
MARC GOODMAN
GELECEĞİN SUÇLARI
DİJİTAL DÜNYANIN KARANLIK YÜZÜ
TİMAŞ

MARC GOODMAN

GELECEĞİN SUÇLARI

DİJİTAL DÜNYANIN KARANLIK YÜZÜ

TİMAŞ

I. KISIM

FIRTINA YAKLAŞIYOR

Bölüm 1

Bağlantılı, Bağımlı ve Savunmasız

"Teknoloji… Teknoloji garip şey;
bir elinde size harika hediyeler verirken,
diğeriyle sizi sırtınızdan bıçaklıyor."
– Charles Percy Snow

Mat Honan'ın hayatı monitörün başındayken gayet güzel görünüyordu. Web tarayıcısının bir sekmesinde yeni doğmuş kızının fotoğrafları açıktı, diğer sekmede ise binlerce Twitter takipçisinden gelen tweet'leri okuyordu. San Francisco merkezli *Wired* dergisinin bir muhabiri olarak, mütevazı bir hayat yaşıyor, teknolojiyi ise herkes kadar yakalamaya çalışıyordu. Bütün bunlara rağmen, dijital dünyasının tamamının sadece birkaç tuş ile silinebileceğinden habersizdi. Bir ağustos günüydü. Fotoğrafları, e-postaları ve çok daha fazlası, bir hackerın ellerine düşmüştü. Her şeyi, dünyanın öbür ucundaki bir çocuk tarafından çalınmıştı. Honan, kolay bir hedefti. Aslında hepimiz kolay birer hedefiz.

Honan, her şeyin yerle bir olduğu o akşamüzerini hatırlıyor: Evinin salonunda kızıyla oyun oynarken bir anda iPhone'u kapandı. Şarjı bitti herhalde, diye düşündü. Önemli bir arama beklediği için de, telefonunu fişe takıp yeniden başlattı. Ancak her zamanki açılış ekranı ve uygulamalarının yerine, büyük, beyaz Apple logosu ile yeni telefonunu kurmasını söyleyen çok çeşitli dillerde yazılmış "hoş geldiniz" ekranıyla karşılaştı. Garipsemişti.

Yine de Honan pek endişelenmedi, nihayetinde her gece iPhone'unu yedeklerdi. O yüzden sonraki adımı çok barizdi, iCloud'a giriş yapıp, telefonu ve içindeki verileri yeniden yükleyecekti. Apple hesabına girmeye çalışırken, doğruluğuna emin olduğu

parolasının, iCloud tanrıları tarafından yanlış görüldüğüne dair bir uyarı aldı. Dünyanın en seçkin teknoloji dergilerinden birinde muhabirlik yapan akıllı Honan, bu sefer başka bir numarasını sahnelemeye karar verdi. Sadece iPhone'unu dizüstüne bağlayacak ve kolaylıkla yerel bilgisayarındaki verileri kurtaracaktı. Fakat bundan sonra olanlar, kalbini durma noktasına getirdi.

Honan, Mac bilgisayarını açar açmaz, Apple'ın takvim programı tarafından gönderilen, Gmail parolasının yanlış olduğuna dair bir uyarı mesajıyla karşılaştı. Mesajın görünmesinden çok kısa bir süre sonra da, dizüstü bilgisayarının o güzeller güzeli ekranı soluk yeşile döndü ve kapandı. Sanki bilgisayarı ölmüştü. Ekranda görünen tek şey, bir komut istemiydi: "Lütfen dört basamaklı parolanızı girin." Honan, bilgisayarı için bir parola kurmadığını biliyordu.

Honan en sonunda, bir hackerın iCloud hesabına erişim sağlayarak, Apple'ın kullanışlı "iPhone'u Bul" uygulaması üzerinden onun dijital dünyasındaki tüm elektronik cihazların yerini belirlediğini öğrendi. Tüm cihazları birer birer ele geçiriliyordu. Hacker, "uzaktan sil" komutunu devreye almış, Honan'ın hayatı boyunca bir araya getirdiği tüm verileri silmeye başlamıştı. İlk düşen iPhone'u olmuştu, sonra iPad'i. En son ise, çok daha ağır bir şekilde MacBook'u gitmişti. Bir anda, kızının dünyadaki ilk senesinde çektiği bütün fotoğraflarla birlikte tüm verileri yok olmuştu. Çok uzun süre önce kaybettiği yakınlarıyla çektirdiği paha biçilemez fotoğrafları da bilinmeyen taraflarca geri getirilemez şekilde silinmişti.

Bunlardan sonra sıra Honan'ın Google hesabına geldi. Göz açıp kapayıncaya kadar, sekiz yıl boyunca dikkatlice toplanmış Gmail mesajları ortadan kalkmıştı. İş ile ilgili sohbetler, notlar, anımsatıcılar ve anılar, sadece bir tıkla dünyadan silinip gitmişti. Son olarak ise hacker asıl hedefine yöneldi: Honan'ın Twitter kullanıcı adı olan @Mat'i istiyordu. Hesabı ele geçirmesi bir tarafa saldırgan, hesap üzerinden Honan'ın binlerce takipçisine ırkçı mesajlar göndermişti.

Bu online katliamın ardından, bir araştırmacı gazeteci olarak Honan neler olduğunu öğrenmek adına parçaları bir araya getirmeye başladı. Apple'ın teknik destek hattını arayarak iCloud

hesabını yeniden almak istedi. Doksan dakika telefonda kaldıktan sonra, Honan bu talepten otuz dakika önce yine kendisinin arayıp parolasının sıfırlanmasını talep ettiğini öğrendi. Anlaşılan, birinin Honan'ın parolasını değiştirmek için bilmesi gereken tek şey, fatura adresi ile kredi kartı numarasının son dört hanesiydi. Honan'ın adresi ise, kişisel internet sitesini kurarken girdiği için Whois İnternet alan adı kayıtlarında yer alıyordu. Orada olmasa bile, WhitePages.com ve Spokeo gibi online servisler üzerinden bunu bulmak da çok kolay olurdu.

Honan'ın kredi kartı numarasının son dört hanesi için de hacker, Honan'ın (birçoğumuz gibi) bir Amazon.com hesabı olacağını tahmin etti ve haklı çıktı. Honan'ın bütün bilgilerine, e-postalarına ve posta adreslerine sahip olan saldırgan, Amazon ile iletişime geçip bir müşteri hizmetleri temsilcisini başarılı bir şekilde kandırarak, kredi kartı numarasının son dört hanesini öğrenmişti. Çok basit görünen birkaç hamle ile birlikte Honan'ın hayatı altüst olmuştu. Bu seferlik öyle olmamış olsa da, hacker kolaylıkla aynı bilgileri kullanarak Honan'ın banka hesaplarına erişim sağlayıp parasını da çalabilirdi.

Nihayetinde saldırıyı üstlenen genç –hacker çevrelerince Phobia olarak biliniyordu–, her gün hayatlarımızı bağladığımız internet hizmetlerinin ne kadar yaygın güvenlik eksiklikleri olduğunu ortaya çıkarmak istediğini iddia etti. Sağ olsun, anladık. Honan daha sonra saldırganıyla iletişime geçmek için yeni bir Twitter hesabı açtı. @Mat hesabını kullanan Phobia, Honan'ın yeni hesabını takip etmeyi kabul etti ve böylece ikili, Twitter'ın direkt mesaj özelliği üzerinden konuşmaya başladı. Honan, Phobia'ya tek bir soru sordu: "Neden? Neden bana bunu yaptın?" Anlaşılan, Honan'ın kaybettiği neredeyse on yıllık veri, sadece ek bir zarardı.

Phobia'nın cevabı kan donduruyordu: "Seninle herhangi bir sorunum yok aslında. Sadece Twitter kullanıcı adını sevdim." Bu kadardı işte. Her şeyin sebebi buydu. Mesele, çok değerli, üç harfli bir Twitter adıydı. Binlerce kilometre uzakta bir hacker bu adı sevmiş ve kendisine ait olmasını istemişti.

Size karşı herhangi bir "sorunu" olmayan birinin, birkaç tuşa basarak dijital hayatınızı yok edebildiği düşüncesi hiç mantıklı değil. Honan'ın hikâyesi, *Wired*'ın Aralık 2012 sayısının kapağında göründüğünde, hatırı sayılır miktarda ilgi çekti… belki bir, belki iki dakikalığına ama. Her gün kullandığımız teknolojileri nasıl daha güvende tutacağımıza dair bir tartışma başladı, ancak birçok internet tartışması gibi bu da yok olup gitti. Honan'ın çektiği onca çile ve sıkıntının ardından neredeyse hiçbir şey değişmedi. Daha hâlâ, biz de Honan'ın o gün yaşadığı kadar savunmasız bir hayat sürüyoruz. Hatta kolaylıkla hacklenebilir mobil ve bulut tabanlı uygulamalara bağlılığımız arttıkça, savunma sistemlerimiz de zayıflıyor.

Birçoğumuzda olduğu gibi, Honan'ın çeşitli hesapları da dijital bir güvenin imzasıymış gibi görünecek şekilde birbirine bağlıydı. Aynı kredi kartı numarası hem Apple profilinde hem de Amazon hesabında yer alıyordu. iCloud e-posta adresi, Gmail'in kapılarını açıyordu. Hepsinde de ortak olan bilgiler vardı. Giriş bilgileri, kredi kartı numaraları ve parolalar ile birlikte bütün veriler, tek bir kişiye aitti. Honan'ın güvenlik önlemleri, dijital bir domino dizisi gibi en ufak bir kuvvet ile teker teker ve hızlıca yıkılmıştı. Honan'ın dijital hayatını, sizin dijital hayatınızı yok etmek için gereken bilgiler,[3] biraz kötü niyetli, biraz da yetenekli birinin parmakları ucunda duruyor.

Bağlantılı Bir Dünyada İlerleme ve Riskler

Birkaç yıllık bir süre içinde Google sadece arama yaptığımız bir yer olmaktan çıkıp yol tariflerinde, takvimde, rehberde, videoda, eğlencede, sesli mesajlarda ve telefon görüşmelerinde, neredeyse üzerine hiç düşünmeden bel bağladığımız bir platform haline geldi. Bir milyar kadarımız, en özel bilgilerini Facebook'a verdi ve arkadaşlarımız, ailemiz ve birlikte çalıştığımız insanların sosyal ağ grafiğini bile isteyerek çizdik. Milyarlarca uygulama indirdik ve internet bankacılığından yemek tariflerine, sağlıklı yaşam uygulamalarından bebek fotoğraflarını saklamaya kadar bir sürü şeyi yapmak için onlara güvenir olduk. Dizüstü bilgisayarlarımızla,

mobil telefonlarımızla, iPad'lerimizle, TiVo'larımızla, PS3'lerimizle, Blu-ray oynatıcılarımızla, Nintendo'larımızla, HD televizyonlarımızla, Rokus'larımızla, Xbox'larımızla ve Apple TV'lerimizle internete bağlandık.

Bu teknolojik evrimin olumlu etkileri gün gibi ortada. Geçtiğimiz yüz yıllık süreçte tıp biliminde gözlenen hızlı gelişim ile birlikte, ortalama insan ömrü iki katına çıkarken, çocuk ölümleri de onda bir oranında azaldı.[4] Enflasyona bağlı kişi başına düşen milli gelir, tüm dünyada üç katına çıktı. Çok uzun yıllar boyunca sadece en seçkinlerin hizmetinde olan yüksek kalite eğitim, artık Khan Academy gibi internet siteleri üzerinden ücretsiz bir şekilde edinilebiliyor. Mobil telefonlar da tek başına tüm dünyadaki ülkelerin ekonomik gelişimine milyarlarca dolar katkı sağlıyor.[5]

En temelindeki mimari üzerinden internetin sağladığı bağlılık, dünyanın dört bir yanındaki bambaşka insanların daha önce olmadığı kadar yakınlaşmasını sağlıyor. Bugün Chicago'daki bir kadın, Hollanda'da hiç tanımadığı biriyle *Words with Friends* oynayabiliyor. Hindistan'daki bir doktor, Florida'daki bir hastanın röntgen sonuçlarını okuyup yorumlayabiliyor. Güney Afrika'daki bir çiftçi, cep telefonuyla internete girip MIT'deki bir doktora öğrencisi ile aynı mahsul verilerine ulaşabiliyor. Bu bağlılık, internetin en büyük güçlerinden biri konumunda ve internet büyüdükçe, küresel ağın gücü ile yararlılığı artıyor. Bu anlamıyla, modern teknolojik dünyamızda aslında sevineceğimiz çok şey var.

Online dünyanın avantajları iyi bir şekilde belgelenmiş ve teknoloji endüstrisinde çalışanlar tarafından sürekli vurgulanıyor olsa da, tüm bu bağlılığın bir de olumsuz tarafı bulunuyor.

Elektrik şebekelerimiz, hava trafiği kontrol ağlarımız, itfaiye sevk sistemlerimiz ve hatta asansörlerimiz, bilgisayarlara kritik ölçüde bağlı durumda. Her gün, ne anlama geldiğini sorgulamak için bir saniye bile duraksamadan, hayatlarımızı küresel bilgi şebekesine aktarıyoruz. Mat Honan ve onun gibi binlercesi bu gerçeği zor yoldan öğrendi. Peki modern toplumumuzun teknolojik tuzakları –artık tamamen bağımlı olduğumuz o temel araçlar– yok olduğun-

da ne yapacağız? İnsanlığın B planı ne ya da öyle bir plan var mı? Tahmin edebileceğiniz gibi, bir planımız yok.

Dünya Dümdüz (ve Apaçık)

Yüzyıllardır, Vestfalya sisteminin bağımsız ulusdevletleri, dünyamızda başarıyla hüküm sürüyor.[6] Yani ülkeler, dışarıdaki makamların içişlerine hiçbir müdahalesi olmadan kendi sınırları içerisinde özgürce varlıklarını sürdürüyor. Vestfalya düzeni; sınırlar, ordular, muhafızlar, kapılar ve silahlardan oluşan bir sistem ile korunuyor. Ülkeye gelen ve ülkeden çıkan göçü sınırlamak için kontrol mekanizmaları kuruluyor. Hatta, ulusal sınırlar arasındaki mal akışını kontrol etmek için gümrük ve denetleme yapıları oluşturuluyor. Yine de 1648 senesinde Vestfalya Anlaşması'nın altına imza atarak günümüz modern dünyasının temellerini atan o öngörülü insanların Snapchat'i düşünebildiğini sanmıyorum.

Ülkelerin, fiziksel sınırları halen önemini koruyor olmasına rağmen, bu birimler online dünyada o kadar da anlaşılır değil. Hiçbir sınır muhafızı, göçmen kontrolü veya gümrük beyannamesi olmadan, bitler ve baytlar bir ülkeden diğerine rahatlıkla akıp gidiyor. Eski nesil hırsızların, kaçakçıların ve mahkûmların yüzleştiği geleneksel uluslararası engeller, günümüz online dünyasında yer almıyor. Kötü niyetli kişiler de, istedikleri bir sanal konuma dilediklerini gibi girip çıkabiliyor.

Şimdi bunu ve güvenliğimiz üzerindeki etkilerini biraz düşünün. Bir zamanlar, suçlular New York Times Meydanı'ndaki bir bankayı soymak isterse, en azından birkaç şeyin aşikâr olduğunu söyleyebilirdik. Her şeyden önce, faillerin NYPD'nin Midtown South Polis Merkezi'nin sınırları içerisindeki fiziksel bir konuma girdiği varsayılırdı. Banka soygunları, hem New York State hem de ABD federal yasasını ihlal ettiği için, NYPD ile FBI soygunu ortak yetki sınırları içerisinde soruşturmaya başlardı. Aynı zamanda kurbanın (bu durumda banka oluyor), konuyla ilgili emniyet yetkililerinin fiziksel yetki sınırları içerisinde olması da soruşturmayı önemli ölçüde kolaylaştırırdı. Davayı çözmek için yapılan girişim-

ler, banka soyguncusunun veznedara uzattığı nottaki parmak izleri, üzerinden atladığı bankoda bıraktığı DNA veya hatta bankanın güvenlik kamerası sisteminde görünen yüzü gibi olay mahallinde bırakılan fiziksel kanıtlar sayesinde önemli bir yol kat ederdi. Ek olarak, bizzat banka soygunculuğunun getirdiği fiziksel engeller olurdu. Çalınan banknotların belli bir ağırlığı ve hacmi olduğu için, ancak bir miktarı taşınabilirdi. Bir ihtimal, para tomarlarının üzerinde, polisin şüpheliyi bulmasını kolaylaştıracak patlayan gizli boya paketleri olabilirdi. Ancak günümüz dünyasında, benzer suçlar ve fiziksel kanıtlara dair uzunca yıllar varlığını sürdürmüş, test edilip onaylamış soruşturma yöntemlerinin hiçbiri artık bulunmuyor.

Şimdi bu Times Meydanı soygun senaryosunu, Vladimir Levin'in 1994 yılında Rusya, St. Petersburg'daki evinden internet üzerinden gerçekleştirdiği banka soygunuyla kıyaslayalım. Bir bilgisayar programcısı olan Levin,[7] Citibank'ın birkaç büyük kurumsal müşteri hesaplarını hackleyip, 10,7 milyon dolar çalmakla suçlanıyordu. Dünyanın farklı bölgelerinden ortakları da olduğu söylenen hacker, yüksek meblağlarda parayı Finlandiya, ABD, Hollanda, Almanya ve İsrail'deki hesaplara havale etmişti.

Peki böyle bir davada yetki kimin? Kurbanın (Citibank) bulunduğu Amerika'daki polisin mi? Yoksa suçu işlediği iddia edilen şüphelinin yaşadığı St. Petersburg polisinin mi? O da değilse, yasadışı yollarla kazanılmış paraların elektronik olarak dolandırıcıların hesaplarına yatırıldığı İsrail, Finlandiya gibi bölgelerdeki yetkililerin mi? Levin, suçun işlendiği Amerika'ya fiziksel olarak hayatı boyunca adım atmamıştı. Ne bir parmak izi, ne de DNA'sını bırakmış, patlayan boyalarla korunan paralara elini sürmemişti. Daha da önemlisi, binlerce kiloluk nakit parayı fiziksel olarak taşıması gerekmemişti. Her şey bir fare ve klavye yardımıyla yapılmıştı. Ne bir maskeye ne de namlusu kesilmiş bir pompalıya ihtiyacı vardı Levin'in. Tek yaptığı, evindeki bilgisayar ekranının karşısına geçip dijital izlerini saklamak için dolambaçlı sanal bir yol çizmekti.

İnternetin doğası gereği, artık her geçen gün dünyamızın sınırları ortadan kalkıyor. Bugün, iyi veya kötü niyetli herhangi biri,

gezegenin diğer ucuna ışık hızında seyahat edebiliyor. Suçlular açısından ise bu teknoloji, polislerin işini bozmak amacıyla sanal olarak bir ülkeden diğerine atlarken büyük kolaylık sağlıyor. Artık internette izlerini nasıl kaybedeceklerini iyi öğrendiler. Akıllı bir hacker, Brezilya'daki bir bankaya düzenleyeceği saldırıyı katiyen Fransa'daki evinden yönlendirmez. Onun yerine, saldırısını açık bir ağdan diğerine yönlendirir: Fransa'dan başlar, Türkiye'den geçer, Suudi Arabistan'dan çıkar ve nihayetinde ilk hedefi olan Brezilya'ya ulaşır. Bu ülke atlama yeteneği (yani internetin en güçlü özelliklerinden biri) çoğu zaman polis kuvvetleri için bölgesel ve idari sorunlara yol açmakla birlikte, siber suç soruşturmalarının bu denli zorlu olmasının arkasındaki en büyük sebeptir. Üstelik, Paris'teki bir polis memurunun São Paulo'da birini tutuklama yetkisi yoktur.

Siber Suçlar Eskiden Ne Güzeldi

Geçtiğimiz yirmi beş yıllık süreçte, siber tehditlerin doğası akıl almaz bir biçimde değişti. Kişisel bilgisayarların ilk günlerinde, hackerlar daha çok bir ":D" veya gülücük almak için bu işi yapıyordu. Sadece *yapabileceklerini* göstermek veya bir şey anlatmak için bilgisayar sistemlerini hackliyorlardı. IBM PC'lere bulaşan dünyanın ilk bilgisayar virüslerinden biri olan Brain, 1986'da Lahore, Pakistan'dan yirmi dört ve on yedi yaşlarında iki kardeş, Amjad Farooq Alvi ve Basit Farooq Alvi tarafından geliştirilmişti.[8] Uzun yılların uğraşı sonunda geliştirdikleri yazılımın, korsan kopyalarının yapılmasını engellemek amacıyla bu zararsız virüsü yazmışlardı. Brain, yazılımın kopyalanmasını engelleyecek ve yasadışı kopyalarını takip etme imkânı sağlayacak şekilde bir disketin önyükleme sektörüne bulaşarak çalışıyordu. Başkalarının parasını ödemeden yazılımlarını çalmasına kızan kardeşler, virüsün bulaştığı bilgisayarların ekranına bir de kaygı verici mesaj gönderiyordu:

Zindan'a hoş geldiniz. ©1986 Brain & Amjad Kardeşler (pvt).
BRAIN BİLGİSAYAR HİZMETLERİ 730 NİZAM BLOK
ALLAMA IQBAL TOWN LAHORE-PAKİSTAN

TELEFON: 430791, 443248, 280530.
Bu VİRÜSE dikkat edin…
Aşılama için bize ulaşın…

Mesajlarında göze çarpan farklı detaylar var. İlk olarak, kardeşler virüsün telifini aldıklarını iddia etmiş, ki oldukça cesur bir hamle olduğunu söylemem gerekiyor. Daha garip olanı ise "aşılama" veya virüsün silinmesi konusunda kullanıcıların geliştiriciler ile görüşmesi için adres ve telefon bilgilerini paylaşmışlar. Bu virüsü geliştirmelerinin arkasında yatan düşünce Basit ile Amjad'ın gözünde gayet mantıklı olsa da, kardeşler ortaya çıkardıkları bu virüsün çoğalıp yayılma özelliği olduğunu fark etmemişti. Nitekim virüs de, eski moda bir şekilde, insanların yanlarında taşıdığı disketleri bir bilgisayardan diğerine sokup çıkarmasıyla yayıldı. Nihayetinde Brain tüm dünyayı gezmiş, Basit ve Amjad'ı herkese tanıtmıştı.[9]

Ancak zaman ilerledikçe, hackerlar da daha hırslı ve kötü niyetli olmaya başladı. Birbirimizle bilgisayarların ilan tahtaları ile bağlı oluşumuz, dijital virüslerin artık "sneakernet", yani disket taşıyan insanlar üzerinden değil, CompuServe, Prodigy, EarthLink ve AOL gibi ilk online hizmetler aracılığıyla telefon hatlarımız ve modemlerimiz üzerinden yayılmasına olanak sağlıyordu. Melissa (1999), ILOVEYOU (2000), Code Red (2001), Slammer (2003) ve Sasser (2004) gibi yeni Trojan ve virüsler, tüm dünyadaki Microsoft Windows bilgisayarlara kolaylıkla bulaşabilirken, sabit disklerimize kaydettiğimiz dönem ödevlerini, yemek tariflerini, aşk mektuplarını ve şirket belgelerini yok ediyordu. Bir anda biz de oyuna dahil olmuştuk.

Kötü amaçlı bilgisayar yazılımları, yani *malware*'ler, İngilizcede kötücül anlamına gelen "malicious" ile yazılım anlamına gelen "software" sözcüklerinin birleşimiyle ortaya çıkmıştır. *Malware*'ler, günümüzde bir veri sistemi veya ağda zarar verme, bozma, çalma ve yasadışı veya yetkisiz işlem yapma amacıyla çok çeşitli şekillerde karşımıza çıkabilmektedir.

- Bilgisayar virüsleri, bir kopyalarını bilgisayardaki başka bir programa sokarak yayılır. Yani, aynı gerçek dünyadaki virüslerin, müsait biyolojik konağa bulaşması gibidir.
- Bilgisayar solucanları da aynı şekilde zarara sebep olurken, bunu ayrı bir yazılım olarak yapar ve çoğalmak için bir konak programa ihtiyaç duymaz.
- İsmini Truva'ya giren Yunanlıların efsanevi tahta atından alan Trojanlar ise çoğu zaman meşru bir yazılım parçasının içinde gizlenir ve kullanıcı hedeflenmiş sisteminde programı kurduğu zaman aktif olur. Trojanlar, hackerların virüslü sisteme devamlı erişim sağlaması için sık sık "arka kapılar" oluşturur. Başka dosyalara bulaşarak çoğalmazlar. Onun yerine kullanıcıları bir dosya veya e-posta ekini açmaya ikna ederek yayılırlar.

Günümüzdeki virüs yazarları, artık sıradan halkın yavaş yavaş (ama çok yavaş) bir şekilde yabancıların gönderdiği dosyaları açmamayı öğrendiğini fark etmiş durumda. Sonuç olarak, suçlular da taktiklerini güncelleyerek, web tarayıcılarında sıklıkla kullanılan Java ve ActiveX gibi betik dillerinde oluşan zayıf noktaları ortaya çıkarmak için *malware* kullanan sözde hızlı download'lar geliştirdi. Dünya artık internete taşındı ve Internet Explorer, Firefox ve Safari gibi hack araçları, suçlular için kusursuz bir ortam yaratıyor. Masum kullanıcılar da bu yeni yöntemlerin bedelini ağır ödüyor. Palo Alto Networks'te çalışan araştırmacılar, modern *malware*'lerin yüzde 90'lık bir bölümünün, daha önce hacklenen popüler bir internet sitesi üzerinden yayıldığını keşfetmiş durumda.[10] Kullanıcıların hiçbir şey yapmasına gerek kalmayan bu yöntemle, site ziyaret edildiği an bilgisayarlar virüsle tanışmış oluyor. İçlerinde dünya genelinde büyük bir ziyaretçi portföyüne sahip Yahoo!'nun da bulunduğu çok sayıda büyük şirketin internet sitesi suçlular tarafından ele geçirilirken, bu şirketler bilmeden de olsa masumca maç sonuçlarını veya piyasa bilgilerini görmek için sitelerine uğrayan kendi müşterilerine de virüs bulaştırdı.[11]

Malware Patlaması

Artık hiçbir şey ":D" için yapılmıyor. Hackerlar para istiyor, bilgi arıyor ve gücün peşinde koşuyor. 21. yüzyılın ilk aylarında suçluların kötü amaçlı yazılımlarını kimlik hırsızlığı veya diğer teknikler ile paraya dönüştürmenin yollarını bulmasıyla birlikte, çok sayıda yeni virüs ortaya çıktı. 2015 itibariyle bu sayı akıl almaz boyutlara ulaşmış durumda. 2010'da, Alman araştırma merkezi AV-Test'in tahminlerine göre, dünyada başıboş dolanan 49 milyon *malware* parçası bulunuyordu.[12] 2011'de, antivirüs şirketi McAfee, her ay iki milyon yeni *malware* belirlediğini duyurdu. 2013'ün yazına geldiğimizde ise siber güvenlik firması Kaspersky Lab, her gün yaklaşık 200.000 yeni *malware* örneğini belirleyip yok ettiğini açıkladı.[13]

Bu istatistiklere alaycı bir tavırla yaklaşıp, antivirüs şirketlerinin mücadele ettikleri alanda ortaya çıkan sorunu abartarak yansıttığını, belirtilen sayıların yüzde 50, hatta yüzde 75'inin doldurma olduğunu bile söyleyebiliriz. Öyle olsa bile, hâlâ her gün en az elli bin yeni virüs ortaya çıkıyor demektir bu. Böylesine eşsiz kodlanmış *malware*'leri yazmak için küresel ölçüde gereken Ar-Ge çalışmalarının ne boyutta olacağını bir düşünün.

Nitekim her işletme sahibinin bildiği gibi, Ar-Ge oldukça pahalı bir öneridir. Öyle ki, uluslararası organize suçların mevcut kötü niyetli bilgisayar programlama çabalarını desteklemek için gereken yatırımın geri dönüşünün muazzam boyutlarda olması gerekir. Güvenilir Consumers Union tarafından yapılan ve *Consumer Reports* dergisinde yayımlanan bağımsız bir araştırma sonuçları da bilgisayar virüslerinin artan etkisini doğrular nitelikte.[14] Dergi aboneleriyle yapılan bir anket sonucunda, Amerika'daki hanelerin üçte birinin önceki yıl içerisinde kötücül bir yazılım sorunu ile karşılaştığı ve bu yazılımların yıllık 2,3 milyar dolar gibi bir zarara yol açtığı belirtiliyor. Üstelik bu sayı, sadece saldırıya uğradığının farkında olan insanları gösteriyor.

Güvenlik İllüzyonu

Dünyanın dört bir yanındaki tüketiciler ve şirketler, her yıl artan bilgisayar virüslerinin tehdidine karşı korunmak için bilgisayar güvenlik yazılımları endüstrisine sırtını yaslamış durumda. Gartner Group tarafından yapılan bir araştırmaya göre, 2012'de dünya genelinde güvenlik yazılımlarına harcanan para 20 milyar dolara yaklaşırken, 2017'de siber güvenlik için yıllık 94 milyar dolar harcanması bekleniyor.[15]

Şu an çıkıp birine bilgisayar virüsleri konusunda ne yapılması gerektiğini sorsanız, alacağınız ilk cevap Symantec, McAfee veya Trend Micro gibi bir firmanın antivirüs programını kurmak olur. Bu cevap, iyi eğitilmiş bir toplumun içgüdüsel olarak verdiği bir cevaptır. Bu tür araçlar, geçmişte faydalı olduklarını kanıtlamış olmasına rağmen artık etkinlikleri hızla azalıyor ve istatistikler de her şeyi gözler önüne seriyor. Aralık 2012'de Kaliforniya, Redwood Shores'tan bir veri güvenliği araştırma firması Impreva'daki araştırmacılar ile Technion-İsrail Teknoloji Enstitüsü'nden öğrenciler, standart antivirüs araçlarını test etmeye karar verdi. Seksen iki adet yeni bilgisayar virüsü topladılar ve içlerinde Microsoft, Symantec, McAfee ve Kaspersky Lab'ın da bulunduğu dünyanın en büyük kırk antivirüs şirketinin tehdit algılama motorlarında çalıştırdılar. Sonuç mu? İlk tehdit algılama oranı sadece yüzde 5'te kaldı.[16] Yani virüslerin yüzde 95'i hiç fark edilmeden bilgisayarlara girdi. Bu sonuç, aynı zamanda evinizdeki bilgisayarda çalışan antivirüs yazılımının, bilgisayara yöneltilen tehditlerin sadece yüzde 5'ini fark edebildiği anlamına geliyor. Vücudunuzun bağışıklık sistemi, virüslere karşı böyle bir ortalamaya sahip olsa, doğduktan birkaç saat sonra ölürdünüz.

Aylar sonra güvenlik yazılımları sektörünün devleri yazılımlarını güncellese de, çoğu zaman iş işten geçmiş oluyor. İşin aslında, suçlular ve virüs yazarları, bizi bu tehditlere karşı korumak için varlığını sürdüren antivirüs endüstrisinden durmaksızın daha yenilikçi hareket ederek her zaman iki üç adım önde oluyor. Daha kötüsü, "tespit etme süresi" –yani başıboş dolanan bir virüsün

keşfedilmesinden önce geçen süre- gittikçe artıyor. Mesela, 2012 senesinde Moskova'daki Kaspersky Lab'da çalışan araştırmacılar, Flame adında oldukça karmaşık bir *malware* keşfetti. Tüm dünyadaki bilgi sistemlerinden veri çalan bu virüs, beş yıldır internette geziniyordu. Bilgisayar güvenliği firması F-Secure'un baş araştırma görevlisi, sektörün saygın isimlerinden Mikko Hypponen, Flame'i antivirüs sektörünün fiyaskosu olarak nitelendirirken, kendisi ve çalışma arkadaşlarının da kendi başlattıkları yarışta birkaç tur geride kaldığını söylüyor. Dünya genelinde milyonlarca insan bu araçlara bel bağlamış olmasına rağmen, artık antivirüs devrinin kapandığı gün gibi ortada.[17]

Hayatımızdaki çok çeşitli teknolojik tehditlere karşı bir şey yapılamamasını gösteren sebeplerden biri de, sözde sıfır gün saldırılarının hızlı bir şekilde sayısını arttırmasından kaynaklanıyor. Sıfır gün saldırıları, bir bilgisayar programındaki, geliştiricilerin ve güvenlik ekibinin henüz çözmeye zaman bulamadığı ve daha önce bilinmeyen açıkları hedef alır. Nitekim antivirüs yazılım şirketleri aktif bir şekilde bu açıkları bulup kapatmak yerine, çoğu zaman belirli veri noktalarını göz önünde bulundurur. Yani daha önce gördükleri kötücül bir kod örneğini, bir daha görülmesi halinde engellerler. En basitinden bir benzetme yapacak olursam, bu durumun, daha önce banka soyduklarını bildiğimiz için her bankaya Bonnie ve Clyde'ın arandığına dair poster yapıştırmaktan bir farkı yoktur. Banka görevlileri bu ikili için gözlerini dört açıp bekliyor olsalar da, o tanıma uyan kimse ortaya çıkmadığı sürece savunmalarını esnetirler. Ancak o anda da başka bir soyguncu tüm parayı alıp kaçar. Bu sıfır gün saldırıları, her gün kullandığımız Microsoft Windows işletim sisteminden Linksys modemlere, Adobe'un tüm dünyadaki PDF Reader'ından Flash Player'ına kadar çok geniş bir yelpazedeki teknolojik ürünleri hedef alır.

Her şeyin ardından, hackerlar ise sistemlerinize girerken ne kadar gürültü çıkarırlarsa, sizin de sorunu o kadar hızla çözüp onları sistemden atacağınızı anladılar. Artık her şey gizli saklı yürütülüyor, sanki bilgisayarınızda bir uyuyan hücre varmış gibi oluyor. Imperva

araştırmasındaki yüzde 5'lik rezalet virüs tespit oranının, sadece evlerinde kişisel güvenlik yazılımları kullanan sıradan vatandaşlar için geçerli olduğunu düşünebilirsiniz. Elbette bilgi teknolojilerine ve güvenliğe ayrılmış devasa bütçelere sahip büyük şirketler, hackerlar karşısında çok daha başarılı bir savunma yapıyordur, değil mi? Alakası yok. Dünyanın en büyük şirketlerine, sivil toplum örgütlerine ve hükümetlere yönelik yapılan on binlerce saldırı sonunda gördük ki, ne kadar para harcarlarsa harcasınlar, kendi bilgilerini koruma konusunda hiçbiri sizden veya benden daha iyi durumda değil.

Verizon'ın *2013 Veri İhlali Araştırma Raporu*'na göre, bir hackerın bilgi sistemlerine girmesi halinde birçok şirketin bunu tespit edemeyecek durumda olduğu anlaşıldı. Verizon kurumsal hizmetlerin, ABD Gizli Servisi, Hollanda Ulusal Polisi ve Birleşik Krallık Polis Merkezi e-Suçlar Birimi ile birlikte yürüttüğü çalışmanın asıl can alıcı noktası ise, şirketlere yönelik gerçekleştirilen saldırıların yüzde 62'sinin en az iki ay sonra fark edildiği gerçeği oldu.[18] Trustwave Holding tarafından gerçekleştirilen benzer bir çalışma da, bir şirketin ağına izinsiz girişin fark edilmesi için korkunç bir 210 gün geçmesi gerektiğini gösterdi.[19] Yani bu sonuç, saldırganın –organize suç örgütü, rakip firma, yabancı bir hükümet ya da adını siz koyun– kurumsal ağ içerisinde dolaşıp sırları çalmak, rekabet avantajı sağlayacak verileri elde etmek, finans sistemlerine erişmek ve kredi kartı bilgileri gibi müşterilerin özel bilgilerini almak için yedi ay gibi uzun bir zamanı olduğu anlamına geliyor.

Üstelik, şirketler en sonunda ağları içerisinde dijital bir casus olduğunu fark ettiği zamanda ise, bunların yüzde 92'sinde ne şirketin bilgi işlem sorumlusu ne güvenlik ekibi ne de sistem yöneticisi durumun farkına varan isim oluyor.[20] Kötü haberi çoğu zaman emniyet görevlileri, kızgın bir müşteri veya bir üstlenici veriyor. Dünyanın en büyük şirketleri, bir araya geldiklerinde siber savunma için milyonlarca dolar harcayan ve ağlarını korumak için 7/24 çalışan profesyonellerden oluşan birimlere sahip olan bu firmalar, hackerlar tarafından böyle kolay bir şekilde mağdur edilebiliyorsa,

evlerinde kendi bilgilerini korumaya çalışan masum kullanıcılar açısından durumun içler acısı olduğunu söyleyebiliriz.

"Peki, sıradan bir bilgisayar sistemine girmek ne kadar zor?" diye soracak olursanız, size cevap olarak, gülünç derecede kolay, derim. Verizon'ın araştırmasına göre, hackerlar ağınızı hedef olarak gözlerine kestirdikten sonra, denemelerin yüzde 75'inde savunmanızı dakikalar içerisinde başarıyla aşıyorlar. Aynı çalışmada, denemelerin yalnızca yüzde 15'lik bir bölümünde sisteme giriş süresinin birkaç saati bulduğu belirtiliyor. Bu sonuçlardan yapılacak çıkarımlar ise çok ağır. Bir saldırgan, dünyanızı hedef aldığı andan itibaren, yüzde 75 oranla oyun dakikalar içerisinde sona eriyor.[21] Size daha neyin vurduğunu anlayamadan yumruğu yiyor, nakavt oluyor ve gözünüzü yerde açıyorsunuz. Günümüz dünyasında, hackerlar aylar boyunca hiç çekinmeden size ait özel veri sistemlerinizin içinde geziyor, bekliyor, izliyor ve parolalarınızdan iş projelerinize kadar her şeyi topluyor. Onların gözünde kolay lokmasınız. Düşününce, toplum olarak buna müsamaha göstermemiz bana çok garip geliyor. Oysa, evimizde dilediği gibi dolanan, uyurken bizi izleyen, duştayken videomuzu çeken bir hırsızla karşılaşsak, hemen telefona koşup yardım çağırırdık (veya çığlık atıp silahımıza da davranabiliriz). Siber dünyada ise her gün bu senaryo tekrar tekrar oynanıyor. Buna rağmen çoğumuz sükûnetini bozmadan, çok büyük açıklarımız olmasına rağmen tüm bu tehditlerden habersiz bir şekilde keyifle yaşamına devam ediyor. Ama haberiniz olsun, kötü adamlar uyurken sizi seyrediyor.

Küresel siber güvensizliğimizin maliyeti ise gün geçtikçe artıyor. Tüm dünyadaki işletmeler, 2017'ye kadar neredeyse 100 milyar doları güvenlik yazılım ve donanımlarına harcayacak olsa da, teknolojik kırılganlığımızın bütün ekonomik etkisi düşünüldüğünde bu sayı yalnızca bir başlangıç olarak kabul edilebilir. Örneğin 2007'de, Amerika'daki T. J. Maxx and Marshalls ve Avrupa'daki T. K. Maxx'ın ana şirketi TJX'e yapılan siber saldırıya bakalım.

TJX davasında, hackerlar 45 milyonun üzerinde müşterinin kredi kartı bilgilerini çalarak, o zamana dek yapılmış en büyük

perakende mağaza saldırısını gerçekleştirdi.[22] Daha sonraki dava dosyalarında, bilgileri çalınan kurban sayısının 94 milyon olduğu anlaşıldı.[23] TJX, Visa, MasterCard ve müşterileriyle 256 milyon dolarlık bir anlaşmaya girse de, birçok uzman asıl maliyetin 1 milyar dolar civarında olabileceğini belirtti.[24] Veri ihlallerinin maliyeti ile birlikte veri koruma ve bilgi güvenliği politikaları alanında bağımsız araştırmalar yapan, sektörün en güveniler kaynaklarından olan Ponemon Enstitüsü, siber güvenlik ihlallerini hesaplarken kayıp analizinde direkt müşteriden çalınan miktarın daha ötesini düşünmek gerektiğini vurguluyor.[25]

Yani, TJX gibi bu tür saldırılarda hedef alınan şirketler, saldırganları barındıran güvenlik açığını tespit etmek, konuyu detaylıca soruşturmak, saldırganları belirlemek ve bilgisayar ağlarını yeniden işlevsel hale getirmek için cömert harcamalar yapmak durumundadır. Bunun dışında, dikkatli müşteriler, güvensiz olduğu anlaşılan şirketin hizmetlerini kullanmaktan kaçınacağı için satışlarda ciddi düşüşler gözlenir. Bunlara bir de kredi kartı değişim ücretlerini (şu an kart başına 5,10 dolar olduğu tahmin ediliyor), kredi kartı çalınan tüketicilerin kartlarıyla alışveriş yapılıp yapılmadığını gözlemek için kredi izleme sistemlerine ödenecek miktarı ve artan siber sigorta primlerini kattığınız zaman, toplam kaybın ne kadar hızlı bir şekilde arttığını görebilirsiniz.[26] Çok sayıda şirketin, saldırıya uğradığını kabullenmekten neden bu kadar rahatsız olduğunu ve neden açıklamayı olabildiğince ertelemeye çalıştığını da buradan anlayabilirsiniz.

Elbette kayıplar burada sona ermedi. Bir siber saldırının ardından piyasaların kurban firmayı borsada nasıl cezalandıracağı ve hisse bedellerinin ne kadar düşeceğini de hesaba katmak gerekiyor. Bir seferinde, benzer bir saldırıya uğrayan Global Payments, New York Borsası hisselerinin alım satımını durdurana kadar tek bir gün içerisinde yüzde 9'luk bir gerileme gördü.[27] Bu davalardaki finansal baş ağrılarına bir de firmanın müşterileri, hissedarları ve düzenleyicileri tarafından açılan grup davalarını ekleyin. Tüm bunları hesaba katan Ponemon Enstitüsü, şirketlerin çalınan her

bir hesap başına 188 dolarlık bir maliyetle yüzleştiğini tahmin ediyor.[28] Bu sayıyı, TJX'in çaldırdığı 100 milyon müşteri hesabıyla çarptığınızda, hack saldırılarının ne kadar hızlı bir şekilde maliyeti katladığını kolaylıkla görebilirsiniz.

Çoğunlukla etkisiz önleyici tedbirlere harcadığımız miktarlar ve atlar kaçıp, hackerlar girdikten sonra kapadığımız siber ahır kapılarını düşününce, toplum olarak teknolojik emniyetsizliğimize cömert harcamalar yapıyoruz. Daha da kötüsü, ağlarla örülmüş dünyaya artan bağlılığımız ve dışarıdan erişime tamamen açık teknolojiler olmadan hayatımızı sürdüremeyecek hale gelmemiz, bize bütün dünya olarak cüzdanlarımızda açılan delikten çok daha büyük zararlar verebilir.

İnternet artık masumiyetini kaybetti. Birbirine bağlantılı dünyamız gün geçtikçe daha tehlikeli bir yer oluyor. Bizler de her geçen gün daha fazla sayıda saldırılara açık teknolojiyi hayatımıza aldıkça iyice savunmasız bir hale bürünüyoruz. Sıradaki Sanayi Devrimi'nin, yani bilgi devriminin temelleri atıldı ve hem kişisel hem de küresel güvenliğimiz için henüz fark etmediğimiz, çok büyük etkileri olacak. Bireylere, şirketlere ve hatta önemli altyapı sistemlerine yönelik tehditler bugün ne kadar göz korkutucu görünüyor olursa olsun, meşhur teknoloji treni istasyondan ayrılıyor ve inanılmaz bir ivme ile hızına hız katıyor. Doğru raylara bakarsanız, treni yakalayabilirsiniz.

Trenin gittiği yere, ufka doğru baktığımızda ise yepyeni teknolojilerle karşılaşıyoruz. Robot teknolojileri, yapay zekâ, genetik, sentetik biyoloji, nano teknoloji, üç boyutlu üretim, beyin bilimi ve sanal gerçeklik gibi dünyamızı kökünden değiştirecek bu algılar, bugünün siber suçlarını çocuk oyuncağıymış gibi gösterecek tam teçhizatlı güvenlik tehditlerini de beraberinde getiriyor. Daha birkaç yıl önce bilimkurgu filmlerinde duyabildiğimiz bu yenilikler, çok yakın bir gelecekte hayatımızın önemli birer parçası haline gelecek. Ancak detaya bile inmeden, geniş ölçekte yapılan çalışmalar, bu yeniliklerin yanında getireceği kasıtsız riskleri anlamamızı sağlıyor.

Bu büyük dönüşüm ve beraberindeki tehlikeler, daha şimdiden birçoğumuzun gözünden kaçmış durumda. Biz farkına bile varmadan, küresel toplumumuz internete bir trilyon yeni cihazı bağlamış olacak ve o cihazlar da hayatımızın her alanına nüfuz edecek. Bu kalıcı bağlantılar, tüm gezegende insan ile makineyi iyi günde, kötü günde buluşturacak; katlanarak artan ortak duyarlılığımızın krallığına sıkıca yapışacak. Sonuç olarak, teknoloji artık sadece makinelerle ilgili bir şey olmaktan çıkacak; gerçek hayatın öyküsü haline gelecek. Arka planda kalan teknolojilerin nasıl çalıştığını bilenler, bunları kendi faydalarına kullanacakları için her geçen gün daha da iyi pozisyonlara gelecek ve gördüğümüz gibi, olan da sıradan vatandaşa olacak. Ne olduğuna bakmadan, adamakıllı düşünmeden hayatımıza kattığımız teknolojiler, geriye dönüp bizi sırtımızdan bıçaklayacak. Tüm bu riskler, yeni normalin ne olacağını gösteriyor: Hiç de hazırlıklı olmadığımız bir gelecek bizi bekliyor. Bu kitap ise, insan ile makinenin; kölenin nasıl sahibe dönüştüğünün öyküsünü anlatıyor.