



PRODUCT BULLETIN NO. 3052

CISCO SECURITY AGENT AND THE ZOTOB WORM

SUMMARY

A new network worm is targeting Microsoft Windows 2000 systems via a vulnerability in the Universal Plug and Play service (MS05-039). The Cisco Security Agent (CSA) version 4.5 running the default security policy is effective in stopping this attack and preventing system compromise by all variants of the worm, even when the uPNP service has not been patched. Older CSA versions (v4.0.2, v4.0.3; others were tested as of this date) running the default configurations also stop the worm and its variants. No reconfiguration of the default CSA security policy or update to the CSA binary is required to stop the worms and variants.

DETAILS OF THE WORM

The Zotob worm and its variants are self-propagating network worms targeting a vulnerability in Microsoft Windows 2000 systems that run the Universal Plug and Play (uPNP) service. It contains a buffer overflow exploit that compromises this service. The worm uses a Null session to connect to the service over TCP port 445. This makes it hard to block in the network, because critical Windows services such as Active Directory rely on port 445.

Once the connection is established, the worm executes a buffer overflow exploit against the uPNP service. Once the buffer overflow is executed, the worm performs several malicious and damaging behaviors. The specific behaviors vary from variant to variant, but include the following:

- Writes executables in system folder
- Creates RUN registry keys
- Modifies HOSTS file
- Downloads files via TFTP
- Connects to 72.20.41.139/IRC
- Starts Command shell running FTP on port 33333, 65533, 11173; TFTP 1171; UDP 69
- Creates up to 300 threads to scan for other systems to infect
- At least one variant use SMTP to spread
- At least one variant deletes registry keys and files
- At least one variant terminates processes

Figure 1 shows the worm lifecycle.

Information about the Zotob worm is available at http://www.cisco.com/en/US/about/security/intelligence/05_08_zotob_worm.html

HOW CSA STOPS THE WORM

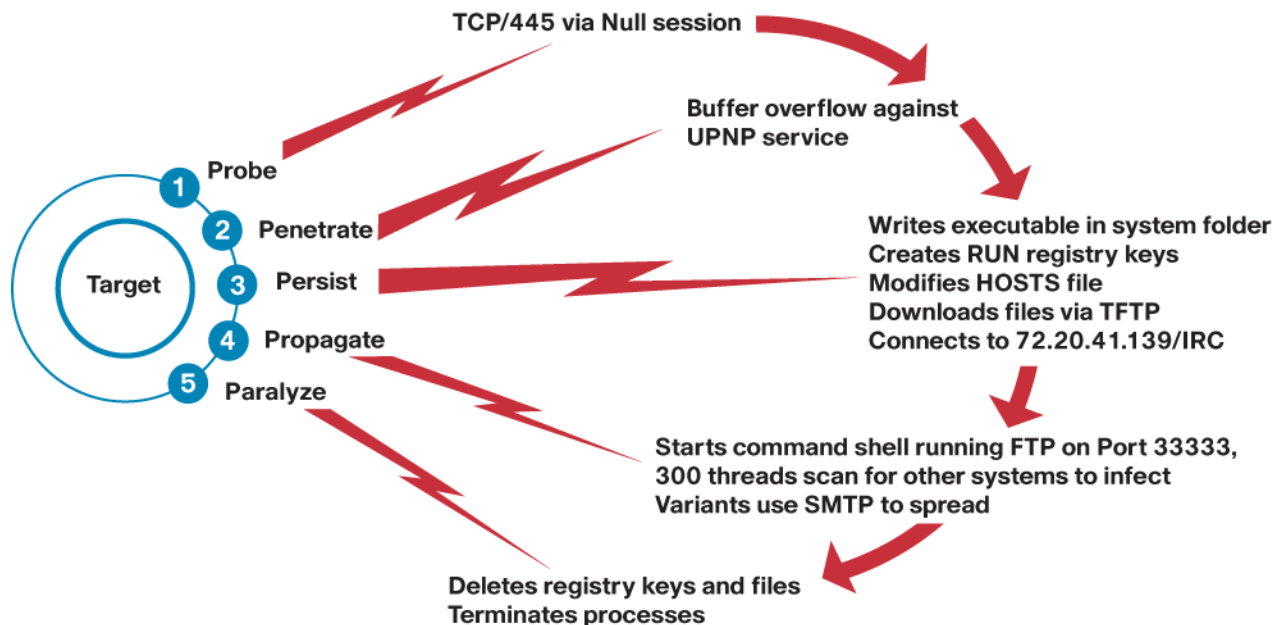
The CSA default policies contain at least six rules that stop the worm and variants. The exact number of malicious activities stopped varies depending on the variant tested, but up to 10 behaviors were identified during testing at Cisco (using the Zotob.B variant). No changes to the CSA binaries or default configuration are required to get this protection.

The following actions have been observed being blocked by CSA running the default security policies:

- An incoming Null Session connection to the uPNP service

- A buffer overflow against the service
- The attacked service attempted to execute a command shell (CMD.EXE)
- An executable file (or files) was written to the %SYSTEM directory
- One of these files was executed
- The application executed from the file tried to modify the hosts file
- The application executed from the file tried to create RUN or RUNSERVICES registry entries

Figure 1. The Zotob Worm (and Variants) in Action



This testing is shown in Figure 2.

Note that the worm was tested at Cisco, with the agent in *Testmode*, which will cause the agent to alert (but not block) malicious behavior. This was done to identify all possible ways that the CSA default policies would stop the worm. When the agent is in protect mode (the typical operational configuration), the first rule would kill the worm, i.e. no other events would be seen, because the worm would be blocked before it could perform any malicious actions. Cisco tested with agents in *Testmode* to determine how deep the CSA defense in depth is for the worms and variants. For the Zotob.B variant, this defense in depth is ten (as shown in Figure 2).

When Cisco Security Agent agents block the worm, they send an alert back to the CSA Management Center server. This alert contains the IP address of the attacking system. The server correlates alerts received from multiple CSA agents, and can quarantine attacking systems by adding their IP addresses to a “Block” List. This Block List is distributed to all agents, including agents that have yet to be attacked, effectively increasing the defense in depth.

Testing was performed against the CSA default policies. No binary or policy update was needed for CSA agents to be effective. In short, this was a true test of “Day Zero” protection. This is very similar to what we have seen with earlier worms—the default CSA configuration stopped the worm, with no binary or policy updates required. Table 1 shows a partial list of prior worms that the CSA has stopped.

Table 1. List of Worms That Cisco Security Agent (CSA) Has Provided Protection Against

Infection	Infection Type
Bagle	E-mail Worm
Blaster	Network Worm
Bugbear	E-mail Worm
Code Red	Network Worm
Debploit	Network Worm
Fizzer	E-mail Worm
Gator/Gain	Spyware
Hotbar	Spyware
SQL Slammer	Network Worm
SQL Snake	Network Worm
JPEG/GDI+	Malware downloader
MyDoom	E-mail Worm
Nimda	Network Worm
Pentagone/Gonner	E-mail Worm
Sasser	Network Worm
Sircam	E-mail Worm
Sobig	E-mail Worm

This worm is only the latest example of new and mutating attacks that can seriously affect organization's computing and network environments. The key to stopping these new attacks is to do so without requiring any changes to default configuration, and multiple rules in the default policies, which provide a defense in depth.

Figure 2. CSA Default Configuration Stops the Zotob.B Worm

ID	Time	Source	Severity	Message	Details	Action
11	8/18/2005 11:08:07 AM	W2K-SVR-Test1	Notice	TESTMODE: The process 'C:\WINNT\system32\haha.exe' (as user NT AUTHORITY\SYSTEM) attempted to call the function CreateThread from a buffer (the return address was 0x406f6a). The code at this address is '0068886e 40006a00 6a00ff15 30804000 6a0aff15 6c804000 ebc3c0 8be55dc2'. This either happens when a process uses self-modifying code or when a process has been subverted by a buffer overflow attack. This would have caused the user to be prompted as to the action to take.	Rule 172 Wizard	Find Similar
10	8/18/2005 11:08:06 AM	W2K-SVR-Test1	Notice	TESTMODE: The process 'C:\WINNT\system32\haha.exe' (as user NT AUTHORITY\SYSTEM) attempted to access the registry key '\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\Windows\CURRENTVERSION\RunServices', value 'csm Win Updates'. The attempted access was a write (operation = WRITE/VALUE). This would have caused the user to be prompted as to the action to take.	Rule 131 Wizard	Find Similar
9	8/18/2005 11:08:06 AM	W2K-SVR-Test1	Notice	TESTMODE: The process 'C:\WINNT\system32\haha.exe' (as user NT AUTHORITY\SYSTEM) attempted to access the registry key '\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices', value '. The attempted access was a write (operation = CREATE/KEY). This would have caused the user to be prompted as to the action to take.	Rule 131 Wizard	Find Similar
8	8/18/2005 11:08:06 AM	W2K-SVR-Test1	Notice	TESTMODE: The process 'C:\WINNT\system32\haha.exe' (as user NT AUTHORITY\SYSTEM) attempted to access the registry key '\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\Windows\CURRENTVERSION\Run', value 'csm Win Updates'. The attempted access was a write (operation = WRITE/VALUE). This would have caused the user to be prompted as to the action to take.	Rule 131 Wizard	Find Similar
7	8/18/2005 11:08:06 AM	W2K-SVR-Test1	Notice	TESTMODE: The process 'C:\WINNT\system32\haha.exe' (as user NT AUTHORITY\SYSTEM) attempted to access the registry key '\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Run', value '. The attempted access was a write (operation = CREATE/KEY). This would have caused the user to be prompted as to the action to take.	Rule 131 Wizard	Find Similar
6	8/18/2005 11:08:06 AM	W2K-SVR-Test1	Notice	TESTMODE: The process 'C:\WINNT\system32\haha.exe' (as user NT AUTHORITY\SYSTEM) attempted to access 'C:\WINNT\system32\drivers\etc\hosts'. The attempted access was a write (operation = OPEN/CREATE). This would have caused the user to be prompted as to the action to take.	Rule 125 Wizard	Find Similar
5	8/18/2005 11:08:06 AM	W2K-SVR-Test1	Notice	TESTMODE: The current application 'C:\WINNT\system32\CMD.EXE' (as user NT AUTHORITY\SYSTEM) is trying to execute the new application 'C:\WINNT\system32\haha.exe'. This would have caused the user to be prompted as to the action to take.	Rule 511 Wizard	Find Similar
4	8/18/2005 11:08:06 AM	W2K-SVR-Test1	Alert	TESTMODE: The current application 'C:\WINNT\system32\services.exe' (as user NT AUTHORITY\SYSTEM) attempted to execute the new application 'C:\WINNT\system32\CMD.EXE'. The operation would have been denied.	Rule 510 Wizard	Find Similar
3	8/18/2005 11:08:05 AM	W2K-SVR-Test1	Alert	TESTMODE: The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to communicate with 10.1.2.150 on TCP port 445. The attempted access was to accept a connection as a server (operation = ACCEPT). The operation would have been denied.	Rule 118 Wizard	Find Similar
2	8/18/2005 11:02:34 AM	W2K-SVR-Test1	Notice	TESTMODE: The process 'C:\WINNT\system32\services.exe' (as user NT AUTHORITY\SYSTEM) attempted to call the function LoadLibraryA ("ws2_32") from a buffer (the return address was 0x55f9b8). The code at this address is 'ffd66653 66683332 68777332 5f54ffd0 68cbdfc 3b50ffd6 5f89e566 81ed0802'. This either happens when a process uses self-modifying code or when a process has been subverted by a buffer overflow attack. This would have caused the user to be prompted as to the action to take.	Rule 172 Wizard	Find Similar
1	8/18/2005 11:02:34 AM	W2K-SVR-Test1	Alert	TESTMODE: The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to communicate with 10.1.2.150 on TCP port 445. The attempted access was to accept a connection as a server (operation = ACCEPT). The operation would have been denied.	Rule 118 Wizard	Find Similar

No rule changes pending Generate rules

Logged in as: admin

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R) 204148.R_ETMG_KM_8.05

