Malware Targeting Point of Sale Systems | CISA

Published: 2016-10-06 · Archived: 2026-04-05 17:14:38 UTC

Systems Affected

Point of Sale Systems

Overview

Point of Sale Systems

When consumers purchase goods or services from a retailer, the transaction is processed through what are commonly referred to as Point of Sale (POS) systems. POS systems consist of the hardware (e.g. the equipment used to swipe a credit or debit card and the computer or mobile device attached to it) as well as the software that tells the hardware what to do with the information it captures.

When consumers use a credit or debit card at a POS system, the information stored on the magnetic stripe of the card is collected and processed by the attached computer or device. The data stored on the magnetic stripe is referred to as Track 1 and Track 2 data. Track 1 data is information associated with the actual account; it includes items such as the cardholder's name as well as the account number. Track 2 data contains information such as the credit card number and expiration date.

POS Targeting

For quite some time, cyber criminals have been targeting consumer data entered in POS systems. In some circumstances, criminals attach a physical device to the POS system to collect card data, which is referred to as skimming. In other cases, cyber criminals deliver malware which acquires card data as it passes through a POS system, eventually exfiltrating the desired data back to the criminal. Once the cybercriminal receives the data, it is often trafficked to other suspects who use the data to create fraudulent credit and debit cards.

As POS systems are connected to computers or devices, they are also often enabled to access the internet and email services. Therefore malicious links or attachments in emails as well as malicious websites can be accessed and malware may subsequently be downloaded by an end user of a POS system. The return on investment is much higher for a criminal to infect one POS system that will yield card data from multiple consumers.

Impact

There are several types of POS malware in use, many of which use a memory scraping technique to locate specific card data. Dexter, for example, parses memory dumps of specific POS software related processes looking for Track 1 and Track 2 data. Stardust, a variant of Dexter not only extracts the same track data from system memory, it also extracts the same type of information from internal network traffic. Researchers surmise that Dexter and some of its variants could be delivered to the POS systems via phishing emails or the malicious actors could be

taking advantage of default credentials to access the systems remotely, both of which are common infection vectors. Network and host based vulnerabilities, such as weak credentials accessible over Remote Desktop, open wireless networks that include a POS machine and physical access (unauthorized or misuse) are all also candidates for infection.

Solution

POS System Owner Best Practices

Owners and operators of POS systems should follow best practices to increase the security of POS systems and prevent unauthorized access.

- **Use Strong Passwords:** During the installation of POS systems, installers often use the default passwords for simplicity on initial setup. Unfortunately, the default passwords can be easily obtained online by cybercriminals. It is highly recommended that business owners change passwords to their POS systems on a regular basis, using unique account names and complex passwords.
- **Update POS Software Applications:** Ensure that POS software applications are using the latest updated software applications and software application patches. POS systems, in the same way as computers, are vulnerable to malware attacks when required updates are not downloaded and installed on a timely basis.
- **Install a Firewall:** Firewalls should be utilized to protect POS systems from outside attacks. A firewall can prevent unauthorized access to, or from, a private network by screening out traffic from hackers, viruses, worms, or other types of malware specifically designed to compromise a POS system.
- **Use Antivirus:** Antivirus programs work to recognize software that fits its current definition of being malicious and attempts to restrict that malware's access to the systems. It is important to continually update the antivirus programs for them to be effective on a POS network.
- **Restrict Access to Internet:** Restrict access to POS system computers or terminals to prevent users from accidentally exposing the POS system to security threats existing on the internet. POS systems should only be utilized online to conduct POS related activities and not for general internet use.
- **Disallow Remote Access:** Remote access allows a user to log into a system as an authorized user without being physically present. Cyber Criminals can exploit remote access configurations on POS systems to gain access to these networks. To prevent unauthorized access, it is important to disallow remote access to the POS network at all times.

Consumer Remediation

Fraudulent charges to a credit card can often be remediated quickly by the issuing financial institution with little to no impact on the consumer. However, unauthorized withdrawals from a debit card (which is tied to a checking account) could have a cascading impact to include bounced checks and late-payment fees.

Consumers should routinely change debit card PINs. Contact or visit your financial institutions website to learn more about available fraud liability protection programs for your debit and credit card accounts. Some institutions offer debit card protections similar to or the same as credit card protections.

If consumers have a reason to believe their credit or debit card information has been compromised, several cautionary steps to protect funds and prevent identity theft include changing online passwords and PINs used at ATMs and POS systems; requesting a replacement card; monitoring account activity closely; and placing a security freeze on all three national credit reports (Equifax, Experian and TransUnion). A freeze will block access to your credit file by lenders you do not already do business with. Under federal law, consumers are also entitled to one free copy of their credit report every twelve months through AnnualCreditReport.com.

Consumers may also contact the Federal Trade Commission (FTC) at (877) 438-4338 or via their website at www.consumer.gov/idtheft or law enforcement to report incidents of identity theft.

References

All About Skimmers

A look at Point of Sale RAM scraper malware and how it works

A message from CEO Gregg Steinhafel about Target's payment card issues

Dexter and Project Hook Break the Bank (PDF)

VSkimmer trojan steals card data on point-of-sale systems

Dexter – Draining blood out of Point of Sales

Point-of-sale malware infections on the rise, researchers warn

New Dexter Point-of-Sale Malware Campaigns Discovered

Happy Holidays: Point of Sale Malware Campaigns Targeting Credit and Debit Cards

Protect your identity from Target security breach

Revisions

January 2, 2014 - Initial Release
