Internet Solucanları

Bilgi otoyolu olarak adlandırdığımız Internet ortamında, geçen her zaman zarfında bilgiler bir sistemden başka bir sisteme akıp gitmektedir. Buna paralel olarak bu otoyolda ilerleyen bilgilerin meraklıları da gitgide artmaktadır. Hal böyle olunca zaman zaman bu otoyol tıkanmaktadır. Öyle ki, bazen bu bilgilerin bize gerçekten arkadaşımız tarafından gönderilip gönderilmediğini anlayamayabiliriz. Bu bilgi karmaşasında insanların sistemlerine etki etmeyi çok seven küçük afacanları hiçbir zaman göz ardı etmemek gerekir. Bu küçük afacanlardan kastımız İnternet Kurtları, diğer bir adıyla İnternet Solucanları.

Bu küçük afacanlar kendisinden istenen işlemleri, yapısında belirtilen koşullarla karşılaştığında birer birer gerçekleştirir. Her bir solucan, kendisini yazanın düşüncesini yansıtır. Kimi solucan ziyaret ettiği sistemdeki şifreleri, kredi kart numaralarını yapımcısının posta adresine gönderir, kimi ise İnterneti olabildiğince yavaşlatmayı çalışır. Bilgisayar dünyasında, son zamanlarda dosyalara bulaşan virüslerden ziyade İnternet Solucanları popülaritesini arttırmıştır. Solucanların virüslerden farkı, kendilerini çoğaltarak sisteme yaymalarıdır. Solucanların en etkilileri genellikle yazılım zaaflarından yararlanarak yayılanlarıdır ki solucanların bu türleri çok kişiyi zor durumda bırakır(CodeRed, Nimda, LovSan/MSBlast).

Günden güne dosya paylaşım(P2P) araçlarının(Gnutella, eDonkey, Kazaa…) kullanımının artması solucan yazarlarının ilgisinin bu yöne artmasına neden olmuştur. Örneğin; Backdoor.k0wbot adıyla bilinen bir solucan Kazaa platformunu hedef alır. Solucan, saldırgana kullanıcıyla aynı hak ve öncelikleri veren Trojan'ı PC'ye yüklenmesini sağlar. Bu tür araçları kullanarak yayılan solucanlara ilişkin haberleri çeşitli Antivirüs ve güvenlik sitelerinden duymaktayız. Buna ilaveten IRC(Internet Relay Chat) ortamlarında bulunan kullanıcıları tehdit eden solucanlarında yayılma oranı da artmıştır. Zira IRC solucanlarının çoğu IRC yazılımlarının kendi bünyesinde bulunan dosyalarına komut ekleyerek(script.ini) yayılmakta idi (geçerliliğini korumaktadır fakat IRC yazılımlarının kendini geliştirmesi ve özellikle Antivirus yazılımları kolaylıkla bu tür yayılan solucanları tespit edebilmektedir). Solucan türlerinden bazıları yukarıda saydığımız yayılma olasılıklarının tümünü bünyesinde barındırmaktadır yani dosya paylaşım araçlarını kullanan, maille yayılan, IRC ortamını da kullanan solucan türleri de bulunmaktadır. Amaç, bir sistemi etkiledikten sonra bu etkilediği sistem vasıtasıyla diğer sistemlere de kendisini kopyalamak. Böylece ağınızdaki bir sisteme entegre olan solucan, kendisini ağınızdaki diğer sistemlere kopyalamaya çalışır. Nimda, kendisini yaymak için kullandığı taktiklerden bir tanesi Microsoft IIS hizmetini kullanan sunucuları bulup, bünyesinde barındırdığı IIS açığını kullanarak sistemi etkiler.

Bu örnekte olduğu gibi yazılım açıkları yayınlandıktan sonra bu açıkları kullanan solucanın sistemleri etkilemesi an meselesidir(Son örneklerden biri MSBlast). Sonucunda tüm bunlardan etkilenen yine kullanıcılar olmaktadır. Kullanıcılar, kendisine gelen bir maili açtıklarında dahi solucanlar bu kullanıcıyı etkilemektedir. Kullanıcının tek suçu güvendiği kimseden geldiğini sandığı maili açmasıdır. An gelir ki kendisine bir solucanın etki ettiğini bile anlayamadan olanlar olur. Solucan içerikli bir mailin okunması bile ağdaki diğer makinelerin güvenliğini tehlikeye düşürmektedir.

Maille yayılma yöntemlerinden biri ve en popüler olanı Outlook adres defterinde yer alan kullanıcıların bir kısmına yada tamamına e-posta gönderme şeklidir. Fakat son günlerde solucanlar mail motorunu kendi bünyesinde barındırmaya başladı. Çünkü herhangi bir e-posta aracına gerek kalmadan kendisini göndermeyi başarabilmektedir. Solucan yazarları sosyal mühendislik kavramını kullanmaktadırlar.

Bu metotlardan biri solucanı taşıyan e-posta mesajına ilginç ve dikkat çekici bir konu satırı yazmaktır. Örneğin, ünlü bir kişilerin resimlerinin bulunduğunu iddia ettiği dosyalar, virüs temizleme programları gibi görünen mesajlar... Amaç kullanıcının merakla e-postasını açıp, solucanın yayılmasını sağlamaktır. Özellikle Kazaa gibi dosya paylaşım araçlarını kullanan solucanlarının çoğunun başvurduğu yöntem bazı dosya uzantılarını (.mp3, .gif, .jpg) değiştirmek ve insanların bu ortamda arayabileceği dosya adları şeklinde çoğalmaktır.

Bu solucanlar öncelikle sistemde paylaşım programlarının paylaştırma dizinlerini ararlar. Arayacağı dizinler, örneğin şu şekilde olabilir:

```
C:\ Program Files\KMD\My Shared Folder
C:\ Program Files\Kazaa\My Shared Folder
C:\ Program Files\Morpheus\My Shared Folder
C:\ Program Files\BearShare\Shared
C:\ Program Files\Kazaa Lite\My Shared Folder
...
```

gibi.

Buldukları dizinler içine aranabilecek dosya adları şeklinde kendini çoğaltırlar. Dosya paylaşım kurtları için kullanılan kendisi çoğaltma kodu genellikle şu şekildedir (VBScript):

```
Set fso=Create Object("scripting.filesystemobject")
Solucan=(wscript.scritptfullname)
Kaza=("C:\ Program Files\Kazaa\My shared Folder") & "\"
If fso.folderexists(Kaza) then
Fso.copyfile solucan, kaza & "ICQ_HACK.exe.vbs"
Fso.copyfile solucan, kaza & "Muzik.mp3.vbs"
Fso.copyfile solucan, kaza & "Hotmail-Hack.exe.vbs"
Fso.copyfile solucan, kaza & "Kernel-Exploit.exe.vbs"
...
```

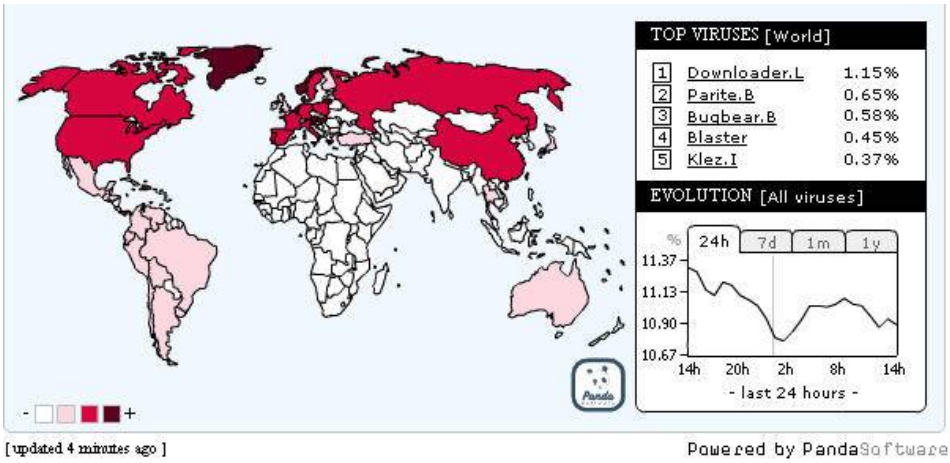
Yukarıdaki kod Kazaa dosya paylaşım dizinine belirtilen dosya olarak kopyalayacaktır.

P2P kurtlarının çoğalma mantığı az-çok bu şekildedir. Aynı şekilde Visual Basic ile yazılan bir kurdun(P2P Solucanı) yayılma mantığı ise şu şekildedir:

```
...
Set obje=CreateObject("Wscript.Shell")
Dizinler=obje.regread("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ProgramFilesDir")
Programlar=Array(Dizinler & "\Kazaa\My Shared Folder\",dizinler & "\Morpheus\My Shared Folder\")
Dosyalar=Array("Yahoo User Hack.exe","Flooder.exe","GTA Trainers.exe")
For Each program In programlar
...
FileCopy yollar,program & file
...
...
```

Yukarıdaki kod ise Dosyalar bölümünde belirtilen dosya adlarıyla kendini programlar bölümünde belirtilen yollara kopyalayacaktır. Solucanlar sisteme bulaşmadan önce uyguladığı bir diğer taktik ise sisteme kurulu olan Antivirus ve Firewall uygulamalarını kapatma işlemidir. Bir kullanıcı durduk yere Antivirus ve Firewall uygulaması kapandığını görüyorsa bazı durumlardan şüphelenmesi gerekir. Güncel solucanlar artık kullanıcıların sistemlerini potansiyel birer posta merkezi olarak görmektedir.

Yeni yayılan solucanların bir çoğunda mail motorları bünyesinde olduğundan herhangi bir posta gönderme aracına ihtiyaç duymamaktadır. Neticesinde kendisini göndermek için solucanın ihtiyaç duyacağı sadece bir başka e-posta adresidir. Bu ihtiyacını da yine sistemde bulunan dosyaları analiz ederek karşılar. Sistemdeki bazı dosya uzantılarına -*.htm, *.htm, *.dbx, *.wab, *.eml, *.txt, ...- sahip dosya içinden e-posta adreslerini alarak kendisini yollayabilmektedir. Bunu yapabilen en son örneklerinden biri Sobig.F'dir. Sobig.F'nin entegre olduğu sistemler teker teker -spam- makinesine dönüştüğü ve çok hızlı yayıldığı belirtilmişti. SoBig'in yayılması için sistemde herhangi bir açık olmasına gerek yoktur. Sisteme tüm yamalar kurulsa bile e-posta yoluyla sisteme SoBig sızabiliyordu. Bu da solucanların tehlike boyutlarını bize gösteriyor. Düşündüğümüzde bulaşma oranı en yüksek virus ve solucanlarının hedefinin Microsoft Windows işletim sistemi kullanıcıları olduğunu görüyoruz. Bunlara bilinen son örnekleri Mimail.M ve MSBlast/LovSan söyleyebiliriz. Antivirüs uzmanlarınca Virüs/Solucanların yayılma oranının genellikle Uzakdoğu ve Avrupada daha fazla olduğunu belirtmektedirler.



Bu son günlerde ortaya çıkan solucanların temel hedefi nedir? Kendilerini nereye ve nasıl kopyalamaktadırlar?

W32/Mimail.M

Mimail.M bulunduğu sistemden arakladığı e-posta adreslerine kendisinin bir kopyasını göndererek yayılmaya başlar. Virüs kendi mail motorunu barındırır. Mesaj içeriği:

Hello Greg,
I was shocked, when I found out that it wasn't you but your twin brother!!!
....

şeklindedir. Ayrıca bazı hostlara DoS saldırısı gerçekleştirmektedir. Saldırmak istediği hostlar kodu analiz edildiğinde açıkça görülmektedir.

```
00401979 r$ 55            PUSH EBP
0040197A .  89E5          MOV EBP,ESP
0040197C .  81EC 00010000 SUB ESP,100
00401982 .  57            PUSH EDI
00401983 .  833D D81E4700 CMP DWORD PTR DS:[471ED8],0
0040198A .v75 19          JNZ SHORT WENDY.004019A5
0040198C .  68 FF000000   PUSH 0FF                          r max len = FF (255.)
00401991 .  68 FE2D4700   PUSH WENDY.00472DFE               L src = "darkprofits.com"
00401996 .  8DBD 00FFFFFF LEA EDI,DWORD PTR SS:[EBP-100]
0040199C .  57            PUSH EDI                          r dest
0040199D .  E8 6E2E0000   CALL <JMP.&CRTDLL.strncpy>        L strncpy
004019A2 .  83C4 0C       ADD ESP,0C
004019A5 >  833D D81E4700 CMP DWORD PTR DS:[471ED8],1
004019AC .v75 19          JNZ SHORT WENDY.004019C7
004019AE .  68 FF000000   PUSH 0FF                          r max len = FF (255.)
004019B3 .  68 EE2D4700   PUSH WENDY.00472DEE               L src = "darkprofits.net"
004019B8 .  8DBD 00FFFFFF LEA EDI,DWORD PTR SS:[EBP-100]
004019BE .  57            PUSH EDI                          r dest
004019BF .  E8 4C2E0000   CALL <JMP.&CRTDLL.strncpy>        L strncpy
004019C4 .  83C4 0C       ADD ESP,0C
004019C7 >  833D D81E4700 CMP DWORD PTR DS:[471ED8],2
004019CE .v75 19          JNZ SHORT WENDY.004019E9
004019D0 .  68 FF000000   PUSH 0FF                          r max len = FF (255.)
004019D5 .  68 DF2D4700   PUSH WENDY.00472DDF               L src = "darkprofits.cc"
004019DA .  8DBD 00FFFFFF LEA EDI,DWORD PTR SS:[EBP-100]
004019E0 .  57            PUSH EDI                          r dest
004019E1 .  E8 2A2E0000   CALL <JMP.&CRTDLL.strncpy>        L strncpy
004019E6 .  83C4 0C       ADD ESP,0C
004019E9 >  833D D81E4700 CMP DWORD PTR DS:[471ED8],3
004019F0 .v75 19          JNZ SHORT WENDY.00401A0B
004019F2 .  68 FF000000   PUSH 0FF                          r max len = FF (255.)
004019F7 .  68 D02D4700   PUSH WENDY.00472DD0               L src = "darkprofits.ws"
004019FC .  8DBD 00FFFFFF LEA EDI,DWORD PTR SS:[EBP-100]
00401A02 .  57            PUSH EDI                          r dest
00401A03 .  E8 082E0000   CALL <JMP.&CRTDLL.strncpy>        L strncpy
00401A08 .  83C4 0C       ADD ESP,0C
00401A0B >  E8 49FFFFFF   CALL WENDY.00401959
00401A10 .  83F8 00       CMP EAX,0
00401A13 .v75 10          JNZ SHORT WENDY.00401A25
00401A15 .  68 CB2D4700   PUSH WENDY.00472DCB               r src = "www."
00401A1A .  FF75 08       PUSH DWORD PTR SS:[EBP+8]         r dest
00401A1D .  E8 BE2D0000   CALL <JMP.&CRTDLL.strcpy>         L strcpy
00401A22 .  83C4 08       ADD ESP,8
```

Solucan, bilgisayar açıldığında otomatik çalışması için registry anahtarı yaratıyor:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "NetMon" = %WinDir%\netmon.exe

W32/Swen@MM

Antivirüs uygulamalarını Regedit uygulamasını kapatır. Kendisini e-posta yolu ile, Dosya paylaşım aracı olan Kazaa aracı ile kendisini paylaştırmaya ekleme ile, Ağ paylaşımı ile, IRC'den kendisini göndererek yayılır.

E-posta ile yayılmak için sistemdeki .html, .asp, .eml, .dbx, .wab, ve .mbx uzantılı dosyalardan e-posta adreslerini araklayarak kendisini bünyesinde barındırdığı mail motoru aracılığıyla gönderir. Solucan analiz edildiğinde sistemden hangi dosyalarda e-posta adreslerini araklamaya çalışıldığı anlaşılmaktadır.

```
004079B6 . 68 D41A4100
PUSH SHOWLETT.00411AD4 ; ASCII "ht"
....
004079CD . 68 D01A4100 PUSH SHOWLETT.00411AD0 ; ASCII "asp"
....
00407A0F > 68 C81A4100 PUSH SHOWLETT.00411AC8 ; ASCII ".mbx"
....
00407A20 . 68 C01A4100 PUSH SHOWLETT.00411AC0 ; ASCII ".dbx"
....
00407A31 . 68 B81A4100 PUSH SHOWLETT.00411AB8 ; ASCII ".wab"
....
00407A42 . 68 B01A4100 PUSH SHOWLETT.00411AB0 ; ASCII ".eml"
....
```

Solucan kendisini ağda bulduğu startup klasörlerine kopyalıyor. Dosya ismini rastgele yaratıyor. Ağ paylaşımlarında hedefteki klasörlerinden bazıları:

```
windows\all users\start menu\programs\startup
windows\start menu\programs\startup
...
winnt\profiles\default user\start menu\programs\startup
winnt\profiles\administrator\start menu\programs\startup
```

P2P üzerinden yayılmak için Solucan temp klasörü içinde rastgele isimde yaratılan bir klasöre kendi kopyalarını yerleştiriyor. Örneklerden bazı isimleri:

```
XboX Emulator
Yahoo Hacker
Hallucinogenic Screensaver
Emulator PS2
XP update
AOL hacker
....
```

W32/Blaster[LovSan]

W32/Blaster solucanı Microsoft'un DCOM RPC arabirimindeki bir zaaflıktan yararlanarak yayılmıştır. Lovsan olarak da adlandırılan solucan yamaları yüklenmemiş Microsoft Windows NT, Windows 2000, Windows XP ve Windows Server 2003 işletim sistemlerine tesir etmektedir.

Solucan, DCOM/RPC açığı için ağdaki diğer sistemleri tarıyor. Sistem tarihi 15 Ağustos olduğunda windowsupdate.com sitesine bir DoS atak gerçekleştirmektedir.

Solucanın otomatik çalışması için registry anahtarına;

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

"windows auto update"="msblast.exe"

değerini ekliyor.

Ayrıca solucan içerisinde Solucan'ın içerisinde aşağıdaki yazı bulunuyor (hiç görüntülenmiyor):

I just want to say LOVE YOU SAN!! billy gates why do you make this possible ? Stop making money and fix your software!!

W32.Wuno.Irc

Bu solucan mIRC kullanıcıları arasında yayılmıştır. Microsoft Visual Basic programlama dili ile yazılmıştır.

Kendisini sistemde Windows dizinine **WinUninst32.exe** ve **<rastgele dosya isimleri>.exe** olarak kopyalamaktadır.

Sistemde otomatik olarak çalışması için registry ayarlarında değişiklik yapar:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "WinUninst3" "C:\%Windir%\WinUninst32.exe"

Sistemde mIRC klasörlerini arayarak bulduğu mIRC klasörüne script.ini isimli dosya yaratarak bu dosyaya IRC üzerinden yayılmak için gerekli kodu ekler(mIRC.ini ile ayni yere dosyayı yaratır).

Kaynaklar

* http://www.olympos.org
* Windows & .Net Magazine 2003/1 Solucanlardan korunmanın 8 yolu [Sayfa 42]
* Byte 2003/7 PC & Internet Güvenliği [Sayfa 68]
* Byte 2002/11 Ağda son kullanıcı güvenliği [Sayfa 66]
* http://www.ntvmsnbc.com/news/246506.asp?0m=T24H&cp1;=1
* http://www.ntvmsnbc.com/news/229896.asp
* http://www.ebcvg.com
* http://www.pandasoftware.com
* http://www.megasecurity.org/Info/wormanalysis.htm
* http://home.t-online.de/home/Ollydbg

tacettink[at]olympos.org

[Aralık 2003]