Cisco Security Agent and the Zotob Worm

Summary

A network Worm has appeared in the wild that targets 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 is a self-propagating network worm 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, since 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 a number of 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 that is stopped varies depending on the variant tested, but up to ten 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

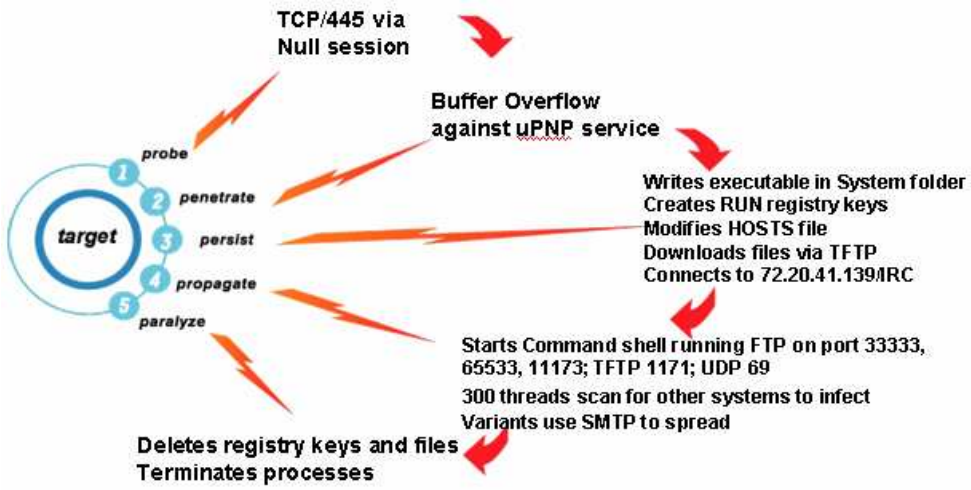

Figure 1. The Zotob Worm (and variants) in action

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, since 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 CSA agents block the worm, they send an alert back to the CSA Management Center (CSAMC) server. This alert contains the IP address of the attacking system. The CSAMC 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. The following is a partial list of prior worms that the CSA has stopped:

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

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

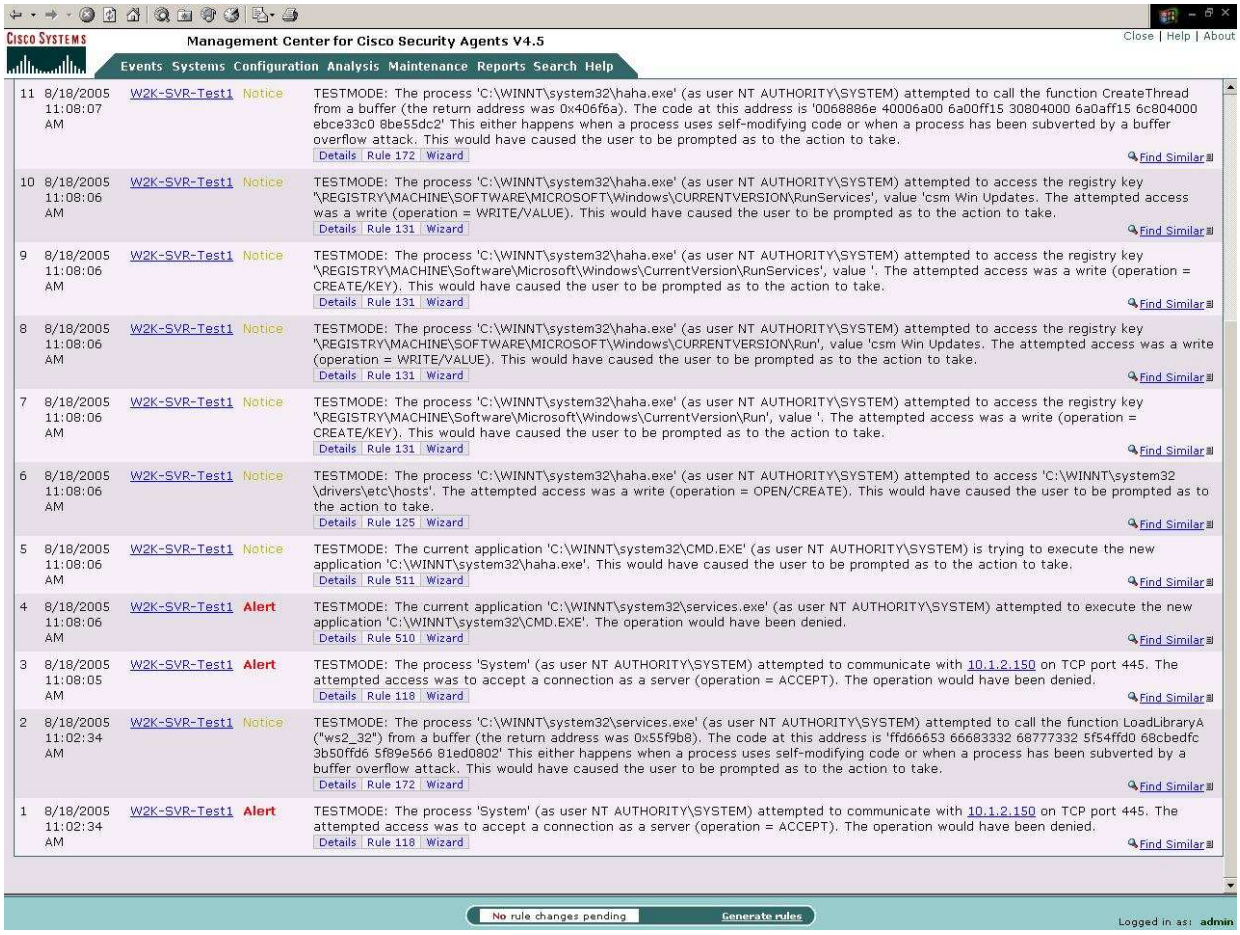

Figure 2. CSA Default Configuration Stops the Zotob.B Worm