

Battling the Conficker Worm

A McAfee Network Security Platform Update

Lately we have seen lots of media coverage on how the Conficker worm is going to cause havoc on April 1. 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 could activate on April Fool's Day. McAfee already offers protection from this worm in its endpoint and network products. Microsoft has also issued a security update to patch this vulnerability. The following information will give you an overview of the worm, and answers to frequently asked questions.

Overview

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 than 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.

For more information regarding the steps you can take to clean an infected system and for measures to prevent a reinfection, please refer to "Finding W32/Conficker.worm," at http://download.nai.com/products/mcafee-avert/documents/combating_w32_conficker_worm.pdf.

McAfee Network Security Platform Coverage for Conficker Worm

McAfee Product	Coverage
Conficker.A	NSP includes coverage for "Microsoft Server Service Remote Code Execution Vulnerability"
Conficker.B	NSP includes coverage for "Microsoft Server Service Remote Code Execution Vulnerability" and has additional signatures to detect Netbios brute-force attacks: NETBIOS-SS: NULL Credentials Login and NETBIOS-SS: Guest Login Succeeded

Conficker.C	NSP includes the following protocol-anomaly signatures: HTTP: Suspicious Time Check Detected P2P: Suspicious UDP Probe WORM: W32/Conficker.C Activity Detected
-------------	---

Frequently Asked Questions

Am I protected from Conficker?

The sigset release of October 23, 2008, includes the signature "NETBIOS-SS: Microsoft Server Service Remote Code Execution Vulnerability," which provides coverage for Conficker.A and Conficker.B. The signature has blocking enabled by default, if you are using default inline IPS policy.

The sigset release of March 30, 2009, includes the signatures "HTTP: Suspicious Time Check Detected," "WORM: W32/Conficker.C Activity Detected," and "P2P: Suspicious UDP Probe," all of which provide coverage for Conficker.C.

How does Conficker.A propagate?

The W32/Conficker.A worm exploits the [MS08-067](#) vulnerability in Microsoft Windows Server Service.

How does Conficker.B propagate?

The W32/Conficker.B worm also exploits the [MS08-067](#) vulnerability in Microsoft Windows Server Service. Aside from the exploit, it can spread over Netbios file shares or via removable media (such as USB drives, etc.). You can find detailed analysis in this [Avert Labs Paper](#).

How does Conficker.C propagate?

Conficker.C does not exploit MS08-067. Conficker.C is just an *update* to previous Conficker versions. It depends on its predecessors to succeed. It has no propagation or spreading mechanism of its own, other than updating itself from the .A or .B versions (via HTTP-signed downloads). Conficker.C requires a successful, active MS08-067 exploit to spread itself.

A machine has triggered the alert "NETBIOS-SS: Microsoft Server Service Remote Code Execution Vulnerability." What does that mean?

The Conficker.A/B worm is "noisy" in nature and tries to spread itself by exploiting more machines. If you see the alert "NETBIOS-SS: Microsoft Server Service Remote Code Execution Vulnerability" from a host, it is highly possible that the machine is infected by Conficker.A/B. If you have the signature configured for blocking (the default inline IPS policy), the attack should be prevented.

A machine has triggered the alert "NETBIOS-SS: NULL Credentials Login" or "NETBIOS-SS: Guest Login Succeeded." What do they mean?

Conficker.B can also propagate via network shares, and will trigger these one of these two alerts on NSP.

A machine has triggered “WORM: W32/Conficker.C Activity Detected” alert. What does it mean?

It is highly possible that the machine is infected by Conficker.C and is probing your network for its peers.

A machine has triggered “HTTP: Suspicious Time Check Detected” alert. What does it mean?

This is a protocol-anomaly check. Conficker.C makes use of a known technique to synchronize the clock on the infected machine. This alert can also be triggered by benign traffic in certain environments.

What makes Conficker.C different from Conficker.A/B?

Variant .C represents the third major revision of the Conficker malware family. This version is a significant revision to Conficker.B. Unlike its predecessor, Conficker.C does not exploit MS08-067. Two new network activities can be observed from a .C infected machine: internet probing and peer-to-peer (P2P) communications.

What is the network behavior of Conficker.C?

Conficker.C makes use of a proprietary P2P-like protocol. It generates both UDP and TCP packets to locate its peers. The source and destination ports used for these packets are generated dynamically and may be used as a mechanism to identify infected nodes via network-flow analysis. McAfee NSP has implemented such heuristic checks in the sigset Versions 4.1.46.16 and 5.1.16.15 to detect Conficker.C activity. The UDP probes are excessive in number. We observed more than 50,000 probes from one infected machine in one day.

Conficker.C also generates a random list of 50,000 domain names. From this list, each infected node appears to pick 500 domains to contact each day. These domains are resolved and “filtered.”* The infected system will then attempt to download a digitally signed binary from these sites. (*Filtering means that all HTTP GET requests that are created by Conficker will have an IP address host value that passes Conficker’s internal filtering functions.)

Conficker.C also makes use of a known technique to synchronize the clock on an infected machine. It sends an HTTP request to a list of popular websites. Once Conficker receives a response, it changes the system time on the infected machine based on the date and time stamp inside the HTTP response header.

If I am not affected by Conficker.A/B, how dangerous is Conficker.C?

As far as our research tells us, Conficker.C relies on previous versions of the Conficker family to propagate. If you have a machine with the MS08-067 patch installed and that is clean of Conficker.A/B, it is highly unlikely to be infected by Conficker.C. McAfee Avert Labs is closely monitoring the situation and will update this document with the latest developments.

I suspect a machine is infected. Should I remotely connect to the machine and debug it?

We do not recommend this.

When the Conficker worm infects a machine, it scans the local network and attempts to infect

machines using the credentials of the currently logged-on user. If the initial login attempt fails, then the worm attempts a brute-force attack to authenticate, using a [hard-coded list of passwords](#). Because most organizations have enforced complex password policies, brute-force attacks are ineffective. However, the moment an administrator logs onto the affected machine using his or her domain account, Conficker runs using the elevated credentials of the domain administrator. The worm can immediately infect any host on the domain using these newly acquired credentials.

To prevent such an outbreak from happening, it is imperative that administrators refrain from logging onto a suspect machine using their own accounts. Logging on using the workstation's local administrator account can also have the same effect; most corporate workstations are ghosted from the same image and could have the same local admin account and password. For more details, please refer to the [Avert Labs Blog](#).

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

McAfee and/or additional marks herein are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.
© 2009 McAfee, Inc. All rights reserved.