Identification

Vulnerability Name: W32.Novarg mass mailing worm.
Key reference includes: CERT® Advisory CA-2004-02 Email-borne Viruses.
http://www.cert.org/advisories/CA-2004-02.html
Additional information:
http://securityresponse.symantec.com/avcenter/venc/data/w32.novarg.a@mm.html

Overview

Two more mass-mailing worms have been recently discovered, W32/Bagle and W32/Novarg, that arrive as an attachment with the file extension .bat, .cmd, .exe, .pif, .scr or .zip. When a computer is infected, the worm will set up a backdoor into the system by opening TCP ports 3127 through 3198, which can potentially allow an attacker to connect to the computer and use it as a proxy to gain access to its network resources, or use the backdoor as a method to download and execute arbitrary files.
The technology used in these viruses is not significantly different from prior mass-mailing viruses such as W32/Sobig and W32/Mimail.

The worm will perform a Denial of Service (DoS) starting on February 1, 2004. It also has a trigger date to stop spreading on February 12, 2004. These two events will only occur if the worm is run between or after those dates. While the worm will stop spreading on February 12, 2004, the backdoor component will continue to function after this date. This virus can impact any system running Microsoft Windows (all versions from Windows 95 and up) and used for reading email or accessing peer-to-peer file sharing services.

Impact

Although the OmniSwitch is not a target of the worm, OmniSwitch configurations can provide some assistance in minimizing the impact for those networks that are not using anti-virus and or firewall protection on all Microsoft Windows systems.

OS-7700/7800/8800 has Hardware Route Cache on the NI. Whenever a request comes in from a PC or an end-station for an unknown destination, it is handled in software, once the destination is learned a route cache entry is created. After a route cache entry is created, the traffic is routed in hardware. This attack starts scanning for the other vulnerable systems, so each workstation will start generating hundreds of random destination addresses resulting in high CPU utilization of the NI processor. This can be observed by using the command “show health <slot>”

“As the workstations generate random unique destination addresses that need to be learned by the switch initially before they are programmed in the Hardware Routing Engine (HRE), so the CPU cycles are used to process the ARP request for the requests received by the switch. Once the entries are learned by the switch and programmed in the HRE, the number of HRE route cache entries can result in high utilization, use the command: "show hre pcam utilization slot/0". This command will show that the HRE utilization is constantly increasing.

Another useful command to observe is "show hre cache utilization slot/0", this command shows the actual number hre cache entries on a slot.

Solution of AOS-based OmniSwitch Products

ACLs can be configured on the OmniSwitch 7700, 7800 and 8800 to stop the propagation of the virus (worm) to other workstations in the network. The following is an example of how to deny all the traffic on TCP ports 3127 through 3198 to deny the traffic to prevent the other workstations backdoors from being accessed. Another option is to use the combination of destination address of internal network and destination the TCP ports. If the OmniSwitch is used as a connection out to the Internet then this would reduce the number of cam entries created, as the traffic destined for the internal network would be blocked, but the traffic to the Internet on these ports would not be blocked. The 6600 cannot do policies for TCP port ranges. A limited number of specific ports could be specified if desired, but it is recommended to use the 7700/8800 for this functionality.

***Please note that any applications that may be using these TCP ports would also be affected once the ports are blocked by the policy.
***Also note that as soon as any changed policies are applied with “qos apply” all learned traffic is flushed from the hardware (HRE) tables and all traffic will momentarily be in software until the flows are relearned. If the switch is under heavy load when “qos apply” is used this can affect performance for a period of time.

Option 1 to drop all destination traffic to these TCP ports.

policy condition cworm destination tcp port 3127-3198
policy action aworm disposition deny
policy rule aworm condition cworm action aworm
qos classifyl3 bridged (Only use this if you want to look at all layer 2 and layer 3 traffic rather than just layer3 traffic. This requires more of the switch resources).
qos apply

Option 2 to drop all destination traffic to the internal network on these TCP ports for subnet 192.168.10.0

policy condition cworm destination ip 192.168.10.0 mask 255.255.255.0 ip protocol 6 destination ip port 3127-3179
policy action aworm disposition deny
policy rule aworm condition cworm action aworm
qos classifyl3 bridged (Only use this if you want to look at all layer 2 and layer 3 traffic rather than just layer3 traffic. This requires more of the switch resources).
qos apply

Option 3 to drop all destination traffic to multiple internal subnets as seen below –

Policy network group internal_network 192.168.64.0 mask 255.255.240.0 192.169.32.0 mask 255.255.224.0 192.170.80.0 mask 255.255.240.0 192.171.176.0 mask 255.255.240.0 192.172.160.0 mask 255.255.240.0 192.173.128.0 mask 255.255.224.0 192.174.208.0 mask 255.255.240.0 192.175.112.0 mask 255.255.240.0 192.176.108.0 mask 255.255.252.0
policy condition cworm destination network group internal_network ip protocol 6 destination ip port 3127-3179
policy action aworm disposition deny
policy rule aworm condition cworm action aworm
qos classifyl3 bridged (Only use this if you want to look at all layer 2 and layer 3 traffic rather than just layer3 traffic. This requires more of the switch resources).
qos apply

***Note – To disable qos after policies have already been applied the following steps can be used.
1. Disable the policy rules "policy rule (name) disable"
2. "qos no classifyl3 bridged" (if it was enabled)
3. "qos disable"
4. "qos apply" (Flushes all hardware tables and has to relearn flows)

If excessive traffic from the DOS is going into software rather than hardware routing the CPU utilization on the NI can go high. Check CPU utilization before and after applying the qos rules with the following command.

> show health all cpu
* - current value exceeds threshold

Cpu	Limit	1 Min Curr	1 Hr Avg	1 Hr Avg	Max
02	80	17	19	16	20
03	80	29	17	16	18
04	80	15	16	17	20

To check the NI pcam utilization use the following command with the slot/slice

> show hre pcam utilization 6/0
HRE PCAM Utilization

Slot/ Slice	Mode	PCAM Total	Hash Inuse	Coll Inuse	Max Depth	Avg Depth
6/0	0	16384	14	2	2	1
6/0	1	16384	33	0	1	1
6/0	2	16384	0	0	0	0
6/0	3	16384	74	52	5	2

Check the Hash in use. If it is a high number near the hardware pcam total then this could be another indication that packets will be routed in software, which could impact network performance.

Tracking the Source

In order to track the most chatty device generating all the traffic in the network, the following command can be used"

debug ip-packet [start] [timeout seconds] [stop] [direction {in | out | all}] [format {header | text | all}] [output {screen | switchlog}] [board {cmm | ni [1-16] | all | none} [ether-type {arp | ip | hex [hex] | all}] [ip-address ip_address] [ip-pair [ip1] [ip2]] [protocol {tcp | udp | icmp | igmp | num [integer] | all}] [show-broadcast {on | off}] show-multicast {on | off}]

There are several options available which helps to classify the kind of traffic one may be interested in.

- ***start*** - Starts an IP packet debug session.
- ***timeout*** - Sets the duration of the debug session, in seconds. To specify a duration for the debug session, enter timeout, then enter the session length.
- ***seconds*** - The debug session length, in seconds.
- ***stop*** - Stops IP packet debug session.
- ***direction*** - Specifies the type of the packets you want to debug:
    - ***in*** - Debugs incoming packets
    - ***out*** - Debugs outgoing packets.
    - ***all*** - Debugs both incoming and outgoing packets.
- ***format*** - Specifies the area of the packet you want to debug:
    - ***header*** - Debugs the packet header.
    - ***text*** - Debugs the packet text.
    - ***all*** - Debugs the entire packet.
- ***output*** - Specifies where you want the debug information to go:
    - ***screen*** - Output will appear on screen.
    - ***switchlog*** - Output will be saved to a log file.
- ***board*** - Specifies the slot (board) that you want to debug:
    - ***cmm*** - Debugs CMM packets.
    - ***ni*** - Debugs packets for a Network Interface (NI). To debug a specific inter-face, enter ni, then enter the slot number of the NI.
    - ***all*** - Debugs packets for all CMMs and NIs on the switch
    - ***none*** - Clears the previous "board" settings.

The output is available on the console or telnet of the switch. This can help to identify the chattiest device, which can be taken off the network to rectify the situation.

Solution for XOS-based Omni Switches

Most XOS-based switches cannot filter on TCP or UDP port numbers. Only the OmniAccess 512 can; the XOS OmniSwitch and OSR cannot.

From a LAN switch's perspective, the worm, is a denial of service attack. The worm generates enough traffic to your site that it denies service to the site's legitimate users. See http://www.cert.org/tech_tips/denial_of_service.html for more info. A DOS attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include:

attempts to "flood" a network, thereby preventing legitimate network traffic
attempts to disrupt connections between two machines, thereby preventing access to a service
attempts to prevent a particular individual from accessing a service
attempts to disrupt service to a specific system or person

How to Identify a DOS Attack from an OmniSwitch

This is best accomplished by capturing statistics from an operational switch that has an MPM-III and HRE-VX. To do this, from the console, run hdstat, systat, taskstat, prn_rc_dbg, and if_vbDebug=33;taskDelay 600;if_vbDebug=0. Consider increasing the taskDelay to 900 or 1200 or take it out entirely. Make sure you turn it off when you are done or reboot the switch.

One resolution to a DOS attack is to patch the offending operating system (Microsoft in this case). A second would be to remove the offending workstation from the network until patched.

An Alcatel customer stated: "We had identified two possible IP addresses which could be infected with the virus. There may be other possible IP addresses that could be infected. We analyzed the captured file and deduced the following:

202.160.24.16 (OK) 202.160.24.33 (OK)
202.160.24.156 (X)
202.160.24.164 (OK)
202.160.24.178 (OK)
202.160.26.7 (X)
202.160.28.4 (OK)
202.160.28.7 (OK)
202.160.29.163 (OK)
202.160.29.180 (OK)

"But we had tested and deduced that only the above two IP addresses are infected PCs. They are 202.160.24.156 and 202.160.26.7. They are currently disabled.

"We are simultaneously monitoring the hreRouteCacheCount and CPU utilization while these IP addresses are enabled and disabled. When we enabled one of the above infected IP address, both reRouteCacheCount and CPU utilization shot up, and when we disabled it, both count and utilization revert to normal condition"

hdstat Results

Device 1	Min 1	Hr 1	Hr
Resources	Limit	Curr	Avg	Avg	Max
---	---	---	---	---	---

Receive 80 01 01 01 01
Transmit/Receive 80 01 01 01 01
Backplane 80 01 01 01 01
CAM [MPM] 80 100* 131 131 131
CAM [HRE] 80 100* 99 100 100
Collisions [HRE] 80 04 04 02 08
CPU 80 53 55 65 100
Memory 80 26 26 26 26
Temperature 62 31 31 30 31
Virtual Ports 80 21 21 21 21

systat Results
System Uptime : 0 days, 12:56:24.37
MPM Transmit Overruns : 0
MPM Receive Overruns : 0
Excessive Ping Requests : 0 in the last 0 days, 01:34:53
MPM total memory : 64MB
MPM free memory : 46965176 bytes
MPM CPU Utilization (5 sec) : 56% (0% intr 2% kernel 53% task 44% idle)
MPM CPU Utilization (60 sec) : 55% (0% intr 1% kernel 51% task 45% idle)
Power Supply 1 State : OK
Power Supply 2 State : Bad
Temperature Sensor : OK - Under Threshold
Temperature: 31.00c 87.80f
Temperature Alarm Masking : Disabled

Dshell Results
-> prn_rc_dbg
The current router cache timer is set to 30 seconds.
The current HREX router cache timer is set to 30 seconds.
157 MPM IP route cache entries aged out in the last 30 seconds
0 MPM IPX route cache entries aged out in the last 30 seconds
7457 HREX IP route cache entries aged out in the last 30 seconds
0 HREX IPX route cache entries aged out in the last 30 seconds
All IP cache entries cleared 3 times. (Last cleared by tRip, 3453 seconds ago
IP network cache entries cleared 25 times. (Network 202.160.12.0 (255.255.255.128)
cleared by tif_vbPMH, 19220 seconds ago Individual IP cache entries have been cleared
1492 times.
(Last entry cleared by tNetTask, 25 seconds ago
All IPX cache entries cleared 0 times.
IPX network cache entries cleared 0 times. Individual IPX cache entries have been
cleared 0 times.
There are 3968 MPM route cache entries.
There are 40960 HREX route cache entries.
value = 0 = 0x

-> hreRouteCacheCount
_hreRouteCacheCount = 0x308586f0: value = 40960 = 0xa000
-> exit
HRE-8205 / %
Additional dshell Results
-> if_vbDebug=33;taskDelay 300;if_vbDebug=0.
-> S:00d095:4e4ec3->00000c:07ac01 IP 202.160.28.4->192.168.132.121 TCP 3992,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.28.4->192.168.202.38 TCP 3993,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.28.4->192.168.26.80 TCP 3994,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.28.4->192.28.170.94 TCP 3995,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.28.4->192.215.146.153 TCP 3996,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.28.4->192.44.1.156 TCP 3997,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.24.33->133.1.96.231 TCP 3278,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.24.33->202.94.179.3 TCP 3279,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.24.39->24.70.145.252 TCP 2110,6346
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.24.33->202.160.47.233 TCP 3280,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.24.33->202.129.137.85 TCP 3281,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.24.33->202.102.165.193 TCP 3282,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.24.33->202.131.23.201 TCP 3283,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.28.7->198.31.218.133 TCP 4098,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.28.7->2.148.106.61 TCP 4099,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.28.7->94.160.131.69 TCP 4100,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.28.4->192.86.8.45 TCP 3998,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.28.4->192.208.138.228 TCP 3999,3127
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.28.4->192.168.112.9 TCP 4000,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.24.33->202.42.87.55 TCP 3297,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.28.4->192.235.158.49 TCP 4001,80
S:00d095:4e4ec3->00000c:07ac01 IP 202.160.28.4->192.182.122.122 TCP 4002,80

If you have any questions, the following contact information should be used:
Web Links
Customers: http://eservice.ind.alcatel.com/
EMEAI Business Partners: http://www.businesspartner.alcatel.com/

Email support@ind.alcatel.com
EMEAI Business Partners: mailto:support.center@alcatel.fr

Phone
North America 1 800-995-2696
Latin America 1 877-919-9526
Europe (EMEAI) +33-388-55-69-04
Asia Pacific +65-394-7933
Other International +1-818-878-4507