

Cisco Security Agent and MPack Enabled Malware

PB417466

Summary

According to various news sources, a widespread Web attack has compromised more than 10,000 legitimate Websites and continues to spread worldwide. The attack was first discovered on June 15, 2007. Legitimate Websites were hacked to include a malicious HTML iFrames tag redirecting visitors to servers armed with an exploit tool called MPack that can target security holes in numerous products. MPack installs a keylogger and a Trojan downloader program on compromised PCs so that the attackers can monitor the compromised system's activity and run other unauthorized programs on the computer.

Cisco® has obtained exploit files, and has confirmed that the Cisco Security Agent is effective in stopping these exploits, using the default security policy configuration. Current supported versions of Cisco Security Agent 4.5.x, 5.0.x, 5.1.x, and 5.2.x are all effective in stopping the exploits seen to date.

Details of the Vulnerability

Details of the vulnerability:

1. HTML_IFRAME is hosted on malicious/hacked sites.
2. When the users visits the affected system, they are directed to an intermediate server that directs them to the site hosting the downloader.
3. This downloader JS_DLOADER.NTJ chooses its exploits based on the target user's browser and operating system. It then downloads another Trojan, TROJ_SMALL.HCK.
4. TROJ_SMALL.HCK, in turn, downloads TROJ_AGENT.UHL and TROJ_PAKES.NC.
5. TROJ_AGENT.UHL acts as a proxy server to allow a remote user to anonymously connect to the Internet through an infected computer. TROJ_PAKES.NC downloads a key logger TSPY_SINOWAL.BJ.¹

Various security vendors report that the MPack-enabled malware exploits several well-known vulnerabilities that have already been patched, so it is dangerous to users who are not running an updated version of their browsers.

How Cisco Security Agent Stops the Exploit

Cisco Security Agent default policies contain multiple rules that stop the exploit from doing any damage. No changes to the Cisco Security Agent binaries or default configuration are required to get this protection.

Cisco Security Agent testing was performed from the viewpoint of the Web user who visited the infected Website and had the MPack-enabled malware delivered to their system. Cisco believes

¹ Trend Micro: <http://blog.trendmicro.com/another-malware-pulls-an-italian-job>

that Cisco Security Agent, if installed on the legitimate Web server itself, would have prevented the installation of the MPack kit and prevented the initial infection of the Website altogether.

The following actions have been observed being blocked by Cisco Security Agent running the default security policies:

- The modification of a system file
- The modification of a registry key
- An attempt to invoke a system function from a buffer

This testing is shown in Figure 1.

Figure 1. Cisco Security Agent Default Configuration Stops the MPack-Enabled Exploit (Tested on Cisco Security Agent 5.2)

w2k-pro-sp4	Notice	TESTMODE: The process 'C:\WINNT\system32\svchost.exe' (as user W2K-PRO-SP4\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\WINNT\system32\svchost.exe is attempting to modify the system file C:\WINNT\system32\rtssystem.dll. Do you wish to allow this?' Details Rule 61 Wizard	14 similar events (same Type/Rule ID/Application) Find Similar
w2k-pro-sp4	Notice	TESTMODE: The process 'C:\WINNT\explorer.exe' (as user W2K-PRO-SP4\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\WINNT\explorer.exe is attempting to invoke a system function from a buffer. Do you wish to allow this?' Details Rule 186 Wizard	Find Similar
w2k-pro-sp4	Notice	TESTMODE: The process 'C:\Documents and Settings\Administrator\Local Settings\Temp\3.tmp.exe' (as user W2K-PRO-SP4\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\Documents and Settings\Administrator\Local Settings\Temp\3.tmp.exe is attempting to modify the registry key \REGISTRY\MACHINE\SOFTWARE\MICROSOFT\Windows\CURRENTVERSION\Explorer\Browser Helper Objects\{3C49DDAC-3DA4-4743-AF6C-5974FEAF875C}\. Do you wish to allow this?' Details Rule 55 Wizard	1 similar event (same Type/Rule ID/Application) Find Similar
w2k-pro-sp4	Notice	TESTMODE: The process 'C:\Documents and Settings\Administrator\Local Settings\Temp\3.tmp.exe' (as user W2K-PRO-SP4\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\Documents and Settings\Administrator\Local Settings\Temp\3.tmp.exe is attempting to modify the system file C:\WINNT\system32\Ymt_32.dll. Do you wish to allow this?' Details Rule 61 Wizard	1 similar event (same Type/Rule ID/Application) Find Similar
w2k-pro-sp4	Notice	TESTMODE: The process 'C:\Documents and Settings\Administrator\Local Settings\Temp\1.tmp' (as user W2K-PRO-SP4\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'A process is attempting to invoke C:\Documents and Settings\Administrator\Local Settings\Temp\3.tmp.exe which has been recently downloaded and may be dangerous. Do you wish to allow this?' Details Rule 454 Wizard	Find Similar
w2k-pro-sp4	Notice	TESTMODE: The process 'C:\Program Files\Internet Explorer\IEXPLORE.EXE' (as user W2K-PRO-SP4\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'A process is attempting to invoke C:\Documents and Settings\Administrator\tm.exe which has been recently downloaded and may be dangerous. Do you wish to allow this?' Details Rule 454 Wizard	1 similar event (same Type/Rule ID/Application) Find Similar

Note: The exploit was tested at Cisco, with the agent in Test mode, which will cause the agent to alert (but not block) malicious behavior. This was done to observe all possible ways that the Cisco Security Agent default policies would stop the exploit. When the agent is in Protect mode (the typical operational configuration), the first rule would kill the exploit: no subsequent events would be seen, since the exploit would be terminated before it could perform any malicious actions.

Testing was performed against the Cisco Security Agent default policies. No binary or policy update was needed for Cisco Security Agents to be effective. In short, this was a true test of "day-zero" protection. This is similar to what Cisco has seen with earlier exploits and worms—the default Cisco Security Agent configuration stopped the exploit, with no binary or policy updates required. The following is a partial list of prior worms and exploits that Cisco Security Agent has stopped via the default security policy settings:

Exploits	Worms	Exploits	Worms
ANI 0Day	OS vulnerability	MyDoom	E-mail worm
Bagle	E-mail worm	MS06-035	OS vulnerability
BigYellow	Network worm	MS06-040	OS vulnerability
Blackworm	Network worm	MS06-070	OS vulnerability
Blaster	Network worm	MS07-014	Application vulnerabilities
Bugbear	E-mail worm	Excel hlink dll	Application vulnerability

Exploits	Worms	Exploits	Worms
Code Red	Network worm	MS RDS ActiveX	OS vulnerability
Debplot	Network worm	MS XML Core Svs	OS vulnerability
DNS 0Day	OS vulnerability	Nimda	Network worm
Fizzer	E-mail worm	Pentagone/Gonner	E-mail worm
Gator/Gain	Spyware	Sasser	Network worm
Hotbar	Spyware	Sircam	E-mail worm
HTTP Dir Traversal	Web server vulnerability	Sobig	E-mail worm
IE Text Range	Application vulnerability	Storm Trojan	E-mail worm
IE VML BO	Application vulnerability	WMF 0day	OS vulnerability
SQL Slammer	Network worm	Word BO	Application vulnerability
SQL Snake	Network worm	W32.Rinbot.H	Network worm
JPEG/GDI+	Malware downloader	Zotob	Network worm

This exploit is only the latest example of new and mutating attacks that can seriously affect an organization's computing and network environments. The key to stopping these new attacks is two-fold: the ability to stop the attack without requiring any changes to the default configuration, and multiple rules in the default policies that provide defense in depth.



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 353-NETS (6387)
Fax: 408 527-0889

Asia Pacific Headquarters
Cisco Systems, Inc.
155 Robinson Road
#29-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Hertofwegpark
Hertofwegweg 13-19
1101 CH Amsterdam
The Netherlands
www.europe.cisco.com
Tel: +31 20 60 020 0/91
Fax: +31 20 657 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Airnet, BPK, Catalyst, CCNA, CCNP, CCIE, CCIP, CCMA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast, Step, Follow Me Browsing, FormShare, Go to Drive, HomeLink, Internet Quotient, IOS, IPPhone, IPTV, IQ Expertise, the IQ logo, IQ Not, Roadshow, Scorecard, QuickStudy, ipsoStream, iInlays, Modeling Place, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, SsookWise, 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. (9705R)