İnternet'in Yeni Belalıları: SOLUCANLAR

Burak DAYIOĞLU
Güvenlik Danışmanı - Pro-G Bilişim Güvenliği ve Araştırma Ltd. Şti.

1998 yılında, R. Morris hem kendisini ve hem de İnternet'i derinden etkileyen bir deney gerçekleştirdi. Kendisini bir bilgisayardan diğerine kopyalayarak ağa bağlı bilgisayarlar üzerinde gezinecek bir solucan programı hazırladı. Solucan (ing. worm), otonom biçimde hareket eden ve kendisini bir bilgisayardan diğerine yetkisiz biçimde kopyalarak yayılan programlar için kullanılan bir terimdir. Morris solucanı herhangi bir anda ağ üzerinde yalnızca yedi bilgisayar üzerinde çalışacak, sekizinci bir bilgisayara kendisini kopyaladığında en eski kopyasını silecek ve böylece hep yedi kopya olacak biçimde bilgisayarlar üzerinde bir gezinti gerçekleştirecekti.

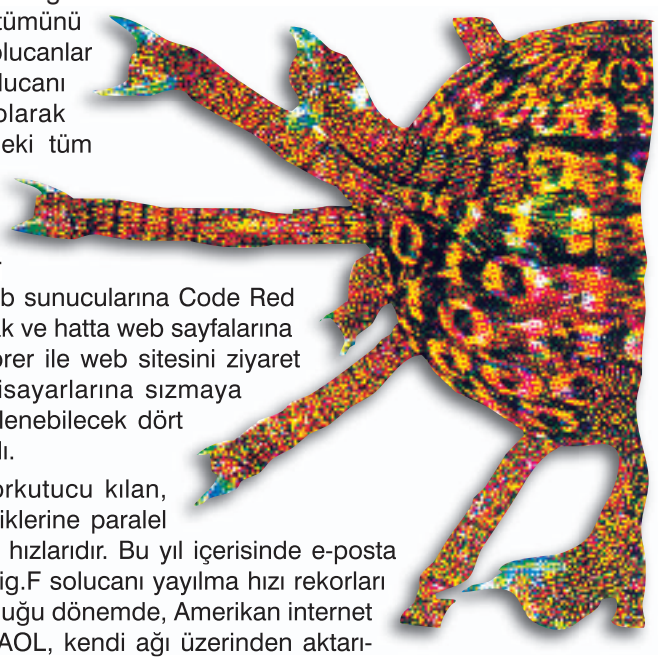
Solucanı denemek üzere İnternet'e bağlı bir bilgisayar üzerinde başlatan Morris, programda yaptığı bir hata nedeniyle İnternet'i çökme noktasına getirdi. Solucan, yeni kopyalarını ürettikten sonra eskilerini durdurmadı ve bu solucandan etkilenen bilgisayarlar üzerinde inanılmaz bir iş yüküne neden oldu; bilgisayarlar, neredeyse durma noktasına getirdi [2].

2001 yılının yazında İnternet'e bağlı olan ve Microsoft IIS web sunucu yazılımını çalıştıran pek çok bilgisayar "Code Red" isimli bilgisayar solucanından (ing. computer worm) etkilendi. Solucan, programcısının tarifi doğrultusunda ihtiraslı ve aceleci bir yayılma çabası içerisinde olduğundan pek çok web sunucusunu hizmet veremeyecek kadar meşgul etti. Dahası, İnternet bağlantılarını aşırı yükleyerek iletişimi ciddi biçimde yavaşlattı [1]. Morris solucanından bu yana görülen en önemli solucan vakalarından birisi olan "Code Red", bir ağ ile bağlanmış çok sayıda bilgisayarın ne denli hızlı bir biçimde ele geçirilebildiğine ilişkin tüm dünyaya önemli bir hatırlatma yapmış oldu; solucan 13 saat içerisinde 350,000'den fazla bilgisayarın denetimini ele geçirdi [3].

Code Red'i programlayanın hedefi http://www.whitehouse.gov adresinden yayın yapan Beyaz Saray web sitesini çökertmekti. Solucanın yerleştiği her bilgisayar, ayın yirminci gününden sonraki her gün Beyaz Saray web sitesine çok yoğun bir biçimde web sayfası istekleri yapıyor ve böylece siteyi erişilemeyecek kadar yoğun kılarak hizmet kesintisine neden oluyordu.

Code Red'in ardından pek çok farklı solucan bilgisayar sistemlerine çok önemli zararlar verdi. Daha önemlisi, her yeni solucan bir öncekinden daha karmaşık ve kapsamlı olmasına rağmen, İnternet'in sağladığı bilgi değişim olanakları nedeniyle solucanların programlanmaları da giderek kolaylaştı. Bugün sıradan bir programcı, İnternet üzerinden topladığı yazılım bileşenlerini ekleyerek kendi solucanını hazırlayabilir ve çok sayıda bilgisayarın denetimini ele geçirebilir.

E-posta aracılığı ile bulaşan Melissa, web sunucu zafiyetleri ile bulaşan Code Red gibi solucanların yerini birden fazla farklı saldırı yöntemine ilişkin bilgisi olan ve bu yöntemlerin tümünü deneyebilen yeni nesil solucanlar aldı. Örneğin Nimda solucanı [4] e-posta eklentileri olarak kendisini adres defterindeki tüm kullanıcılara göndermek, bilgisayarlar arası klasör paylaşımlarını aramak ve paylaşımlar aracılığı ile yayılmak, web sunucularına Code Red ile aynı biçimde saldırmak ve hatta web sayfalarına bulaşarak Internet Explorer ile web sitesini ziyaret eden kullanıcıların bilgisayarlarına sızmaya çalışmak biçiminde listelenebilecek dört farklı teknikten faydalandı.



Solucanları daha da korkutucu kılan, saldırı tekniklerine etkinliklerine paralel biçimde gelişen yayılma hızlarıdır. Bu yıl içerisinde e-posta mesajları ile yayılan Sobig.F solucanı yayılma hızı rekorları kırdı. Sobig.F'in etkin olduğu dönemde, Amerikan internet servis sağlayıcılarından AOL, kendi ağı üzerinden aktarılan 40.5 milyon mesajın yarısından fazlasının bu solucanı barındırdığını duyurdu [5].

Bir solucanı kim programlamak ister ya da diğer bir deyişle bir solucan kimin ne işine yarar? Meraklı bir programcı yalnızca "yapabildiğini görmek" ve kendisini tatmin etmek için bir solucan programı yazabilir. Uygunsuz reklam e-postaları (spam) göndermek isteyen birisi çok sayıda bilgisayarı ele geçirmek ve bu bilgisayarların üzerinden reklam mesajlarını dağıtmak isteyebilir. Yasadışı bir örgüt, İnternet'teki web sunucuları ele geçirip yayınlanan web sayfaları üzerine kendi sanal pankartlarını asmak isteyebilir. Bir terör örgütü, eylemlerine hedef seçtiği bir kuruluşun ve hatta ülkenin tüm bilgisayar sistemlerini çalışmaz duruma getirmek isteyebilir. Bir istihbarat teşkilatı, solucan aracılığı ile, ele geçirdiği tüm bilgisayarların disklerini ve ağ iletişimlerini gözleyerek belirli niteliklere uyan durumlarda ilgili dosyayı ya da ağ iletişimini kendi merkezine kopyalayabilir ve istihbarat ağını bu biçimde güçlendirebilir. Devletler, savaş durumunda, bir diğer devlete ait tüm bilgisayar sistemlerini çökertebilir ya da tüm ağ iletişimini durdurabilir.

İnternet üzerine bırakılan solucanların yayılma stratejileri ve hızları konusundaki güncel araştırmalar, önceki paragrafta özetlenen senaryoların ne kadar kolaylıkla gerçekleştirilebilir olduğunu da göstermesi açısından önemlidir. On birinci USENIX Güvenlik Sempozyumu'nda Staniford, Paxon ve Weaver "Boş zamanlarınızda İnternet'i nasıl ele geçirebilirsiniz" başlıklı bildirilerinde [6] son derece yavaş hareket eden ve böylece fark edilmeyecek bir solucan programı ile 10 milyon bilgisayar sisteminin nasıl ele geçirilebileceğine ilişkin analizlerini sundular. Weaver'ın [7] ve daha sonra Staniford ve arkadaşlarının [8] yaptığı çalışmalar ise bir solucanın elindeki araç kümesi ile İnternet'te sızabildiği tüm bilgisayarlara otuz saniyelik bir sürenin içerisinde yerleşebileceğini göstermektedir.

Bir solucan bilgisayarlara nasıl sızabilir? Bu sorunun yanıtı "bir bilgisayar korsanı bilgisayarlara nasıl sızabilir?" sorusunun yanıtından farklı değildir. Her iki durumda da, saldırıya hedef olan bilgisayar ya da bu bilgisayarın kullanıcısının bir zafiyetinden faydalanılmaktadır. Bilgisayar yazılımlarının hatalarından, programların geliştiricileri tarafından programların içerisi-

ne yerleştirilmiş arka kapılardan, ön-tanımlı ayarlardan ve kullanıcı hatalarından kaynaklanabilecek güvenlik problemleri bir saldırgan tarafından da, bir solucan tarafından da aynı biçimde kötüye kullanılabilir.

Kişisel bilgisayar sistemlerini solucan saldırılarından korumak için genellikle dört ana alanda çalışmaların yapılması önerilmektedir. En temel çalışma alanı, bilgisayarlar üzerinde çalışan işletim sistemlerini ve sistem yazılımlarını güncel tutmaktır. Pek çok saldırı, bu yazılımlardaki hatalardan kaynaklanan zafiyetlere yöneliktir ve güncellenen sistemler ile bu saldırıları bertaraf etmek mümkündür. Microsoft Windows kullanıcıları, firma tarafından sağlanan otomatik güncelleme hizmetinden [11] faydalanabilirler.

Kişisel bilgisayar korumasına yönelik ikinci ana çalışma alanı, e-posta istemcisinin ayarlarını düzenleyerek güvenlik ayarlarını gerçekleştirmektir. Pek çok modern solucan kendisini e-posta mesajları ile çoğaltmaya çalışmaktadır. Ayarları doğru yapılandırılmış bir e-posta istemcisi ile bu türden saldırılara karşı konulması mümkündür; elektronik postalarına Outlook ile erişenler SecurityFocus sitesinde yayınlanan [9] ve [10] belgelerinden faydalanabilirler.

Kişisel bilgisayarlar üzerinde antivirüs yazılımlarının kullanılması solucanlara karşı korunma konusunda faydalanılabilecek önemli bir diğer temel savunma uygulamasıdır. Modern solucanların çok hızlı bir biçimde yayıldığına ve ileride daha da hızlı yayılmalarının beklendiğine önceki paragraflarda değinilmişti. Anti-virüs yazılımlarının günde bir ya da iki düzeyindeki güncelleme sıklıkları da öngörüldüğünde, birden fazla farklı anti-virüs yazılımının bir arada çalıştırılmasının da savunmaya katkısı olduğu önerilebilir. İki geleneksel ve bir sezgisel anti-virüs motorunu tek bir yazılım içerisinde sunan F-Secure firmasının anti-virüs ürünleri [12] şimdilik bu kategoride sunulan tek ürün ailesidir.

Kişisel bilgisayar savunmasına ilişkin dördüncü ve son temel çalışma alanı, kişisel güvenlik duvarı yazılımlarının kullanılmasıdır. Kişisel bir güvenlik duvarı kullanılması ile bilgisayara ağ üzerinden gelen bağlantılar engellenebilir ve bilgisayardan ağa doğru yapılan bağlantılar kısıtlanabilir. İlk modeldeki uygulama solucanların bilgisayara sızmasını, ikinci modeldeki uygulama ise solucanın bilgisayara sızması durumunda başka bilgisayarlara doğru yayılmasını engellemek üzere kullanılabilir. Pek çok modern anti-virüs yazılımı, kişisel güvenlik duvarı bileşeni ile birlikte dağıtılmaktadır. Böylesi bir kombine paket ya da işletim sistemi tarafından sağlanan güvenlik duvarı işlevselliği bu amaca yönelik olarak önerilmektedir. Microsoft Windows kullanıcıları yeni nesil Windows'lar ile birlikte sağlanan "Internet Connection Firewall" yazılımından da faydalanabilirler.

REFERANSLAR

[1] Eeye Digital Security, ".ida" `Code Red' Worm, http://www.eeye.com/html/Research/Advisories/AL2001-0717.html.

[2] Mark Eichin and Jon A. Rochlis, `With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988, http://www.mit.edu/people/eichin/virus/main.html

[3] D. Moore and C. Shannon, The Spread of the Code-Red Worm, http://www.caida.org/analysis/security/code-red/coderedv2_analysis.xml.

[4] E. J. Aronne, The Nimda Worm: An Overview, http://www.sans.org/rr/papers/index.php?id=95.

[5] Bill Tucker, SoBig.F breaks virus speed records, http://www.cnn.com/2003/TECH/internet/08/21/sobig.virus/.

[6] S. Staniford, V. Paxson and N. Weaver, How to 0wn The Internet in Your Spare Time, http://www.cs.berkeley.edu/~nweaver/cdc.web/index.html

[7] N. Weaver, Warhol Worms: The Potential for Very Fast Internet Plagues, http://www.cs.berkeley.edu/~nweaver/warhol.html

[8] S. Staniford, G. Grim, R. Jonkman, Flash Worms: Thirty Seconds to Infect the Internet, http://www.silicondefense.com/flash/

[9] S. Granneman, Securing Outlook, Part One: Initial Configuration, http://www.securityfocus.com/infocus/1648

[10] S. Granneman, Securing Outlook, Part Two: Many Choices to Make, http://www.securityfocus.com/infocus/1652

[11] Microsoft Windows Update, http://windowsupdate.microsoft.com/

[12] F-Secure Corporation, http://www.f-secure.com