

## Visa Data Security Alert

### Key Logger Malware: Key Stroke and Screen Capture

October 6, 2008

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 to take steps to mitigate these risks.

#### Key Logger Malware: Key Stroke and Screen Capture

“Key logging” is a method of capturing and recording keystrokes used by organizations to troubleshoot problems within computer systems. Software used to perform this function is commercially available and easy to obtain.

However, Visa Cyber Security and Investigations has recently become aware of malware versions of this software that are being used to target the payment industry. Investigations have revealed that this new “key logger” malware is capturing payment card data and/or user credentials including passwords. This information is captured in real-time and sent directly to hackers over the Internet. Additionally, newer advances provide the ability to intermittently capture screenshots from the key logged computer.

Key logger malware is widely available via the Internet and can be installed on virtually any operating system. Key loggers, like most malware, are distributed as part of a Trojan Horse or virus, either sent via e-mail (as an attachment or by an infected web link or site) or, in a worst case scenario, installed by a hacker with direct access to the victim’s computer.

The key logger malware Visa has identified was installed on a POS system and was equipped to send payment card data to a fixed e-mail or IP address accessible to the hacker. The installation of this malware was possible due to insecure remote access and poor network configuration.

#### Recommended Mitigation Strategy

Although key loggers can be difficult to detect, the following best practices should be utilized to mitigate the risk of exposure to critical systems including point-of-sale (POS) systems, payment processing servers, database servers or other servers where cardholder data resides:

- Secure your remote access connectivity. See Data Security Bulletin “*Top Three POS System Vulnerabilities*,” dated November 21, 2006, available at [www.visa.com/cisp](http://www.visa.com/cisp).
- Implement a secure network configuration. Organizations must have a dedicated firewall and configure it to **only** allow those ports or services necessary to conduct business. See Data Security Alert “*Improperly Segmented Network Environment*,” dated October 31, 2006, available at [www.visa.com/cisp](http://www.visa.com/cisp).
- Organizations should constantly observe which programs are installed on their systems and question any unknown applications. Periodically check for any unknown devices connected to your keyboard and/or mouse.
- Implement anti-spyware applications to detect key loggers and cleanse them from applicable systems.
- 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.
- Monitor your network and host. Monitoring can alert organizations whenever a software application is attempting to contact malicious IP addresses or when malicious IP addresses are attempting to contact your network. This gives organizations a chance to prevent the key logger from exporting sensitive data from your network.

For more information or questions regarding the information in this alert, please visit [www.visa.com/cisp](http://www.visa.com/cisp) (see “Alerts and Bulletins”) or e-mail [cisp@visa.com](mailto:cisp@visa.com).