

Protecting Your Organization Against Conficker

The Conficker worm was first released in late 2008 and by late January 2009, infections had topped 15 million systems. Security researchers have discovered that on April 1, Conficker will change how it updates itself, making it extremely difficult to mitigate and protect unpatched systems. Conficker may also take advantage of April 1 to wreak more havoc on compromised systems. Whether April Fool's Day triggers mass denial of service, data destruction, or simply pop up banner ads, it is critical to protect vulnerable systems. And security experts agree that patching is the most effective deterrent for Conficker.

How nCircle Can Help

nCircle provided coverage for the vulnerability required for the Conficker worm to compromise a system (MS08-067) shortly after Microsoft released the patch on Thursday October 23rd 2008. Even though this patch was not released on Patch Tuesday, nCircle VERT still released coverage in less than 24 hours.

Additionally, on March 30, 2009 nCircle released additional checks that can positively identify systems already compromised by the Conficker worm. Together, the checks ensure that nCircle customers can easily and automatically identify *any vulnerable systems* as well as any system that is *already compromised by the Conficker worm*.

Conficker takes specific action to disable anti-virus programs and other host countermeasures. It cannot, however, disable or interfere with nCircle's agentless scanning solutions since there is no agent to tamper with or disable. nCircle will ensure each system is audited and administrators are alerted to any changes or problems, including disabled anti-virus.

Some key tasks that enterprises must perform to protect themselves from Conficker include:

- Make sure operating systems and applications are patched. Up-to-date operating systems and applications have less known vulnerabilities. Also ensure any installed anti-virus and anti-malware applications are up to date and running.
 - ✓ nCircle can scan systems to ensure that the vulnerability required for the Conficker worm to compromise a system (MS08-067) has been patched.
 - ✓ nCircle can scan systems automatically and regularly to ensure operating systems and applications are generally up to date, including service packs and software and security updates.
 - ✓ nCircle can scan the network and produce a list of systems that remain vulnerable to the Conficker worm.
 - ✓ nCircle can scan the network to ensure that anti-virus is installed, running, and up to date on all specified systems.

Read More on the nCircle Blog

nCircle's Andrew Storms blogged about this topic back in January in his post "Protecting Your Enterprise from Conficker": http://blog.ncircle.com/blogs/sync/archives/2009/01/protecting_your_enterprise_fro.html

About nCircle's 24-hours SLA

nCircle has committed to our customers to provide vulnerability checks, within 24 hours, for all critical Microsoft Security Advisories. With this guarantee, nCircle's customers can be assured that within 24 hours of the announcement of the critical vulnerability by Microsoft, nCircle will provide a check with which they can test their systems for the vulnerability. No other vulnerability management vendor has made such a commitment to its customers.

A Note on Protecting Home Systems

While most people will focus on enterprise systems, home systems should not be ignored. Home users should also ensure that their systems are up to date and patched using the built-in Microsoft update. It's a good idea to check and make sure anti-virus programs are up to date and running on home systems as well.