

Microsoft COFEE Brews Concern Over Penetration Tools

John Girard

Rumors that Microsoft has given law enforcement a "back door" into its systems appear to be unfounded. But this event is grounds for enterprises to take precautions to protect sensitive data against real penetration tools.

NEWS ANALYSIS

Event

On 2 May 2008, Microsoft briefed Gartner on the Computer Online Forensic Evidence Extractor (COFEE), a USB device that the company began distributing to law enforcement agencies in 2007. COFEE enables law enforcement to gather digital evidence, decrypt passwords and analyze computer and Internet activity without seizing a workstation, taking it offline or shutting it down. Media reports in the preceding week had suggested that COFEE could provide a "back door" into Microsoft operating systems and applications. In its Gartner briefing, however, Microsoft stated that COFEE offers little more than a set of scripts that will help law enforcement take a system "snapshot."

Analysis

Microsoft states that the real purpose of COFEE — which is an initiative of the company's legal organization, rather than a companywide project — is to make the process of taking a system snapshot faster and more consistent and allow data to be analyzed later. COFEE is intended to be used by law enforcement agents who are not computer experts but have served a warrant and are faced with a "live" system. The device has been distributed widely but informally, because Microsoft regarded the initiative as being in its pilot phase. The USB key holds more than a hundred commands that can be executed automatically with a few starting scripts. Microsoft says that the commands are all public; no new code has been written, and no back doors are present.

Gartner believes — and Microsoft agrees — that it was a mistake to widely deploy the COFEE initiative without public disclosure and a formal distribution plan. We also believe that Microsoft should work closely with professional third-party forensics product and service vendors to develop, manage and track future data capture utility projects. Another concern raised by Microsoft's failure to offer public information about this initiative is that the widespread attention it has drawn will likely encourage otherwise well-intentioned enterprise IT personnel to search the Internet for penetration tools with which to experiment. Enterprises should review their internal protection measures to ensure that their business data is secure and private.

RECOMMENDATIONS

Chief information security officers (CISOs) and other enterprise security decision-makers

- Recognize that commonly available tools can be used — whether by law enforcement authorities or by criminals — to recover sensitive data from enterprise workstations.
- Review all internal protection policies and practices to ensure that business data is secure and private.
- Take immediate action to protect business data from exposure by using strong authentication, stored data encryption and secure backups.

RECOMMENDED READING

- "What Every IT Manager Should Know About Digital Forensics" — IT managers must have a basic understanding of digital forensic techniques and technologies, as well as their implications on the business. **By John Bace and Jay Heiser**

- "Assessment Methodology for Open-Source Security Testing Tools" — Gartner's Security Testing Ratings Scale can help CISOs to assess the value of free and open-source security testing tools in enterprise environments. **By Rich Mogull and John Girard**

(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