The Evolution of Point-of-Sale (PoS) Malware

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-evolution-of-point-of-sale-pos-malware

In 2014, we saw several data breach incidents where Point of sale (PoS) malware was used to hit organizations, institutions, and users. Since the bad guys naturally go where the money is, it's easy to see why cybercriminals target PoS terminals, given that they know the different places where credit cards are routinely used. As we have observed multiple PoS malware

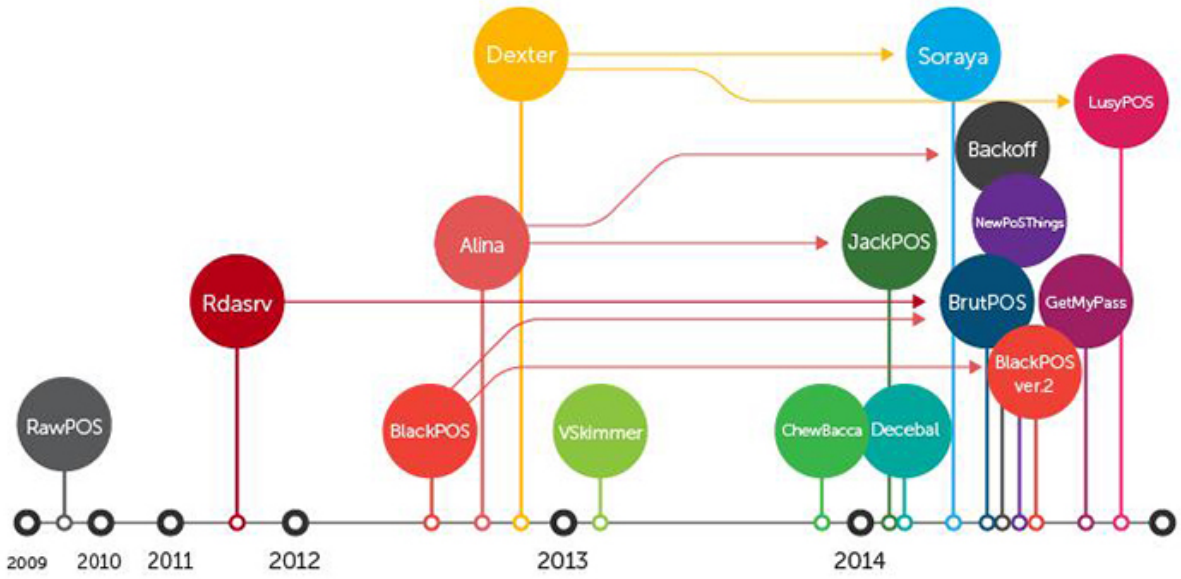
families, it is important to learn that personal and sensitive information stolen from credit and debit cards can be used to impersonate unsuspecting customers. This could result in fraudulent purchases, financial loss, and damaged credit standing.

PoS malware has evolved rapidly over the past few years, targeting mostly big retail companies from which they could obtain large chunks of data as opposed to individual sources.

PoS Systems and Evolving Threats

A PoS device is designed to complete transactions as it calculates the amount of purchases made by a customer, as well as provide other operational information such as inventory management, accounting, and tracking sales. PoS systems require a connection to a network to validate payments by sellers. Small businesses may use a cellular data connection, while bigger companies employ internal networks. Most PoS devices run on Windows and UNIX operating systems, making them easy to operate, maintain and develop software for devices. However, this also means that malware could easily be developed to infect these systems.

In the past, criminals devised physical skimmers to rub payment cards and steal data. This required the bad guys to be physically close to the PoS terminal and thus risked being found out. Today, cybercriminals resort to using malware for stealing data primarily from credit cards, and the malware used has continually evolved. As shown in the timeline below, they've branched out into various malware families that target PoS devices. And where does all the stolen data go? They're either used for illegal purchases, or traded in underground markets.



How PoS Malware Works

The payment card industry complies with a set of security standards that enforce end-to-end encryption of sensitive payment data captured from payment cards during transactions. However, the data that can be found inside the PoS device memory could be in stored in an unencrypted form. Typical PoS RAM scraper malware captures the payment card information directly from the memory, where it scrapes customer data and information.

While they all typically share a similar end-goal, the different PoS malware types are designed to do the deed in different ways. Here are some of the notable PoS malware types we have reported on in the past few months:

Backoff – a successor of Alina (aka Track) whose variants are known for scanning all running processes to retrieve card track data and gather affected system information, Backoff, uses the same installation technique used in the Alina family of PoS RAM-scraping malware. Based on our research, Backoff implements an updated data search function and drops a watchdog process to ensure that it continuously runs in the system. Discovered by the US Computer Emergency Readiness Team (US CERT), this PoS malware targeted the US. Interestingly, we saw a clear decrease of hits during "dead hours" specifically at 2:00 AM, and an apparent recurring rise of hits at 10:00 AM. This trend follows regular business operation hours wherein PoS devices are more likely to be active and in use. Generally, the hits increase during business hours and decline during off-hours.

BlackPoS version 2.0 – this PoS malware clones the exfiltration technique that the BlackPoS variant used to compromise US retailer Target. BlackPoS version 2.0 pretends to be an antivirus product installed on a system to avoid user suspicion. Our researchers in Trend Micro found that the source code of the original BlackPoS was leaked, enabling other cybercriminals to enhance its code. According to our findings, this malware appears to have been used in the massive data breach that targeted Home Depot.

[Read: Home Depot confirms breach, reported to be largest on record]

In 2014 alone, PoS malware was used to hit several large retail companies in the US. In the wake of these attacks, we also recently found a new PoS malware that emerged in time for the holiday shopping weekend. Called GetMyPass, this new PoS malware is dependent on its configuration file, which means that it was designed to be flexible. Based on other PoS malware routines we analyzed, GetMyPass appears to be designed as a multicomponent malware similar to an earlier BlackPoS variant. We continue to monitor this malware as it develops.

Additional Resources:

Defending Against PoS Malware

PoS malware attacks continue to be prevalent, as shown by new malware families that have been recently discovered. As such, we have brought together some recommendations for both companies and their customers to protect against such attacks.

Since most attacks target mostly retail and hospitality industries, it is critical for merchants to take these preventive measures:

- Secure PoS devices and networks
- Comply with Payment Card Industry (PCI) security guidelines
- Strengthen anti-malware security
- Deploy patches accordingly

Customers must also take some steps to ensure that their accounts are not at risk:

- Check your bank and credit statements. Reviewing transactions on a regular basis can help you monitor and spot fraudulent transactions made on their card.
- Make sure all operating systems across all devices are up-to-date
- Install security software on devices used for online transactions

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats, PoS Malware, Data Breach