VISA DATA SECURITY ALERT August 2013

Retail Merchants Targeted by Memory-Parsing Malware - *UPDATE*

This is an update to the Visa alert sent in April 2013. Click here for a copy of the April 2013 alert http://usa.visa.com/download/merchants/alert-prevent-grocer-malware-attacks-04112013.pdf. This alert is intended to provide guidance for Information Security and/or IT Security professionals on how to protect against this threat.

Since January 2013, Visa has seen an increase in network intrusions involving retail merchants. Once inside the merchant's network, the hacker will install memory parser malware on the Windows based cash register system in each lane or on Back-of-the-House (BOH) servers to extract full magnetic stripe data in random access memory (RAM).

The malware is configured to "hook" into payment application binaries. These binaries are responsible for processing authorization data, which includes the full magnetic stripe data. When authorization data is processed, the payment application will decrypt the transaction on the cash register system or BOH server, and store the authorization data in RAM. The data needs to be decrypted in order for the authorization to be completed. Hackers are taking advantage at the point in time when data is stored in RAM, and use malware such as memory parsers to steal full track data from the systems.

Visa is issuing this alert to make clients aware of new malware information and malicious IPs, and to remind Visa merchants to secure their payment processing (and non-payment) networks from unauthorized access. A list of new malware signatures and malicious IPs are included on this alert (Appendix A). Visa highly recommends merchants implement these signatures on security solutions to detect a suspected breach. However, Visa recommends performing sufficient due diligence prior to implementing any block to avoid any inadvertent connectivity issues for legitimate access.

At the present time, Visa is only aware of the malware impacting a Windows operating system.

Recommended Mitigation Strategy

These strategies are broken down into four categories (Network, POS, Administrators and Incident Response) to ensure a defense-in-depth approach to minimize the possibility of an attack and mitigate the risk of a card data compromise:

Network Security

- Review your firewall configuration and ensure only allowed ports, services and IP addresses are communicating with your network. This is especially critical on outbound (e.g., egress) firewall rules, where compromised entities allow ports to communicate to any IP on the Internet. Hackers will leverage this misconfiguration to exfiltrate data to their IP address.
- Segregate the payment processing network from other non-payment processing networks.
- Apply access controls lists (ACLs) on the router configuration to limit unauthorized traffic to the payment processing networks.
- Create strict ACLs segmenting public facing systems and backend database systems that house payment card data.
- Review systems that have direct connectivity or access to the payment processing environment and ensure systems are secure.

Cash Register and POS Security

- Implement hardware-based point-to-point encryption. Visa recommends EMV enabled PIN Entry Devices or other credit only accepting devices that have Secure Reading and Exchange of Data (SRED) capabilities. SRED approved devices can be found on www.pcisecuritystandards.org.
- Install PA-DSS compliant payment applications and ensure applications are installed in a PCI DSS compliant manner. Merchants should also review their payment application to ensure it is not configured in a debug/troubleshooting mode. This type of configuration can result in storage of clear-text cardholder data.
- Perform periodic scans on systems to identify storage of cardholder data and secure delete the data.
- Deploy the latest version of operating system and ensure it is up-to-date with security patches, anti-virus software, File Integrity Monitoring, and a host-based intrusion detection system.
- Assign strong passwords to your security solution to prevent application modification.

- Perform a binary or checksum comparison to ensure unauthorized files are not installed on systems. Merchants should consider implementing application "whitelisting" to help prevent installation of malicious software and other unapproved programs from running.
- Deny Remote Desktop Protocol (RDP) logons whenever possible.
- Ensure any automatic updates from third-parties are validated. This means performing a checksum on the updates prior to deploying on the POS systems. Merchants should work with their POS vendors to obtain signatures/hash values in order to perform this checksum validation.
- Disable unnecessary ports and services, null sessions, default users and guests.
- Enable logging of events and confirm you have a process to monitor logs on a daily basis.
- Implement least privileges and ACLs on users and applications on the system.

Limit Administrative Access

- Use two-factor authentication when accessing the payment processing networks. Even if a Virtual Private Networking (VPN) is used, it is important that 2-factor authentication be implemented. This will help to mitigate key logger or credential dumping type of attacks.
- Limit administrative privileges on users and applications.
- Periodically review systems (local and domain controllers) for unknown and dormant users.
- Do not use NTLM or LM hash for password hashing as the algorithm is known to be compromised and susceptible to a Pass-the-Hash type of attack. Visa recommends implementing salted one way password hashing. For more information on Pass-the-Hash attacks and additional password mitigation controls, go to http://www.microsoft.com/security/sir/strategy/default.aspx#!password_hashes.

Incident Response

- Deploy Security Information and Event Management (SIEM). A SIEM is a system that serves as a central point for managing and analyzing events from network devices. A SIEM has two primary responsibilities:

    1. Aggregate events and logs from network devices and applications

    2. Use intelligence to analyze and uncover malicious behavior on the network

- Since anti-forensic techniques are used by hackers to avoid detection, Visa recommends offloading logs to a dedicated server in a secure location to prevent unauthorized users from tampering with the logs.
- Invest in a dedicated incident response team (IRT). The IRT should have the knowledge, training and certification to respond to a breach. For more information on IRT training, go to www.sans.org.
- Test and document your incident response plan to identify and remediate any gaps in the process prior to an actual event. The plan should be tested and updated periodically to address emerging threats.

APPENDIX A

Malware Signatures

Latest Malware Signatures

File Name	Description	File Size (bytes)	Hash Value
System32.exe	Backdoor	618570	**MD5**: b9cf8e70681755c1711c38944695eeaa **Fuzzy**:1536:5kZ3maVDa38JpAZlivO2/L0txCDPfsIQlwLnfyZ/ph/mDfgovLPnjt:GD1asJpvbukPfBQenfyZ/ph/mDYmLPjt **SHA1**: 4D66F06E05E0869BBA1082E1F7847B847A3D02C9
Svcsec.exe	Backdoor	614474	**MD5**: 25f7b169b43c4d5db472afb0ee09b035 **Fuzzy**:1536:TIo9rvJYWmP/PYHK6bnGyUolA3aXkJTROGibGj+clGQEGs2aT3jt:84rlmPYHK66tolaEuTROaj+sGe2TTt **SHA1**: B1E1FB5EE7460D41AD1C932C48B4BACC73BD5658
oposvc.exe	Memory scrapper malware	69632	**MD5**: dd90c44afa5da730b8cb979667ae8fd3 **Fuzzy**:768:gNnzPGkP7Rr/TMjMzcZd566QCeu4MgycfUuxGIfLNTQhY0oCsHv97zJ2aBvsXkW:cxBqzm6QfutUf1YIBUhY0CsUzyd0pl8 **SHA1**: D5CA1D0627C9F1FCF44A1EE744704ABF71D1117B
svchosts.exe	Memory scrapper malware (non-functional)	249856	**MD5**: 0561344c4e4460077fdc79a4679508ed **Fuzzy**: 6144:i+FxGNVi3y5eXRyuC34gY0NtFrDelYBXlmwHGO:i+RyQ0ufmNtFrDFXlm **SHA1**: 2026A04702E4A8BE8899B085859348BBD1D46702

Latest Malicious IPs/Domains

IP	Description
89.35.148.67	Embedded within system32.exe
examene.uvvg.ro	Embedded within svcsec.exe
rghost.net	Russian file sharing web site. Note that some activity to this site might be legitimate

To request information or report a data breach, contact Visa Fraud Control:

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- Canada Region, Latin America Region, United States: USFraudControl@visa.com