McAfee Avert Labs
Protecting yourself from the Conficker worm

Lately we have seen lots of media coverage on how the Conficker worm is going to cause havoc on April 1st. The Conficker worm, formally named W32/Conficker.worm, started infecting systems late last year by exploiting a vulnerability in Microsoft Windows. Since then we have seen a couple of variants of this worm and lots of binaries that carry this malicious payload. Conficker.C is the latest variant; it will change the behavior of its "call-home protocol" on Wednesday, April 1st. Conficker may use this protocol to update itself to include some as-yet unknown functionality. McAfee already offers protection from this worm in its endpoint and network products. Microsoft has also issued a security update to patch the vulnerability that the Conficker family has used to propagate.

The following information will give you an overview of the worm, the steps one can take to clean an infected system, and measures to prevent reinfection.

What is the Conficker worm?

The W32/Conficker worm exploits the MS08-067 vulnerability in Microsoft Windows Server Service. If the vulnerability is successfully exploited, it could allow remote code execution when file sharing is enabled. Machines should be patched and rebooted to protect against this worm's reinfecting the system after cleaning, which may require more that one reboot.

- Upon detecting this worm, reboot the system to clean memory correctly. May require more than one reboot.
- The worm often creates scheduled tasks to reactivate itself.
- The worm often uses autorun.inf files to reactivate itself.

We have identified thousands of binaries that carry this payload. Depending on the specific variant, the worm may spread via LAN, WAN, web, or removable drives and by exploiting weak passwords. Conficker disables several important system services and security products and downloads arbitrary files. Computers infected with the worm become part of an army of compromised computers and could be used to launch attacks on web sites, distribute spam, host phishing web sites, or carry out other malicious activities.

Conficker.C is the most recent variant of this worm and is dependent on its predecessors, the .A and .B variants. Exposure to .C is limited to systems that are still infected with the earlier variants.

Symptoms

- Blocks access to security-related sites
- Locks user out of directory
- Sends traffic through port 445 on non-Directory Service (DS) servers
- Denies access to admin shares
- Places autorun.inf files in recycled directory

Steps to remove Conficker and prevent reinfection

We recommend customers take the following steps to prevent the W32/Conficker.worm from spreading.

1. Clean the infected systems

Use anti-malware solutions such as ToPS for Endpoint to clean the infection. Use the behavioral detections techniques like buffer overflow protection in Host IPS to prevent future infections. This is important because Conficker can propagate via portable media such as infected USB drives. As the media are accessed, the system processes autorun.inf and executes the attack. For more information, read McAfee Avert Labs' document "Combating Conficker Worm."

2. Identify systems at risk of infection

You need to identify which systems are at risk. This list includes systems that either are not patched against Microsoft vulnerability MS08-067 or do not have proactive protection controls to mitigate the vulnerability. McAfee Vulnerability Manager and ePolicy Orchestrator can identify systems that are vulnerable and not protected.

3. Limit the threat's ability to propagate

By using network IPS in strategic points in your network you can quickly limit the ability of the threat to spread, allowing time for you to either update your client anti-virus signatures or modify policies to block the threat using the behavioral controls.

4. All computers must have Microsoft Security Update MS08-067 installed.

McAfee product coverage for Conficker worm

McAfee Product	Coverage
ToPS Endpoint & ToPS Service	The signature (DAT) files include detection and repair for this worm Buffer overflow protection in scan engine and Generic Buffer Overflow in host IPS are expected to cover code-execution exploits. Host IPS also includes signature for "Vulnerability in Server Service Could Allow Remote Code Execution" (CVE-2008-4250)
Network Security Platform (IntruShield)	Includes coverage for "Microsoft Server Service Remote Code Execution Vulnerability"
McAfee Network Access Control (NAC)	Identifies nodes that have not been patched and denies them access to the network unless they are updated
McAfee Vulnerability Manager (MVM)	Includes coverage for MS08-067. Identifies machines vulnerable to infection by Conficker as well as machines infected by Conficker C
McAfee Web Gateway (formerly Webwasher)	Includes signature to detect and block the worm at the gateway

Links and resources

Conficker removal tools and documentation

- Avert Stinger Tool for Removing Conficker
- Combating Conficker Worm: Steps to mitigate risks from Conficker

McAfee Avert Labs blog entries on Conficker

- More Comments Regarding Conficker
- W32/Conficker: Much Ado About Nothing?
- McAfee Debuts ''Combating Threats'' Series
- What Have We Learned From Past Virus Infections?

- New BackDoor Attacks Using PDF Documents
- Shrinking Patch Timelines—The Need for HIPS
- Conficker Worm Using Metasploit Payload To Spread
- Further MS08-067 Woes

McAfee Virus Information Library entries

- McAfee VIL: W32/Conficker.worm
- McAfee VIL: MS08-067—Microsoft Windows Server Service

Please contact your McAfee representative or channel partner with any questions. Call us at 888.847.8766, 24 hours a day, seven days a week.

About McAfee, Inc.

McAfee, Inc., the leading dedicated security technology company, headquartered in Santa Clara, California, delivers proactive and proven solutions and services that secure systems and networks around the world. With its unmatched security expertise and commitment to innovation, McAfee empowers businesses, the public sector, and service providers with the ability to block attacks, prevent disruptions, and continuously track and improve their security.

McAfee®

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com