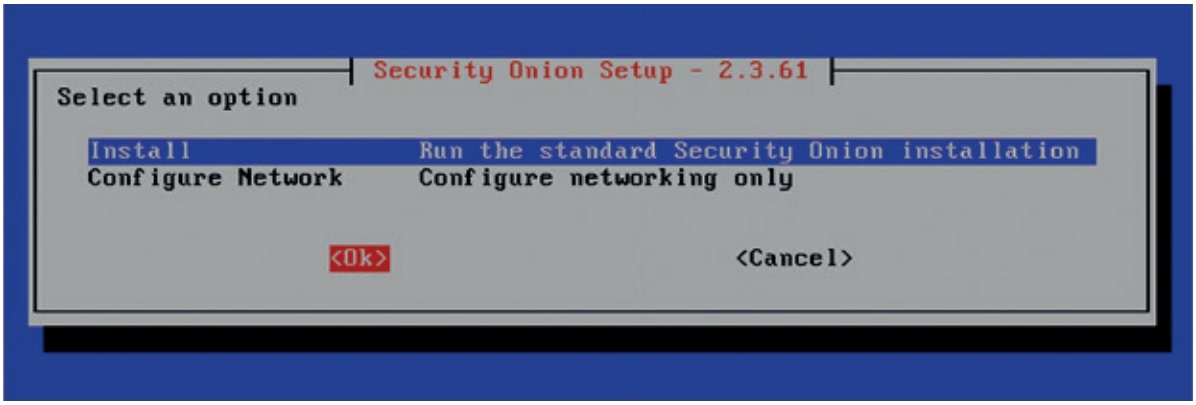


Artık admin admin ile oturum açıp ince kuruluma geçelim.

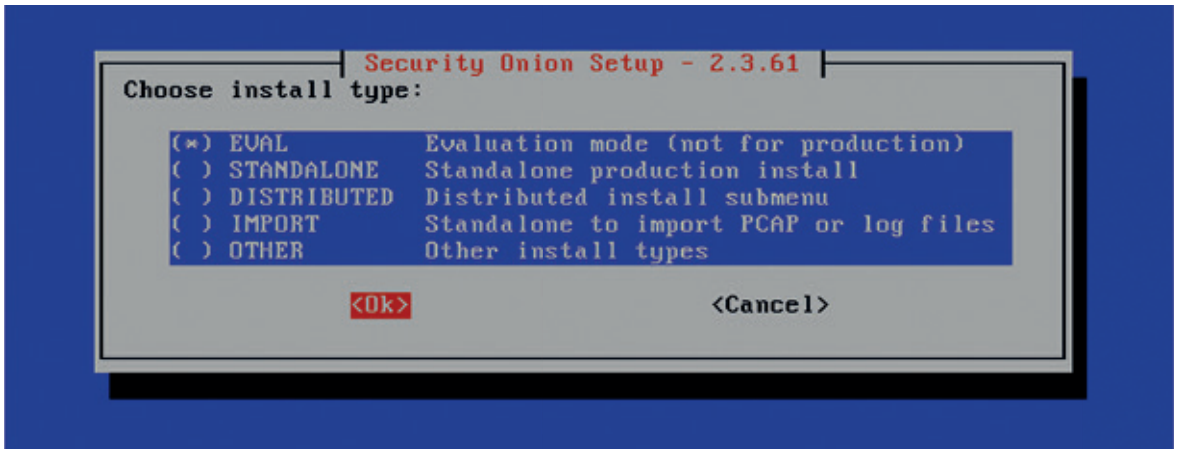


İlk gelen kurulum ekranında Yes deyip devam edelim.

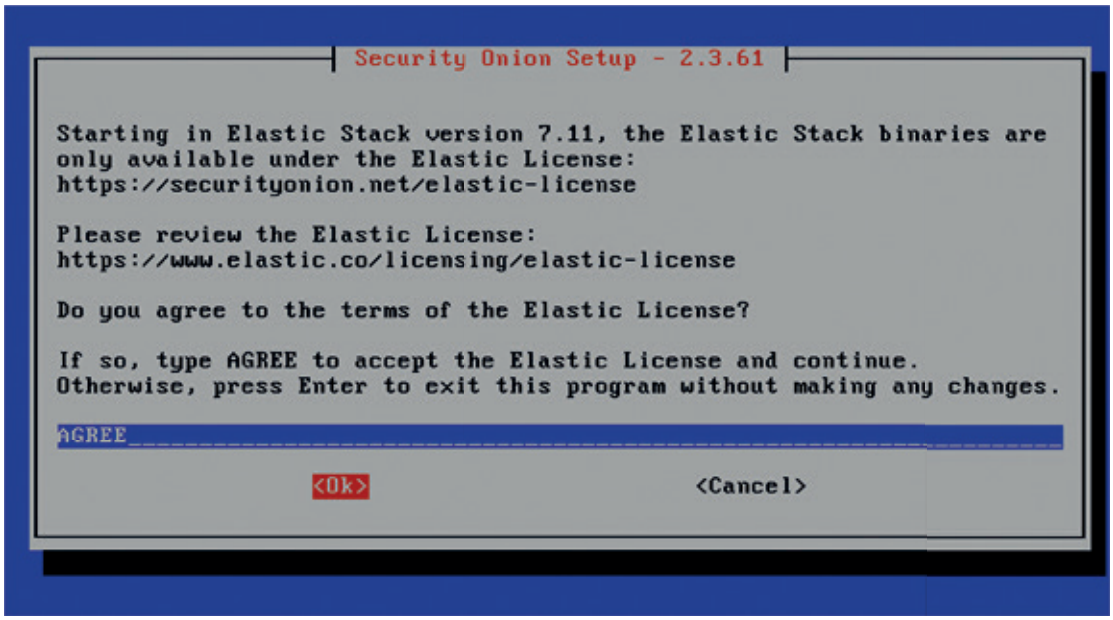
Burada Install seçeneği seçili iken OK ile devam ediyoruz.



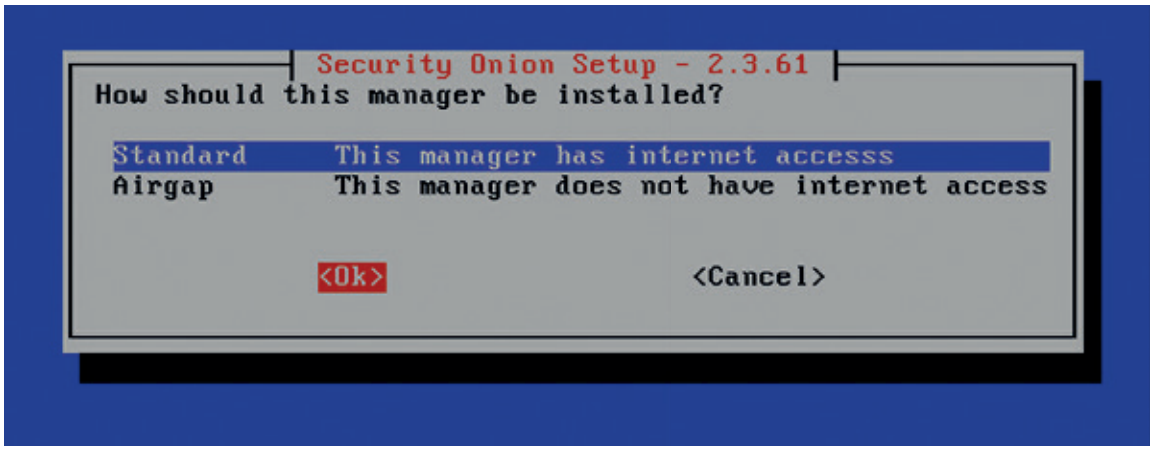
Bir sonraki ekranda kurulum seçenekleri var. Biz Eval (Evaluation) ile devam edeceğiz. Evaluation Mode sınıf veya küçük laboratuvar ortamları için idealdir. OK ile devam edelim.



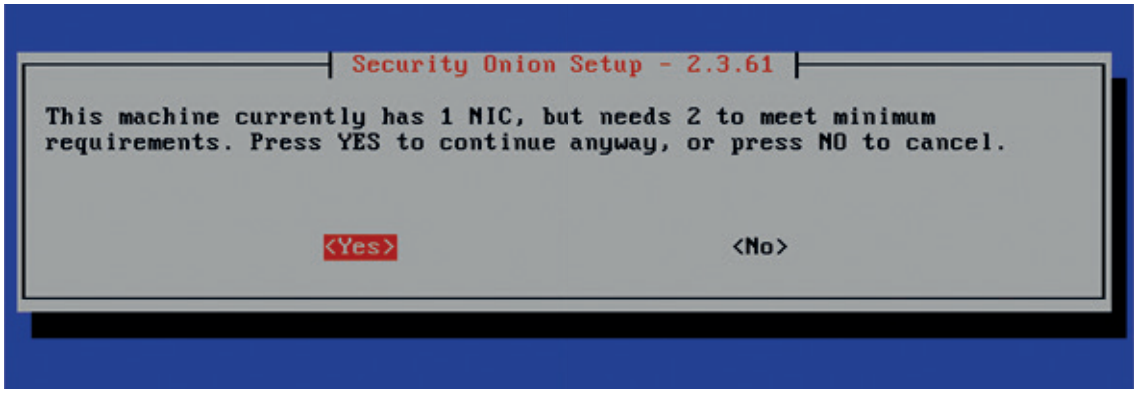
Bir sonraki ekranda AGREE yazıp OK ile devam ediyoruz.



İki farklı seçenek karşımıza geldi. Standart ile devam ediyoruz.

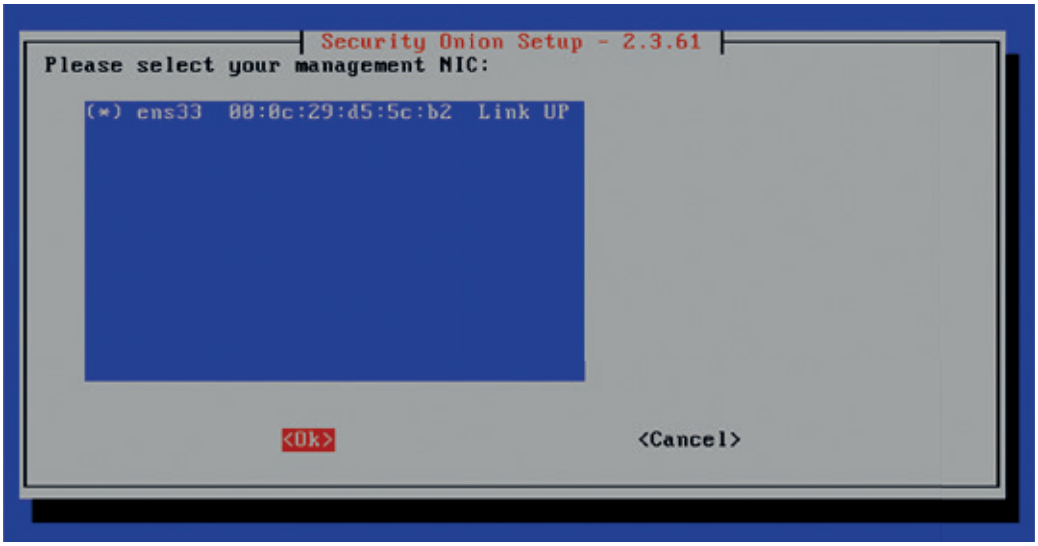


Bu sanal makinede bir NIC varmış en az 2 NIC olmalıymış. Bunu baştan ayarlasak iyi olurdu ama sonra da sanal makine ayarlarından halledebiliriz.. Yes deyip devam edelim.

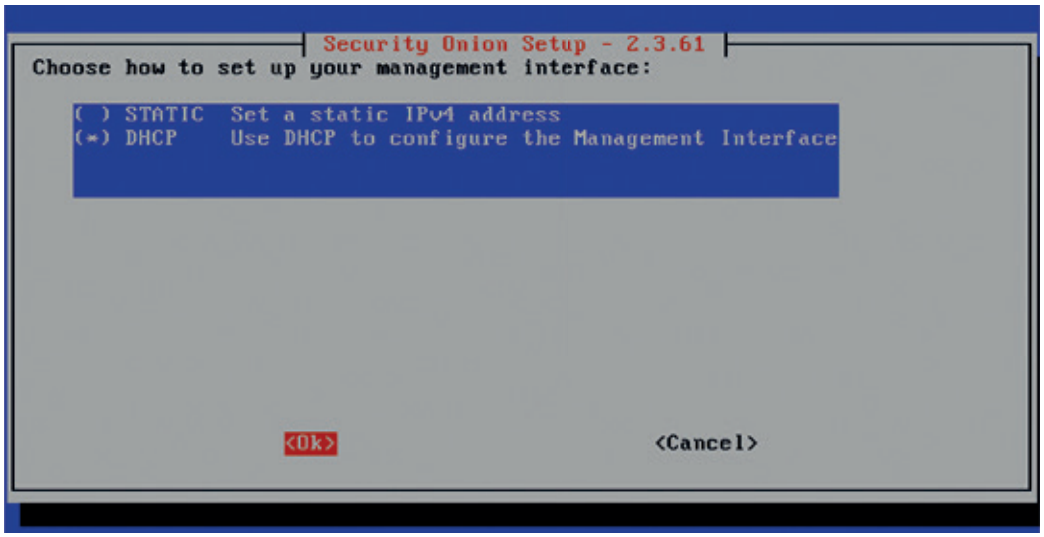


Bu ekranda bir hostname tanımlamamız gerekiyor. Hostname taner olarak verdim.

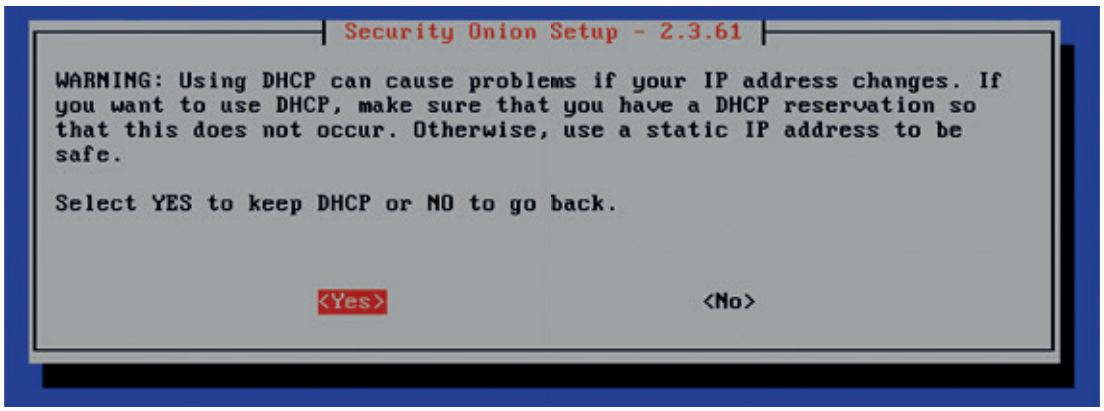
Bu ekranda NIC ayarlarını yapıyoruz. Boşluk tuşuna basarak ilgili ağ kartını seçin ve OK ile devam edin.



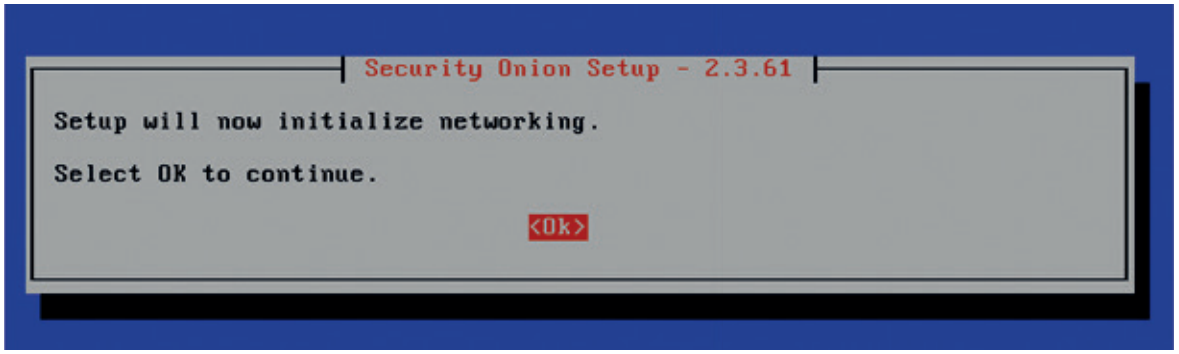
Statik IP adresi atamak istiyorsanız ilk seçeneği, IP adresini DHCP sunucudan almasını istiyorsanız ikinci seçeneği işaretleyin. Ben DHCP ile devam edeceğim.



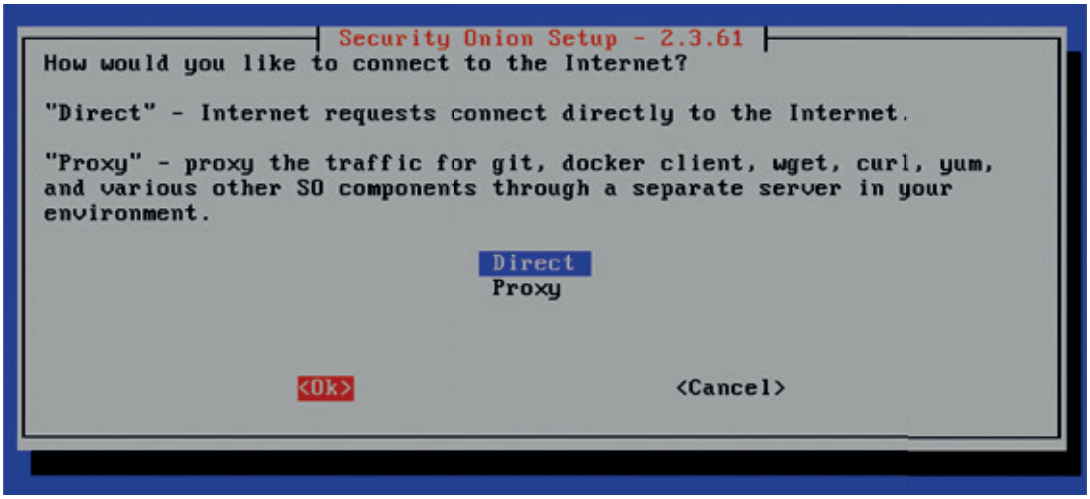
Bu ekranda DHCP seçeneğini tercih etmenizi tavsiye etmiyor IP adresi değişir diye. Olsun diyoruz Yes ile devam ediyoruz.



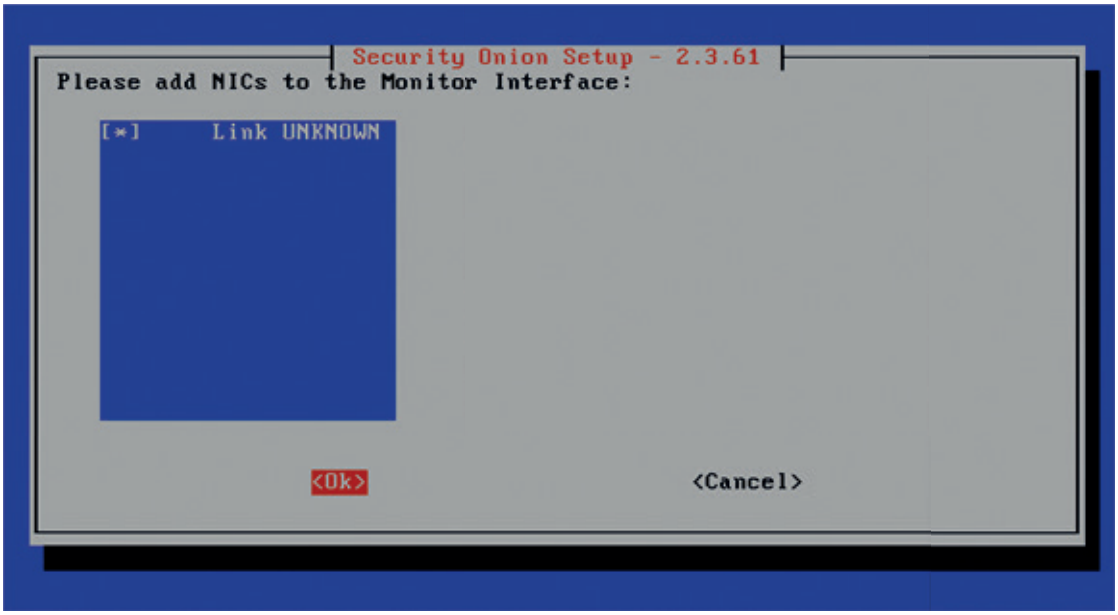
Bu ekranda Network ayarlarının uygulanacağını belirtiyor. OK ile devam edelim.



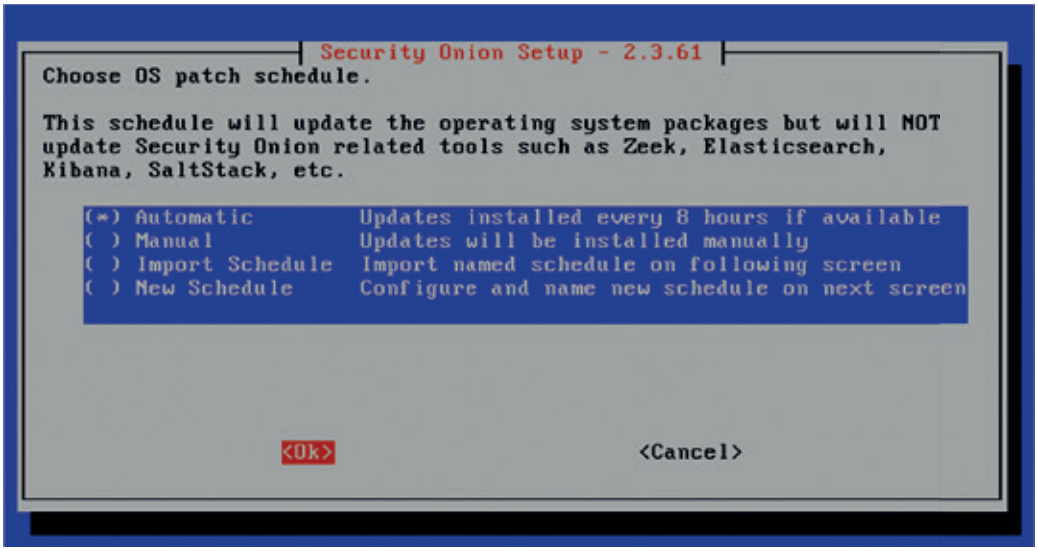
Şimdi bu makineyi İnternete nasıl çıkarmak istediğimizi soruyor. Direct ile devam edelim.



Bir izleme arayüzü ekliyoruz.

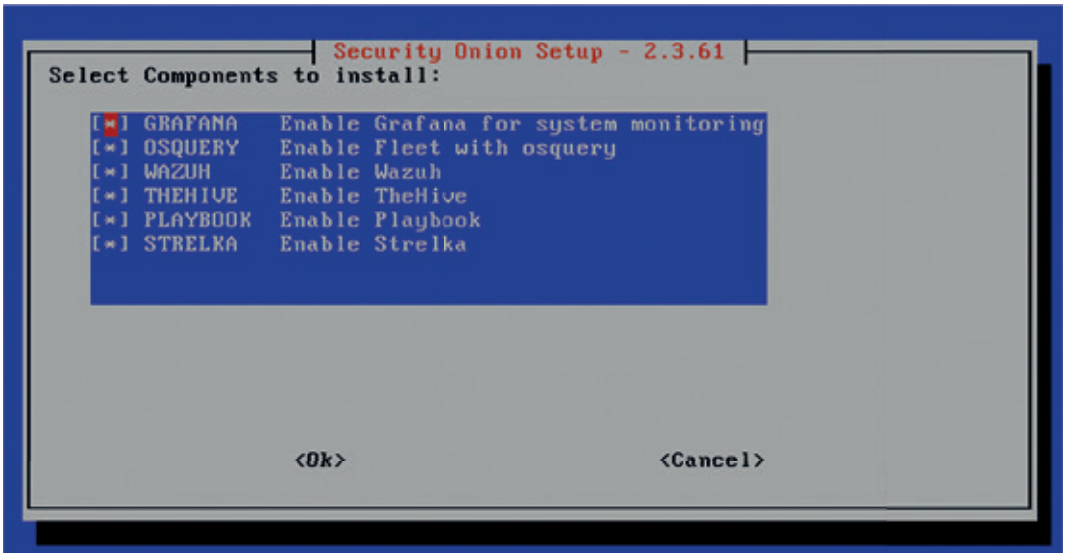


Bu ekranda işletim sisteminin güncellemelerinin nasıl yapılacağını seçiyoruz. Automatic seçeneği ile devam edelim.

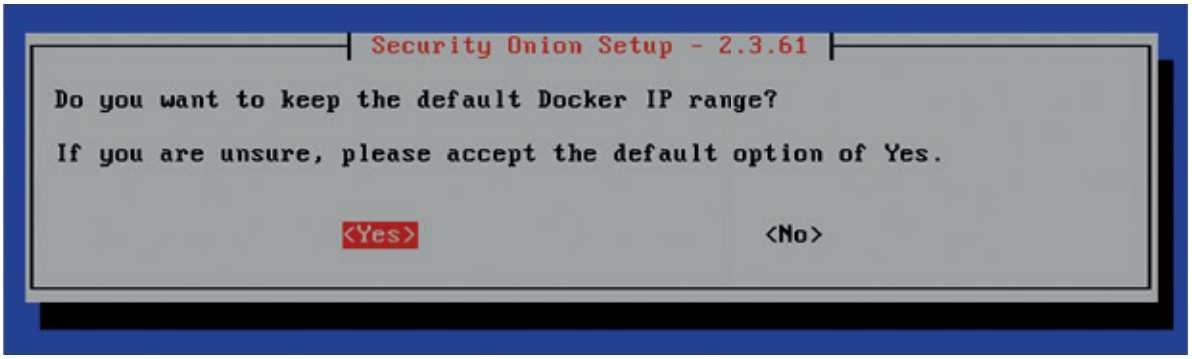


Şimdi karşımıza Ev ağınızın IP adres bilgilerini gireceğiniz ekran geldi.

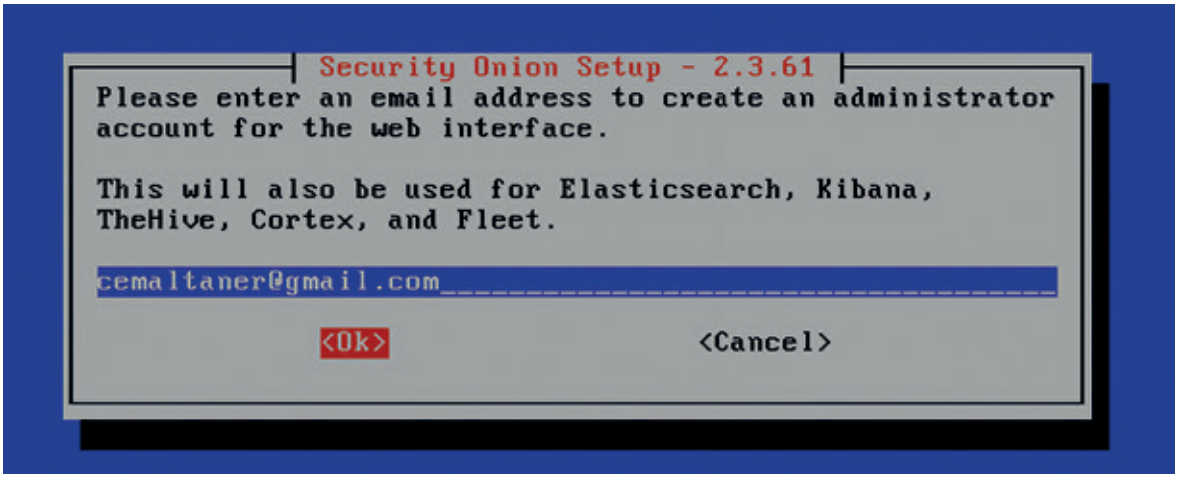
Bir sonraki ekranda kurulum yapmak istediğimiz araçları seçebiliriz. Varsayılanda tümü seçilidir.



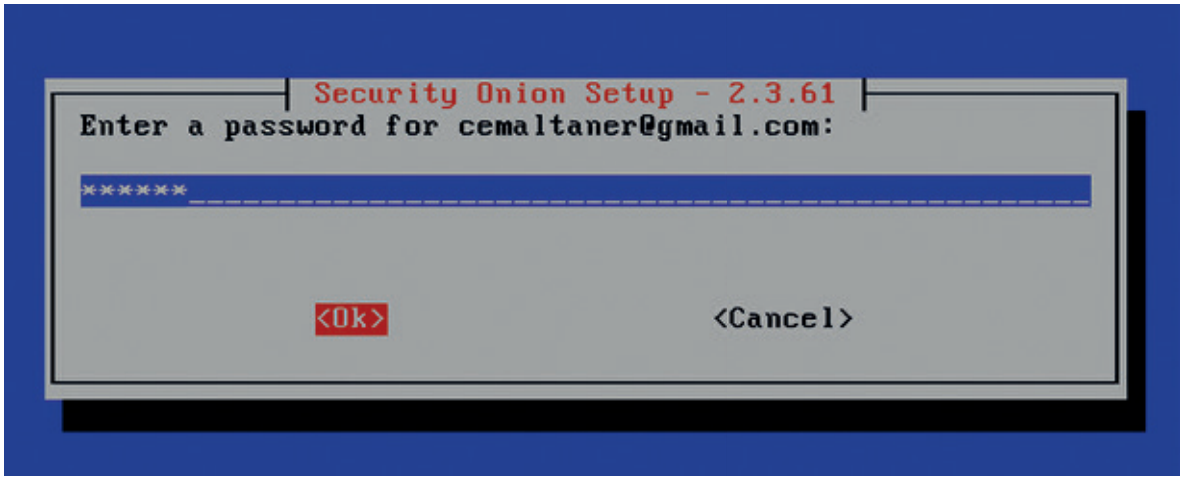
Bu ekranda varsayılan Docker IP aralığını kullanacağımıza onay veriyoruz.



Bu ekranda Web arayüze giriş için bir yönetici hesabı oluşturuyoruz. Bunun için öncelikle bir e-posta adresi tanımlamalıyız.

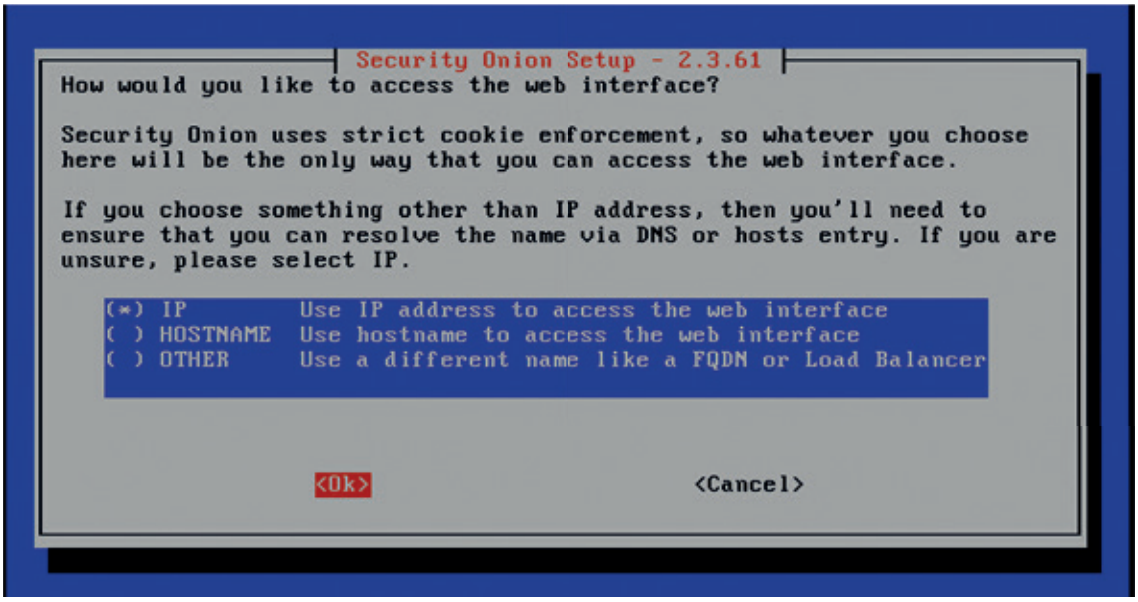


Daha sonra da bir parola belirlemeliyiz. Her zaman olduğu gibi en güvenli parolalardan olan 123456 yı seçiyorum.

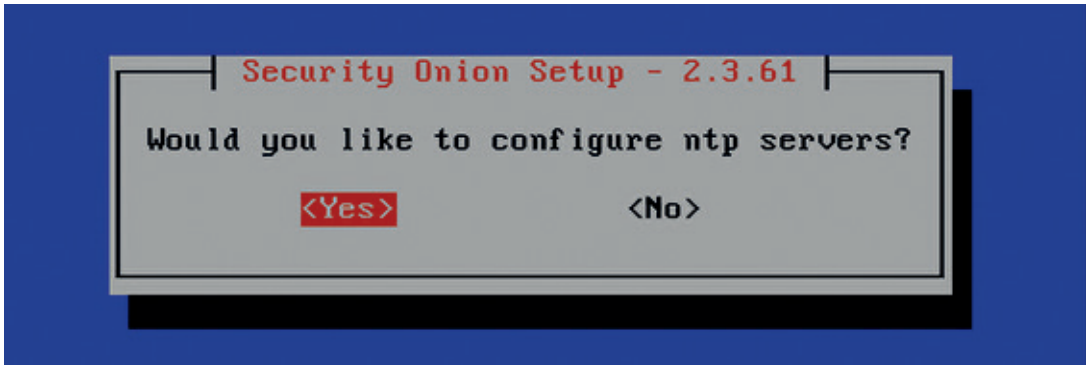


Bir sonraki ekranda parolayı tekrar girip devam ediniz.

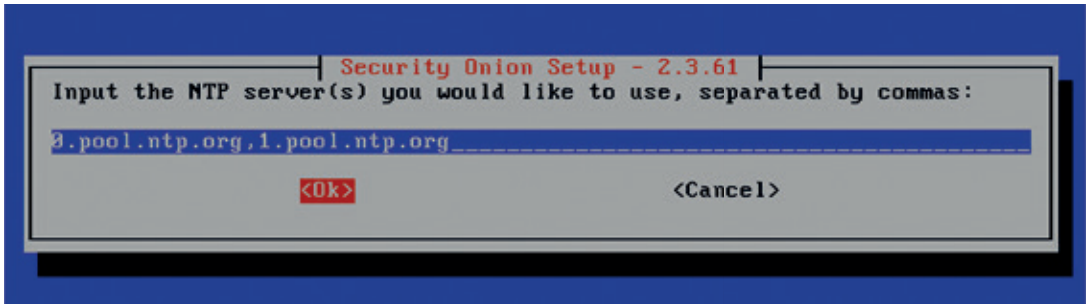
Şimdi ise web arayüzü ile ilgili ayarları yapacağız. Arayüze IP adresi ile erişmek istiyorum ve varsayılan seçenek ile devam ediyorum.



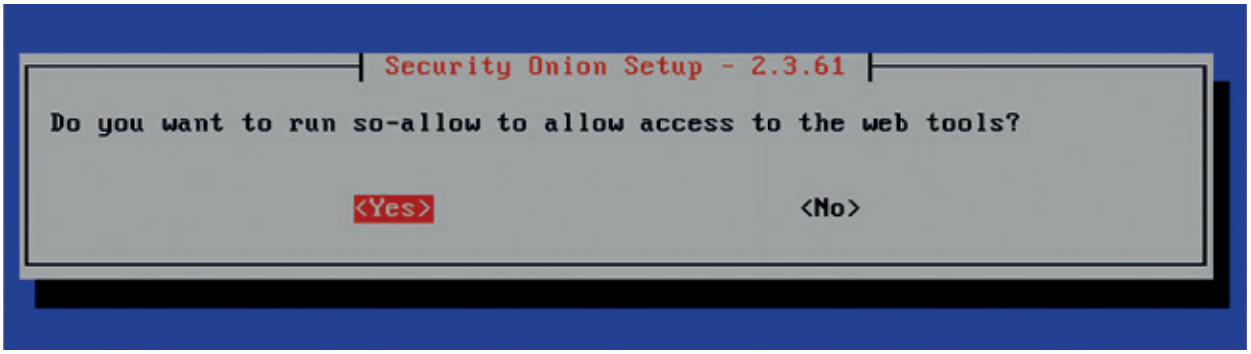
Şimdi NTP sunucu ayarlarını yapmalıyız. Logların sıhhati açısından bu ayar çok önemlidir.



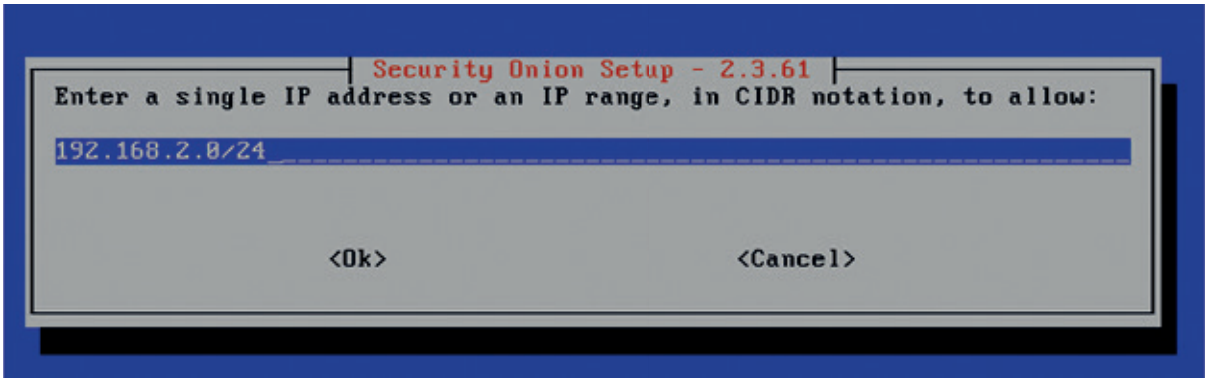
Farklı bir NTP sunucu kullanmak istiyorsanız adresini bu alana yazınız değilse varsayılan ayarlar ile devam ediniz.



Bu ekranda da Yes ile devam edelim.

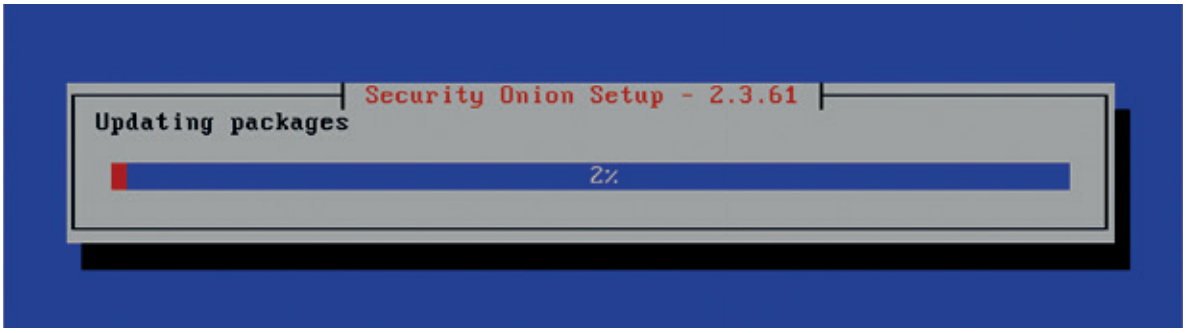


Burada makineye erişim için izin verilmiş gerekli IP adres veya subnet tanımlamasını yapıyoruz.

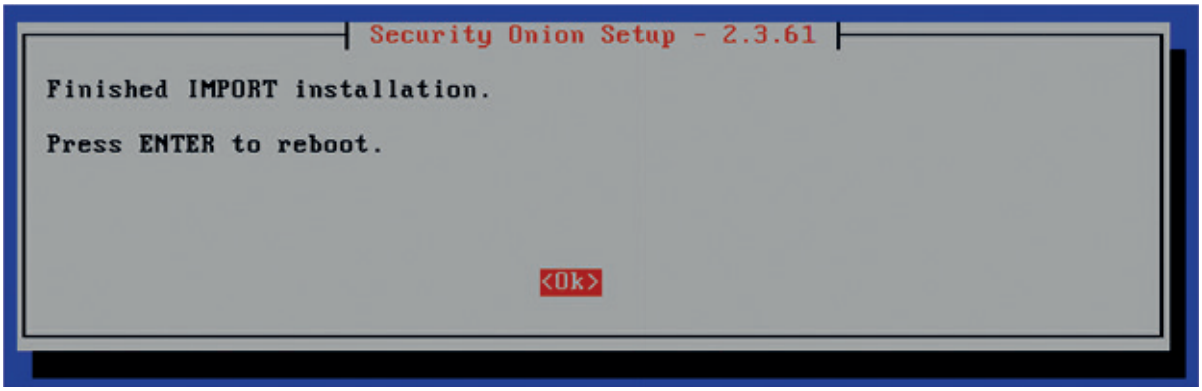


Yaptığımız ayarları bu ekranda onaylayabiliriz. Makineye ve Web arayüzüne 192.168.80.131 IP adresinden erişeceğim.

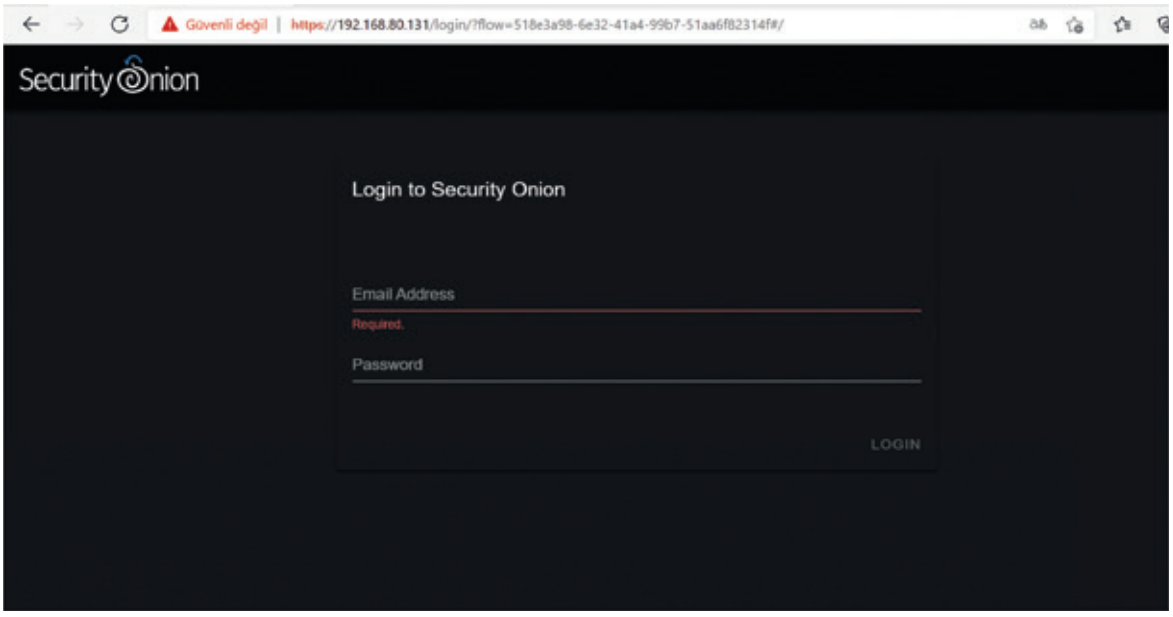
Şimdi kurulum başladı.



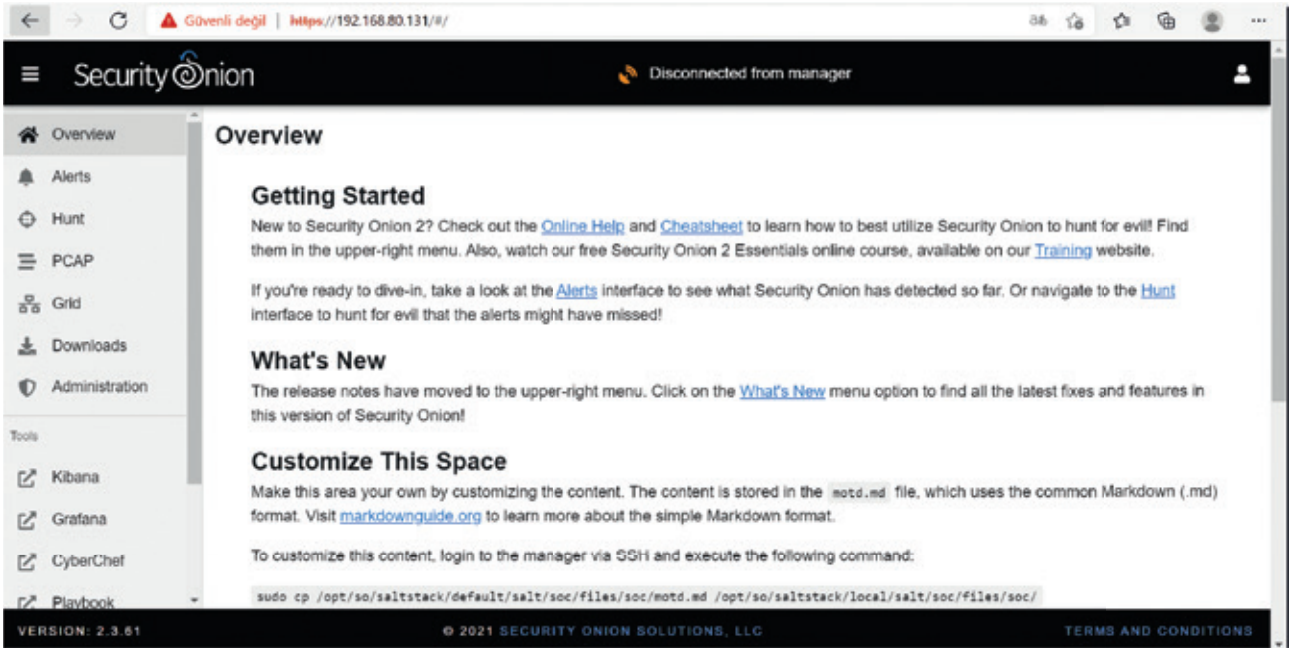
Kurulum bitiyor. Makineyi tekrar başlatmak için Enter tuşuna basıyoruz.



Makine tekrar açıldıktan sonra az önceki ekranda gördüğümüz IP adresi üzerinden belirlediğimiz kullanıcı adı ve parola ile web arayüzünden giriş yapabiliriz.



Ve Ana sayfa karşımızda



Bir sonraki yazımızda Security Onion ile gelen araçları tanımaya başlayacağız.

Mertcan Coşkuner • mcan.coskuner@protonmail.com

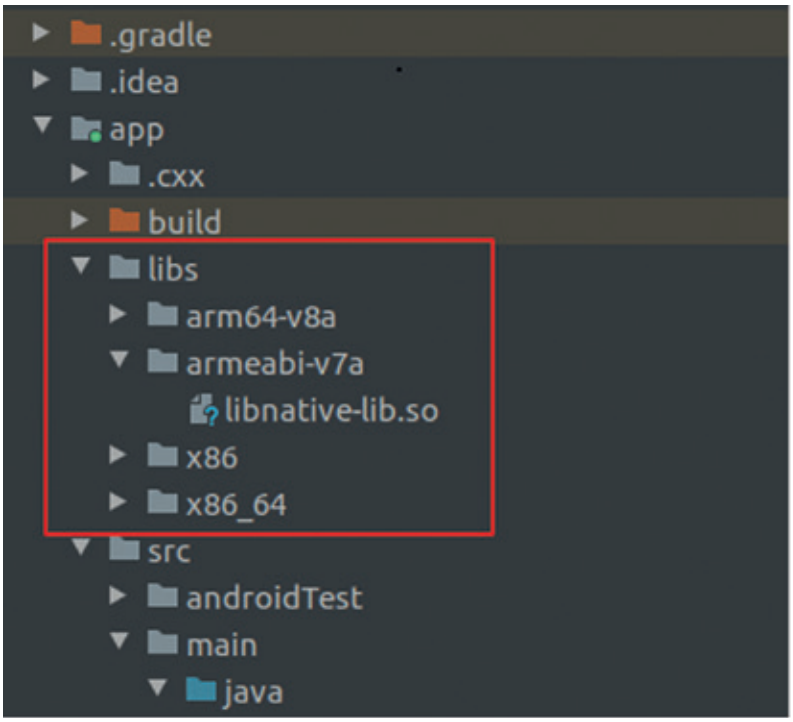
Android'de Frida Öğreniyorum - III

Android'te Frida Öğreniyorum yazı dizisinin son yazısında Frida ile native kütüphaneleri manipüle edeceğiz. İlk olarak incelemek istediğimiz herhangi bir apk içerisinde yüklenen kütüphanelere bakmamız gerekiyor. Kendiniz bir tane yazmak isterseniz, örnek bir native C kodunu aşağıda bulabilirsiniz.

```
#include <jni.h>
#include <stdlib.h>
#include <time.h>

jint Java_com_mert_test_MainActivity(JNIEnv *env, jobject this) {
    srand((unsigned int) time(0));
    int intrandom = (rand() % (990 - 101)) + 101;
    return intrandom;
}
```

C kodunu projenizin içerisine koyduğunuzda, projenizin yapısı aşağıdaki gibi görünecektir.



Kodun Java katmanındaki yansıması ise aşağıdaki gibi görünecektir.

```
...
    static {
        System.loadLibrary("native-lib");
    }

    public native int Jniint();

    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        TextView textview = findViewById(...);
        textview.setText(String.valueOf(Jniint()));
...
```

Eğer uygulama bir kütüphane kullanıyorsa, apk dosyasının içi aşağıdaki gibi gözükecektir.

```
├── AndroidManifest.xml
├── classes2.dex
├── classes.dex
├── lib
│   ├── arm64-v8a
│   │   └── libnative-lib.so
│   ├── armeabi-v7a
│   │   └── libnative-lib.so
│   ├── x86
│   │   └── libnative-lib.so
│   └── x86_64
│       └── libnative-lib.so
├── [...]
```

Tercihinize göre incelemek üzere ARM ya da x86 versiyonu kullanabilirsiniz. nm --demangle --dynamic libnative-lib.so komutu ile seçtiğiniz apk içerisindeki kütüphane detaylarına bakabilirsiniz. Komutu çalıştırdığınızda aşağıdakine benzer bir çıktı göreceksiniz.

```
$ nm --demangle --dynamic libnative-lib.so
00002000 A __bss_start
         U __cxa_atexit
         U __cxa_finalize
00002000 A _edata
00002000 A _end
```

```
00000630 T Java_com_mert_test_MainActivity
         U rand
         U srand
         U __stack_chk_fail
         U time
```

`Java_com_mert_test_MainActivity` benim seçtiğim uygulamada dikkat çeken fonksiyon. İsminden de anlayacağınız üzere, kullanıcı tarafından implement edilmiş bir fonksiyon. Hedefimiz, APK içerisindeki kod akışını değiştirmek ve buradaki fonksiyonun döndüğü değeri istediğimiz bir değerle değiştirmek olacak.

Bunu iki şekilde yapabiliriz:

1. Java kodunu hook'layarak JNI tarafına yaptığı isteği manipüle edebiliriz. Böylelikle C koduyla uğraşmayız.
2. `Java_com_mert_test_MainActivity` fonksiyonunun implementasyonunu anlamak için tersine mühendislik yapar, bulduklarımızla C kodunu hook'larız.

Önceki yazılardan da tahmin edeceğiniz üzere, ilk seçenek daha kolay. Fakat, bazı durumlarda C kodunu direkt olarak hooklamak işinize daha çok yarayacaktır. Ne yapmak istediğiniz ya da uygulamanın nasıl davrandığına bağlı olarak değişecek bu karar, pratik yaptıkça daha rahat alır hale gelebilirsiniz. Ben aşağıda sadece C koduyla alakalı olan kısmın hook kodunu göstereceğim. Android kısmını merak edenler araştırma yaparak aşağıdaki kodu Java katmanında çalışacak hale uyarlayabilir.

```
Interceptor.attach(Module.getExportByName('libnative-lib.so', 'Java_com_
mert_test_MainActivity'), {
    onEnter: function(args) {
    },
    onLeave: function(retval) {
      retval.replace(0);
    }
});
```

Kodun yaptığı adımları inceleyecek olursak:

- **libnative-lib** içerisinde **Java_com_mert_test_MainActivity** fonksiyonunu arıyor.
- Fonksiyon çalıştığında, asıl kodu eğer onEnter'da yer alan bir kod varsa onunla, çalışmayı bitirdiğindeyse onLeave'de yer alan bir kod varsa onunla değiştiriyor.

Bizim hooking kodumuza göre, `Java_com_mert_test_MainActivity` ne zaman çağırılırsa çağırılsın, çalışmayı bitirdiğinde her zaman '0 (sıfır)' dönecek.

Serinin son tavsiyesi olarak Frida ve Android tersine mühendisliğinde ilgili derinleşmek isteyenlere son önerim, r2frida (https://github.com/nowsecure/r2frida) projesine göz atmaları olacak.

Başka bir seride tekrar buluşmak üzere.

Neslihan Helvacıoğlu • sneslihanhelvacioglu@gmail.com

Broken Authentication

Sizlere bu yazımda OWASP Top 10 saldırılarında 2. Sırada yer alan Broken Authentication'ı anlatmak istedim. Umarım benim gibi bu konuları yeni öğrenen arkadaşlar için faydalı bir yazı olur. Keyifli okumalar.

Authentication

Bilgiye saniyeler içerisinde erişebilmenin ve bilgiyi saniyeler içerisinde paylaşabilmenin sağlamış olduğu kolaylık, insanlığın büyük bir dönüşüm yaşamasına neden olmuştur. Teknolojilerin hızla gelişmesi, çeşitli hizmetlerin Internet'ten verilebilir hale getirilmesi, özel kalması istenen her bilgiyi kötü niyetli kişilerden koruma ihtiyacını da beraberinde getirmiştir.

Kayıtlı olduğu web uygulaması hesabına giriş yapmak isteyen bir kullanıcı, ilk aşamada sistem tarafından doğrulama işlemine tabi tutulacaktır. Sistemin burada temel amacı; giriş yapmak isteyen kişinin gerçekten o kullanıcı olup olmadığını anlamaktır. Gerçekleştirilen bu doğrulama işlemlerinin tümüne Authentication adı verilir. Kimlik doğrulama metodları uygulamaların ihtiyaçlarına göre farklılıklar gösterebilir.

Broken Authentication nedir?

Kimlik doğrulama mekanizmasının tasarımında yer alan eksikliklerden dolayı ortaya çıkan zafiyet türüdür. Session yönetimi ve kimlik doğrulama aşamasındaki zayıflıklardan faydalanabilen bir saldırgan, kullanıcının yetkisine göre sistem içerisinde hareket edebilme imkanı yakalayabilir ve yapabilirse tüm sisteme zarar verebilecek eylemlerde bulunabilir.

Bu zafiyet otomatize araçlar ile tespit edilememektedir, daha çok manuel testler kullanılarak tespiti gerçekleştirilmektedir. Daha sonrasında otomatize araçlardan faydalanarak ilerleme sağlanabilir.

Nasıl Etkiler Doğurabilir?

- Veri ihlalleri,
- Yetkisiz Erişim,
- Hassas bilgilerin ifşası,
- Kimlik hırsızlığı,
- Kara para aklama, gibi etkiler doğurabilir.

Hangi durumlarda Broken Authentication ortaya çıkabilir?

- Kötü parola seçimine izin verilmesi,
- Ayrıntılı hata mesajları verilmesi,
- Hassas verilerin savunmasız şekilde iletilmesi,
- Brute-force saldırılarına karşı önlem alınmaması,
- Parolaların güvensiz şekilde saklanması,
- Güvensiz şekilde parola sıfırlanması,
- Zayıf session-token yönetimi,
- Kusurlu çok faktörlü kimlik doğrulama yapılarının kullanılması gibi durumlarda broken-authentication ortaya çıkabilir.

Kötü parola seçimine izin vermek:

Günümüzde kullanıcıların birçoğu kolay hatırlamak için basit parolalar kullanmayı tercih ediyor. Kullanıcıları oluşabilecek tehlikeler konusunda bilgilendirmenin yanı sıra sistemlerin de kolay parola kullanımına izin vermeyecek şekilde yapılandırılması gerekiyor. Maalesef büyük kitlelere hitap eden uygulamalar hala bu tarz önlemler almamaya devam ediyor.

Basit parola tercihleri saldırganın brute-force yaparken işini önemli derecede kolaylaştırmaktadır. Saldırgan, saldırı öncesi hedef olarak belirlediği kullanıcı hakkında detaylı araştırma ile parola tahminini güçlendirebilir.

> *Brute-force (kaba kuvvet) saldırısı, bir saldırganın sisteme deneme yanılma yöntemi ile birçok kez kullanıcı adı veya parola göndererek hedeflediği bilgiye ulaşmaya çalıştığı bir saldırı yöntemidir. Genellikle parola tespitlerinde kullanılır.*

Ne Yapılmalı?

- En az sekiz karakter uzunluğunda parola kullanılmasına izin verilmeli,
- Büyük ve küçük harfler ve rakamlar kullanılmalı,
- En az bir tane özel karakter yer almalı,
- Belirli aralıklarla parola değişimi istenmeli,
- Zayıf ve kolay tahmin edilen parolalar kara listeye alınıp, kullanımları engellenmeli.

Kullanıcı Nelere Dikkat Etmeli?

- Tekrarlanan karakterler kullanmamalı. (Örnek: AAAA,aaaa)
- Parolasında kişisel bilgilerine yer vermemeli.
- Aynı parolayı uzun süre kullanmamalı.
- Tahmin edilebilir sayı dizilerine (1234), harf dizilerine (qwerty) yer vermemeli.
- Aynı parolayı farklı uygulamalarda kullanmamalı.

Not: Kullanıcıları sıklıkla parola değiştirmeye zorlamak, daha basit parolalar tercih etmelerine neden olabilir.

Daha ayrıntılı bilgi için: https://en.wikipedia.org/wiki/Password_strength

E.N: Günümüz itibari ile 8 karakterli, karmaşık parolalar yeterli seviyede güvenli sayılmamaktadır. Güvenli bir parola için 32 karakterli, karmaşık parolalar ve parola yöneticisi kullanılabilir.

Ayrıntılı hata mesajları vermek:

Hatalı giriş yapıldığında, hatanın ne olduğuna dair ayrıntılı şekilde bilgilendirme yapılmamalıdır. Basit bir örnek olarak, kullanıcı parolasını yanlış girdiğinde "Geçersiz parola" gibi bir hata geri dönmektense, "Geçersiz kullanıcı adı ve/veya parola" gibi net olmayan hata mesajları dönmek daha yararlı olacaktır. Ayrıntılar verildiği takdirde saldırganın oturum açma işleminin her aşamasını hedef almasını sağlayarak, yetkisiz erişim elde etme olasılığı artmaktadır.

Brute-force saldırılarına karşı önlem alınmaması:

Kullanıcının belirli sayıda hatalı giriş yapmasına izin verilebilir ve deneme hakkını aşan kullanıcıya belirli bir süre erişim kısıtlaması getirilebilir. Aksi takdirde kullanıcının verileriyle beraber uygulama işleyişi de tehlikeye atılacaktır.

Tabii bazı durumlarda hesap kilitleme, işe yarar bir sonuç doğurmayacaktır.

- Saldırgan birden fazla kullanıcıda brute-force deneyerek hizmet reddine neden olabilir.
- Saldırgan var olan kullanıcı hesaplarını keşfetmek için bu saldırıyı gerçekleştirebilir. Başarısız denemelerden elde ettiği kullanıcı bilgilerini daha sonraki saldırı aşamasında kullanmak üzere liste haline getirebilir.
- İnatçı bir saldırgan, erişim engeline uğramamak için belirli bir süre bekleyip sonra denemelerine devam edebilir.

Ne Yapılmalı?

- Başarısız oturum açma girişlerini sınırlayın.
- Multi Factor Authentication kullanın.
- CAPTCHA kullanın.
- Kullanıcı hesabını tamamen kilitlemek yerine sınırlı bir şekilde kilitleme moduna geçirin.
- Logları izleyin.

Daha ayrıntılı bilgi için: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

Kimlik bilgilerinin savunmasız iletimi:

Şifrelenmemiş (SSL'siz) bağlantılar üzerinden kullanıcının hassas verileri iletiliyorsa, saldırganın konumlandırdığı dinleyici tarafından iletilen veriler okunabilir. Olası sızıntılara karşı önlem olarak hassas verilerinizi mutlaka şifrelenmiş bağlantılar üzerinden iletin. Yalnızca dışarıdan gelebilecek yabancı bir tehdite karşı değil, kendi yerel ağınızda veya varsa departmanınızın içerisinde bulunan yetkili bir kişiden/kişilerden gelebilecek tehditlerin de önüne geçmiş olursunuz.

Nasıl ortaya çıkar?

- HTTP üzerinden hassas verilerin iletilmesi,
- URL'de açık olarak iletilen hassas veriler,
- Cookie'lerde hassas verilerin saklanması.

Ne Yapılmalı?

- Web geliştiricileri, kimlik bilgileri, session token, kredi kartı bilgileri gibi hassas olan verilerin iletimini HTTP ile değil, mutlaka HTTPS ile sağlamalıdır.
- Sunucuya kimlik bilgilerini iletmek için yalnızca POST istekleri kullanılmalıdır.
- Kimlik bilgileri asla URL parametrelerine veya cookie'lere (hatta geçici olanlara dahi) yerleştirilmemelidir.
- Kimlik bilgileri hiçbir zaman yeniden yönlendirme parametrelerinde bile istemciye geri iletilmemelidir.

Parolaların güvensiz şekilde saklanması

Kullanıcılara ait parolalar veri tabanında güvensiz şekilde tutulduğunda meydana gelir. Veri tabanı ihlal edilse bile kullanıcılara ait verileri saldırganların ele geçirmesini önleyebilecek şekilde tutulması gereklidir ve bu, uygulama sahibinin sorumluluğundadır.

Zayıflık Nedenleri

- Parolaların açık şekilde (clear text) saklanması,
- Tersine çevrilebilen şifreleme algoritmaları kullanılması,
- Zayıf hash algoritması tercih edilmesi,
- Tuzlama (Salt) kullanılmaması

Saldırgan, güvenliği ihlal edilmiş diğer sitelerden elde edilen kullanıcı adı ve parola listelerinden faydalanarak, uygun sistemi kurduğunda başarılı bir kırma işlemi gerçekleştirmesi mümkündür.

Neler Yapılabilir?

- Tuzlama, temelde parolaya benzersiz, rastgele oluşturulan dize eklemek olarak geçer. Argon2id, bcrypt ve PBKDF2 gibi modern algoritmalar kullanılarak önlem alınabilir. Bu algoritmalar ek bir işlem yapmanıza gerek bırakmadan parolaları otomatik olarak tuzlarlar.

Daha ayrıntılı bilgi için: https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Güvensiz Şekilde Parola Sıfırlama:

Uygulamanın, parola sıfırlama sürecinde gerekli sıkılaştırmaları gerçekleştirmediği zaman ortaya çıkar. Örneğin;

- Başarılı bir sorgulama işleminden sonra unutulan parolanın ifşa edilmesi,
- Kullanıcı adı ve parolayı açıkça gösteren bir ileti gönderilmesi,
- Ardışık sırayla veya herhangi bir sırayla URL'ler gönderilmesi,
- Kurtarma URL'inin kullanımında zaman sınırı olmaması

Ne Yapılmalı?

- Kullanıcının kayıt sırasında tanımlamış olduğu e-posta adresine kurtarma URL'i gönderilmeli,
- Tek kullanımlık, tahmin edilemez, zaman sınırlı bir kurtarma URL'i kullanılmalı,
- Kullanıcıya parola değişikliği yapıldığını belirten bilgilendirici e-posta gönderilmeli

Zayıf Session/Token Yönetimi:

Session ve token, kullanıcıların kimlik doğrulamalarıyla ilgili bilgilerinin web uygulamasının erişim denetimle-

rine ve HTTP trafiğine bağlanmasını sağlar. Geliştirici tarafından doğru şekilde ele alınmadığında ciddi problemler ortaya çıkar.

Nasıl Oluşur?

- Session ID ifşası,
- Session'ın yakalanması,
- Tahmin edilebilen session'lara yer verilmesi,
- Brute-force ve session fixation (session sabitleme) saldırılarına yol açılması

Saldırgan uygulamada session işleyişi hakkında fikir elde edebilirse kullanıcının rolüne bürünüp oturum kaçırma saldırısı gerçekleştirebilir. Bu tür saldırılarda, saldırgan belirli bir kullanıcıyı veya yetki düzeyi yüksek bir kullanıcıyı hedef alabilir. Benzer şekilde sıradan bir kullanıcıyı hedef alarak da hareket edebilir. Saldırgan, belirlediği hedef için sosyal mühendislik, CRLF injection, Man In The Middle gibi teknikler kullanabilir.

Ne Yapılmalı?

- Session ID adı açıklayıcı olmamalı ve kimliğin amacı ve anlamı hakkında ayrıntılar vermemelidir.
- Session ID değeri saldırganın brute-force saldırılarını önleyebilecek kadar uzun olmalıdır. Uzunluk en az 128 bit olmalıdır.
- Session ID'nin tahmin edilemez olması çok önemlidir ve bunun için iyi bir CSPRNG kullanılmalıdır.
- Session ID en az 64 bit entropi değeri sağlamalıdır.
- Rastgele Session ID değerleri kullanmak yeterli değildir, kimliklerin yinelenmemesi için benzersiz olmalıdır.
- GET/POST değişkenlerinden Session ID kabul edilmemelidir.
- Şifrelenmemiş bağlantılar üzerinden Session ID iletilmemelidir.
- URL'de Session ID'ye yer verilmemelidir.
- Session ID'ler zaman aşımına uğramalı, oturum kapatıldığında veya tarayıcı kapandığında geçersiz kılınmalıdır.
- Başarılı bağlantı gerçekleştirildikten sonra yeni bir Session ID tanımlanmalıdır.
- Session fixation saldırısını önlemek için HTTPS, anti-CSRF token'ları, Cookie ve SameSite cookie flag'leri kullanılabilir.

Daha ayrıntılı bilgi için: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

Kaynaklar:

The Web Applications Hacker's Handbook

https://medium.com/shallvhack/owasp-broken-authentication-attacks-51a59bf3e5ce

https://auth0.com/blog/what-is-broken-authentication/

https://blog.eccouncil.org/most-common-cyber-vulnerabilities-part-4-broken-authentication/

https://portswigger.net/kb/issues/00300100_clear-text-submission-of-password

https://www.packetlabs.net/broken-authentication/

SİBER GÜVENLİKTE PURPLE TEAM YAKLAŞIMI İLE COBALT STRİKE SALDIRISI VE TESPİTİ

Merhaba Değerli Arka Kapı okuyucuları, bu sayıdaki yazımda sizler için biraz daha **"Purple Team"** kıvamında bir çalışma gerçekleştirmiş oldum.

Gerçekleştirmiş olduğum çalışma kapsamında;

- İlk olarak, Windows işletim sistemine sahip bir bilgisayarı **Cobalt Strike** yazılımını kullanarak ele geçirecek ve sistem içerisinde zararlı aktiviteler gerçekleştireceğim.
- Tüm bu zararlı aktiviteler sonrasında da ele geçirilmiş bir sistem üzerinde **DFIR** (Digital Forensics Incident Response) tekniklerini uygulayarak saldırının kalıntılarını tespit ediyor olacağız.

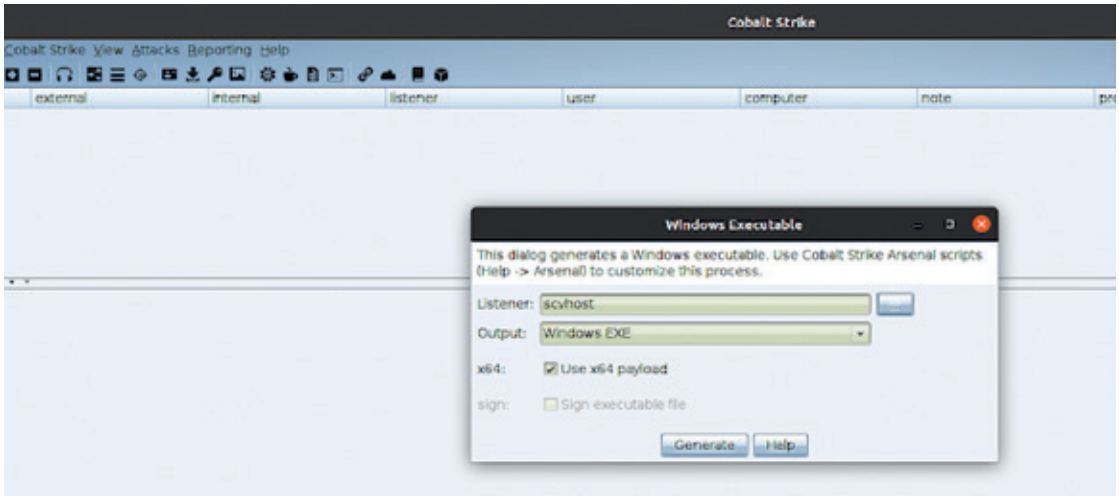
Çalışma kapsamımız anlaşıldığına göre çalışmaya koyulabiliriz :)

Saldırı Aşaması

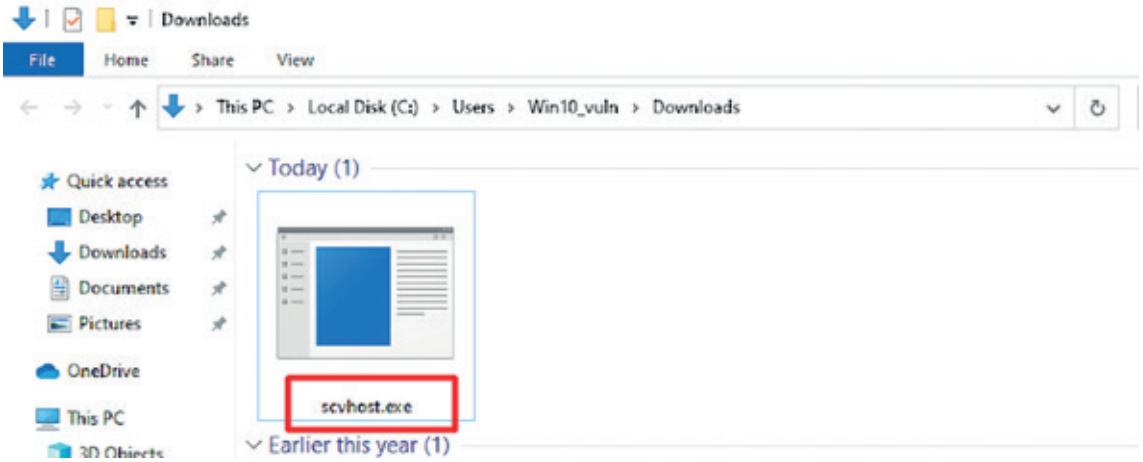
Cobalt Strike yazılımını çalıştıralım ve hedef sistem ile bizim aramızda irtibatı sağlayacak exe uzantılı bir zararlı oluşturalım. Cobalt Strike kullanarak farklı türlerde (Emetot, Windows çalıştırılabilir dosyası, web sayfası klonu, payload'lar vb.) zararlılar oluşturabilmekteyiz. Bu çalışma kapsamında Windows çalıştırılabilir dosyası oluşturarak hedef sistem üzerinde çalıştırıyor olacağız.

Çalışma kapsamının amacı zararlıyı bulaştırmak ve tespit etmek olduğundan, zararlıyı hedef sistem üzerindeki herhangi bir açıklıktan yararlanmadan direkt olarak çalıştıracağım. Bu kısımdaki senaryolar saldırganın isteğine kalmış bir durumdur. Örneğin; bir word dokümanı içerisine zararlı macro kodlarının eklenerek mail atılması ve kurbanın dokümanı açarak zararlıyı aktifleştirmesi vb. şekilde örnekler arttırılabilir.

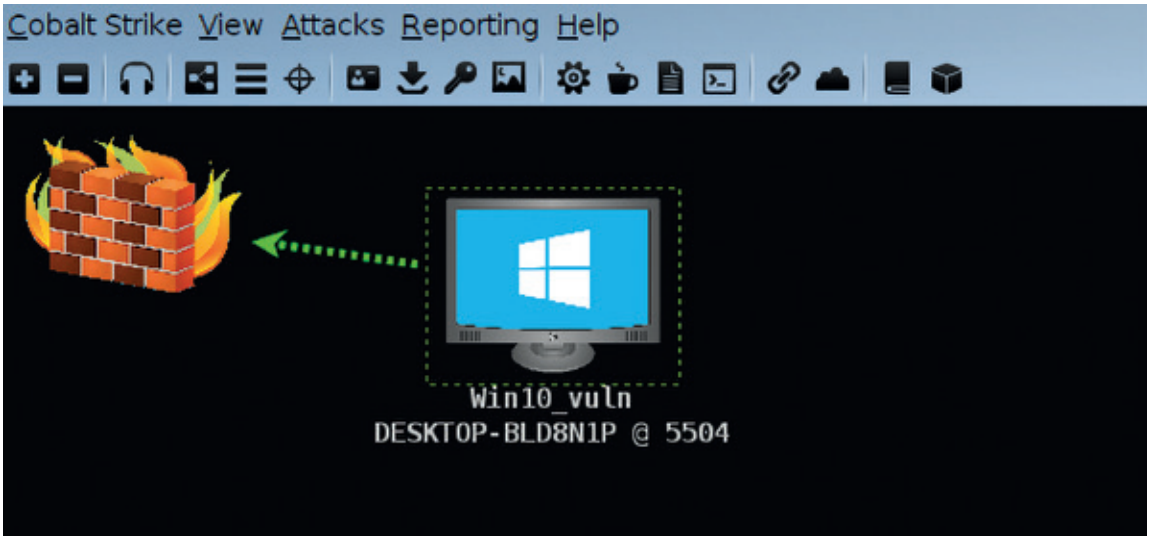
- **scvhost.exe** isimli bir zararlı oluşturalım.



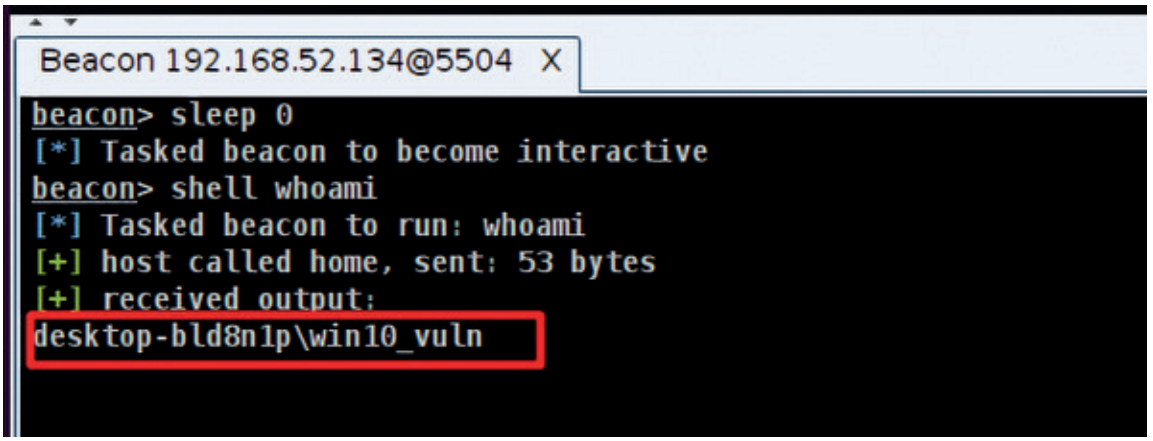
- Oluşturmuş olduğumuz scvhost.exe zararlısını hedef sistem içerisinde çalıştıralım.



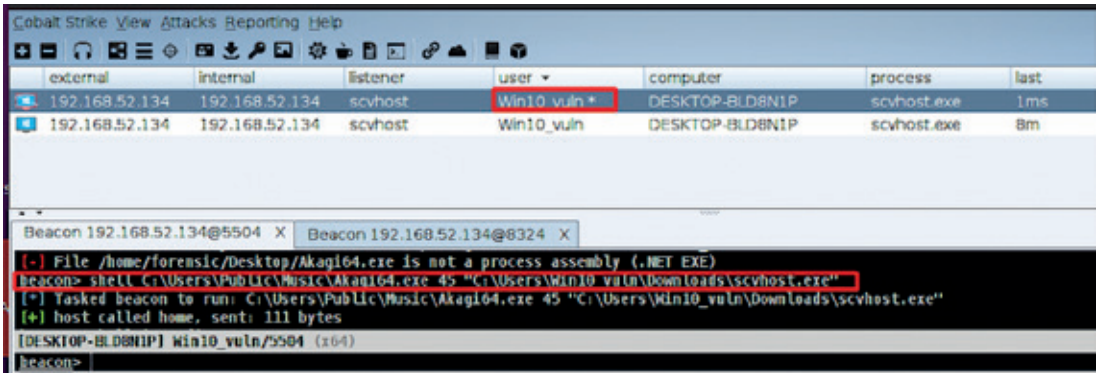
- Zararlımızı çalıştırdıktan sonra hedef sistemle aramızda bir aktif bağlantı oluştu.



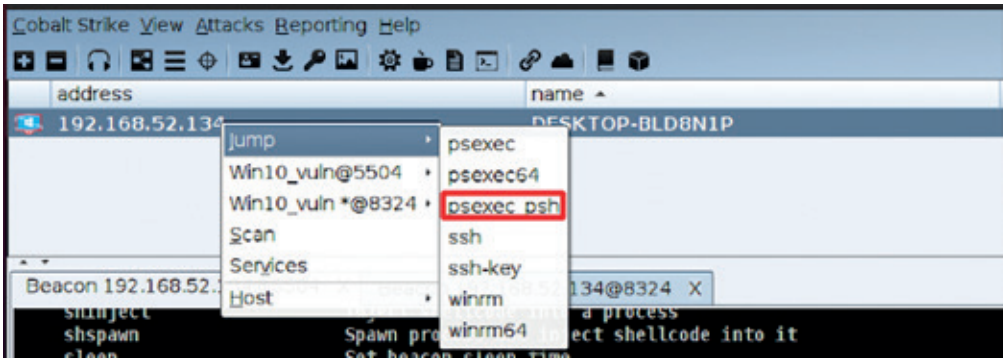
- Çalıştırma işlemini **yönetici olarak çalıştır** demeden direkt olarak çalıştırdığımız için hedef sistem ile aramızda sağlanan bağlantının yetki seviyesi oldukça düşük. Ancak hedef sistemde basit komutlar çalıştırabiliyor ve hedef sisteme dosya upload edip çekme işlemlerini gerçekleştirebiliyoruz.

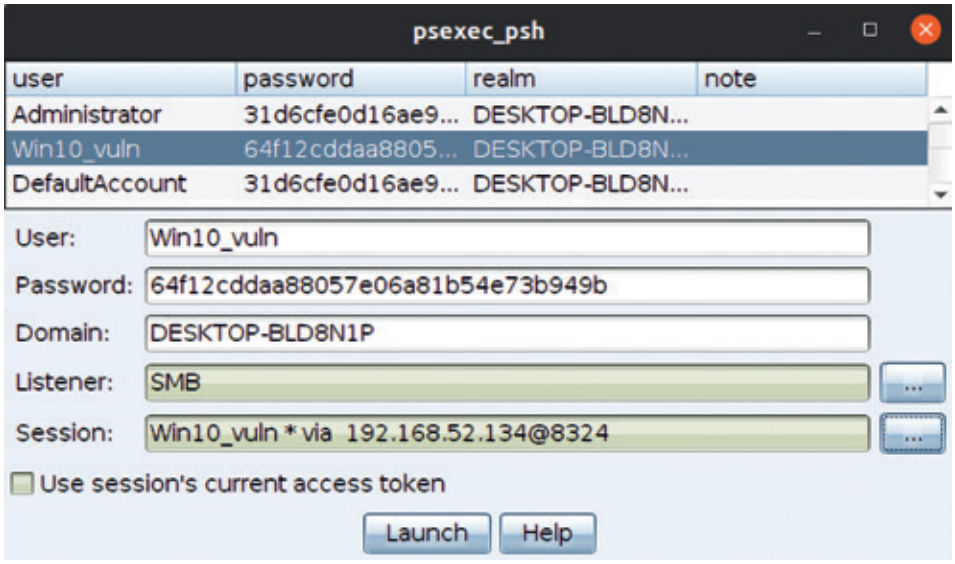


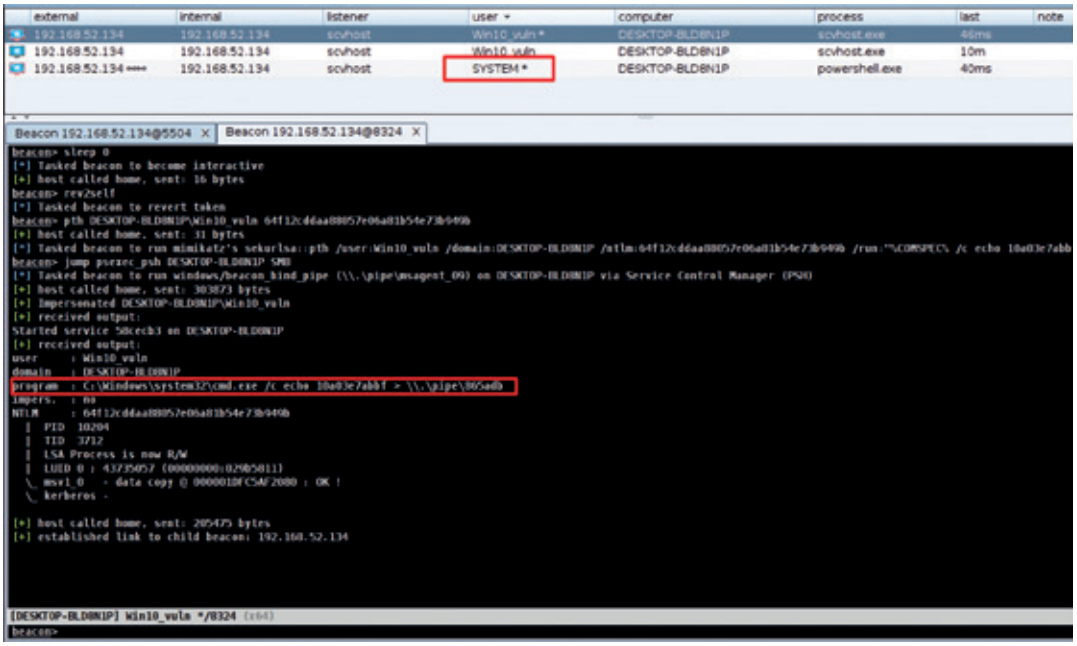
- Hedef sistemde parola bilgilerini elde etmek, zararlı aktivitelerin etkisini arttırmak ve yan hareketeler gerçekleştirebilmek için elde etmiş olduğumuz **Shell**'in yetki seviyesini arttırmamız gerekiyor. Şu anki ilk amacımız sistemde **SYSTEM** yetkisinde bir shell elde edebilmek, bunun içinde **psexec** aracından yararlanıyor olacağız. Ancak hatırlayacağınız üzere zararlımızı yönetici modunda değilde direkt normal modda çalıştırmıştık bu yüzden *psexec* aracını da kullanabilmek için öncelikle **UAC** (User Account Control) yapısını atlatmamız gerekecek. Hemen yapalım...
- Mevcut yetki seviyemizle hedef sisteme dosya yükleyebildiğimizden UAC'ı atlatmak için gerekli aracımı hedef makinenin **"C:\users\public\music"** dizinine upload ediyorum ve çalıştırıyorum.

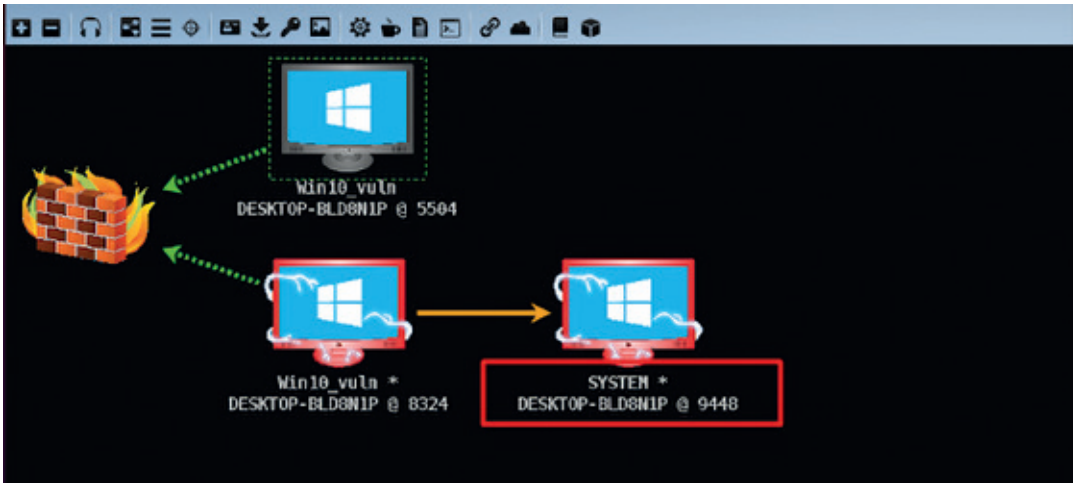


- UAC yapısını atlattık ve artık yönetici modunda istediğimiz bir aracı çalıştırabileceğimiz yeni bir shell elde ettik. Şimdiki amacımız elde etmiş olduğumuz bu shell'i kullanarak, psexec aracını çalıştırmak ve SYSTEM yetkisinde sahip yeni shell elde etmek. Hemen yapalım...

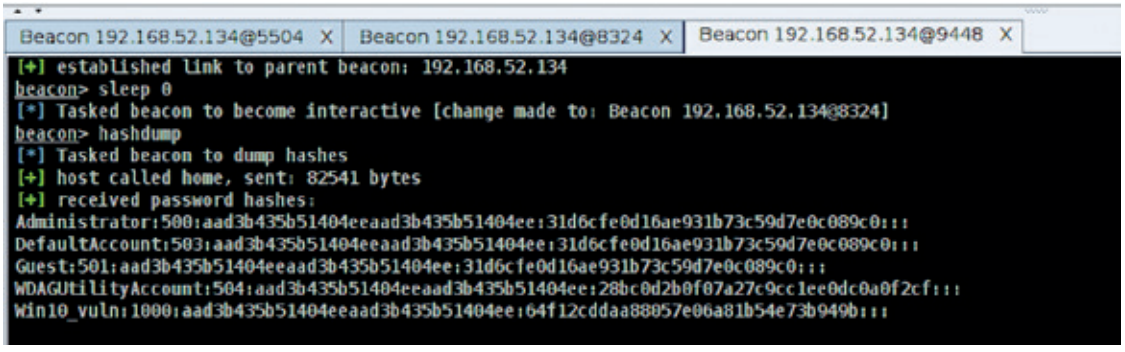


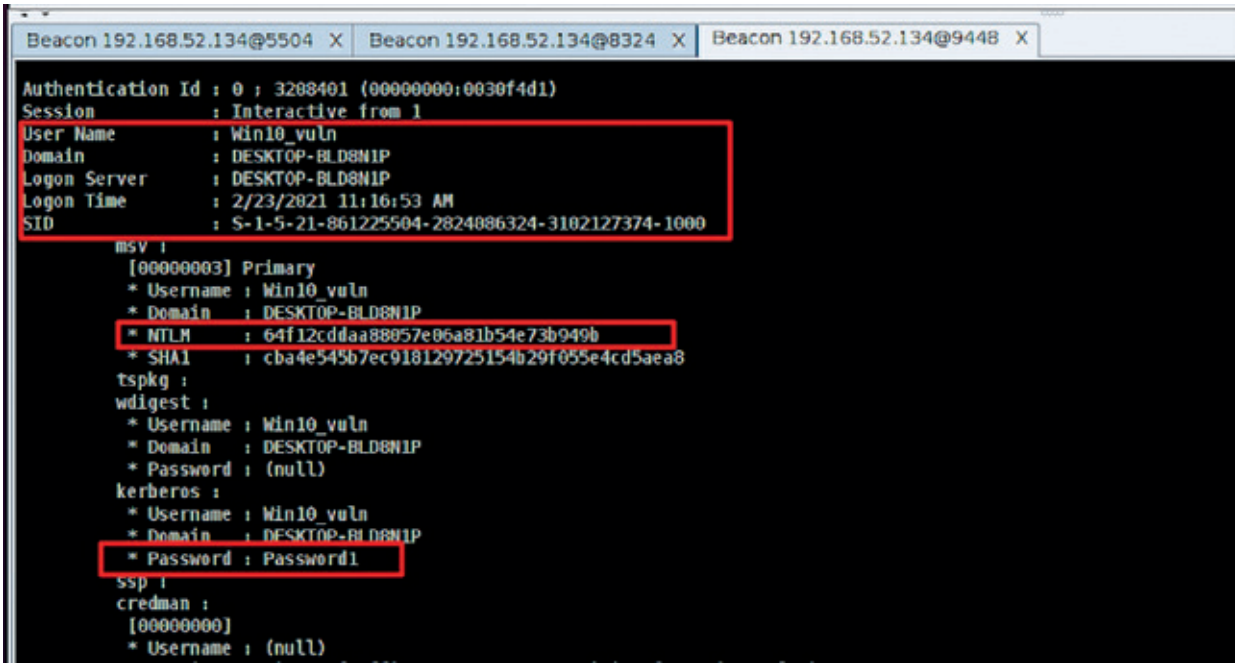




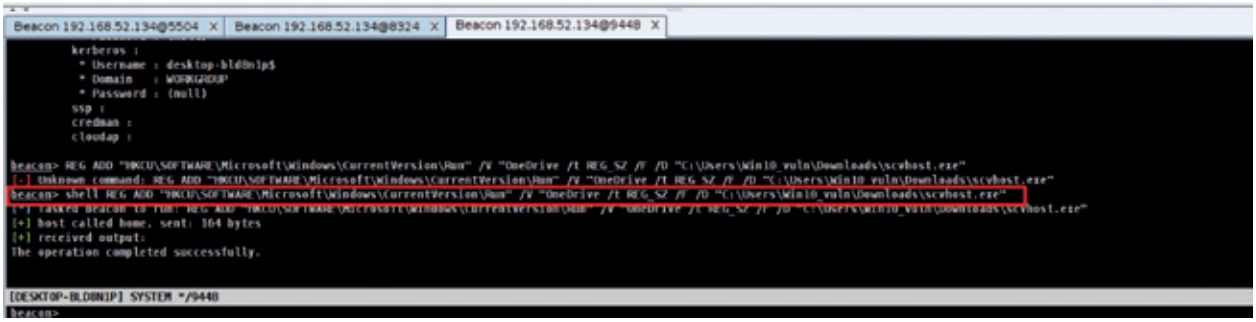


- Artık sistem yetkisinde bir shell elde ettiğimize göre içeride istediğimiz şekilde yan hareketler gerçekleştirebiliriz. Sistem içerisindeki kullanıcıların **NTLM Hash** bilgilerini görüntüleyelim ve **mimikatz** çalıştırmayı deneyelim :)





- Görüldüğü üzere artık amaçlarım doğrultusunda hareketler gerçekleştirebiliyor ve hedef sistemde yanal hareketlerimi gerçekleştirebileceğim verileri elde edebiliyorum. Bu aşamadan sonraki hareketler saldırganın keyfine kalmış bir durumdur. İster ağ içerisindeki Domain Controller'ı ele geçirmeye çalışır, ister sistemlere fidye yazılımı bulaştırır, örnekler bu şekilde çoğaltılabilir.
- Kalıcılık sağlamak amacıyla son olarak hedef sistem içerisinde **Autorun** (bilgisayar açıldığında otomatik olarak çalışan uygulamalar) kaydı oluşturalım ve artık bu aşamayı sonlandıralım :)

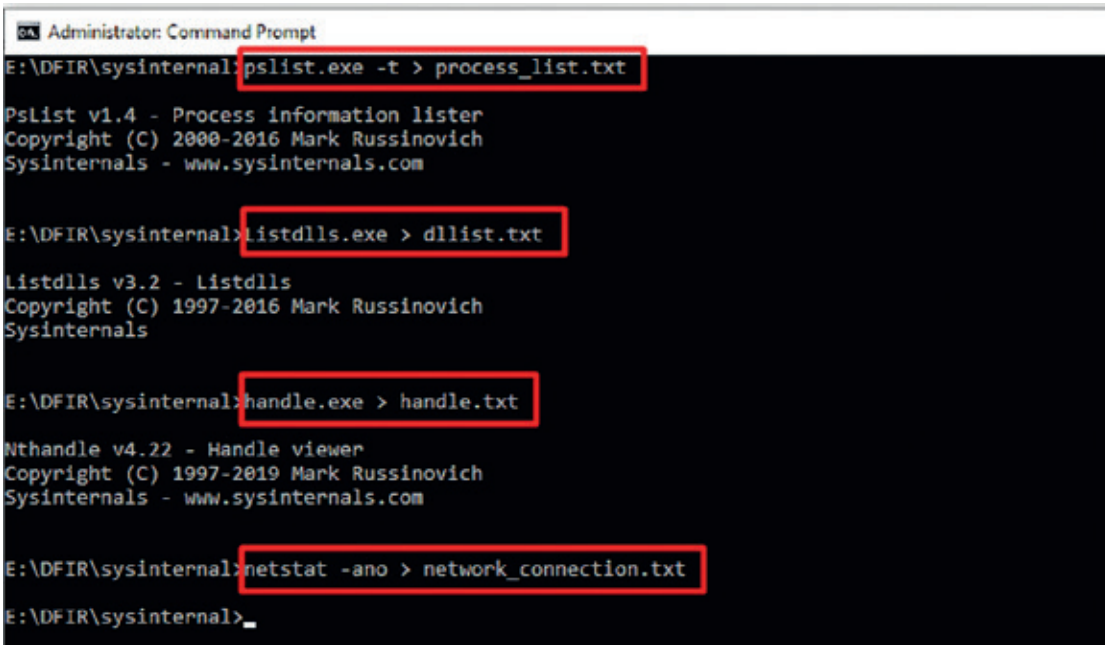


Buraya kadar saldırı yaparak hedef sistemi ele geçirmiş olduk. Şu anda bu yazıyı okuyanlar arasına kimini sadece bu aşama heyecanlandırmış olabilir, ama benim daha keyif aldığım kısım tüm bunları hedef sistemde tespit etme aşaması :) Haydi oraya geçelim...

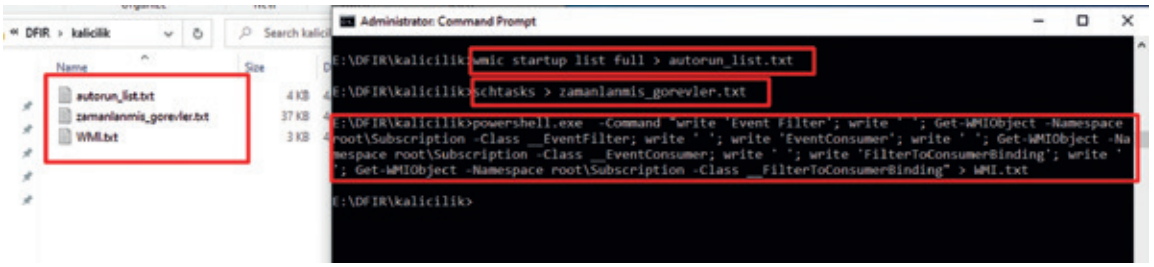
Tespit ve Analiz Aşaması

Bu aşamayı gerçekleştirirken planlı ve düzenli ilerlemek gözden kaçıracağınız noktaları en aza indirgeyecektir o yüzden olabildiğince planlı ve düzenli çalışmaya özen göstermenizi tavsiye ediyorum. Analiz kapsamında elde edeceğimiz verileri manuel olarak tek tek toplayabileceğimiz gibi otomatik açık kaynak araçlar kullanarak da veri elde etme aşamasını hızlandırabiliriz. Başlayalım...

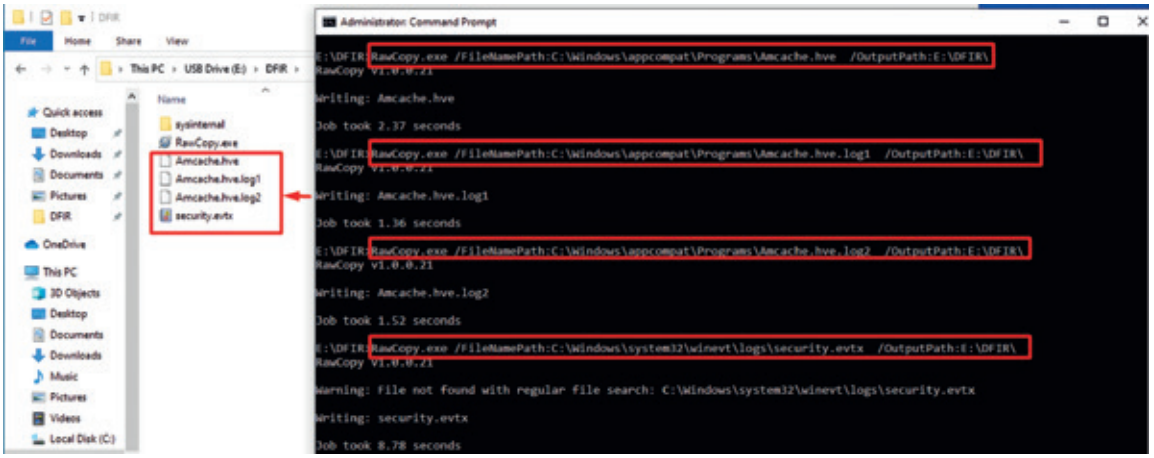
- İlk aşamada, sistem içerisindeki uçucu birkaç bilgiyi hızlıca elde edelim.



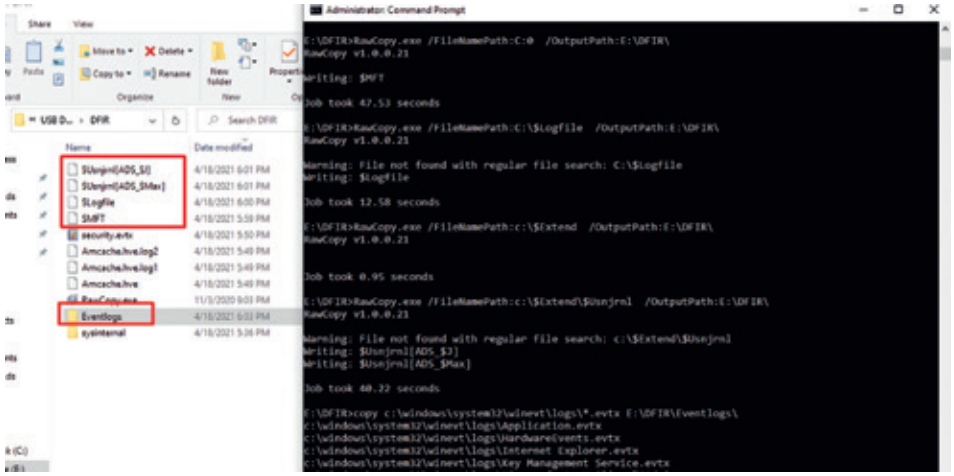
- Kalıcılık mekanizmalarının kontrolü için **WMI, Autorun ve Schtasks** (zamanlanmış görevlerin) listesini de hızlıca elde edelim.



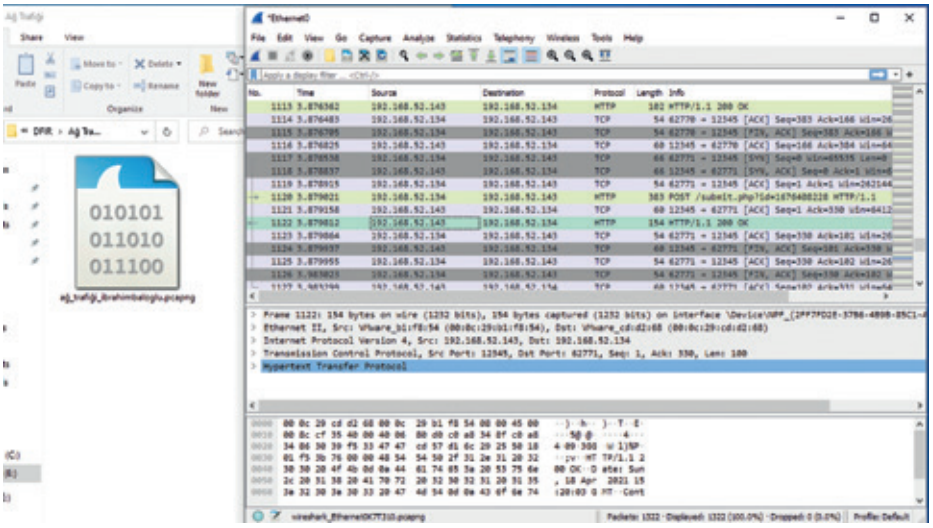
- Çalıştırılabilir uygulamalar kullanılarak ele geçirilmiş sistemlerde program çalışma geçmişlerinin elde edilebilmesi amacıyla ilk incelenmesi gereken dosyaların başında **Amcache, Shimcache** ve **Security** loglarındaki **4688** Event ID değerine sahip kayıtlar gelmektedir. Bu verileride elde edelim.



- Şimdi veri elde etme kapsamımızı biraz daha genişleterek **$MFT, $UsnJrnl, $LogFile** ve diğer Event log dosyalarını da toplayalım.



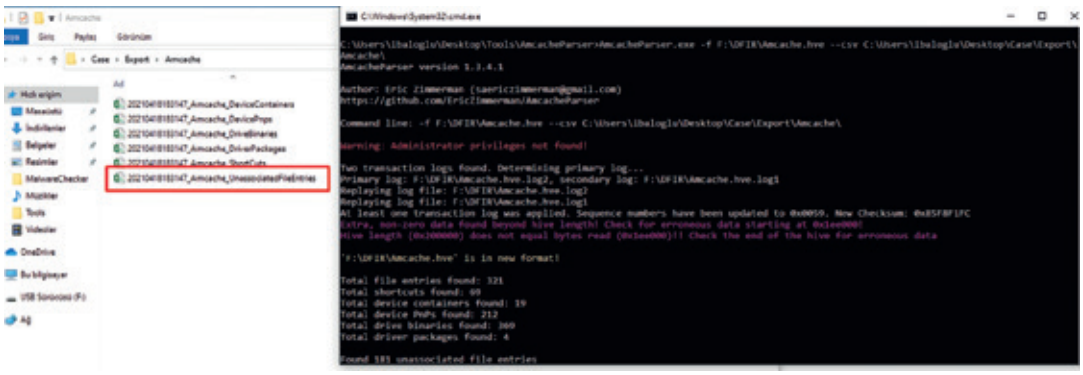
- Ağ trafiğinin belli bir süre kopyasını alalım.

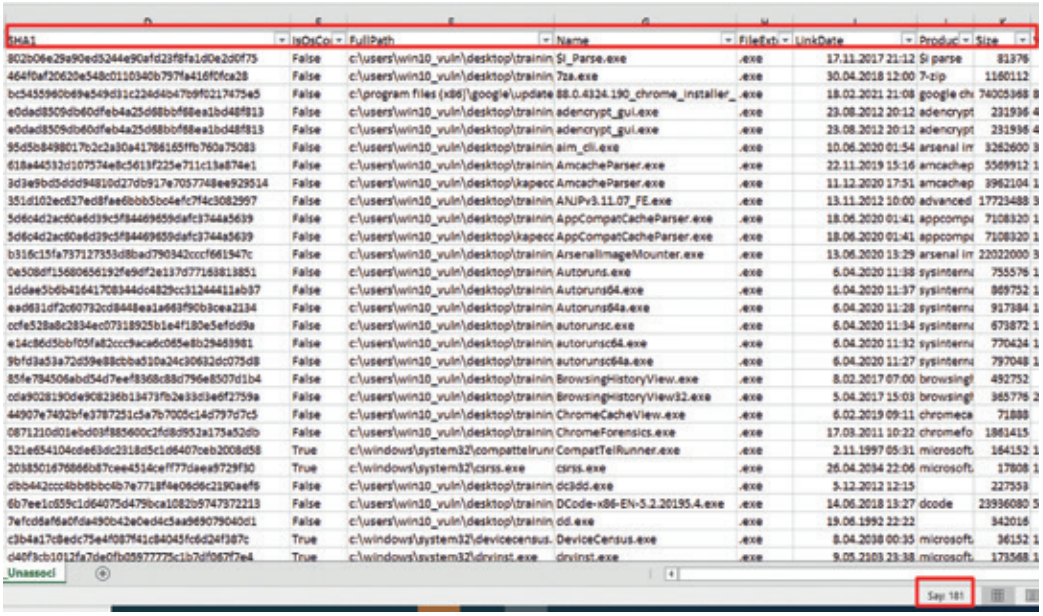


- Temel seviyede elde etmemiz gereken önemli birçok dosyayı elde etmiş olduk. Toplanacak veriler arttırabilir. Şuan için toplamış olduğumuz veriler bizim için yeterli.

Topladığımız verileri analiz etmeye başlayalım:

- Sistem içerisinde çalışan programların kayıtları için **Amcache** dosyamızı ayrıştırarak içerisindeki program çalışma kalıntılarını ve hash değerlerini elde edelim.





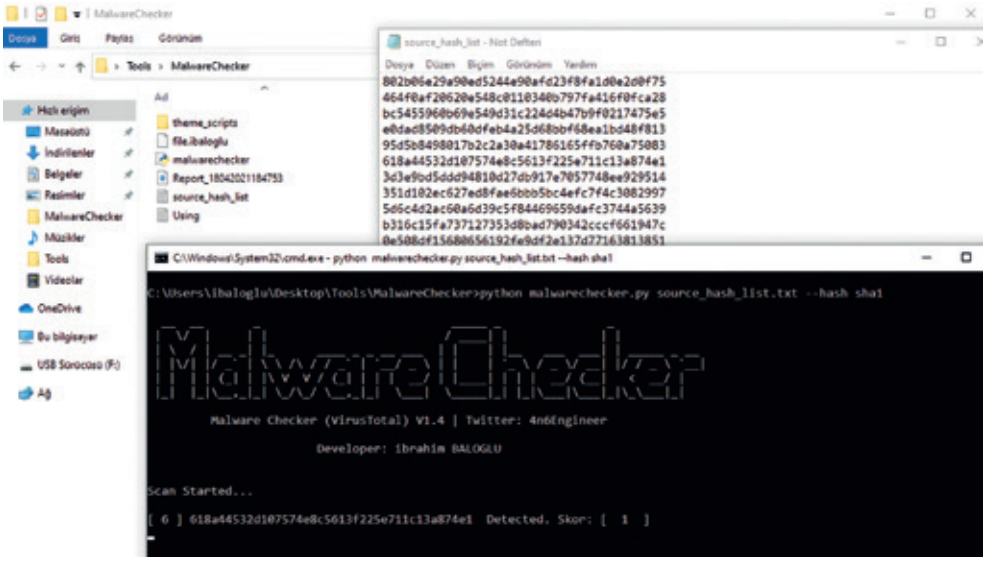
SHA1	IsOsCo	FullPath	Name	FileExt	LinkDate	Produc	Size
802b06e29e90ed3244e90afd23f8fa1d0e2d0f75	False	c:\users\win10_vuln\desktop\trainin	SI_Parse.exe	.exe	17.11.2017 21:12	SI parse	81376
464f0af20620e548c0110340b797fa416f0fca28	False	c:\users\win10_vuln\desktop\trainin	7za.exe	.exe	30.04.2018 12:00	7-zip	1160112
bc5455960b69e549d31c224d4b47b9f0217475e5	False	c:\program files (x86)\google\update	88.0.4324.190_chrome_installer_	.exe	18.02.2021 21:08	google ch	74005368 8
e0dad8509db60dfeb4a25d68bbf68ea1bd48f813	False	c:\users\win10_vuln\desktop\trainin	adencrypt_gui.exe	.exe	23.08.2012 20:12	adencrypt	231936 4
e0dad8509db60dfeb4a25d68bbf68ea1bd48f813	False	c:\users\win10_vuln\desktop\trainin	adencrypt_gui.exe	.exe	23.08.2012 20:12	adencrypt	231936 4
95d5b8498017b2c2a30a41786165ffb760a75083	False	c:\users\win10_vuln\desktop\trainin	aim_cli.exe	.exe	10.06.2020 01:54	arsenal im	3262600 3
618a44532d107574e8c5613f225e711c13a874e1	False	c:\users\win10_vuln\desktop\trainin	AmcacheParser.exe	.exe	22.11.2019 15:16	amcachep	5569912 1
3d3e9bd5ddd94810d27db917e7057748ee929514	False	c:\users\win10_vuln\desktop\kapecc	AmcacheParser.exe	.exe	11.12.2020 17:51	amcachep	3962104 1
351d102ec627ed8fae6bbb5bc4efc7f4c3082997	False	c:\users\win10_vuln\desktop\trainin	ANJPv3.11.07_FE.exe	.exe	13.11.2012 10:00	advanced	17723488 3
5d6c4d2ac60a6d39c5f84469659dafc3744a5639	False	c:\users\win10_vuln\desktop\trainin	AppCompatCacheParser.exe	.exe	18.06.2020 01:41	appcompi	7108320 1
5d6c4d2ac60a6d39c5f84469659dafc3744a5639	False	c:\users\win10_vuln\desktop\kapecc	AppCompatCacheParser.exe	.exe	18.06.2020 01:41	appcompi	7108320 1
b316c15fa737127353d8bad790342cccf661947c	False	c:\users\win10_vuln\desktop\trainin	ArsenalImageMounter.exe	.exe	13.06.2020 13:29	arsenal im	22022000 3
0e508df156806561926fe9df2e137d77163813851	False	c:\users\win10_vuln\desktop\trainin	Autoruns.exe	.exe	6.04.2020 11:38	sysinterns	755576 1
1ddae5b6b41641708344dc4829cc31244411ab37	False	c:\users\win10_vuln\desktop\trainin	Autoruns64.exe	.exe	6.04.2020 11:37	sysinterns	869752 1
ead631df2c60732cd8448ea1a663f90b3cea2134	False	c:\users\win10_vuln\desktop\trainin	Autoruns64a.exe	.exe	6.04.2020 11:28	sysinterns	917384 1
ccfe528a8c2834ec07318925b1e4f180e5efdd9a	False	c:\users\win10_vuln\desktop\trainin	autorunsc.exe	.exe	6.04.2020 11:34	sysinterns	673872 1
e14c86d5bbf05fa82ccc9aca6c065e8b29483981	False	c:\users\win10_vuln\desktop\trainin	autorunsc64.exe	.exe	6.04.2020 11:32	sysinterns	770424 1
9bfd3a53a72d39e88cbba510a24c30632dc075d8	False	c:\users\win10_vuln\desktop\trainin	autorunsc64a.exe	.exe	6.04.2020 11:27	sysinterns	797048 1
85fe784506abd54d7eef8368c88d796e8507d1b4	False	c:\users\win10_vuln\desktop\trainin	BrowsingHistoryView.exe	.exe	8.02.2017 07:00	browsingl	492752
cda9028190de908236b13473fb2a33d3a6f2759a	False	c:\users\win10_vuln\desktop\trainin	BrowsingHistoryView32.exe	.exe	5.04.2017 15:03	browsingl	365776 2
44907e7492bfe37872f51c5a7b7005c14d797d7c5	False	c:\users\win10_vuln\desktop\trainin	ChromeCacheView.exe	.exe	6.02.2019 09:11	chromeca	71888
0871210d01ebd03f885600c2fc8d952a175a52db	False	c:\users\win10_vuln\desktop\trainin	ChromeForensics.exe	.exe	17.03.2011 10:22	chromefo	1861415
521e654104cde63dc2318d5c1d6407ceb2008d58	True	c:\windows\system32\compattelrunr	CompatTelRunner.exe	.exe	2.11.1997 05:31	microsoft	164152 1
20b85016766866b87cee4514cef77daea9729f30	True	c:\windows\system32\csrss.exe	csrss.exe	.exe	26.04.2034 22:06	microsoft	17808 1
dbb442ccc4bb6bbc4b7e7718f4e06d6c2190aef6	False	c:\users\win10_vuln\desktop\trainin	dc3dd.exe	.exe	5.12.2012 12:15		227559
6b7ee1c659c1d64075d479bca1082b9747372213	False	c:\users\win10_vuln\desktop\trainin	DCode-x86-EN-5.2.20195.4.exe	.exe	14.06.2018 13:27	dcode	23936080 5
7efcd8af6a0fda490b42a0ed4c5aa969079040d1	False	c:\users\win10_vuln\desktop\trainin	dd.exe	.exe	19.06.1992 22:22		342016
c3b4a17c8edc75e4f087f41c840455fc6d24f387c	True	c:\windows\system32\devicecensus.	DeviceCensus.exe	.exe	8.04.2038 00:35	microsoft	36152 1
d40f3cb1012fa7de0fb05977775c1b7df067f7e4	True	c:\windows\system32\drvinst.exe	drvinst.exe	.exe	9.05.2103 23:38	microsoft	173568 1

Unassoci

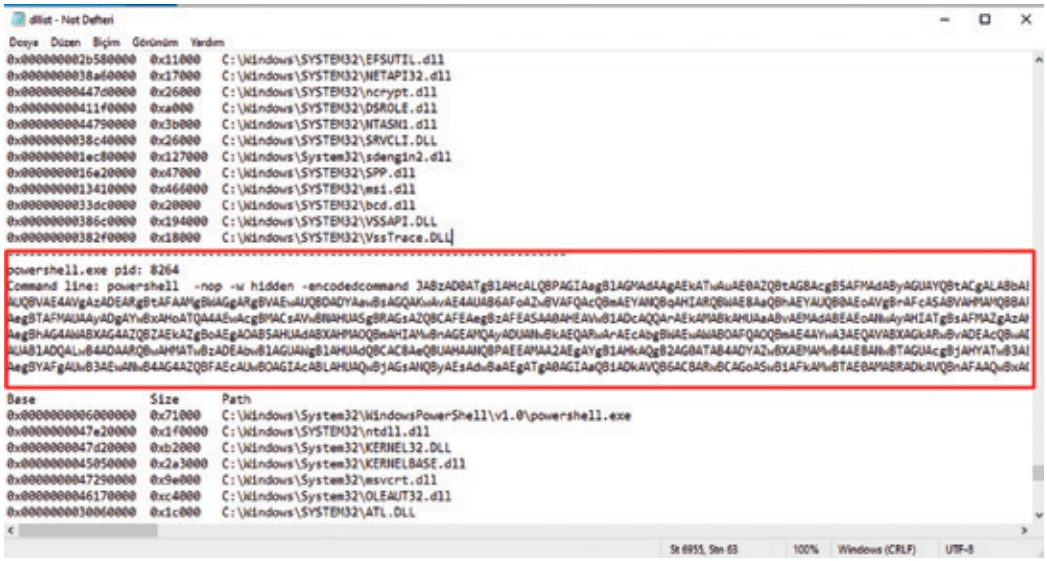
Say: 181

- Ayrıştırma sonrası toplam 181 adet kayıt olduğunu tespit ettik. (Bu sayı oldukça iyi bir oran, bunun binlerce satır olduğunu düşünün:/) **Ee peki biz bunlardan hangisinin zararlı hangisin legal kayıt olduğunu nasıl tespit edeceğiz?** Bu kayıtlar içerisindeki yer alan SHA1 hash değerleri işimizi bu noktada kolaylaştırmakta. Çünkü bir programın ismine bakarak onun zararlı olup olmadığını kesin olarak söyleyemezsiniz. Program isimleri legal Windows process'leri ile değiştirilebilir ama hash (imza) değerleri yalan söylemezler, bizler için dosyanın orjinali hakkında bilgi edinmemizi sağlamaktadırlar.

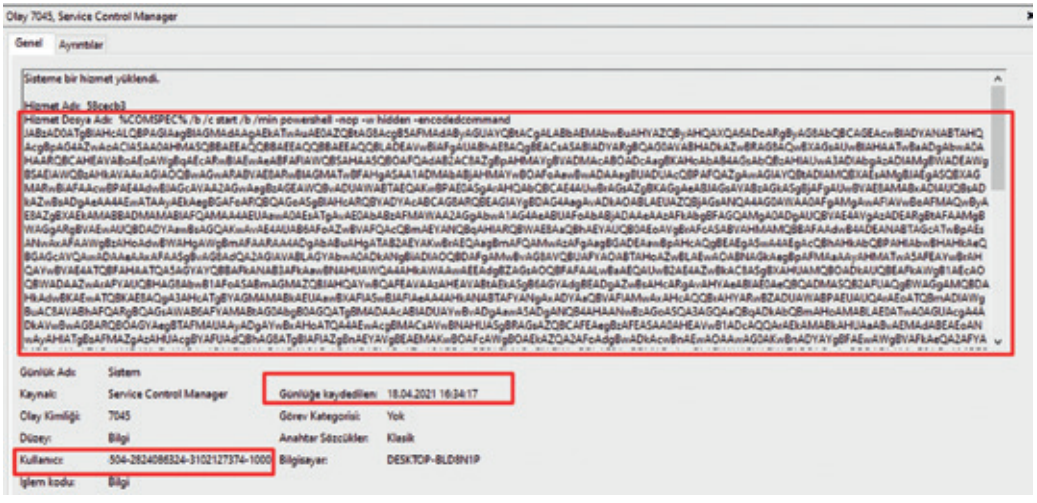
- Peki bu tüm bu hash değerlerini tek tek mi kontrol edeceğiz? Hayır tabii ki de! Bu işlemleri yaparak vakit kaybetmemek için açık kaynak olarak yazmış olduğum **MalwareChecker** (https://github.com/4n6Engineer/MalwareChecker) aracım bu işlemleri otomatik olarak yapıp bana rapor çıktısı üretecek bende oradaki çıktılara bakarak hangisi zararlı hangisi legal ayırt etmiş olacağım. Haydi yapalım...



- Sysinternal aracı ile elde etmiş olduğumuz çıktılara bir göz atalım, içerisinde dikkatimizi çeken bir şeyler çıkabilir. Dllist ile elde etmiş olduğumuz kayıtlara baktığımızda powershell.exe nin çalıştırmış olduğu ve kod karmaşıklığı uygulanmış komut dikkatimizi çekiyor.

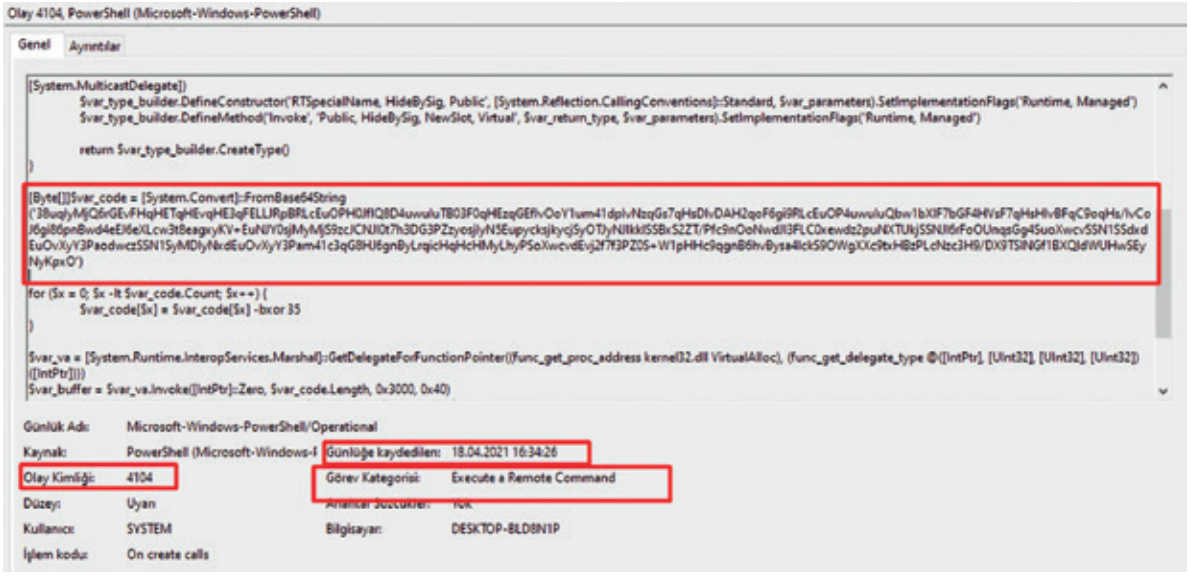


- Bu durumu teyit etmek ve ne zaman gerçekleştirildiğini tespit etmek amacıyla toplamış olduğumuz event loglarımızın içerisinde yer alan **Windows Powershell.evtx** ve **System.evtx** dosyalarını inceleyelim. Log dosyalarını incelediğimizde her iki log dosyasında da aynı kaydın yer aldığını ve bu işlemin ne zaman gerçekleştirildiğini tespit etmiş olduk.



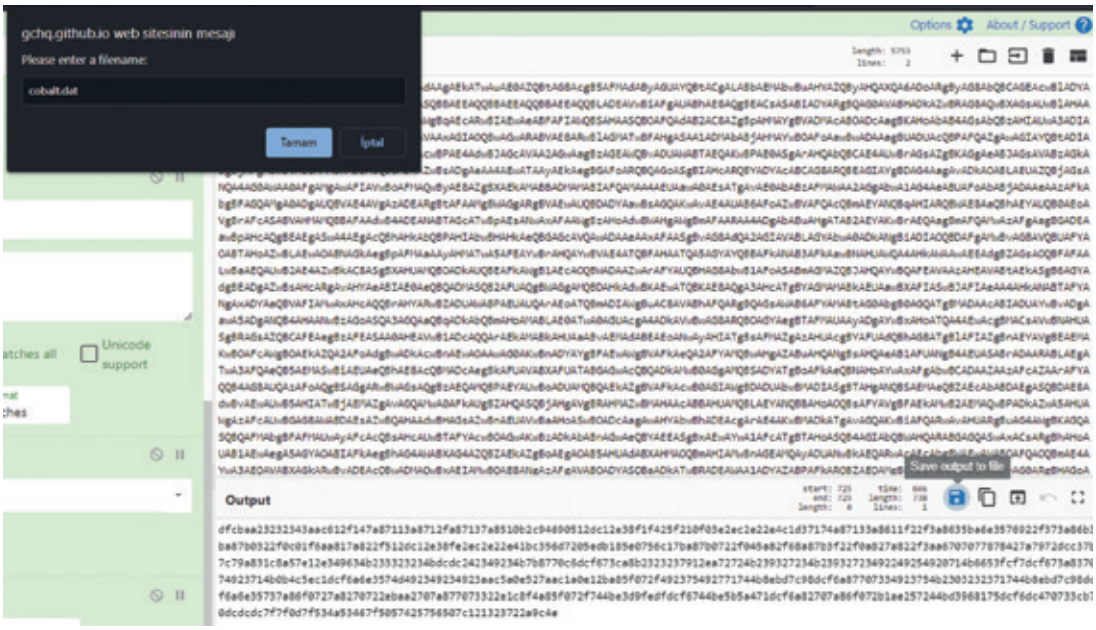
- Şimdiki amacımız bu kod karmaşıklığına son vermek ve okunabilir hale dönüştürmek. Haydi yapalım...

- Yukarıda birde fazla aşama sonunda elde ettiğimiz kod karmaşıklığının buraya kadarki bölümünü aslında **Microsoft-Windows-PowerShell%4Operational** event logu içerisinden de elde edebiliyoruz :)



- Kod karmaşıklığını birçok farklı aşamadan geçirerek ipucu elde edebileceğimiz noktayı yakalamış olduk, yukarıdaki ekran görüntüsündeki çıktı formatı Cobalt Strike ve Meterpreter tarafından kullanılan bir format olduğundan bu bilgisayarda bu ikisinden biri çalıştırılmış diyebiliyorum. Bu işlemleri yaparken de **MalwareChecker** aracımda arka planda zararlı hash tespitlerini gerçekleştiriyor, onun çıktısındaki verilerde bu durumun netleşmesinde bize fayda sağlıyor olacak. Yukarıdaki resimde yer alan kodumuz hala net değil ve kod karmaşıklığını gidermeye devam edelim.

- Kod karmaşıklığını biraz daha giderdikten sonra **"\\.\pipe\status_10"** değerini elde etmiş olduk. "\\pipe\pipe" ile başlayan bir değer elde ettiğim için komuta kontrol merkezinin SMB üzerinden gerçekleştirildiğini söyleyebiliyoruz. Şayet kod karmaşıklığı sonrası **"http://xx"** şeklinde bir yapı elde etmiş olsaydık komuta kontrol merkezinin elde etmiş olduğumuz url olduğunu söyleyebilirdik.
- Kod karmaşıklığını gidermeyi biraz daha devam ettirip, kodumuzu *.dat* dosyasına dönüştürelim ve *scdbg* aracı ile komuta kontrol adresinin çıkıp çıkmayacağına görelim.



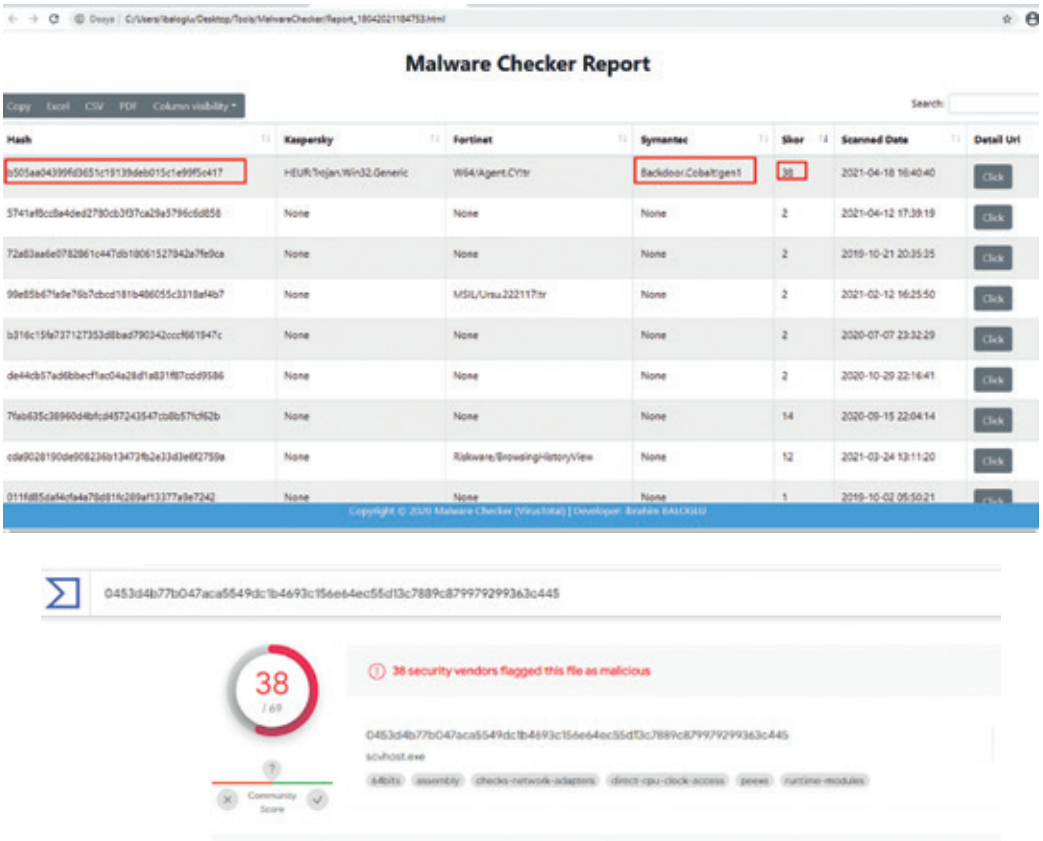
- **cobalt.dat** ismiyle kayıt etmiş olduğumuz dat dosyasını **scdbg** aracı ile kontrol ettiğimizde komuta kontrol merkezinin **192.168.52.143** olduğunu ve **12345** portu üzerinden haberleştiğini elde etmiş olduk.

```
Detected straight hex encoding input format converting...
Initialization Complete..
Max Steps: 2000000
Using base offset: 0x401000

4010a2  LoadLibraryA(wininet)
4010b0  InternetOpenA()
4010cc  InternetConnectA(server: 192.168.52.143, port: 12345, )

Stepcount 2000001
```

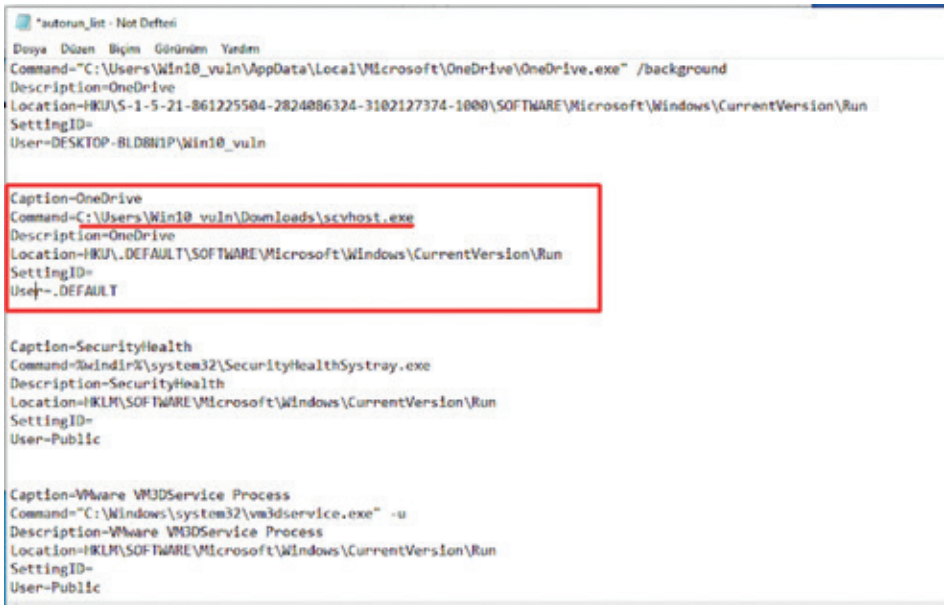
- Tüm bu işlemler sonrasında **MalwareChecker** aracının kontrolü bitti ve üretmiş olduğu raporu incelediğimde Cobalt Strike yazılımına ait bir zararlıyı tespit ettiğini görüyorum. Böylelikle bir önceki aşamada tespit etmiş olduğumuz powershell komutunun Cobalt Strike yazılımına ait olduğunu teyit etmiş olduk.



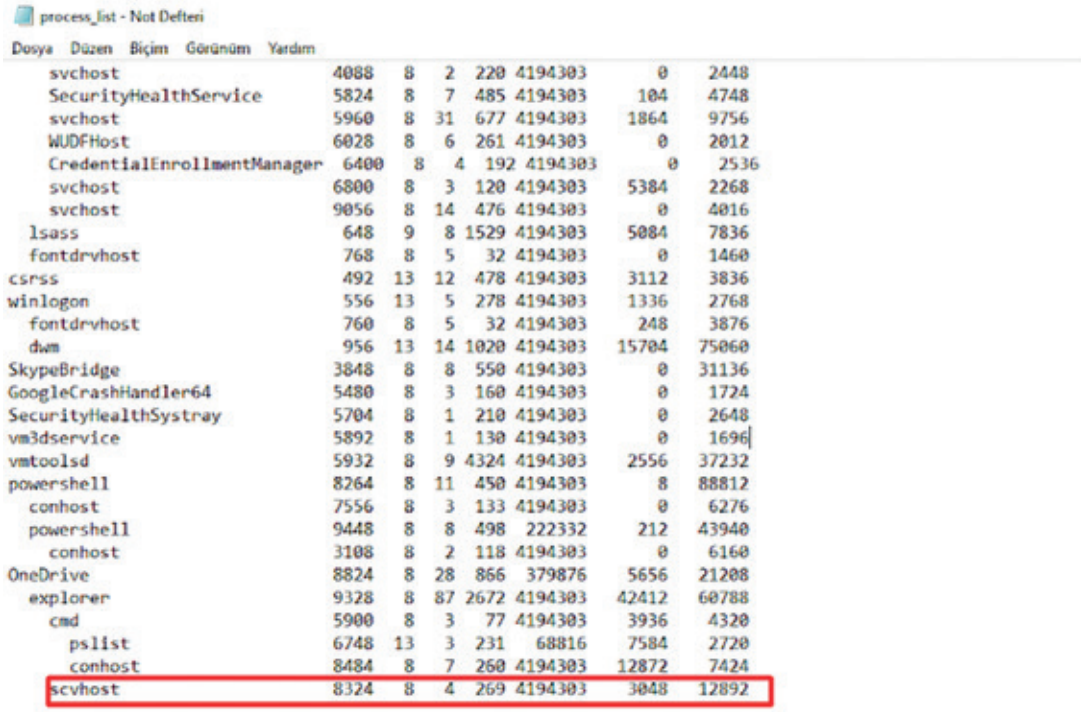
- Tespit etmiş olduğumuz hash değerini tekrar **Amcache** çıktısı içerisinde arattığımızda, hash değerinin **scvhost.exe** isimli dosyaya ait olduğunu ve çalışma tarihine ilişkin detayları elde etmiş olduk. (Zaman Dilimi: UTC)

C	D	E	F	G
FileKeyLastWriteTimestamp	SHA1	IsOsCom	FullPath	Name
18.04.2021 12:51	b505aa04399fd3651c19139deb015c1e99f5c417	False	c:\users\win10_vuln\downloads\scvhost.exe	scvhost.exe

- Kalıcılık sağlayan alanlardan toplamış olduğumuz verilerimizi incelediğimizde **scvhost.exe** isimli zararlının auto-run kayıtları içerisinde **OneDrive** ismiyle yer aldığını görüyoruz. Bu kalıcılık sayesinde bilgisayar her açıldığın scvhost.exe zararlısı da otomatik olarak başlamaktadır.

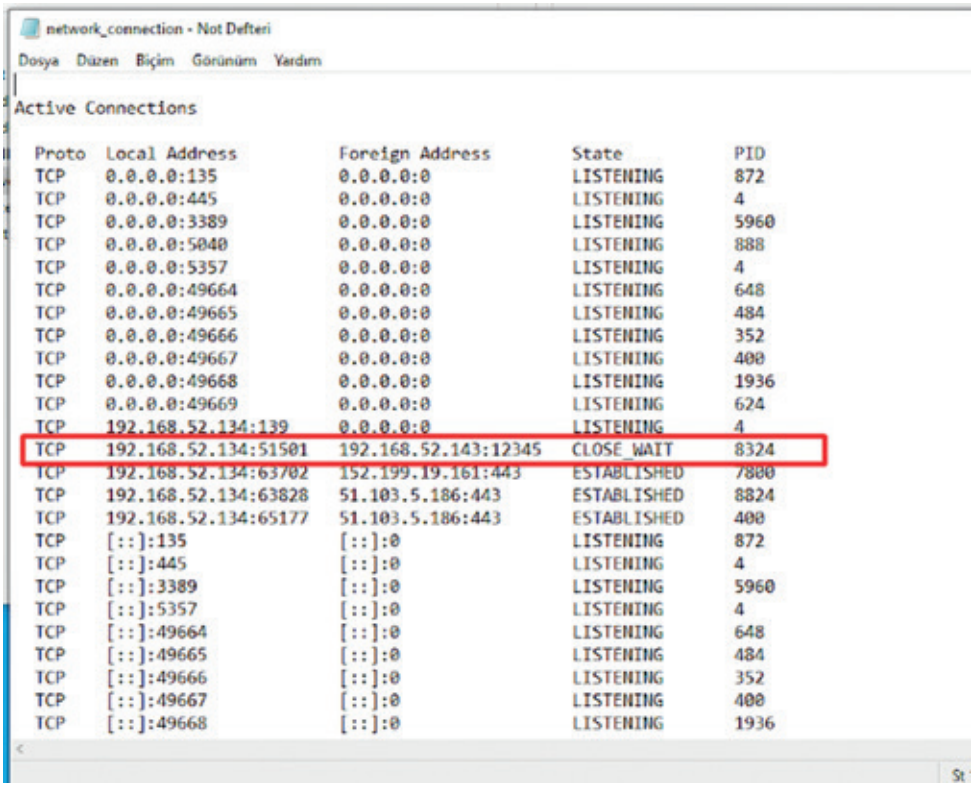


- Bilgisayara müdahale ettiğimizde scvhost.exe nin hala çalışır durumda olup olmadığını anlamak için elde etmiş olduğumuz proses çıktısına baktığımızda, zararlının aktif olarak hala çalıştığı ve 8324 numaralı PID değerine sahip olduğunu görüyoruz.

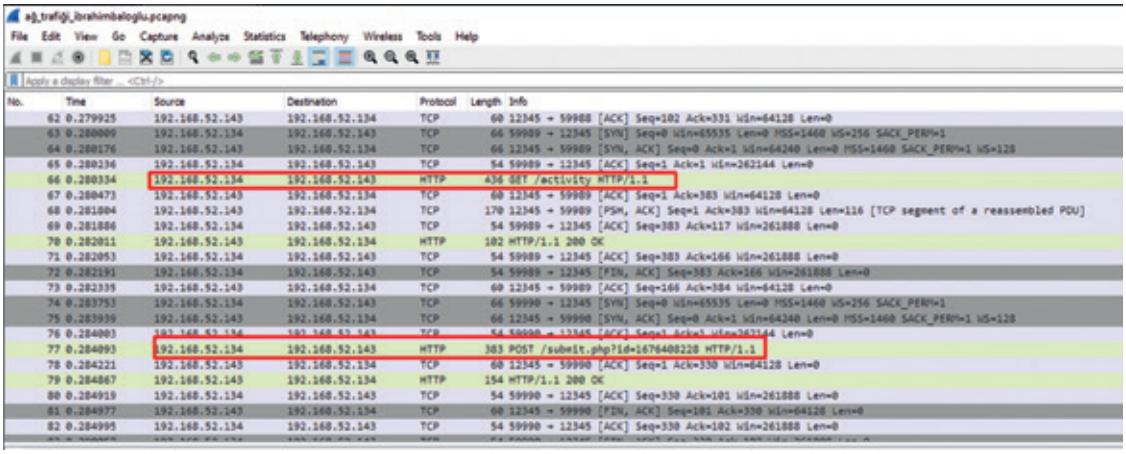


- Zararlının PID değeri ile tetiklenmiş bir aktif ağ bağlantısının olup olmadığını öğrenmek amacıyla elde etmiş olduğumuz ağ kayıtlarını incelediğimizde, **8324** PID değerine karşılık gelen bir bağlantının olduğu ve bu

bağlantının da **CLOSE_WAIT** (Sunucunun istemciden ilk FIN sinyalini aldığını ve bağlantının kapanma sürecinde olduğunu gösterir. Bu, soketin uygulamanın yürütülmesini beklediği anlamına gelir) durumunda olduğunu görüyoruz. Her zaman bu durumu yakalamak mümkün değil, şayet biz network kayıtlarını alırken **CLOSE_WAIT** durumunda olmayıp bağlantı aktif bir şekilde devam ediyor olsaydı bu kaydı burada göremeyecektik. Sonuç olarak **scvhost.exe** zararlısının **192.168.52.143** numaralı ip ve **12345** portu üzerinden haberleştiğini tespit etmiş olduk.



- Kayıt etmiş olduğumuz ağ paketlerini de incelediğimizde yine aynı ip adresiyle haberleşmenin olduğunu görebiliyoruz.



Buraya kadar çoğu kalıntıyı tepit etmiş olduk. Son olarak, scvhost.exe isimli zararlıya ait diğer detaylar için **MFT, UsnJrnl ve LogFile** dosyalarını da inceleyelim. (Zararlının hala bilgisayar içerisinde var olup olmadığı, yer almıyorsa

ne zaman oluşturulduğu ne tür değişimlere uğradığını bu dosyalar sayesinde elde edebiliriz)

- **MFT** çıktısını inceleyelim. (Zaman dilimi: UTC)

Created0x10	Parent Path	File Name	File Size	Extension
		scvhost.exe		
2021-04-18 13:29:35.8576416	.\Users\Win10_vuln\Downloads	scvhost.exe	17920	.exe
2021-04-18 13:30:18.1742926	.\Windows\Prefetch	SCVHOST.EXE-DD3B4432.pf	7785	.pf

- **UsnJrnl** çıktısını inceleyelim. (Zaman dilimi: UTC)

a column header here to group by that column

Update Timestamp	Name	Update Reasons	Extension	Entry...	Sequence ...	Pare...
	scvhost.exe					
2021-04-18 13:29:43.9695553	scvhost.exe	RenameNewName	.exe	106647	3	889...
2021-04-18 13:29:43.9695553	scvhost.exe	RenameNewName|Close	.exe	106647	3	889...
2021-04-18 13:29:44.2115890	scvhost.exe	StreamChange	.exe	106647	3	889...
2021-04-18 13:29:44.2115890	scvhost.exe	NamedDataExtend|StreamChange	.exe	106647	3	889...
2021-04-18 13:29:44.2115890	scvhost.exe	NamedDataExtend|StreamChange|Close	.exe	106647	3	889...
2021-04-18 13:29:44.2125251	scvhost.exe	NamedDataExtend	.exe	106647	3	889...
2021-04-18 13:29:44.2125251	scvhost.exe	NamedDataExtend|Close	.exe	106647	3	889...
2021-04-18 13:29:44.2135420	scvhost.exe	NamedDataExtend	.exe	106647	3	889...
2021-04-18 13:29:44.2145870	scvhost.exe	NamedDataExtend|Close	.exe	106647	3	889...
2021-04-18 13:30:09.4651706	scvhost.exe	StreamChange	.exe	106647	3	889...
2021-04-18 13:30:09.4651706	scvhost.exe	StreamChange|Close	.exe	106647	3	889...
2021-04-18 13:30:21.3228745	SCVHOST.EXE-DD3B4432.pf	DataTruncation	.pf	101375	4	865...
2021-04-18 13:30:21.3228745	SCVHOST.EXE-DD3B4432.pf	DataExtend|DataTruncation	.pf	101375	4	865...
2021-04-18 13:30:21.3228745	SCVHOST.EXE-DD3B4432.pf	DataExtend|DataTruncation|Close	.pf	101375	4	865...

- **Logfile** çıktısını inceleyelim. (Zaman dilimi: UTC+3)

_Output.xlsx | 20210418201759_MFTECmd_$J_Output.csv | NLT_LogFile_2021-04-18 23-24-06.csv

r here to group by that column

File/Directory Name	Full Path	Modified Time
scvhost.exe		
scvhost.exe	\Users\Win10_vuln\Downloads\scvhost.exe	2021-04-18 16:29:44
SCVHOST.EXE-DD3B4432.pf	\Windows\Prefetch\SCVHOST.EXE-DD3B4432.pf	2021-04-18 16:30:21

Bu blog yazısı ile **temel seviyede** bir saldırı ve bu saldırının tespitine yönelik çalışmaların nasıl olduğuna/olabileceğine değindim. İnceleme ve saldırı aşamalarındaki alanlar daha da detaylandırılmaya açıktır. Amacım, DFIR alanındaki uygulanan bazı yöntemleri siz değerli adli bilişim meraklılarına aktarmaktı. Özellikle manuel olarak yapmamızın sebebi ise neyin nerden geldiğini görmeniz içindir. Umarım keyif alarak okuduğunuz incelediğiniz bir yazı olmuştur.

DFIR Araştırma Tavsiyesi: Eric Zimmerman Tools, Sans Windows Forensic Poster, Loki Scanner, Thor Lite Scanner.

Soru, görüş ve önerileriniz olması durumunda iletişim formundan veya sosyal medya hesaplarım üzerinden bana ulaşabilirsiniz.

Sevgilerle.

Ziyahan Albeniz • ziyahanalbeniz@gmail.com

TAKLİT ASLINA ÖVGÜDÜR:

DEVİCE SPOOFING'E DAİR GÖZDEN KAÇAN AYRINTILAR

Konuşmacı olarak davet edildiğim CloudTalk 2021 konferansına **Alice and Bob Tarayıcıların Harikalar Ülkesi'nde** sunumumla katılacağım için çok heyecanlanmıştım. Yeni bir saha olarak girdiğim device fingerprint, özellikle de browser fingerprint alanına dair ufak ufak not ettiğim, kesin sonuç almak için olmazsa olmaz püf noktalarını paylaşmak için sabırsızlanıyordum.

Moderatörün son beş dakikanız kaldı ihtarıyla birlikte, toplam 10 dakika olan konuşma süremde konuları nasıl toparlayacağımı düşünüp, hızlıca devam ettim. Şehirler arası yolculuk yapanlar hatırlayacaktır, bir mola yerine varılır, öncelikle kimi ihtiyaçlar görülür, en sonda da açlığın çaresine bakılır. Sipariş edilen bir yemek, mutfakta biraz geciktiyse, nefis kokularıyla önünüze konduğunda birkaç lokma ile kifayet etmek zorunda kalır, sofradan boynu bükük kalkarsınız. Sofradaki o güzelim yemek de ebeveynlerimizin tabiriyle "arkamızdan ağlar"

Neyse ki Arka Kapı Dergi'de bize tahsis edilecek birkaç sayfa boyunca, o günkü konuşmada ayrıntılarına giremediğim, belki layıkıyla katılımcılara aktaramadığım pek çok konuyu paylaşma şansı bulacağım.

Neden device spoofing'e ihtiyaç duyarız?

İlk cevaplanması gereken sorunun bu olduğunu düşünüyorum. Neden device spoofing'e ya da başka bir cihazı taklit etmeye ihtiyaç duyarız?

Buna verebileceğim ilk cevap, mesleki dezenformasyon gereği, güvenlik perspektifinden olacak.

Farklı türde cihazlar kullanıyoruz. Kâh ekonomik durumumuz, kâh mensubu olduğumuz kurum ve kuruluşlar, kâh yaptığımız işten ötürü farklı cihazları tercih ediyoruz. Ekonomik durumumuz yeterli ise daha üst segmentlerde teknolojik cihazları kullanıyoruz örneğin. Hizmet sağlayıcılar daha fazla kişiye hitap edebilmek için daha fazla cihazı desteklemek için büyük yatırımlar yapıyorlar.

Örneğin büyük bir sektöre dönüşen dijital video yayıncılığı, her türlü internet bağlantı hızı ve cihaza, ekran çözünürlüğüne yönelik içerikler hazırlıyorlar. Tasarımcılar, farklı ekran görünümleri için dizaynlar yapıyorlar. Akıllı televizyonunuzda bulunan tarayıcıdan internete eriştiğinizde, bağlandığınız cihazın akıllı televizyon olduğunu anlayan reklam ağları, bu cihazda kullanabileceğinizi düşündükleri içerik üreticilerinin reklamlarını göstermek istiyor. Scientia Mobile firması örneğinde görebileceğimiz gibi müşterilerine, web sayfalarına bağlanan cihazların üretim yılı ve piyasa fiyatını dahi söyleyen bir hizmet sunuyorlar. Zengin kullanıcıları doğrudan hedeflemek için birebir :=)

Güvenlik perspektifinden bakışımızın sonucunu şöyle özetleyebilirim, bunu güvenlik uzmanları zafiyet bulmak için bir önerme olarak düşünebilir: Her ne kadar büyük mühendislik yatırımları söz konusu olsa da, bir cihaz için pekala iyi tasarlanan güvenlik hassasiyetine, başka bir cihaz için önem verilmiyor olabilir.

Hemen bir örnek verelim: Pek çok büyük servis sağlayıcının normal web sitelerinde bulunmayan güvenlik zafiyetleri mobil cihazlar için tasarladıkları versiyonlarında bulunabiliyor. Bunun esas sebebi ise şu, bu işin mühendislik tarafındaki akıl risk ölçümünü saldırganlara göre değil, bu tasarımın ya da uygulama versiyonunun hitap ettiği cihazların kapasitesini düşünerek yapıyor.

"Nasıl olsa mobil tarayıcıda developer toolbar'ı açamayacaklar" varsayımıyla, uygulama akışında kritik öneme sahip bir veriyi cookie ya da bir Javascript değişkeninde saklayabileceklerini düşünüyorlar.

Cihazları taklit etmeyi güdüleyen bir başka neden de bazı şirketlerin X türü bir cihazdan erişimlere öncelik ya da limitli erişim sunması. Firmaların mobil cihazlardan erişimlere özel bir indirim kuponu sağladığını düşünelim. Bu şartlar altında neden bir mobil cihazı tercih ya da taklit etmeyesiniz?

Buraya kadar hep bir özne olarak kullanıcıları, yani gerçek insanları konuştuk. Bir de internet trafiğinin yüzde 40'ına tekabül eden botlar var. Bu botların kimisi -arama motoru botları örneğin- gayet meşru bir amaca hizmet etse de alışveriş botları, ticket botları, sneakers botları gibi sistem yöneticilerinin sistemlerinden uzak tutmak istediği botlar da var. Bu botlar da sistemlere sorunsuz erişebilmek için normal bir kullanıcı davranışını, dolayısıyla normal bir tarayıcı davranışını taklit etmek zorundalar

Sıfırıncı Kural: Javascript render kapasitesi

Javascript hayatımıza 1994'de girdi. İlk zamanlarda sadece web sayfalarını şenlendirmek, mouse imlecinin peşinde sürüklenen yıldızlar, kayan yazılar için kullanılsa da 2000'li yılların başında AJAX yani asenkron istekler kavramıyla web'e yeni bir soluk getirdi. Bugün backend dünyasında da hatırı sayılır bir yere sahip olan Javascript en çok tercih edilen yazılım dilleri arasında.

Bugün bütün tarayıcılar Javascript render etme, yani Javascript kodunu çalıştırabilme beceresine sahip.

Python ile yazdığınız bir scraping botu (Eğer Selenium ya da Puppeteer gibi bir automation framework'u kullanmıyorsanız), CURL ile yaptığınız istekler Javascript kodu render edemeyecekler. Dolayısıyla primitive yani ilkel botların neredeyse tamamını client'ın Javascript render kabiliyetiyle yakalamak mümkün. E peki nasıl olacak? Bugün front end dünyasında yaygın olarak kullanılan Javascript frameworkler, Single Page Application'lar bu ilkel botlar için, yani Javascript çalıştırabilme kapasiteleri olmadığı için, bu botlara hiçbir anlam ifade etmeyecek.

Ayinesi iştir kişinin lafa bakılmaz: User-Agent String'i

Tarayıcı fingerprint alanında çalıştığımı duyan hemen herkes *"biz o işi User-Agent string'ini değiştirerek yapıyoruz"* tepkisini veriyor. Tabii kazın ayağı öyle değil. Cevaben söylediğim gibi, bu bilinen en basit ve tespit edilmesi en kolay yöntem.

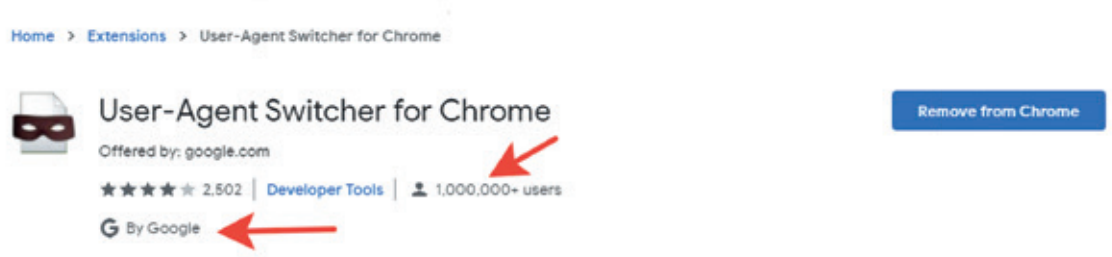
User-Agent string'i web'in neredeyse ilk günlerinden beri hayatımızda olan bir parametre. HTTP istekleriyle birlikte gönderilen bu değer kullandığımız tarayıcının kimliğini, versiyon numarasını, işletim sistemimiz gibi bilgileri sunuculara bildiriyor.

Peki ama neden bunu yapıyor? Bu tarayıcı savaşları olarak bilinen döneminden yadigar bir alışkanlık. Microsoft, Netscape gibi tarayıcı üreticileri kavgaya tutuşlarında bu ticari kavganın yansımaları tarayıcıların yoğurt yiyişlerini de yansıdı. Her firmanın tercih ettiği farklı render etme yöntemleri web sitesi sahipleri için bir kabusa dönüştü. Dolayısıyla *"siz ne halt ederseniz edin, bana yaptığınız isteklerde hangi tarayıcı olduğunuzu söyleyin gerisini biz hallederiz"* demekte çareyi buldular. Bugünden bakılınca sisli ve karanlık gözüken o yıllarda web site yöneticileri User-Agent ile gelen tarayıcı kimliğine göre o tarayıcının desteklediği web sitesi kopyasını servis ediyordu.

```
GET / HTTP/1.1
Host: example.com
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en
```

Bir HTTP isteğindeki örnek bir User-Agent stringi görünümü.

Bu stringi değiştirmek, evet kolay. Bu amaç için tasarlanmış pek çok tarayıcı eklentisi mevcut. Örneğin Google(!) tarafından tavsiye edilen, yaklaşık 1 milyon kullanıcısı bulunan User-Agent Switcher for Google eklentisi

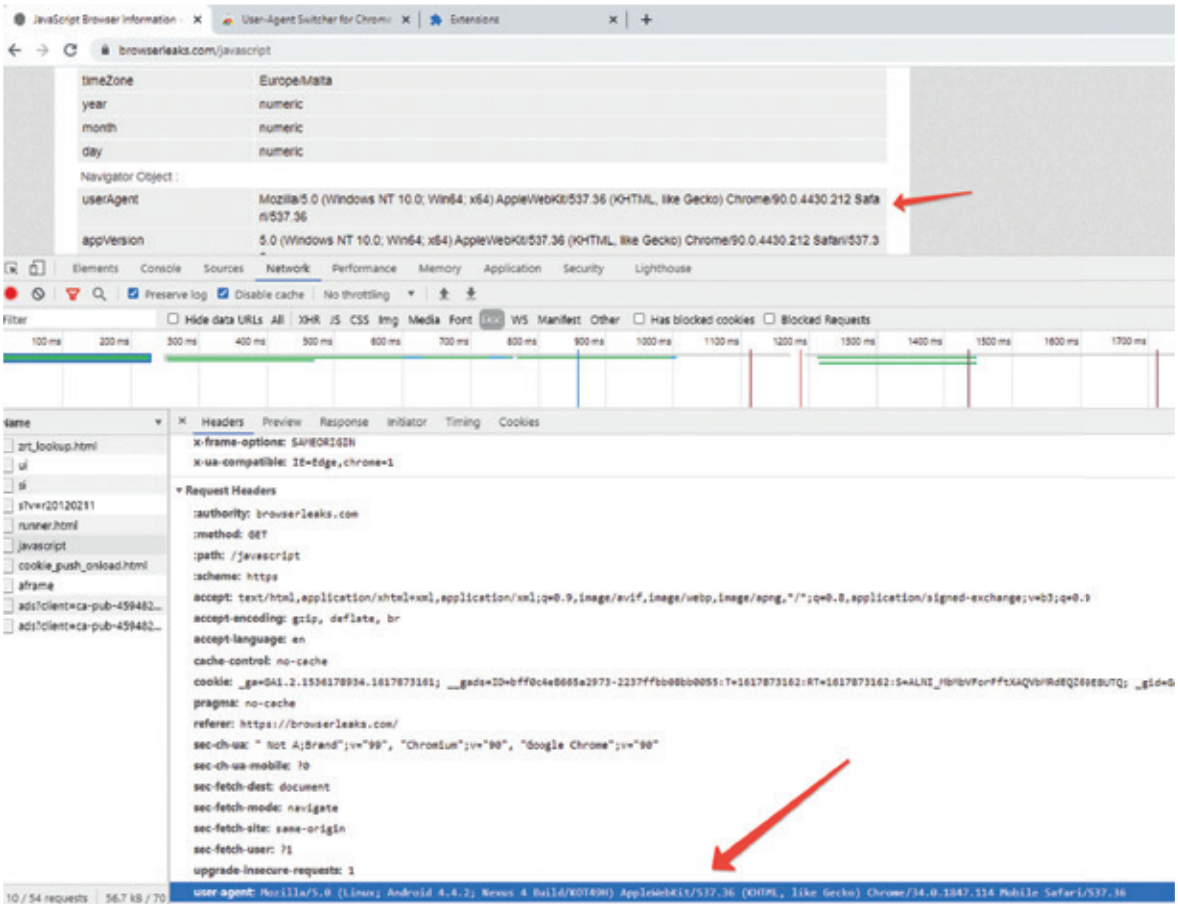


Tarayıcının User-Agent değeri yukarıdaki görselde de gördüğümüz üzere HTTP isteğindeki User-Agent alanından alınsa da, yani ilk elden eklentinin yaptığı değişiklik işe yarar gibi gözükse de sonuç maalesef hezimet olacak. Google'ın kendisi dahi User-Agent değeri için HTTP header'a müracaat etmiyor.

User-Agent stringini bu şekilde yani HTTP isteğindeki User-Agent header'ından almak pasif analiz olarak değerlendirilebilir. Bunun yanı sıra, bu değişikliğin maskesini düşürecek daha geçerli yöntemler de mevcut. Örneğin tüm tarayıcılarda bulunan navigator API'inin userAgent attribute'u:

```
navigator.userAgent
```

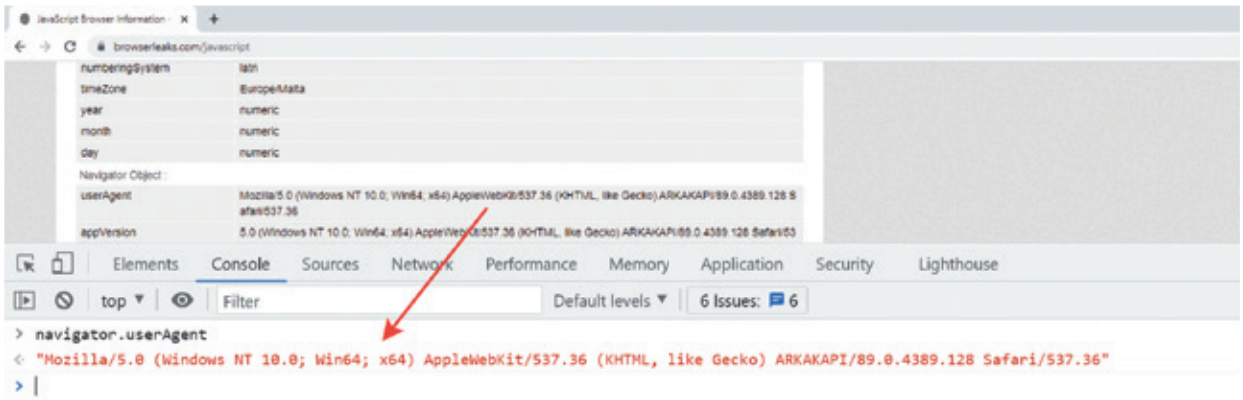
Aşağıdaki ekran görüntüsünden de göreceğiz üzere Browserlaks.com sitesi her iki değeri de gösteriyor. Böylece oluşturduğunuz anomali doğrudan tarayıcının bloklanmasına, bot olarak değerlendirilmesine yol açabilir.



*navigator.user*Agent değerini Javascript Injection ile değiştirebilmek mümkün. Bu bölümü daha fazla uzatmamak adına daha kolay bir yöntem paylaşacağız. Chrome tarayıcısını user-agent flag'i ile başlatmak:

```
"C:\Program Files\Google\Chrome\Application\chrome.exe"  --user-agent="-
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) ARKAKAPI/89.0.4389.128 Safari/537.36"
```

Göreceğiz üzere hem User-Agent request headerı hem de navigator.userAgent değeri birbirine eşdeğer bir string ile sabitlendi:

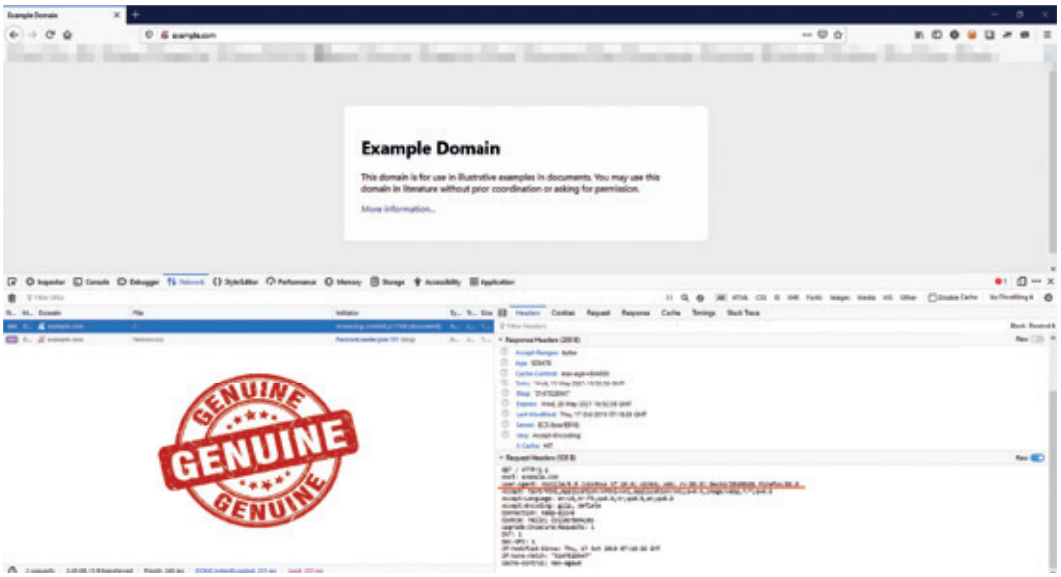


Yalancının Mumu Yatsıya Kadar Yanar

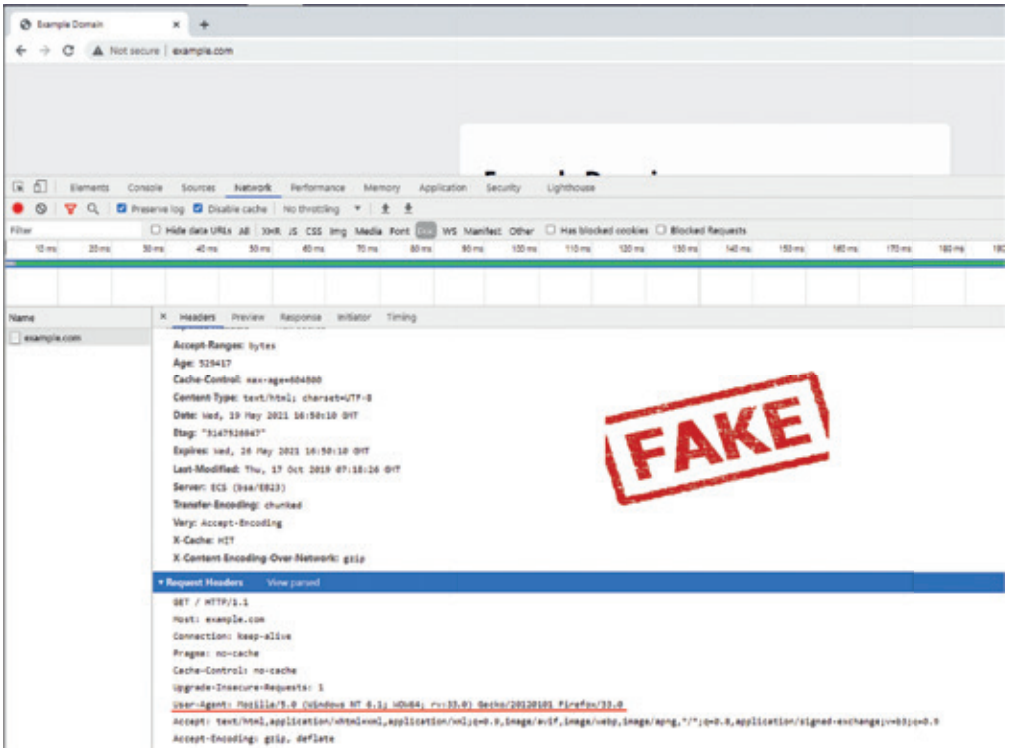
Sadece bu kadar da değil, keşke her şey bir User-Agent string'ini değiştirmek kadar kolay olsaydı…

Firefox bir tarayıcıyı Chrome, Chrome bir tarayıcıyı Firefox gibi göstermek için User-Agent değerini değiştirmek derdinize deva olmayacak. Çünkü tarayıcıların ayırt edici özellikleri, ki pek çok bot detection sistemi bu konularda büyük yatırımlar yapıp araştırma için büyük bütçeler ayırıyor, sizi ele verecek.

İşte gerçek bir Firefox tarayıcıdan yapılan HTTP isteği:



Ve ikinci ekran görüntümüzde her ne kadar User-Agent değeri ile kendini Firefox bir tarayıcı gibi gösterse de, anında enselenmiş bir tarayıcı:

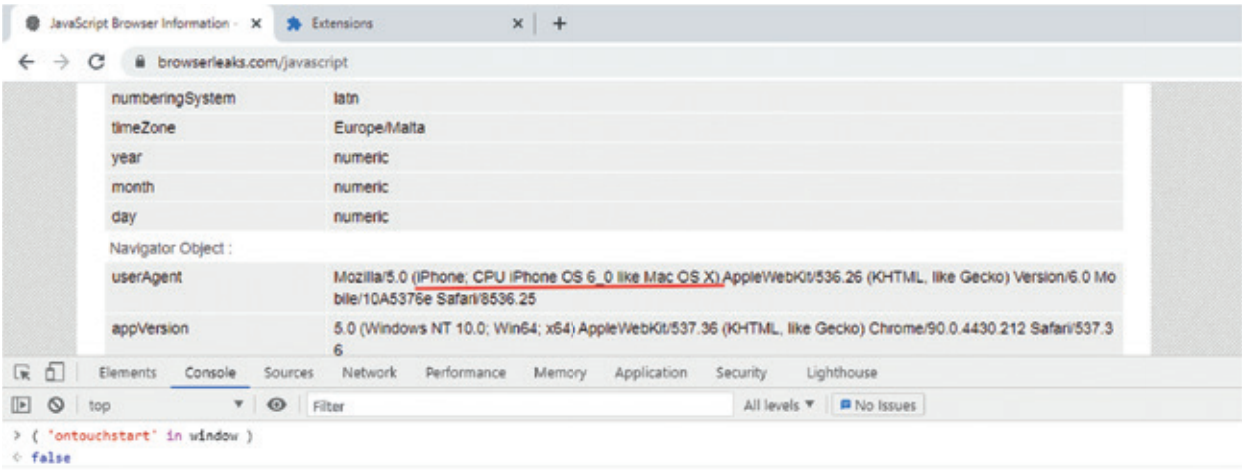


Sebebi basit, Firefox tarayıcılarda User-Agent string'i her zaman HTTP isteklerinde üçüncü sırada yer alır. Öncelikle HTTP verb'i (GET, POST, HEAD, vb), her HTTP isteğinde zaruri olan Host headerı ve ardından User-Agent stringi.

Devam edelim…

Yazımızın başlığında da belirttiğimiz gibi taklit aslına övgüdür. Dört başı mamur gibi spoofing için taklit ettiğiniz cihazın hiç değilse temel özelliklerini bilmelisiniz.

İşte User-Agent string'i ile iPhone olduğunu iddia eden bir istemci. Fakat her ne hikmetse bu telefonun dokunmatik özelliği yok! Daha ilk adımda yakayı ele vermesi işten bile değil!

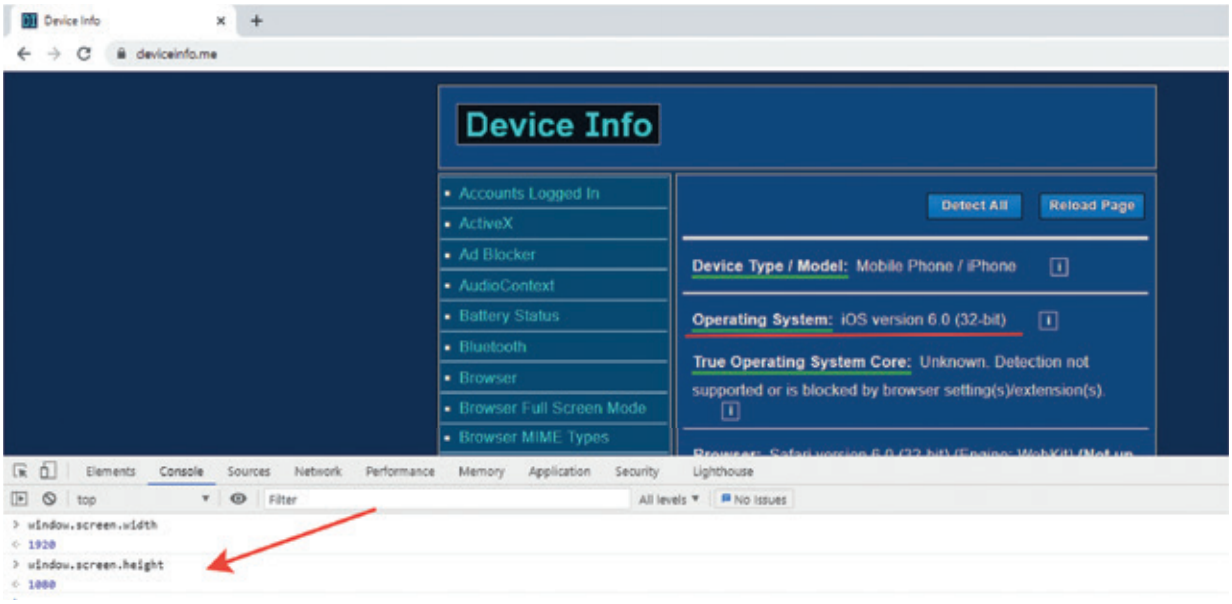


Mobil cihazların en temel karakteristiği dokunmatik ekranlarının olmaması, bugün yaygın olarak kullanılan cihazlardan söz ediyoruz elbette. Spoofing yaparken dikkat edilmesi gereken bir başka önemli ayrıntı da taklit ettiğiniz cihazın işletim sistemine dair temel bilgiler. Aşağıda gördüğümüz örnekte yine iPhone olduğunu iddia eden bir cihaz navigator.platform API'ile aslında Windows işletim sistemine sahip olduğu bilgisini ele veriyor. Bu aşamadan sonra detection sistemlerinin size reva görecekleri aksiyonu söylememize gerek var mı?

Bir mobil cihazı taklit etmek istiyorsanız, hiç değilse temel özelliklere dair bilgi sahibi olmalısınız.

Örneklerimize devam edelim:

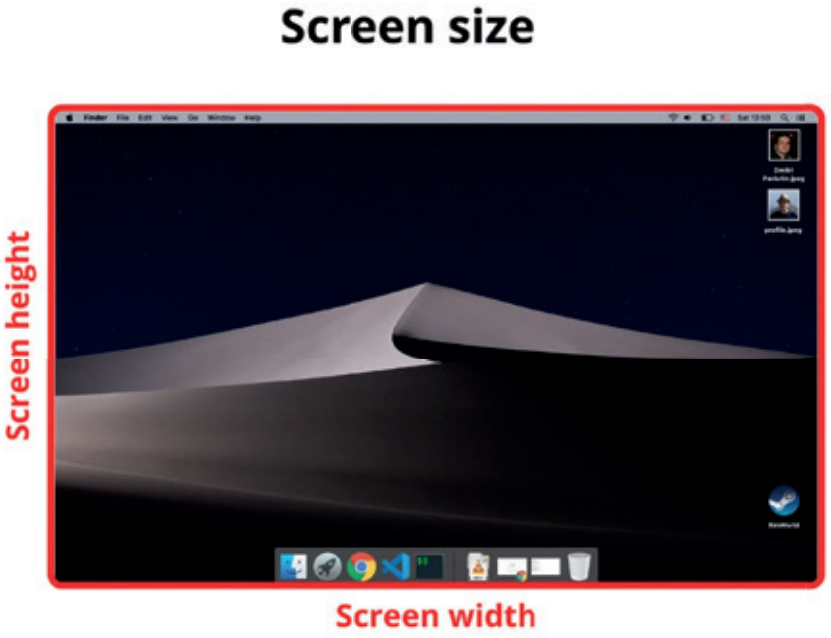
Nush ile uslanmadıysanız, GSM Arena gibi bir kaynaktan hiç değilse taklit edeceğiniz cihazın ekran çözünürlüğüne bile dikkat etmediyseniz bir bot detection tarafından hakkınız kötek olarak belirlenecek. İşte can alıcı bir başka örnek:



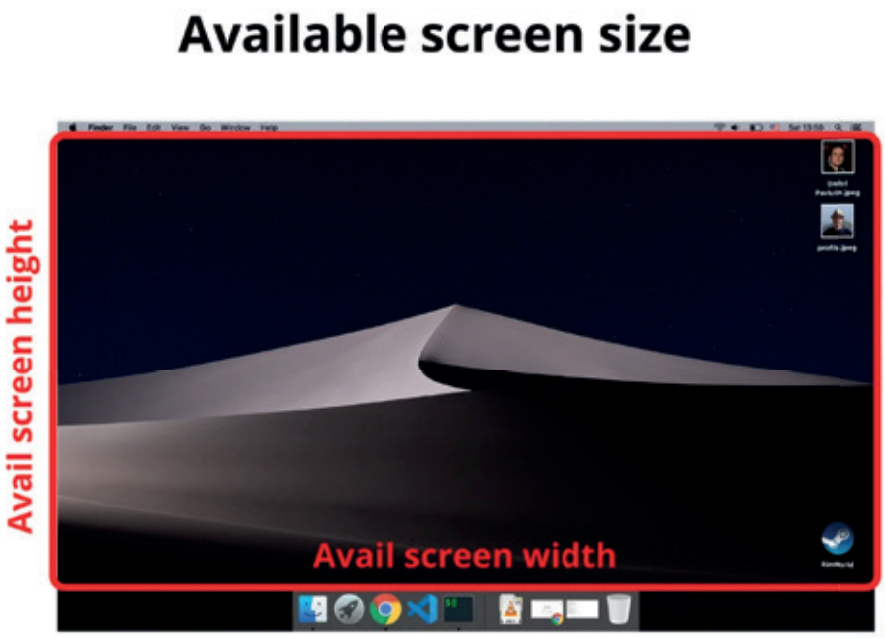
Siz hiç 1920 X 1080 ekran çözünürlüğüne sahip bir mobil telefon gördünüz mü? Ankesörlü bir telefondan söz etmiyoruz… Bot detection sistemleri mutlaka window.screen.width ve window.screen.height gibi bilgileri de elde edip, üstelik bu bilgilerin tutarlılıklarını da test edecektir.

Bu hususta bazı temel bilgileri burada zikretmekte fayda var:

Tarayıcıların Screen API'ları cihazınızın ekranı konusunda önemli ayrıntılar paylaşıyor.



Cihazınızın fiziksel genişlik ve yüksekliği **screen.width** ve **screen.height** ile elde edilebilir. (Görsel: https://dmitri-pavlutin.com/screen-window-page-sizes/)



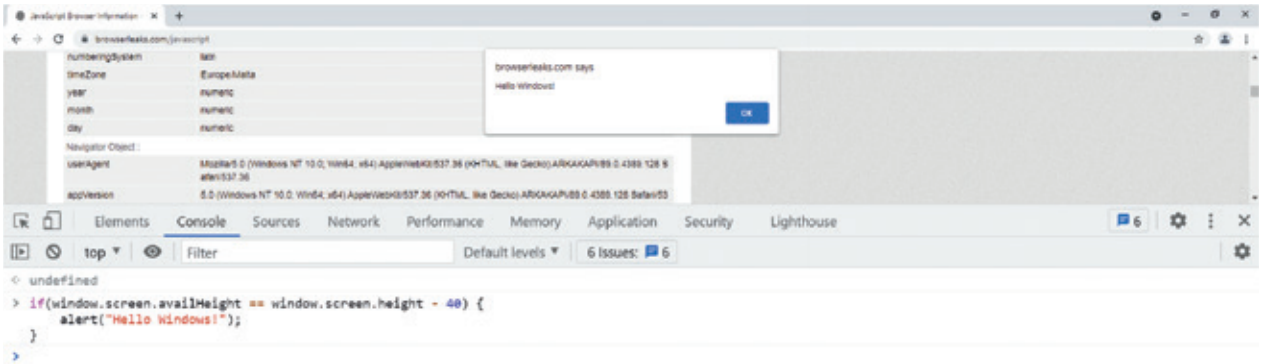
(Görsel: https://dmitripavlutin.com/screen-window-page-sizes/)

Yukarıdaki ekran görüntüsünde de görüleceği üzere tarayıcımız fiziksel boyutları dışında işletim sistemi tarafından bizim kullanımızı sunulmuş bir de alanı var.

Her işletim sistemi task bar (başlat menüsünün olduğu çubuk örneğin) gibi elementlerle kullanıcısına kimi görsel özellikler sunar. Windows işletim sistemindeki başlat menüsü, Linux ve macOS sistemlerde üst menü çubuğu bunlardan bazıları. Bunlar dışında kalan alanlar tarayıcıların Screen API'ı tarafından **availWidth** ve **availHeight** değeri olarak kodlanmaktadır.

Örneğin Windows işletim sisteminde -normal şartlar altında- taskbar 40 pixellik bir yükseklik işgal ediyor. Fiziksel yükseklik değerinden 40 değerini çıkarttığınızda elde ettiğiniz değer availHeight'e eşit ise, kullanıcının Windows işletim sistemini kullandığını doğrulayabilirsiniz.

```
if(window.screen.availHeight == window.screen.height - 40) {
        alert("Hello Windows!");
}
```



Elbette kullanıcılar taskbar'ın yerini değiştirmiş olabilir. Teorik bir senaryo olarak bilinmesinde fayda gördüğümüz için paylaşmak istedik.

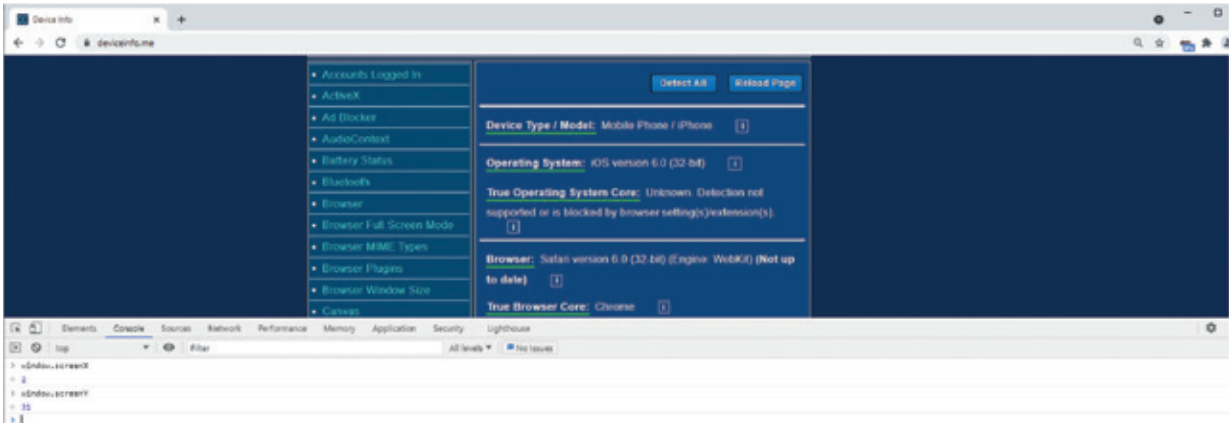
Mobil cihazlara dair önemli birkaç ayrıntı

Mobil cihazları taklit ederken sonuç cepte diye düşünmeyin! Birazdan açıklayacağımız ayrıntılar spoofing maceranızı hüsrana uğratabilir.

Yukarıdaki ekran görüntüsünde de görüleceği üzere tarayıcılar mobil cihazlarda açıldıklarında tam ekran modunda çalışırlar. Bu da pencerenin X ve Y değerinin her zaman 0'a eşit olması anlamına geliyor.

Eğer spoofing ile mobil bir cihaz olduğunuzu iddia ediyor ve böylesi basit bir testten sınıfta kalıyorsanız, anti-bot sistemleri tarafından ya banlanacak ya da kötü bir skor ile puanlanacaksınız.

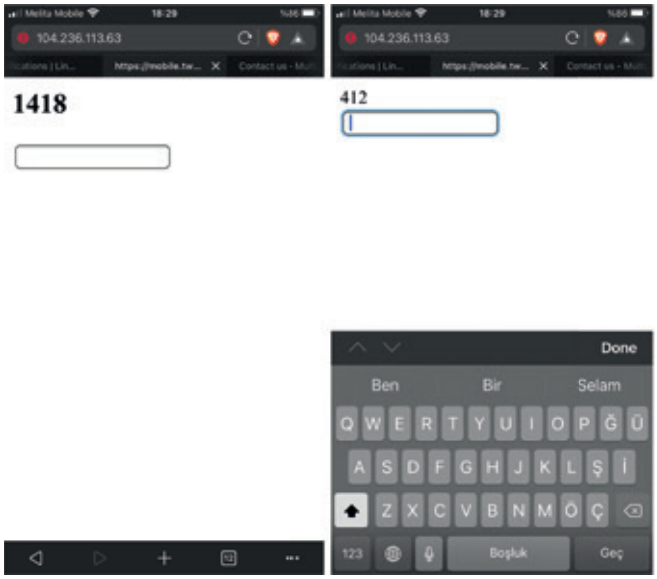
İşte bu testten sınıfta kalan bir spoofing girişimi:



Masaüstü ya da laptop cihazlar için paylaştığımız yukarıdaki görseller cep telefonları için de geçerli. Yani cep telefonları ekranlarının da fiziksel bir genişlikleri olduğu gibi, işletim sistemi tarafından kullanılan alanlar dışında kalan bir de available alanları var. Yani **availHeight** ve **availWidth** değerleri mobil cihazlarda için de söz konusu.

Masaüstü ve laptop işletim sistemlerinde bu alanlar taskbar gibi görsel elemanlar tarafından kullanılıyordu. Mobil cihazlarda da yazı yazmak için kullanılan virtual keyboardlar available alanı daraltan en önemli unsurlardan.

Özetle bir text kutusuna veri girilirken dahi gerçekten mobil bir cihaz olup olmadığınızı kolaylıkla anlayabilirler. Text kutusuna tıkladığınız anda beklenen davranış açılan virtual keyboard'ın ekranınızı daraltması yani **availHeight** değerinin text kutusuna focus yapmanızdan önceki değerden daha düşük olması.



Yukarıdaki ekran görüntüsünde text kutusuna tıklamanızdan hemen önce **availHeight** yani kullanılabilir ekran yüksekliği değeri 1418 iken, kutuya tıklandıktan sonra açılan virtual keyboard bu alan değerini 412'ye düşürüyor.

Yine işletim sistemleri ve cihazlara özel olarak tasarlanan emojiler de cihazlarımızın gerçek kimliğinin tespit edilmesinde bot detection sistemlerinin kullandığı ayrıntılardan.

Native [1]	Apple [2]	Android [3]	Android [3]	Symbola [4]	Twitter [5]	Unicode
😀	😀	😀	😀	😀	😀	U+1F600

Görüldüğü üzere her ne kadar emojilerin unicode değeri aynı olsa da cihaz ve işletim sistemine göre render edilmeleri de bir o kadar farklı.

Bu konuda yaptığımız küçük bir testin sonuçlarını paylaşmak istiyoruz:

Here is hashed version of **U+1F600** smile emoji from different devices.

os	osVersion	browserName	browserVersion	Hashed version of emoji
iOS	12.3.2	Mobile Safari	12.1.1	ec563f348e696c5346210 4c6bd4ecb608bf274b757d75e2c500518cbd3fde402
iOS	11.0	Mobile Safari	11.0	ec563f348e696c5346210 4c6bd4ecb608bf274b757d75e2c500518cbd3fde402
iOS	14.3	Mobile Safari	14.0.2	efa226a121be563aaaf91d6387435c106d5b90a0c537ed9d1266c4819a521edf
iOS	14.3	Mobile Safari	14.0.2	efa226a121be563aaaf91d6387435c106d5b90a0c537ed9d1266c4819a521edf
iOS	14.4.2	Mobile Safari	14.0.3	efa226a121be563aaaf91d6387435c106d5b90a0c537ed9d1266c4819a521edf
iOS	14.0.1	Mobile Safari	14.0	f789752a86fccc5fbf77679cd98823cb49e5b54f120f715fb07a8bef76429efe

Here sha256 hashed out of same emoji obtained from different version of Google Chrome on Windows 10 OS.

os	osVersion	browserName	browserVersion	Hashed version of emoji
Windows	10	Chrome	90.0.4430.72	ec132669c7edae4b60a262a128ae934c780d082631d8b82a84b527e5f6479930
Windows	10	Chrome	89.0.4389.90	ec132669c7edae4b60a262a128ae934c780d082631d8b82a84b527e5f6479930
Windows	10	Chrome	87.0.4280.66	ec132669c7edae4b60a262a128ae934c780d082631d8b82a84b527e5f6479930

Bilgi güçtür!

TÜNELİN UCUNDAKİ IŞIK:
SSH PORT FORWARDING

Arka Kapı Dergi'nin ilk sayılarından itibaren okurlarımıza çevrim içi gözetime, içerik engellerine karşı bağışıklık kazandırmak için, bir cangıla dönen internet dünyasında hayatta kalmalarını sağlayacak pek çok ipucu paylaştık. Kendi VPN sunucunuzu nasıl kuracağınızdan, iyi bir VPN bağlantısını nasıl tesis edeceğinize dair yazılar Arka Kapı Dergi arşivinde meraklı okurları bekliyor.

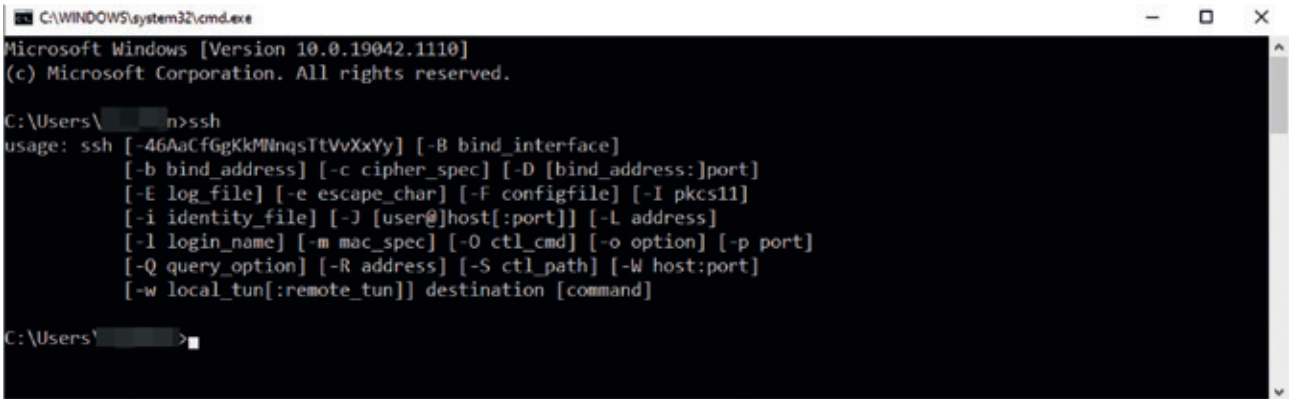
Bu yazımızı 1995 yılından beri internet dünyasının gündeminde olan, daha çok sunucu yönetimi gibi konularda tercih edilse de son kullanıcı için de pek çok elverişli özellik sunan SSH'e, yani Secure Socket Shell'e ayırdık.

SSH protokolü istemci ve sunucu arasında güvenli bir bağlantı sağlayıp, uzak sunucuları ekranlarımıza getiriyor, dosya paylaşımı ve transferi gibi pek çok alanda kullanışlı özellikler sunuyor. Bu saydıklarımızın sadece sistem yöneticilerinin ilgi alanlarına girdiğini düşünen okurlarımıza çabucak pes etmemelerini salık veririz; zira SSH son kullanıcılar için de özellikle de gizlilik ve mahremiyet gibi konularda titizlenen son kullanıcılar için de harika imkânlar sunuyor.

Gözetimden kurtulmak, coğrafi kısıtları ya da sansür engelini aşıp dilediğiniz içeriklere ulaşmak mı istiyorsunuz? VPN hizmeti satın almak epey tuzlu, kurulum yapmak için de yönergeleri takip edecek sabrınız mı yok? Elimin altındaki üç beş araç gereçle, bilgisayarınızdaki hali hazırda kurulu bulunan birkaç programla internette "anonim" olup, dilediğiniz içeriğe ulaşmak mı istiyorsunuz? Öyle ise başlayalım…

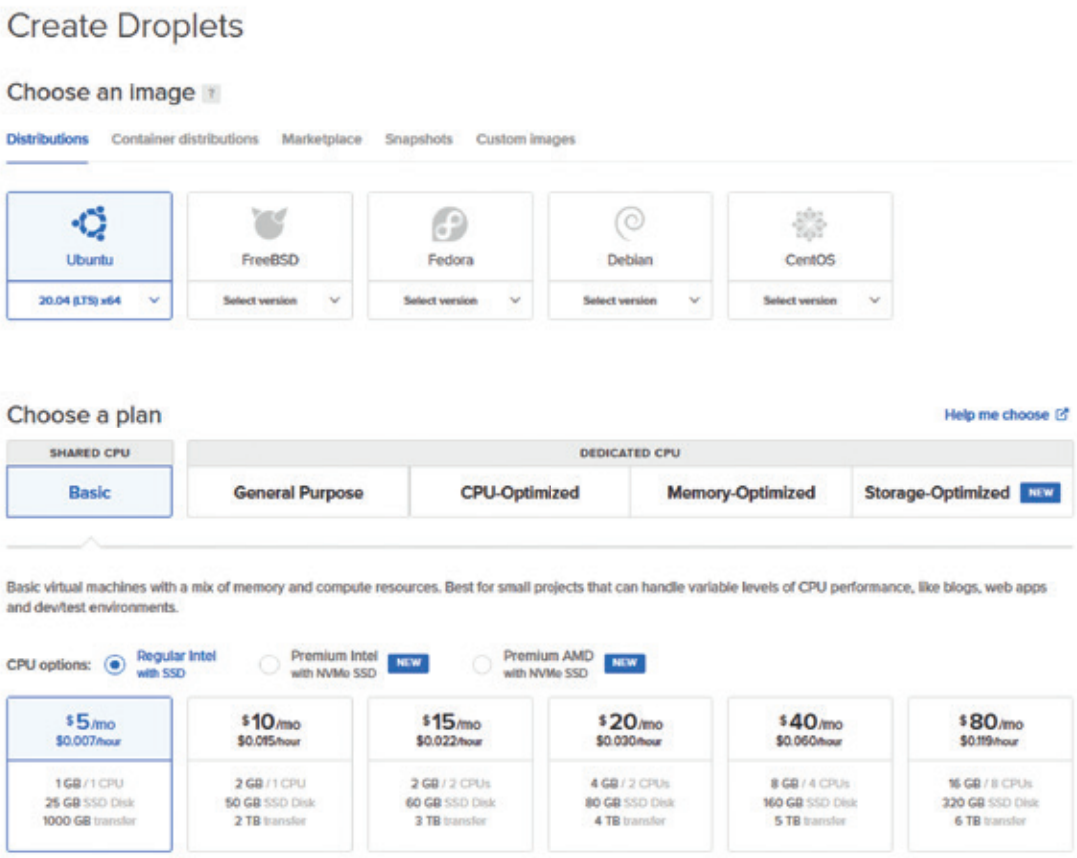
Herhangi bir hosting sağlayıcısından temin edeceğiniz bir hosting ve Windows 10, Linux ve macOS yüklü bilgisayarlarda yüklü halde gelen SSH programı bu maceramızda bize eşlik edecek. Şayet Windows işletim sisteminizde SSH yüklü değilse, bunun yerine Putty (1) isimli programı kullanabilirsiniz.

İşletim sisteminizdeki ssh programının kurulu olup olmadığını anlamak için komut istemcisinde SSH yazarak enter tuşuna basabilirsiniz:

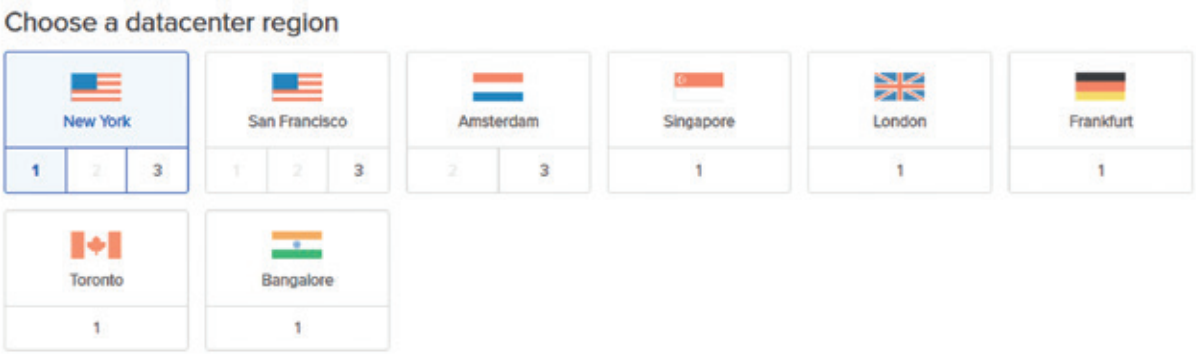


SSH işletim sisteminizde yüklü ise yukarıdaki gibi parametre varyasyonlarını gösteren bir çıktı alacaksınız.

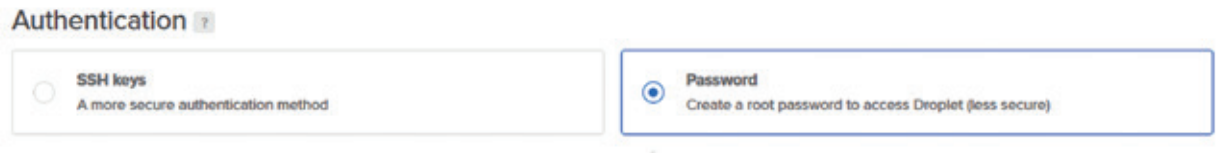
İşletim sistemimizde yüklü olan SSH programı aslında bir client, dolayısıyla bu client ile bağlanacağımız bir de sunucu yani server olması lazım. Yazı kapsamında kullanacağımız sunucu ihtiyacını Digital Ocean'dan bir Droplet kiralayarak karşılayacağız:



Aylık ortalama maliyeti 5 Dolar olan bir sunucu kiralamak için seçeneklerimi belirtiyorum. Digital Ocean'da sunucunuzun barındırılacağı lokasyonu da seçebilirsiniz:



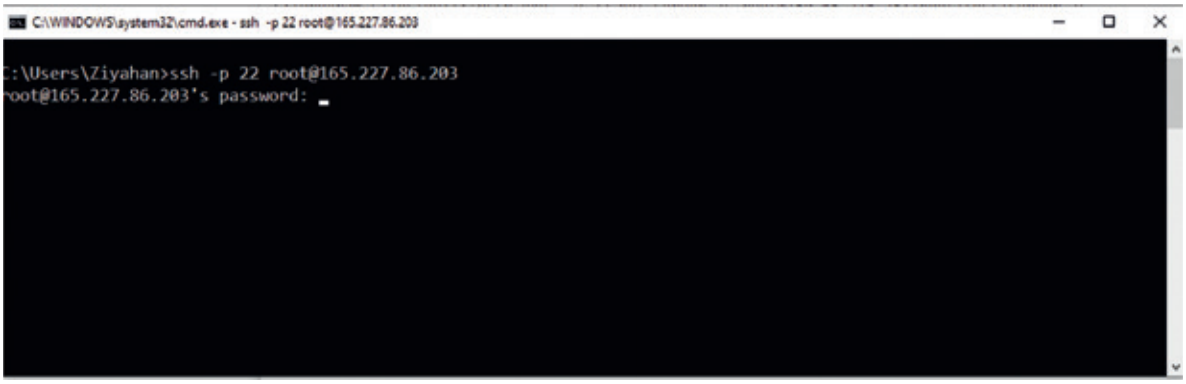
Oluşturacağımız sunucuya bağlanmak için iki farklı yetkilendirme tipi mevcut: SSH anahtarı oluşturmak ya da bir kullanıcı parolası belirlemek. SSH anahtarları oluşturmak, oluşturulan anahtar çiftlerini istemci olarak kullanacağımız kendi makinemize kaydetmek gibi bu yazının kapsamı dışında olan konular olduğu ve yazıyı uzatmamak niyetinde olmadığımız için affınıza sığınarak yetkilendirme için Password seçeneğini seçerek devam ediyoruz.



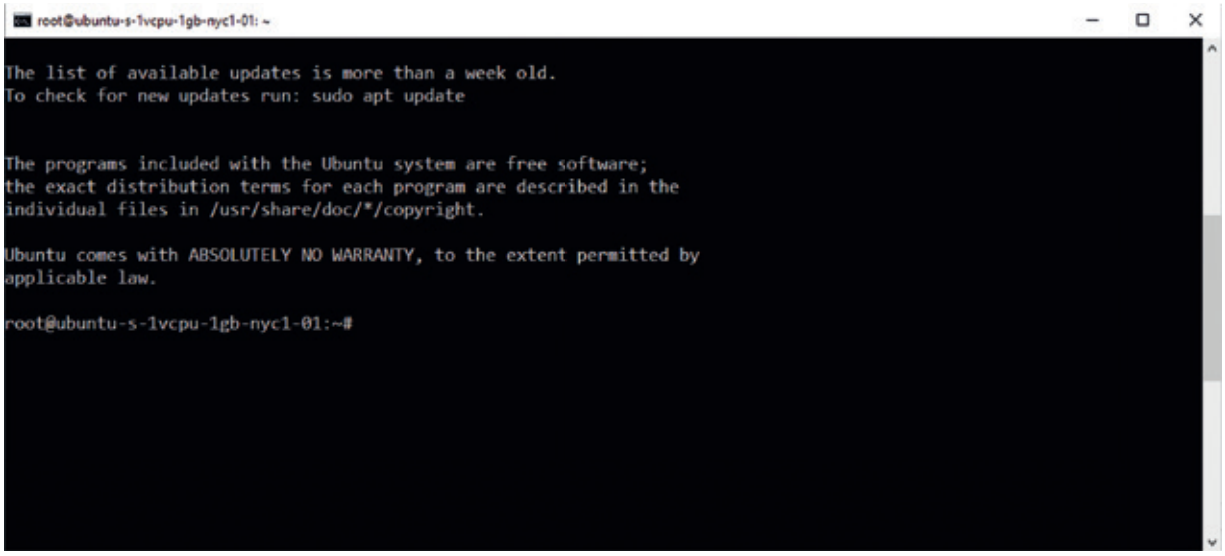
Create Droplet dediğinizde sunucumuz birkaç saniye içinde hazır olacak:

Sunucumuz hazır olduğuna göre, artık Windows makinemizdeki SSH programını kullanarak bağlanabiliriz:

```
ssh -p 22 root@165.227.86.203
```



Sunucu kurulumu esnasında belirlediğimiz parolayı girdiğimizde, artık sunucumuz parmaklarımızın ucunda olacak.



Karşımızda duran terminal ile Amerika Birleşik Devletleri'nin New York şehrinde barındırılan sunucumuza hükmedebiliriz. Fakat bu yazının amacı elbette ki bu kadarla sınırlı değil, bunca gevezeliğe rağmen hâlâ yazıya devam etmek için merakınız uyanıksa devam edelim…

SSH Local Port Forwarding

Yazımız sistem yöneticilerinin uzaktan bir makinenin bakımını nasıl yapabileceklerini anlatmak için yazılmadı. Esas amacımız SSH'in sunduğu imkânları güvenli ve gizlilik ekseninde kullanmak.

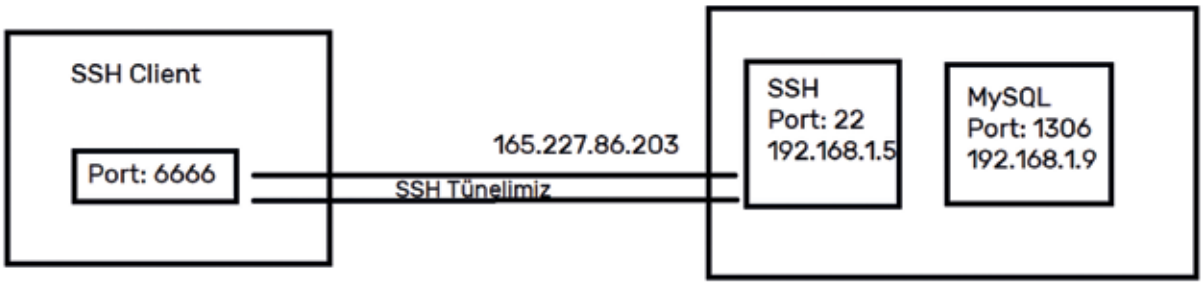
SSH'in sunduğu önemli olanaklardan biri olan local port forwarding ile başlayalım.

Diyelim ki şirketinizde dışarıdan erişime kapalı olan bir web sunucusu ya da bir veritabanı sunucusu var. Bu veritabanı ya da web sunucunuzu dışarıya açmamak, öte yandan da güvenli bir yolunu bulup uzaktan da olsa erişebilmek istiyorsunuz. SSH local port forwarding bunun için var.

SSH istemcisinin çalıştığı makinenizdeki bir portu, ssh sunucunuz ile aynı ağ içerisinde olan ve dışarıdan erişime kapalı olan sunucunuza bağlayabilirsiniz. Erişime kapalı olan makinenize giden tüm trafik önce ssh istemcinizden ssh sunusuna şifreli bir biçimde ve ssh paketi olarak çerçevelenmiş bir şekilde iletilecek; ssh sunucusu aynı ağdaki veritabanı sunucusuna sizin yerinize bu paketi iletip, dönen yanıtı da size aktaracak.

Senaryomuzu şöyle özetleyelim: SSH istemcimizin kurulu olduğu makinemizde, yani Windows 10 makinemizdeki 6666 numaralı portumuzu, ssh sunucumuz ile aynı ağdaki dışarıdan erişime kapalı olan 192.168.1.9 IP'sine sahip makinenin 1306 numaralı MySQL portuna bağlayacağız.

```
ssh -L 6666:192.168.1.9:1306 root@165.227.86.203
```



Artık localhost hostname'i ya da 127.0.0.1 IP'si üzerinden 6666 numaralı porta gönderilen her istek şifreli bir şekilde SSH tünelimizden geçerek, ssh sunucusu ile aynı ağda bulunan ve dışarıdan erişime kapalı olan 192.168.1.9 numaralı MySQL kurulu makineye ulaşacak. Tebrikler!

SSH Remote Port Forwarding

Bir önceki başlık altında incelediğimiz local port forwarding'in tam tersi olarak bu defa kendi makinemizde bulunan ve dışarıdan erişime kapalı olan bir servisi dışarıya açacağız.

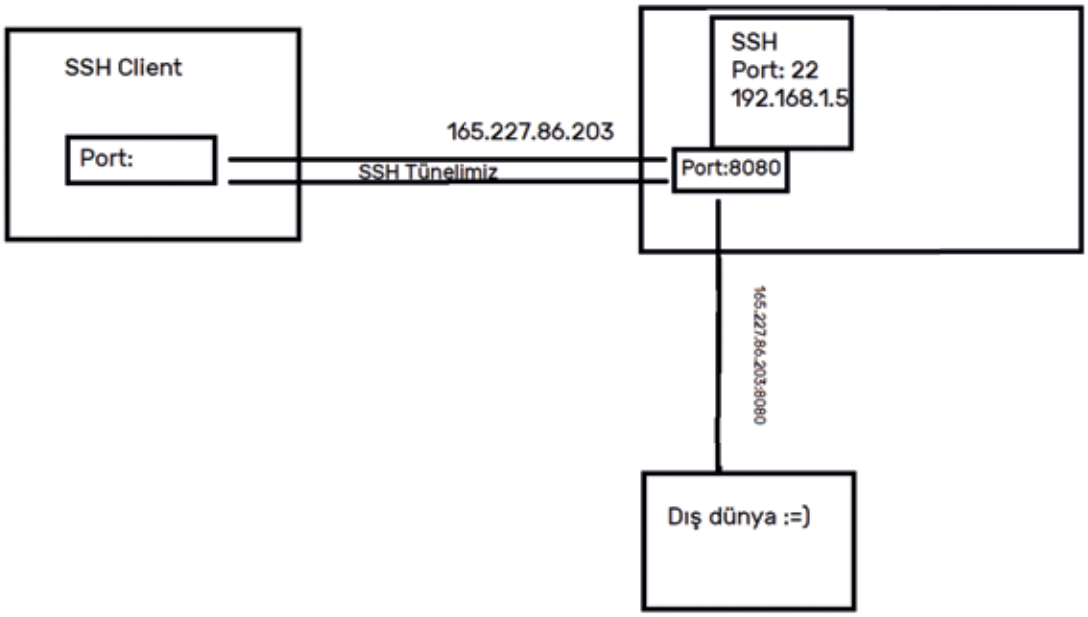
Mutlaka local makinenizde bir web sunucusu kurmuş, kimi denemeler yapmış, ve yine mutlaka bu denemeleri bir arkadaşınıza göstermek istemişsinizdir. Modem arayüzünden portlara erişimi açıp makinenize yönlendirmek zahmetli gelmiş olabilir. Porta erişim açıp sonra unutmak da cabası. Hiç bu topa girmek istememenizi anlayışla karşılıyorum.

Teknik olarak biraz daha fazla işin içerisinde olanlar Ngrock gibi çözümler de denemiş olabilir. SSH remote port forwarding bu konuda tam aradığımız çözümü sunacak.

Bu defa ssh sunucusu üzerindeki bir portu, kendi local makinemizdeki bir servise yönlendireceğiz. Local makinemizde 80 numaralı porttan yayın yapan web sunucumuzu dış dünyaya açacağız.

Dış dünyaya açarken bize bu yolda ssh sunucumuz yardımcı olacak. Yani bizim local makinemizdeki sunucuya erişmek isteyenler -evet garip gelebilir- ssh sunucumuzun IP'sini kullanacaklar.

```
ssh -R 8080:localhost:80 root@165.227.86.203
```



Yukarıdaki komutu çalıştırdıktan sonra, ssh bağlantımız devam ettirdiği süre boyunca SSH sunucumuzun IP adresi üzerinden 8080 numaralı porta istek yapanlar, bizim yerel (local) makinemizdeki web sunucusuna erişecekler.

SSH Dynamic Port Forwarding

Yazımızın yüzü suyu hürmetine yazıldığı esas konuya geldik. Bunca kelam bu alt başlık için edildi. Ama inanın beklediğinize değecek.

Dikkatinizi çekmiş olmalı, ssh istemcisi ve sunucusu arasındaki yönlendirmeleri port numaralarını sabitleyerek yaptık. Bu yöntem gündelik pek çok işi kolaylaştıracaktır fakat yazımızın başlığında da belirttiğimiz gibi eğer ssh'ı tünelin ucundaki bir ışık olarak lanse ettiysek, sansür ve dijital gözetim karanlığından da bir an çıkmamız gerekiyor. Artık bir şeyler yapmalı!

SSH'ın dinamik port forwarding'i ile artık bir SSH proxy'ye sahip olabiliriz. Haydi adını da söyleyelim, POSSH! Kısaltma sizi ürkütmesin Proxy over SSH demek :)

POSSH'un HTTP proxy ve VPN seçeneklerine göre çok fazla artısı var. Öncelikle yazının bu noktasına dek farketmiş olacağınız gibi kullanımı gayet basit, hiçbir ekstra program kurmanıza gerek yok.

Diğer taraftan, HTTP proxy'ler çoğunlukla HTTP ve HTTPS protokolleri üzerinden veri trafiğini sağlayıp, şayet anonymity için kullanıyorsanız, WebRTC, DNS Leak gibi yöntemlerle gerçek kimliğinizi ifşa edebilir. SOCKS ise protokol agnostik (bilinmezci), yani protokol bağımsız çalışıyor. Özetle her türlü isteği, hatta DNS isteklerini dahi SSH protokolü ile sarmalayıp SSH sunucusu üzerinden gönderip alıyor.

VPN seçeneğinde de pek çok VPN'in tıpkı HTTP proxyler gibi WebRTC ve DNS Leak gibi başlıklarda malul olduklarını biliyoruz. Üstelik daha pahalı bir seçenek.

Şimdi SSH sunucumuz ile dinamik bir port forwarding bağlantısı kurup, sonrasında tüm tarayıcı trafiğimizi ssh sunucumuz üzerinden hedefe ileteceğiz.

```
ssh -D 24000 root@165.227.86.203
```

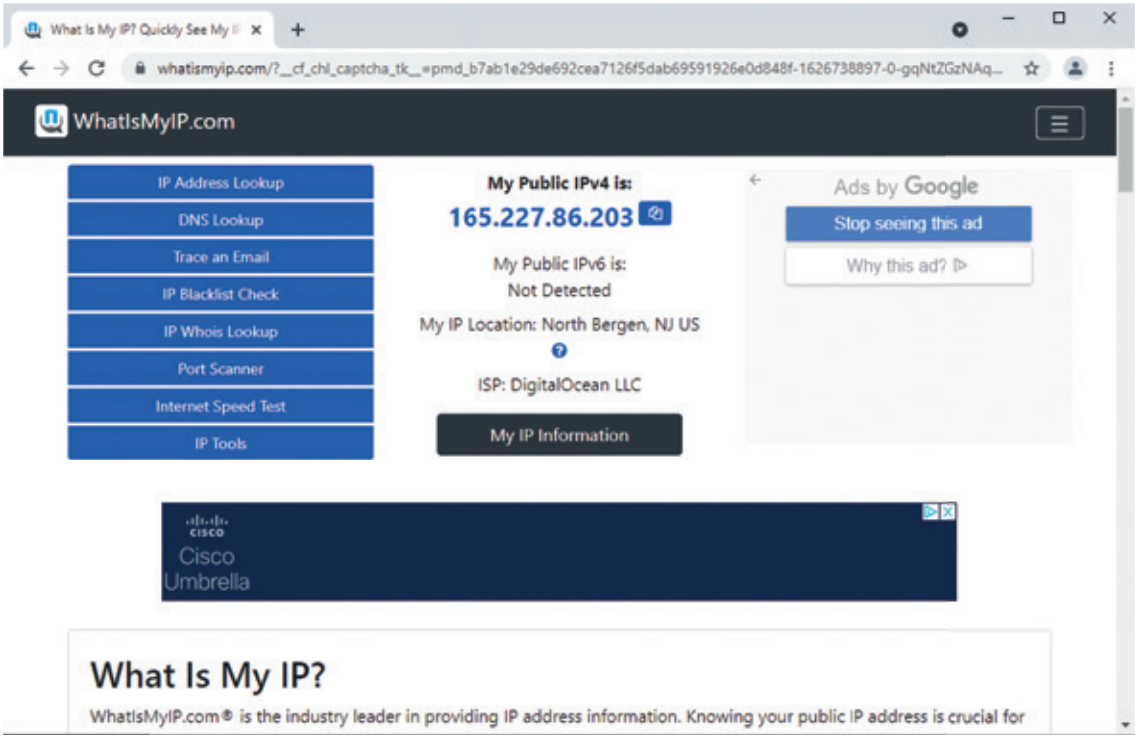
-D parametresi ile kendi makinemizdeki 24000 numaralı porta gönderilecek tüm isteklerin ssh sunucusuna yönlendirilmesini sağladık. SSH sunucusu da bu istekleri ilgili yerlere gönderip, aldığı yanıtı tekrar bize iletecek, tıpkı bir proxy ya da VPN gibi. Böylece ziyaret ettiğimiz sitelerde bizim IP'miz değil, ssh sunucumuzun IP'si gözükecek. Bu bağlantı güvenli bir bağlantı olduğu için ağı izleyen biri sadece SSH paketlerinin gidip geldiğini görecek, şifreli paket içeriğine erişemeyecek.

Tarayıcınızda ya da SOCKS proxy desteği olan herhangi bir programda proxy ayarlarını **localhost:24000** olarak değiştirip, gerçek IP'nizi gizleyerek internette gezinmenin tadını çıkartabilirsiniz.

SSH bağlantısı kurulduktan sonra, şimdi sıra tarayıcımızı tüm trafiği SOCKS proxy üzerinden göndermek için ayarlamaya geldi.

Chrome tarayıcısının Settings/Advanced Settings ayarlarından SOCKS proxy ayarlamak maalesef göründüğü gibi kolay değil. Fakat aşağıdaki yöntemi kullanarak tarayıcınızı SOCKS proxysi kullanacak şekilde başlatabilirsiniz:

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --proxy-server=so-
cks5://localhost:24000
```



Her ne kadar DNS resolving istekleri dahil, her türlü isteğin SOCKS sunucusuna gönderileceğini söylediysek de iki noktayı hatırlatmakta fayda var. Google'ın ifadesine göre DNS prefetch isteklerinin SOCKS proxy'i bypass etme ihtimali var. Yanı sıra artık bir URL şema olarak kullanılamasa da -en azından Chrome'un son versiyonlarında- ftp:// URL şeması ile yapılan istekler de SOCKS proxy'i bypass edebilir.

DNS prefetch'i engellemek için Google'ın Chrome tarayıcılarda tavsiye ettiği yöntem açılış parametresi olarak kullanabilirsiniz:

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --proxy-server="socks5://localhost:24000"

--host-resolver-rules="MAP * ~NOTFOUND"
```

Tüm DNS istekleri böylece geçersiz bir adrese yönlendirilecek.

Sonuç harika değil mi? Gördüğünüz gibi Whatismyip.com 'u ziyaret ettiğimizde Digital Ocean'da oluşturduğumuz sunucunun IP'sini görüyoruz. Başka bir yazıda görüşmek dileği ile :)

2021 YILININ SİBER GÜVENLİK İSTATİSTİKLERİ

İyisiyle kötüsüyle geride bıraktığımız 2021 yılında siber güvenlik istatistikleri nasıldı buyrun birlikte bir bakalım.

Hatırlarsınız bir sabah uyandığımızda gündemimize bomba gibi düşen WhatsApp Gizlilik Sözleşmesi ile başlamıştık 2021'e. Kapanışı ise bildiğimiz kadarıyla Log4j2 kütüphanesinde çıkan güvenlik açığı ile bitirdik (umarız bununla bitirmişizdir:). *"Sahi sözleşmenin akıbeti ne oldu?"*, derseniz: Yine hatırlayacağınız üzere WhatsApp, ocak ayında sözleşmeyi kabul etmeyen kullanıcıların hesaplarının silineceğini duyurmuştu. Gelen tepkiler üzerine sözleşmenin işleme alınmasını mayıs ayına ertelemişti. Mayıs ayında ise hiç kimsenin hesabının silinmeyeceğini fakat sözleşme uyarısının bir süre daha kalıcı hale geleceğini ve sözleşmeyi halen onaylamamış kullanıcıların hesaplarında işlevselliğin azalacağını duyurmuştu.

Şimdi gelelim bu yazımızın konusu olan 2021 yılı siber güvenlik istatistiklerine:

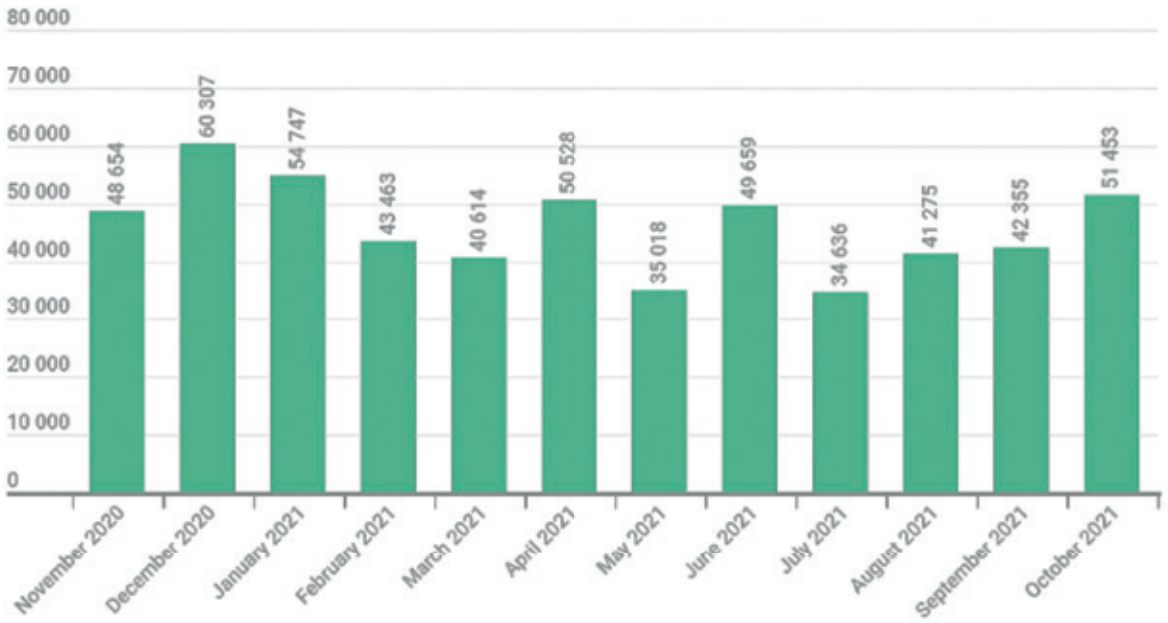
Cisco'nun yayımladığı *2021 Siber Güvenlik Tehdit Trendleri* raporuna göre bu yılki siber saldırılar arasında; kripto para madenciliği, kimlik avı - oltalama, fidye virüsleri ve Truva Atı saldırılarının en aktif tehditler olduğu duyuruldu.

Kaspersky'ın Ekim 2020 ile Ekim 2021 periyodu için derlediği *Kaspersky Güvenlik Bülteni 2021 İstatistikleri raporunun* bir kısmının tercümesi ise aşağıdadır (orijinal raporun tamamı için lütfen kaynaklar'a bakınız):

Yılın Rakamları

- Yıl boyunca, dünya çapındaki internet kullanıcısı bilgisayarlarının %15,45'i en az bir kötü amaçlı yazılım saldırısına uğradı.
- Yaklaşık 115 Milyon (114.525.734) benzersiz - kötü amaçlı URL, web anti-virüs bileşenlerini tetikledi.
- Raporlama döneminde madenciler yaklaşık 1.2 Milyon (1.184.986) kullanıcıya saldırdı.
- Banka hesaplarına çevrim içi erişim yoluyla para çalmak için tasarlanmış kötü amaçlı yazılım bulaştırma girişimleri, yaklaşık yarım milyon (429.354) kullanıcının cihazına kaydedildi.

Finansal Tehditler

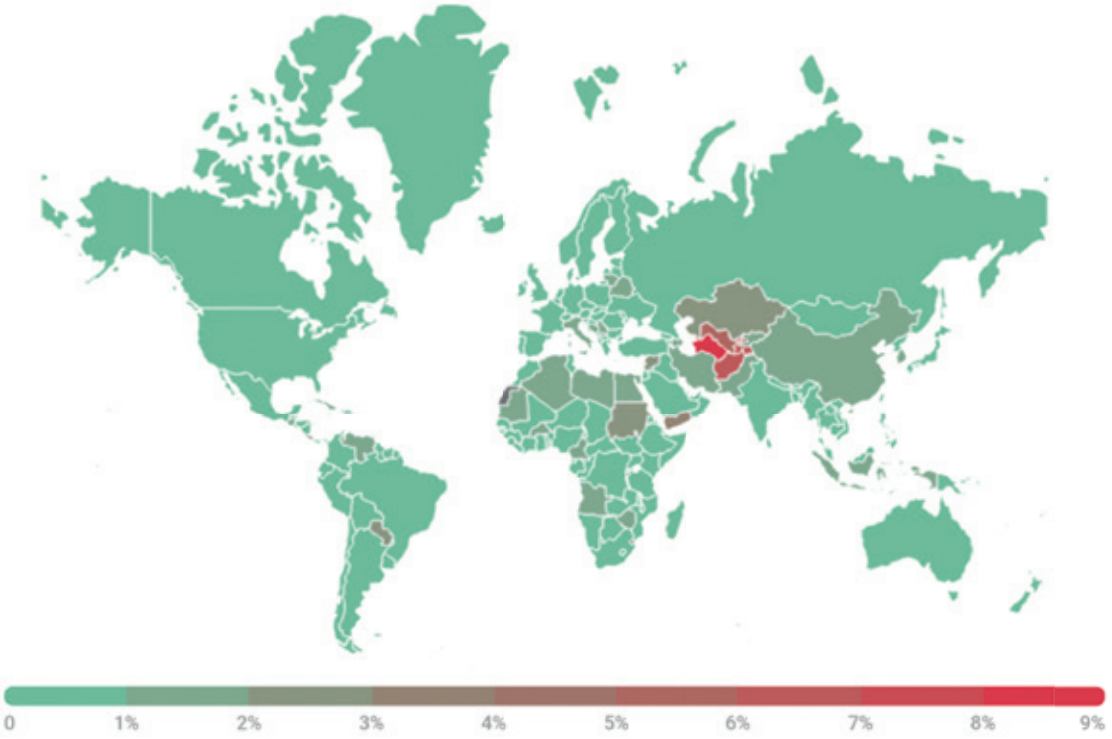


Finansal kötü amaçlı yazılımlar tarafından saldırıya uğrayan kullanıcı sayısı,
Kasım 2020 — Ekim 2021

Top 10 finansal kötü amaçlı yazılım ailesi:

Sıra	Adı	Yüzdesi (%)
1	Zbot	21.6
2	CliptoShuffler	12.7
3	SpyEye	10.1
4	Trickster	4.7
5	RTM	4.4
6	Nimnul	3.7
7	Danabot	3.1
8	Cridex	3.0
9	Nymaim	2.1
10	Neurevt	1.7

Saldırıların Coğrafi Dağılımı:



Bankacılık kötü amaçlı yazılım saldırılarının coğrafi dağılımı,

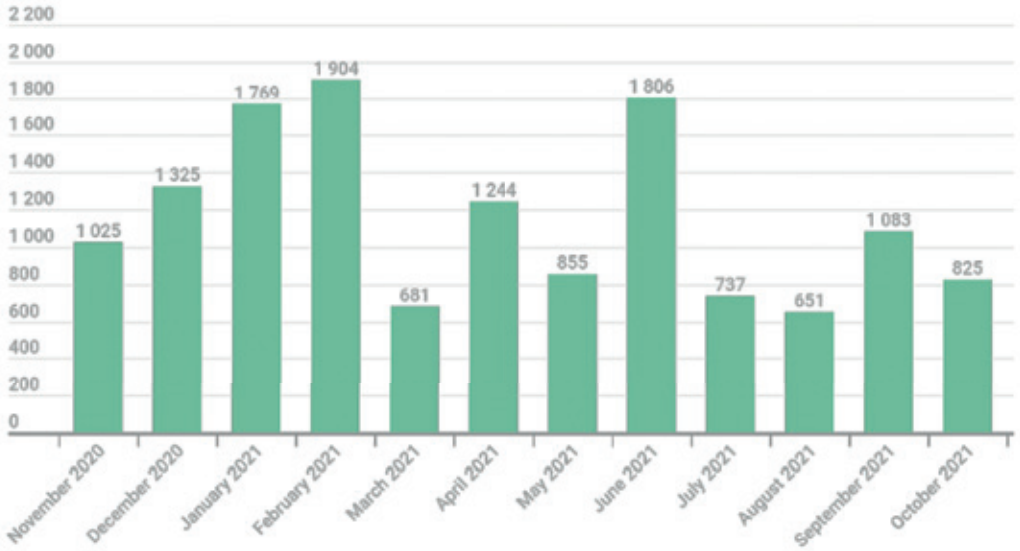
Kasım 2020 — Ekim 2021

Saldırıya uğrayan kullanıcılara göre ilk 10 ülke:

Sıra	Ülke	Yüzdesi (%)
1	Türkmenistan	8.4
2	Afganistan	6.7
3	Tacikistan	6.6
4	Özbekistan	5.7
5	Yemen	3.1
6	Paraguay	2.9
7	Kosta Rika	2.7
8	Sudan	2.4
9	Kazakistan	2.2
10	Suriye	2.2

Fidye Yazılımları:

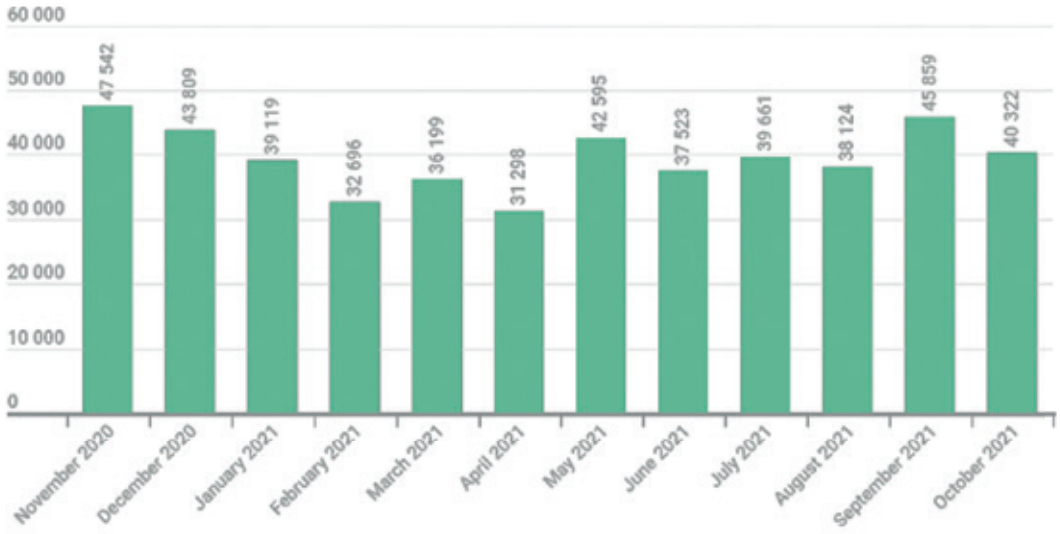
Kaspersky, raporlama döneminde 13.905'ten fazla fidye yazılımı değişikliği tespit etti.



Tespit edilen yeni fidye yazılımı değişikliklerinin sayısı,

Kasım 2020 — Ekim 2021

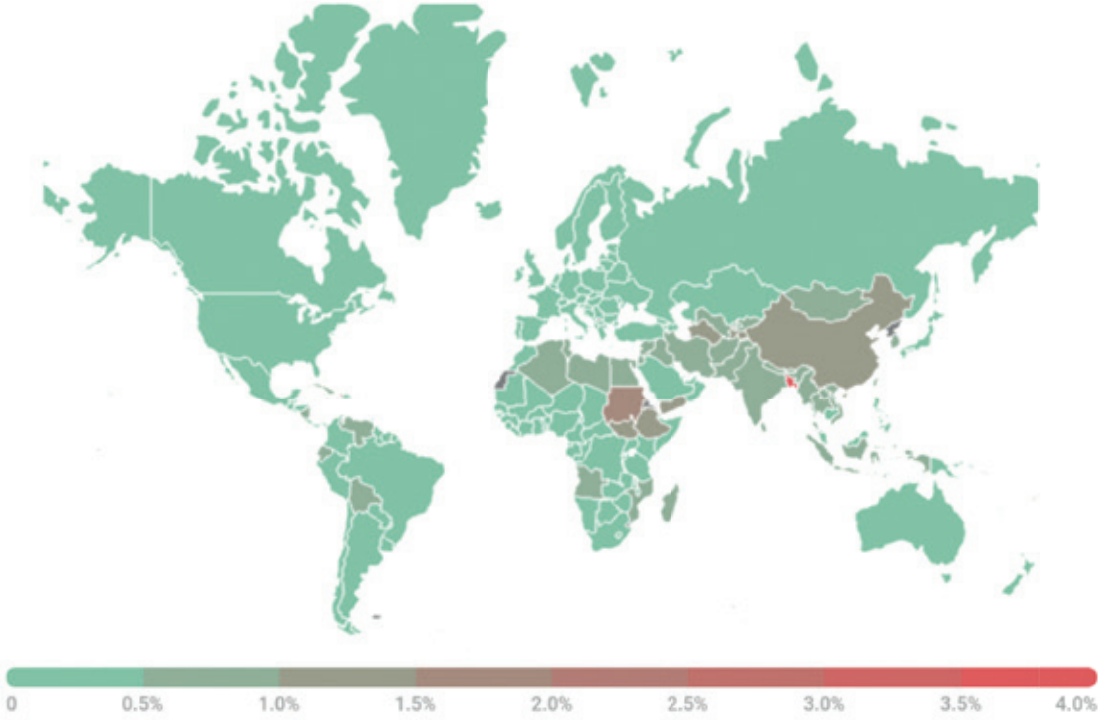
Raporlama döneminde fidye yazılımı truva atları, 92.863 kurumsal kullanıcı (KOBİ'ler hariç) ve küçük ve orta ölçekli işletmelerle ilişkili 12.699 kullanıcı dahil olmak üzere 366.256 benzersiz kullanıcıyı etkiledi.



Fidye yazılımı truva atları tarafından saldırıya uğrayan kullanıcı sayısı,

Kasım 2020 — Ekim 2021

Saldırıların Coğrafi Dağılımı



Fidye yazılımı truva atları tarafından yapılan saldırıların coğrafi dağılımı,

Kasım 2020 — Ekim 2021

Fidye yazılımı truva atlarının en çok görüldüğü 10 ülke:

Sıra	Ülke	Yüzdesi (%)
1	Bangladeş	3.69
2	Haiti	1.79
3	Sudan	1.69
4	Türkmenistan	1.41
5	Filistin	1.33
6	Yemen	1.10
7	Tacikistan	1.03
8	Çin	1.01
9	Etiyopya	1.00
10	Pakistan	0.87

MacOS'a Saldırılar:

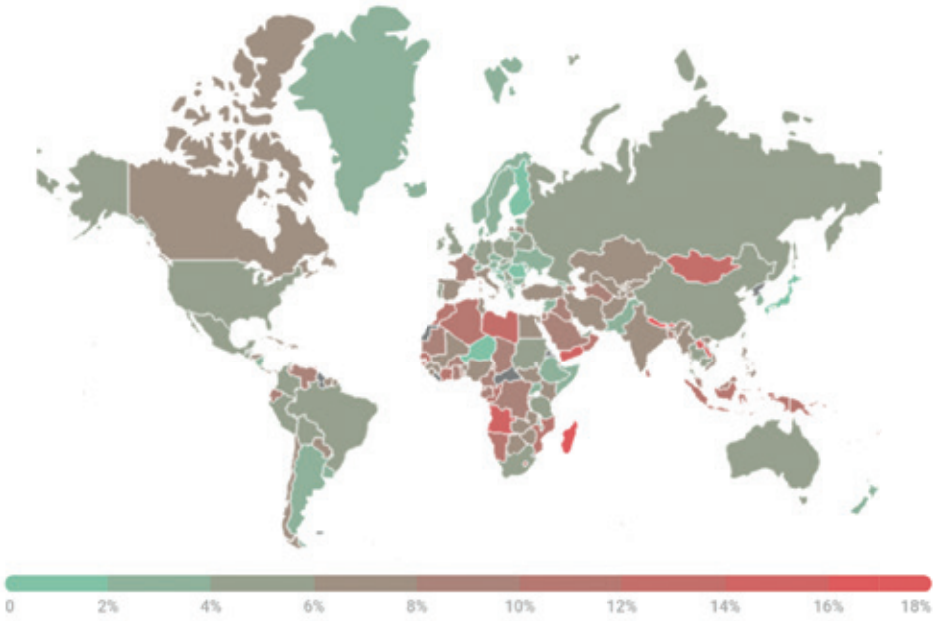
* İlgili rapora göre Türkiye'nin ilk 10'da yer aldığı tek başlıktır.

Raporlama dönemindeki en ilginç bulgular arasında Apple'ın M1 işlemcili MacBook'u için kötü amaçlı yazılım, MacOS için Rust'ta yazılmış yeni Convuster reklam yazılımı ve xCode geliştirme ortamındaki projelere bulaşan ve tarayıcılar ve diğer uygulamalardaki verileri çalan XCSSET truva atının yeni örnekleri vardı.

MacOS için en büyük 10 tehdit:

Sıra	Tehdit	Yüzdesi (%)
1	AdWare.OSX.Pirrit.ac	14.44
2	AdWare.OSX.Pirrit.j	11.39
3	AdWare.OSX.Bnodlero.at	9.91
4	Trojan-Downloader.OSX.Shlayer.a	9.33
5	AdWare.OSX.Pirrit.gen	9.00
6	Monitor.OSX.HistGrabber.b	8.49
7	AdWare.OSX.Pirrit.o	8.28
8	AdWare.OSX.Pirrit.aa	7.60
9	Trojan-Downloader.OSX.Agent.h	6.38
10	AdWare.OSX.Bnodlero.t	6.27

Tehditlerin Coğrafi Dağılımı:



MacOS için tehditlerin coğrafi dağılımı,

Kasım 2020 — Ekim 2021

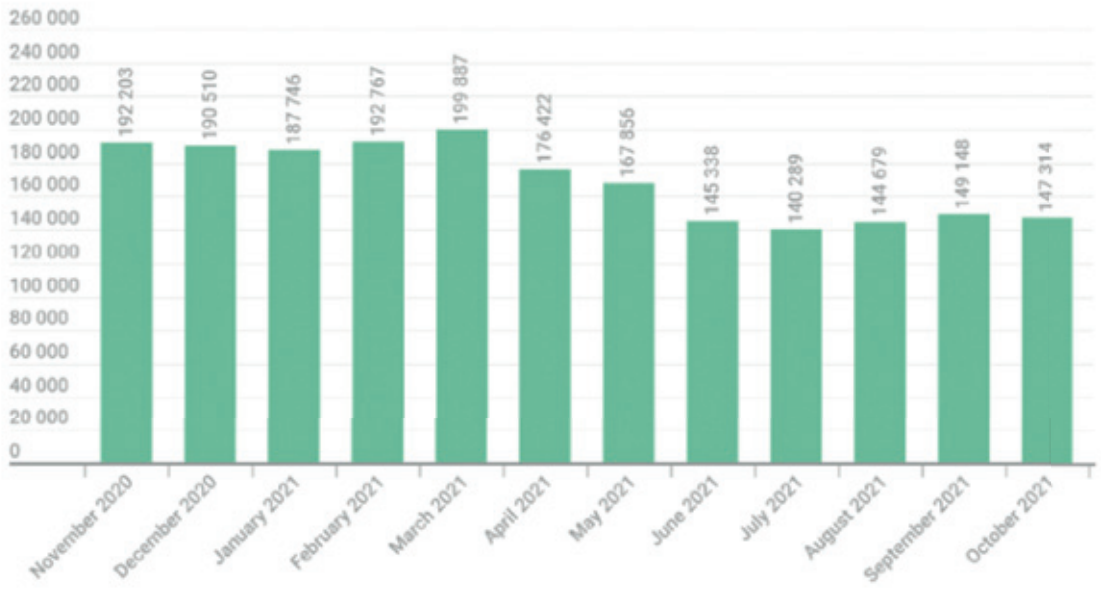
Saldırıya uğrayan kullanıcılara göre ilk 10 ülke:

Sıra	Ülke	Yüzdesi (%)
1	Ekvador	9.01
2	Fransa	8.04
3	İspanya	7.30
4	Vietnam	6.89
5	Kanada	6.81
6	Hindistan	6.45
7	İtalya	6.27
8	Türkiye	6.19
9	Birleşik Devletler	5.91
10	Meksika	5.60

Kripto para madencileri:

Madenciler tarafından saldırıya uğrayan kullanıcı sayısı

Raporlama döneminde, yaklaşık 1.2 Milyon (1.184.986) benzersiz kullanıcının bilgisayarına madenci (kripto para madenciliği kötü amaçlı yazılımı) yükleme girişimleri tespit edildi. Madenciler, tüm saldırıların %2.19'unu ve tüm Risktool tipi programların (sistemdeki dosyaları gizleme, çalışan pencereleri gizleme, etkin işlemleri sonlandırma vb. işlevleri olan programların kategorisi) %16.88'ini oluşturuyordu.

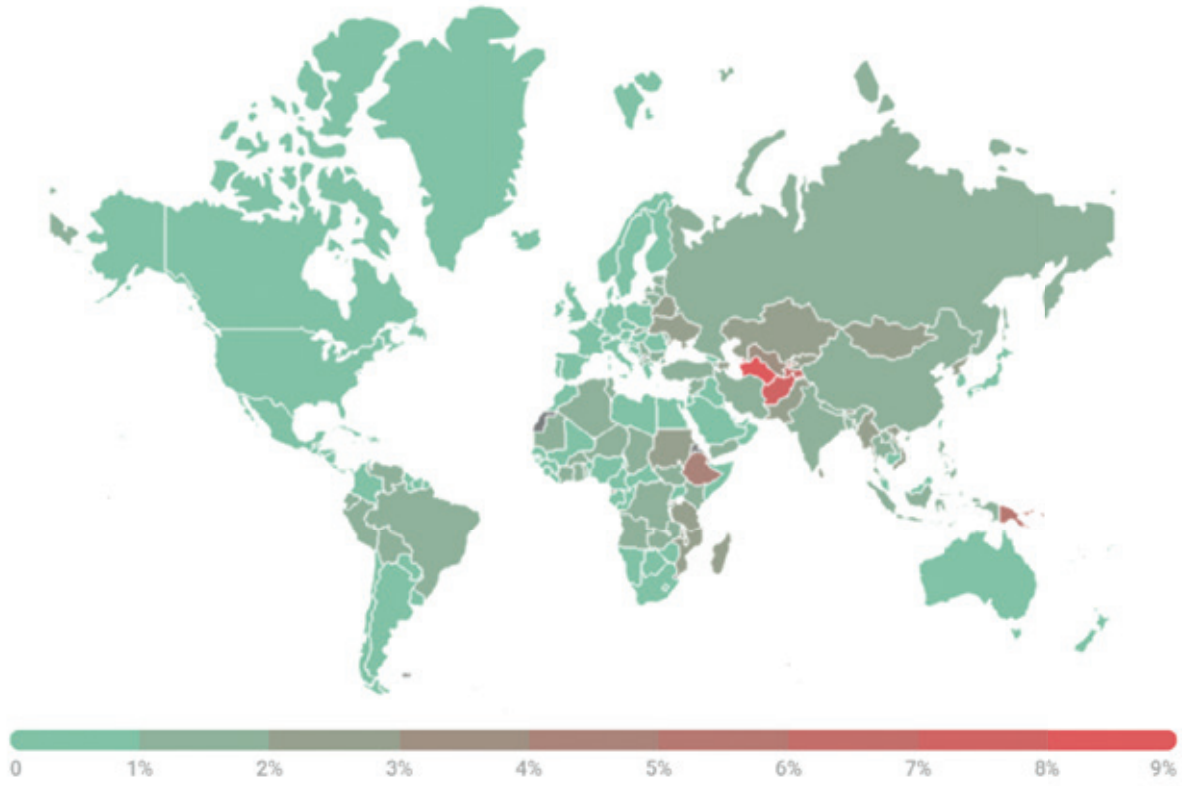


Madencilerin saldırdığı kullanıcı sayısı,

Kasım 2020 — Ekim 2021

Raporlama döneminde, Kaspersky ürünleri Trojan.Win32.Miner'ı diğerlerinden daha sık tespit etti ve madenciler tarafından saldırıya uğrayan tüm kullanıcıların %20,73'ünü oluşturuyordu. Bunu Trojan.Win32.Miner.gen (%11,58), Trojan.Win32.Miner.ays (%8,73) ve Trojan.Win32.Miner.vogh (%3,52) takip etti.

Saldırıların Coğrafi Dağılımı



Madencilerle ilgili saldırıların coğrafi dağılımı,

Kasım 2020 — Ekim 2021

2021'in En Büyük Veri İhlallerinden Bazıları

1. Facebook Veri Sızıntısı - 553 Milyon hesap:

Güvenlik araştırmacısı Alon Gal, nisan ayında Facebook'a ait 533 milyon hesap içeren sızdırılmış bir veri tabanı keşfetti.

Veriler, 106 ülkeden Facebook kullanıcılarının kişisel bilgilerini içeriyor. Insider (bir araştırma firması), sızdırılan verilerin bir örneğini inceledi ve bilinen Facebook kullanıcılarının telefon numaralarını veri setinde listelenen kimliklerle eşleştirerek birkaç kaydı doğruladı. Insider ayrıca, Facebook'un kullanıcının telefon numarasını kısmen ortaya çıkarmak için kullanılabilen parola sıfırlama özelliğinde veri setindeki e-posta adreslerini test ederek kayıtları doğruladı.

2. Bykea Veri Sızıntısı - 400 Milyon hesap:

Ocak ayında, araştırmacı Sen tarafından yönetilen Güvenlik Dedektifleri ekibi, belirli bağlantı noktalarında rutin IP adresi kontrolleri sırasında bir Elastik sunucu güvenlik açığı keşfetti. Sunucu, merkezi Pakistan Karaçi'de bulunan nakliye, lojistik ve teslimatta nakit ödeme şirketi olan Bykea için API günlüklerini içeriyordu.

Araştırmacılar, Bykea'nın tüm üretim sunucusu bilgilerini parola koruması veya şifreleme olmadan herkese açık olarak ifşa ettiğini ve 400 milyondan fazla kayıt içeren 200 GB'tan fazla veriye erişime izin verdiğini keşfetti. Veriler, kişilerin tam adlarını, konumlarını ve hacker'ların potansiyel olarak maddi manevi zarar vermek için kullanabilecekleri diğer kişisel bilgilerini içeriyordu.

3. Android Kullanıcıları Veri Sızıntısı - 100 Milyondan Fazla:

Mayıs ayında, güvenlik araştırmacıları, bulut hizmetlerinin çeşitli yanlış yapılandırmaları nedeniyle açığa çıkan 100 milyondan fazla Android kullanıcısının kişisel verilerini keşfetti. İndirmeleri 10.000 ila 10 milyon arasında değişen 23 uygulama tarafından kullanılan korumasız gerçek zamanlı veritabanları, dahili geliştirici kaynaklarını içeriyordu.

Check Point araştırmacıları, kullanıcıların adları, e-posta adresleri, doğum tarihleri, sohbet mesajları, konumları, cinsiyetleri, parolaları, fotoğrafları, ödeme bilgileri, telefon numaraları ve anında iletme bildirimleri gibi hassas ve kişisel bilgilerine erişilebileceğini keşfetti.

4. Brezilya Veri tabanı - 223 Milyon:

Ocak ayında Brezilya tarihinin en büyük kişisel veri ihlali keşfedildi. Veri setleri PSafe tarafından keşfedildi ve sonrasında Technoblog tarafından rapor edildi. Veri tabanları ad, vergi numarası, adres, telefon numarası, e-posta, kredi puanı, maaş ve daha fazlasını içeriyordu. Ayrıca 104 milyon araç kaydı da mevcuttu. OpenDemocracy (Birleşik Krallık merkezli siyasi bir web sitesi), bilgilerin genel olarak kredi puanlama büroları tarafından kullanıldığını ve bunun da araştırmacıların sızıntının Brezilya'nın önde gelen firmalarından Serasa Exprerian'dan şüphelenmesine yol açtığını söyledi. Veriler, bir Darknet forumunda ücretsiz olarak sunuldu.

Yılın Özeti

Bu yıl, fidye ve kripto para madenciliği kötü amaçlı yazılımlarına maruz kalan kullanıcı sayısı oldukça fazla idi. Pandemi ile birlikte daha sık duyduğumuz "uzaktan çalışma" prensibi, ev ofislerindeki koruma seviyesinin, bilişim teknoloji güvenlik ekipleri tarafından güvenlik duvarları, yönlendiriciler ve erişim yönetimi gibi güvenlik önlemlerinin uygulandığı merkezi ofislerden çok daha düşük olmasından dolayı güvenlik risklerini de beraberinde getirdi.

Uzaktan çalışmanın popülerleşmesi, mobil cihazların sayısının daha da artmasına neden oldu. Uzaktan çalışanlar için halka açık Wi-Fi ağları ve uzaktan işbirliği araçlarını kullanarak tabletler ve telefonlar gibi çeşitli mobil cihazlar arasında geçiş yapmak normal oldu. Bunların bir sonucu olarak da mobil tehditler büyümeye ve gelişmeye devam etmektedir.

2022'de Nasıl Güvende Kalınır?

Kritik Erişim Yönetimi, bir kuruluşu veri ihlallerinden ve olası siber saldırılardan korumanın anahtarıdır. Bir kuruluş, kritik erişim yönetiminin üç sütununu (erişim yönetimi, erişim denetimi ve erişim izleme) izleyen çözümleri uygulayarak, kimin neye erişimi olduğu konusunda görünürlük kazanabilir, Sıfır Güven Ağ Erişimi gibi ayrıntılı erişim kontrolleri uygulayabilir ve önleme için erişimi daha iyi izleyebilir.

2021'in gösterdiği ve 2022'nin kesinlikle tekrar göstereceği gibi, hacker'lar kayıtsızlığa güveniyor ve kuruluşlar içinde istismar edilebilecek zayıflıklar bulmaya devam edecekler. Erişim noktalarının ve varlıkların güvenliğinin sağlanması artık isteğe bağlı değil, kritik öneme sahip.

Kaynaklar

- https://securelist.com/kaspersky-security-bulletin-2021-statistics/105205/
- https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list
- https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021
- https://securityboulevard.com/2021/12/reviewing-the-biggest-data-breaches-of-2021/

ISSN 2618 6373