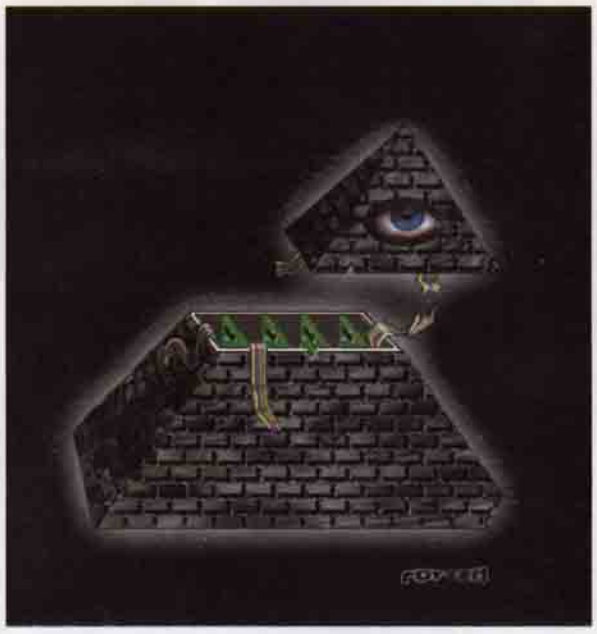
İnternet Korsanları

İnternet'in gelişmesiyle beraber bilgisayar korsanlarının saldırılarının sayısı da artıyor. Buna karşın devletler de boş durmuyor. Sırf bu saldırılara karşı, özellikle ABD'de güvenlik birimleri kuruluyor. Alınan tüm önlemlere karşın, hâlâ bu bilgisayar saldırılarından dolayı her sene milyonlarca dolarlık zararlar meydana geliyor.



2 Mart gecesi ABD'deki askeri, kamu ve üniversitelere ait binlerce bilgisayarın "kırılması" dikkatli bir şekilde hazırlanmış örgütlü bir eylemin üzerinde şüpheleri yoğunlaştırdı. Ancak güvenlik uzmanları 6 hafta öncesinden böyle bir olayın olabileceği konusunda uyarıda bulunmuşlardı.

ABD Enerji Bakanlığı'na bağlı CIAC (Computer Incident Advisory Capability Unit) dairesinden güvenlik uzmanı William Orvis'e göre bu rahatsız edici bir durumdan da öte. Bu olaydan nasibini alan 5000 il, 10000 Microsoft NT ve Windows 95 bilgisayarından sadece bir kaçı zarar gördü. Çoğu servis, "Denial of Service" veya "Teardrop" saldırıları karşısında, sonraları Microsoft sistemlerini de çökerten "ölümün mavi görüntüsü"ne (blue screen of death) maruz kaldılar.

Saldırıya makinaları sabit sürücüye kayıt yaparken uğrayanların, kaydedilen dosyaların bozulabileceğini belirten Orvis, gene de bozuk olan bu dosyaların da kurtarılabileceğini belirtiyor.

Orvis'e göre bütün gün İnternet'e bağlı olan, kamu, askeri ve üniversitelere ait bilgisayarların bu tür saldırılara maruz kalmaları çok muhtemel. Orvis aynı zamanda özel şirketlerden veya kişisel bilgisayar kullanıcılarından çok fazla bir şikayet duymadıklarını da belirtiyor.

Bu saldırılar çok kötü niyetli olmamasının yanında önlenebilirdi de. Çünkü CIAC Windows'un kırılabilirliğini 6 hafta öncesinden duyurmuştu bile.

Ancak saldırılar incelendiğinde, hedef kamu daireleri değil yalnızca belli bir şirket gibi görünüyor: Microsoft!.. "Şu an mevcut kamu çalışanlarına yönelik saldırılar olup olmadığını bilemem. Ancak saldırıların Windows NT ve Windows 95 çalıştıran makinaları hedef alması Bill Gates ile ilgili bir durum olduğu üzerinde düşündürüyor" diyor Orvis.

Ancak CIAC'nin Windows NT ve Windows 95 sistemlerini çökertebilecek "Teardrop 2" saldırıları uyarısı üzerine Microsoft bu problemi önleyebileceğini belirttiği güncel bir yama (patch) çıkardı.

Teardrop Nedir?

Teardrop saldırıları makinanıza 2 paket gönderir. Makinanız da bunları belleğe yerleştirir. Ancak paket öyle bir şekilde yazılır ki ikinci paket, birinci paketin üzerine onu bozacak şekilde yerleştirilir. Paket çok büyük değil ancak sistemin onu büyük bir paketmiş gibi düşünmesini sağlayan bir işarete sahip. Bu da öbür paketi örter. Bu ikisinin kombinasyonu da sistemin cevap vermesini gerektirecek bir mesaj doğurur. Eğer sistem nasıl cevap vereceğini bilmez ise ölür. İşte bu da ölümün mavi görüntüsüdür ve sistemin bir hataya maruz kaldığını gösterir.

Bu Teardrop saldırıları o kadar çok ki büyük bir ihtimalle 10000'den fazla bilgisayar bu saldırıdan nasibini aldı. Ancak bütün gün İnternet'e bağlı üniversite, kamu ve askeri bilgisayarlar dışında çok fazla bilgisayar bu saldırılara pek maruz kalmadı. Kişisel bilgisayar kullanıcılarından fazla bir şikayet gelmemesinin bir nedeni de, bu bilgisayarların bütün gün boyunca İnternet'e bağlı kalmaması. Üstelik kişisel bilgisayar kullanıcısı böyle bir saldırıya maruz kaldığında bunu bilmeyebilir. Makina çöker, ancak kullanıcı bunu bir saldırı sonucu olarak yorumlamaz. Aradaki fark böyle bir saldırı sonucunda bir yerel ağdaki tüm bilgisayarların bir anda çökmesi. İşte bu şekilde kullanıcılar bir şeyler olduğuna kanaat getirir.

Peki gelecekte buna benzer saldırılar olacak mı? Bu konuda güvenlik uzmanları sistemdeki gedikleri kapatacak şekilde çalışmalar sürdürüyor ve bundan sonra da artık makinaları kırmak daha da zorlaşacak. Ancak hacker'lar da makinalarda boşluk bulma ve bunları kırma konusunda daha da gelişmiş hale geliyorlar. Orvis'e göre şu anda evinde bilgisayarlarla yetişen ve bilgisayarlardan anlayan yeni bir çocuk kuşağı var. Bu durumda herhangi bir çocuk, bu küçük saldırı programcıklarının nasıl çalıştığını tam bilmeden, bunları çalıştırıp bir takım yerlere saldırıda bulunabilir. Bu, 10 yıl öncesinin hacker'larından çok farklı bir durum. Çünkü onlar makinaların çalışma prensipleri konusunda gerçekten bilgi sahibiydiler.

Bu durumda ne yapılabilir? Şu anda bir takım insanlar bu tür saldırılara karşı makinalarının açıklarını kapatmak için çılgınca makinalarına çıkarılan yamaları yerleştiriyor. Bu yolla en azından bilinen, belli bir takım saldırılardan makinalarını kurtarmış oluyor.

Hacktivism Mantıklı Bir Mücadele mi?

Şu anda İnternet'te "hactivism"in (aktivist amaçla bir yerin hack edilmesi (kırılması)) mantıklı bir mücadele olup olmadığı üzerine tartışmalar sürüyor. Hatta köşe yazarları bile bu konu üzerinde kendi saflarını belirlediler. Özellikle geçenlerde İnternet'in en tanınmış WWW indeksleme Arşivi Yahoo'nun (www.yahoo.com) kırılması büyük tartışmalara neden oldu. Bu eylemdeki amaç ABD'de hapsedilen Kevin Mitnick'in serbest bırakılması isteğiydi.

Kimilerine göre hacktivism, yapıcı özelliğinden çok aktivizmin dayandığı prensiplere aykırı. Böyle bir eylem de hacker'lık değil tam aksine "cracker"lık olarak değerlendiriliyor. Bilindiği gibi bir sistemin "crack" edilmesi, o bilgisayar sisteminin kırılıp, o sistemde yasal olmayan hareketlerde bulunulmasıdır. Diğer taraftan "hack" etmenin amacı bilgisayarlar hakkında bilgi sahibi olmaktır.

ABD'nin ünlü hacker'larından Ira Winkler'a göre Yahoo gibi, Adalet Bakanlığı gibi yerlerin bilgisayarlarını kırılması bir suç teşkil ediyor. Ona göre insanların bir WWW arşivini kendi seslerini duyurmaları amacıyla kırmasının mantıklı bir açıklaması yok. "Bir WWW arşivini kırıp içeriğini değiştirip kendi düşüncelerinizi koyarsanız onların düşünce özgürlüğünü engellemiş olursunuz. Eğer kendi düşüncelerinizi ifade etmek istiyorsanız kendi WWW arşivinizi kurmalısınız. Eğer insanlar sizin sitenize uğramadıklarından yakınıyorsanız, o zaman insanlar sizin amacınızla ilgilenmiyor demektir."

Winkler'a göre Nelson Mandela, Ghandi, Martin Luther King ya da Tiananmen Alanında gösteri yapan

Bilgisayar güvenlik boşluklarının doğurduğu boşluklar (1997 - 1998)

- İzinsiz girişler	150 milyon $
- Özel bilgi hırsızlığı	38 milyon $
- Telekomünikasyon yolsuzluğu	17 milyon $
- Finansal yolsuzluk	11 milyon $

Çinli öğrencilerin hepsi aktivistti. Çünkü bunlar düşünceleri doğrultusunda kendilerini ortaya koyabilen insanlardı. Ancak hacktivism olayında kimse kendini ortaya koymuyor ve meydana gelebilecek durumlara karşı yüz yüze gelmek yerine siberuzayda kendilerini gizlemeye çalışıyorlar.

Winkler bunu aktivizm olarak değil sadece bir takım insanların sistemleri kırma eylemlerine bir kılıf arama olarak görüyor. "Eğer insanlar yaptıkları eylemlerde toplum karşısında sorumluluk duymak yerine kendilerini gizliyorlarsa, o zaman eylemleri gerçekleştiren insanların amaçlarına inanıp inanmadıkları konusunda kuşku duyarsınız".

"Diğer yandan sadece bir kişi bilgisayarı kırarak böyle bir eylemde bulunuyor. Gerçek bir aktivizm olabilmesi için bunun belli sayıdaki bir topluluk tarafından desteklenmesi gerek. Protesto yürüyüşleri, oturma eylemleri de bunu yerine getiriyor".

"Tek bir kişilik WWW arşivi kırma eylemi geniş kitle desteği görmüyor. Aktivizmi vandalizmden ayıran nokta da burada: bu eylemi kaç kişinin desteklediği"...

Yahoo örneğine bakıldığı taktirde Kevin Mitnick'in serbest bırakılması istenmekte. Belki de bu WWW arşivini kıran kişinin hiç umurunda değil Kevin Mitnick'in davası. Winkler, Mısır'da meydana gelen turistlerin katledilmesi olayına da değinmek istiyor. Her ne kadar adam öldürmeyle bilgisayar kırmayı eş tutmasa da aradaki benzerliğe dikkati çekiyor. "Her ne kadar amaçlarını bilmesem de, yaptıklarına, uyguladığı yöntemlerden dolayı kesinlikle karşıyım".

Aynı şekilde bilgisayar kırmada da, eğer biri aktivist bir eylemde bulunmak istiyorsa bunu herkes tarafından kabul edilebilir bir şekilde ifade etmesi gerektiğini belirtiyor. Ve bilgisayar kırmanın toplum tarafından kabul edilebilir bir şekil olmadığını ve insanları böyle bir eylemin amaçlarına karşı getirdiğini ve üstelik yasalara da aykırı olduğunu belirtiyor.

Tüm zamanların en çok aranan bilgisayar suçlusu Kevin Mitnick.

Kevin Mitnick Kimdir?

Kuzey Carolina'daki Raleigh şehrinde tutuklanmasıyla Mitnick'in portresi, hayatta başarılı olabilmek için birçok fırsat yakalayan ama her seferinde bilgisayar dünyasının karanlık yüzünün çekiciliğine karşı koyamayan 31 yaşında bir bilgisayar programcısı olarak çıkıyor.

Kevin David Mitnick 1970'lerin sonunda Los Angeles banliyösünde büluğ çağına girmişti. Bu aynı zamanda kişisel bilgisayar endüstrisinin patlama yıllarıydı. Annesi babası boşanmışlardı. Renksiz bir alt-orta sınıf çevresinde Mitnick başarısız, yalnız bir gençti. Telefon şebekesi üzerinde kuracağı hakimiyetin çekiciliğine kapılmıştı. Aslında 10 yıldan fazla bir zamandır Kevin'de telefonları bedava kullanma yeraltı kültürü gelişmişti ve o sıralar analogdan sayısal dünyaya geçiş sürecinin ortalarıydı. Bir kişisel bilgisayar ve modem kullanarak uzaktan bir telefon şirketinin merkezindeki sayısal santrale bağlanıp ona hükmetmek mümkün hale gelmişti. Kevin de bu işin uzmanı oldu. Yerel telefon şirketinin santraline hükmetme, sadece bedava telefon konuşmalarına olanak vermiyor; başkalarının hayatlarına girmeyi, zengin ve güç sahibi olanların veya düşmanlarının konuşmalarını dinleme olanağı veriyordu.

Mitnick kısa bir süre sonra Hollywood'da, bir pizza restoranında buluşan ve bedava telefon konuşması yapan bir çeteyle tanıştı. Bu çetenin yaptığı daha çok, telefon santra-

Kevin Mitnick'in yakalanmasını sağlayan fizikçi ve bilgisayar güvenliği uzmanı Japon Tsutomu Shimomura

lindeki operatörlerin yerine geçerek, yardım için bu operatörleri arayanlara "Evet, aradığınız numara 8750 buçuk" demek ve ondan sonra "buçuğun nasıl çevireceğinizi biliyor musunuz?" gibi şakalar yapmaktı. Ya da bir şahsın ev telefonunu ödemeli telefon statüsüne çeviriyorlardı ve o telefon arandığında banda alınmış bir ses kutuya 20 sent daha atmalarını istiyordu.

Ancak bütün yaptıkları bu kadar masum olmuyordu. Çete üyelerinden biri, San Fransisco bilgisayar şirketinin bilgisayarlarına girerek bu şirketin dosyalarını yok etti ve polis 1 yıl boyunca bunu yapanı bulamadı. Sonunda, Los Angeles telefon şirketinin santraline kaçak girenleri araştıran polis, çete üyelerinden birinin kız arkadaşından ayrılmasıyla ve kız arkadaşının da polise gidip durumu anlatmasıyla Mitnick ve arkadaşlarını yakaladı.

1981 yılının ABD'nin savaşta kaybettiği askerlerini anma gününde Kevin ve iki arkadaşı Los Angeles'ın şehir merkezindeki Pacific Bell'in COSMOS (Computer System for Mainframe Operations) telefon santraline girdiler. COSMOS ABD'nin birçok şirketinin telefon sisteminin "temel kayıt saklama işlevi" için kullanılan bir veritabanıydı. COSMOS sisteminin odasından bilgisayar şifrelerini ve 9 Pacific Bell şirketinin merkez bürolarının kapı şifreleri dahil olmak üzere hepsini alıp götürdüler. Ancak Kevin ve arkadaşları gene bir çete üyesinin kız arkadaşı tarafından yapılan ihbar sonucu tutuklandılar.

O tarihte 17 yaşında olan Kevin, Los Angeles çocuk tutukevinde 3 ay geçirmeye mahkum edildi. Polisle başının belaya girmesi bilgisayar konusunda parlak gençleri yasal yollara sevketmesi gerekirken, Mitnick bilgisayar yeteneğini yaratıcı ve üretici bir şekilde geliştirmek yerine, bilgisayarları kırmanın kısa yollarını öğrenmeyi ve bir takım fantezilerini uygulamak için kirli yollara başvurmayı yeğledi. Bunlar da onu 80'lerde polisle birçok kez karşı karşıya getirdi. Gittikçe artan ününün ona getirdiği toplum ilgisi ve kişiliği etrafında yaratılan efsaneler çok hoşuna gidiyordu. Daha sonra 1975'lerde Robert Redford'un oynadığı "Condor'un Üç Günü" filmini izledikten sonra kendine savaş ismi olarak Condor'u seçti.

Hapishaneden çıktıktan sonra Nissan marka arabasının plakasına X Hacker yazdırdı. Bundan sonraki tutuklanması, 1983 yılında Güney California kampüsünde ARPANet'e girmek için yasal olmayan bir giriş bulmaya çalışırken oldu ve bundan 6 ay hüküm giydi . 1987'den itibaren hayatını bir düzene sokmaya çabaladı. Ancak içindeki şeytan boş durmadı; bu defa, yasal olmayan telefon kredi kartı kullanma yüzünden yakalandı ve 36 ay polis gözetiminde kalmaya mahkum edildi. Polisle devamlı başının belaya girmesi onda, gittikçe artan ve kendinin çok kudretli olduğuna dair bir güven geliştirdi.

1987 ve 1988 yılında Kevin ve arkadaşı di Cicco, DEC'in Palo Alto'daki araştırma laboratuvarındaki bilim adamlarıyla bir savaşa girdiler. Mitnick Digital'ın işletim sistemi VMS'nin bir kopyasını almak istiyordu. Bunu da EasyNet olarak bilinen şirketin bilgisayar ağına girerek yapmaya çalışıyordu. Mitnick ve di Cicco modem saldırılarını di Cicco'nun çalıştığı bir California şirketinden başlattılar. Bu modem saldırıları hemen keşfedildiyse de ne FBI ne de yerel polis bunların nereden geldiğini anlayamadı. Çünkü Mitnick modem çağrılarının kaynağını saklamak için telefon santralini kullanıyordu. Ancak sonunda gene polis onları buldu; bu onun beşinci kez bir bilgisayar suçundan yakalanmasıydı. Yargıç, Mitnick'in bilgisayar sistemlerini kırmasıyla bir uyuşturucu bağımlısının uyuşturucu bulmaya çalışması arasında benzerlik kurarak ona bir yıl hapis ve 6 ay da danışmanlık programına katılma kararı verdi.

Bu cezalarını çektikten sonra Mitnick Las Vegas'a gitti ve bir bilgisayar şirketine alt düzey programcı olarak girdi. Daha sonra 1992 yılında bir detektiflik şirketinde çalışmaya başladı. Eylül ayında FBI evini aradı ve 2 ay sonra bir federal yargıç, 89'daki polis gözetiminde kalma kurallarını çiğnediği için onun yakalanmasını istedi. Ancak Kevin ortadan kayboldu. Bu kaçışında Güney California gazeteleri kendisini parlak, ele avuca sığmayan ve polisin bir türlü başa çıkamadığı bir siber hırsız olarak niteleddiler.

İki yıllık bir izlemeden sonra bir FBI timi 31 yaşındaki Mitnick'i yakaladı. Mitnick'in arkasında bilgisayar sistemlerinden binlerce veri dosyası ve en az 20 000 kredi kartı numarasının çalınması gibi suçlar bulunuyordu. Bu da bütün zamanların en çok aranan bilgisayar suçlusunun yakalanması olarak nitelendi.

Peki bu tüm zamanların en çok aranan suçlusunun bulunmasında başrolü üstlenen kimdi: Tsutomu Shimomura.

1994 yılı Noel gecesi, çevre kirliliğinden AIDS'e kadar birçok araştırma yapan, bilgisayar bilimi ulusal laboratuvarı San Diego Supercomputer Merkezi, sıradışı yöntemler kullanılarak bir hacker tarafından saldırıya uğradı. Bu Kevin Mitnick'ti.

Mitnick sisteme girdikten sonra, ülkenin en başarılı bilgisayar sistemleri uzmanlarından olan Tsutomu Shimomura tarafından yakalandı. Shimomura daha sonra bu olay üzerine John Markoff ile "Takedown: The Pursuit and Capture of America's Most Wanted Computer Outlaw -- By The Man Who Did It (Amerika'nın En fazla Aranan Bilgisayar Korsanı)" adlı kitabını çıkardı.

Shimomura'nın danışmanı Sid Karin'in dediği gibi "Burada önemli olan nokta, kötü çocuklar her zaman iyi çocuklardan yetenekli olmak zorunda değiller".

Alkım Özaygen

Kaynaklar
www.news.com
www.wired.com
www.takedown.com
www.zdnet.com
www.hacker.org/subspace/cyber/mitnick.html