Guide to POS Security

givex®

Guide to POS Security

Intro

You might be underestimating the threat to your POS system's security.

Firstly ask yourself a few questions:

Do you know what types of malware attack POS systems the most?
Do you know how much you can be fined for not being PCI compliant?

If you don't know the answers to these questions you may be in trouble.

Fraudulent activities and malicious malware have cost big businesses their reputation and sales profit and have resulted in small businesses shutting down.

If you do not want to be next, read on to learn what threats exist, how they work and how to best protect yourself.

Malware

Problem

POS malware is malicious software written and installed in a POS to steal customer payment data, especially customer credit card data.

There are many different types of malware, all designed to infiltrate your POS, with differences in how the varying malwares work.

MalumPOS, vSkimmer, BlackPOS, GamaPoS for example all work in different ways with the same endpoint – infiltrating your POS system.

Here is a rundown of how a sampling of different malwares work and infect the POS:

Variants

MalumPoS

The MalumPoS malware can be reconfigured by cyber thieves to breach a wide range of POS systems. It especially targets Oracle Forms, Shift4 systems and those accessed via Internet Explorer so watch out if your employees are accessing the Internet on downtime!

Once it is successfully installed in a POS system, this malware disguises itself as the "NVIDIA Display Driver" or displays as "NVIDIA Display Driv3r". For users the familiarity of NVIDIA components help disguise this malware and make it seem harmless. However this malware is far from harmless, as it selectively looks for any data on Visa, MasterCard, American Express, Discover, and Diner's Club cards. This malware is very configurable and can evolve rapidly.

Affected Brand:
Dairy Queen

395 locations were attacked by Backoff POS malware leading to approximately 600,000 credit and debit cards being affected.

Backoff

Backoff scrapes memory from running processes on targeted devices. It is a prevalent maleware and has been planted on POS systems by cyber thieves aiming to steal consumer card data. It has many variants such as ROM, Wed and 1.5.

vSkimmer

The vSkimmer malware targets POS systems using Windows OS to steal credit card information. It infects the POS in the file named 'iexplorer.exe'. It then stays active by rewriting itself in the registry key and then hijacks credit card data and transfers it to a command-and-control server. This may all sound really technical but the bottom line is that this malware takes over a core part of Internet Explorer on Windows machines.

Affected Brand: Target

Target saw 70 million records stolen in a malware attack. These records included the name, address, email and phone numbers of Target customers. Target saw a 46% drop in profits after this attack.

BlackPOS

BlackPOS a.k.a "Kaptoxa" targets POS systems with readers running Windows. It's important to note that this was the malware found on Target and Home Depot's POS systems when they had their massive breaches. BlackPOS discovers systems through automated Internet scans. It then compromises POS systems through weak remote administration credentials or un-patched vulnerabilities. It scans for Track 1 and Track 2 formatted data, and stores it in a file called 'output.txt' before uploading it to a compromised server.

Affected Brand: Home Depot

56 million customer debit and credit card numbers were stolen from Home Depot's POS system. It cost $62 million for Home Depot to recover from the attack.

GamaPoS

GamaPoS removes credit card data from PoS systems. It is different as it uses malware coded using the .NET framework. So basically it overpowers and infects POS systems by launching a large volume of malware. Targeting by using a 'dynamite fishing' approach it launches spam with the intent to distribute Andromeda botnet. You should watch out for malicious emails that contain attachments that actually contain malware or links to compromised websites.

This list is not exhaustive – remember there are always new threats and cyber thieves are constantly evolving the malware they use to attack vulnerable POS systems. Hackers are always ready to attack your business and cause irreparable damage in the form of loss of sales and reputation. Your business should always be ready to defend itself with a secure POS.

The Solution

Malware is contracted in a number of ways, depending on how each malware is designed. However there are certain key ways you can decrease the likelihood of being targeted and infected by a POS malware.

Ways to defend against Malware :

- **Limit unauthorized Internet browsing** – Many malwares infect the POS via the Internet. Unauthorized Internet browsing on the part of your employees could result in a disaster. Some malwares even infiltrate the POS via unsuspicious-seeming emails. POS apps which operate via the Internet expose you to malware threats. Choosing a POS like Vexilor which restricts unauthorized Internet browsing is key to avoiding malware attacks.

- **Watch out for Windows XP based POS software** – Windows embedded for Point of Service SP3 is the produc t in use for point of sale systems. Built from Windows XP Embedded its Extended Support will end April 12, 2016. So if your POS is running on Windows XP you may be vulnerable soon and an upgrade can be costly.

- **Make sure your POS is up-to-date with security patches** – Pick a POS provider that regularly provides security patches and software upgrades at no extra cost. Also get security software with advanced monitoring, vulnerability management and applications control capabilities and anti-fraud functions.

- **Choose a cloud POS** – Pick a cloud POS that will not store credit card on your POS itself. This lessens the attractiveness of your POS as a potential target for cyber criminals who target POS systems mainly for the sensitive information they house.

PCI

Problem

PCI compliance is a must for companies that process store or transmit credit card information. Specifically PCI compliance is a set of requirement designed to ensure that companies maintain a secure environment.

There are 6 main requirements for PCI compliance. The company must:

1) Build and maintain a secure network
2) Protect cardholder data
3) Maintain a vulnerability management program
4) Implement strong access control measure
5) Regularly monitor and test networks
6) Maintain an information security policy

PCI Exempt

Certain POS systems, such as Vexilor by Givex, are PCI Exempt. This is due to the way we structure the architecture such that we never see, hold or transmit unencrypted credit card data. We are one of the first POS providers to do this and provide this exceptional level of security to our clients.

As a result of our PCI Exempt status, Vexilor is now one of the most well integrated systems with payment providers adhering to this methodology.

Furthermore, the Givex platform is certified PCI Level 1, the most secure possible.

What Will Happen if You Are Not PCI Compliant or PCI Exempt?

- **Noncompliance Fines:** The fines you can face for being noncompliant range from $5,000 to $500,000. These fines are levied by banks and credit card institutions. Banks can fine based their forensic research which they must do to address noncompliance. Credit card institutions who levy fines for noncompliance may propose a timeline for how they will increase fees. For example after 3 months the fine could go up to $50,000 monthly after initially being $10,000 per month.
- **Suspension:** There may be potential suspension of credit card account from your provider.

What if you are Breached?

- **Reputation Loss:** Big brands and small businesses alike can lose hard-won reputation with customers, suppliers, and partners as a result of a breach in regards to cardholder data.
- **Legal:** Possible civil litigation from your breached customers.

The Solution

It is important that you ensure your POS is PCI Compliant or PCI Exempt no matter what your business size. A knowledgeable POS provider such a Givex will be able to go over PCI and its ramifications with you.

If you want a commitment free call to discuss which options work for your business vertical and size contact us!

Also follow us on Twitter and LinkedIn.

givex®

More About Givex

Givex is a technology company offering clients a global reach with cost-effective gift card, omni-channel loyalty, analytics, stored value ticketing and cloud-based POS solutions. Our core distinction is taking on the tough task of managing all aspects of the transaction to ensure companies can deliver maximum customer satisfaction. With over 450 POS integrations, Givex powers more than 165 000 installations world-wide. Givex products and services give you insight into your data to enable you to better drive sales growth, customer relationship management and enterprise resource planning.