



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

March 31, 2009

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2009-018

SUBJECT: April 1, 2009 – Conficker C Activation

Since its emergence in November 2008, the Conficker worm, also known as Downadup, has gone through several variations. The current variant of the malware, first observed March 6, 2009, is known as Conficker C. This variant contains logic that will become active on April 1, 2009. The exact nature of the activity that will occur on that day is not known at this time. It is known that the malware will begin querying domains for new instructions/payload, as it has done in the past. It is critical that currently infected systems are cleaned before April 1. It should be noted that Conficker C no longer spreads like the previous versions, making detection of infected hosts more difficult. The current variant has added additional defenses against detection and removal, such as disabling Windows services, anti-virus products and analysis tools and preventing the infected host from reaching security-related websites.

All machines in your organization should have the patch to MS08-067 applied, disabled Autorun/Autoplay and ensure strong passwords are used on network shares. The removal of Conficker C is hindered by the various defenses, including blocking the patch from being applied. The best method of remediation of a Conficker C infected host is to wipe the host and reinstall.

RECOMMENDATIONS:

We recommend the following actions:

- Use the Microsoft Malicious Software Removal Tool to scan for the Conficker C worm on your hosts.
- Remove any infected hosts from your network immediately and rebuild them to a known clean state.

REFERENCES:

SRI:

An Analysis of Conficker C
<http://mtc.sri.com/Conficker/addendumC/>

F-Secure:

Questions and Answers: Conficker and April 1st
<http://www.f-secure.com/weblog/archives/00001636.html>

Byron Acohido:

Timeline

<http://lastwatchdog.com/evolution-conficker-globe-spanning-worm/>

Microsoft:

Malicious Software Removal Tool

<http://www.microsoft.com/security/malwareremove/default.mspx>

Secureworks:

Conficker Analysis

<http://www.secureworks.com/research/threats/downadup-removal/>