

Data Encryption Not Enough to Prevent FTP Credential Theft

L. Frank Kenney, Peter Firstbrook

The reported theft of 88,000 FTP credentials reaffirms that using SSL technologies or encrypting the payload is not enough to secure managed file transfer solutions and avoid regulatory and compliance audits.

NEWS ANALYSIS

Event

On 26 June 2009, security researchers at the security tool vendor Prevx announced they had uncovered a cache of stolen FTP credentials belonging to a variety of corporations, including Symantec, McAfee, Bank of America, Amazon and Cisco Systems. Prevx claims that a trojan stole approximately 88,000 unencrypted FTP logins. The company has set up a page where users can check whether their logins have been compromised, at <http://www.prevx.com/ftplogons.asp>.

Analysis

Companies are becoming increasingly aware of the risks posed by transmitting data over nonsecure or unmanaged FTP solutions. The FTP credential theft reaffirms that simply using SSL technologies or encrypting the payload is not enough to ensure secure FTP. Malware such as the Zeus trojan is capable of stealing and exporting SSL credentials and exploiting FTP servers as distribution points for malware. Compromised Web sites already serve as a prime channel for distributing malware to unsuspecting Web site visitors. The FTP focus of this attack indicates that Internet-facing FTP servers may be the next target.

In this particular case, it is not clear that the credentials were actually used; nevertheless, the fact that attackers were able to access an FTP site poses sufficient risk. Gaining access to the FTP server enables attackers to host malware on a legitimate, trusted resource. Crafty social engineering of file names (for example, naming the malware "Executive salary.exe") would be enough to ensure that users downloaded malware into their systems and continued its propagation. Legitimate FTP servers could also become unwitting vehicles for the trafficking of illicit and pirated media, applications and data. Data protection is essential, the server and users' credentials must also be safeguarded. The attraction of a simple, easy-to-use FTP site should not outweigh security considerations, particularly when a plethora of security technologies is available, ranging from low-cost and downloadable to global-class solutions, such as Axway's Synchrony, Group Logic's Mass Transit and Ipswich's Moveit.

RECOMMENDATIONS

Enterprises: If you have deployed an FTP site that handles high-value data or application areas without proper mechanisms for managed and secure file transfer, data at rest, and file server and client administration, immediately consider deploying a managed file transfer solution with appropriate data loss protection capabilities. Data encryption is mandatory, but is not the end of your responsibilities with regard to file transfer. Consider placing FTP servers behind secure Web gateways to monitor FTP traffic for the upload and download of malicious applications.

RECOMMENDED READING

- "Key Issues for Managed File Transfer 2009" — Gartner is expanding its managed file transfer research agenda to reflect the growing importance of governance and the diversity of deployment models. **By L. Frank Kenney**
- "A Buyer's Guide to Endpoint Protection Platforms" — Endpoint protection platforms are rapidly replacing "point" antivirus and anti-spyware tools and personal firewalls. **By Peter Firstbrook**

(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