

# Every **KEY** You Make, Every **STROKE** You Take, **THEY'LL BE WATCHING YOU**

**C**riminals have a reputation for being resourceful and relentless in their attempts to steal payment card information. A recent trend targeting the hospitality industry and other merchant sectors provides a strong case in point.

Visa has recently found an increase of criminal instances of keystroke logging (also referred to as key logging) through the course of analyzing payment card data security breaches. This criminal tactic intercepts every stroke typed into a victim's computer keyboard and records this information to be retrieved. Most of

their victims have no idea this is occurring. In the hospitality industry and for other merchants, this means that without proper safeguards in place, you may be unknowingly transmitting your customers'

payment card information and other sensitive data directly to hackers.

Key loggers, like most forms of malware, can be distributed as part of a Trojan horse, a virus or other malware, 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 unauthorized 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.

This system vulnerability is generally due to insecure remote access and poor network configuration which allows criminals unauthorized and unfettered access. Based on forensic 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 used 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.

**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.

**Check your systems against the known key logger malware signatures** that Visa has collected from forensic investigations (see chart below).

**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 suspect that you've become a victim of key stroke logging or if you detect a security breach, notify your acquiring bank immediately. You can also contact Visa Fraud Control at [usfraudcontrol@visa.com](mailto:usfraudcontrol@visa.com). For more information, please refer to *Visa's What To Do If Compromised* document available at [www.visa.com/cisp](http://www.visa.com/cisp).



## Key Logger Malware

This chart includes some of the hash values identified on March 11, 2010. The complete list is available on [www.visa.com/cisp](http://www.visa.com/cisp). Please be aware that hash values will change with new malware variants, and Visa will update the information online as new malware variants are identified.

Filename	Size	MDS
bpkhk.dll	489,984	35f5478e190cc6614a6a5d4f1f380855
bpk.exe	1,090,560	663267d3ed4af3582ea57ba03fb0da92
bpk.exe	401,408	18bc32bb8a8d5a85cdafad5a4ecc4c73
bpkr.exe	747,520	7231b6c5ca6add905db7677200833e2
fstsmtplib.exe	1,560,661	80ee23ede41504b1a83654334148306f
xxx.exe	Unknown	994ffae187f4e567c6efee378af66ad0
SMTPListener.exe	Unknown	5e289e10a2f3fe6b3080825f5dbf588f
dll32.exe	438,272	bae0fb25bcf05a5da7fde8dce759ee0d
ToolKeylogger.exe	2,007,040	4cf8307cac714fe4f2c2cb5d46f5cf243
ToolKeylogger.xml	6,432	3f4ad41f10ec18a7f27f2339ee500dda