Visa Data Security Alert

17 March 2010

Key Logger: Key Stroke and Screen Capture

To promote the security and integrity of the payment system, Visa is committed to helping clients and payment system participants better understand their responsibilities related to securing cardholder data and protecting the payment industry. As part of this commitment, Visa issues Data Security Alerts when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

Payment system participants may share this alert with their stakeholders to help ensure they are aware of emerging vulnerabilities and take steps to mitigate risks.

Key Logger: Key Stroke and Screen Capture

In recent weeks, Visa has noticed an increase in key logger attacks involving the merchant community. Key logging is a method of capturing and recording keystrokes; key logging software is widely available via the Internet.

Key loggers, like most malware, can be distributed as part of a Trojan Horse or a virus, sent via e-mail (as an attachment or by clicking to an infected web link or site) or, in the worst cases, are installed by a hacker with direct access to a victim's computer.

The particular key logger malware identified by Visa is equipped to send payment card data to a fixed e-mail or IP address accessible to the hacker. In these instances, the hacker is able to install key logger malware on the point of sale (POS) system due to insecure remote access and poor network configuration. Based on Visa's review of the malware, it uses File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP) on default ports (20, 21 and 25 respectively) to send data out of the network.

Recommended Mitigation Strategy

Although key loggers can be difficult to detect, the following measures that support an organization's Payment Card Industry Data Security Standard (PCI DSS) compliance should be utilized to mitigate the risk of exposure to critical systems, such as POS systems, payment processing servers, database servers or other servers where cardholder data resides:

- Remove unnecessary remote access. If remote connectivity is required, secure remote access by turning on remote access only when needed. Do not use default or trivial passwords; only use remote access applications that offer strong security controls. Always use two-factor authentication.
- Implement a secure network configuration. Organizations must have a dedicated firewall and must implement strict network traffic ingress (inbound) and egress (outbound) filtering to ONLY allow those ports/services necessary to conduct business. Disable FTP, SMTP and other insecure ports if your organization does not require these services.
- Organizations should constantly observe which software programs are installed on their systems, determine any unknown applications, and take appropriate actions (e.g., remove, disable, configure properly, etc.) to mitigate the risk of a compromise.

- Periodically check for any unknown devices connected to systems, including devices connected to keyboards and/or mice.
- Organizations should check their systems against the known key logger malware signatures that Visa has collected from forensic investigations (see Table 1).
- Implement the latest anti-virus engine and signature files to detect known malware. If heuristic technology is available on an organization's anti-virus product, enable it to detect unknown malware. Most anti-virus software will detect off-the-shelf key loggers.
- Implement anti-spyware applications to detect key loggers and cleanse them from applicable systems.
- Monitor your network and host. Monitoring can alert organizations whenever a software application attempts to contact malicious IP addresses or when malicious IP addresses attempt to contact your network. This action will give organizations a chance to prevent key loggers from exporting sensitive data from the network.

If you detect a security breach, notify your acquiring bank immediately. You can also contact Visa Fraud Control at 650-432-2978 or usfraudcontrol@visa.com.

Table 1: Key Logger Malware

The hash values below were identified on 11 March 2010. Please be aware that hash values will change with new malware variants. Visa will update this list as new malware variants are identified.

Filename	Size	MD5
bpkhk.dll	489,984	35f5478e190cc6614a6a5d4f1f380855
bpk.exe	1,090,560	663267d3ed4af3582ea57ba03fb0da92
	401,408	18bc32bb8a8d5a85cdafad5a4ecc4c73
bpkr.exe	747,520	7231b6c5ca6addd905db7677200833e2
fstsmtp.exe	1,560,661	80ee23ede41504b1a83654334148306f
xxx.exe	Unknown	994ffae187f4e567c6efee378af66ad0
SMTPListener.exe	Unknown	5e289e10a2f3fe6b3080825f5dbf588f
dll32.exe	438,272	bae0fb25bcf05a5da7fde8dce759ee0d
ToolKeylogger.exe	2,007,040	4cf8307cac714fe4f2cbc5d46f5cf243
ToolKeylogger.xml	6,432	3f4ad41f10ec18a7f27f2339ee500dda

Related Documents

"What To Do If Compromised," available at www.visa.com/cisp.

For More Information

For more information or to ask questions about the information in this alert, please visit www.visa.com/cisp (see “Alerts & Bulletins") or e-mail usfraudcontrol@visa.com.