LABRIS SOC RAPORU

/// 2015
SİBER GÜVENLİK RAPORU

/// 2016
SİBER GÜVENLİK ÖNGÖRÜLERİ

Labris NETWORKS

LABRIS
NETWORKS INC.

TELİF HAKKI

FERAGATNAME

Labris Networks, 2002 yılından bu yana, global olarak kanıtlanmış ürünleriyle Ar-Ge odaklı ve hızla büyüyen bir ağ güvenlik çözümleri sağlayıcısı olmuştur. Labris Networks, LABRIS UTM, Labris LOG ve Harpp DDoS Mitigator cihazlarında Güvenlik Duvarı/VPN, Web Güvenliği, E-posta Güvenliği, Yasal Dinleme ve Erişilebilirlik Koruma çözümlerini içeren geniş ürün yelpazesi aracılığıyla en üst düzey ağ güvenliğini garanti etmektedir. Gelecek nesil çözümler, sızmalar, virüs, spam, zararlı yazılım ve erişilebilirlik saldırılarına karşı bir akıllı kalkan sağlayarak her türlü gerçek zamanlı tehditleri, uygulamaları tespit etmek, tanımlamak üzere geliştirilmiştir.

Labris Networks ürünleri çeşitli topolojiler ve dağıtım senaryolarına sahip tüm boyutlardaki ağları korur. Labris FLEX donanım yazılımı seçenekleri sayesinde kullanıcılar ihtiyaç duydukları güvenlik yazılımının yanı sıra Kablosuz Misafir Kimlik Doğrulaması, Ayrıntılı İnternet Raporlama, Yasal Dinleme ve Günlükleme gibi ekstra modülleri alma ayrıcalıklarına sahiptir. Müşteri odaklı, geleceğe yönelik ve esnek bir yaklaşıma sahip olan Labris Networks, yazılımlarını Bulut içerisinde de sunmaktadır.

20'den fazla ülkede hızla büyüyen küresel ağlarda işlemleri olan Labris ürünleri, işletmeleri, markaları, devlet kurumlarını, hizmet sağlayıcıları ve kritik altyapıları korumaktadır.

Dünya çapındaki ortakları ile Labris Networks, çok dilli Küresel Destek Merkezi ile en iyi satış sonrası desteği sağlayarak en yüksek düzeyde müşteri memnuniyeti ve sadakatine kendisini adamıştır. Hızla büyüyen küresel bir oyuncu olan Labris müşterilerine en uygun maliyetle en üst düzeyde güvenlik sunmaktadır. Ankara, Türkiye merkezli olan Labris Networks, Avrupa, Orta Doğu, Kuzey Afrika, Kafkaslar, Orta ve Güneydoğu Asya'ya hizmet veren ofislere sahiptir.

2015

GÜVENLİK TEHDİTLERİNE BAKIŞ

///YILIN BAZI ÖNEMLİ AĞ SALDIRILARI

ÖNEMLİ BİLGİSAYAR KORSANLIĞI VE BİLGİ KAÇAKLARI

ABD Personel İşleri Dairesi (OPM)'ye İki Kez İzinsiz Girildi, OPM Direktörü İstifa Etmek Zorunda Kaldı

Çinli Bilgisayar Korsanları, Aralık ayında Personel İşleri Dairesi'nin bilgisayar sistemini ihlal etti fakat bu durum ancak Haziran 2015'te açıklandı. Mevcut ve eski 4 milyon federal çalışanın kişisel verileri ele geçirildi. Temmuz ayında bir saldırı daha yapıldı ve bu sefer 21,5 milyon kişinin Sosyal Güvenlik numaraları ve diğer gizli bilgileri sızdırıldı.

Sonuçta OPM yöneticileri doğrudan senatoya izahat vermek zorunda kaldı. Bu olay, yöneticilerin senatörler tarafından güvenlik ihlallerine karşı yetersiz önlemlerden sorumlu tutulabileceklerini gösterdi.

BRITISH AIRWAYS

British Airways'in Sık Uçan Yolcu Programı Hesapları Ele Geçirildi

Bilgisayar korsanları, on binlerce British Airways sık uçan yolcu bilgisine izinsiz erişti.

T-Mobile

15 Milyon T-Mobile Müşterisinin Gizli Bilgileri Açığa Çıktı

Eylül 2015'te, iletişim operatörü T-Mobile'dan hizmet almak için başvuruda bulunan 15 milyon kişinin verileri sızdırıldı. T-Mobile CEO'su John Legere, sızdırılan veriler arasında isimler, adresler, doğum tarihleri, Sosyal Güvenlik numaraları, ehliyet ve pasaport numaraları bulunduğunu açıkladı.

37 MİLYON VERİ SIZDI

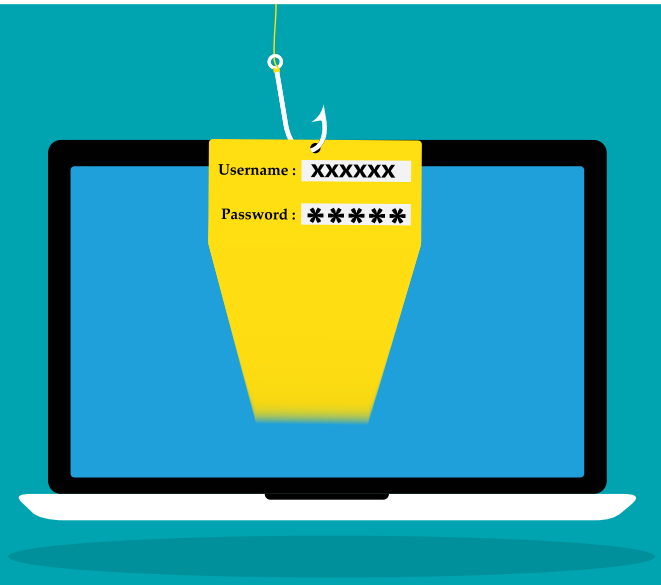
Online Aldatma Sitesi AshleyMadison Ele Geçirildi

Temmuz 2015'te, AshleyMadison'ın 37 milyondan fazla üyesine ait veriler sızdırıldı. Sızdırılan veriler arasında müşteri profillerinin yanı sıra gizli cinsel fanteziler ve kredi kartı işlemleri, gerçek isim, adresler ve çalışanlara ait belgelerle e-postalar gibi bilgiler yer alıyordu.

Adult FriendFinder Ele Geçirildi

Mayıs 2015'te, 3,9 milyon Adult FriendFinder üyesinin gizli verileri sızdırıldı. Yayınlanan veriler, hesaplarının siteden silinmesini isteyen kişilerin bilgilerini de içeriyordu. Çalınan veriler arasında kullanıcıların cinsel tercihleri, eşcinsel olup olmadıkları, hatta evlilik dışı ilişkiler arayıp aramadıkları gibi son derece özel bilgiler yer alıyordu. Ek olarak, bilgisayar korsanları kullanıcıların e-posta adreslerini, kullanıcı adlarını, doğum tarihlerini, posta kodlarını ve IP adreslerini de yayınladılar.

/// SİBER GÜVENLİK TRENDLERİ



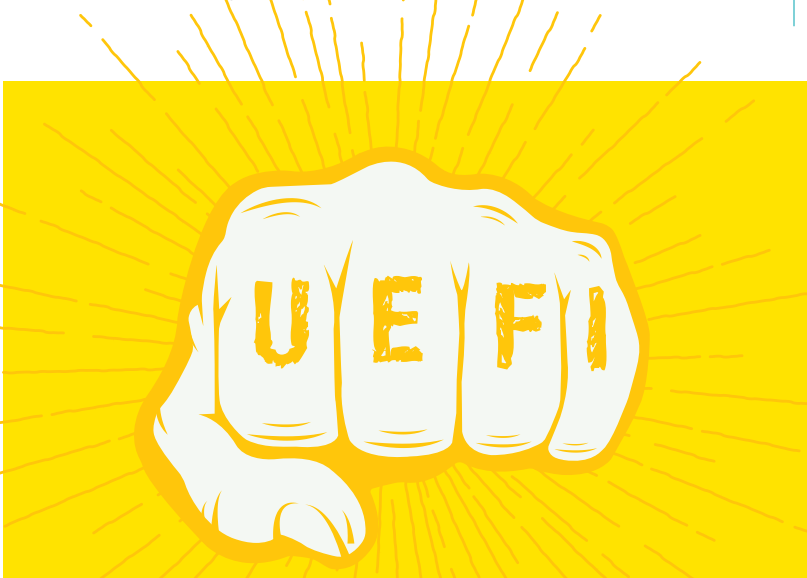
CryptoLocker

CryptoLocker fidye yazılımı, 2015 yılı boyunca yayılmaya devam etti. Yazılım, ağırlıklı olarak en büyük mobil ağ operatörlerinden ve kargo şirketlerinden gelmiş gibi görünen kimlik avı e-postalarıyla yayıldı. Fatura görünümündeki e-posta, sahte bir "Faturanız hakkında ayrıntılı bilgi" ve benzeri bağlantı aracılığıyla kurbanı fidye yazılımını indirmeye yönlendiriyordu. Fidye yazılımı indirilerek çalıştırıldığında, tüm belgeler (.doc, .xls, .pdf, vb) şifreleniyor ve belgeleri geri almak için kurbandan yaklaşık 1000$ fidye isteniyordu. Labris SOC, şimdiye kadar fidye yazılımı içeren onlarca kötücül yazılım ve binlerce alan adı belirledi ve her gün yeni alan adları keşfetmeye devam ediyor.

Fidye Trendi Yükselişte

Bu yıl, fidye amacıyla vatandaşlara yapılan rastgele saldırılarda da kurumları hedef alan saldırılarda da artış yaşandı. Fidyeler genellikle bitcoin olarak talep ediliyor. Merkezi İsviçre'de bulunan şifreli e-posta sağlayıcısı ProtonMail, 2015'te bir DDoS saldırısına maruz kaldı. İlginç bir şekilde, saldırganlar talep ettikleri 15 bitcoin (yaklaşık 6.000$) fidyeyi alarak amaçlarına ulaştılar. Ancak DDoS saldırıları hiçbir şey olmamış gibi devam etti.

Yunan bankaları da Kasım 2015'te DDoS saldırılarına hedef oldu. Saldırganlar, her bir bankadan 20.000 Bitcoin (7 milyon Euro) talep ettiler. Fidye ödenmedi. Birleşik Arap Emirlikleri Bankası da 3 milyon dolar fidye vermedikleri takdirde müşteri verilerinin sızdırılacağı tehdidiyle karşı karşıya kaldı. Birleşik Arap Emirlikleri Bankası fidyeyi ödemeyince, bilgisayar korsanları müşteri verilerini yayınladı. Artık fidyenin siber korsanların en önemli hedeflerinden olduğu söylenebilir hale geldi.



Bu yıl, ünlü "Hacking Team" ekibi siber saldırıya uğradı ve eylemlerine ilişkin 400GB'ın üzerinde verisi sızdırıldı. Hacking Team özetle devlet ve bilinmeyen aktörlerin vatandaş bilgisayarlarına sızmaları için yazılım ve sistemler sağlayan bir şirketti. Hacking Team'in, Galileo adlı Uzaktan Kontrol Sistemini kurbanlarının bilgisayarlarında tutabilmek için bir UEFI BIOS Rootkit'i kullandıkları ortaya çıktı. İşletim sistemini yeniden yüklemek veya yeni bir sabit disk satın almak bile bu kötü amaçlı yazılımdan kurtulmayı sağlamıyordu. Sızdırılan verilere göre, birçok devlet kurumu da bu hizmetten yararlanıyordu.

Zombi Mobil Aygıtlar

Cep telefonlarının performansı ve mobil ağların hızı arttıkça, cep telefonları da büyük ölçekli saldırılarda kullanılmaya başlandı. Ağustos 2015 sonlarında, cep telefonları kullanılarak bir web sitesine büyük bir DDoS saldırısı yapıldı. Ele geçirilen 650.000 akıllı telefondan saniyede 275.000 HTTP paketi ile 4,5 milyar istek gönderildi.

IoT Güvenlik Tartışmaları

Kasım ayında, çocuklara yönelik akıllı oyuncaklar ve tabletler üreten oyuncak markası Vtech'in sistemine izinsiz girildi. Dünya çapında toplam 5 milyon müşteri hesabı ve bu hesaplarla ilişkili çocuk profili saldırıdan etkilendi. Sızdırılan veriler arasında isimler, e-posta adresleri, parolalar, parola yenilemek için kullanılan gizli sorular ve yanıtları, IP adresleri, posta adresleri ve indirme geçmişleri bulunuyordu. Üstelik, veritabanında çocuklara ait isim, cinsiyet ve doğum tarihi gibi bilgiler de vardı. Çocuklarla ebeveynlerine ait fotoğraflar, birbirleriyle yaptıkları sohbetlerin içerikleri bile yayınlandı.

Araştırmacılar Charlie Miller ve Chris Valasek, mobil şebekeye bağlı bir araç eğlence sisteminin açıklarından yararlanarak bir Jeep Cherokee'yi kilometrelerce öteden kontrol etmenin mümkün olduğunu gösterdiler.

Yalnızca oyuncaklar ve arabalar değil, ayrıca buzdolapları, bebek monitörleri, keskin nişancı tüfekleri ve akıllı televizyonlar da izinsiz giriş ve güvenlik araştırmalarının odak noktasında yer aldı.

Sağlık Sektöründe Güvenlik Bilinci Düşük

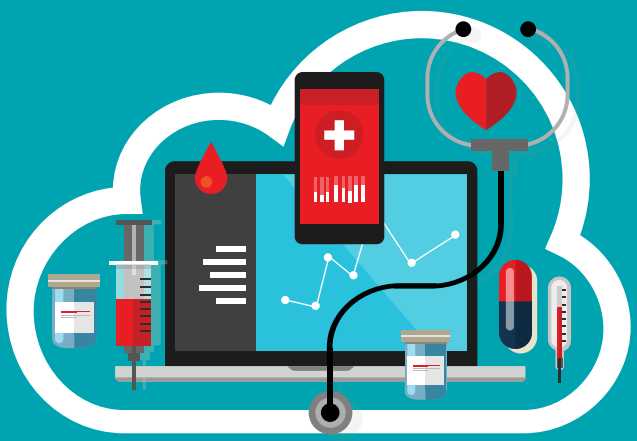
Amerika'nın en büyük sağlık sigortası şirketi Anthem, sektörün belki de en büyük siber saldırılarından birinin kurbanı olduğunu açıkladı.

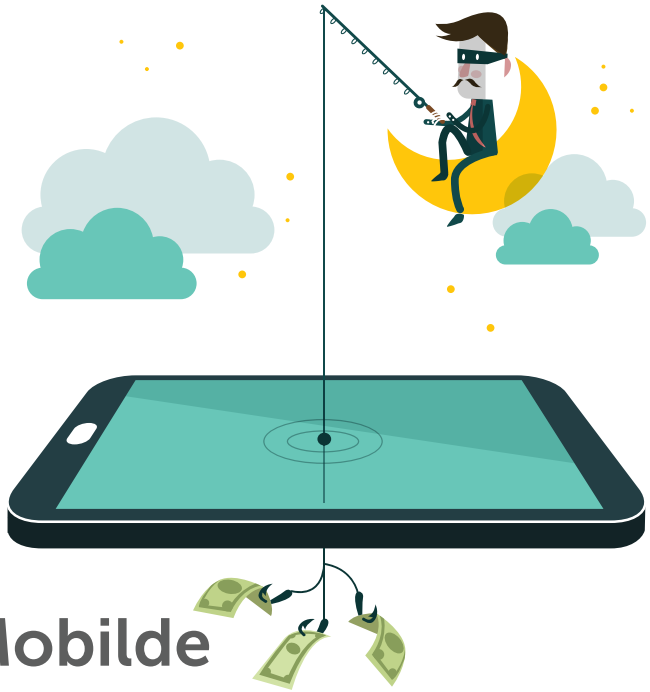
Anthem, 24 Şubat 2015 tarihinde bilgisayar korsanlarının sunucularına girdiklerini ve kişileri tanımlayıcı bilgiler içeren 78,8 milyon kaydın muhtemelen çalındığını bildirdi. Ele geçirilen bilgiler arasında isimler, doğum tarihleri, tıbbi kimlikler, sosyal güvenlik numaraları, sokak adresleri, e-posta adresleri, istihdam bilgileri ve gelir bilgileri yer alıyordu.

Premera Blue Cross sağlık sigortası şirketi, Mart 2015'te yaklaşık bir yıl önce 11 milyon hasta kaydına erişildiğini fark etti.

Bilgisayar korsanları, Temmuz 2015'te UCLA Sağlık Sistemi veritabanını hedef aldılar. 4,5 milyonun üzerinde hastanın şifrelenmemiş kayıtlarına erişmiş olabilecekleri düşünülüyor.

Sağlık kurumları artık yüksek güvenlikli yazılım ve sistemler geliştirme konusunda deneyim sahibi ve daha fazla saldırıya maruz kalıyorlar. NIST'e göre, Sağlık kritik önemli bir altyapı ve buna göre yönetilmesi gerekiyor.





Mobilde Güvenlik Şart

ABD'de yeni bir Android kilit ekranı fidye yazılımı yayılmaya başladı. Aygıta bulaşan yazılım, yeni bir PIN belirliyor ve kullanıcıdan 500$ fidye ödemesini istiyor. Ne yazık ki, bu yazılımın bulaştığı aygıtlara yeniden erişim sağlamanın etkili bir yolu bulunmuyor.

Akıllı L7 DDOS – APT – Bir Hizmet Olarak Hack

VPS bulut hizmeti sağlayıcısı Linode, Noel döneminin başından beri birçok DDoS saldırısına maruz kalıyordu. Saldırılar, 2016'nın ilk günlerinde de devam etti. DDoS saldırısı, Linode'nin Atlanta, Fremont, Newark, Dallas, Singapur ve Londra'daki veri merkezlerinin çoğunu etkiledi. Büyük hizmet kesintileri, müşterilerin olumsuz tepkilerine yol açtı.

Kötü amaçlı kişilerin, Linode'nin işlerine önemli derecede zarar vermek için büyük miktarlarda botnet kapasitesi satın aldığı ortaya çıktı. Saldırı kampanyası; DNS, volumetrik, Layer7 HTTP ve yönlendirici kontrol kartlarını hedefleyen saldırılardan oluşuyordu.

Harpp DDoS CERT'in istatistiklerine göre bu tür karma DDoS saldırıları giderek daha fazla kullanılıyor.

Politik Amaçlar Devletleri Ana Hedef Haline Getiriyor: Türkiye'nin Önemli Altyapılarına DDoS Saldırıları

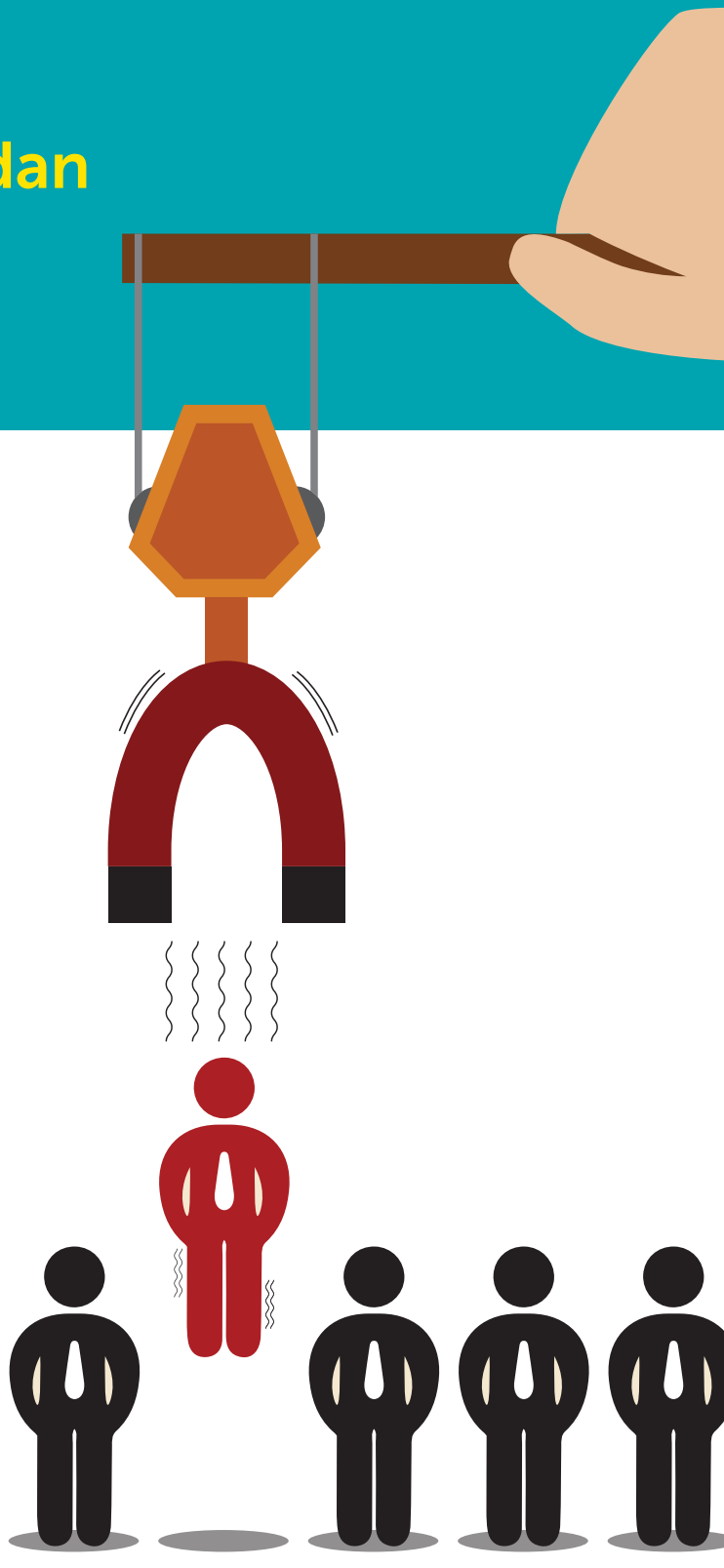
Kasım 2015'te, Tayland devletine ait birçok web sitesi DDoS saldırılarına hedef oldu. Bu saldırılar sonucunda bazı Tayland kamu sitelerine saatlerce ulaşılamadı.

14 Aralık 2015'te, saldırılar ".tr" uzantılı alan etki alanlarının kök DNS sunucularını hedef aldı. Saldırılar, DNS kuvvetlendirme saldırıları olarak başladı. Saldırının amacı, ".tr" DNS sunucularını yanıt veremeyecek hale getirerek ".tr" uzantılı web sitelerine erişimi engellemekti. 200 Gbps'ye ulaşan saldırılar, 40 Gbps fiber bağlantılara aşırı yük oluşturdu. Bu, Türkiye'nin şimdiye dek karşılaştığı en güçlü saldırıydı. 24 Aralik'ta, başka bir saldırı dalgası Türkiye'nin önde gelen bankalarını hedef aldı. Kredi kartı ve bankacılık işlemlerinde bazı sorunlar yaşanmasına yol açtı. Kredi kartı terminalleriyle ödeme alınamadı. Bu saldırılar, ünlü bilgisayar korsanı grubu Anonymous tarafından üstenildi. Rus savaş uçağının Kasım 2015'te Türk Hava Kuvvetleri tarafından düşürülmesi ile yakın dönemde gerçekleşmesiyle bu siber saldırılar Rusya ile de ilişkilendirildi. Bu saldırıların ilermesi ve hedeflerin seçimi Rusya tarafından 2009 'da gerçekleştirilen Estonya siber saldırı dalgasındakilerile de benzeşiyordu.

Global Yönlendirici Botnet'leri

Şubat ayında, VOIDSEC'teki bir güvenlik uzmanı, kişisel web sitesinde olağandışı bir durumun tekrarlandığını gözlemledi. WordPress sitesine deneme yanılma saldırısı yapılıyordu. Biraz daha araştırdığında, saldırganların genellikle İtalyan servis sağlayıcılardan ve tamamının Aethra modemler ve yönlendiricilerden geldiğini anladı. LizardSquad tarafından Xbox Live ve Play Station Network'e yapılan ünlü saldırılar sırasında da Botnet kullanıldığı ortaya çıkmıştı. Dolayısıyla Labris SOC 2015 öngörülerin yer verildiği şekilde dünyada yaygın olarak kullanılan bir takım yönlendiricilerden botnet oluşturmasına tanık olunmuş oldu.

Linux Tabanlı Bot'lar ve eski Protokoller tarafından yapılan saldırıların boyutları artıyor



Kasım ayında, Labris SOC bal çanağı (honeypot) sunucularımızdan birine SSH deneme yanılma saldırısı yapıldığını keşfettik. SSH oturum açma girişimleri 6 Kasım 2015 tarihinde başladı ve 8 Kasım'da SSH oturum açma girişimi tek bir gün içinde 500.000'i aşarak zirve yaptı. 12 Kasım'a kadar süren saldırı, gücünü giderek yitirdi. Saldırgan, 168 benzersiz IP adresinden SSH oturum açma girişimi uyguladı ve 4 günün sonunda saldırganlar SSH parolasını kırmayı başardılar. Bal çanağından takip edildiğinde SSH parolasını ele geçiren saldırganın, sisteme erişerek hedefine kötü amaçlı bir yazılım yüklediğini ve kötü amaçlı yazılımın kendini birçok dizine kopyaladığı bir sistem servisi oluşturduğu ve kendini başlangıca eklediğini tespit ettik. Bu yazılım komuta kontrol sistemi üzerinden DDoS saldırısı emri alabiliyordu. İncelediğimizde yazılımın desteklediği saldırıların şunlar olduğunu tespit ettik: SYN Flood, ACK Flood ve DNS Kuvvetlendirme saldırıları.

Bu durum, 2015 yılında saldırı boyutlarının artmasındaki nedenlerden biridir. Artık sunucular botnet'lerin parçası haline geliyor. Bunlar gibi birçok ele geçirilmiş sunucunun gücü bir araya getirilerek büyük ölçekli DDoS saldırıları düzenleniyor. Ele geçirilen Linux tabanlı bu bot'ların Aralık ayında Türkiye'ye yapılan büyük ölçekli DDoS saldırılarında kullanılmış olma olasılığı da oldukça yüksek.

Öte yandan, 2015 içinde yansıtılmış DDoS saldırıları da yeni vektörler kazandı. Chargen ve SSDP'nin, 2015 yılında artan DDoS saldırılarının yeni yansıtma ve yükseltme protokolleri olduğunu gördük.

DDoS Saldırısı, Veri Hırsızlığını Gizlemek için Paravan Olarak Kullanıldı

Bilgisayar korsanları, merkezi İngiltere'de bulunan cep telefonu satıcısı Carphone Warehouse'a DDoS saldırısında bulundular. Ancak bu saldırı, 2,4 milyon müşterinin kişisel bilgilerinin çalındığı saldırıları gizlemek için paravan olarak kullanıldı. Saldırganların, yaklaşık 90.000 müşterinin şifrelenmiş kredi kartı bilgilerine erişmiş olabileceği bildirildi.

Ekim 2015'te, 4 milyonun üzerinde müşterisi olan İngiliz telekomünikasyon şirketi TalkTalk'un verilerine erişildi. 56.959 müşterinin hesabı bu ihlalden etkilenirken böylece müşterilerinin %4'ünün finansal verileri ele geçirilmiş oldu. TalkTalk, kaybettikleri verilerin şifreli olmadığını ve yasal olarak bu verileri şifrelemekle yükümlü olmadıklarını bildirdi. DDoS saldırısı bu sızmada da güvenlik uzmanlarını oyalamak için yine paravan olarak kullanılırken, bilgisayar korsanlarının da farklı bir açıktan yararlanarak sitedeki kişisel verileri ele geçirdiği görüldü.

Yetersiz Güvenlik Ürünleri Güvenilirliği Zedeliyor

9 Ocak'ta FortiOS'un eski sürümlerini etkileyen bir SSH arka kapısı bulunduğu açıklandı. Fortinet, sorunun kötü amaçlı bir arka kapı yazılımı değil, yönetim kimlik doğrulama hatası olduğunu iddia etti.

Juniper, Aralık 2015'te ScreenOS'ta bir saldırganın NetScreen aygıtlarına yönetici erişimi sağlamasına yol açabilecek izinsiz bir kod keşfetti. Güvenlik açığı, bir SSH arka kapısı kullanıyordu ve bir başka açıksa güvenli olmayan bir VPN modu kullanıyordu.

Bu iki önemli sorun, güvenlik ürün sağlayıcılarına duyulan güveni sarstı.

2016

SİBER GÜVENLİK HAKKINDA 2016 ÖNGÖRÜLERİ

/// BAŞLICA ÖNGÖRÜLER

/// DİĞER ÖNGÖRÜLER

/// BAŞLICA ÖNGÖRÜLER

DDoS Saldırıları, Veri İhlallerini Gizlemek için Paravan Olarak Kullanılacak

CarPhone Warehouse ve TalkTalk'a yapılan veri ihlali saldırılarının başarılı olmalarında DDoS saldırılarının paravan olarak (smokescreen) kullanılmasının da etkisi var. Saldırganlar bunun başarılı bir teknik olduğunu fark ettiler ve veri ihlallerinde dikkat dağıtmak için DDoS saldırılarının paravan olarak kullanıldığına daha fazla tanık olacağız.

HTTPS Üzerinden Yapılan Saldırılar

Kötü amaçlı reklamlar (malvertising), kötü amaçlı yazılımları yaymak için kullanılan online reklamlara verilen addır. Kötü amaçlı reklamlar, meşru online reklam ağlarına ve web sitelerine kötü amaçlı yazılım içeren reklamlar ekliyor. Bazı ürünler ve hizmetler kötü amaçlı reklamları algılamada giderek daha başarılı olsa da saldırganlar yeni teknikler bulmakta gecikmiyor. 2016'da HTTPS aracılığıyla yayılan ve başarılı olan kötü amaçlı reklamlarda artış olmasını bekliyoruz. Kurumunuz HTTPS trafiğini takip eden güvenlik ürünleri kullanmıyorsa, risk altında olabilirsiniz.

Mobil ve IoT, Botnet'lerin Önemli Bir Parçası Olacak

Botnet'lere eski CCTV'lerin ve akıllı televizyonların da katılması, yakın gelecekte IoT aygıtları ve mobil cihazların da botnet'lerin önemli birer parçası haline geleceğinin işareti niteliğinde. 4G-5G ağlarının sunduğu hız göz önüne alındığında, saldırı kapasitelerinin küçük ölçekli olmayacağını söyleyebiliriz.

İnternet Servis Sağlayıcılar da Kritik Altyapılar Olarak Kabul Edilmeli

Linode saldırıları gösterdi ki, İSS'lar tarafından işletilen ve internetin kapılarını aralayan yönlendiriciler de saldırıların hedefi oluyor. Saldırganlar, internet erişimimizin yanı sıra, internete açılan yoldaki bazı ara cihazları etkilemeye çalışıyorlar. HARPP DDoS CERT'te, hem yönlendiricileri hem de BGP noktalarını hedef alan birçok DDoS saldırısına tanık olduk ve müdahale ettik. Yönlendiricilerin kontrol devre kartlarını hedefleyen saldırılar cihazların yönlendirme devre kartlarını da etkileyerek cihazların yönlendirdiği trafikler sorunlar oluşturdu. 2016 yılında da bu tür saldırıların devam etmesini bekliyoruz. Ne yazık ki, ara yönlendiricilerin çoğu, kendilerini hedefleyen paketleri almaya açık durumda. Tüm İSS'ler, ara ağ ekipmanlarının güvenliğini belirli bir düzeye çıkaracak düzenlemelere tabi tutulmalı.

Ulusal Güvenlik Daha Yerel Hale Gelirken, Güvenlik Ürünlerinde Bilerek veya İstemeden Ortaya Çıkarılan Güvenlik Açıkları ve Arka Kapıların Sayısı Artacak

2015'te, Fortinet ve Juniper ürünlerinde çeşitli güvenlik açıkları ve arka kapılar bulunduğunu gördük. Bu olaylar, güvenlik ürünlerinin kendi güvenlik ve güvenilirliklerinin sorgulanmasına yol açtı. Bu nedenle araştırmacılar bu yıl dikkatlerini güvenlik ürünlerine yönlendirecek ve sonucunda daha fazla güvenlik açığı ve arka kapı keşfedilecek. Bu güvenlik açıkları ve arka kapılar, Amerika dışında dünyanın diğer bölümlerinde ulusal siber güvenlik endişelerini arttırıyor. Ülkeler, siber güvenlik konusunda kendi ulusal önlemlerini geliştirmeye başladı ve artık milli çözümler bu noktada tek güvenli çözüm olarak kabul görüyor.

/// DİĞER ÖNGÖRÜLER

Sosyal Mühendislik ve Hedef Odaklı Kimlik Avı

Güvenlik zincirinin en zayıf halkası insanlar ve saldırganlar da bu gerçeğin farkında. Sosyal mühendislik, her zaman için saldırganların kullandığı ana taktiklerden biri olmuştur. 2015 yılında birçok veri ihlali gerçekleştiğinden, sızdırılan bu veriler ve gizli kişisel bilgiler, hedef odaklı kimlik avı e-postalarının meşru görünmeleri için kullanılacak. Şirketler, en yeni sosyal mühendislik tekniklerini de içeren güvenlik farkındalığı eğitimlerine daha fazla yatırım yapmalılar.

Mobilde Fidye Yazılımı

Geçtiğimiz yıllarda, çoğunlukla CryptoLocker ve türevleri ile olmak üzere birçok fidye yazılımı saldırısına şahit olduk. Bu kötü amaçlı yazılımlar tarafından kullanılan şifreleme yöntemleri geliştikçe, şifrelenen verileri çözmek de neredeyse imkânsız hale geldi. Bu nedenle birçok şirket şifrelenen verilerini kurtarmak için fidye ödemek zorunda kaldı. 2015 yılında, Android sisteminde kilit ekranı türünde birçok fidye yazılımı gördük. Android ve diğer mobil sistemlerin iş amaçlı kullanımı arttıkça, bu tür cihazlarda yer alan verilerin değeri de artıyor. Bu nedenle 2016 yılında mobil cihazlarda daha fazla fidye yazılımı içeren saldırı yapılmasını bekliyoruz.

Devlete Ait Siteler Başlıca Ana Hedef Olmaya Devam Edecek

Terörizm ve politik amaçlar da saldırıların ardında yatan başlıca nedenler arasında yer alıyor. Terörizm durmuyor, DAEŞ ve diğer terörist organizasyonlar saldırılarına devam ediyor. Siber alan da bir savaş alanı olduğundan, bu saldırılar siber alanda da yer alıyor. Türkiye'ye ve Tayland'a yapılan DDoS saldırılarının yanı sıra, Çin'in Amerikan Personel İşleri Dairesi'ne izinsiz girişinde olduğu gibi ABD'ye ait devlet sistemlerinde de güvenlik ihlalleri ve veri sızıntıları oldu. Devlet siteleri ve sistemleri, geçmiş yıllardaki gibi terörist organizasyonların, diğer devlet aktörlerinin ve vekillerinin ana hedefleri olmaya devam edecek.

/// DİĞER ÖNGÖRÜLER

IoT Kullanımındaki Artış IoT Tehditlerini de Artırıyor

2015'te IoT kapsamındaki ürün ve teknolojilerde birçok güvenlik ihlali yapıldı. Giderek daha fazla cihazın Nesnelerin İnterneti'nin bir parçası haline geliyor. Ama IoT cihazlarının, çoğu açıdan güvenli olarak tanımlanmaya hazır olmaması nedeniyle bu tehdit potansiyeli de artmaya devam edecek. IoT'deki sorunların artışındaki başlıca nedenler ise temel güvenlik korumalarının eksikliği, bellek ve işletim sistemi özelliklerinin yetersizliği ve çok geniş bir saldırı yüzeyine sahip olmasıdır.

Daha Fazla DDoS Saldırısı Yolda

2015 yılında yapılan DDoS saldırılarının sayısı rekor seviyelere ulaştı. 2015'te ayrıca 500 Gbps'ye kadar çıkan saldırılara tanık olduk. Saldırıların sayısındaki ve gücündeki bu artış, birçok faktörle ilişkili olabilir: Artan bant genişliği, ele geçirilen bilgisayar sistemi sayısının artması, kullanımı kolay DDoS araçlarının yayınlanması ve saldırı motivasyonunun artması. Bu faktörlerin hiçbirinde azalma olmadığından, yapılacak saldırıların sayıca ve güç bakımından artmaya devam edeceğini ve yeni rekor düzeylere ulaşacağını kolayca söyleyebiliriz.

Veri İhlalleri Şirketleri Batırmaya, Yöneticileri Kovdurmaya ve Muhtemelen Can Almaya Devam Edecek

Ashley Madison sitesindeki veri ihlalinin birçok sonucu oldu. Bilgileri sızdırılan kullanıcılar, Ashley Madison'ın sahibi olan Avid Dating Life ve Avid Media'ya 567 milyon dolar değerinde toplu dava açtı. Bu veri ihlalinin kurbanı olan en az üç kişi intihar etti. Bir başka veri ihlalinin kurbanı olan Vtech şirketi ise düşen hisse senedi fiyatları yüzünden Hong Kong borsasındaki işlemlerini durdurmak zorunda kaldı. ABD Personel İşleri Dairesi direktörü de iki veri ihlalinden sonra istifa etmek zorunda kaldı.

Bu veri ihlallerinin başarılı olduklarını, birçok şirketin ve kişinin çöküşüne neden olduğunu gören saldırganlar, daha da motive oldular. Artan motivasyon ve amacına ulaşan veri ihlalleri yüzünden ileride daha fazla ihlal olmasını bekliyoruz.

Mobil Uygulamalar Daha Sık Hedef Alınacak

Bazı mobil uygulamalar e-postalarımıza, kişilerimize, telefon numaralarımıza, coğrafi konumlarımıza, mesajlarımıza ve hatta fotoğraflarımıza erişebiliyor. Snapchat gibi popüler uygulamaların çoktan hedef alındığını biliyoruz. Makaleleri kaydederek internet erişimi olmadığında okumak için saklamaya yarayan popüler Android uygulaması Instapaper'da da bir güvenlik açığı bulundu. Artan müşteri talebini veya mobil uygulama ihtiyacını karşılamak isteyen uygulama geliştiricilerinin uygulamalarını yayınlamak için acele etmeleri ve güvenlik bakışlarının eksik olması güvenlik açıklarının gözden kaçmasına neden oluyor. Erişebildikleri bilgilerin değeri göz önüne alındığında, mobil uygulamaların güvenlik kalitesinin düşük olması bunları 2016'daki ana hedeflerden biri haline getirecek.