Understanding Malware

Topic(s): Fraud/Risk, Security

Applies to:	✓ Acquirers	✓ Issuers	✓ Processors

Summary:	Malware is software used by hackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Hackers introduce malware into private networks by targeting systems that may be vulnerable to compromise due to weak data security controls. MasterCard is providing detailed information about malware to help customers understand how compliance with the *Payment Card Industry* (PCI) *Data Security Standard* (DSS) can aid in the detection and prevention of malware fraud attacks.
Action Indicator:	**A** Attention warranted
Effective Date:	Immediately

Overview

What is malware? Contrary to popular belief, malware is not used to compromise or hack a system. Rather, malware is a tool that hackers use to collect data and remove it from a compromised system. When hackers compromise a system, they generally gain a foothold through a security misconfiguration (such as weak remote access) or through exploiting a bug in an application (as is done in a SQL injection attack). This initial exploit provides the hackers access to a system. Once the hackers gain access to a system, they install a malware tool to identify and collect valuable information in the environment. In other words, the hackers first must compromise a system before they can install the malware.

Malware comes in many shapes and sizes, and can be:

- Installed on a payment server to capture card data as it passes the network
- Run as a utility that searches file servers for stored card data
- Act as a keystroke logger on a cash register to capture card data as it is entered

In some cases, hackers may custom-create malware to operate in a specific environment. Some fraud experts argue that this customization makes malware completely undetectable; however, there are security controls that allow for the detection of even custom-created malware. Some security controls include, but are not limited to:

- File Integrity Monitoring (FIM) tools
- Outbound Internet filtering
- Anti-virus software

FIM Tools

FIM tools monitor sensitive systems to identify whether or not a file has changed or a new file has been installed. If malware has been installed on a system or saves card data to a file, FIM software can detect the change and alert on the behavior.

Outbound Internet Filtering

Placing restrictions on outbound Internet connections can prevent a hacker from removing card data from the environment. There are various levels of restrictions that MasterCard customers can utilize. A system with card data should not have the ability to access any system on the Internet. MasterCard customers should restrict access to help ensure that the system can only access authorized sites.

In addition to basic firewall controls, MasterCard customers can implement additional controls such as content filtering to inspect outgoing network traffic for sensitive information. Application proxies can also be utilized to help ensure that outgoing network traffic follows a proper protocol.

Anti-Virus Software

In some cases, custom malware uses shared code. While the malware may be customized for a certain environment, the hacker may be reusing the core of the malware code. This means that the customized malware may have similarities with other identified malware and be detectable by common anti-virus software.

In addition, "heuristic" anti-virus software is often able to alert on custom malware based on the behavior of the malware. This type of anti-virus software watches for certain suspicious or unusual behaviors rather than a specific type of malware file.

Maintaining PCI Compliance

The PCI DSS provides layered security through preventative, detective, and reactive controls. **Perhaps the most important way to address malware is to prevent hackers from ever installing it on a system.** If hackers are unable to compromise a system, they are unable to install malware and, thus, unable to gain access to payment card data.

When implemented properly, the numerous preventative controls outlined by the PCI DSS offer robust security measures that hinder a hacker's efforts to access card data. Detective controls including FIM tools, outbound Internet filtering, and anti-virus software are all required by the PCI DSS and can aid as a last line of defense in the detection of malware if preventative controls are not completely implemented.

Once detected, the PCI DSS requires reactive controls regarding Incident Response to help ensure that any potential intrusion is identified and responded to in a timely manner.

By implementing the layers of security required by the PCI DSS, MasterCard customers will be positioned to prevent, detect, and react to malware installed on their systems. PCI DSS version 3.0 was released in November 2013 and has various updates based upon industry feedback and latest attack trends. This version of the standard can be located in the **Documents Library** under the **PCI Standards & Documents** tab on the following website:

PCI Security Standards Council

Website: www.pcisecuritystandards.org

For More Information

For more information about PCI controls, visit the MasterCard complimentary PCI 360 education portal at:

Website: www.mastercard.com/pci360

Customers with additional questions about the information in this article should contact Customer Operations Services using the Contact Information provided in this bulletin, their regional Help Desk, or a regional Customer Security and Risk Services representative.