

Conficker Update 3/26/2009

This is serious.

The Conficker worm is set to activate on April 1 and an estimated 12 million machines have been infected.

Microsoft posted a bounty of \$250,000 (a quarter of a million US dollars) to find the person(s) responsible for Conficker.

Variant "C" of Conficker is thought to have been released March 4th and is an extremely professionally written piece of code.

It employs very sophisticated encryption protocol. It uses Dr. Rivest's latest MD-6 algorithm and the author(s) of Conficker updates it within days of any revisions to MD-6.

Variant "C" increased the number of rendezvous points to 50,000 randomly generated domain names.

It employs P2P communication over TCP and UDP channels to coordinate with peers and update itself.

It is "able to terminate, disable, reconfigure, or blackhole native operating system (OS) and third-party security services."
SRI International Technical Report

To quote SRI:

Finally, we must also acknowledge the multiple skill sets that are revealed within the evolving design and implementation of Conficker. Those responsible for this outbreak have demonstrated Internet-wide programming skills, advanced cryptographic skills, custom dual-layer code packing and code obfuscation skills, and in-depth knowledge of Windows internals and security products. They are among the first to introduce the Internet rendezvous point scheme, and have now integrated a sophisticated P2P protocol that does not require an embedded peer list. They have continually seeded the Internet with new MD5 variants, and have adapted their code base to address the latest attempts to thwart Conficker. They have infiltrated government sites, military networks, home PCs, critical infrastructure, small networks, and universities, around the world. Perhaps an even greater threat than what they have done so far, is what they have learned and what they will build next.

Please see the entire SRI Technical document at: <http://mtc.sri.com/Conficker/addendumC/>

Please see the SANS Internet Storm Center Diary entry for additional Conficker information at:

<http://isc.sans.org/diary.html?storyid=5860>

TippingPoint and Conficker

How Can TippingPoint Protect Your Network?

IPS Note:

It is extremely important to have deployed IPS units within the core or the network as well as the perimeter for maximum effective protection.

The IPS units only take action based upon the packets that actually pass through them. Therefore if the IPS units are only on the perimeter they will function extremely well blocking any MS-RPC attacks coming in

from outside the network. However they will be of limited value in detecting any internal propagation of the attacks or the brute password cracking attacks.

1) The TippingPoint IPS units provide excellent protection against the first attack vector. They have had DV filters for the MS-RPC vulnerabilities for years.

TippingPoint IPS units with current Digital Vaccines provide protection against the Conficker/Downadup Worm with 4 filters that cover the MS08-067 vulnerability (MS-RPC) and they are enabled to Block + Notify by default. They are:

5457: MS-RPC: Microsoft Server Service Buffer Overflow

6515: MS-RPC: Microsoft Server Service Buffer Overflow

6545: MS-RPC: Microsoft Server Service Buffer Overflow

6565: MS-RPC: Microsoft Server Service Buffer Overflow

Verify that these filters are Enabled to Block+Notify in your currently distributed profiles.

2) TippingPoint IPS and SMS units can be a major assistance in locating and isolating the second vector to detect and block the brute force password attacks by enabling these filters:

1400 SMB: Windows Logon Failure

1660 SMB: Windows Logon Failure

2178 SMB: ADMIN\$ Hidden Share Access

2796 SMB: Windows Repeated Logon Failure (Possible Brute Force)

6863 KERBEROS Authentication ERROR (TCP)

6864 KERBEROS Authentication ERROR (TCP)

The IPS units will detect multiple failed logon attempts with these filters. Then the SMS can have a quarantine action set created to take appropriate action if the failed logon attempts exceed a reasonable number per time period (not just a user fat-fingering their password).

The brute force password attack will trigger the quarantine action set and the attacking host can be identified and network security alerted, or the compromised host can be placed into quarantine. The SMS quarantine action can work with managed switches to place the attacking host into a quarantine VLAN or execute a port shutdown at the switch totally isolating the host from the network at the switch port level.

3) The third attack vector is outside the domain of any network Intrusion Prevention System. Disabling AutoPlay on the PCs is not reliable, see CERT Technical Cyber Security Alert TA09-020A, so the best action is to disable the use of all removable devices, particularly USB memory sticks, with AD Group Policies or third-party software.

Latest from TippingPoint: (3/26/09)

"Folks,

We are looking at Conficker.C with the hope to have new filters available next Monday/Tuesday in time for April 1. We will update the mailing list when we have more information.

Wayne Blackard

TippingPoint Technologies, Inc."

Defense in Depth!

Immediately:

- Verify that all PCs, servers, and any device running an MS operating system have all the Microsoft patches to date applied. Don't forget Virtual Machines.
- Verify that all PCs are running AV software and that all the .dat files are up to date.
- Pay special attention to laptops.
- Route VPN and other "trusted" outside connections through an IPS before entering the network.
- Check all firewall, IDS, and syslog server logs, especially for "phone-home" traffic to the Conficker sites.

Thoughts:

Methodically execute your incident response plan. If you don't have one, create one now. Plan the response and then execute the response. If you're playing "Whack-a-Worm" you'll miss one and lose your network.

Robert Kerr, CISSP

EVP CTO

NetSpec, Inc.

A TippingPoint Elite and NAC Authorized Partner

446 Catalina Dr., Newport Beach, CA 92663

TEL 949.515.5127, FAX 949.515.5182, Cell 949.705.7593