Title: Internet Worms, and the Malicious URL feature
Document Number: CASE-261-001
Version: 1.1, September 19, 2001
OS Ver. this Paper Applies to: 2.6.1r2 and above
HW Platforms this Paper Applies to: All
Audience (Internal or External): External

Internet Worms and the Malicious URL feature

Introduction

Recently, several new types of Worms spread across the Internet. NetScreen takes customer network security seriously, and wants to ensure our customers are as secure as possible. This Whitepaper helps explain how these new Worms work, and what NetScreen customers can do to help minimize the impact of these Worms on their networks. Please also reference NetScreen's Whitepaper "Fundamentals of Secure Network Design (CASE-260-002)" for important additional information.

Concepts

Throughout this paper, terms and concepts common to network security professionals will be used. The following is a brief glossary of terms used, as well as other security terms and concepts you should be aware of.

Port Scanning – A technique for determining which ports a server is listening to. A port-scanning program will barrage a server with connection requests on a range or list of ports, and report back which ports the server responded on.

Worm – A self-replicating attack program. Worms differ from typical viruses in that they are completely automatic – no interaction with a user is required

Intrusion Detection System (NIDS) – A system that monitors all data flowing past its network interface, looking for hostile data patterns. A flexible IDS will have user-definable data patterns or "**Signatures**" which allow it to detect new types of attacks as they evolve. If a packet contains the same pattern as the signature, a warning or other action (such as blocking/dropping) would occur.

Details

As of the writing of this paper, four major worms have recently made a Network Security Administrator's job a little busier. All three use recent Internet Information Server™ (by Microsoft™) vulnerabilities for at least one vector of their attack strategy.

Code Red – First discovered in mid-July 2001, it would infect unpatched IIS servers via the ISAPI vulnerability. This worm would only attack Microsoft Windows NT or 2000 servers running IIS. The patch for this vulnerability was available June 2001. Code Red is a memory-resident (only) self-propagating worm which scans for targets for the first part of the month (days 1-19), and attacks (flood) an IP originally assigned to www.whitehouse.gov (198.137.240.91) near the end of the month (days 20-30), then will go inactive until the first of the next month. Since Code Red is memory-resident only, a reboot of the system

purges the infection. If the website was running the English (US) version of Windows NT/2000, it would divert traffic from the web page to a memory-resident web page that said “Hacked by Chinese”.

Code Red had a bug in the scanner section that made propagation inefficient – each instance would start scanning the same sequence of IP’s over again – thereby attempting re-infection of already compromised servers. Sysadmins with servers towards the beginning of the sequence found their servers flooded with incoming connections from the outside – all of them trying to re-infect their servers.

Code Red II – Appearing in early-August 2001, Code Red II uses the same infection vector as Code Red, but also installs a Trojan horse backdoor, replacing Internet Explorer (explorer.exe). This allows an attacker remote access to the system. Code Red II also solves the IP randomization/re-scan problem, and also adds a new code segment that makes it prefer local subnets for scanning. Other than these improvements, it otherwise behaves like its namesake – scanning from the 1st through the 19th, and attacking 198.137.240.91 from the 20th through the 30th of the month.

Code Blue – Debuting in early-September 2001, Code Blue is similar in propagation to Code Red variant, but it uses a different infection vector. It uses IIS Web Server Folder Traversal vulnerability, a patch has been available since October 2000. This worm, like Code Red and Code Red II, only attacks Microsoft Windows NT or 2000 servers running IIS. Code Blue is more subtle than Code Red; it has an extra algorithm to detect if a target is running IIS before it attempts the IIS exploit.

Unlike Code Red, Code Blue is not merely memory resident – it saves a copy of itself to the hard drive and configures the system to reload the virus upon reboot – a reboot will not purge the system. It also does not like Code Red – upon detection, it will actively remove either variant from memory, effectively un-infecting the system of Code Red. It has a local-subnet scanning algorithm like the improved Code Red II. At intervals, it will attack a Chinese security company website in a fashion similar to how the Code Red variants would attack the Whitehouse web site. There has been speculation that Code Blue was a misguided attempt to ‘inoculate’ systems against Code Red.

Nimda Concept Virus – First discovered in mid-September 2001, Nimda (“admin” backwards) is both a worm and a virus. This has proven to be the most prolific worm to date. All released Microsoft Windows platforms (Windows 95/98/ME/NT/2000) are potentially vulnerable, as it uses a variety of vulnerabilities to spread. This worm/virus hybrid has four infection vectors:

1) Scans random IP’s for web servers and attacks unpatched IIS servers with the ISAPI vulnerability (same as Code Red) and the Web Server Folder Traversal vulnerability (same as Code Blue). It also attempts to use backdoors left by a Code Red II infection. Servers infected by this worm will also attempt to send the worm (as an email file that auto-downloads) to anyone visiting the web page (Worm Mode).
2) Emails the worm to people found in an Outlook address book (Worm Mode).
3) Scans shared network folders (“My Network Neighborhood” – SMB Shares) for Microsoft Word™ documents, infecting them with a macro virus version of it (Virus Mode).
4) Infects several commonly used *.exe and *.dll files, and adds registry entries to ensure these files are run at every boot-up (Virus Mode).

The email sent via the Outlook mailing or downloaded via web page browsing does not have to be opened for the victim to be infected. Emails loaded into the ‘preview’ pane in Outlook will infect the system without user intervention – a bug in the MIME handler allows the email’s payload to run without prompting, as it disguises itself as an audio (*.wav) file. There is currently no known hostile payload to this worm, other than its propagation activity.

Defense

NetScreen always suggests keeping your client and server patches as updated as possible to prevent security breaches. Reading and applying concepts found in NetScreen's Whitepaper "Fundamentals to Secure Network Design v1.1" (CASE-260-002) is also highly recommended.

Several problems faced by users of NetScreen devices under attack by these worms were:

1) The device would not prevent an infection, despite the traffic flowing through the NetScreen to the target.
2) The systems on the internal network now infected by these worms would scan tens of thousands of IP's going back outward, filling up the sessions in the NetScreen device. Two of these worms (Code Red and Code Blue) also had 'attack modes' where they would flood a target site, accelerating the process of maxing out the session count.
3) Attacks against the NetScreen's WebUI management port would lockout the device from remote management.

These problems were not a design flaw or a failure on the part of the device – the NetScreen device is a Layer 3 and 4 stateful inspection firewall. Traffic destined to port 80 on a web server that was permitted by policy would go through, because the NetScreen was told to permit it – including a malicious URL. Additionally, traffic originating from the inside going out, if permitted by policy would be let out, until the number of simultaneous sessions the device could track were exhausted. If one inside source address used all 128,000 sessions an NS-100 could track, no other user would be able to gain access past the NetScreen.

NetScreen devices have a specific number of sessions allocated for connections to the device (this amount varies by device). If a NetScreen device allows a connection to it, and the connection does not close, the NetScreen will wait the appropriate timeout for that service (HTTP, Telnet, SSH, etc) - typically 30 minutes - before releasing the session. Especially problematic on the NS-5, NS-5XP, and NS-10, connections to the device from a Worm-infected (Code Red, Code Red II and Nimda) server trying to infect the NetScreen's WebUI will occupy all management sessions, making the device impossible to manage remotely. This issue is easily remedied in one of three ways:

1) Change the TCP port number the WebUI listens on. Nimda will attempt 16-23 separate attempts against port 80. If the WebUI is not listening on the port, it will not respond, and the server will not occupy management sessions.
2) Disable the WebUI on the interface that is facing infected servers. Each interface on the NetScreen has separate settings for each type of management. If a management type is not needed on a particular interface at that time, it should be turned off. Servers attempting to connect to an interface that is not listening for connections cannot use up management sessions.
3) Set Management Client IP's for all management stations. By default, the NetScreen will accept management connections from any source IP (within the restrictions imposed by interface permissions). Adding an entry to the Management Client IP will restrict access to only those IP's in the list. Any Worm-infected server that is not on the list cannot connect to the NetScreen, and therefore not use up management sessions.

NetScreen has now created two new features to assist in the containment of these malicious worms – the "User-Definable Malicious URL" feature, and "Source-IP-Based Session Threshold" feature. Both of these issues address the problems specified above.

User-Definable Malicious URL Detection – Allows a basic active "Network Intrusion Detection System" (NIDS) feature on the firewall. With this feature enabled, the NetScreen device will monitor traffic destined to port 80 (the port for web servers). If data destined for this port contains a URL that

matches the signature the user has defined for a Malicious URL entry, the NetScreen will drop that packet and send a RST packet to both sides of the connection – effectively stopping the attack.

This feature is currently only available from the Command Line Interface (CLI). The command is:

set firewall malicious-URL "Name" pattern "URL String" [length <num>]

Where "Name" is a user-specified identifier for this particular entry (limited to 8 characters), the "URL String" is a pattern (currently limited to 24 characters) that uniquely identifies a URL as a malicious URL. There is also an optional length setting, which is explained later in this paper. In order for the malicious URL feature to work, the URL must match starting at the beginning. The URL's:

"GET /Evil_Dir/Bad_Program.exe" and
"GET /Evil_Dir/Evil_Program.exe"

would be captured by a common Malicious URL of

set firewall malicious-URL "Evil" pattern "GET /Evil_Dir/"

However these URL's:

"GET /Evil_Dir/Bad_Program.exe" and
"GET /Bad_Dir/Evil_Program.exe"

would not be captured by a common Malicious URL entry of "Program.exe". These two URL's would need separate complete entries in Malicious URL:

set firewall malicious-URL "Evil" pattern "GET /Evil_Dir/"
set firewall malicious-URL "Bad" pattern "GET /Bad_Dir/"

Some Malicious URL attacks are of the 'overflow' variety, where they attempt to send a very long URL in the hopes that the URL will be too long for the server to handle properly, pushing part of the URL into running memory, where the code will run. A secondary option of the Malicious URL feature is a character length. Code Red uses an overflow vulnerability – its URL is very long:

"GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%u
cbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190
%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0"

An option on the end of the CLI command allows you to specify a length. If the pattern is matched, and the length specified is equal or greater, the packet is considered "Malicious" and is dropped. A valid Malicious URL entry for this signature could be:

set firewall malicious-URL "Code Red" pattern "GET /default.ida?NNNNNNNNN"
length 200

This specifies a unique pattern – repeating N's (which would rarely be valid) and also specifies a length (we specify 200 to be safe – this URL is over 380 characters long) that if both the pattern and length match, then this is a Malicious URL and should be dropped. However, adding this entry to your NetScreen is not necessary, as the Code Red Worm has been pre-programmed with ScreenOS 2.6.1r2. It is enabled with the hidden CLI command:

set firewall malicious-URL code-red-worm

Different NetScreen platforms allow for a different number of user-defined Malicious URL entries. The pre-programmed Code Red Worm entry does not apply towards the user-defined limit.

Platform	# Of Malicious URL Entries
NS-5, NS-5XP, NS-10	8
NS-100	16
NS-500	32
NS-1000	64

Source IP Session Threshold – If a system is already infected behind a firewall, it will scan outbound, trying to infect new servers. This can max the session count, prohibiting access through the NetScreen. A new feature can limit the number of concurrent sessions any one source IP can have. This option is currently only available from the Command Line Interface:

```
set firewall session-threshold source-ip-based <num>
```

Where <num> is the maximum number of active sessions any single IP can use at a time. Here is an example:

A network with a NetScreen-10 protecting it has four servers, which are infected with Code Red II. They are each scanning outbound at a rate of 10 new sessions a second (typical rate for CRII). A NetScreen-10 has a maximum active session limit of 4096. Assuming no other traffic is flowing, and assuming all IP's scanned do not reply to port 80, it would take approximately 100 seconds (about a minute and a half) for all sessions on the NetScreen-10 to be taken. These sessions would time out by default in 30 minutes, to be immediately replaced by more scans from the servers. Each server would occupy approximately 1,000 sessions, if all started scanning simultaneously. If the command:

```
set firewall session-threshold source-ip-based 800
```

were set on this NS-10, the scanning servers would be limited to 800 sessions each, leaving 1696 sessions (4096 – 2400) available for use by other users.

This command should be used with care, as it is a global setting; it applies equally to all source IP's. Some fine-tuning may be needed, to allow servers to serve without restriction, but still protecting from 'session hogs'.

Summary

The current trend suggests self-replicating, self-propagating worms are here to stay. While Network System Administrators try to keep up with the myriad of server and client patches, worm authors are working hard to make Sysadmins' lives more difficult. In the space between initial attack and a successful patch, it is useful to have additional tools to help stem the flood. NetScreen Technologies is committed to providing our customers with the most powerful, most useful security tools we can create. Proper application of the information presented in this whitepaper will help keep your networks flowing smoothly and worm-free.

Reference

The Reference section has been divided into two major groups: Online and Offline (hardcopy). Most of the online sites have cross-links to other similar sites. Additionally, Google has a great index of network security sites at: http://directory.google.com/Top/Computers/Security/News/

Online:

Microsoft™
http://www.microsoft.com

Since all worms mentioned in this paper use infection vectors from various Microsoft product vulnerabilities, they have been listed first. Listed below are the official Microsoft bulletins for the vulnerabilities. At these sites you will find additional technical information and links to patches to correct the problem. Please keep in mind these are Microsoft patches for Microsoft products, NetScreen neither warrants nor requires their application in order to use NetScreen devices.

ISAPI overflow vulnerability, MS01-033 (used in Code Red, Code Red II, and Nimda):
http://www.microsoft.com/TechNet/security/bulletin/MS01-033.asp

IIS Web Server Folder Traversal vulnerability, MS00-078 (used in Code Blue and Nimda):
http://www.microsoft.com/TechNet/security/bulletin/MS00-078.asp

MIME vulnerability, MS01-044 (used in Nimda):
http://www.microsoft.com/TechNet/security/bulletin/MS01-044.asp

eEye Security
http://www.eeye.com/html/

eEye Security was the first security group to identify and disassemble the Code Red and Code Red II worms.

Code Red analysis:
http://www.eeye.com/html/Research/Advisories/AL20010717.html

Code Red II analysis:
http://www.eeye.com/html/Research/Advisories/AL20010804.html

Internet Security Systems, Inc.
http://www.iss.net/index.php

ISS was the first group to identify and disassemble the Code Blue worm.

Code Blue analysis:
http://xforce.iss.net/alerts/advise96.php

SANS Institute
http://www.sans.org

The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization comprised of system administrators, security professionals, and network administrators. They have great network security courses, as well as certification in network security.

SANS “Incidents Handler” for Nimda:
http://www.incidents.org/react/nimda.php

Common Vulnerabilities and Exposures
http://www.cve.mitre.org/

A freely available, community supported, standards body for vulnerabilities. Its goal is to make it easier to share data across separate vulnerability databases and security tools. While CVE may make it easier to search for information in other databases, CVE should not be considered as a vulnerability database on its own merit.

CERT Coordination Center
http://www.cert.org

Federally funded network security research organization out of Carnegie Mellon University.

Security Focus
http://www.securityfocus.com

For-profit, private organization with a lot of security information available for free.

NT Bugtraq
http://www.ntbugtraq.com

Non-profit, non-Microsoft™ organization dedicated to detecting and tracking bugs (and vulnerabilities) in Microsoft products. This site also has great email newsletters.

Offline/Hardcopy:

Hacking Exposed, 2nd Edition, by Joel Scambray, Stuart McClure, George Kurtz
Paperback - 703 pages 2nd edition (October 11, 2000)
McGraw-Hill Professional Publishing; ISBN: 0072127481

A great overview of hacking techniques and concepts.

Network Intrusion Detection: An Analyst's Handbook, 2nd Edition, by Stephen Northcutt, Donald McLachlan, and Judy Novak.
Paperback - 450 pages 2nd edition (September 22, 2000)
New Riders Publishing; ISBN: 0735710082

Great book on the forensics of hacking: How to handle a break-in, how to keep one from happening.

Maximum Security, 3rd Edition, by Anonymous
Paperback - 864 pages 2nd edition (September 15, 1998)
Sams; ISBN: 0672313413
Paperback - 896 pages 3rd edition (May 17, 2001)
Sams; ISBN: 0672318717

In-depth details of exactly how to hack, different editions cover different techniques, get all of them to have complete coverage. These are big books!

Legal Notice

This paper has made references to many websites ("Linked Sites"). The Linked Sites are not under the control of NetScreen and NetScreen is not responsible for the contents of any Linked Site, including without limitation any link contained in a Linked Site, or any changes or updates to a Linked Site. NetScreen is not responsible for web casting or any other form of transmission received from any Linked Site nor is NetScreen responsible if the Linked Site is not working appropriately. NetScreen is providing these links to you only as a convenience as a reference to this paper, and the inclusion of any link does not imply endorsement by NetScreen of the site or any association with its operators. You are responsible for viewing and abiding by the privacy statements and terms of use posted at the Linked Sites. This paper is for educational purposes only.