





Internet Worms

Many Internet commentators have already earmarked 2004 as "The Year of the Worm". To date there has sadly been a plethora of Internet worms bombarding our firewalls, our inboxes and our patience. They Irish Honeynet Project has been investigating the impact of these worms for some time now and it is clear that many Internet users are vulnerable. With the increase in DSL broadband connections both at home and in the office the situation looks set to get worse.

A worm attack captured by the Honeynet Project in recent times is a good example of how exactly these worms work and gives us a good indication as to what can be done to prevent them. This month we will analyse a worm infection of a windows 98 home computer. If the google search engine's statistics are a good indicator of the prevalence of a given operating system almost one quarter, or 24%, of computers on the Internet are still running the Windows 98 operating System and many of these have a dedicated broadband Internet connection.

An external system scanned the honeynet looking for Window systems. It found our Windows 98 computer and began querying it. If first began by getting the system name and determined if sharing was enabled. Once it determined that sharing was enabled, it then probed for specific binaries on our system. Its goal was to determine if a specific worm was installed, and if not, then it would install itself. In this case, the specific worm was not installed. The worm is known as the "Win32.Bymer Worm". The purpose of this worm is to take advantage of your CPU cycles to help an individual win the distributed.net contest. Distributed.net is group that uses the idle process of distributed computers for various challenges (such as cracking RC5-64 challenge). People are awarded prizes if they crack the challenge. The more computers and CPU cycles you have under your control, the better of your chances of winning. In our case, someone "volunteered" us for the project by installing the worm on our system.

A virus writer created a self-replicating worm that would find vulnerable Window systems and install the distributed.net client on unsuspecting systems. Once installed and executed, the worm utilises your CPU cycles in attempt to help the author win the contest. Meanwhile the worm begins probing for other vulnerable systems it can take over. The goal is to have access to as many computers and CPU cycles as possible. This process grows exponentially as more systems are compromised. Lets take a look at the attack using packet captures of the network traffic (in this case, we used the IDS sniffer snort). Throughout the sniffer traces below, the system 172.16.1.105 is the IP address of the honeypot.

The worm begins by first checking to see if the file **dnetc.ini** is on the system. This is the standard configuration file for the distributed.net client. This configuration file tells the main server who should get credit for all the CPU cycles. This is also the person that most likely created the worm. Here we see the packet trace where the remote system copies the configuration file to our honeypot.

Below we see the actual file transfer of the configuration file dnetc.ini. Notice who is the point of contact for this, bymer@inec.kiev.ua. This is the individual that receives the credit for the CPU cycles, and most likely the author of the worm attacking us.

11/01-15:29:18.729337 xxx.xxx.92.10:2900 -> 172.16.1.105:139 TCP TTL:112 TOS:0x0 ID:50747 DF *****PA* Seq: 0x1293125 Ack: 0x66B70AD Win: 0x2140 00 00 01 11 FF 53 4D 42 0B 00 00 00 00 00 01 00SMB...... 00 00 02 D2 05 00 00 E1 00 00 00 00 00 E1 00 E4 00 01 E1 00 5B 6D 69 73 63 5D 20 0D 0A 70 72 6F[misc] ..pro 6A 65 63 74 2D 70 72 69 6F 72 69 74 79 3D 4F 47 ject-priority=OG 52 2C 52 43 35 2C 43 53 43 2C 44 45 53 0D 0A 0D R,RC5,CSC,DES... 0A 5B 70 61 72 61 6D 65 74 65 72 73 5D 0D 0A 69 .[parameters]..i 64 3D 62 79 6D 65 72 40 69 6E 65 63 2E 6B 69 65 d=bymer@inec.kie 76 2E 75 61 0D 0A 0D 0A 5B 72 63 35 5D 0D 0A 66 v.ua....[rc5]..f 65 74 63 68 2D 77 6F 72 6B 75 6E 69 74 2D 74 68 etch-workunit-th 72 65 73 68 6F 6C 64 3D 36 34 0D 0A 72 61 6E 64 reshold=64..rand 6F 6D 70 72 65 66 69 78 3D 32 31 37 0D 0A 0D 0A omprefix=217.... 5B 6F 67 72 5D 0D 0A 66 65 74 63 68 2D 77 6F 72 [ogr]..fetch-wor 6B 75 6E 69 74 2D 74 68 72 65 73 68 6F 6C 64 3D kunit-threshold= 31 36 0D 0A 0D 0A 5B 74 72 69 67 67 65 72 73 5D 16....[triggers] 0D 0A 72 65 73 74 61 72 74 2D 6F 6E 2D 63 6F 6E ..restart-on-con 66 69 67 2D 66 69 6C 65 2D 63 68 61 6E 67 65 3D fig-file-change= 79 65 73 0D 0A yes..

The next file to be transferred is the actual distributed.net client, dnetc.exe. This is a valid executable, it is not malicious in nature. We confirmed this by taking an MD5 signature of the client found on the honeypot. We then downloaded the client from distributed.net and took an MD5 hash of the dnetc.exe client. The MD5 hashes

were identical (d0fd1f93913af70178bff1a1953f5f7d), indicating that this code is not the worm. This is the binary that uses your CPU cycles as part of the distributed.net challenge. However, the worm intends on using this binary without your permission nor knowledge, all for the author's gain.

Next we see the actual worm being transferred, msi216.exe. This is the self-replicating worm that randomly probes for vulnerable systems and copies itself. This is the worm that is most likely causing a great number of the scans we are receiving.

Last, the worm first modifies then uploads a new win.ini file. The worm does this so the system will execute the worm upon reboot. Remember, it can be difficult to remotely execute a file on a Win98 system, so this is the worm's method of getting it executed. It does this by adding itself to the boot up configuration file c:\windows\win.ini and has itself loaded during the boot process. The new win.ini file is then uploaded to our compromised system.

65 3D 30 0D 0A 0D 0A 5B 69 6E 74 6C 5D 0D 0A 69 e=0....[intl]..i

That's it. The Worm is now complete and the honeypot has now been infected. All that needs to happen now is the system to reboot and the Worm will take effect. Once it takes effect, several things happen.

The distributed.net client begins, using the CPU cycles in the contest.

The Worm begins searching for other vulnerable systems to replicate itself to. This is what is causing all the UDP 137 and TCP 139 scans.

The worm may add the following keys to the registry.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersio n\Run\Bymer.scanner HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersio n\RunServices\Bymer.scanner

One may think that having to wait for a system to reboot is an unreliable way to execute. Keep in mind, the targets are Windows desktop systems. How often do you reboot your Windows desktop?

The Irish Honeynet, set up by Espion, Deloitte, and Data Electronics, operational since April 2002, is designed to mimic the Internet infrastructures commonly used by organisations, but it is 'wired' with detection sensors that capture all activity to and from the system. The Honeynet is not advertised in any way so any traffic to it from the Internet is suspicious by nature, as it arises from hackers and crackers who are deliberately attempting to identify and attack systems that are vulnerable.

For more information please send an email to <u>honeynet@espion.ie</u> or <u>honeynet@deloitte.ie</u>