

Conficker Is a Serious Threat but the 1 April 'Deadline' Is Not

John Pescatore

The Conficker worm represents a serious threat to enterprise and home PCs, but the approaching "deadline" is not as urgent as the media hype suggests. Gartner does not expect a widespread system meltdown on 1 April.

NEWS ANALYSIS

Event

On 30 March 2009, media outlets reported that security researchers have found a flaw in the widespread Conficker worm that may aid efforts to isolate and repair systems infected by it. Conficker is thought to contain code scheduled to cause unspecified damage to infected systems beginning 1 April, but researchers appear to have found a way to avoid Conficker's self-concealment capabilities. Several leading providers of vulnerability assessment (VA) technology also report being able to isolate Conficker-infected PCs.

Analysis

Gartner believes that the intense media attention being paid to the supposed 1 April Conficker deadline is largely unwarranted. Conficker, which is believed to have infected more than 3 million PCs worldwide, is a serious problem that enterprises and security technology providers must address. However, there is no reason to believe that some spectacularly damaging event will occur on 1 April. Paradoxically, the hype surrounding Conficker, and the enterprise response, is a major factor limiting its likely impact. Enterprises should be much more concerned about unrecognized threats.

Conficker (also known as Downadup) exploits known vulnerabilities in Microsoft Windows Server services. Downadup first appeared in October 2008, a month after the release of Microsoft Security Bulletin MS08-067, which contained patches for the vulnerable services. Many PCs were not patched in time and were compromised. Conficker takes steps to make it appear that an infected machine has been patched, making it more difficult to detect compromised PCs. It also uses encryption and many techniques to evade detection and communicate with malicious command-and-control servers.

Despite Conficker's unusual sophistication, most detailed analyses of the worm's code have shown there is no "apocalyptic" event slated for 1 April. On that date, one of the more recent Conficker variants will dramatically increase the number of domain names that may potentially host malicious servers. This will increase the pressure on simple URL blocking techniques, but will not significantly increase the threat level, because compromised machines already have many communications capabilities. The most likely outcome on 1 April is denial-of-service conditions resulting from increases in network bandwidth. The major risk of Conficker is the ongoing threat that compromised PCs present to both enterprises and home users.

RECOMMENDATIONS

Enterprise security professionals:

- Monitor credible sources for information on Conficker, which is being updated almost continuously.
- Contact providers of VA technology to ensure that their capabilities have been updated to detect PCs compromised by Conficker. Make VA scans of all PCs a critical priority.
- Review URL blocking and inbound malware secure Web gateway capabilities and network access control capabilities to ensure that the most aggressive possible short-term stance is being taken against Conficker.

- If employees are permitted to use their own PCs for business purposes, inform them of the urgency of checking and cleansing their these PCs and instruct them about how to do so.
- Place prominent warnings on enterprise Web sites directing consumers to antivirus sites with information on how to check their PCs.

RECOMMENDED READING

- "Case Study: Early Detection of PCs That Have Been Compromised via Botnet Clients" — New forms of detection are required to identify and mitigate attacks that use botnet clients as their entry points. **By John Pescatore and Adam Hills**
- "Magic Quadrant for Secure Web Gateway" — Incumbent providers in this market have been slow to respond to changing demands, while new vendors are struggling to achieve the right product mix and prove themselves with enterprises. **By Peter Firstbrook and Lawrence Orans**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509