



THE TEK REPORT



Presented by Call-a-Tek

www.callatek.net

March/April 2009 Issue

614-447-9514

SecurityNewsPortal

Multiple vulnerabilities found fixed in OpenSSL

Malicious Web Site / Malicious Code
 SEO Poisoning
 Major Chinese Game Duowan Spoofed Web Site
 Serving Trojan Ranked Top in Ba

New BIOS attack renders antivirus useless

Troj/Delf-FBT

Troj/Bifrose-XB

Troj/Bdoor-AUK

Troj/Banker-EQR

Troj/Bancos-BFJ

Troj/Agent-JJO

Troj/Agent-JJN

Troj/Agent-JJM

Troj/Agent-JJI

Mal/Caco-A

TrojanDownloaders

TrojanDownloaderAg

Conficker worm confounds security experts

The Conficker worm (aka Downadup, officially named Win32/Conficker and Win32.Worm.Downadup.Gen) has surprised security researchers by becoming the first major computer threat of 2009, as well as the most perplexing virus/worm in several years.

Since its emergence in October 2008, Conficker has gradually infected millions of computers worldwide. Finnish security company F-Secure estimated that Conficker managed to infect over a million computers on a single day in January 2009. Microsoft issued its Security Bulletin MS08-067 in October to patch the vulnerability in the SVCHOST.EXE file that allows remote code execution. Nevertheless, estimates of PC infections by Conficker range from two million to 12 million computers worldwide with the potential to become the largest "botnet" in existence.

One of the biggest concerns the Conficker worm presents is that on April 1st, all of its infected hosts will contact its creators to receive further instructions which are presently unknown. These instructions could include commanding its botnet to issue a massive Denial of Service (DDoS) attack on a high-profile website or websites, or to serve some other nefarious purpose. Of additional concern are the two additional variants of the worm that have emerged in recent months, dubbed Conficker.B and Conficker.C.

In an effort to combat the Conficker worm, researchers from Microsoft and the Internet Corporation for Assigned Names and Numbers (ICANN) formed a group dubbed the "Conficker Cabal." The group has attempted to track the worm's origins, and worked to disrupt Conficker's attempts to contact its programmers. Microsoft has even offered a \$250,000 bounty for information leading to the capture of Conficker's creators.

There are several steps users can take to prevent and remove the infection. First, users should be sure their PCs have installed the most recent Windows Update, especially the **MS08-067** patch. (Microsoft's Malicious Software Removal Tool has also been checking for and removing Conficker infections since December.) Second, users can download free tools built to remove the Conficker infection made by **BitDefender**, and the aforementioned **F-Secure**.

As Conficker's clock continues to tick down to April 1st, security experts continue to race against time to minimize the yet-untold havoc that could be unleashed by this evasive computer worm.

Bill Kurzenberger
 Network+, A+, MCP, MCDST
 Published March 26, 2009

Featured Application

Malwarebytes' Anti-Malware

Malwarebytes' Anti-Malware (MBAM), although a relatively new name in the computer security industry, has proven to be a formidable malware removal tool. MBAM identifies and removes malicious software, and restores the computer back to optimum performance.

MBAM's additional features include FileASSASSIN, which can delete locked files on a PC, Quarantine, and an optional Bug Reporting feature.

MBAM is available as a free download, and a more powerful Protection Module is available for purchase.

Website:
www.malwarebytes.org

Interested in advertising with Call-a-Tek? Contact our representatives to have your ad placed here.