Emerging Threat: Parsing Track Data from RAM

Attackers Using Malware to Steal Payment Card Data via a Computer's Random Access Memory (RAM)

Trustwave Forensic Experts Observe Disturbing Technique, the Parsing of Track Data from RAM, in Payment Card Compromise Cases

In a number of cases of payment card compromise recently investigated by Trustwave's payment card compromise investigation team, experts have uncovered a technique used by attackers to steal cardholder data even if that data isn't written to disk (i.e., stored or saved). While Trustwave has known of precursors to the technique for some time, Trustwave investigators have not seen real-world examples of the use of the technique until now.

This development in card compromise techniques concerns Trustwave because even if a merchant that accepts payment card transactions uses a payment application that complies with Visa's Payment Application Best Practices (PABP), the merchant may still be at risk. If the merchant's network environment does not comply with the Payment Card Industry Data Security Standard (PCI DSS), an attacker may gain access to the network system and exploit the system to gather data from a PABP-validated payment application.

Because increasing numbers of payment application vendors are aware of the importance of protecting the processing, storage and transmission of cardholder data; many vendors know that their payment applications cannot store track data. Track data is the information coded on the magnetic stripe of a payment card and includes account numbers and other sensitive data.

The card brands have spent significant resources to educate vendors, merchants and service providers about eliminating the storage of track data. Hackers seek track data because they can use or sell this information for the creation of fraudulent payment cards.

The technique discovered by Trustwave involves an attacker accessing a computer that hosts a payment application and installing unauthorized applications (malware) onto the host computer. That malware then collects unencrypted/plain-text track data via the Random Access Memory (RAM) used by the payment application to interact with the host computer. Again, even if the payment application used by a merchant complies with Visa's Payment Application Best Practices (PABP) and does not write track data to disk, an unauthorized individual can access that data by parsing it from RAM.

Payment applications running on Windows operating systems are particularly vulnerable to the technique. However, if a merchant complies with the PCI DSS, a hacker could not gain the access needed to steal unencrypted track data via a computer's RAM.

Complying with the PCI DSS will protect a merchant against this technique.

See the following page for additional recommendations for preventing the parsing of track data from RAM.

Trustwave®
Information Security & Compliance

To ensure their protection against the parsing of track data from RAM, Trustwave recommends that any merchant that uses a payment application take the following actions—if they have not done so already:

- Install anti-virus programs on all systems processing or accepting cardholder data
- Regularly update anti-virus programs
- Regularly review the security logs to monitor the installation of windows services
- Protect the processing environment with a properly configured firewall
- Only allow the use of services necessary to business operations via egress and ingress filtering on the firewall
- Prohibit direct access to remote-access applications via the Internet
- Implement a PCI DSS-compliant authentication control, such as two-factor authentication, for any remote access
- If any malware (unauthorized applications) listed in the table below is found within the network environment, immediately contact Trustwave

File name	MD5 Hash(s)
csrsvc.exe	1f9d0d200321ad6577554cc1d0bb6b69
MemPDumper.exe	dbaab511f2210228e41c3ffdbe5d3fce
dnsmgr.exe	bf27e87187c045e402731cdaa8a62861
dirmon.chm	ac15d275d4d01c453aab907da7051f81
WinMgmt.exe	3e19ef9c9a217d242787a896cc4a5b03
install.bat	a7c24031cae3f29ec0c30d220c52a087
dump.bat	9393aaf96f3fc25bfcc6649e33edc560
psexec.exe	579b43e13294eb85faa7c28b470b19c1
play.bat	fcb37de3b9b1c831a52a836b7a2f2695
Far.exe	d1d9c26a77beb82b13c82e854042dc92
compenum.exe	bcc61bdf1a2f4ce0f17407a72ba65413
shareenum.exe	3ca6ec07c6b840e7a256d09839ba0c4f

Trustwave periodically issues Security Alerts such as this one to inform customers about threats that may affect their efforts to protect cardholder data, secure their network environment and comply with the Payment Card Industry Data Security Standard. Trustwave deemed the threat discussed in this alert severe enough to warrant distribution among our customer base.

Trustwave®
Information Security & Compliance