

TippingPoint and the Conficker/Downadup Worm

The Conficker/Downadup worm appeared in October 2008 and has now infected almost 10 million PCs and is spreading fast.

It is creating one of the largest botnets to date. The real exploits and damage will most likely appear later when the infected machines in the botnet are activated in the compromised networks to extract business critical data, Intellectual Property, personal information, mount Distributed Denial of Service attacks within and without the network, become SPAM generating networks, and so on.

It is a blended attack using three attack vectors to propagate:

- 1) an exploit against the Microsoft RPC the MS08-067 vulnerability,
- 2) a brute force dictionary password attack against administrator passwords to install itself through Microsoft ADMIN\$ shares, and
- 3) it installs itself into removable storage devices, USB memory sticks, and uses Windows' removable device AutoPlay to startup and present the user a specially crafted AutoPlay prompt that tricks the user into executing the worm.

This blended threat is the perfect example why we need Defense in Depth in our networks.

How Can TippingPoint Protect Your Network?

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

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.

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.

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

References:

<http://en.wikipedia.org/wiki/Conficker>
<http://isc.sans.org/diary.html?storyid=5695&rss>
http://www.f-secure.com/v-descs/worm_w32_downadup_al.shtml