SECURITY RESPONSE

A SPECIAL REPORT ON

Attacks on point-of-sales systems

Version 2.0 – November 20, 2014

> “*Cybercrime gangs organize sophisticated operations to steal vast amounts of card data before selling it in underground marketplaces.*”

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

CONTENTS

OVERVIEW

Credit and debit card data theft is one of the earliest forms of cybercrime and persists today. Cybercrime gangs organize sophisticated operations to steal vast amounts of data before selling it in underground marketplaces. Criminals can use the data stolen from a card's magnetic strip to create clones. It's a potentially lucrative business with individual cards selling for up to US$130.

There are several routes attackers can take to steal this data. One option is to gain access to a database where card data is stored. But another option is to target the point at which a retailer first acquires that card data – the point-of-sale (POS) system.

Point-of-sale malware is now one of the biggest sources of stolen payment cards for cybercriminals. Although it hit the headlines over the past year, the POS malware threat has been slowly germinating since 2005. Attackers have honed their methods, paving the way for the mega-breaches of 2013 and 2014, which compromised approximately 100 million payment cards in the US.

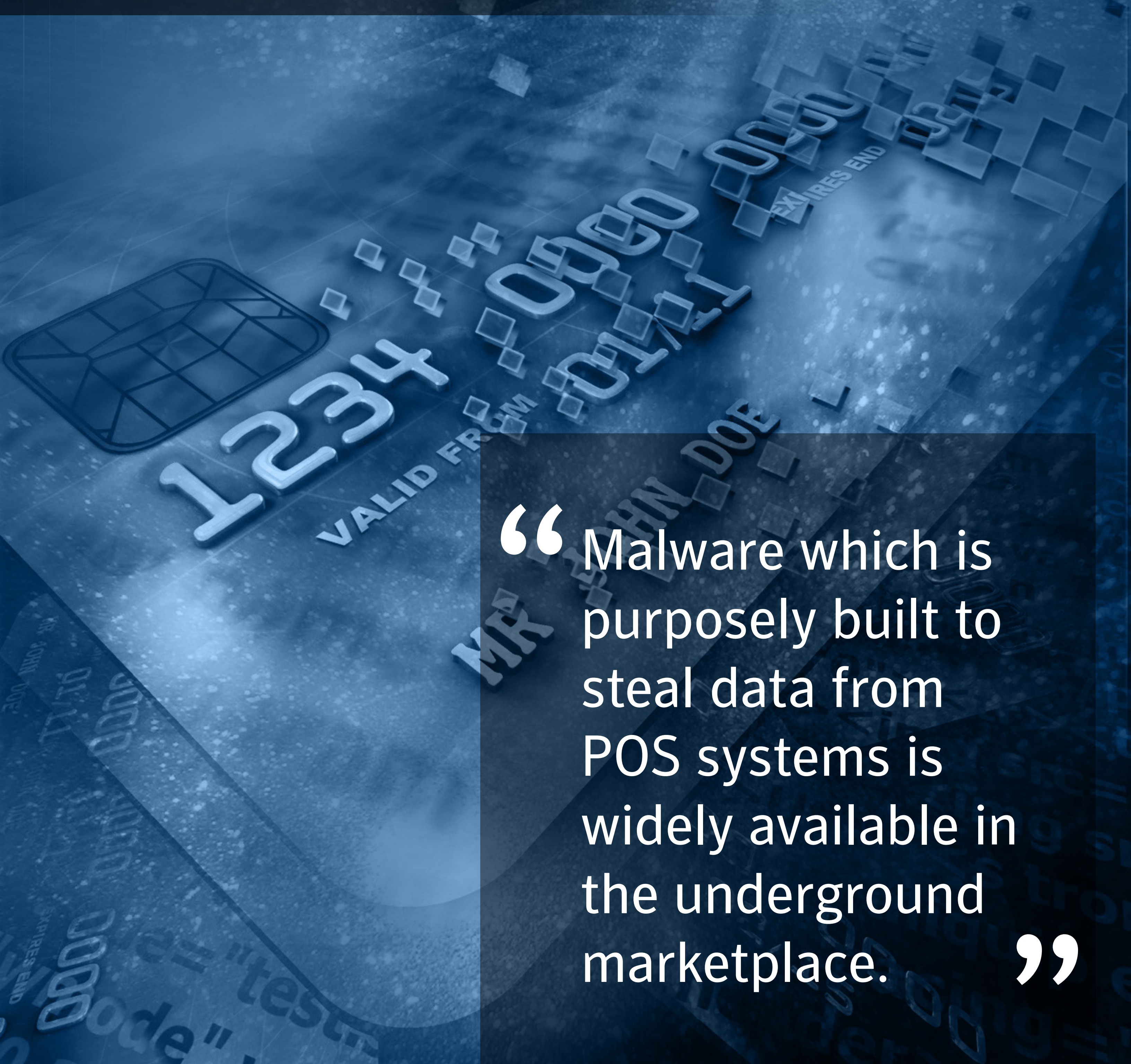
The massive scale of attacks is explained in part because POS malware kits are now widely available on the cybercrime underground. For a modest investment, attackers can buy tools that can potentially net them millions.

Despite improvements in card security technologies and the requirements of the Payment Card Industry Data Security Standard (PCI DSS), there are still gaps in the security of POS systems. This coupled with more general security weaknesses in corporate IT infrastructure means that retailers find themselves exposed to increasingly resourceful and organized cybercriminal gangs.

Many US retailers are still vulnerable to point-of-sale malware attacks and are likely to remain so until the complete transition to more secure payment card technologies in 2015.

Symantec

BACKGROUND



> “Malware which is purposely built to steal data from POS systems is widely available in the underground marketplace.”

Background

Thriving marketplace for stolen cards

While the malware used to mount POS attacks is usually sold on underground forums, these forums are also often where the bounty of those attacks returns to be sold. For example, stolen credit card details from some of the biggest US breaches were sold on a forum known as Rescator.

Research from Symantec found that prices for payment card details can vary heavily depending on a number of factors, such as the type of card and its level, i.e. gold, platinum, or business. Card data originating from the US tends to be cheaper because of the widespread availability stolen US cards. Card details along with extra information, known as “Fullz”, tend to attract higher prices because details such as someone’s date of birth or credit card security password make it easier to perform identity theft.

Single credit cards from the US tend to cost $1.50 to $5, with discounts often available for those who buy in bulk. Single cards from the EU tend to cost more, selling for $5 to $8. Fullz start at $5 and can range up to $20. A single embossed plastic card with custom number and name meanwhile will sell for approximately $70. The stolen cards uploaded to Rescator were initially selling at a cost of $45 to $130 per card before prices later settled down.

Evolution of the threat

The term “POS device” most commonly refers to the in-store systems where customers pay merchants for goods or services. While a lot of POS transactions are carried out using cash, many of these payments are made by customers swiping their cards through a card reader. These card readers may be standalone devices but modern POS systems, particularly those in larger retailers, are all-in-one systems which can handle a variety of customer transactions such as sales, returns, gift cards and promotions. Most importantly from a security standpoint, they can handle multiple payment types.

Attacks on point-of-sale terminals have their genesis as far back as 2005, when attackers began using networking-sniffing malware to intercept payment card data while in transit. A group of attackers led by Albert Gonzalez were the main perpetrators, sstealing more than 90 million card records from retailers.

As payments processors and retailers tightened up their security, the attackers adapted and attention turned to the point-of-sale terminal. When a card is swiped, its details are briefly stored in the terminal’s memory while being transmitted to the payment processor. This provides a brief window for malware on the terminal to copy the card data, which it then transmits back to the attackers. The technique is known as “memory scraping” and it is behind most of the major POS malware attacks seen in 2013 and 2014.

POS security issues

Many all-in-one POS systems are based on general purpose operating systems such as Windows Embedded, Windows XP and later versions, and Unix operating systems including Linux. Consequently, these systems are susceptible to a wide variety of attack scenarios which could lead to large scale data breaches.

Accessibility

All organizations that handle payment card data are required to implement safeguards set down in the PCI DSS. This standard helps organizations to ensure that their systems and procedures are properly secured.

The standard describes a concept known as the cardholder data environment (CDE) and the need to protect it. This is defined as "The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components."

The current standards recommend, but do not require the CDE to be network-segmented from other non-POS systems and the public internet. While a strictly controlled and completely isolated POS system network would be quite secure, it is too impractical for serious consideration. The POS systems must be accessible for software updates and maintenance, allow business data to be exported to other systems (e.g. purchasing data and inventory), allow system and security logs to be exported, have access to required support systems such as network time protocol (NTP) servers (as required by the PCI DSS), and have connectivity to external payment processors.

Despite lacking a rule for segmentation, the PCI DSS does mandate certain levels of access security. For example, if remote access from a public network is allowed, the access must employ two-factor authentication (2FA).

In most mature retail environments, the CDE is appropriately segmented to reduce risk. However, in these environments, pathways still exist from the general corporate network to the CDE.

While previous breaches have occurred by gaining direct access to POS systems, the most common attack route against POS systems is through the corporate network. Once an attacker gains access to the corporate network, for example through a vulnerable public-facing server or spear-phishing email, the attacker could traverse the network until they gain access to an entry point to the POS network. This entry point is often the same as a corporate administrator would utilize to maintain the POS systems.

Lack of point to point encryption (P2PE)

When an individual pays by swiping a credit card at a POS system, data contained in the card's magnetic stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor. When this data is transmitted over a public network, the data must be protected using network level encryption (e.g. Secure Sockets Layer (SSL)).

However, within internal networks and systems, the credit card number is not required to be encrypted except when stored. Albert Gonzalez famously took advantage of this weakness in 2005 by infiltrating many retail networks and installing network-sniffing tools, allowing him to gather over 100 million credit card numbers as they passed through internal networks.

In response, many retailers today use network-level encryption even within their internal networks. While that change protected the data as it travelled from one system to another, the credit card numbers are not encrypted in the systems themselves and can still be found in plain text within the memory of the POS system and other computer systems responsible for processing or passing on the data. This weakness has led to the emergence of "RAM-scraping" malware, which allows attackers to extract this data from memory while the data is being processed inside the terminal rather than when the data is travelling through the network.

Secure card readers (SCR) exist and have been implemented in some environments, enabling P2PE. This can defeat RAM-scraping attacks that work by searching the memory of the POS system for patterns of digits that match those of payment card numbers. Such card readers encrypt the card data at time of swipe and the credit card number remains encrypted throughout the process even within the memory and underneath network-level encryption.

Using P2PE within POS environments is not a new concept. Items such as PINs, when used with debit cards, must be encrypted at the PIN pad terminal. When provisioning terminals, a payment processor or sponsor must provision the terminal by performing “key injection” where a unique encryption key is deployed directly to the device. With this scheme, the PIN remains encrypted at all times.

Software vulnerabilities

Many POS systems are running older operating systems, such as Windows XP or Windows XP Embedded. These versions are more susceptible to vulnerabilities and are therefore more open to attack. It should also be noted that support for Windows XP ended on April 8, 2014 but for Windows XP Embedded, the deadline has been extended to January 12, 2016. No more patches will be issued for any vulnerabilities found in these operating systems after the cutoff dates. This inevitably places POS operators under increased risk of a successful attack and POS operators should have mitigation plans in place. Organizations should verify with Microsoft the exact end-of-life date for the versions of Windows that they are using and plan accordingly.

Susceptibility to malicious code

As many POS systems are running a version of Windows, they are also capable of running any malware that runs on Windows. This means that attackers do not need specialized skills in order to target POS systems and malware that was not specifically designed for use on POS systems could be easily repurposed for use against them.

POS malware was first discovered October 2008, when Visa issued an alert on a new type of exploit. During a fraud investigation, it found that attackers had been installing debugging software on POS systems that was capable of extracting full magnetic stripe data from its memory. Little heed appears to have been taken of this warning, allowing malware authors time to perfect their methods. In the intervening period, the malware authors have worked to streamline the malware, integrating all functionality into a single piece of software.

This development process eventually led to fully featured POS malware kits emerging on underground markets from 2012 onwards. What followed was a flood of high profile breaches, with several major US hit by POS malware attacks.

Case in point: BlackPOS

One of the most widely used forms of POS malware is BlackPOS (detected as Infostealer.Reedum), which is also known as KAPTOXA, Memory Monitor, Dump Memory Grabber, and Reedum. Variants of BlackPOS have been used to mount some of the biggest retail POS breaches.

Its development mirrors the evolution of the broader POS malware market. The earliest versions of BlackPOS date from 2010. Over time, it has evolved into a highly capable cybercrime tool which employs encryption to cover its tracks and can be customized to suit the target environment.

By February 2013, BlackPOS was ready for the mass market and the group behind one of its variants began selling it on underground forums, charging customers $2,000 for the package.

Slow adoption of EMV

Europay, Mastercard and Visa (EMV) is a set of standards for card payments. It is often referred to as "chip and PIN" and is a replacement for traditional magnetic stripe-based cards. EMV cards contain embedded microprocessors that provide strong transaction security features. EMV never transmits the credit card data in the clear, mitigating many common POS attacks. EMV cards are also less attractive to attackers as they are difficult to clone.

While EMV is commonly used in some parts of the world such as Europe, US merchants in particular have been slow to adopt the EMV standard and will not start implementing it until 2015.

Typical anatomy of attacks against POS systems

Attacks against POS systems in mature environments are typically multi-staged. First, the attacker must gain access to the victim's network. Usually, they gain access to an associated network and not directly to the CDE. They must then traverse the network, ultimately gaining access to the POS systems. Next, they will install malware in order to steal data from the compromised systems. As the POS system is unlikely to have external network access, the stolen data is then typically sent to an internal staging server and ultimately exfiltrated from the retailer's network to the attacker.

Infiltration

There are a variety of methods an attacker can use to gain access to a corporate network. They can look for weaknesses in external-facing systems, such as using an SQL injection on a web server or finding a periphery device that still uses the default manufacturer password. Alternatively they can attack from within by sending a spear-phishing email to an individual within the organization. The spear-phishing email could contain a malicious attachment or a link to a website which installs a back door program onto the victim's computer.

Network traversal

Once inside the network, the attackers need to gain access to their ultimate targets–the POS systems. Attackers will typically use a variety of tools to map out the network in order to locate systems within the CDE. While they may exploit vulnerabilities or use other techniques to gain access to these systems, often the simplest method of gaining access is by obtaining user credentials. User credentials may be obtained through keylogging Trojans, password-hash extraction, cracking, and/or replaying captured login sequences, or even brute force. Eventually, the attackers may obtain administrative-level credentials. The attackers may even gain control of a domain controller, giving them full access to all computers in the network. Once in control, they can then gain access to the CDE even if it is in a segmented network by using network and data pathways established for existing business purposes. Once inside the CDE, they can then install malware which allows them to steal card data from the POS systems.

Data-stealing tools

Malware which is purposely built to steal data from POS systems is widely available in the underground marketplace. In some attacks, network-sniffing tools are used to collect credit card numbers as they traversed internal unencrypted networks. Other times, RAM-scraping malware is used to collect credit numbers as they are read into computer memory. Any gathered data is then locally stored in a file until time for exfiltration. Often, this data file needs to be transferred to multiple computers, hopping through the internal network until reaching a system that has access to external systems.

Persistence and stealth

Because the attacker is targeting a POS system and these attacks take time to gather data, they need their code to remain persistent on the compromised terminal. Unlike database breaches where millions of records are immediately accessible, POS system breaches require the attacker to wait until transactions happen and then collect the data in real-time as each credit card is used. Because of this, early discovery of the attack can limit the extent of the damage. Malware persistence can be achieved using simple techniques to ensure that the malware process is always running and restarts any time the system restarts.

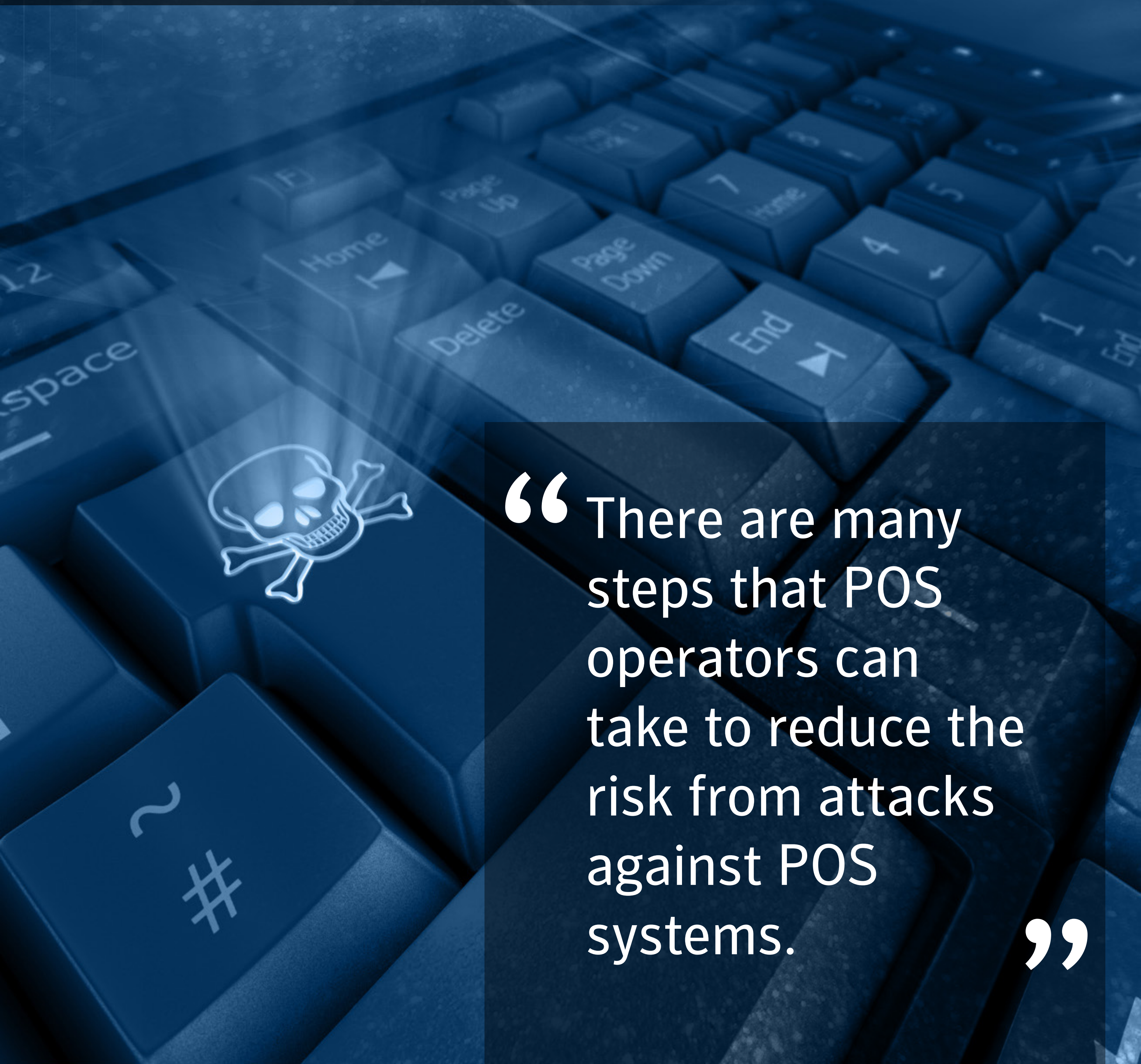
Stealth techniques vary from simplistic obfuscation of filenames and processes to specific security software-bypass techniques. In more secure environments, in order for attackers to succeed, they are already likely to have access to compromised administrative credentials and can use them to scrub logs, disable monitoring software and systems, and even modify security software configuration (e.g. change file-signing requirements or modify whitelisting entries) to avoid detection.

Exfiltration

The attackers may hijack an internal system to act as their staging server. They will attempt to identify a server that regularly communicates with the POS systems and piggyback on normal communications to avoid detection. Any data collected by the RAM-scraping malware will be sent to this staging server, where it is stored and aggregated until a suitable time to transmit to the attacker. At the appropriate time, the attackers may transfer the gathered data through any number of other internal systems before finally arriving at an external system such as a compromised FTP server belonging to a third party. By using compromised servers from legitimate sites to receive the stolen data, the traffic to these sites is less likely to arouse suspicion on the part of the compromised retailer, particularly if they are sites that are often visited by users within the victim organization.

Symantec™

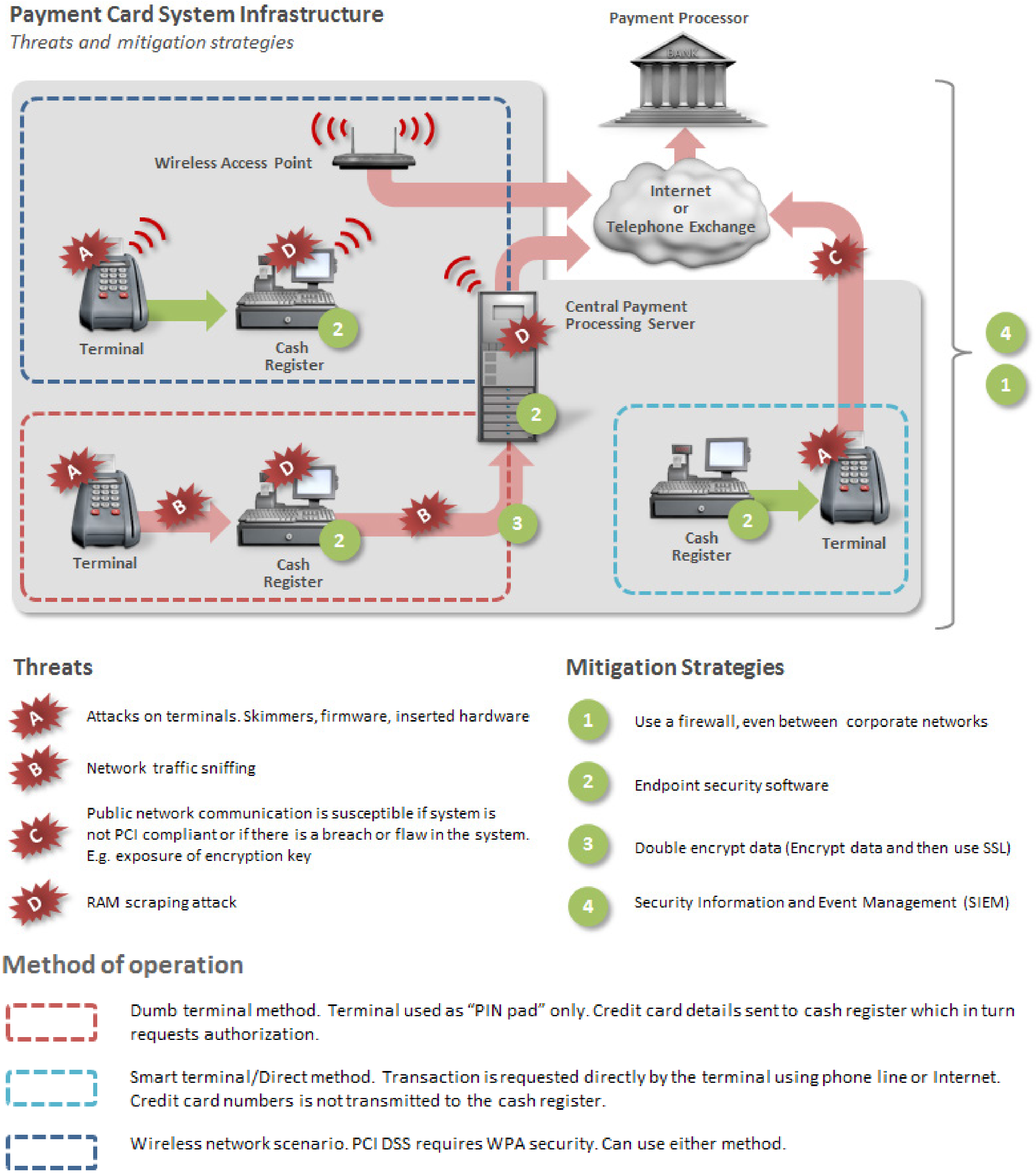
PROTECTING POS SYSTEMS FROM ATTACK



> “There are many steps that POS operators can take to reduce the risk from attacks against POS systems.”

Protecting POS systems from attack

There are many steps that POS operators can take to reduce the risk of attacks against POS systems. The following diagram illustrates the typical infrastructure of payment card systems and the threats against them, along with mitigation strategies that can be employed at various points in the system.



Threats

A Attacks on terminals. Skimmers, firmware, inserted hardware

B Network traffic sniffing

C Public network communication is susceptible if system is not PCI compliant or if there is a breach or flaw in the system. E.g. exposure of encryption key

D RAM scraping attack

Mitigation Strategies

1 Use a firewall, even between corporate networks

2 Endpoint security software

3 Double encrypt data (Encrypt data and then use SSL)

4 Security Information and Event Management (SIEM)

Method of operation

Dumb terminal method. Terminal used as "PIN pad" only. Credit card details sent to cash register which in turn requests authorization.

Smart terminal/Direct method. Transaction is requested directly by the terminal using phone line or Internet. Credit card numbers is not transmitted to the cash register.

Wireless network scenario. PCI DSS requires WPA security. Can use either method.

Figure: Threat to payment card system and possible mitigation strategies

Practical steps to take

- Implementation of PCI DSS
    - Install and maintain a firewall to facilitate network segmentation
    - Change default system passwords and other security parameters
    - Encrypt transmission of cardholder data across open, public networks
    - Encrypt stored primary account number (PAN) and do not store sensitive authentication data
    - Use and regularly update security software
    - Use intrusion protection system (IPS) at critical points and the perimeter of the CDE
    - Use file integrity and monitoring software
    - Use strong authentication including two-factor authentication for remote systems
    - Monitor all network and data access (SIEM)
- Test security systems, perform penetration testing, and implement a vulnerability management program
- Maintain security policies and implement regular training for all personnel
- Implement multi-layered protections including outside the CDE. Typically, the attacker needs to traverse multiple networks and layers of security before reaching a POS system. Any single layer that the attacker is unable to bypass prevents successful data exfiltration.
- Implement P2PE or EMV (“Chip and PIN”)
- Increase network segmentation and reduce pathways between the CDE and other networks.
- Maintain strict auditing on connections to between the CDE and other networks. Reduce the number of personnel who have access to systems that have access to both the CDE and other networks.
- Employ two-factor authentication at all entry points to the CDE and for any personnel with access rights to the CDE
- Employ two-factor authentication for all system configuration changes within the CDE environment
- Implement system integrity and monitoring software to leverage features such as system lockdown, application control, or whitelisting

Symantec protection

Symantec products detect all of the currently known variants of point-of-sale malware, including:

BlackPOS

- Infostealer.Reedum
- Infostealer.Reedum!g2
- Infostealer.Reedum.B
- Infostealer.Reedum.C

FrameworkPOS

- Infostealer.Reedum.D

Dexter

- Infostealer.Dexter

Chewbacca

- Infostealer.Fysna

JackPOS

- Infostealer.Jackpos

RawPOS

- Infostealer.Rawpos
- Infostealer.Rawpos!g1

Vskimmer

- Infostealer.Vskim

Backoff

- Trojan.Backoff
- Trojan.Backoff!gm

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems.

Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY . The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.