

Conficker Survival Guide – April Fools' Edition

March 30, 2009

Summary

The Conficker worm, also known as “Downup” or “Downadup”, is a worm that was originally discovered in October, 2008. As of this writing, three variants are known and named variants “A”, “B” and “C” accordingly. There are estimates that thus far, more than 10 million hosts have been infected. The third and latest variant (as of this writing) is rumored to spread on a massive scale on April 1st and as such, has garnered the attention of many major media outlets. This document describes how TippingPoint customers can go about putting countermeasures in place before April 1st, when the worm is expected to do the most damage.

Conficker Background Information

Since its initial discovery, the Conficker worm has evolved from a run-of-the-mill server exploit worm to a serious one with mass infection (and thus, DoS) potential. Initially, Conficker first infects its victim by exploiting a known Microsoft server vulnerability, known as MS08-067. This is a server buffer overflow vulnerability that gives the attacker remote code execution capabilities.

The worm basically spreads itself by exploiting the aforementioned vulnerability and then downloading the malicious payload from the Internet. Initial infections were introduced via an infected USB flash drive. Then in the next variant, propagation was achieved by spreading itself over named pipes (standard Windows communications). In the latest variant of the worm, payloads are propagated via an ad-hoc peer-to-peer network, negating the need for downloading the payload from the Internet.

There is one aspect of Conficker.C that is worrying everybody, and that is that it will apparently try to connect to up to 50,000 random domains per day, starting April 1st, 2009. For those people out there who have not patched their Windows server by then, it will be a nasty April Fools surprise indeed, especially with all the media attention the worm has received up to that point.

Detecting and Preventing Conficker

TippingPoint users can protect their networks from the spread of this latest (and arguably most dangerous) version of Conficker by utilizing a combination of IPS filters and the SMS Responder (aka “SMS Quarantine” in pre-SMS v. 2.6) feature.

There are several filters that were released in October, 2008 to protect against the MS08-067 vulnerability. These filters should be used to protect unpatched Windows servers that could be potential exploit vectors for the worm. 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

The filters above are all set to Block/Notify by Recommended Settings. No further action is necessary.

The following filters were released by TippingPoint on March 30, 2009, and can be used to detect and block the propagation of the latest variant of Conficker. Please note that some of the following filters will need to be used in conjunction with the SMS Responder feature in order to avoid false positives. Details on how to go about this will follow the list of filters.

137: ICMP: Destination unreachable (All Codes) Response
171: ICMP: Time-To-Live Exceeded in Transit
6924: DNS: NXDOMAIN Response
6934: HTTP: Suspicious (Possible Worm) HTTP Request
6945: TCP: Microsoft Windows Executable Transfer Over High Ports
6946: TCP: Suspicious File Transfer

Filters 137 and 171 should be used in an SMS Responder policy for alerting purposes. Conficker tries to identify other potentially vulnerable hosts by way of large scale UDP and TCP port scanning. We expect many hosts to respond with "Destination Unreachable" and "TTL Exceeded" responses. Thus, a threshold can be set to alert administrators when a high number of these filter hits are reported. Users should implement this SMS Responder policy before April 1st to try to determine what is considered normal for their networks. Then the thresholds should be adjusted accordingly.

Filter 6924 detects the "NXDOMAIN" response. On April 1st, infected systems are expected to begin making up to 50,000 random DNS requests on a daily basis. Because most of these domains will be non-existent, we expect a large number of "NXDOMAIN" responses. Filter 6924 can be used in its own SMS Responder policy to alert administrators of a large number of hits from this filter. Similar to the use case for filters 137 and 171 above, the SMS Responder policy utilizing this filter should be implemented prior to April 1st to establish a baseline of what is considered a normal amount of activity, and then the thresholds should be adjusted accordingly. Note: If you choose to use the IPS Quarantine action set either by itself or as part of an SMS Responder action set, you should whitelist the DNS server so that it won't accidentally get quarantined.

Filters 6934, 6945 and 6946 should be deployed with the following considerations.

Filter 6934 detects a suspicious HTTP GET request that the Conficker worm uses specifically. However, the GET request looks very similar to Internet Explorer GET requests so this filter may block legitimate traffic depending on where it is deployed. For example, if a server farm does not have any web applications or should not have any users on it that should be browsing the Internet; this filter can probably be enabled to Block + Notify. On the other hand, for Internet perimeter segments or any other segment where web browsing occurs frequently, this filter should be used with the IPS Quarantine action set (blocks based on x number of hits in y minutes) with appropriate thresholds. Alternatively this filter can also be put in its own SMS Responder policy for notification only.

Filter 6945 detects the transfer of Microsoft Windows executables between two high ports. Conficker utilizes this method, and as such, this filter may be used to block the transfer of malicious payloads. This filter can be deployed similarly to any other filter that is disabled by Recommended Settings. It can either be deployed initially in "Permit + Notify" or "Block + Notify" right away. Setting the filter to Permit + Notify initially allows the administrator to determine if there are any potential false positives and put

in exceptions before changing the filter to Block + Notify. Setting the filter to Block + Notify right away may cause false positives that exceptions would need to be created for after the fact. Choose the appropriate setting for your environment.

Filter 6946 detects suspicious file transfers known to be associated with Conficker. This filter should be deployed with the same considerations as filter 6945 above.

Summary

The Conficker worm has shown us that it is not easy or simple to stop the “intelligent” worms of today’s threat landscape. We must adapt and improvise whenever possible to keep up with the latest and greatest. By using the TippingPoint IPS, its filters and SMS, we can go a long way towards mitigating and stopping these threats.

If you have any questions about any of these filters or features mentioned in this document, please consult your local TippingPoint SE.

References

<http://mtc.sri.com/Conficker/>

<http://en.wikipedia.org/wiki/Conficker/>

<http://dvlabs.tippingpoint.com/>