STORMSHIELD

The Biggest Threat to Retail Data Ever:

Backoff Malware (and other memory scrapers) are targeting POS systems!

Security like AV and Whitelisting have proven that they can't protect you.

Can you stop Backoff?

ENDPOINT SECURITY

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

Table of Contents

EXECUTIVE SUMMARY:

Retailers are under an unprecedented wave of IT security attacks. Over the past year or so many cyber-criminals have discovered and are exploiting weaknesses in the encryption of data as it moves from the point of the credit card swipe through the PoS system to the processor. This type of malware is called "memory scraping" and it attempts to see and steal the credit card data when it is actually viewable in the memory of the PoS PC for a tiny slice of time. One of the most prominent memory scraping malwares that has been used in many of the most damaging attacks is called Backoff.

Despite significant investments in a multi-layered IT security system and IT security staff and being PCI DSS compliant, the headlines seem to have a new victim listed every week with larger and larger credit card data losses – Home Depot, Target, Goodwill, Dairy Queen, Schnuck's, etc. These retailers thought that they were safe and took what they believed were the necessary actions to safeguard their data yet were still breached. Worse, in nearly every case, the time between when the initial breach occurred and the theft started and when it was discovered and stopped was multiple months.

The economic impact on the breached organizations is often devastating. In addition to crisis management expenses, such as notification to potentially impacted individuals, forensics, credit monitoring and public relations efforts and consumer class actions, retailers can and do face very significant liability arising from claims by payment card brands, such as Visa and MasterCard, and banks and other financial institutions that either issue credit and debit cards to consumers or that process a merchant's credit card and debit card transactions (respectively referred to as "issuing" and acquiring" financial institutions), in addition to potential fines and penalties for noncompliance with the Payment Card Industry Data Security Standards (PCI DSS). There are also harder to measure costs such as revenue declines based on a loss of shopper confidence and a drop in company stock value.

Unfortunately, the reason that Backoff (and all of its variations and other memory scraping malwares) has proliferated so much as a threat to retailers is that it works and the defenses that are generally being used do not stop it. Despite all of the attention and notoriety that Backoff has had the leading security vendors do not have an answer for how to stop it. Their recommendations generally fall into one of two categories: try to stop the malware from ever getting into you PoS computer and, if this fails, invest in better analytic tools so that you will know sooner (versus months later) that you have been attacked and credit card data has been stolen. The challenge with the approach of stopping the malware from getting into your system is that the cyber-criminals are well funded, sophisticated, devious, etc. and, as proven in the new breach headlines in the news every week, they will get past the perimeter defenses to get into your PoS system. Security products like antivirus and whitelisting are helpful in reducing the attack surface but are defenseless against a determined attacker.

The estimates are that Backoff alone has infected over 1,000 retail organizations and only a few hundred of these retailers are currently aware of it in their systems. For the others it will be a very bad surprise when it activates and starts to steal their data. The new approach for IT security vendors is to admit that they can't stop the attacks and suggest that you buy more security software – this time to have better information about an attack after it is working on your PoS system. This approach may

help make the losses smaller but for Home Depot "only" losing 5,000,000 or 10,000,000 credit card data records is still devastating. It is too soon to give up – Backoff malware can be detected and stopped.

Stormshield Endpoint Security (SES) has the unique capability to identify and stop memory scraping malware like Backoff even if it has gotten past the perimeter defenses and is trying to get the credit card data in memory. This paper does a deep analysis of the stages that Backoff uses to penetrate, install, run, hide, steal (scrape) the data, move it out of the PoS and repeat. Each of the stages is examined and an analysis of how SES works to stop it is done for each of these stages. The critical memory scraping stage is examined to show how SES can identify and stop memory scraping.

Memory scraping is a real and significant threat to retail organizations and it is not being stopped by traditional security products. However there is an answer. If a retail organization is concerned that they may already be infected with a Backoff variation (or similar malware) or that they may be a target of an attack, SES will identify the malware if it is already on the PoS and stop any new incursions.

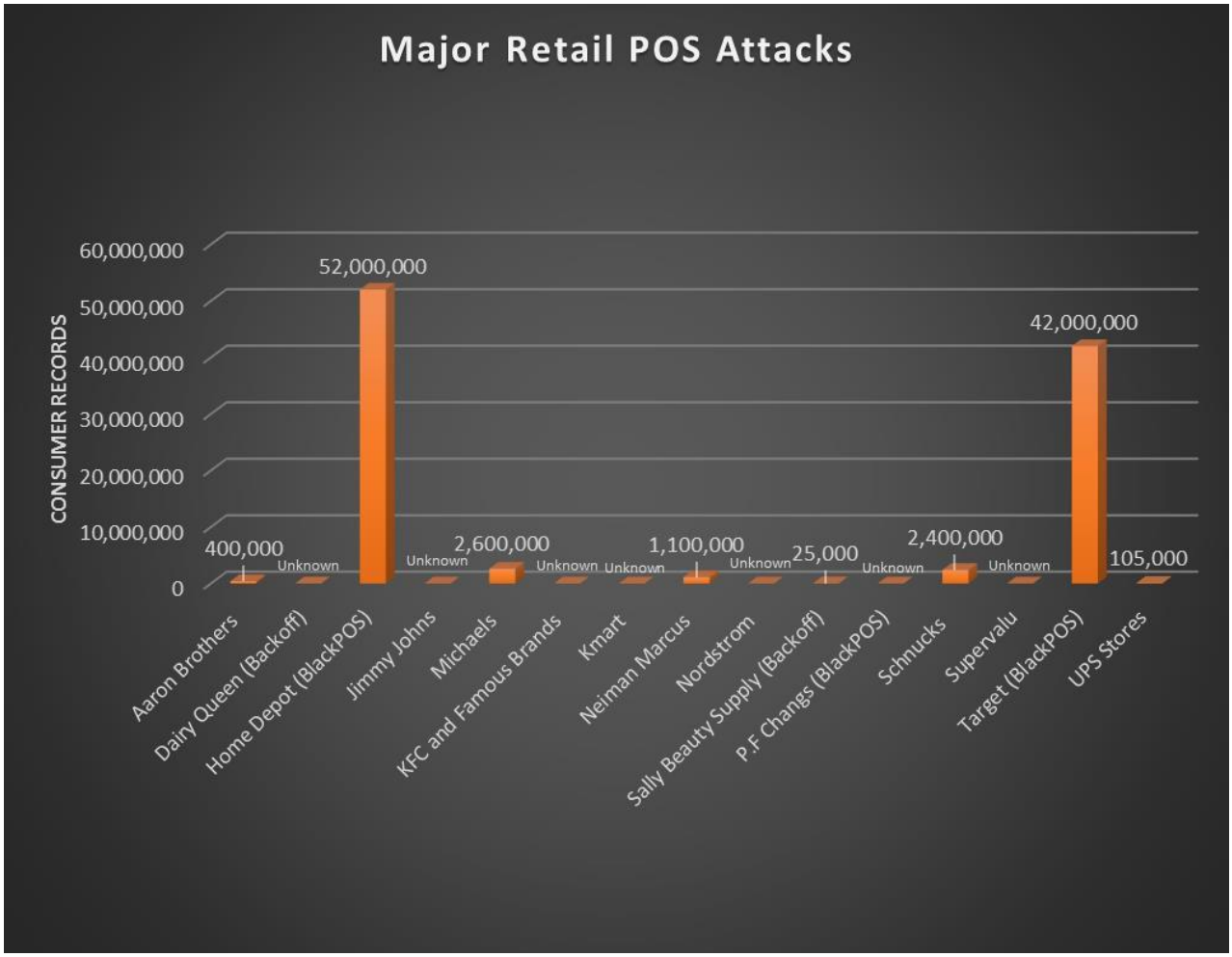
1. Backoff Analysis (and other memory scraping malware)

As a retailer or financial services company you are aware of the relentless attacks by cybercriminals that continue to increase over time. Unfortunately, despite incredible investments in technology and people as well as ensuring certification by standards organizations like PCI DSS, the attackers seem to be having ever-greater success. The attacks are relentless and attackers are dedicated, persistent and very clever. Criminals operate development enterprises that mimic Silicon Valley software companies with development cycles, R&D, QA labs, etc. They find a malware attack strategy that works and then exploit it as effectively and broadly as possible.

The retail industry is an especially lucrative target for these attackers. There is a huge volume of credit/debit card transaction activity and it is being conducted at geographically distributed retail sites where it is difficult to provide great support from a centralized headquarters. The malware using cybercriminals are winning and it is clear that traditional security controls and methods are not sufficient to provide protection.

The recent compromises of high profile name brand retail store chains are making headlines seemingly daily and worrying consumers about the security of their credit and personal data. Recently, the news broke that Home Depot was compromised, before that it was Staples, last month it was Dairy Queen and Goodwill. Home Depot, Dairy Queen and Goodwill are doing investigations like their predecessors Target, Nieman Marcus, Kmart, Supervalu, Michael's, Sally Beauty Supply, Schnuck's and other big

retail name brands that have been compromised. It is clear that many of these breaches started months before they were discovered and disclosed and, as a result of running undetected for extended periods of time, the data for hundreds of millions of customers has been compromised.



2. Economic Impact of Malware

These breaches are not only growing in number but the economic toll that they are taking on the breached retailer is also becoming larger and larger. In addition to crisis management expenses, such as notification to potentially impacted individuals, forensics, credit monitoring and public relations efforts and consumer class actions, retailers can and do face very significant liability arising from claims by payment card brands, such as Visa and MasterCard, and banks and other financial institutions that either issue credit and debit cards to consumers or that process a merchant's credit card and debit card transactions (respectively referred to as “issuing” and acquiring” financial institutions), in addition to potential fines and penalties for noncompliance with the Payment Card Industry Data Security Standards (PCI DSS).

New “records” are being set every few months for the number of credit card holder’s data that is lost by a single retailer’s breach. The costs can be huge and, sometimes more damaging, unknown. Consider these comments from Home Depot in September:

…the Atlanta-based retailer cautioned that its latest fourth-quarter earnings estimate doesn't include a long laundry list of potentially major costs related to the cyber attack that put payment card information at risk for some 56 million customers. Following an investigation that began September 2, the company eliminated malware related to the attack from its U.S. and Canadian networks as of Thursday. The attacks are believed to have occurred from April through September of this year. An array of yet-to-be estimated and potentially steep costs aren't included in the company's latest earnings outlook. Among unknown costs for Home Depot are reimbursements to credit card companies for fraud and card re-issuance costs; liabilities from civil litigation, governmental investigations and enforcement proceedings; legal and investigation fees as well as further expense for fixing the problem.

From SC Magazine March 20, 2014: “*The cost of a data breach or malware infection extends well beyond the dollars spent on responding and addressing security issues — productivity takes a big hit as enterprises and consumers spend countless hours dealing with the threats, according to a joint study from IDC and the National University of Singapore (NUS).*

While researchers predicted that enterprises around the globe will spend around $500 billion in 2014 on making fixes and recovering from data breaches and malware, consumers worldwide will likely spend $25 billion as a result of those security threats. They also waste 1.2 billion hours dealing with their after-effects, according to “The Link Between Pirated Software and Cybersecurity Breaches,” which surveyed 951 consumers as well as 450 CIOs and IT managers. The study was released by Microsoft as part of its global Play It Safe campaign.”

The Target breach has become the poster child for the immense cost that a data breach can have on a company including the huge direct remediation/compensation costs, loss of revenue due to shaken consumer confidence a lower stock price the resignation of the CIO and CEO. It will cost Target, Neiman Marcus and Michaels, and/or their banking partners, $5 to replace each standard credit card account with a new account number and plastic. That's $550 million if Target has to replace 110 million cards. That expense does not include any penalties, credit watch expenses, law suit settlements and beefed up cybersecurity systems costs.

As a result of the breadth and scale of this issue in the retail sector, the Department of Homeland Security's US-CERT sent out an alert on July 31st about the widespread prevalence of one single malware variant used in POS machines – Backoff. More than 1,000 organizations have been compromised by Backoff malware that may not even be aware of it according to the U.S. Secret Service. Backoff was first observed in October 2013 and has grown to encompass several variants. Also, Backoff is only one of many, many similar malware tools loosely classified under the umbrella of attacks called Memory Scrapers. For every Backoff malware there are likely to be dozens to hundreds of similar malwares all with the same target – POS and banking systems and their credit/debit card data.

As the graph below illustrates, for every larger attack that receives general press attention, there are dozens of other lesser known attacks hard at work attacking and stealing. This snapshot from January does not even show the most recent serious threat Backoff although, most experts say that it was already breaching retail PoS systems and stealing data from as far back as October 2013. How many others are running undiscovered today?

"Seven [point of sale] system providers/vendors have confirmed that they have had multiple clients affected," noted the advisory released by the Secret Service recently. "Reporting continues on additional compromised locations, involving private sector entities of all sizes."

The Backoff malware is primarily concerned with stealing payment card information from point of sale, or POS, terminals. It does so using a number of sophisticated methods --including keylogging and memory scraping techniques--to gain access to, and to facilitate in the exfiltration of stolen data.

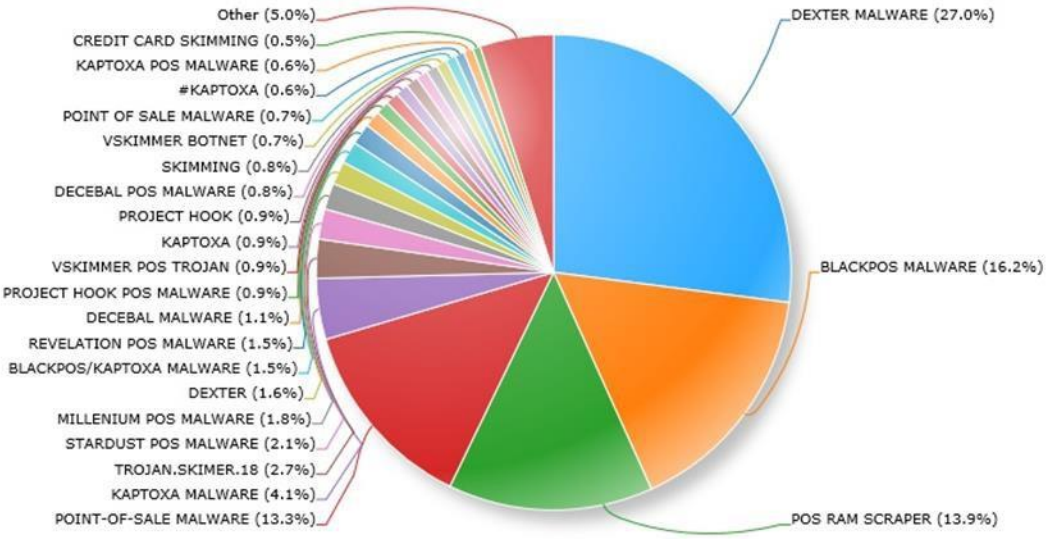
The Backoff malware (and its many variations) does not make use of any new techniques or employ creative new infection methods but researchers at US-CERT who have analyzed the malware, believe that it is a serious threat. Backoff malware is being used by cyber-criminals as the second stage of attack campaigns that begin with locating systems with remote desktop (or similar) tools and then brute-forcing the credentials to access them, often, if possible, for an administrator account. At the onset, hackers scan corporate networks for remote access software, such as Microsoft's Remote Desktop, Apple Remote Desktop or LogMEIn, PCAnywhere and Join.Me, just to name a few. These programs operate by constantly listening for communications from remote desktop users seeking access.

Once they have achieved that, the attackers seek PoS devices and install the Backoff malware as broadly as possible. Once installed on a PoS device, the malware injects a small piece of malicious code into the explorer.exe process. It is designed to have the ability to "scrape" memory from running processes to gather many data points including payment card track data, keystrokes and communicate with a remote command-and-control infrastructure.

Point-of-Sale Attack Practices

Consumer Goods – Special Report

January 2014



The variations of Backoff reviewed by Homeland Security were enabled with a variation of four functions: (i) scraping memory for track data, (ii) logging keystrokes, (iii) Command & Control (C2) communication (this uploads discovered data and updates the malware) and (iv) injecting malicious stub into explorer.exe (this maintains the malware in the event that it crashes or is forcefully stopped).

"The malicious stub that is injected into explorer.exe is responsible for persistence in the event the malicious executable crashes or is forcefully stopped. The malware is responsible for scraping memory from running processes on the victim machine and searching for track data. Keylogging functionality is also present in most recent variants of 'Backoff'. Additionally, the malware has a C2 component that is responsible for uploading discovered data, updating the malware, downloading/executing further malware, and uninstalling the malware," the advisory from US-CERT says.

There are multiple known variants of the Backoff malware, each with slightly different functionality. The C&C communications are done via HTTP POST requests to domains that are hardcoded into the malware. Data sent to the C&C servers is encrypted.

3. Impact on Retail and Banking

If you are part of a retail or financial services organization you are undoubtedly quite concerned about the threat of Backoff (and all of the other similar memory scrapers that are out there) and wonder how to stop it. Clearly, while no organization is perfect in their IT and security decisions, implementations

and ongoing monitoring, it would seem from the outside that the retail stores that are getting the big headlines for being breached and losing the credit card data for millions of people have also invested heavily in IT security. It is clear that all of these retail businesses have spent a great deal on IT security – products and staffing. Another fact that should send a chill through all organizations and consumers is that, in each of these publicized breach cases, these breached organizations were PCI DSS certified!

Companies that were PCI DSS certified that spent a great deal of money on IT security were breached – how can you avoid the same fate? Have you already been breached but not even know it? DHS thinks that 1,000+ retail businesses have been infected with Backoff and only 100 or fewer have discovered that they were breached. How do you know that you have not already been breached or that malware will penetrate your systems tomorrow?

There are countless articles and vendor claims about how to be safe from the memory scraper threat. They usually sound something like this (Analysis comments have been added in blue.):

> ***How to prevent a Backoff attack***
>
> *To mitigate and prevent Backoff malware attacks, the DHS' recommendations include the following:*
>
> - ***Control remote desktop access.*** *Limit the number of users and administrative privileges, require complex passwords and two-factor authentication, and automatically lock out users after inactivity and failed login attempts.* Clearly, it is important to try to limit malware from getting onto computers and networks.
> - ***Configure network security.*** *Reevaluate IP restrictions and allowances, isolate payment networks from other networks, use data leakage and compromised account detection tools, and review unauthorized traffic rules.* Good advice, limit the penetration and movement of malware.
> - ***Manage cash register and POS security.*** *Use hardware-based point-to-point encryption, use only compliant applications and systems, stay up-to-date with the latest security patches, log all events and require two-factor authentication.* Good advice, difficult to implement and enforce.
> - ***Implement an incident response system.*** *Use a Security Information and Event Management (SIEM) system to aggregate and analyze events and have an established incident response team. All logged events should also be stored in a secure, dedicated*

server that cannot be accessed or altered by unauthorized users. Post attack awareness has value in limiting the amount of data stolen but tends to be reactive versus preventative.

Or, this:

> ***Below are suggested methods to better protect your organization and your customers' information:***
>
> • ***Multi-factor Authentication*** *- Requires employees to use two authentication factors (e.g.: something you know, like a password; something you have, like a credit card; something you are, like a fingerprint). This will add an extra layer of security to your PoS and to help ensure only authorized users have access to credit card data.* It is always good to limit access to credit card data – however, malware scrapers are stealing the data from memory.
>
> • ***Monitoring Networks*** *- Most organizations have already invested time and resources into software such as Intrusion Detection, but fail to utilize them to the fullest. It is likely that the network is trying to notify you about suspicious activity, you just need to listen and react.* Yes, but the challenge is that the leading Intrusion Detection products on the market continue to miss attacks like Backoff.
>
> • ***Defensive Readiness*** *- Attacks are inevitable – prepare for them. It begins with education and awareness at every level of the organization. Once you have an understanding of how attackers perform breaches, you will be able to prepare for them. For example, Social Engineering (e.g., phishing campaigns) is a popular method of compromise. To prepare, look at how your company might be profiled and educate your employees on what to look out for and proper response procedures.* Employee education is vital but still has limitations. Careless, criminal or poorly trained humans will always be a significant risk factor.
>
> • ***Point-to-Point Encryption*** *- P2PE encrypts sensitive data (e.g., credit card number and expiration date) at the point of entry and protects throughout the transaction, significantly reducing risk.* Complete P2PE can be effective in stopping malware scrapers but is expensive to implement and manage and there does not seem to be a rush to make this investment by most retail organizations.

From most security vendors you read advice on stopping malware like:

> *Our product XXXXXX protects PoS systems and includes System Lockdown, Application Control, Device Control and Firewall capabilities, providing multiple layers of protection to maximize security. These tools allow you to minimize the attack surface by limiting the specific applications running on the system, as well as regulate which devices and applications are allowed to access the network. Limiting applications and network accessibility on the machines can render malware useless.* This approach sounds good at a high level but the evidence is clear – all of the well-known high profile breached retailers referenced above were using this kind of a multi-layered security strategy – and it failed them.

Unfortunately, these are good solid recommendations for reducing your risk "surface" lessening the risk for an attack to get into your network – but they will not stop Backoff. Did they work for Target? For Home Depot? For Goodwill? For Dairy Queen? A well-funded, determined cyber-criminal will find a way to get their malware into your network/POS systems.

All organizations should do everything that they can to reduce the risk of malware actually getting onto one of their systems – there are multiple methods including those listed above. But, the enemy is well funded, creative, crafty and persistent and you are defending PCs and systems with inherent weakness being used by a very weak link – human beings.

Will my current security layers provide protection? Two security layers are often viewed as protections against memory scraping malware. Will my anti-virus and/or whitelisting software detect and stop malware?

4. Why Anti-Virus Does Not Stop Backoff

The anti-virus engine is based on the concept of identifying hash values belonging to known malicious files. Hash values are generated by taking a file and processing it with a mathematical algorithm that yields an alpha-numeric string. This string serves as a "fingerprint" for that file and is unique to that specific file. As AV has evolved, the latest generations of AV products combination of heuristic, behavioral and generic detection rules. The implementation of using detection based on heuristics allows anti-virus engines to protect against variations of known malware, even if it is not an exact match. This allows for the possibility of preventing infection from previously unknown malware.

Given these capabilities, why is it that current anti-virus products regularly fail to detect POS malware?

One reason is that POS malware is very specific and targeted. The R&D developers of malware create and modify their malware in the development process until they create a version that will not be detected by the anti-virus that is used by the company that they are targeting.

Additionally, because these cyber-criminals are focused on POS systems, the malware that they create represents only a miniscule fraction of the totality of malware that exists in the world. Also, the POS malware that they create is distributed in a very targeted way that restricts the distribution. Unlike other types of malware that are spread broadly through multiple vectors and sources there is very limited distribution.

This limited distribution of a POS malware family results in two barriers to AV being effective in stopping them: First, because signature lists are based on the detection of the overall volume of attacks, these POS focused attacks rarely have enough

activity to be noticed by the AV vendors. Second, it means that anti-virus vendors do not regularly encounter this malware and, as a result, can't improve their heuristic detections because they have limited views into the developer's methods and techniques.

As a result, it is clear why POS malware developers are able to ahead in the anti-virus arms race. Unfortunately, this leads to a death spiral - anti-virus is not very successful at detecting POS malware so retail POS organizations tend to avoid the expense. "PoS malware has been around for at least a decade, and retailers have been continually targeted since that time," said Nicholas J. Percoco, vice president of strategic services at cybersecurity firm Rapid7. "The issue is that traditional antivirus does not typically detect variants of this malware since it only targets a fraction of their customer base." Even if malware is reported as being the "same" as in a previous attack, Percoco said, there are typically enough technical differences in each deployment that antiviruses miss it the next time.

In summary, AV will not protect you – new variations of the malware occur every day so whatever signature database you have, it is already out of date. Also, the cyber-criminals have a copy of the signature database from your AV provider – sophisticated attackers do not use attacks that are in your database. The value of AV is that, like many other recommended protections, it can protect against *known attacks* that are in the signature database.

5. Can whitelisting provide protection?

Whitelisting seems like an attractive option: the vendors dependent on this approach say things like "just stop the attackers from running anything new on your endpoints." Create a master list of blessed applications that are allowed to run on your PCs and PoS devices and do not let anything run that is not on that list. It can be an arduous process with significant administrative effort to create and maintain the whitelists. This seems interesting until you discover that malware attacks can be introduced, hidden and run without creating an application or "anything new" that will be visible to the whitelist security application.

Whitelisting reduces the surface of the risk area for a PC – certainly a laudable step. However, since sophisticated attacks, and more and more frequently, less sophisticated attacks, are "hiding" their attacks within legitimate applications that will almost always be whitelisted, this protection offers little real protection.

Whitelisting is based on the concept that reducing the number of applications that an end user can load and use will reduce the risk exposure to attacks. The whitelists are normally assembled from one of two ways – or a combination of both. There is normally an option available for the customer to define their own list of applications that are allowed. Also, some whitelist vendors analyze applications and attempt to identify "bad" applications and "good" applications. The results are then provided to

the customer in the form of a list of "good" applications that have been deemed to be safe to run on the customer's PCs. Using whitelisting can reduce the number of applications that are permitted to run on a PC and, as a result, obvious known applications with a history in the past of representing threats can be stopped and the overall number of applications can be limited.

NOTE - Important technical distinction: Whitelisting/application control is *not* designed to stop attacks. It is designed to try to limit the possibility of the *delivery* of attacks. This security method is designed to lessen the risk of the delivery of the attack by providing some control over the applications that can run on a PC. Thus, if an organization wants to have real protection that is reliant on whitelisting/application control, they are using the presumption that attacks will not be delivered by whitelisted applications. Unfortunately, this is not the case. Cyber criminals are creative and aware of whitelisting. Thus, they construct their attacks to hide within applications that they know will be "whitelisted". Alternatively, the cyber-criminals use a variety of masking techniques to make their application "look" like a standard application that should be on the whitelist. As a result, the administrator, in the midst of evaluating and managing many applications may inadvertently whitelist the malicious application.

As a result, while whitelisting is recommended as part of a broader strategy to reduce the risk surface at the PoS at the endpoint, it is not an effective reliable method to stop sophisticated cyber-criminals attempting to use memory scraping malware.

The follow on issue is: If the whitelisting aspect of the whitelisting/application control product does not protect against many attack types, are there other security capabilities that can recognize and stop attacks that have gotten past the whitelists? The whitelisting/application control marketing materials use the right industry buzzwords and, at a high level, seem like they may be adequate for protection. However, since, for example, they will not stop Java and .net attacks, there are still significant holes that an organization will need to fill with some other technology.

6. "We can't stop the attacks – buy our better analytics."

The other somewhat recent trend in the security industry is also worth discussing. Many of the best known vendors in the IT security industry have been forced to admit that they do not/cannot stop sophisticated cyber-criminals launching advanced attacks. As detailed above, their methods for detecting and stopping attacks are not working. Unfortunately, their response is not to develop and deliver better security protections – it is to push analytics. They like to point out statistics like the recent Trustwave global survey that indicated that the average number of days between the date of the initial intrusion and breach containment was 114 days in 2013. As mentioned above, it seems that the Home Depot breach is a good example of this discovery lag – they were losing credit card data for 5 months before the breach was discovered.

So the new advice from these vendors is "We can't stop that attacks but buy our new analytics and detection products and we will help you to know sooner that you have been breached." If you apply that recommendation to another industry that has big security concerns, banking, it would look

something like this: Can you imagine if a bank manager told the bank's board of directors that they had a new strategy for dealing with the loss of cash from their bank: "We think that we are being robbed but we aren't sure how much money we are losing nor who is stealing it. Worse, we don't know how to stop the robberies. But, we are going to buy a new system that won't stop the thefts but we are hoping that we may know that we have been robbed a little sooner than it is taking us to discover it now. We will still be losing money in robberies but we will know about it within a couple of weeks of the robbery instead of a couple of months." Unacceptable!

Like AV and whitelisting, analytics, logging, SIEMs, data analysis, etc., etc. provide some value and are normally part of any serious IT security strategy. But, too often, the campaign to sell the new wave of analytics products are based on the "straw man" argument that you have a firewall, blacklists/whitelists, AV and similar protections but since they can't protect you so it is time to give up and buy our new solution. This argument ignores that there are new innovative effective solutions being developed and provided that actually can provide real protection against malware like Backoff. Better analytics may have allowed Hope Depot to know about the malware attack sooner than it was discovered but how is "only" losing 5,000,000 or 10,000,000 records acceptable? It is too soon to give up on identifying and stopping the attack at the time of the attack!

7. How can a retail business avoid the fate of Target, Home Depot, Goodwill, etc.? Is there a way to stop Backoff and other Memory Scraping Malware?

The people who are responsible for the IT/POS security at their company wake up every morning with the same haunting thoughts: Have I already been infected with malware at my PoS systems and do not know it and, even if my systems are not infected right now, will my systems be targeted and attacked today and not be able to stop it – or even notice? We have established above that these are legitimate concerns – the threats are real and the current implemented protections inadequate. What can be done to provide real protection against memory scraping malware?

Matrix Global Partners, Inc. (Matrix) specializes in providing and supporting security solutions to clients across industries including major governments, financial services, retail, Fortune 1000 and healthcare. As part of our client services, we work with our clients to identify critical security issues and then seek the best possible protections for them. In the past year or so our retail clients have been increasingly expressing concern about memory scraping malware and their exposure. Matrix evaluated the possible options available across dozens of security vendors and confirmed that there is an option that can address both of the worst fears of retailers: First, confirm that they have not already been

breached by malware, second confirm that they are infected and remove it and, third stop and block all future memory scraping malware attacks.

8. Stormshield Endpoint Security

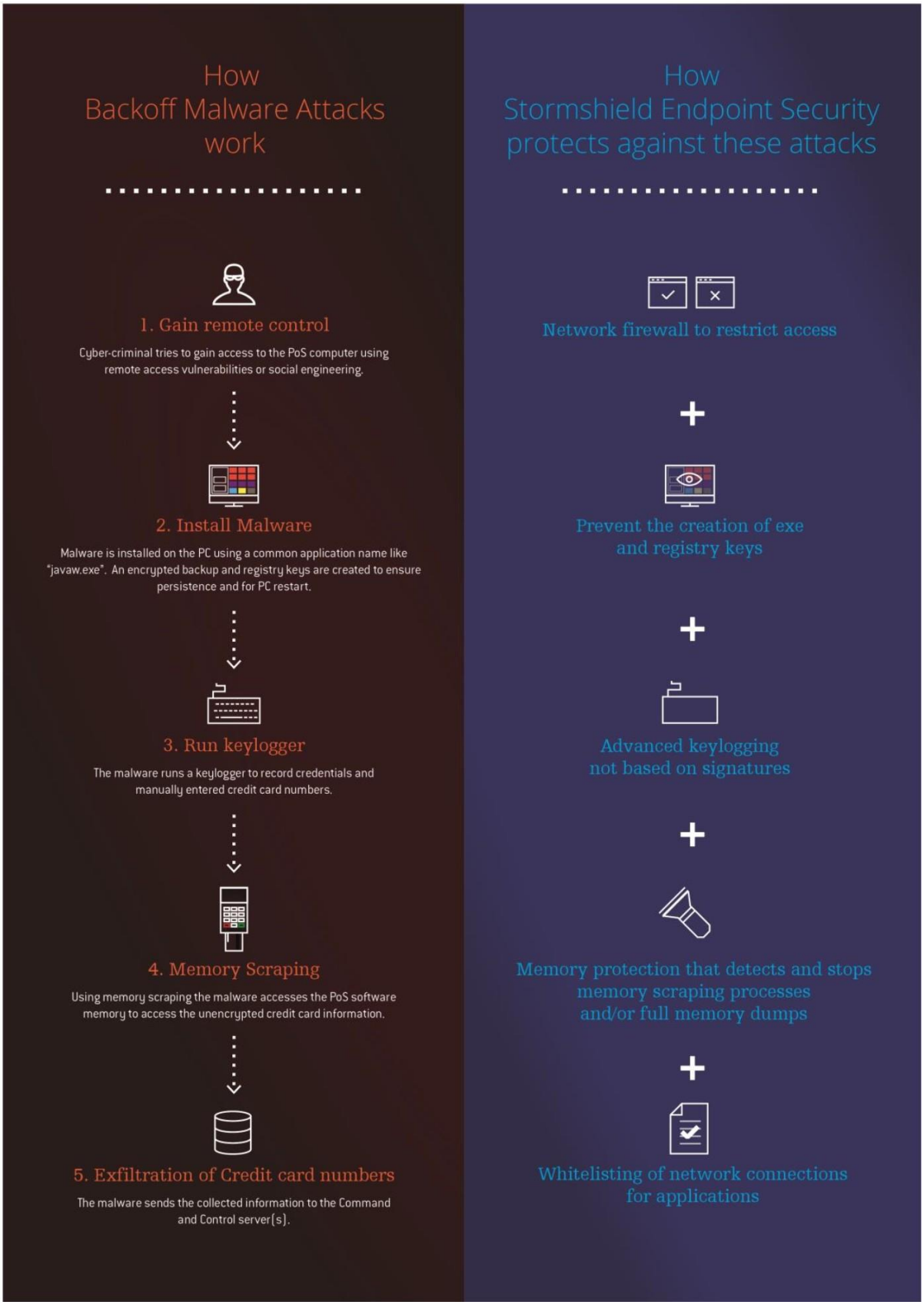
The security product that Matrix is recommending to stop malware attacks like Backoff is Stormshield Endpoint Security (SES) from Stormshield (part of the Airbus Defence and Space Cybersecurity Group). Matrix has determined that SES not only provides the option of choosing from a suite of risk mitigating security modules (like whitelisting/application control described above) but does something that does not seem to be available from other security vendors – a unique memory protection that can identify memory scraping and keylogging malwares like Backoff using techniques that don't require signatures, whitelisting or traditional PoS security protections.

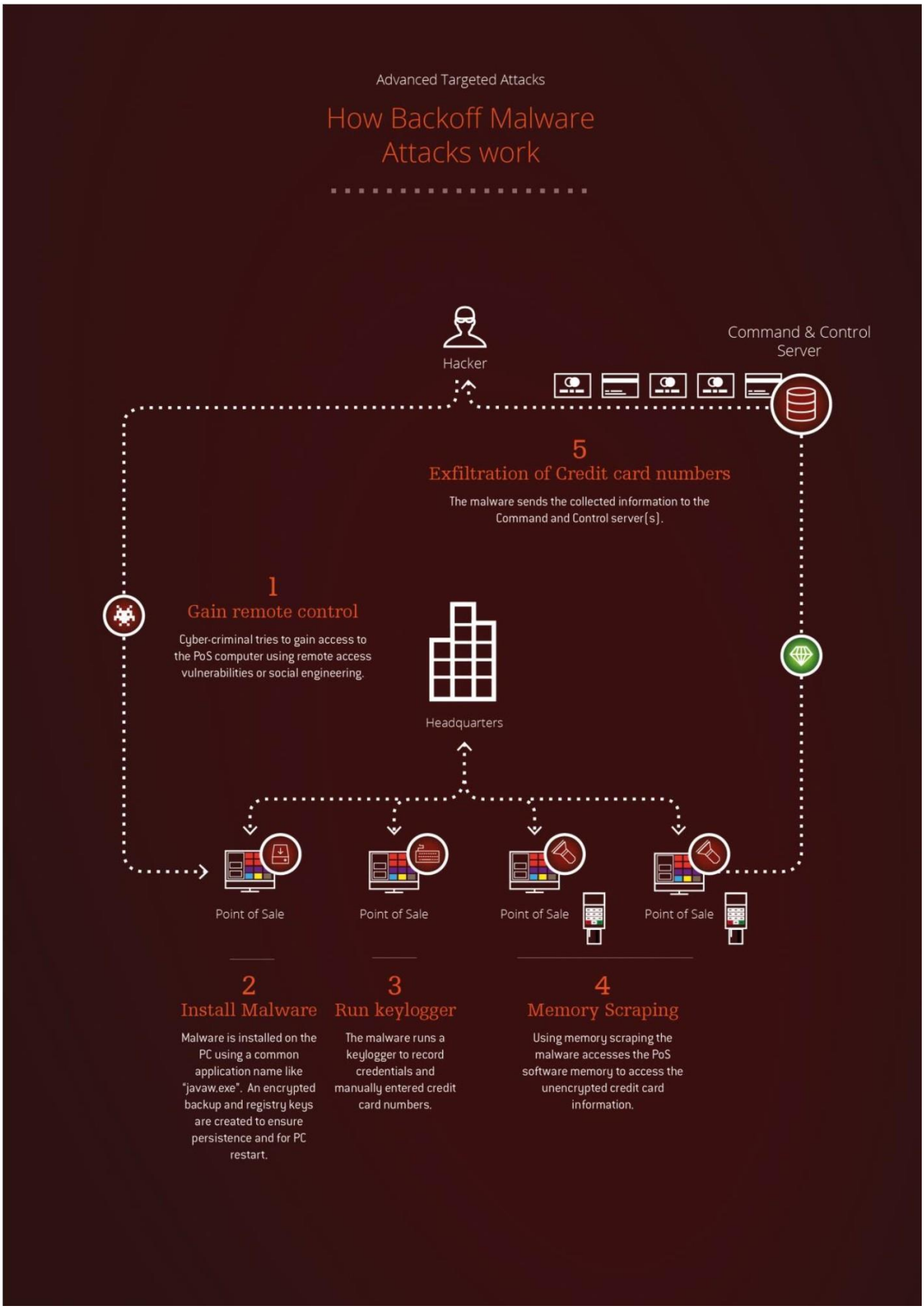
Because of the approach for memory monitoring and protection that SES uses, the protection is proactive – the Matrix retail clients that are using SES are protected against malware like Backoff, new Backoff variations and the dozens of other similar memory scraping and keylogging malware attacks that seem to crop up every week no matter how it gets into the PoS system and even if it has never been seen anywhere on earth before. The issue that is apparent with each of the reports of another major retail store breach of the attack going on for months undetected is not a risk for SES users.

The other significant advantage over other protection options like whitelisting is the dramatically lower administrative overhead of SES. Deploy the SES agents using the automated tools provided and you will know if you have been infected with a malware issue like Backoff (and it will be blocked and you notified) and you are also assured that no new attacks will be able to do their memory scraping. While SES includes a whitelisting capability, many customers have found that, like all whitelisting products, the initial set up and ongoing maintenance of these lists is too burdensome to make the somewhat limited protection worthwhile.

9. How does Backoff (and other similar malware) work and how does SES provide protection?

In order to better understand why Backoff (and similar) malware is such a threat and how SES can provide real protection it is important to understand how the attacks work and where SES intervenes to provide protection. The illustrations and analysis below describe the 5 stages of a Backoff malware attack and how SES can provide protection at each stage:


How
Backoff Malware Attacks
work
1. Gain remote control
Cyber-criminal tries to gain access to the PoS computer using remote access vulnerabilities or social engineering.
2. Install Malware
Malware is installed on the PC using a common application name like "javaw.exe". An encrypted backup and registry keys are created to ensure persistence and for PC restart.
3. Run keylogger
The malware runs a keylogger to record credentials and manually entered credit card numbers.
4. Memory Scraping
Using memory scraping the malware accesses the PoS software memory to access the unencrypted credit card information.
5. Exfiltration of Credit card numbers
The malware sends the collected information to the Command and Control server(s).
How
Stormshield Endpoint Security
protects against these attacks
Network firewall to restrict access
+
Prevent the creation of exe
and registry keys
+
Advanced keylogging
not based on signatures
+
Memory protection that detects and stops
memory scraping processes
and/or full memory dumps
+
Whitelisting of network connections
for applications


Advanced Targeted Attacks
How Backoff Malware Attacks work
Hacker
Command & Control Server
5
Exfiltration of Credit card numbers
The malware sends the collected information to the Command and Control server(s).
1
Gain remote control
Cyber-criminal tries to gain access to the PoS computer using remote access vulnerabilities or social engineering.
Headquarters
Point of Sale
Point of Sale
Point of Sale
Point of Sale
2
Install Malware
Malware is installed on the PC using a common application name like "javaw.exe". An encrypted backup and registry keys are created to ensure persistence and for PC restart.
3
Run keylogger
The malware runs a keylogger to record credentials and manually entered credit card numbers.
4
Memory Scraping
Using memory scraping the malware accesses the PoS software memory to access the unencrypted credit card information.

10. Backoff PoS Malware Stages (also used by other memory scraping malware):

1. The first step is for the attacker to find a way to breach the defenses of the intended target to introduce the malware. The cyber-criminal must get the malware package onto the targeted systems. The cyber-criminal can use multiple diverse methods to gain access to a Point of Sale (POS) System. For example:

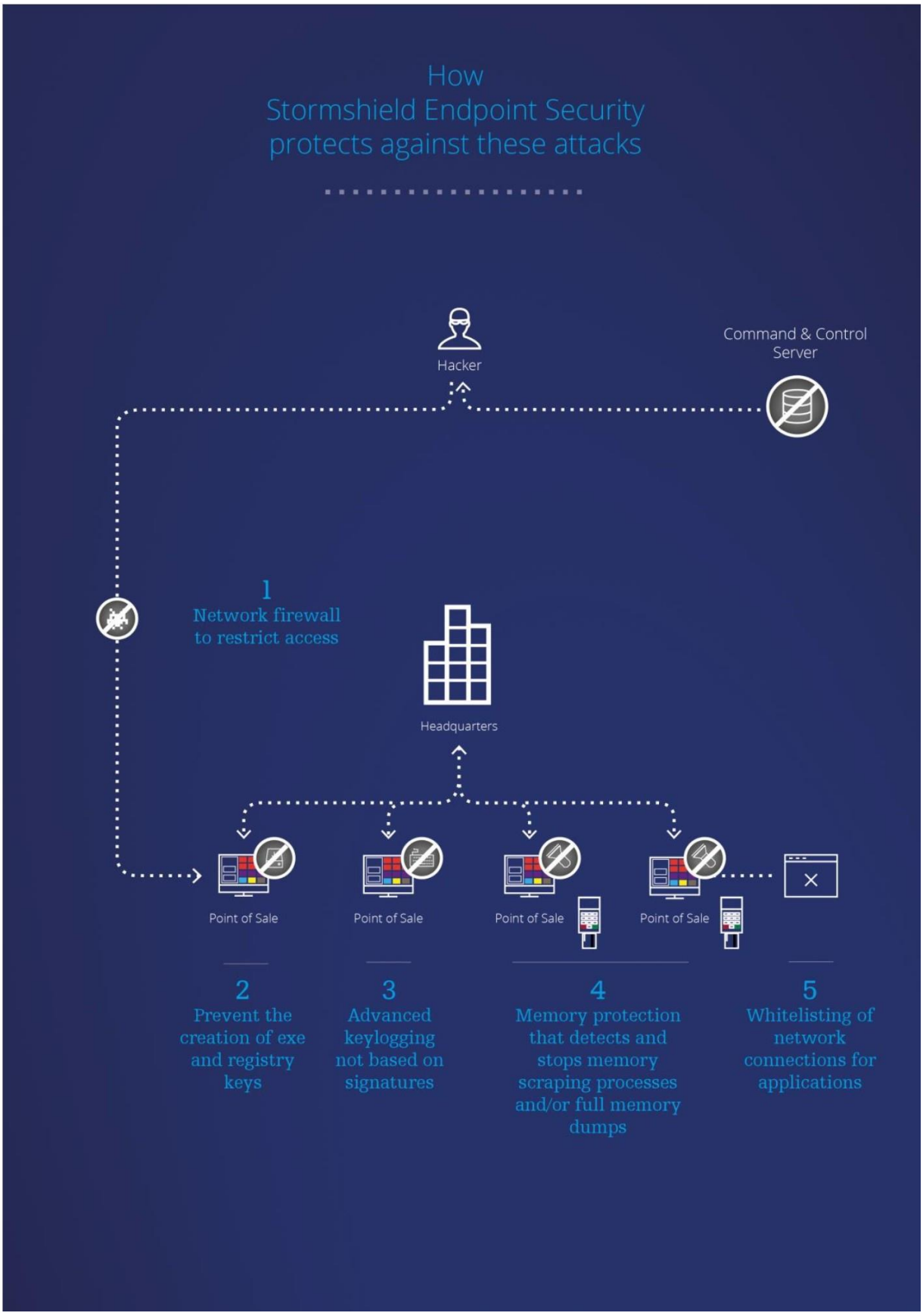
    a. Exploiting remote access software (for example RDP, Logmein or VNC) with weak credentials (Login/password). Most PoS systems have remote access capabilities in order for the IT support team to maintain the systems. PoS systems often have a default login/password made by the PoS vendor that sometimes is not changed or disabled. Or, alternatively, for ease of access and less administrative burden for the IT support team, identical or simple passwords are often assigned to the individual PoS systems – once one is broken all of the rest of the systems are vulnerable.
    b. Gaining physical access to the PoS system by using social engineering or unauthorized access methods. In this use case, the PoS system can be accessed remotely via the internet. The PoS systems are sometimes using a private network that can't be used by the cyber-criminal. The malware is installed by bypassing the operating system (booting from a USB/CD-ROM or directly accessing the hard drive). Using the same access methods, the cyber-criminal will come back to recover the recorded credit cards.
    c. Software vulnerabilities: If the PoS system is running an unsupported OS (for example, Windows XP) or is missing security patches, the cyber-criminal can exploit the Zero Day vulnerability or similar holes in the security protections.

2. Once the malware has breached the security perimeter it needs to install, run and hide. The malware that is often installed on the PoS System is a copy of an executable using a common name like "Javaw.exe" – the name of a Java runtime. This approach was used for some variations of the Backoff malware. As a result it can look like an authorized application. The malware also needs to make sure that it is running even after the restart of the PoS system or in case the malware file is deleted. So it activates its persistence techniques such as:
    a. Windows OS has a registry key to auto-start an application: HKLM\Software\Microsoft\Windows\CurrentVersion\Run). By adding an entry, the malware is launched automatically each time the system restarts.
    b. An encrypted backup is made just in case the malware is removed. So the malware in memory monitors that its file is still present on the disk. If it detects that a user or an application has removed the file, it automatically restores it from the encrypted backup.

3. As part of the attack scenario the malware will activate its keylogging feature in order to record a variety of credentials such as when a system administrator accesses the system. This can be

useful to gain access to other PoS systems or to record credit card information that is entered manually during a transaction. When this attack is done by a reasonably competent cyber-criminal, this dangerous keylogging behavior will not be detected by the antivirus because it will not have a signature for the keylogger application. This keylogging component also can be used to act as a "trigger' for other actions. For example, to indicate when the memory scraping should start because the credit/card button has been pressed on the PoS System.

4. These first three steps have provided the foundation for the true goal of the Backoff malware attack – stealthily hide in the memory for an extended period of time watching for credit card data, copying it and storing it for future exfiltration. The credit card information is normally encrypted when it moves between the PoS system and the processing center. Any credit card information should be stored encrypted (a PCI DSS requirement). When a customer swipes a credit card, the PoS Software reads the credit card information (15-16 digits, expiration date and Card Verification Number) from the magnetic stripe. When the data is read from the card reader, a temporary buffer is used in memory before encrypting the information. During this very short time window, the information is available for theft.
   The most important component of the attack is the memory scraper that scans the computer memory to recover the credit card information. The malware injects its memory scraper inside the process of the PoS Software. Being inside the PoS Software, it is very easy to scan the entire memory used by the application to search for Credit the card number's 15-16 digits + expiration date 4 digit + CVN 3-4 digits. Individual credit card information is quite small (24 bytes) so a 1MB memory dump can contain roughly 42,000 credit card numbers. So most malware will try to store the stolen data locally and send it in small chunks of data or send it in real time after each credit card is detected and the data "scraped" so that only a very small amount of data is sent at one time. Another possible, but less likely, memory scraping scenario is a full memory dump that can be triggered by the keylogger and is designed to search for the credit card information that has a known format. But this is a relatively slow and inefficient data collection method because a full memory dump is so large. In addition to slow and inefficient, the size of the file holding the stolen data may trigger a security alarm.
5. The last step that this type of malware must take is to exfiltrate the data that it has gathered to a computer outside of the PoS system (often a Command and Control server (C&C)) using an http connection Server. For example, some Backoff variations encrypt the credit card information using the RC4 algorithm and encode the data in Base64 so it can be sent via http. The C&C server receives the information and can also update the malware with additional protections to continue to prevent detection. (The most serious credit card data loss instances that have been reported have involved attacks that were often running for many months before they were discovered.) For a PoS system that has no internet connection, the credit information is stored locally on the PoS system for a later physical recovery by the cyber-criminal.


How
Stormshield Endpoint Security
protects against these attacks
Hacker
Command & Control
Server
1
Network firewall
to restrict access
Headquarters
Point of Sale
Point of Sale
Point of Sale
Point of Sale
2
Prevent the
creation of exe
and registry
keys
3
Advanced
keylogging
not based on
signatures
4
Memory protection
that detects and
stops memory
scraping processes
and/or full memory
dumps
5
Whitelisting of
network
connections for
applications

11. How SES provides general malware protections and identifies and stops Backoff

This analysis takes each of the defined attack stages that are explained and analyzed above and describes how SES can protect PoS systems from Backoff:

1. The first step is for the attacker to find a way to breach the defenses of the intended target to introduce the malware. How can SES help protect against the attack even getting into a PoS system?

   a) Exploiting remote access software: SES includes a network firewall that can be used to restrict which IP can connect to the PoS PC from the remote access software application. So only the IP Addresses from PoS administrators can reach the PoS computers, preventing any hacker from connecting to the PoS computers. The SES stateful NDIS firewall is multiprotocol (over Ethernet, over IP, over TCP/UDP/ICMP) and provides protocol checks & port scan detection. It can be used to prevent any unauthorized network connections. It is administered through the SES management console.

   b) Gaining physical access to the PoS system by using social engineering or unauthorized access methods: SES prevent any tampering of the Hard-drive by providing full disk encryption. If the hacker tries to load another operating system using a USB device or CD-ROM, SES will block the capability to read or modify the hard drive. When the computer is already started and running, the SES Device Control module can disable the access to USB/CD-ROMs on the computer even if the user has administrator rights.

   c) Finally, the cycle of vulnerabilities occurring in applications becoming generally known that are then patched by the product manufacturers within a few days, weeks or months (Zero Day vulnerabilities) provide huge openings for the introduction of attacks like Backoff. Often, these vulnerabilities are noticed and exploited by cyber-criminals before they are noticed by the manufacturer.

SES provides unprecedented protection against these vulnerabilities. SES Zero Day protection and Monitoring Services provide protection against vulnerabilities without the requirement for the patching of the OS or other applications. SES has built-in mechanisms for detecting and blocking suspicious activity that would otherwise go undetected by signature-only and non-behavioral

technologies. Here is a description of how these memory protections work.

- Backtrace: this module is able to monitor critical syscalls of the operating system. The backtrace technology uses a disassembly engine to understand the machine code that is being executed.
- NX byte detection: when the processor has the NX byte technology StormShield uses it to detect malicious code executed on the heap or in the stack. This module is an enhancement of the Windows DEP technology but doesn't replace it. The NX/XD byte is used to monitor if a specific page of memory is executable (i.e. contains machine code) or not (for example when it contains data like a jpeg image).

- A return-to-libc (Ret-2-LibC) attack usually starts with a buffer overflow in which the return address on the call stack is replaced by the address of a function that is already loaded in the binary or via a shared library. The attacker simply calls preexisting functions in order to bypass NX byte protections. In software like Windows operating systems, code is inside an executable or in libraries. Windows includes core libraries used for common actions like opening a file, launching an executable etc. Inside these libraries are functions. A function is a piece of code that is called by name. It can be data handed over to operate on (i.e. the parameters) and can optionally return data (the return value). For example, in the library kernel32.dll, there is a function named "OpenFile" with 3 parameters. All data that is passed to a function is explicitly passed. SES Ret-2-LibC protection monitors approximately 100 of these critical functions. Each time a call is made to these functions, SES does an analysis of the context of the call and blocks the process if the function's call originates from a buffer overflow.

- HeapSpraying Protection: HeapSpraying attacks are the newer evasive techniques used to bypass HIPS protections and web browser protections on a PC/server. The cyber-criminal crafts a memory space on the target computer using JavaScript, Python, etc. The crafted memory space matches the needs of the attack to bypass security protections. Then the real attack is launched using a Zero-Day vulnerability that is redirected to this memory space. SES is the only product tracking the crafting and redirection of memory space. For a PoS PC that is still running Windows XP, the SES ExtendedXP version provides protection for POS machines running Windows XP. A security team is constantly monitoring and providing customer reports about all Windows XP, IE and 3rd party applications that are running on Windows XP like older versions of Office, Java or Flash.

2. To prevent the malware from being installed on the PoS computer, SES has a feature to prevent the creation of executables on the machine. Except for trusted deployment tools, no executables can be added to the computer. Even if the attacker is able to create an

executable he has to find a way to install the malware. SES provides a Whitelisting module that restricts the applications that can be executed.

SES provides three ways to identify an authorized application. A checksum (MD5 or SHA-1) can be quickly imported and managed. Permanently updating a list of checksums can be extremely burdensome for the IT security team because a PoS PC can run hundreds of executables. So SES provides the capability to use digital signatures and a tool to digitally sign applications allowing a workflow with a validation process to be put into place. For example, one protection could be to require that any new application has to go through a validation process before being deployed on the PoS computer. Similar to Apple and their Apple store which verifies applications before allowing a user to install them.

Finally, if the malware try to hide itself using its encrypted backup, SES can restrict the access to the folders and registry keys that can be used by malware for persistence. SES application control can prevent any application on the PoS computer from using any known techniques that permit a software application to automatically restart after a reboot of the computer running on a Windows OS. This provide a safety net in case a malware is authorized by the IT security team by mistake. This is a feature that is not available with a simple whitelisting software like that offered by some leading whitelist security vendors.

3. SES can protect PoS PCs against keylogging applications without the use of signatures. SES can block any advanced GUI hooking mechanism which aims at capturing all events related to the graphical user interface in connection with keyboard activity. SES also monitors the usage of any API used for keylogging. This ensures that no custom or new keylogger will be able to exploit a computer even if a malware is authorized to run on the computer.

4. Stealthily hide in the memory for an extended period of time watching for credit card data, copying it and storing it for future exfiltration: SES includes advanced process access. This means that SES protects the process running from being opened or hijacked by a malware to access the PoS credit card processing application. By design, Windows is not restricting the memory access between processes from the same user. So a malware running with the same user as the PoS software can read the memory of the PoS application. This is available because it is necessary within the PC system for any software development and debugging purposes. For example, when an application crashes error report tools can then gather information for the editor of the application. SES is shielding each process from peeking into any other process. As a result, no memory scraping malware can scan the memory of the PoS Software.

For a full memory dump using a driver (which is not practical for malware because each memory dump is roughly the size of the total memory used on the machine - 4 to 8GB for each memory dump) the computer would run out of space quickly and processing this huge amount of data would use all the CPU resources of the machine – both things would normally lead to discovery of the attack. But, just in case an attacker takes this approach, SES includes a rootkit detection module that can detect dangerous behaviors from drivers and also alerts if any new driver is loaded in memory.

5. The last step that this type of malware must take is to exfiltrate the data that it has gathered to a computer outside of the PoS system. The SES application and network firewall can be used to restrict which applications have access to the network. With SES Application Control, a list of application that can access the network can be defined. So only the applications required to access the internet are allowed. The SES network firewall can be used to restrict which IP the PoS can connect to so that the unknown applications or malwares cannot have access to the network. This can prevent the malware from reaching any C&C server.

Conclusion:

The analysis above details the five steps that malware like Backoff uses and how SES can provide protection. It is important to note that many organizations have already implemented some of the protections that are described above that SES also offers such as whitelisting, disk encryption, HIPS, keylogging protection, rootkit controls and others. Whether they are acquired through SES or another product, they are still recommended as part of a multi-layered protection strategy. It is certainly good to reduce the risk surface.

However, while all security layers that can help limit the penetration of an attack have value the sad reality is that, despite the best efforts, no system of safeguards to keep attacks out is completely secure. As is often said about national security protecting us from terrorists, we have to be "right" every time and they only have to be "right" once. In order for a retail organization to build a complete security solution against attacks like Backoff that are being used by sophisticated cyber-criminals, the most important of the safeguards listed above that SES uniquely provides is #4 – stopping the memory scraping malware even if it has gotten past all of the other defenses and is launching the attack.

Too many security strategies are based on two different failed strategies. The one that has been dominant for the past decade or so and promoted by leading security vendors is – stop the attack from getting in. It has become apparent to retail businesses, their customers, their partners, regulators and security software vendors that sophisticated attackers will find a way to breach the perimeter security defenses.

Since it is now clear that this approach cannot/will not work, the same security vendors have switched to a new strategy – "We can't stop the attacks from getting into your systems but we can provide

analytic tools to help you discover sooner that you have been breached." This latter approach concedes that you have been or will be breached and that data is being stolen. But, their sales pitch is that maybe these tools can reduce the amount of data being stolen or at minimum, have you learn about the attack and data loss prior to your customers or business partners finding out. With SES memory protection, no matter how the malware got into the PoS system, it will be identified and stopped. Because of the unique design of SES Memory Protection there is no requirement for signature files or dependency on attributes like reputation. As a result, there is no Zero Day exposure and Backoff and other similar memory scraping attacks are stopped.

This paper is titled "**The Biggest Threat to Retail Data Ever: Backoff Malware (and other memory scrapers) targeting POS systems! Security like AV and Whitelisting have proven that they can't protect you. Is there a way to be safe?"** The answer is yes. The recommended approach is to continue to use security measures to reduce the risk of attacks from penetrating but, accept that a breach may happen and count on the unique memory protections of SES Memory Protection to identify and stop the malware when it attempts to steal your data.

This White Paper is sponsored by Matrix Global Partners, Inc.

Headquartered in Indianapolis, Indiana Matrix Global Partners, Inc. (Matrix) is a national leader in information security solutions, integration and professional and managed services. Matrix offers a complete line of security technologies and, as the exclusive distributor in the Americas for the award-winning Stormshield security products, Matrix products and support are provided through direct and partner/reseller sales and support organizations**.**

Matrix Global Partners, Inc. 484 East Carmel Drive, Carmel, IN 46032 (317) 500-4571 www.MatrixGP.com

NOTES:

Examples of Malware Targeting PoS Systems

• Dexter: First discovered in December 2012, Dexter is a custom made malware tool used to infect point of sale systems. According to Seculert, Dexter steals the process list from the infected machine, while parsing memory dumps of specific PoS software related processes, looking for Track 1 / Track 2 credit card data.

• Stardust: A Dexter variant which was recently used to create one of the first known point of sale botnets, allowing card data to not only be exfiltrated but for commands to be relayed back to the PoS system. To remain hidden, the software transfers card details only when the terminal is inactive and the screensaver is on. It also uses the RC4 cipher to encrypt data before sending it to the control server.

• Millenium: A Dexter variant.

• Revelation: A Dexter variant which has the capability to exfiltrate data using FTP rather than HTTP.

• Project Hook: A similar malware to Dexter which intercepts Track 1 and 2 data.

• vSkimmer: A Trojan which can steal credit card information from machines running Windows for financial transactions and credit card payments. The malware can detect the card readers, grab all the information from the Windows machines attached to these readers, and send that data to a control server. This malware also has an offline extraction option.

• BlackPOS/Kaptoxa: BlackPOS infects computers running Windows that are part of POS systems and have card readers attached to them. These computers are either infected by insiders or found during automated Internet scans because they have unpatched vulnerabilities in the OS or use weak remote administration credentials. Once installed on a POS system, the malware identifies the running process associated with the credit card reader and steals payment card Track 1 and Track 2 data from its memory. BlackPOS is a RAM scraper, or memory-parsing software, which grabs encrypted data by capturing it when it travels through the live memory of a computer, where it appears in plain text. The captured information is uploaded to a remote server via FTP.

• Alina: POS malware that targets applications containing Track data, applies basic encryption and exfiltrates the information. This malware has a command & control structure which allows it to search for and install automatic updates when they are released.

• Decebal: Romanian POS malware released January 3, 2014--after the Target breach.

It is written in VBScript and is capable of checking to see if the computer on which it's deployed is running any sandboxing or reverse engineering software. Decebal can also validate that the stolen payment card numbers are legitimate.