



# Security breach at Sonic Drive In

## Memory Scraping Malware - RAM

Vyanktesh Chandurkar

A00268808

Athlone Institute of Technology

## Overview

Security breach is the access of the personal, sensitive or confidential information without authorization by the unauthorized users, and further leaking it to the unsecure environment like dark web. Leaked data could include public service numbers, credit/debit cards information, user account data like username and password, and internal data of an organization.

Data breach results from the poor IT infrastructures and failure to maintain security on the data. It can negatively affect the organization operation and might lead to serious situations.

## Introduction

Sonic Drive-In , one of the famous US fast food chain, experienced Data breach in september 2017. Breach affected an unknown number of its store payment card systems and compromising millions of customers credit and debit card credentials. The payment card information was stolen from the POS point-of-sale system.

Franchisee of Sonic drive-In situated in Oklahoma city was notified by their credit card service provider about suspicious activities of fraudulent transactions on the cards which were used recently at the stores. Store payment systems (known as POS) were compromised in this breach exposing credit and debit card accounts.

All the stolen cards have been obtained from different locations and were made available for purchase on the underground market. Rates were set high for the recent batch of stolen cards.

Sonic did not disclose the details about the type of attack it has experienced, but POS malware attacks have been identified during this phase of the year which involved installing memory scraping malware at the point-of-systems.

In the POS malware attack, to steal the credit and debit card information from the organization, the POS system is hacked remotely by seeding the system with memory scraping malware that can copy account data stored on the card's magnetic stripe. The stolen data is further used to clone the cards for transactions and payments.

## Memory Scraping Malware (RAM)

A common type of hack to steal credit and debit card information is by installing memory-scraping malware known as RAM on point-of-sale system.

Memory Scraping Malware examines the memory for the sensitive data and allows a hacker to find and steal personal data.

### Scope for RAM

Generally the plastic credit cards contain two sets of information.

- The first is contained within the magnetic stripe and within the stripe are two tracks of electronic information that identifies the card account and account holder.
  - Track 1 contains an alphanumeric sequence based on a standard developed by the International Air Transport Association (IATA). This sequence contains the account number, cardholder's name, expiration date and other data in a sequence recognizable by all POS machines.
  - Track 2 uses a shorter but analogous sequence developed by the American Bankers Association (ABA).
  - Track 3 is almost entirely unused.
- The second identifier on a credit card is the three- or four-digit code often located on the back of the card, known as the card verification number (CVN) or card security code (CSC). This number can add an additional layer of security if it is not included in the electronic data contained in the magnetic stripe.

The data that a POS terminal collects from Track 1 and Track 2, sometimes including the CVN or CSC in Track 1, are held in the memory of that POS machine until it is periodically purged.

All parties to the credit card transaction chain are beholden to the 12 security requirements detailed in the Payment Card Industry Data Security Standard (PCI DSS), but hackers have taken advantage of gaps in this framework.

**The gap that is directly vulnerable to RAM scrapers is the temporary storage of large amounts of intact credit card data stored in the POS machines' software for a short period after transacting a sale. Small merchants are a relatively easy target for cybercriminals, but larger retailers like Sonic Drive-In are far more attractive due to the massive amounts of data they retain at any given time.**

## Functioning of RAM

Data security standards of the payment card industry known as PCI-DSS has a set of standards which includes end-to-end encryption of sensitive payment data when it is transmitted, received or stored.

This payment data is decrypted in the PoS's RAM for processing, and the RAM is where the scraper strikes. Using regular expression searches, they harvest the clear-text payment data and send that information to unsecure servers.

Some of the Memory scraping malwares discovered :

- **RawPOS** : the first PoS RAM scraper which targeted the processes of known PoS software
- **BlackPOS** : this variant was responsible for compromising targets and pretended to be a component of a commercial antimalware program.
- **NewPoSThings** : along with the scraping RAM for stealing credit card data, this malware also attempts to steal Virtual Network Computing passwords from infected systems.
- **GetMyPass** : this malware was designed to read instructions from a configuration file, which allows hackers to specify processes to target for scanning.

## Injection of RAM to infect POS systems

**Inside jobs** : Trustworthy employees of an organization abuse certain privileges to take revenge on their employers.

**Phishing** : Cybercriminals compromises the email accounts injecting malicious messages directly into legitimate conversations between account owners and their contacts, which make it very hard to spot malicious emails, since they come from trusted sources and are part of existing message exchanges.

**Vulnerability exploitation** : Software updates and patches are exploited to compromise the systems as because the patches for vulnerabilities are not applied routinely.

**Security standard noncompliance** : Payment Card Industry Data Security Standard (PCI DSS) provides a set of requirements which maintain a secure environment. But Companies incorrectly configure their PoS environments due to lack of expertise or resources, which makes them susceptible to different malware attacks.


## Strategies to defend RAM:

Companies should implement strategies based on the POS defense model consisting of four layers,

- **Point of entry** : Initial layer where the malware can be blocked before its gets injected into the system to prevent further damage
- **Lateral movement** : If the initial layer fails to block the malware then this layer comes to an effect to identify the suspicious and malicious behaviour and stop it from spreading further.
- **Data collection** : This is the protection layer which prevents the POS malware from stealing sensitive data from the system.
- **C&C and data exfiltration**: Final layer where it prevents the malware from communicating with C&C servers and exfiltrating stolen credit and debit card information.

Some of the Technologies (based on the defense model)

1. **Access Control Lists (ACLs)** : Can be used to restrict read, write, or execute permissions on PoS system directories and folders. This blocks normal PoS RAM scraper behaviors, thus preventing execution, lateral movement, and data theft.
2. **Breach Detection Systems (BDSs)** : BDSs can analyze network traffic patterns across multiple protocols, identify malicious domains, and using emulation sandboxing, model the behavior and impact of dropped or downloaded malicious files. They identify and alert IT administrators about the presence of PoS RAM scrapers.
3. **Firewalls** : Firewalls monitor traffic to unknown and bad domains and identify applications or endpoints that generate or request bad traffic. They block data exfiltration and C&C traffic.
4. **Host-based Intrusion Prevention Systems (HIPSS)** : HIPSSs monitor and analyze events that occur on hosts to identify suspicious or malicious activities.

- 
5. **Intrusion Prevention Systems (IPSs) / Intrusion Detection Systems (IDSs)** : IDS / IPS are network security systems that examine traffic flow to detect and prevent network-based attacks. IDS are passive systems that generate reports when known bad events are identified. IPS reject packets when known bad events are identified.
  6. **OS hardening** : Making an OS more secure by reducing its surface of vulnerability exposure. This can be achieved by installing security software; applying patches; enforcing password complexity requirements; and eliminating unnecessary software, user accounts, services, network ports, drivers, subsystems, features, and others.
  7. **Security Information and Event Management (SIEM)** : SIEM software and services provide real time analysis of security alerts generated by network hardware, servers, endpoints, and applications.
  8. **Penetration Testing** : Penetration testing on systems, networks, and Web applications allows IT administrators to find vulnerabilities that attackers can exploit.
  9. **IT Security Professionals** : IT security professionals specialize in detecting, preventing, and resolving computer security threats in a business environment. They also maintain the integrity and confidentiality of the company's data and information systems.

## Payment processing architectures to prevent RAM scrapers

The underlying principle behind the new payment-processing architectures is if the information present on the tracks of the magnetic stripe of the card is not present in PoS systems RAM.

Leading solutions based on this principle are encryption plus tokenization and secure element which works with the EMV credit cards.

## ENCRYPTION PLUS TOKENIZATION

The encryption plus tokenization payment architecture encrypts and tokenizes credit card data, making credit card data theft virtually impossible.

In this architecture,

1. Customers swipe their credit cards at merchants PoS terminals to complete purchases.
2. The PoS terminals read, encrypt, and transmit credit card data to the payment service providers (PSPs) for processing. The PSPs then forward the credit card data to banks—acquirers and issuers—for authorization. PSPs use a tokenization algorithm to replace actual credit card data with tokens.
3. The tokens and their bank authorization statuses are then sent back to merchants PoS systems, which store tokens instead of actual credit card data in all places.

The encryption plus tokenization payment architecture ensures that actual credit card data is never present in PoS systems' RAM or on any other merchant system. Stolen tokens cannot be used to create counterfeit credit cards and cannot be used in card not-present transactions.

## SECURE ELEMENT

Another architectural solution created by Intel uses a secure element to process credit card transactions.

Credit card data is read by PoS terminals and directly sent to a secure element, which Intel calls "Protected Applet," bypassing the PoS software. Protected Applet manages all transaction-processing requests with banks and can be configured to share certain data with PoS software. Moving all credit-card-processing actions to the secure element and completely bypassing PoS systems RAM ensures that sensitive data cannot be stolen by malware. Secure element is designed to be tamper resistant and cannot be infected by PoS RAM scrapers.

## Conclusion

Cybercriminals usually compromise POS systems by Phishing emails to steal and use the administration credentials, through physical access, by Vulnerability exploitation through malicious software updates or patches. Preventing such attacks depends on many aspects of an organization's security posture.

As PoS RAM scrapers become more prominent threats, big businesses will heavily invest in cybersecurity to prevent attacks against their PoS environments.

The new measures of EMV and PCI DSS standards will significantly change the PoS field for attackers.

If there is a successful implementation of the new measures, there will be a decline in the number of PoS-related data breaches. As businesses upgrade to new secure payment systems, attackers will attempt to come up with new strategies against improved systems and environments.

Hackers will find new ways to breach the security of target companies via third-party vendors who have access to their corporate networks. Third Party vendors will be the weakest link in the chain because they may not necessarily have the same level of security as their corporate customers. PCI DSS standards aim to strengthen third-party vendors security requirements to minimize the risks they pose to their corporate customers.

New payment technologies and compliance standards aim to stop PoS system breaches. Their complete deployment will successfully prevent a majority of the PoS system attacks. But because easy money making is involved, it is safe to assume that cybercriminals will figure out new breach strategies to compromise the security of systems, businesses, and consumers.



## References

Brian Krebs. (10 October 2013). Krebs on Security. "Nordstrom Finds Cash Register Skimmers." Last accessed on 22 August 2014, <http://krebsonsecurity.com/2013/10/nordstrom-finds-cash-registerskimmers/>.

Numaan Huq. (September 2014). Trend Micro Security Intelligence. "PoS RAM Scraper Malware: Past, Present, and Future." Last accessed on 11 December 2014, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf>.

Numaan Huq. (4 December 2014). TrendLabs Security Intelligence Blog. "Planes, Trains, and Automobiles—Are You Safe from PoS Malware Anywhere?" Last accessed on 11 December 2014, <http://blog.trendmicro.com/trendlabs-security-intelligence/planes-trainsautomobiles-are-you-safe-from-pos-malware-anywhere/>.

Anthony Joe Melgarejo. (27 November 2014). TrendLabs Security Intelligence Blog. "New PoS Malware Kicks Off Holiday Shopping Weekend." Last accessed on 17 February 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/new-pos-malware-kicks-off-holidayshopping-weekend/>.

<https://securityboulevard.com/2017/10/sonic-drive-blames-credit-card-breach-malware/>  
<https://medium.com/swlh/data-security-breach-at-sonic-drive-in-e9a71ac61cf7>  
[https://en.wikipedia.org/wiki/Memory-scraping\\_malware](https://en.wikipedia.org/wiki/Memory-scraping_malware)