INFONALIGY
Security Today for Tomorrow's Threats

The Plastic Breach

PROTECTING THE RETAIL SECTOR

THE PLASTIC BREACH

PROTECTING THE RETAIL SECTOR

THE RISING COST OF FRAUD

Who would have thought that a small piece of plastic measuring a mere 2.125 inches by 3.370 inches could open a window to so much mayhem? For the past three years, cybercriminals have been targeting the retail industry. During 2014, we saw large-name retailers like Michaels, Neiman Marcus, PF Chang's, Staples, Dairy Queen, Goodwill, UPS, Target, and Home Depot all make headlines.

With over 1 billion credit cards in circulation in the US alone and over 7 billion worldwide, fraud in the retail sector has been on the rise for years. Cyber criminals have been targeting Point of Sale (PoS) terminals and hacking networks of retailers to steal millions of identity and credit card records — as well as other data and merchandise.

In 2014, 81 percent of companies that Check Point researchers studied experienced a data loss. Data breaches worldwide increased 49% and the number of data records lost or stolen increased 78% from 2013 to 2014 according to a Wall Street Journal blog. The article cites a 2015 report from digital security firm Gemalto, estimating 1 billion data records were compromised across 1,500 attacks last year. Of these, the retail industry suffered the most, representing 55% of the total data breaches with much of the focus on point-of-sale (PoS) systems.

The cost of those losses are increasing as retailers have to invest in protecting their customers as well as their networks. At the same time, they're managing huge waves of media attention and investor scrutiny.

According to a 2014 LexisNexis study called the True Cost of Fraud:

- Every dollar of fraud cost merchants
- $3.08 in 2014. Lose $10 million of data and expect it to cost your organization
- $30 million, driven up by costs to manage and secure mobile payment and on-line ordering systems
- The average merchant suffered 133 successful fraudulent transactions per month in 2014, up 46% from last year

IN THE WORLD OF HACKING, THERE IS ONE CONSTANT: THERE IS ALWAYS A WAY IN

CONTINUED >

There are several layers of security needed to protect customer credit card and identity data. It is no longer simply a data center issue. Securing your central information databases with good next-generation firewalls against advanced persistent threats (APTs) and bots, and ensuring compliance modules and threat management and monitoring is in place is definitely important. But what about protecting retail locations and PoS terminals?

In the world of hacking, there is one constant: there is always a way in. When you patch one security hole, cyber criminals find another. To help address the issues, we provide insights into how to spot a potential infection, and best practices your organization can adopt to better secure your entire network, starting with your PoS terminals. A thoughtful security plan leads to reduced risk, which in turn leads to happier and better protected customers.

INFECT ONE PoS TERMINAL AND IT IS SIMPLE TO INFECT THEM ALL

2014

81 PERCENT
OF COMPANIES STUDIED HAD EXPERIENCED A DATA LOSS

WHY PROTECT THE POS

Good security starts at the edge, which in the case of much of the retail industry means store locations and PoS terminals. Many in the industry believe having a more secure credit card will mitigate risk with transactions. A new global standard for credit cards hopes to do just that. Europay, MasterCard, and Visa
(EMV) promises better security through inter-operation of integrated circuit (IC) chips in credit cards.

The United States has started to take a major step in catching up with European markets that already use some form of EMV cards. Whether chip and PIN, or chip and signature, according to the Wall Street Journal, lenders are planning on issuing 575 million of these cards in 2015. While the EMV cards will be more secure in general, they also force retailers to upgrade all of their PoS terminals to support the new technology, thereby improving security.

CONTINUED >

Unfortunately, EMV solutions do not safeguard online or already infected PoS terminals. So, they will not magically solve all PoS vulnerabilities.

PoS terminals typically run a fairly simple operating system without a lot of heavy security protections, which is what makes them easy targets. They are often not updated regularly with modern anti-virus software; worse, they are typically connected both to each other and to a corporate network. Infect one and it is simple to infect them all. Infections like the 'BackOff' malware that impacted more than 1,000 U.S. businesses, actually highlighted a larger security vulnerability. BackOff pre-installed tools in the supply lines of seven major manufacturers of PoS terminals before being shipped to merchants worldwide. Weak or unchanged admin passwords allowed hackers remote access into devices.

The larger problem, however, is that huge media coverage of BackOff exposed how easily and effectively a PoS terminal could be hacked. ■

EVERY DOLLAR OF FRAUD COSTS MERCHANTS $3.08

How To Spot A Hack

IT DEPARTMENTS HAVE TO BE SAVVY across a range of topics to keep complex networks operating; expand business capabilities; and maintain safety. Knowing when something looks suspicious speeds both the detection and defusing of malware on your network. Following are simple steps to help spot and identify the attributes of a suspicious set of files.

STEP 1

BE SUSPICIOUS OF THE ALMOST ORDINARY

Malware is often made up of rogue files designed to hide in plain sight. Like a forger, a cybercriminal recognizes their files will be seen and will need to pass at least visual inspection. They use file names that look familiar, embed digital certificates that appear valid, and insert comments in their code to signal it was written by a valid company. On the surface, everything may look reasonable, but any kind of close inspection will uncover flaws.

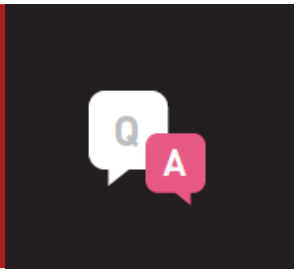
If you suspect there is malware in a directory, look across the file names for any files that look out of place — especially if they have legitimate looking names but are in the wrong directory.

If you find one, use common and basic inspection tools (such as the Microsoft SysInternals suite) to examine it.

- Using the Strings utility, look for references or file names containing anything suspicious: Mimikatz (a tool for extracting passwords from memory) or Getmypass (a tool designed to scrape RAM memory that is sometimes used to steal credit card data).
- Look for file sizes that are larger than expected. Use tools from Microsoft SysInternals to get a better understanding; examine a certificate if it exists; and keep the vendor information so you can look it up.

STEP 2

KNOW WHAT QUESTIONS NEED ANSWERING



Once you identify a set of files that might be malware, there are several questions you want to answer. Knowing what questions need answering will help you focus your search efforts.

- What can you discern about the nature of the files?
- What is the malware's purpose and target?
- Can you explain how the malware was inserted?
- Can you uncover how the malware extracts data?
- Can you find clues about the identity of the malware authors or location?

Knowing the answers to these questions can help a forensic analysis team focus their efforts. Knowing the answer to one might help uncover answers to other questions.

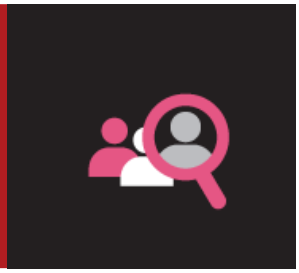
For instance:

- If the PoS device was new out of the box and contained suspicious files, you know that it came that way from the manufacturer.
- If there is a unique file name, you can search the Internet to see if others have encountered similar issues and perhaps find additional data.
- Executable files may contain debug information. Knowing that, you can uncover the project path as created on the malware author's computer, which provides unique information such as project names or purposes.
- All digital signatures need to be registered. So, following the links from a digital signature application that was granted, then revoked, would supply additional data on the malware authors or their location.

Each piece of data can provide clues and pointers to more data. Before you know it, a picture will emerge as each of your questions gets answers.

STEP 3

ISOLATE, THEN INVESTIGATE



There are two main methods for analyzing malicious files:

1. Static analysis that gathers evidence from the binary file without actually running it.
2. Dynamic analysis that runs the file and observes its behavior.

As you can see from Steps 1 and 2 (detailed on previous two pages), static analysis and keen observation can produce quite a bit of information. Some facts, however, only come to light once activating the files. That's where dynamic analysis comes in.

For instance, where the malware is targeting to obtain its data, how the data is stored, and where the malware sends the hacked information might only be revealed when the rogue code is active.

When performing dynamic analysis, we highly recommend using threat emulation technologies, as well as the analysis tools they provide, for protection of your data. Isolating rogue code to a threat emulation system will ensure the malware does not steal any of your actual data since it isolates its activities outside your normal network.

Threat emulation systems also come with special tools that allow for analysis of the malware in action. Ideally, these systems should offer the best catch rates of unknown malware and be offered within OS emulation as well as have CPU-level exploit identification.

STEP 4

USE YOUR RESOURCES

There are many tools to analyze malware that are industry-safe open source tools. When analyzing something as potentially dangerous and complex as modern day malware, we recommend using all the tools and resources at your team's disposal.

As we noted earlier, the static analysis tools of smart IT people who understand software is an ideal place to start. It is also useful to search online for issues and problems that others experience with the same equipment. This often makes the analysis proceed at a much faster rate.

When it comes to dynamic analysis tools, there are many open-source software suites capable of analyzing suspicious files. In the Check Point Malware Analysis blog we referenced on page 8, we used Cuckoo Sandbox but there are several others that will also work. As cybercriminals tend to favor producing fake analysis tools, we recommend taking advice on which tools are best from a known, reputable source.

STEP 5

FOLLOW THE TRAIL

When you analyze suspect files statically, you can probably answer at least some of the questions posed in Step 2 (page 10). The dynamic analysis should produce even more data. At this point, we recommend writing down everything you know from the two analyses and see if you can derive additional information. For instance, when you go back and answer some of your initial questions, follow the format of this example:

- **Understand the nature of the files**

STATIC ANALYSIS: Found the files had some of the characteristics of manually-operated hacking tools but no actual malware was detected. One of the files was identified as a memory scraping tool used to steal credit card data from PoS systems.
DYNAMIC ANALYSIS: Found that the files were, in fact, hacking tools that were customized and obfuscated to avoid detection.

- **Understand the malware capabilities and estimate its damage potential**

STATIC ANALYSIS: The tools allowed an outsider to gain remote access and gather OS and domain passwords using theMimikatz tool; scan network computers using the SoftPerfect network scanner; and scrape memory for credit cards using theGetmypass PoS memory scraper.

- **DYNAMIC ANALYSIS:** Discovered the attacker would require access to the computer to operate the tools, but the damage could be anywhere from leaked private data up to a full network disclosure.

- **Explain how the malware extracts data**

DYNAMIC ANALYSIS: Found one of the samples to be a version of WinSCP used to extract files from a network. The tool maybe run manually or by another tool to try to connect to specific IPs, possibly giving away the hacker's stolen data drop location.

- **Obtain clues about the identity of the actors behind the malware**

STATIC ANALYSIS: Found that the digital certificate used was issued, then revoked minutes later. The registration data for that digital signature traced back to a Russian teenager who could be directly or indirectly involved in the incident.

Just these two simple techniques with a little knowhow and time produce a great deal of data. When you use this data to search further, you can build a profile of the hacker and their techniques. Using the tools could dramatically increase the security posture of your network and reduce the chances of data loss.

Protect Yourself And Your Customers

PROTECTING YOUR BUSINESS IS NOT JUST about protecting your PoS terminals, but protecting the entire network. To protect against fast-evolving attacks, companies must adopt a security mindset with dynamic architectures that update with real-time protections. In the following pages, we provide some principles that all organizations should keep in mind.

PRINCIPLE 1

PROTECT YOUR DATA AT REST AND IN TRANSIT

Encrypt your data. It is surprising how seldom this is done — even when companies store sensitive data. The early 2015 discovery of the breach of US health insurer Anthem, for example, stored the Social Security numbers of 80 million customers without encrypting them.[1] Worse, less than four percent of all 2014 data breach incidents involved data that was encrypted either in part or in full.[2]

Secure your data at rest and in transit and proactively block exfiltration attempts.

1 Wall Street Journal Blog, "1 Billion Data Records Stolen in 2014," Feb 12, 2015
2 Gemalto Breach Level Index Report, Feb 12, 2015

PRINCIPLE 2

BUILD GOOD FENCES

The old expression good fences make good neighbors definitely applies to security segmentation. Imagine leaving your back gate open, the back door to your house, and your jewelry safe unlocked for anyone to see. Why do the equivalent with your network?

Creating a security plan means segmenting each part of your network. This makes it more difficult for a hacker to move horizontally through your infrastructure. Follow what is called a 'zero-trust' network approach, where all network communication between segments is clearly delineated and assigned an associated risk value based on three main factors:

1. Whether the transmission is of critical information
2. Whether it is within the PoS management plane, and
3. Whether it contains critical credit card data

Use secure communications and strict access controls, and monitor traffic from segment to segment to limit movement.

Segment PoS systems from other network-connected machines and ensure customer payment data only flow to required areas of the network.

PRINCIPLE 3

CREATE LAYERS OF PROTECTION WITH CHECKS AND BALANCES

You give a lot of thought to your work and how to best position yourself for success. Now do the same with securing your business. Create a protection plan for your network that applies three main elements to each of the segments you created: (1) Enforcement Layer with protection rules; (2) Control Layer that outlines who should have access to what segments and defines how data should flow through your network; and (3) Management Layer to monitor and control it all. The implementation of this strategy could be as follows:

1. Enforcement Layer: Create a gateway- and endpoint-based protection plan that scans, identifies and blocks malware, botnets and weaponized content that's designed to infect machines, and collect and exfiltrate customer information. Assign network - and application-access authentication rules to prohibit unauthorized users and systems from accessing sensitive areas of the network.
2. Control Layer: Establish administrator-determined security policies and automated protections. Create rules that specifically define access control and data security policies with enforcement points. Restrict applications and system behavior according to 'least privilege' guidelines.
3. Management Layer: Monitor all business-aligned administrator privileges and create comprehensive reporting. Implement intelligence-based threat prevention that updates independently and proactively distributes new protections to enforcement points. Keeping up to date is one of the huge vulnerabilities in most networks. Implement event management with logging and reporting tools that identify events in real-time and include filtering and analysis tools. This ensures administrators have visibility into attacks without getting lost in less critical noise.

You can find more detail on implementing a security architecture in Check Point's Software- Defined Protection (SDP) architecture.

PRINCIPLE 4

BE DISCIPLINED

It takes discipline to commit to a strong security posture. We frequently see merchants trying to save money by combining their PoS network with their corporate and customer WiFi network connections. Other points of vulnerability: employees browsing the Internet when business is slow and accidentally downloading malware on the corporate network. We have even seen cases where a well meaning employee downloaded what they thought was a computer registry cleaner to speed up performance and accidentally downloaded malware that infected the entire corporate network. Make sure your employees understand risks and responsibilities around data.

CONCLUSION

CREATE A PROACTIVE SECURITY PLAN

A multi-layer approach like SDP provides a modular and manageable security architecture that helps address today's and tomorrow's security challenges. Create your security plan. Implement your plan. Stick to your plan.

Infonaligy has many tools designed to protect the retail environment. For a detailed analysis of the steps you can take to secure your business, we recommend reading Check Point's **POINT OF SALE SECURITY SOLUTION BRIEF** and contacting your Check Point account team.

For more information on Check Point's Software- Defined Protection (SDP) solutions, please visit:

https://www.infonaligy.com

To learn more about how to secure your organization, please visit www.infonaligy.com