BİR WORM'UN ANATOMİSİ

Gökhan AKIN* , Asım GÜNEŞ *

(*) İstanbul Teknik Üniversitesi, Bilgi İşlem Daire Başkanlığı, 34360, İSTANBUL
gokhan.akin@itu.edu.tr, asim.gunes@itu.edu.tr

ÖZET

İstanbul Teknik Üniversitesi Ağında tespit edilmiş bir wormun çalışma mekanizması anlatılmaktadır. Ayrıca aynı mekanizma kullanılarak worm bulaşmış bir bilgisayarın nasıl tespit edilebileceği de anlatılmaktadır.
Anahtar Kelimeler: Worm, Exploit, DoS

ANATOMY OF A WORM

ABSTRACT

Working mechanism of a worm, this was found out in Istanbul Technical University Network, was explained. Also how to detect the worm inflected pc with using the same mechanism was explained.

Keywords: Worm, Exploit, DoS

1. GİRİŞ

Son yıllarda klasik virüs yazılımları yerlerini direk ağ erişimi üzerinden veya eposta ile kendini bulaştırarak çoğalan worm yazılımlarına bırakmıştır. Wormların yarattığı istek dışı trafik özellikle kampüs ağları olmak üzere bütün internet alt yapısında ciddi bir bant genişliğini israf etmektedir. Bu sebeplerden dolayı bu çalışmada ağ tabanlı kendini bulaştıran bir wormun çalışma sistemi incelenecek ve buna karşı çözümler aranacaktır.

2. WORMLAR

Worm kendini ağ üzerinden direk erişim veya e-postalar ile kendisini başka bilgisayarlara kopyalayıp bulaştığı yeni bilgisayarda kendisini aktive eden yazılımlardır. Kendisini başka sistemlere kopyalamasının yanı sıra wormlar yazılma amacına göre uzaktaki bir bilgisayardan emir alabilmekte veya bilgi sızdırabilmektedirler. Buradan da anlaşılacağı üzere bazı wormlar aynı zamanda trojen (Truva Atı) işlevini de taşıyabilmektedir. Trojen yazılımlar bir bilgisayarın ağ üzerindeki başka bir bilgisayar tarafından yönetilmesini sağlayan yazılımlardır. Trojenler, cd-rom cihazının kapağını açmak gibi masum işlemler yapabileceği gibi, online-bankacılık şifrelerinin çalınmasına veya başka bir bilgisayara DoS atak yapmasına da sebep olabilirler.

Wormlar bulaştığı bilgisayara zarar vermesinin yanı sıra kendini bulaştırmak için yarattıkları trafik ile de bant genişliğinin israfına ve bütün ağ kullanıcılarının erişim kalitesinin düşmesine sebep olmaktadırlar. Ayrıca ağ cihazlarında gereksiz işlemci yüküne, daha da kötüsü toplu bir DoS atağı yapmaları durumunda bütün altyapıyı felç de edebilmektedirler.

Bu bildiride incelediğimiz worm türü kendisini ağ erişimi sayesinde başka bilgisayarlara bulaştıran bir wormdur. Bu tür wormlar kendisini bulaştırmak için hedef bilgisayarlardaki güvenlik açığını değerlendiren exploitlerden yaralanmaktadırlar.

3. EXPLOITLER

İşletim sistemlerinin çok kullanıcılı olmasından sonra kullanıcılar arasında farklı yetkilendirme seviyeleri oluşturulmuştur. Bu seviyelendirme ile en yüksek yetkili kullanıcıya o bilgisayar ile ilgili bütün işlemleri yapabilme yetkisi verilmiştir. (Linux'de root kullanıcısı , Windows'da

administrator kullanıcısı gibi) Diğer kullanıcılara ise sadece o kullanıcının sistemde ihtiyacı olan yetkiler verilmiştir. Zaman içinde yönetici yetkisi olmadığı halde o yetkileri elde etmek amacı ile exploit adı verilen sistemin zaaflarından yararlanan programlar yazılmıştır. Exploitler direk bu sistem üzerinde çalıştırılan dahili yazılımlar olabileceği gibi, ağ üzerindeki harici bir kaynaktan kullanılabilecek programlar olabilirler.

Hemen hemen her işletim sistemi için (Windows, Linux, FreeBSD, MacOS ..vs için) exploit yazılmıştır. Exploit işletim sisteminin genel mimarisindeki bir açıktan yararlanabileceği gibi, işletim sisteminin üzerine kurulmuş bir yazılımda bulunan bir açıktanda yaralanabilirler.

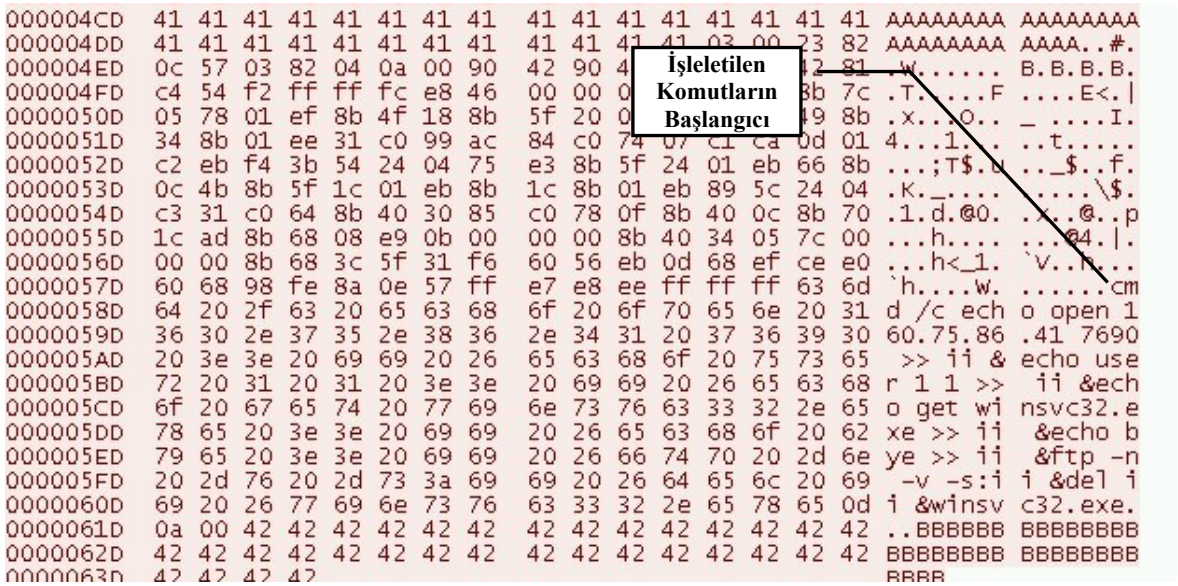
İstanbul Teknik Üniversitesi ağ altyapısında Windows bilgisayarlar çoğunlukta olduğu için bildiri kapsamında Windows 2000/XP işletim sistemine bulaşan bir exploit incelenmiştir.

4. WORMUN TESPİTİ

Wormların nasıl dağıldığı ve neler yaptığı teoride bilinse bile gereksiz trafik yayan bu yazılımların tam işleyiş prosedürünü incelemek amacı ile gereken güvenlik yamaları yapılmayan bir bilgisayar ağa dahil edilmiştir. Ağ erişimine takıldığı ilk andan itibaren bilgisayara gelen ve bilgisayardan giden bütün trafik bir izleme yazılımı ile kaydedilmiştir. Bir süre sonra bilgisayarın ITU/NET IP adresi aralığına anlamsız bir şekilde paketler yaymaya başlamasını gözlemledikten sonra bilgisayarın ağ erişimi kesilip bütün giren ve çıkan paketler incelenmiştir.

5. WORMUN İZLEDİĞİ YOL

Worm'un Windows XP işletim sistemindeki 445. porttan çalışan SMB hizmetine saldırdığı gözlemlenmiştir. Worm SMB hizmetinde bulunan buffer over flow açığını kullanarak hedef makinede bazı komutlar çalıştırmıştır. [1] (Resim 1)



Resim 1. Worm'un Kendi Bulaştırma Kısmı

Wormun exploitten yararlanarak işlettiği komutlar Sırası ile:

1- cmd /c: Peşinden gelen dizini komut satırında çalıştır ve daha sonra pencereyi kapat.

2- Aşağıda belirtilmiş satırları sırası ile ii isimli yeni oluşturulan dosyanın içine yaz.

- echo open 160.75.200.200 7690 >> ii
- echo user 1 1 >> ii
- echo get winsvc32.exe >> ii
- echo bye >> ii

3- ftp -n -v -s:ii : ftp programını aşağıda detayları verilmiş parametreler ile aç.

"-n": Otomatik kullanıcı adı şifre sorma kısmını atla.

"-v": Bağlanılan sunucunun yolladığı yazıları atla.

"-s ii" : "ii" isimli dosyadaki komutları çalıştır. Yani 160.75.200.200 isimli sunucunun

7690inci portuna bağlan, kullanıcı adı şifre olarak 1 ve 1 ver. Winsvc32.exe isimli dosyayı ftp sunucusunda idir ve ftp programını kapat.
4- del ii : Ftp erisimde kullanılanı ii isimli dosyayı sil.
5- winsvc32.exe : Wormu çalıştır.
Wormun programcısı saldırılan makinedeki ftp yazılımını kullanarak kendini o makineye kopyalama üzerine bir sistem oluşturmuştur. Bu amaçla önce "ii" isminde bir dosyanın içinde ftp yazılımında çalıştıracağı bütün komutları yazdırmış daha sonrada ftp programın açtırıp bu satırları işlettirmektedir. Bunu sonucu kendisini yani "winsvc32.exe" dosyasını kopyalatmış ve kendini çalıştırmıştır. Son olaraktan ftp erişiminde kullandığı "ii" isimli dosyayı da silmiştir.

Gerçekten bağladığı ftp sunucusun çalışıp çalışmadığını anlamak için 7690inci portuna aynı kullanıcı adı ile wormu içeren bilgisayara bağlanılıp winsvc32.exe dosyasının var olduğunu tespit edilmiştir. Dosyayı indirilmesi ile beraber Norton Antivirus yazılımı bu dosyanın "W32.Spybot.Worm" isimli worm olduğunu ve 16 Nisan 2003'ten beri var olan bir worm'un türevi oluğunu belirtmiştir.[2]

Bu bilgi ışığında yapılan incelemede benzer wormların kendileri kopyalamak için ftp istemci yazılının yanı sıra tftp ve telnet gibi araçları da kullandığı tespit edilmiştir.

Worm yeni bilgisayarda aktif hale geldikten sonra sutt.p0rr.org isimli siteye 7475 numaralı porttan bağlantı kurmuştur. Bağlantı sonrası sunucu ile irc haberleşmesine benzer bir haberleşme yapmaktadır. Emin olmak için aynı sunucuya bir irc istemci ile bağlanılmış gerçektende irc sunucusu olduğu tespit edilmiştir. (Resim 2)
Wormlu bilgisayar irc sunucusunda "PRIVMSG #renats :[SCAN]: Random Port Scan started on 160.75.x.x:2967 with a delay of 5 seconds for 0 minutes using 99 threads." şeklinde bir mesaj yollamış ve daha sonra bağlantıyı erişimi sonlandırmıştır. Hemen peşine 160.75.0.0 B sınıfı İTÜ/NET IP aralığına daki PC'lere raslansal bir şekilde 2967 portlarından SYN atak yapmaya başlamıştır. Buradan da anlaşıldığı üzere üzerinde çalıştığımız worm dışarıdaki bir sisteme bilgi sızdırabileceği gibi dışarıdaki bir sistemden emir alabilmektedir, yani aynı zamanda trojen karakteristiği göstermektedir.

Resim 2. Wormun Bağladığı IRC Sunucusu

6. WORMA KARŞI ÇÖZÜM

Worm yazılımlarının kullandığı aynı exploit kullanılarak bazı çözümler üretilebilir.

Bunlar güvelik açığına sahip bilgisayarlarının belirlenmesi, kullanıcı bilgisayarında bir uyarı mesajı çıkartılması ve hatta açık bulunan bilgisayarlara kullanıcının haberi

olmadan güvenlik yamasının yapılması olabilir. Bu amaçla İTÜ Bilgi İşlem Daire Başkanlığı dahilinde Karga isimli bir yazılım geliştirilmiştir. Programın ismi Worm yani Solucan yazılımlara karşı yazılmış bir program olmasından dolayı bu şekilde verilmiştir. Karga V1.0 ile güvenlik açığı bulunan bilgisayara sahipleri uzaktan uyarılabilmekte ve açık bulunan bilgisayarların listesi çıkartılabilinmektedir. Şu anda sadece bu makale kapsamında bulunan worm'a karşı yazılmakta olup gelecekte modüler bir yapıya kavuşturulup daha çok güvenlik açığını kapsaması planlanmaktadır.

7. SONUÇ

Worm yazılımları içerilerinde kendilerini klonlamak amacı temel bir ftp, tftp veya web sunucu barındırmaktadırlar. Ayrıca irc benzeri uzaktaki bir kaynak ile veri haberleşmesi yapabilecekleri bir istemci yazılımı da barındırmaktadırlar. Bu sayede kullanıcıdan istenilen her bilgi sızdırılabilinmektedir. Bunun yanı sıra uzaktan wormlu bilgisayara istenilen her türlü emirde verilebilir hale gelmiştir. Bu sayesinde yüzlerce pcden oluşan bir DoS atak ordusu oluşturulabilir.

En kötüsü bir kere programlanmış bir worm daha sonra kodunda yapılacak çok küçük bir müdahale ile yeni exploitler için revize edilip tekrar tehdidini sürdürmeye devam etmektedir.

Wormlar ile sebep olunan durumda ciddi bir ulusal güvenlik sorunu oluşturmaktadır. Wormlu veya güvenlik açığı bulunan bilgisayarların tek tek tespiti yerine aynı exploitin kullanıcının uyarılması için kullanılması durumunda wormun ağdan temizlenme süresini çok kısaltmaktadır. Ancak bunun için sürekli yeni çıkan güvenlik açıkları takip edilmeli ve bir kütüphane oluşturulmalıdır. Bu amaç A.B.D.'de Ulusal CERT kurumlarının sponsorluğu ile Ulusal Güvenlik Açıkları Veritabanı oluşturulmuştur.[3] (National Vulnerability Database) Yeni güvenlik açıklarının ortaya çıkması ile yeni wormların çıkması sürekli devam edeceğinden kullanıcıları bu türden ulusal bir veritabanı oluşturacak bir birim oluşturulması ve kullanıcıları uyaracak bu türden yazılımlarda paralelinde geliştirilmesi çok faydalı olacaktır.

8. KAYNAKLAR

[1]. Microsoft Security Bulletin MS03-049, http://www.microsoft.com/technet/security/bulletin/MS03-049.mspx , Microsoft Corp.

[2]. W32.Spybot.Worm, http://www.symantec.com/security_response/writeup.jsp?docid=2003-053013-5943-99&tabid=1 , Symantec Corp.

[3]. National Vulnerability Database, http://nvd.nist.gov/ , National Institute of Standards and Technology