

9

CC: Adam

Lashway, Lisa

From: egg@dca.state.nj.us
Sent: Tuesday, March 31, 2009 9:32 AM
To: Lashway, Lisa
Subject: Conficker Worm

Dear Municipal Clerk:

This is to notify local officials that there a computer worm, known as Conficker worm that is scheduled to affect Microsoft Windows-based computers on April 1, 2009. The worm lets an outside user control certain aspects of the computer and cause malicious damage. Recipients of this e-mail should take appropriate local action to ensure their computers are protected. Details on this have been previously sent to members of the Technology Coordinator's List Serve maintained by the DLGS. To sign up for this useful List Serve, go to: <http://www.nj.gov/dca/surveys/tcsurvey.htm>.

By this time, Microsoft systems should have been updated to protect against the worm. What follows below is information from Microsoft to help users by providing answers to common questions, steps that can be taken to protect their systems, and steps that can be used to recover systems that have been infected.

Answers to Common Questions

Q: What will happen on April 1, 2009?

A: Based on our collective technical analysis, we've determined that systems infected with the latest version of Conficker will begin to use a new algorithm to determine what domains to contact. We have not identified any other actions scheduled to take place on April 1, 2009.

Q: Will an updated version of Conficker go out to already-infected systems on April 1, 2009?

A: It is possible that systems with the latest version of Conficker will be updated with a newer version of Conficker on April 1, 2009 by contacting domains on the new domain list. However, these systems could be updated on any date before or after April 1, 2009 as well using the "peer- to-peer" updating channel in the latest version of Conficker.

Q: Should the general public be alarmed? Why or why not?

A: No, the general public should not be alarmed. Most home users and non-networked PCs have been protected by Microsoft Security Update MS08-067 (<http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx>) being applied automatically.

Q: What should people who are worried about April 1, 2009 and Conficker do?

A: We recommend that home users and non-networked users who have not yet enabled automatic updates do so and ensure their security software is up to date with the latest antivirus signatures for Windows Live OneCare, or the antivirus product they use.

If you run your own network, your network administrator should have taken action to protect your systems by now. If not. It is recommended that network or system, administrators should continue to focus on the guidance from Microsoft and take multiple measures to minimize the risk of getting infected:

- Fully Install MS08-067 (<http://www.microsoft.com/technet/security/bulletin/ms08-067.msp>) on all Windows computers in your environment. Because 100 percent deployment can be challenging in diverse enterprises, the next defense-in-depth steps can help minimize the risk too.
- Use an antivirus product that has solid detection of Conficker. Such an antivirus program should be able to block the worm from copying itself to other machines.
- Use strong passwords both for any user account and also for any file share in your environment.
- Make sure to use only AutoPlay options that you are familiar with as other options may have been added by malicious software. Some customers may prefer to disable the AutoRun functionality altogether.
- Evaluate additional security best practices in accordance with their organization's policies and procedures.

Customers who believe they are affected and need additional support can contact Microsoft Customer Service and Support. Contact CSS in North America for help with security update issues or viruses at no charge using the PC Safety line (866) PCSAFETY or resources found at: <http://www.microsoft.com/protect/support/default.msp>.

Resource summary:

Microsoft has published new information today on the following web pages:

- Microsoft Conficker guidance page for IT Professionals and those focused on security in the enterprise: <http://www.microsoft.com/conficker>.
- Microsoft Conficker guidance page for consumers and home users: <http://www.microsoft.com/protect/computer/viruses/worms/conficker.msp>.
- The Microsoft Malware Protection Center (MMPC) encyclopedia page for the Conficker family of malware: <http://www.microsoft.com/security/portal/Entry.aspx?name=Win32/Conficker>.
- The Microsoft Malware Protection Center blog: <http://blogs.technet.com/mmpc/>.
- The Microsoft Security Response Center Blog: <http://blogs.technet.com/msrc/>.

THIS E-MAIL HAS BEEN SENT TO THE FOLLOWING OFFICIALS: Municipal Clerk, County Clerk to Board of Freeholders, Authority Officials, Fire District Officials.

PLEASE REMEMBER: If your e-mail address changes please make the change to your GovConnect User Profile. If you change employers please send us the details by replying to this e-mail. Helpdesk 609.943.4724