Preventing Memory-Parsing Malware Attacks on Grocery Merchants

Since January 2013, Visa has seen an increase in network intrusions involving grocery merchants. Once inside a merchant’s network, hackers install memory-parsing malware on Windows-based cash register systems or back-of-house (BOH) servers to extract full magnetic-stripe data.

The malware is configured to “hook” into certain payment application binaries. These binaries are responsible for processing authorization data, which includes full magnetic-stripe data. When authorization data is processed, the payment application decrypts the transaction on the cash register system or BOH server and stores the authorization data in random access memory (RAM). The data must be decrypted for the authorization to be completed, so hackers are accessing full track data when it is stored in RAM and using malware such as memory-parsers to steal it.

Hackers are also using anti-forensic techniques such as tampering with or deleting security event logs, using strong encryption or modifying security applications (e.g., whitelist malware files) to avoid detection.

The malware can be configured or compiled to work on merchant segments other than grocery merchants. At this time, it is known to affect only Windows operating systems. Visa is offering guidance to help clients secure their networks and protect their Windows-based point-of-sale (POS) and BOH systems from unauthorized access. A list of malware signatures is included in this article, and Visa highly recommends that clients implement these signatures in their security solutions.

**Recommended Mitigation Strategies**

The following mitigation strategies, broken down into four categories, are a defense-in-depth approach to minimizing the possibility of an attack and mitigating the risk of data compromise:

- **Network Security**
  - Review firewall configurations and ensure that only allowed ports, services and Internet protocol (IP) addresses are communicating with your network. This is especially critical for outbound (e.g., egress) firewall rules, in which compromised entities allow ports to communicate to any IP address on the Internet. Hackers leverage this misconfiguration to exfiltrate data to their IP addresses.
  - Segregate payment processing networks from other networks.
  - Apply access control lists (ACLs) on the router configuration to limit unauthorized traffic to payment processing networks.
  - Create strict ACLs segmenting public-facing systems and backend database systems that house payment card data.

- **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 at the Payment Card Industry Security Standards website.
  - Install Payment Application Data Security Standard-compliant payment applications.
  - Deploy the latest version of an 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 a strong password to security solutions to prevent application modification.
Perform a binary or checksum comparison to ensure unauthorized files are not installed.

Ensure any automatic updates from third parties are validated. This means performing a checksum comparison on the updates prior to deploying them on POS systems. Visa recommends that merchants work with their POS vendors to obtain signatures and hash values to perform this checksum validation.

Disable unnecessary ports and services, null sessions, default users and guests.

Enable logging of events and make sure there is a process to monitor logs on a daily basis.

Implement least privileges and ACLs on users and applications on the system.

**Administrative Access**

Use two-factor authentication when accessing payment processing networks. Even if a virtual private network is used, it is important that two-factor authentication is implemented to help mitigate key-logger or credential-dumping attacks.

Limit administrative privileges for users and applications.

Periodically review systems (local and domain controllers) for unknown and dormant users.

**Incident Response**

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

- Aggregates events and logs from network devices and applications.
- Uses intelligence to analyze and uncover malicious behavior on the network.

Offload logs to a dedicated server in a secure location where unauthorized users can't tamper with them.

Invest in a dedicated incident response team (IRT) that has the knowledge, training and certification to respond to a breach. For more information on IRT training, visit the SANS Institute website.

Test and document incident-response plans to identify and remediate any gaps prior to an attack. Plans should be updated periodically to address emerging threats.

**Malware Signatures**

The following malware signatures were identified during recent grocery store breaches. Merchants should implement these signatures to help detect a potential data breach on their systems.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
<th>Size (Bytes)</th>
<th>MD5 Hash Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rtcli.dll</td>
<td>Information stealer / downloader</td>
<td>118272</td>
<td>4bd819d9e75e4e8ecf1a9599f44af12a</td>
</tr>
<tr>
<td>mstdc.exe</td>
<td>Backdoor</td>
<td>64512</td>
<td>57703973ff74503376a650224aa43da</td>
</tr>
<tr>
<td>mstdc.bak</td>
<td>Backdoor</td>
<td>106496</td>
<td>67ed156e118b9aa65ed414a79633a3d4</td>
</tr>
<tr>
<td>msaudit.dll</td>
<td>Memory-parsing malware</td>
<td>97792</td>
<td>27bffa7d034a94b79d3ef7fda50084</td>
</tr>
<tr>
<td>mn32.exe</td>
<td>Prefetch file indicating execution of the malicious code</td>
<td>179200</td>
<td>89a8844c1214e7fc977f026be675a92a</td>
</tr>
<tr>
<td>si.vbs</td>
<td>Visual basic script used by hacker to deploy malware onto POS systems</td>
<td>2772</td>
<td>40efe7632b01116eefab438c9bbe34</td>
</tr>
<tr>
<td>sd32.exe</td>
<td>Anti-forensic utility to remove malware from POS systems</td>
<td>134000</td>
<td>9c3a1d3829c7a46d42d5a19fe05197f3</td>
</tr>
<tr>
<td>Process Name</td>
<td>Description</td>
<td>Size</td>
<td>Hash</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>TcpAdaptorService.exe</td>
<td>Memory-parsing malware</td>
<td>73728</td>
<td>cfee737692e65e0b2a358748a39e3bee</td>
</tr>
<tr>
<td></td>
<td></td>
<td>118784</td>
<td>85f94d85ceff32fa18d55491e355d2b</td>
</tr>
<tr>
<td>Osq.exe, svchosts.exe</td>
<td>Tool used with TcpAdaptorService.exe to send track data to bad IP</td>
<td>122880</td>
<td>4b9b36800db395d8a95f331c4608e947</td>
</tr>
<tr>
<td>oposwin.exe</td>
<td>Memory-parsing malware</td>
<td>245760</td>
<td>3446cd1f4bee2890afc2e8b9e9e76a2</td>
</tr>
<tr>
<td>svcmon.exe</td>
<td>Memory-parsing malware</td>
<td>253952</td>
<td>0ff972080248406103f2093b6892134</td>
</tr>
<tr>
<td>nYmT�权JSjLLFfgQ.bat</td>
<td>Batch file used to whitelist malware executables on FIM</td>
<td>74</td>
<td>eae4718ea5a860cc372b5728e96af656</td>
</tr>
<tr>
<td>tbcsvc.exe</td>
<td>Performs cryptographic operations</td>
<td>293583</td>
<td>1aa662d329cc7c51d2e9176024fedee8</td>
</tr>
<tr>
<td>mssec.exe</td>
<td>Attempts outbound communication via port 443</td>
<td>135242</td>
<td>d7e5e85cc6c71a39b99a9228313cc33</td>
</tr>
<tr>
<td>msproc.exe</td>
<td>Malicious unknown purpose</td>
<td>184128</td>
<td>2e5677707730ed2c76b162a97dcf28c05</td>
</tr>
</tbody>
</table>

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