



Güvenlik tehditleri raporu: 2009

Bu yılın yeni tehditlerine karşı hazırlıklı olun

SOPHOS

Güvenlik tehditleri raporu: 2009

Genel Görünüm

2 Kasım 1988 tarihinde Cornell Üniversitesi'nden, 22 yaşında, Robert Morris adındaki bir öğrenci UNIX işletim sisteminin zayıf yönlerini istismar edebilen bir internet solucanını yaydı. Bu solucanın internetin yüzde onunu enfekte ettiği tahmin ediliyor. O günden yirmi yıl sonra, kötü amaçlı yazılım sorununun ölçeği, astronomik olarak artmıştır. Günümüzün internet saldırıları organize olup, tüketiciler ve şirketlerden bilgi ve kaynak çalmak üzere tasarlanmışlardır. Siyasi ve dinsel güdülerle yapılan saldırı örnekleri olsa da, asıl dürtü finansaldır.

Günümüzde web'in siber suçluların bilgisayarları enfekte etmek için kullandıkları ana yol oluşunun temel nedeni, giderek artan sayıda kuruluşun e-posta ağ geçitlerini güvenceye almış olmasıdır. Sonuç olarak, siber suçlular masum web sitelerine kötü amaçlı kodlar yerleştirmektedirler. Bu kodlar daha sonra sadece beklemeye geçerek, ziyaretçi bilgisayarları sessizce enfekte ederler.

Bu küresel suç etkinliğinin ölçeği öyle oranlara ulaşmıştır ki, Sophos yılda 365 gün, günde 24 saat düzeniyle, her 4.5 saniyede bir, enfekte olmuş yeni bir web sayfası keşfetmektedir. Ayrıca dünya çapındaki tehdit analiz merkezleri ağıımız SophosLabs'a her gün 20,000 civarında yeni kuşku kod gönderilmektedir.

En büyük kötü amaçlı yazılım tehditleri – Web sitelerine karşı SQL enjeksiyon saldırıları ve panik yazılımlarındaki artış

Yeni web enfeksiyonları – Sophos her 4.5 saniyede bir, enfekte olmuş yeni bir web sayfası keşfetmektedir

Kötü amaçlı e-posta ekleri – 2008'in sonunda, başına oranla beş kat artmıştır

Spam-ile ilişkili web sayfaları – Sophos her 15 saniyede bir, yeni bir web sayfası keşfetmektedir

Yeni panik yazılımı web siteleri – Her gün beş tanesi tanımlanmaktadır

En fazla kötü amaçlı yazılım barındıran ülke – Yüzde 37 ile A.B.D.

En fazla mesaj bombardımanı yayan kıta – Yüzde 36.6 ile Asya

Amount of business email that is spam – 97 percent

2008 kötü amaçlı yazılımların sadece bir Microsoft sorunu olmanın ötesinde bulunduğunu kanıtlamıştır. Salt Windows'a yönelik tehditlerin sayısının diğer platformlardaki saldırıları açık ara ile geçmesine karşın, siber suçlular dikkatlerini Apple Macintosh gibi diğer işletim sistemleri ile, kırılabilir çapraz platform yazılımlarına çevirmektedirler. iPhone, iPod Touch, Google Android telefon ve süper taşınabilir defter tipi Internet bilgisayarları gibi cihazların artan popülerliği ile, bu durumun 2009'da da sürmesi olasıdır.

Kuruluşların kendilerini yalnız e-posta ve web ağ geçitlerinde değil, her iş düzeyinde savunmaları konusu, taşıdığı büyük önemi hiç yitirmemiştir. Ağlar, masaüstü ve dizüstü bilgisayarlar ve taşınır cihazların gizli suçların kaynaklık ettiği çok sayıda tehdide karşı kapsamlı olarak güvenceye alınması zorunludur.

Web tehditleri

Yasal web sitelerinin istismarı

Son iki yıldan bu yana, web siber suçlular için ana bir saldırı yoluna dönüşerek, eskiden e-posta sistemlerine olan bağımlılıklarının yerini almıştır. Bilgisayar korsanları, zayıf korunan, yasal web sitelerini istismar etmek suretiyle, buralara, her ziyaretçiyi enfekte etmeye çalışan zararlı kodlar yerleştirebilmektedirler. Web'in bu denli popüler olmasının nedenlerinden biri, yasal web sitelerinin, her biri potansiyel birer kurban olan çok sayıda ziyaretçiyi çekmesidir.

2008'de birçok tanınmış kuruluş ve marka bu tip saldırıların kurbanı oldu. Gerek büyük, gerekse küçük kuruluşların hedeflenmesi, web güvenliğinin herkes için taşıdığı önemi vurguladı.

- **Ocak 2008:** Fortune 500 şirketlerine, resmi kurumlara ve okullara ait binlerce web sitesi kötü amaçlı kodlarla enfekte oldu.
- **Şubat 2008:** İngiliz yayın kuruluşu ITV Windows ve Mac kullanıcılarına panik yazılımları önermek üzere tasarlanan, zararlı bir web reklam kampanyasının kurbanıydı.
- **Mart 2008:** 2008 Avrupa Futbol Şampiyonası biletlerini satan bir site ele geçirilirken, anti-virüs firması Trend Micro web sayfalarının bir bölümünün risk altında olduğunu keşfetti.
- **Nisan 2008:** Cambridge University Press web sitesine sızılıp çevrim içi sözlük ziyaretçileri yetkisiz bilgisayar korsanı kodlarına maruz bırakıldı.
- **Haziran 2008:** Wimbledon tenis turnuvasının İngiltere'deki açılışında, Tenis Profesyonelleri Birliği'nin sitesi enfekte oldu.
- **Temmuz 2008:** Sony'nin A.B.D.'deki PlayStation web sitesi, ziyarette bulunan tüketicileri bir panik yazılımı saldırısı riski altında bırakan bir SQL enjeksiyon saldırısına maruz kaldı.
- **Eylül 2008:** *BusinessWeek* dergisi Rusya tabanlı bir sunucudan kötü amaçlı yazılım indirmeye çalışan bir SQL enjeksiyon saldırısı ile enfekte oldu.
- **Ekim 2008:** Adobe web sitesinin video web günlüğü tutanlara destek sunmak üzere tasarlanan bir bölümü bir SQL enjeksiyon saldırısı riskiyle karşı karşıya kaldı.

SQL enjeksiyon saldırıları

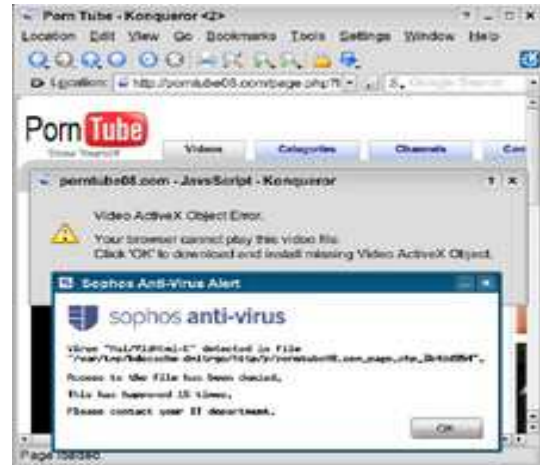
2008'de manşetlerin en büyük konularından biri SQL enjeksiyon saldırısıydı. Bu tip saldırılar güvenlik açıklarını suistimal eder ve kötü amaçlı kodları (örneğin kod taşıyan etiketleri) bir siteyi işletmek için kullanılan veritabanına yerleştirirler. Örneğin bir web formundaki kullanıcı girişi doğru olarak filtrelenmez ya da sınanmazsa, kod veritabanına zararlı komutları eklemektedir. Kurtarma işlemi güç olabilir ve web sitesi sahiplerinin veritabanlarını temizledikten yalnızca birkaç saat sonra yeniden hedef oldukları çeşitli örnekler vardır.

Otomatik sistemler

Bilgisayar korsanları Google gibi arama motorlarını potansiyel zayıflık gösteren web sitelerini saptayacak biçimde kullanan ve sonra sunuculara kod enjekte eden otomatik araçlar geliştirmişlerdir. Web siteleri nadiren özellikle hedef alınmıştır ve genellikle sadece siber suçluların zararlı yazılım dağıtma aracı tarafından keşfedilecek kadar şanssız olmuşlardır.

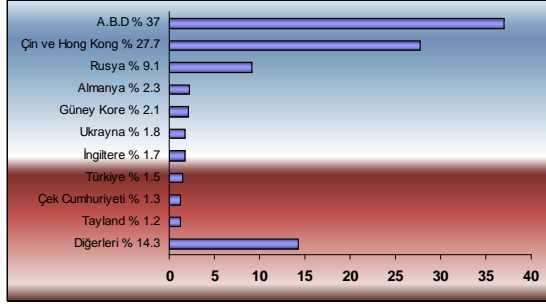
Siber suçlular, kullanıcıların sıkı bir tanımlanma sürecini geçirmelerinin gerekmediği, ücretsiz web barındırma servislerini sıklıkla kullanarak, kendi zararlı kod enfeksiyonu içeren sitelerini de kurmaktadır. Bu kişiler daha sonra yasal web günlükleri ve forumlarına, enfekte olmuş siteleri işaret eden zararlı bağlantılar yerleştirmek için, otomatik sistemlerden yararlanırlar.

Örneğin, Sophos 2008 içinde birçok yasal web günlüğü ve ileti panosunda, cinsel içerikli videolarla bağlantılı olduğunu iddia eden, ancak aslında herhangi bir şey göstermeden önce, bir tarayıcı yama güncellemesini isteyen not örnekleriyle karşılaştı. Kullanıcıya yüklenen güncelleme yapan düzmece kod ya da Flash Player taklidi yazılım, aslında onu korkutarak, düzmece güvenlik yazılımı satın almaya yönlendirmeye çalışan panik programlarıydı.



Web’de en çok zararlı yazılım barındıran ilk 10 ülke

2008 A.B.D., Çin ve Rusya’nın dünyada kötü amaçlı yazılım yayan web sitelerinin yaklaşık dörtte üçünden sorumlu olduğunu gösterdi. Ancak soruna diğer ülkelerin de katkısının bulunmadığına inanmak yanıltıcı olacaktır.



En çok zararlı yazılım barındıran ilk 10 ülke

Sophos’un araştırması, sınırları içindeki web sayfalarında kötü amaçlı yazılımlar barındıran 150’den fazla ülkenin katılımıyla, grafiğin son dilimini oluşturan bir “uzun kuyruk” etkisini ortaya çıkarmıştır. Etki altındaki bu web sayfalarından % 85’i suçlu kişilerin ele geçirdiği yasal web sitelerindedir.

Kötü amaçlı yazılım grafiğinden özet notlar

- A.B.D. enfekte olan her sekiz sayfadan neredeyse üçünü barındırarak, listenin doruğuna yerleşti. Bu durum A.B.D.’nin 2007’de sorumlu olduğu her dört sayfada birin altındaki (% 23.4) orana göre bir artışı işaret ediyor.
- 2007’de dünyadaki tüm kötü amaçlı yazılımların yarısından fazlasına (% 51.4) ev sahipliği etmenin sorumluluğunu taşıyan Çin, günümüzde sorundaki payını hemen yarıya indirdi.
- Çek Cumhuriyeti listeye yeni katıldı ve dünyanın web’de olan tüm kötü amaçlı yazılımlarının yüzde birinden fazlasını barındırıyor.
- 2007’de Polonya, Fransa, Kanada ve Hollanda sırasıyla 6., 8., 9. ve 10. konumlardaydılar ancak bugün, listeye giremeyecek kadar az sayıda kötü amaçlı web siteleri var.

Kullanıcı direnci

Web güvenliğinin kötü amaçlı yazılımlar ve diğer tehditlere karşı korunmak üzere tasarlanmış olmasına karşın, kimi kullanıcılar olumsuz tepki vermiş ve korumayı bozan adımlar atmıştır. Bu durum, şirket ve kuruluşların örneğin sosyal ağ ya da video web sitelerini engelleme gibi politika nedenleri ile, belirli web sitelerini gösteren URL’leri filtrelemeleri halinde özellikle geçerlidir.

Vekillerin (proxy) anonimleştirilmesi

Birtakım kullanıcılar web’in filtrenmesine, bir kuruluşun erişim izni denetimini aldatmak amacıyla bir web sitesinin gerçek yapısını kamufle eden vekil anonimleştirme yöntemini, kullanma yanıtını vermiştir.

Genel anonim vekillere ilişkin bilgiler binlerce web günlüğü, forum ve web sitesinde serbestçe paylaşılmaktadır ve kişisel ya da küçük grup kullanımı için kurulmuş bilinmeyen sayıda özel anonim vekil vardır. Bu durum kullanıcıların bir anonim vekile erişimini çok kolaylaştırırken, yöneticilerin izleme ve engelleme işini zor ve zaman alıcı hale getirmektedir. Kullanıcılar anonim vekiller üzerinden web sörfü yaptıklarında, URL filtresini atlatmanın yanı sıra, sınırlardaki içerik filtrelemesinin etrafından dolaşmak suretiyle, enfeksiyon riskini önemli ölçüde çoğaltmaktadırlar.

Sophos kendileri de kötü amaçlı yazılımlarla enfekte olmuş birçok anonim vekil dahi bulmuştur. Anonim vekillerin enfeksiyonun masum kurbanları mı yoksa içlerine gömülen kötü amaçlı yazılımlarla kurulmuş mu olduklarını söylemek olanaksızdır. Ancak enfeksiyonun kasti olup olmadığına bakılmaksızın, bu vekilleri kullanan herkes kendi bilgisayarını ve bağlı olduğu ağı enfekte etmenin gerçek olasılığını yaşar.

Anonim vekil kullanımı, teknoloji meraklısı öğrencilerin kabul edilebilir kullanım politikalarını ihlal etmeye çalıştığı eğitim kurumlarında özellikle yaygın olarak görülmektedir. Sophos yeni anonim vekil hizmetlerini bulmak için internet forumlarını aktif biçimde izlemekte ve web donanımındaki trafik denetimi ile, özel anonim vekillerin gerçek zamanlı keşfine katılmaktadır.

E-posta tehditleri

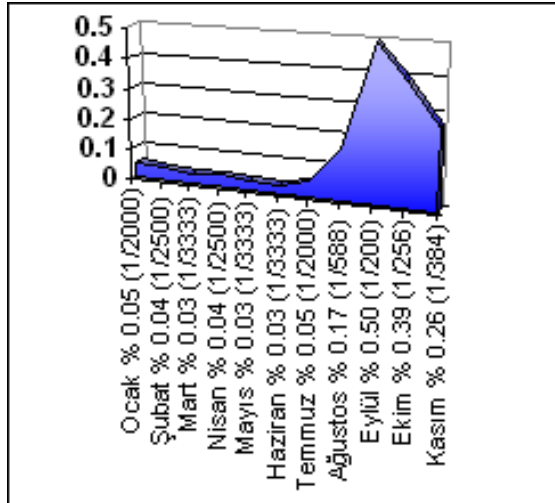
Eklere bulunan tehdit sayısı artıyor

Geçmiş yıllarda, e-posta eki üzerinden yayılan tehdit sayısı azalmaktaydı:

Yıl	Enfekte olmuş ek taşıyan e-postalar (ortalama)
2005	1 / 44
2006	1 / 337
2007	1 / 909
2008	1 / 714

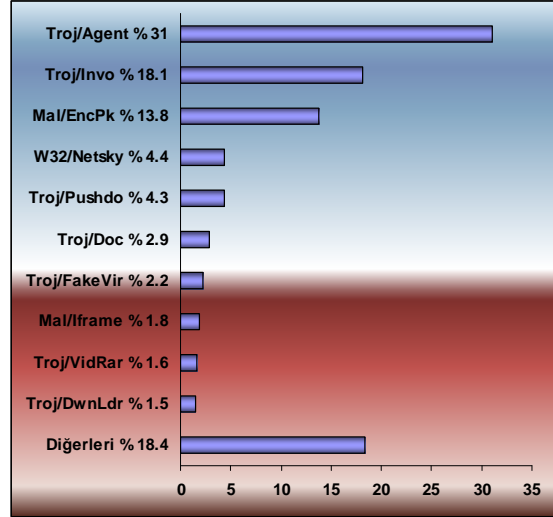
Ancak, son 12 ay içinde web tabanlı tehditler kötü amaçlı yazılım günlüğünde ağır basarken, 2008'in sonunda yıl başına göre beş kat daha fazla zararlı e-posta eki vardı.

Artış aylık olarak gösterildiğinde daha fazla göze batıcı olmaktadır: yılın ilk çeyreğinde 1/3333 gibi düşük bir değerden Eylül sonunda 1/200 gibi yüksek bir değere ulaşılmıştır.



2008'de, enfekte olmuş e-posta eklerinin aylık yüzdeleri

Sophos bu artışı çoğunlukla, Ağustos 2008'den itibaren mesaj bombardımanı gönderenlerin yaptığı büyük ölçekli birkaç zararlı yazılım saldırısına bağlamıştır. Bu dönemdeki yüksek profilli saldırıların arasında, FedEx ve UPS gibi firmalardan gelen başarısız bir gönderi uyarısı gibi görünen Invo-Zip Truva atı¹⁰, iPhone oyunu Penguin Panic Apple kılığında mesaj bombardımanı ile gönderilen Agent-HNY Truva atı¹¹ ve bir Microsoft güvenlik yaması olduğu iddiasındaki EncPk-CZ Truva atı¹² bulunmaktadır.



2008'de e-posta ekine bağlı, en yaygın ilk on kötü amaçlı yazılım

2008'in ikinci yarısındaki e-posta saldırılarının ölçeği Angelina Jolie ve Nicole Kidman'ın çıplak fotoğrafları gibi görünen ve yılın ilk yarısındaki tüm raporların % 31'inden sorumlu olan Pushdo Truva atı¹³ üzerinden izlenebilir.

Troj/Agent ve Troj/Invo'nun e-posta eki tabanlı zararlı yazılım listesine hızla baskın hale gelmeleri (hemen hemen % 50), 2004'ün başlarındaki çıkışından itibaren listenin üst sıralarını sürekli işgal eden Netsky solucanını geçmelerinden ötürü dikkate değer¹⁴. Netsky kendini içerdiği kodlarla kopyalayabilir ve internet üzerinden yayılabilirken, Agent ve Invo Truva atları kendi olanaklarıyla hareket edemeyip, genellikle ele geçirilmiş bir bilgisayardan gönderilen mesaj bombardımanlarına bağlıdır.

Kötü amaçlı bağlantılar

Sibersuçlular, kötü amaçlı e-posta eklerini kullanmanın yanı sıra, e-postalara kötü amaçlı bağlantılar gömmeye ve kullanıcıların merakından yararlanmak üzere tasarlanmış, yaratıcı ve iyi zamanlanmış mesaj bombardımanı saldırılarına devam ediyorlar.

Sophos örneğin Ağustos 2008'de MSNBC ve CNN'den gelen flaş haberler olma iddiasında, yaygın bir mesaj bombardımanı dalgasına karşı uyarı yayınladı¹⁵. Gelen her e-posta kullanıcıları haberin ayrıntılarını okumak üzere bir bağlantıya tıklamak için cezbediyor, ancak onları ayrıntılar yerine, Windows tabanlı bilgisayarı Mal/EncPk-DA Truva atı ile enfekte eden zararlı bir web sayfasına götürüyordu.

CNN.com. THE DAILY TOP 10

TOP 10 STORIES

#1. West Nile virus cases reported in California

2. Boy thrown outside window in school
3. Andre Agassi admits drug abuse
4. Murderer on the loose after cop bungle in Iowa
5. West Nile virus cases reported in California
6. Virgin Galactic shows off mothership space craft
7. JFK heir found
8. Internet exposes Obama affair
9. Massive earthquake in Japan kills thousands
10. GE declares 100 million deficit

Eylül 2008’de, A.B.D. başkan adayı Barack Obama’nın pornografik bir videosuna bir bağlantının bulunduğu iddia edilen bir e-posta geniş bir mesaj bombardımanı ile yayıldı¹⁶. Oysa web sayfası gerçekte Mal/Hupig-D zararlı yazılımını kurmaktaydı.



Obama’nın başkanlık yarışındaki zaferinin ertesi günü, mesaj bombardımanı ile yayılan diğer bir kötü amaçlı yazılım kampanyası, alıcılarını başarılı Demokrat adayın bir videosunu izlemek üzere, bir web bağlantısına tıklamaya davet etmekteydi¹⁷. Bu web sitesine yapılan ziyaret, aslında kurbanın bilgisayarından bilgi çalınmasına ve Ukrayna’nın Kiev kentindeki bir sunucuya gönderilmesine yol açabiliyordu.

Kötü amaçlı yazılımlar

Enfeksiyon korkusu

2008'de siber suçluların para kazanmak için uyguladıkları belirgin yöntemlerden biri, panik yazılımı (scareware) ya da dolandırma yazılımı (rogueware) olarak bilinen, sahte anti-virüs yazılımlarının kullanılmasıydı. Bu tip saldırılar BT güvenliği korkularından beslenmekte ve kullanıcıları, bilgisayarlarında hiçbir güvenlik sorunu yokken, bunun olduğuna inandırarak aldatmaktadır.

Panik yazılımları tipik olarak aniden beliren reklamlar ya da kamufle olmuş program yüklemeleri biçiminde web sitelerine yerleştirilirler. Öte yandan, bilgisayar korsanlarının panik yazılımlarını ya da bu yazılımlarının bağlantılarını, kullanıcıları eklere ya da bağlantılara tıklamak üzere kandırarak, geleneksel sosyal mühendislik hilelerinden yararlanarak, mesaj bombardımanları ile yaydığı durumlar da vardır. Sophos mesaj bombardımanı tuzaklarının yalnızca birinde, bu tip e-postalardan her gün yaklaşık 5000 tanesini bulmuştur.

Panik yazılım bağlantılı web siteleri genellikle, yazılımın virüs öldürmedeki etkinliği ile ilgili, sahte inceleme sonuçları ile birlikte, dürüst olma iddiasındaki güvenlik yazılımlarını taşımaktadırlar. Web siteleri kimi zaman da kullanıcıların kredi kartı ayrıntılarını ele geçirirler.

Bilgisayar korsanı çeteleri meşru güvenlik sağlayıcısı taklidi olan ve profesyonel görünümdeki düzmece web sitelerini hızla üretme konusunda uzmanlaşmışlardır. Sophos ortalama olarak, her gün beş yeni panik yazılımı web sitesini keşfederken, kimi durumlarda bu sayı günde 20 adedin üzerine çıkmaktadır. Norton AntiVirus¹⁸ ve AVG gibi kurumsal güvenlik markaları dahi hedeflenmiştir.

Meşru ürünlerin satışlarını arttırmak amacıyla panik yazılım kullanarak sahte reklamlar veren bağlantılarının üzerinden, birtakım meşru yazılım şirketleri dahi bu aldatmacalara karıştırılabilmektedir.

Panik yazılımı sorununu yaratan çeteleri yönlendiren dürtü, Kore'deki bir anti-virüs şirketinin eski genel müdürü Lee Shin-ja vakasında açıkça görülüyor. Lee'nin sahte güvenlik uyarıları görüntüleyerek, kullanıcıları şirketin Doctor Virus temizleme çözümünü satın almaya yönlendiren ücretsiz bir casus yazılım karşıtı ürün aracılığıyla, 2005'ten bu yana 9.8 milyon A.B.D. dolarından fazla kazanç sağladığı belirtildi¹⁹.

Panik yazılımı sorununun Windows tabanlı bilgisayarlarla sınırlı olmadığı bilgisi de kayda değer. Sophos Şubat 2008'de gerek Windows, gerekse Apple Mac kullanıcılarını hedefleyen panik yazılımı kampanyaları ile karşılaştı²⁰.

Hareket halindeki zararlı yazılımlar

USB bellek çubukları üzerinden aktarılan zararlı yazılımlar da artıyor. 2008'de ortaya çıkan belki de en tuhaf USB üzerindeki kötü amaçlı yazılım öyküsü, gevşek güvenlik kıstasları nedeniyle uluslararası uzay istasyonundaki bilgisayarları enfekte olan astronotlara aitti²¹.

Sosyal ağ işlemleri üzerinden kötü amaçlı yazılım saldırıları

2008'de kötü amaçlı yazılımları yaymak için sosyal ağ web sitelerinin kullanımı çok daha fazla ilgi gördü. Facebook Ağustos ayında, ağzıyla 'Zort!' sesi çıkaran bir jokerin hareketli resmini görüntülediği sırada gizlice bir Truva atını sisteme kuran bir saldırı ile, 1800 kadar kullanıcısının profillerinin bozulduğunu itiraf etti²² ve 23.



Öte yandan, Facebook üyeleri arkadaşlarının sosyal ağ üzerindeki ele geçmiş hesaplarının üzerinden, alıcının bilgisayarını enfekte etmek üzere tasarlanmış üçüncü parti web sitelerine bağlantılı mesajları da alıyorlar²⁴. Bilgisayar korsanları Facebook hesaplarını ele geçirmenin, kullanıcı adı ve şifreleri çalmanın ve sonra bu profilleri bir atlama tahtası olarak kullanıp kötü amaçlı yazılım saldırıları ve mesaj bombardımanları yaymanın harcanan emeğe değdiği görüşündeler²⁵.



Aniden beliren sinir bozucu reklamlar görüntülemek için tasarlanmış, üçüncü parti Facebook uygulamaları da mevcut²⁶. Ancak Facebook kullanıcı arayüzünü değiştirerek üçüncü parti uygulamaları daha az görünür hale getirdiğinden bu yana, bunlar belkisi kadar tehditkar değiller.



Daha yaygın programların suistimal edilmesi

Bilgisayar korsanları, yalnızca işletim sistemi ve tarayıcılardaki kırılğan noktaları suistimal etmeyi değil, Adobe Flash ve PDFler gibi diğer yaygın kullanılan program ve araçların da güvenlik açıklarını araştırıyorlar.

Kötü amaçlı Flash ve PDF dosyalarındaki artış kısmen, bubi tuzaklı kod içeren web saldırısı sayfaları oluşturan zararlı yazılım üretme kitlerinin kullanımı ile açıklanabilir. Flash ve PDF içeriklerinin saldırılara dahil edilmesi, yaygın olarak kullanılan Adobe tarayıcısı eklerindeki kırılğan noktaları hedeflemekte ve bunların güncel tutulmasının öneminin altını çizmektedir.

Ayrıca 2008’de çekirdek kipli, işletim sistemi öncesi kodların (rootkit) sayısında % 46’lık bir artış oldu. Bu kodlar karmaşık alt düzeyli işletim sistemi tekniklerini kullanmak suretiyle kendilerini kamufle ederek, geleneksel güvenlik ürünlerince saptanmaktan kaçınmaya çalışıyorlar.

Konumlarına göre, kötü amaçlı yazılımlar

SophosLabs’ın yaptığı araştırma, incelenen zararlı kod örneklerinin % 47.9’unda konum bilgisinin çıkarılmamasına karşın, toplam 44 değişik dilde yazılmış kötü amaçlı yazılımı ortaya çıkardı.

Çin tüm kötü amaçlı yazılımların % 11.6’sının sorumluluğunu taşıyor. Bu oran, Çinli bilgisayar korsanlarının, belirli bir bölgeden gelen zararlı kodların % 21’inden sorumlu olduğu 2007’ye göre küçük kalmaktadır. Dillerin kesin dağılımı şöyle:

- İngilizce konuşulan bölgeler - % 24.5
- Çince - % 11.6
- Almanca – % 3.7
- Fransızca – % 3.1
- Rusça – % 3.0
- Brezilya Portekizcesi – % 1.6
- Diğer – % 4.6
- Bulunamayan - % 47.9

Analiz dünyadaki değişik bilgisayar korsanı gruplarının güdeleri ve kullandıkları taktikler arasındaki birtakım ilginç farkları da ortaya çıkardı.

Çin kökenli kötü amaçlı yazılımların çoğu arka kapı Truva atları biçiminde; ancak bu yazılımların belirli bir bölümü de çevrimiçi oyuncuların şifre çalma güdüsünü taşıyor.

Brezilya’da yazılan kötü amaçlı kodların çoğu çevrimiçi işlem yapan bankalardan bilgi çalmak üzere tasarlanmış Truva atlarıdır. Bu arada Rus bilgisayar korsanlarının ise genellikle robot bilgisayar ağları (botnet) yaratmaya ve ele geçirilmiş bilgisayarlara uzaktan erişim vermek için, siber suçlulara arka kapılar açmaya yoğunlaştığı gözleniyor.

Üç internet şirketinin öyküsü

Atrivo

Intercage olarak da bilinen, Kaliforniya kökenli bu Internet Servis Sağlayıcısı, ağının büyük bölümlerinin sahte anti-virüs yazılımı (aslında panik yazılımı) ve kötü amaçlı yazılım satmak üzere kullanıldığını gösteren kanıtların yayınlanmasının ardından, Eylül’de Internet’ten çıkarıldı²⁷.

ESTDomains

Kısa süre sonra, Estonya’da yaşayan Rus kökenli Vladimir Tsastsin hakkında sorular sorulmaya başlandı²⁸. Tsastsin bir etki alanı kayıt servisi ve tesadüfen Atrivo’nun müşterisi olan EstDomains’in kurucusuydu. Şirketi suçlulara kötü amaçlı etkinlikleri için etki alanları kayıtları sağlamak ve EstDomains suistimal raporları aldığı dahi, bu etkinliklerin kapatılmamasını güvenceye alan, sağlam bir liman sunmakla suçlandı.

Estonya hükümetinin Tsastsin hakkında kredi kartı sahtekarlığı, kara para aklama ve diğer konularda suçlamalarda bulunmasının ardından ICANN, firmanın etki alanı kayıt servisi lisansını geri aldı.

McColo

Sahibi Rus olan başka bir ağ, yani McColo’nun beş büyük robot bilgisayar ağının (Srizbi (Zlob), Mega-D, Rustock, Dedler ve Storm) komuta ve denetim merkezlerini barındırdığı yaygın bir kanı idi.

McColo 11 Kasım 2008 saat 13:23’te Internet’ten çıkarıldığı²⁹, robot bilgisayar ağlarının çevrimdışı kalması mesaj bombardımanı düzeylerinde büyük bir düşme sonucunu doğurdu. McColo’nun çevrimdışı olmasının hemen ardından, mesaj bombardımanı hacmi % 75 oranında düştü³⁰. Bilgisayar korsanları o günden bu yana bu robot bilgisayar ağlarının denetimini yeniden elde etmeye çalışıp, bir ölçüde başarı sağladılar³¹.



Bu örneklerin gösterdiği gibi, güvenlik toplumunun bir arada çalışması, siber suç etkinliklerini global ölçekte, ciddi olarak engelleyebilir. McColo’nun alaşağı edilmesi gerçekten de dünya çapındaki mesaj bombardımanı düzeylerinde (geçici dahi olsa) herhangi bir bilgisayar korsanının yetkililerce tutuklanmasıyla elde edilene göre daha büyük bir etkiye neden olmuştur.

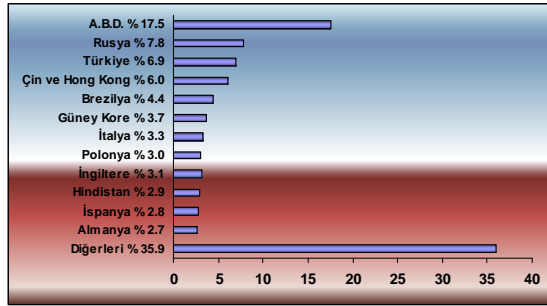
Mesaj Bombardımanı (Spam)

Mesaj bombardımanları hala popüler

Sophos'un araştırmasının ortaya çıkardığı sonuca göre, tüm iş nitelikli e-postaların % 97'si gibi inanılmaz bir oranını istenmeyen e-postalar oluştururken, bu durum işletmeler için belirgin bir sorun olmaya devam ediyor. Sophos'un dünya çapındaki istenmeyen mesaj tuzakları ağına her gün milyonlarca yeni mesaj gelmektedir.

Ülkelere göre mesaj bombardımanları

2008'de 240 ülkeden mesaj bombardımanı yapıldı. A.B.D. 2007'de elde ettiği % 22.5 oranının ardından, bu yıl mesaj bombardımanı sorununa yaptığı katkıyı azaltarak, tüm istenmeyen mesajların % 17.5'ini gönderdi. Ancak, sorunun üstesinden gelmek için hala çok çalışması gerekiyor.



2008'de en fazla mesaj bombardımanı yapan ilk 12 ülke

Bu durumda halen A.B.D. dünyadaki istenmeyen e-postaların –bunların bir bölümü de kötü amaçlı yazılım eklenmiş ya da kötü amaçlı veya enfekte olmuş web siteleriyle bağlantılıdır– çoğundan sorumludur. Bu mesaj bombardımanlarının çoğu bilgisayarlarının bir robot ağının parçası olduğundan habersiz ev kullanıcılarından gelmektedir.

Ancak robot bilgisayar ağı sorunu gerçekte tüm dünyada mevcuttur. Daha fazla bilgisayarın güncel anti-virüs koruması ile en son güvenlik yamalarına ve halkın, genel olarak, kişisel bilgileri ile bilgisayarlarını risk altında bırakmaktan nasıl kaçınılacağı konusunda, daha eğitilmiş olmaya geresinin duyduğu açıktır.

Siz de mesaj bombardımanı yapıyor musunuz?

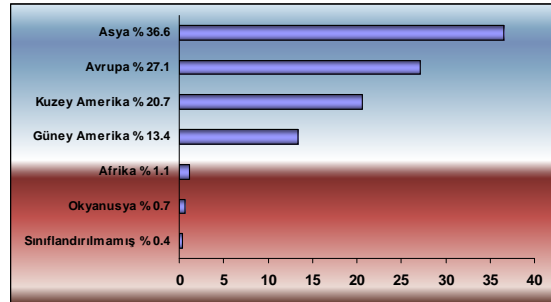
İstenmeyen mesajların hemen tümü, "robot" ya da "zombi" olarak anılan, başarıyla saldırılıp ele geçirilmiş ve artık sahiplerinin bilgisi dışında çok sayıda mesaj gönderen, dağıtım hizmet engelleme saldırıları başlatan ya da gizli bilgileri çalan bilgisayarlardan gelir.

Güncel anti-virüs koruması bulundurmak, bir güvenlik duvarı kurup etkinleştirmek ve tüm güvenlik yamalarını hem işletim sistemi hem de kurulu diğer uygulamalar için bulundurmak ele geçirilme riskini belirgin biçimde azaltacaktır.

Sophos ZombieAlert™ Servisi³² ele geçirilip, bilgisayar korsanları adına e-postalar gönderen iş bilgisayarlarını tanımlamaktadır.

Kitalara göre mesaj bombardımanları

Asya tüm mesaj bombardımanlarının üçte birinden fazlasını gönderirken, Avrupa ile birleştiğinde dünyadaki tüm istenmeyen e-postaların yaklaşık üçte ikisinin sorumluluğunu almaktadır.



2008'de, her kitadan yapılan mesaj bombardımanları

Web günlükleri üzerinden mesaj bombardımanı

Mesaj bombardımanları yalnızca e-posta üzerinden yapılmıyor. Ziyaretçileri yorum yazmaya davet eden web günlüklerinin tipik olarak zayıf sayfaları arayan robotlar tarafından kullanımı da giderek artmakta.

Birçok web günlüğü yayınlanmadan önce üzerlerindeki yorumları istenmeyen mesajlardan temizlemek için ücretsiz araçlar kullansa dahi, yazılan tüm web günlüğü yorumlarının % 85'inden fazlasının aslında istenmeyen mesajlar olduğu tahmin ediliyor³³.

Mesaj bombardımanı ve sosyal ağlar

Mesaj bombardımanı yapanlar, 2008 boyunca pazarlama mesajları ve kötü amaçlı yazılımlarını dağıtmak için yeni yöntemler denemekten çekinmediklerini kanıtladılar. Facebook ve Twitter gibi sosyal ağ web siteleri bu kişiler arasında giderek daha popüler hale geldi.



Bilgisayar korsanları, tipik olarak üyelerin kullanıcı adı ve şifrelerini çalıp, kurbanın arkadaşlarıyla ailesini kabaca kamufle olmuş pazarlama mesajlarına boğarak, onları üçüncü parti web sayfalarına yönlendirmektedirler.

Sosyal ağların ele geçirilmesinde ilginç bir eğilim de ortaya çıktı. Dolandırıcılar bir kişi olarak görünmek için, temiz Facebook hesaplarına girmektedirler. Daha sonra kişinin arkadaşlarına, yabancı bir şehirde tatil yaparken saldırıya uğrayıp cüzdanlarını ve uçakla dönüş biletlerini yitirdiklerini iddia eden mesajlar yağdırmaktadırlar. Sonraki adım ise Western Union³⁴ üzerinden kendilerine para gönderilmesini istemektir.

Alıştıkları gelen kutusuna düşen benzer e-postalardan normal olarak kuşkulanan bilgisayar kullanıcıları, arkadaşları olduğuna inandıkları bir Facebook bağlantısı üzerinden yapılan iletişimde etkilenmeye daha açık olabilirler. Dolandırıcılar seçtikleri kurbanla, elde ettikleri hesap bilgilerini kullanan uzun bir konuşmayı sürdürmek suretiyle, ağdaki suistimallerini daha da ilerletebilirler. Örneğin ele geçirilen hesabın sahibi durum mesajı ile, Facebook'taki arkadaşlarına belirli bir ülkeye yolculuk yapacağını söylemişse, saldırıya uğrama öyküsü iyice inanılır olmaktadır.

İnternet kullanıcıları gelecekte bu tip güven hilelerinden kaçınmak istedikleri takdirde, böyle mesajlara karşı daha kuşkucu ve olumsuz davranmaları gerekecektir.

Kasım 2008'de, Facebook, ele geçirdiği hesaplar üzerinden kullanıcılara dört milyondan fazla mesaj gönderdiği bildirilen, Montreal kökenli bir mesaj bombardımancısına karşı açılan bir davada 873 milyon A.B.D. doları tutarında tazminat kazandı³⁵. Sophos sosyal ağ web sitelerinin üzerinden gönderilen mesaj bombardımanı sayılarında bir artış gözlemiş ve bu artışın süreceğini öngörmüştür.

Mesaj bombardımanlarında diğer eğilimler

Mesaj bombardımanı yapanlar meşru e-posta haber bültenlerinin şablon ve tasarımlarını kopyalayarak, "haber bültenli" mesaj bombardımanının, popüler bir gönderim yöntemi olduğunu gösterdiler. CAPTCHA (completely automated procedure for telling computer and humans apart – bilgisayarları insandan ayırt etmek için, tümüyle otomatik yordam) sistemini kıran bilgisayar korsanları, tüm dünyaya istenmeyen mesajlar göndermek için, Gmail, Hotmail ve Yahoo gibi web postası hesaplarını da kullanmaktadırlar.



Apple

Mac kullanıcıları: Rahat bir hedef

Apple'daki kötü amaçlı yazılım sorunu Windows kullanıcıları için olanla kıyaslandığında ufak kalmaktadır. Ancak, 2007 sonlarında Mac OS X'e yönelik finansal dürtü taşıyan ilk zararlı yazılımın çıkışından bu yana, bilgisayar korsanlarının Mac bilgisayarları enfekte etmek için giderek artan sayıda deneme yaptığı görülmektedir.

Şubat 2008'de, Flash tabanlı yeni bir Truva atı olan Troj/Gida-B₃₆, kullanıcıları sahte güvenlik yazılımı satın almaları için korkutmak amacıyla tasarlandı. Bu panik yazılımı saldırısı gerek Mac, gerekse Windows bilgisayarlarında aynı ölçüde iyi çalışan, zararlı web reklamları kullanıyordu.

Haziran 2008'de keşfedilen OSX/Hovdy-A Truva atı³⁷, Mac OS X bilgisayarlara da bulaşabilme becerisine sahip ve şifreleri çalmaya, güvenlik duvarlarını açmaya ve güvenlik ayarlarını devreden çıkarmaya çalışıyor. Kök erişimini elde etmek için Mac OS X'te bulunan ARDAgent zayıflığından yararlanıyor. Bir bilgisayar bir kez enfekte olduktan sonra, bilgisayar korsanı tam denetim elde edip sistem işlem kayıtlarını devre dışı bırakmak suretiyle izlerini kapatabilir.

Ağustos 2008'de bilgisayar korsanlarının arka kapı Truva atları yaratmasına yardımcı bir Mac OS X aracı olan Troj/RKOSX-A₃₈ keşfedildi. Sophos üç ay sonra, web sitelerine yerleştirilen yeni bir Mac zararlı yazılımı olan OSX/Jahlav-A₃₉'nin keşfedildiğini bildirdi. Bu Truvat atı meşru bir uygulama gibi görünmekte, ancak kurulumdan sonra, Hollanda'daki bir sunucudan ek bileşenler indirmektedir.



Ortalıkta sayıca daha az Mac tabanlı kötü amaçlı yazılım olsa da, Mac kullanıcılarının uyanık olmalarını gerektiren birkaç neden var:

- Mac topluluğunda yüksek düzeyli bir iç huzuru, birçok kullanıcının hatalı olarak Internet güvenlik tehditlerine karşı bağışık olduklarına inanmaları anlamına gelmektedir. Bu durum onları gelecekteki saldırılar için rahat bir hedef haline getirmektedir.
- Apple Mac donanımında Intel tabanlı yongaların kullanımı Mac'lerde Windows kullanımını yaygınlaştırmıştır. Bu durum Mac'lerin Windows zararlı yazılımlarını barındırmasını ve yaymasını eskiye kıyasla daha muhtemel hale getirmektedir.
- 2008'de birtakım kullanıcıların hiç kuşkusuz Windows Vista'dan hoşnutsuzlukları nedeniyle PC'lerini değiştirmelerinden ötürü, rekor sayıda Apple Mac bilgisayar satışına tanık olundu⁴⁰. Apple Mac'leri Pazar payı büyürken, Mac kullanıcılarının kendilerine yönelik daha fazla saldırıyla karşılaşması da muhtemel.

Birçok Windows ev kullanıcısının kendilerini kötü amaçlı yazılımlar ve casus yazılımlara karşı düzgün koruma yeteneğinden yoksun olduğu gözlenirken, bu kullanıcıların bir bölümünün Apple Mac platformuna geçmesini önermek akla yakın gelmektedir. Bunun nedeni Mac OS X'in daha üstün olması değil, şimdilik ona yönelik yazılmış, belirgin ölçüde az sayıda kötü amaçlı yazılımın bulunması nedeniyle. Öngörülebilir gelecekte, karlarını azamileştirmek arayışındaki siber suçluların çoğunlukla Windows'a saldırıyı sürdürmeleri muhtemeldir.

Ancak, Mac'lere yönelik kötü amaçlı yazılımlar yazılmaya devam edecektir ve kullanıcıların güvenli bilgisayar kullanımında, bir anti-virüs ürününü çalıştırmak ve güvenlik yamaları ile güncel kalmak gibi en iyi pratikleri izlemeleri gereklidir.

Mobil telefonlar ve Wi-Fi cihazlar

Akıllı telefonlardaki güvenlik açıkları

2008'de, Apple iPhone'un 3G sürümünün başlangıcı ve Google Android mobil işletim sistemini kullanan ilk telefon büyük gösterilerle ortaya çıktı.

Apple iPhone

iPhone'un 3G sürümünün üstün bağlanabilme becerisi ve daha ucuz fiyatından ötürü, önceline kıyasla iş ve Internet kullanıcıları için daha çekici olduğu tartışılmaz. Apple en güncel finansal sonuç raporunda iPhone'un satışlarının RIM'in sevilen Blackberry cihazını geçtiğini bildirmiştir⁴¹.

Öte yandan Apple'ın artan pazar payı, gelecekte suçluların ellerindeki cihazlardan yararlanmak üzere daha yoğun çabalar göstereceğinin habercisi olabilir.

Hali hazırda yalın zararlı yazılımlar ortaya çıkmış olsa da, iPhone henüz belirgin bir saldırının hedefi olmamıştır. Ancak, Apple'ın mobil e-posta uygulaması ve web tarayıcısı Safari'de güvenlik açıkları bulunmuştur ve şirket, bu açıklar için yamaları, Mac OS X çalıştıran diğer bilgisayarları ile aynı zamanda hazırlamaması bakımından eleştiri almıştır.

iPhone kullanıcıları, masaüstü kullanıcılarına kıyasla, ortalama (phishing) saldırılarına karşı daha zayıf durumda olabileceklerini de bilmelidirler. Zira:

- URL'leri dokunmaya duyarlı ekran üzerinden girmeleri gereklidir ve e-posta bağlantılarına tıklayıvermeye daha istekli olabilirler.
- Safari'nin iPhone sürümü üstlerine tıklanmadıkça, e-postalara gömülmüş URL'leri görüntülememektedir. Bu nedenle kullanıcıların bağlantının örneğin sahte bir banka sitesine gidip gitmediğini söylemesi daha güçtür.
- iPhone'un tarayıcısının adres çubuğunda yalnızca kısmi URL'leri görüntülemesi siber suçluların kullanıcıları meşru bir web sitesinde olduklarına inandırarak aldatmasını çok daha kolaylaştırmaktadır.

Google Android

Bu raporun yazıldığı an itibarıyla, piyasada Google Android işletim sistemini kullanarak, bilgisayar korsanlarına bu işletim sistemine ilk gerçek incelemeyi sağlayan tek mobil telefon T-Mobile G1 dir. Önceki izlenimlerin tipik olarak Apple iPhone ile olan kozmetik farklılara (kayarak çıkan klavye ve daha az esnek olan dokunmatik ekran) yoğunlaşmasına karşın, G1'in web tarayıcısındaki bir güvenlik zaafı hemen bulundu⁴².



Bu arada, Google'ın uygulamalara karşı "açık" davranışının, kötü amaçlı programların, telefonunun kullanıcıları arasında çok daha kolay dağıtılabilmesi anlamına gelebileceğine ilişkin kaygılar da açığa çıkmıştır.

Sophos bu işletim sistemlerine yönelik ilk kötü amaçlı yazılım örneklerinin muhtemelen, finansal dürtüleri olan suçlular yerine, manşetlere geçmek isteyen hevesliler tarafından yazılacağına inanmaktadır. Ancak, milyonlarca yeni kişi daha mobil telefonları satın aldıça, bu telefonlara yönelik tehditlerin yaratılması, akılları suça işleyen kişiler için de giderek daha çekici olacaktır. Bunun bir örneği, Mac bilgisayar ve iPhone'un ortak özelliklerini ve teknolojisini tehdit edebilecek, jenerik bir Mac OS X saldırısının yaratılması olabilir⁴³.

Benzer biçimde, Google Android kullanıcılarına yönelik deneysel saldırıların görülmesi de sürpriz olmayacaktır.

Bu tip saldırıların, kullanıcıları tehlikeli kod çalıştırmak üzere aldatmak için yazılım zaafılarından, sosyal mühendisliğe dayanması beklenir. Bu durumda, üçüncü parti uygulamaları tedbirsizce yüklemek alışkanlığında olan mobil telefon kullanıcıları cihazlarını enfekte etme olasılığını da arttıracaklardır.

Veri sızdırma

Güvensiz veriler

2008'de şirketler ve hükümet gizli bilgilerinin korumada gevşek davrandıklarını gösterdikçe, veri sızıntıları haberleri başlıkları doldurdu⁴⁴.

Her boyuttaki kuruluşlar günümüzün hareket halinde ve işbirliği içindeki iş gücünün, iş arkadaşları ve ortaklarıyla veri paylaşımı becerisinin yanında, ofis içi ve dışında bilgiye erişim gereksinimi duyduğunu anlamaktadırlar.

Kullanıcılar bilgiyi gizliliği ve düzenleme kurallarını düşünmeksizin, rutin olarak kullanmakta ve paylaşmaktadırlar. Neredeyse % 30'u sözleşme ve finansal bilgileri, müşteri bilgilerini, satış hedeflerini, bağlantı ayrıntılarını ve kişisel hesap bilgilerini çıkarılabilir ortam üzerinde tutmaktadır⁴⁵. Bu durum veri kaybının kötü amaçlı değil, daha çok kaza sonucunda ortaya çıktığı çeşitli olaylara yol açmıştır.



Kullanılmış donanım

Güvenli olarak silinmemiş, eski bilgisayar donanımlarının eBay gibi açık arttırma sitelerinde satılmasının ardından, gizli bilgilerin kamuya açıldığı bir dizi olay raporlanmıştır⁴⁶.

Bu durum birtakım gözlemcilerin eBay'de, kullanılmış sabit disklere yepyeni olanlara kıyasla daha yüksek talep olduğunu (ve dolayısıyla daha büyük fiyatların önerildiğini) iddia etmelerine neden oldu. Kurtarılabilme potansiyeli taşıyan gizli bilgi miktarı gözönüne alındığında, bu hiç de sürpriz değil⁴⁷.

Şifreleme

Veri sızdırmasını durdurmanın en önemli adımı duyarlı bilgileri, dizüstü bilgisayarları, çıkarılabilir saklama cihazlarını ve e-postaları şifrelemektir. Veriler bir şifre kullanılarak şifrelenmişse, şifre bilinmeden deşifre edilemez ya da kullanılamazlar. Bunun anlamı, diğer tüm güvenlik kıstasları bir bilgisayar korsanını en duyarlı bilgilerinize erişmekten alıkoyamasa dahi, bilgilerinizin okunamayacağı ve böylece bilgi bütünlüğünüzün zarar görmeyeceğidir.

Veri kaybı çok maliyetlidir

Ağustos 2008'de A.B.D. yetkilileri 11 kişiyi 40 milyondan çok kredi ve banka kartı numarasının çalındığı bir vurguna karışmakla suçladılar. Etkilenen perakendeciler arasında OfficeMax, Barnes & Noble, Boston Market, İngiltere'de TK Maxx olarak bilinen TJ Maxx perakende mağazalarını işleten TJX ve Marshall's bulunuyordu.

Gizli Servis ve Adalet Bakanlığı'na göre, otomobile gezerek, güvenli olmayan ve girilebilecek kabloşuz şirket ağları arayan çete kötü amaçlı programlar kurup çalınan bilgileri A.B.D. ve Doğu Avrupa'daki diğer suçlulara satıyordu. Daha sonra, sahte kredi kartları kullanılarak ATM'lerden gayrimeşru onbinlerce dolarlık tutarlar çekiliyordu.

Başka bir olayda ise, İngiliz İçişleri Bakanlığı 130,000 civarında sabikalının şifrelenmemiş kişisel ayrıntılarını içeren bir USB bellek çubuğunun kayıp olduğunu kabul etti. Bilgiler arasında isimler, adresler, doğum tarihleri ve mahkumlardan bir bölümünün salıverilme tarihleri bulunuyordu. USB bellek çubuğu sonuçta İngiliz hükümeti ile yaptığı 1.5 milyon £ tutarındaki bir sözleşmeyi kaybeden, dış yüklenici PA Consulting tarafından kullanılmaktaydı.

İkinci adım kullanıcıların bilgiye nasıl davrandığının denetlenmesidir. USB çubuklarına şifrelenmemiş bilgilerin aktarılması gibi riskli davranışları durdurmak istemeniz doğaldır. ch as transferring unencrypted information onto USB sticks. Kuruluşlar,

- Bilginin kullanımını denetlemek
- İşlem etkinliğini garantilemek
- Çeşitli düzenlemelerin getirdiği gereksinimleri karşıladıklarını kesinleştirmek

için kötü amaçlı yazılım karşıtı altyapılarını genişletmelidirler.

Kuruluşların, 2009'da artan iş kayıpları olasılığıyla, ayrılan elemanların kullandığı cihazların düzgün biçimde şifrelendiğinden ya da güvenli biçimde silindiğinden emin olma konusunda da dikkatli davranmaları gerekmektedir. Bilgi ile ayrılan ya da karşı casusluğa girişen hoşnutsuz elemanların taşıdığı potansiyel risk de ayrıca düşünülmelidir.

Devlet destekli siber suç

Dijital casusluk artıyor

Ülkeler politik, ticari ve askeri yararlar nedeniyle birbirlerini gizlice izlerler ve bunu yaparken bilgisayarlarla internetin yardımını kullanmayacaklarını düşünmek saflık olur.

2007’de, örneğin Çin genelkurmayının Eylül’de Pentagon’daki bir bilgisayar sistemine siber saldırıda bulunmaktan suçlanması olayındaki⁴⁸ gibi, ülkelerin birbirlerini açıkça Internet üzerinden casuslukla suçlaması olağan hale geldi. İngiliz gizli servisi MI5’in İngiliz şirketlerinin 300 üst yöneticisi ve güvenlik sorumlusuna yaptığı yazılı “elektronik casusluk saldırısı” uyarısının 2007 sonlarında keşfinin ardından, devlet destekli siber suç kaygıları zirveye vurdu.

2008’de bunlardan da fazla, hükümet destekli siber suç iddiasındaki rapor örneği görüldü. Bir devlet tarafından onaylanan bir saldırıyı kanıtlamak çok güç olsa da, 2009’un Internet üzerinden birbirlerine saldıran ve birbirlerini izleyen ülkelere ilişkin daha fazla iddiayı getirmesi muhtemel.

- **Nisan 2008.** *Der Spiegel*’in bildirdiğine göre, BND – Alman harici istihbarat servisi – Afganistan Ticaret ve Sanayi Bakanlığı’na izlemek için casus yazılım kullanmıştır⁴⁹. Gizli belgelerin, şifrelerin ve e-posta iletişimlerinin Alman casuslarınca ele geçirilip BND merkezine gönderildiği iddia edildi. Bu haber BND’nin *Spiegel*’de muhabiri Susanne Koelbl ve Afganistan Ticaret Bakanı Amin Farhang arasındaki e-postalara girdiğine ilişkin açıklamaları izledi ve sonucu ülkeler arasında diplomatik bir kavga oldu.
- **Mayıs 2008.** Yeni Delhi’deki kıdemli Hindistan güvenlik görevlilerinin, Çinli bilgisayar korsanlarının, Dışişleri Bakanlığı ile, Hindistan’daki diğer yönetim kuruluşlarının yanında, merkez ve eyalet hükümetlerin ağ omurgasını oluşturan Ulusal Enformatik Merkezi’ni hedeflediklerini kabul ettiği bildirildi⁵⁰. İsimleri belirtilmeyen görevlilerin olaydan Çin’in potansiyel bir rakibin üzerinde “asimetrik avantaj” kazanma yolu olarak söz ettiği açıklandı.
- **Mayıs 2008.** Belçika da Federal Hükümete karşı yapılan bilgisayar korsanlığı saldırılarının Çin kökenli olduğunu ve muhtemelen hükümet emriyle yapıldığını iddia ederek, Çin hükümetini siber casuslukla suçladı⁵¹. Ayrıca Belçika Dışişleri Bakanı, parlamentoya bakanlığının birkaç hafta önce Çin ajanlarının siber casusluk hedefi olduğunu söyledi.

- **Ağustos 2008.** Güney Osetya’da gerginlik artarken, Rus ve Gürcü bilgisayar korsanları birbirlerine karşı saldırılar başlattılar⁵². Örnekler arasında Güney Osetya hükümetinin web sitesine karşı, dağıtımlı bir hizmet engelleme saldırısı ve Gürcistan Dışişleri Bakanlığı’nın web sitesinin görünüşünün Gürcistan cumhurbaşkanı Mikhail Saakashvili ve Adolf Hitler resimlerinin bir kolajıyla değiştirilmesi bulunuyordu⁵³.



- **Eylül 2008.** Seul Kuzey Kore’deki rakiplerini casus yazılımlar ve bir kadın ajanı kullanarak, askeri görevlilerden evrak çalmakla suçladı⁵⁴. Casus yazılım saldırısı, enfekte edilen bilgisayarlardan evrak çalmak için tasarlanmış, kötü amaçlı bir e-posta eki biçimindeydi. E-posta adreslerini sağlayan kişi, 35 yaşındaki Won Jeong Hwa idi.

Tutuklamalar ve hukuk

Parmaklıklar arkasında

Uluslararası bilgisayar suçları otoriteleri siber suçluları ortadan kaldırmak için güç birliği yaparken, son oniki ayda yüksek profilli ve finansal getirisi fazla bilgisayar suçlarına karışan kişilere yönelik daha fazla tutuklama ve daha ağır cezalar görüldü.

Aşağıda 2008’de haber başlıklarını oluşturan vakalardan yalnızca bir bölümü verilmektedir.

- **Ocak 2008.** Özenle hazırlanmış bir e-posta dolandırıcılığına girerek 1.2 milyon A.B.D. dolarının üzerindeki bir tutarı çalan üç kişi New York’taki bir mahkemece suçlu bulundu⁵⁵. Bu kişiler ölümcül gırtlak kanseri olan ve hayır işlerine 55 milyon A.B.D. doları bağışlamak isteyen bir kurbanın ağzından yazılmış e-postalar gönderiyorlardı. Daha sonra, çete üyelerinden biri olan Nnamdi Chizuba Ainsiohi’nin, hastalık çeker gibi sesini değiştirerek alıcılara telefon ettiği belirtildi.
- **Şubat 2008.** Bir Amerikan genci yüzbinlerce zombi bilgisayarı ele geçirerek onları para getiren reklamlar göstermek için kullanmaktan suçlu bulundu⁵⁶. Ele geçirilen bilgisayarların bir bölümü A.B.D. Donanma Hava Kuvvetleri Savaş Merkezi ve A.B.D. Savunma Bakanlığı’nda bulunuyordu.



- **Mart 2008.** Bir Çin mahkemesi Internet bankacılığı hesap bilgilerini çalmak için bir Truva atını kullanan dört kişiye 6.5 ila 8 yıl arasında değişen hapis cezaları verdi⁵⁷.
- **Nisan 2008.** Bir İsrail mahkemesi Modi’in Ezrahi özel dedektiflik şirketinin üç elemanını ticari bilgileri çalmak için bir Truva atı kullanmaktan suçlu bularak hapse atılmalarına karar verdi⁵⁸.
- **Mayıs 2008.** A.B.D. ve Romanya yetkilileri toplam 38 şüpheliyi ortalama e-postaları ve SMS mesajları üzerinden yüzlerce finans kuruluşunu hedefleyen uluslararası bir suç şebekesi kurmak nedeniyle suçladılar⁵⁹.

- **Haziran 2008.** 19 yaşındaki Jason Michael Milmont Windows bilgisayarları enfekte eden zararlı yazılım Nugache’in programcısı olduğunu itiraf etti⁶⁰. Bu kötü amaçlı yazılım bilgisayarları eşler arası (P2P) denetlenen, aynı anda 5,000 ila 15,000 adet ele geçirilmiş bilgisayardan oluşan, karmaşık bir robot bilgisayar ağına dönüştürüyordu. Milmont hesaplara erişmek ve alışveriş yapmak için çalınmış banka bilgilerini kullanmaktaydı.
- **Temmuz 2008.** Manhattan’da bulunan bir federal mahkeme 17 yaşındaki Adam Vitale’i bir haftadan az sürede 1.2 milyondan fazla istenmeyen mesaj gönderdiği için 30 aylık hapis cezasına mahkum etti⁶¹. Vitale mesajlar üzerinden yapılan mal satışlarından kar payı almayı umuyordu.
- **Ağustos 2008.** FBI ve Brezilya Federal Polisi’nden yardım alan Hollanda’lı yetkililer Leni de Abreu Neto ‘yu tutukladı⁶². 35 yaşındaki Brezilya’lının 100,000 bilgisayardan oluşan bir robot bilgisayar ağını işlettiği ve kiraladığı iddia ediliyordu.
- **Eylül 2008.** Calgary’de bulunan bir şirketten 1.8 milyon Kanada doları (yaklaşık 1.69 milyon A.B.D. doları) çaldığı belirtilen ve kredi kartı verileri hırsızlığı yaptığı iddia edilen bir çete Kanada polisince tutuklandı⁶³. Tutuklananlardan biri, 10 yıl önce Pentagon bilgisayarlarına yasadışı yollarla girdiği için yakalanan “Analizci” lakaplı Ehud Tenenbaum idi.
- **Ekim 2008.** Federal Ticaret Komisyonu (FTC) bir mahkemeyi, büyük bir uluslararası mesaj bombardımanı işleminden şüphelenilen bir grubu kapatmaya ikna etti⁶⁴. FTC mesaj bombardımanı kampanyası ile ilgili, çoğu “% 100 güvenli ve doğal bitkisel” erkeklik geliştirici ilaç öneren e-postalar alan bilgisayar kullanıcılarından, üç milyonun üzerinde şikayet aldığını iddia ediyordu.
- **Kasım 2008.** Bir A.B.D. mahkemesi CyberSpy Software LLC’yi RemoteSpy tuş vuruşu kaydetme yazılımını satmaktan men ederken, FTC bu yazılımın yasadışı kullanılıp kullanılmadığını araştırıyordu⁶⁵. Yasak Aralık ayında kaldırıldı⁶⁶.



Gelecek

Saldırıların karmaşıklığında artış

Böyle hızlı evrimleşen bir ortamda geleceği tahmin etmek neredeyse olanaksız. Tehditlerin ne kadar hızlı biçimde ciddileştiğini görmek için, kişinin yalnızca, günümüzde yeni kötü amaçlı yazılımların çıkış oranını beş yıl öncekine kıyasla hesaba katması yeterli.

Yine de kesin görünen şeyler var:

- Organize suçluların bilgi, kimlik ve kaynakları çalmak amacıyla bilgisayarlara girme isteği **saldırıların çeşitliliği** ve sayısındaki artışın sürmesine neden olacak.
- **Veri sızdırma**, özellikle mobil teknolojilerin artan ölçüde kullanımı ile, her zamankinden de büyük bir kaygı konusu haline gelecek. Birçok ülkede katı ifşaat yasaları getirilmiş ya da yakında getirilecektir. Bu yasaların hedefi şirketlerin güvenlik ihlallerini halının altına süpürmesini durdurma. Çok kısıtlı bir veri güvenli ihlali dahi, bir kez ifşa edildikten sonra, bir kuruluşun ürün ve hizmetlerine duyulan tüm güveni etkileyebilir.



- Gerek ev, gerekse iş ortamında, **ele geçirilen PC'ler** mesaj bombardımanlarının birincil kaynağı olarak kalmaya devam edecek. Merkezi olmayan, P2P tipinde bir işletim uygulayan birçok robot bilgisayar ağı söz konusu iken, McColo sağlayıcısının barındırdığı robot bilgisayar ağı komuta ve denetim merkezlerinin çökertilmesindeki başarı örneğinde görülen hızlı kazanımların elde edilmesi güçleşecektir.

- **Web'deki güvensizlik**, özellikle SQL enjeksiyonları gibi uzaktan yapılan otomatik saldırılara karşı olan zaafılar web üzerindeki kötü amaçlı yazılımları dağıtmanın birincil yolu olmayı sürdürecektir. Siber suçlular bu adımın ardından meşru ama ele geçirilmiş web sayfalarına bağlanan, masum görünümlü mesaj bombardımanları yapabilmektedir. Ele geçirilen bu siteler fark ettirmeden, kötü amaçlı içerik ile bağlantılı durumdadırlar.
- **Kötü amaçlı e-postalar** giderek artan oranlarla program olmayan (EXE uzantısız) dosya ekleri ya da bağlantıları içerecek. Bunlar yazılım zaafalarını suistimal eden bubi tuzaklarıyla donatılmış, Word belgeleri ya da PDF'ler gibi meşru görünümlü veri dosyaları olacak. Güvenlik yamaları yapılmış bir bilgisayarda bu dosyaları incelemek zararsız olacakken, yamanmamış bir bilgisayarda görünmeyen felaketlere yol açabilecek.
- **Kimlik hırsızlığı** müşteri bağlılığını olumsuz yönde etkilemeyi sürdürecektir. Şirketler önümüzdeki yıl müşterilerini düzgün ve tam güvenlik kıstaslarının uygulandığına ve böylelikle ihlal riskinin asgaride kaldığına ikna etmek zorunda olacaklar.

Suçlular para kazanmak ve kargaşa yaratmak için yeni teknolojileri devreye aldıkça, bilgisayar kullanıcıları da cihazlarını güvenceye almak ve denetlemek konusunda daha büyük güçlüklerle karşılaşacaklar. Bunların yanı sıra, insan hataları nedeniyle kimlik hırsızlığı ve dolandırıcılık gibi tehditler uzak gelecekte de yer almaya devam edecek.

Ancak, bu sorun düzgün ele alındığı takdirde aşılmaz olmasa gerek. Güçlü güvenlik pratikleri, güncel koruma ve etkin biçimde bilgi kalma çabası bir araya gelerek, önümüzdeki yıl içinde iş ağlarının savunmasına yardım edebilirler.

İyi haber ise şu: Güvenlik yazılımları sürekli olarak iyileşiyor. Yeni ve bilinmeyen kötü amaçlı yazılım tehditlerinin proaktif olarak keşfedilmesi konusu her zaman yükseliştir ve makul, düzgün korunan bilgisayar kullanıcıları riskleri dramatik ölçüde azaltabilirler.

Kaynaklar

1. www.sophos.com/pressoffice/news/articles/2008/02/poisoned-adverts.html
2. www.sophos.com/pressoffice/news/articles/2008/03/euro2008.html
3. www.sophos.com/security/blog/2008/03/1186.html
4. www.sophos.com/security/blog/2008/04/1292.html
5. www.sophos.com/pressoffice/news/articles/2008/06/infected-tennis-sites.html
6. www.sophos.com/pressoffice/news/articles/2008/07/playstation.html
7. www.sophos.com/blogs/gc/g/2008/09/15/hackers-infect-businessweek-website-via-sql-injection-attack/
8. www.sophos.com/pressoffice/news/articles/2008/10/adobe-infection.html
9. www.sophos.com/security/sophoslabs/anonymizing-proxies.html
10. www.sophos.com/security/blog/2008/08/1685.html
11. www.sophos.com/blogs/gc/g/2008/09/17/hackers-distribute-trojan-as-iphone-game/
12. www.sophos.com/blogs/gc/g/2008/10/13/malicious-microsoft-security-patch-spammed-out-before-patch-tuesday/
13. www.sophos.com/pressoffice/news/articles/2008/07/security-report.html
14. www.sophos.com/pressoffice/news/articles/2004/03/va_bagelnetsky.html
15. www.sophos.com/blogs/gc/g/2008/08/07/exposed-cnn-top-ten-video-malware/
16. www.sophos.com/blogs/gc/g/2008/11/05/the-president-elects-first-malware-campaign/
17. www.sophos.com/blogs/gc/g/2008/09/10/barack-obama-sex-video-malware-campaign/
18. www.sophos.com/blogs/gc/g/2008/09/23/free-norton-antivirus-hackers-disguise-fake-product-to-spread-trojan/
19. www.sophos.com/pressoffice/news/articles/2008/03/lee-shin-ja.html
20. www.sophos.com/pressoffice/news/articles/2008/02/poisoned-adverts.html
21. www.sophos.com/blogs/gc/g/2008/08/27/computer-worm-strikes-international-space-station/
22. www.sophos.com/blogs/gc/g/2008/08/08/up-to-1800-profiles-hit-by-malware-attack-says-facebook/
23. www.sophos.com/blogs/gc/g/2008/08/07/more-malicious-links-seen-on-facebook/
24. www.sophos.com/blogs/gc/g/2008/08/04/facebook-and-myspace-malware/
25. www.sophos.com/blogs/gc/g/2008/09/17/facebook-malware-is-a-real-threat/
26. www.sophos.com/pressoffice/news/articles/2008/01/facebook-adware.html
27. <http://voices.washingtonpost.com/securityfix/2008/09/internet-shuns-us-based-isp-am.html>
28. <http://voices.washingtonpost.com/securityfix/2008/10/icann-de-accredits-estdomains.html>
29. www.sophos.com/security/blog/2008/11/1970.html
30. <http://voices.washingtonpost.com/securityfix/2008/11/the-badness-that-was-mccolo.html>
31. www.sophos.com/security/blog/2008/11/2028.html
32. www.sophos.com/products/enterprise/alert-services/zombiealert.html
33. <http://akismet.com/stats>
34. www.sophos.com/blogs/gc/g/2008/11/10/facebook-friend-stranded-in-nigeria-would-you-rescue-them/
35. www.sophos.com/blogs/gc/g/2008/11/25/facebook-takes-on-spammer-and-wins-873-million/
36. www.sophos.com/pressoffice/news/articles/2008/02/poisoned-adverts.html
37. www.sophos.com/pressoffice/news/articles/2008/06/machovdyA.html
38. www.sophos.com/security/blog/2008/11/1999.html
39. www.sophos.com/security/blog/2008/11/2024.html
40. www.apple.com/pr/library/2008/10/21results.html
41. www.apple.com/pr/library/2008/10/21results.html
42. www.nytimes.com/2008/10/25/technology/internet/25phone.html
43. www.sophos.com/blogs/gc/g/2008/11/03/guest-blog-will-hackers-make-the-iphone-an-iphOwn/
44. www.sophos.com/blogs/gc/g/category/data-leakage/
45. Utimaco Removable Media survey, 2007.
46. www.sophos.com/blogs/gc/g/2008/09/30/who-needs-to-steal-data-when-you-can-buy-it-on-ebay/
47. www.sophos.com/blogs/gc/g/2008/08/26/are-your-bank-details-being-sold-on-ebay/
48. www.sophos.com/pressoffice/news/articles/2007/09/chinese-hack.html
49. www.sophos.com/blogs/gc/g/2008/04/28/german-spooks-deploy-spyware-against-afghan-ministry/
50. www.sophos.com/blogs/gc/g/2008/05/09/china-crisis-now-india-claims-hackers-are-attacking-it-from-behind-thebamboo-curtain/
51. www.sophos.com/pressoffice/news/articles/2008/05/belgium.html
52. www.sophos.com/blogs/gc/g/2008/08/12/update-on-website-attacks-in-georgia-and-russia/
53. www.sophos.com/blogs/gc/g/2008/08/12/conflict-between-russia-and-georgia-turns-to-cyber-warfare/
54. www.sophos.com/blogs/gc/g/2008/09/02/sex-spyware-and-north-and-south-korea/
55. www.sophos.com/news/2008/01/nigerian-scam.html
56. www.sophos.com/news/2008/02/sobe.html
57. www.sophos.com/news/2008/03/zhang.html
58. www.sophos.com/blogs/gc/g/2008/04/29/i-spy-with-my-private-eye
59. www.sophos.com/news/2008/05/phishing-gang.html
60. www.sophos.com/news/2008/06/milmont.html
61. www.sophos.com/blogs/gc/g/2008/07/16/30-months-of-bread-and-water-for-spammer/
62. www.sophos.com/blogs/gc/g/2008/08/22/brazilian-charged-with-selling-access-to-100000-pc-botnet/
63. www.sophos.com/blogs/gc/g/2008/09/05/gang-arrested-in-canada-for-alleged-credit-card-data-heist/
64. www.sophos.com/blogs/gc/g/2008/10/14/ftc-shuts-down-major-international-spam-operation/
65. www.sophos.com/blogs/gc/g/2008/11/18/court-orders-company-to-stop-selling-spyware/
66. www.prweb.com/releases/spy/software/prweb1706254.htm