



ICASI Alert

Updated: Conficker Malware Threat

Introduction

ICASI is releasing this alert to provide guidance on issues that have been raised regarding the behavior of the Conficker malware. Historically, once botnets reach a sufficient size, their purposes tend to evolve and change organically to meet the needs of the owners. This trend is likely to also occur with Conficker, and many supporting indications have already been observed. Readers are advised to check the resources linked within this alert regularly to ensure they are armed with the latest information concerning Conficker.

This alert provides a consolidated view and information from ICASI member companies.

What is the threat?

The Conficker worm has grown to be a large active botnet. At this time Conficker affects a variety of Windows operating system platforms, including Windows 2000, XP, Vista and Server 2003. While systems which did not apply the Microsoft update MS08-067 were initially compromised through this vulnerability, the majority of current infections are occurring via open fileshares, weak passwords, shared USB devices and socially engineering efforts that trick users into installing this malicious code.

Analysis and observation of this most recent variant of Conficker malware reveals a change in the method the worm utilizes to communicate from infected systems back to the operators of the botnet. This change will likely be utilized to propagate additional capabilities to the malware itself, and will likely include modifications to current behaviors and symptoms. At this time, the method the botnet operators have chosen to alter the behavior of the infected systems is not known.



However, as with most botnets the continued evolution of the malware to fit the needs of the operators is likely.

The evolution of Conficker has shown that the authors are skillful and conversant in the defenses that are deployed against them. Conficker already takes advantage of a number of weaknesses that could be avoided through good security practices. We encourage the review of security Best Practices on a regular basis to minimize the impact of any malware attack.

What is the impact to enterprises?

Computers infected with this malware could experience operating system integrity and availability issues. These issues could result in loss or exposure of data assets to which the systems have access.

More specifically, compromised computers could be used in Distributed Denial of Service attacks, SPAM transmission, click-thru fraud, information loss via keystroke logging and subsequent retrieval of data files residing on compromised computers. This type of malware often opens connections to remote systems and downloads additional malware.

While Conficker does represent a threat to the enterprise, the current size of the botnet is not unprecedented.

What can be done to mitigate this threat?

Many of the steps that mitigate propagation of this malware are fundamental to sound enterprise security practices. Due to the blended nature of Conficker, the following multiple actions are required

- Stay current with software updates – for Conficker specifically, this means MS08-067.
- Use strong passwords, particularly on system and network

fileshares.

- Disable autorun for shared media storage devices such as USB.
- Quickly identify compromised systems and immediately isolate and remediate them.
- Ensure your antivirus/anti-malware systems are up to date.
- Be alert for social engineering attacks, such as attachments in email or messenger clients could contain a vulnerability.
- Ensure that enterprise and host based firewalls are enabled and securely configured.

Additional Information:

Additional information and detailed analyses have been made available by ICASI members at the links below:

Microsoft has provided a consolidated information page concerning the Conficker worm at the following link:

<http://www.microsoft.com/conficker>

Cisco Systems has provided several documents via the Cisco Security Center regarding the Conficker worm at the following links:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=17121>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=16944>

A collection of Cisco-provided Best Practice documents can be found at the following link:

<http://tools.cisco.com/security/center/intelliPapers.x?i=55>



IBM has produced a document from ISS X-Force that can be found at the following link:

<http://www.iss.net/threats/conficker.html>

Aliases/Variants

Conficker is also commonly known as:

Conficker.C

Conficker.D

Downadup.C