

# TippingPoint Digital Vaccine Filter Updates for Conficker

Today TippingPoint released 6 new DV filters specifically aimed at Conficker. They were released in:

## Digital Vaccine #DV7670

March 30, 2009

The Release Notes make no reference to Conficker but the Conficker filters are:

0137, 0171, 6924, 6934, 6945, and 6946.

Descriptions from "Filter Details" are:

**0137:** This filter detects ICMP Destination Unreachable packets (type = 3). A Destination Unreachable error message is sent by a router or host when the original packet cannot be delivered as specified. This filter is intended for catching all ICMP Destination Unreachable responses. A series of ICMP Destination Unreachable responses sent to an individual system is indicative of an infected system that is scanning for possible victims or Command/Control servers, **such as Conficker.C**. This filter is designed to be used with thresholding values. Upon reaching the configured threshold, a Quarantine Action can be used to isolate the infected system. A baseline of number of Destination Unreachable responses per hour should be established for a network, and any number of hits on this filter greater than 150% of that baseline should be treated with suspicion.

**0171:** This filter detects ICMP Time Exceeded packets (type = 11). In particular, this signature detects the error code "Time to Live exceeded" (code = 0). A Time To Live Exceeded error message is sent by a router when the Time To Live (TTL) field of the packet reaches zero (the packet is also dropped). This error code was defined in the original ICMP RFC 792. A series of ICMP Time Exceeded responses sent to an individual system is indicative of an infected system that is scanning for possible victims or Command/Control servers, **such as Conficker.C**. This filter is designed to be used with thresholding values. Upon reaching the configured threshold, a Quarantine Action can be used to isolate the infected system. A baseline of number of Time Exceeded responses per hour should be established for a network, and any number of hits on this filter greater than 150% of that baseline should be treated with suspicion.

**6924:** This filter detects a normal Domain Name System response indicating that the requested name does not exist. This could be due to a typing mistake by a user, but a large number of such responses could indicate a domain enumeration attack. This filter is designed to be used with the Quarantine feature to block hosts making continuous DNS queries to domains that do not exist. This may be indicative of a host infected with a worm, **such as Conficker.C**. A baseline of number of NXDOMAIN responses per hour should be established for a network, and any number of hits on this filter greater than 150% of that baseline should be treated with suspicion. Hosts that generate several events of this type in a short period of time may be infected with a worm. Note that recursive nameservers may generate large numbers of these events on behalf of clients, so nameservers should be explicitly whitelisted from firing this filter.

**6934:** This filter detects a suspicious HTTP GET Request that may be an indication of a worm activity. This filter is designed to be used with the Quarantine feature to block hosts making HTTP requests that looks suspicious. This may be indicative of a host infected with a worm, **such as Conficker.C**. Note: This filter might also match on HTTP requests from users not accepting cookies.

**6945:** This filter detects the transfer of a Microsoft Windows executable program over high ports. Some organizational security policies prohibit end users from downloading and installing untrusted applications from the Internet. Additionally, many web-based exploits can leverage browser vulnerabilities to silently **download keystroke loggers, Trojans, or other malicious software**. Enabling this filter to block will prevent the download

of Windows applications over high ports. Note that this includes non-malicious executables, such as Microsoft Hotfixes and other normal Windows utilities. If this filter fires, the destination IP address indicates the computer which attempted to download such a file.

**6946:** This filter detects the transfer of suspicious files across the network. **These files have been linked to the Conficker worm** and are seen transferred after an infection. The worm attempts to disguise such files as innocuous or unrelated, as a result, this filter may fire on files that unrelated to Conficker but that share certain characteristics.

**Please note that they filters were distributed with their Recommended settings as Disabled.**

The Modified filters in the DV release are also Conficker oriented filters.

I set all of these in the IPS protecting the NetSpec network to Block + Notify + Email.

I personally suggest that you do the same until at least mid-April. But exercise the same caution and planning that you have used in the past when you made any filter modifications away from the **Recommended** mode. Be particularly careful with any Profiles used by internal network physical or virtual segments, i.e. those not on the Internet facing edge.

That makes the full complement of filters from TippingPoint for Conficker to be:

1) 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

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 (UDP)  
6864 KERBEROS: Authentication Error (TCP)

3) Just released filter in **Digital Vaccine #DV7670, March 30, 2009**

0137, 0171, 6924, 6934, 6945, 6946 as discussed above.

If you have any questions feel free to give me a call immediately, (949) 515-5127.

## 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  
[rkerr@netspec.com](mailto:rkerr@netspec.com)  
[www.netspec.com](http://www.netspec.com)

---

You have received this email because you are a NetSpec, Inc. client or have expressed an interest in NetSpec services or products. If you do not want to receive future emails or newsletters from NetSpec please send an email with "Remove" in the subject line to: [rkerr@netspec.com](mailto:rkerr@netspec.com). Thank you.