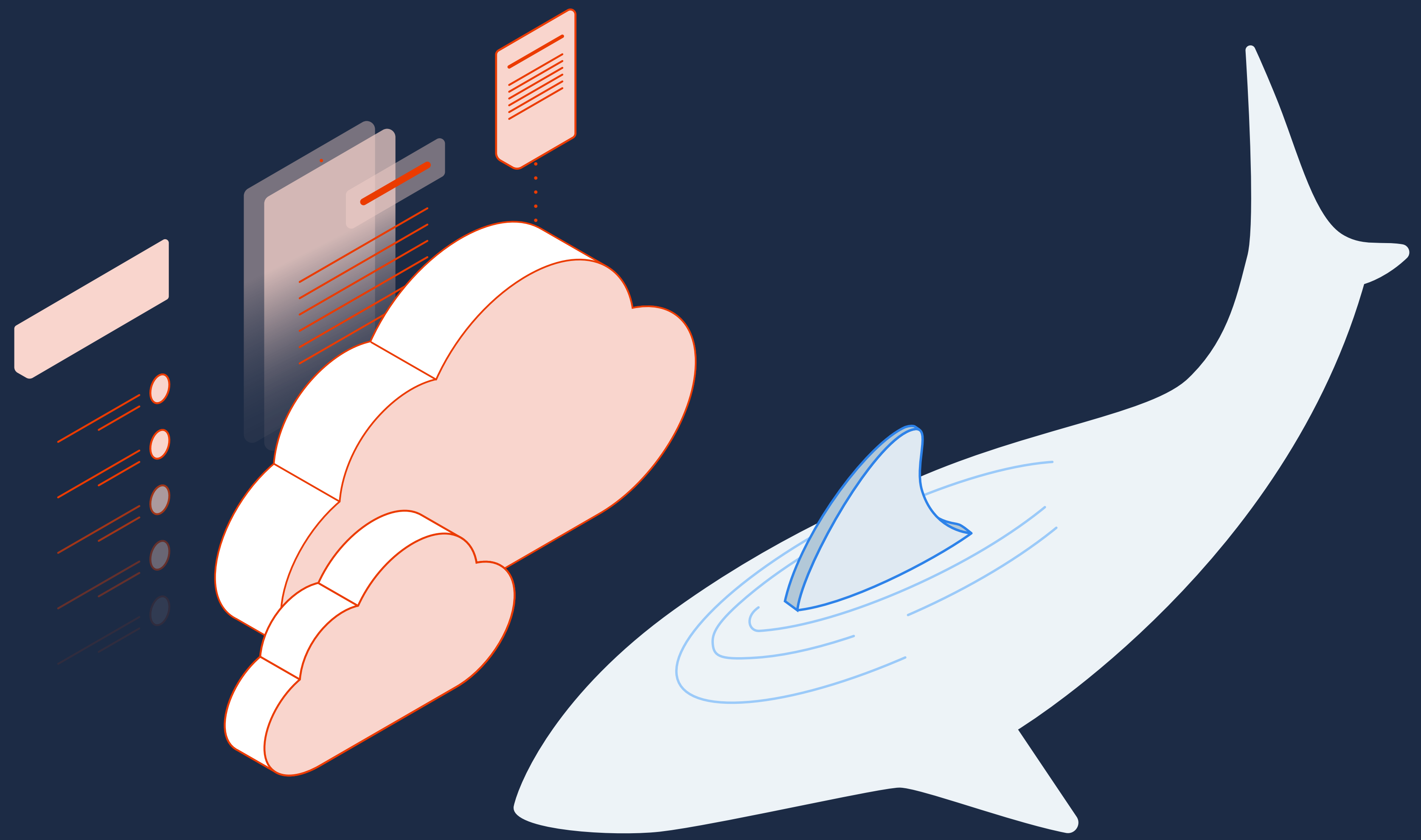


ALSID ACADEMY

Episode 12

POS: PREVENTING MALWARE IN POINT-OF-SALE SYSTEMS

In this whitepaper, Alsid looks at the resurgence of point-of-sale (POS) malware and what steps you can take to prevent it from infecting your networks.

While organizations should follow regulations to protect credit card transactions, compliance isn't always enough to safeguard data. Case in point, POS malware exploded in 2019. Restoring infected systems, settling lawsuits, and bandaging up reputational damage carried a hefty price tag. Target spent $18.5 million just in payouts from lawsuits from 47 U.S. states over a data breach of its POS systems.

POS malware reaps big rewards for cybercriminals. Hackers can steal funds and sell credit card data on the dark web, inflicting losses for both clients and retailers. POS malware usually aims to steal credit card data, but ransomware can also affect POS systems. Instead of demanding money or cryptocurrency to get your data back, hackers take down POS until a ransom is paid. Being locked out of your POS systems has a devastating impact, and the entire business can grind to a halt.

POINT-OF-SALE MALWARE IN 2019

New POS malware variants and the ubiquity of old malware code mean that POS attacks remain an active threat. Data from 2019 on two new strains of POS malware shows that hackers are actively targeting credit card data. The first, known as GlitchPOS, appeared in 2019 and is completely new. The second, called DMSniff POS, has been active for four years but was only discovered in 2019.

Ransomware is also an increasing problem for organizations that are not prepared for an attack. The FBI advises against paying ransoms because it fuels criminal activity. Paying ransoms doesn't guarantee data will be decrypted or that POS systems can be returned to service. But many organizations choose to pay regardless.

Malware can lay dormant for long periods before it is activated. A long gestation period makes it harder to recover systems from backups also infected with the same malware. Rebuilding networks from scratch is often the best way to recover if backups are also infected.

Many POS devices run on embedded versions of Windows 7 without up-to-date security patches or antivirus protection. And because Windows 7 Embedded POSReady is not always properly secured, it is an easy target. In recent years, the reach of POS systems has extended to mobile devices (mPOS), which are equally susceptible to compromise. If malware spreads beyond POS, organizations need to pay to clean up entire networks.

EXAMPLES OF POINT-OF-SALE BREACHES

POS malware poses a threat to businesses unprepared for an outbreak. Here are some examples of POS malware that have been active in the past few years. As you will see, POS is not always the initial target. And attackers use sophisticated methods to eventually access and steal information from POS as credit cards are being processed.

Active Directory used by POS malware in Target attack

The popular TrickBot malware was updated in 2018 to include a new POS module. What is interesting is how the module identifies POS devices. It queries Windows Server Active Directory (AD) to detect potential POS terminals on a network.

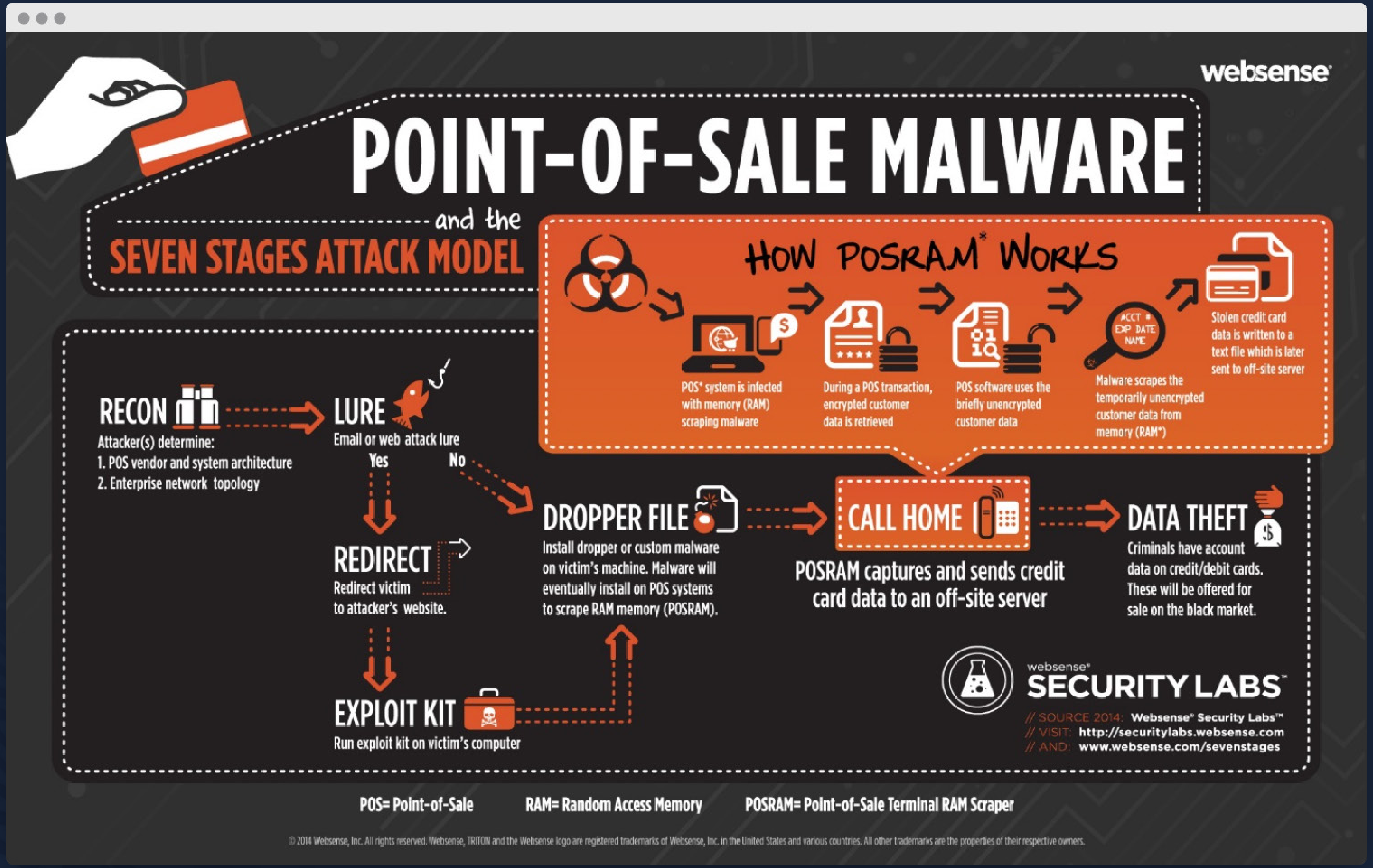
The POS module runs LDAP queries against Active Directory Global Catalog servers to find substrings that might identify POS devices. Searches include terms like *POS*, *RETAIL*, *STORE*, and *TERM*.

This isn't the first time AD has been used for reconnaissance purposes by POS malware. A well-publicized attack in 2013 saw criminals steal personally identifiable information (PII) from 70 million Target customers, including 40 million credit and debit card details.

The initial compromise used a phishing campaign via email to access Target's HVAC vendor. Malware was then installed to steal credentials that gave the hackers access to Target's web services.

Vulnerabilities in the web servers were exploited to upload files and run commands to locate servers containing credit card and customer information. Active Directory was also used to collect data on all of Target's computers, services, and servers using standard administration tools.

Figure 1 – POS malware attack model



POS* system is infected with memory (RAM) scraping malware

During a POS transaction, encrypted customer data is retrieved

POS software uses the briefly unencrypted customer data

Malware scrapes the temporarily unencrypted customer data from memory (RAM*)

Stolen credit card data is written to a text file which is later sent to off-site server

RECON: Attacker(s) determine:
1. POS vendor and system architecture
2. Enterprise network topology

LURE: Email or web attack lure

REDIRECT: Redirect victim to attacker's website.

EXPLOIT KIT: Run exploit kit on victim's computer

DROPPER FILE: Install dropper or custom malware on victim's machine. Malware will eventually install on POS systems to scrape RAM memory (POSRAM).

CALL HOME: POSRAM captures and sends credit card data to an off-site server

DATA THEFT: Criminals have account data on credit/debit cards. These will be offered for sale on the black market.

// SOURCE 2014: Websense® Security Labs™
// VISIT: http://securitylabs.websense.com
// AND: www.websense.com/sevenstages

POS= Point-of-Sale RAM= Random Access Memory POSRAM= Point-of-Sale Terminal RAM Scraper

© 2014 Websense, Inc. All rights reserved. Websense, TRITON and the Websense logo are registered trademarks of Websense, Inc. in the United States and various countries. All other trademarks are the properties of their respective owners.

The criminals went one step further and used a method known as ‘Pass-the-Hash’ (PtH) to impersonate an AD domain administrator. Domain Admins have complete access to Active Directory and devices joined to the domain. Administrative access to AD allowed the criminals to infect Target’s POS system.

Target was PCI DSS compliant, so the hackers were unable to get credit card details stored on Target’s servers due to encryption. Instead, the criminals targeted POS systems to scrape memory and capture credit card data as it was being processed (Figure 1). The AD domain administrator credentials came in handy again, allowing the attackers to set up a file share on an FTP-enabled (File Transfer Protocol) server and transfer the stolen information from the POS systems. A script was then used to send the captured files to the hacker using FTP.

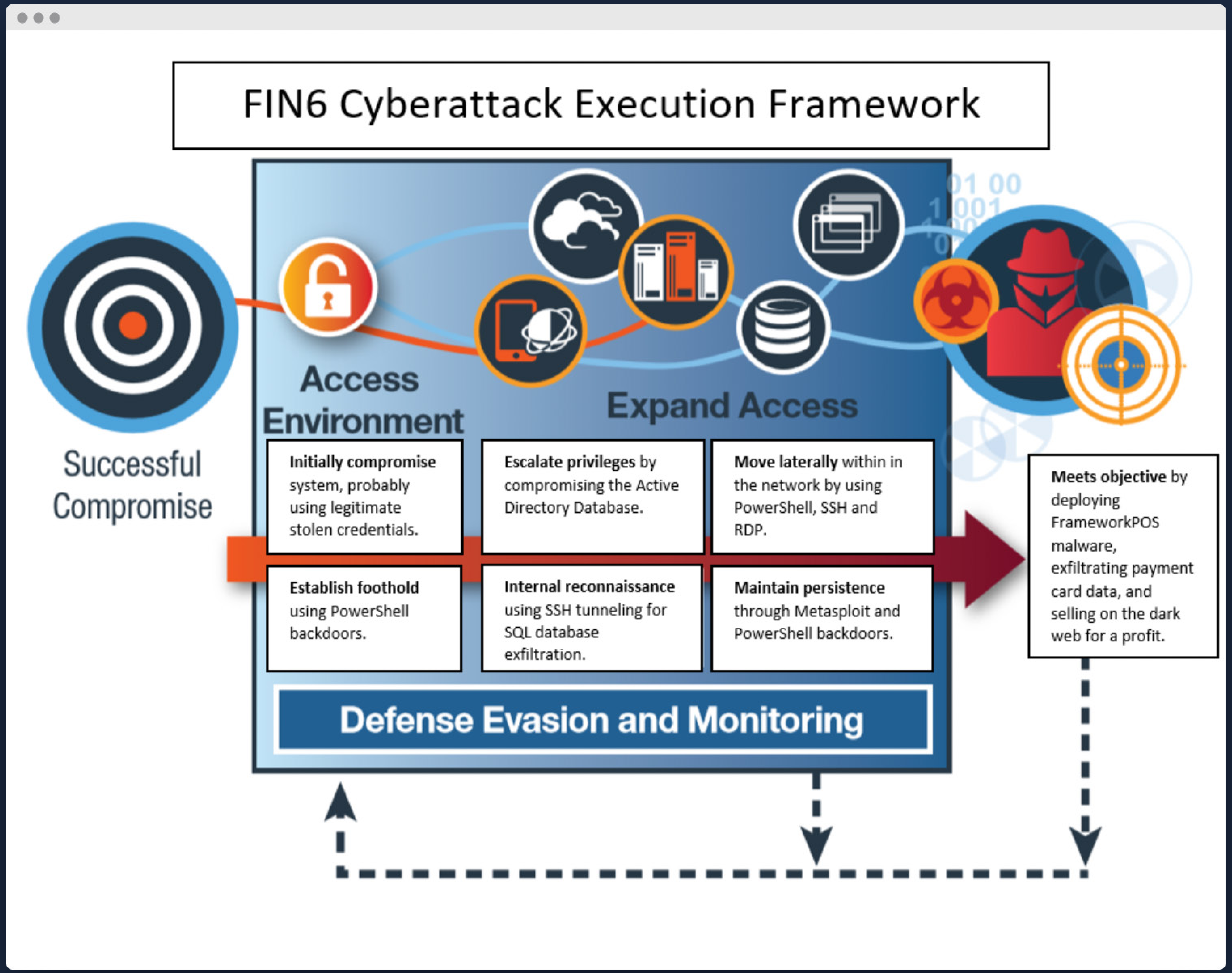
Retailers in Europe and the U.S. compromised by Trinity (FrameworkPOS) POS malware

In Q3 2018, retailers in Europe and U.S. were targeted by a campaign reportedly connected to the FIN6 criminal group. Exploiting POS devices using malware known as Trinity, sometimes called FrameworkPOS, FIN6 was able to 'scrape' the memory (RAM) of POS devices to collect credit card data and upload it to a command-and-control server. FIN6 then sold the data on the dark web.

The initial compromise method varies, but one way FIN6 gained access to POS devices was through Windows Management Instrumentation (WMI). WMI can be used to run PowerShell commands on remote systems (Figure 2). FIN6 obfuscated the commands using base64 encoding and gzip compression to evade detection by security software.

Tip: Windows 10 can scan obfuscated PowerShell code in a sandbox environment to allow the built-in antimalware engine to detect malicious code before it runs. Third-party antimalware solutions can also access the same feature through an API.

Figure 2 - FIN6 Cyberattack Execution Framework



FIN6 Cyberattack Execution Framework

Initially compromise system, probably using legitimate stolen credentials.

Establish foothold using PowerShell backdoors.

Escalate privileges by compromising the Active Directory Database.

Internal reconnaissance using SSH tunneling for SQL database exfiltration.

Move laterally within in the network by using PowerShell, SSH and RDP.

Maintain persistence through Metasploit and PowerShell backdoors.

Meets objective by deploying FrameworkPOS malware, exfiltrating payment card data, and selling on the dark web for a profit.

U.S. fuel dispensers hacked

Fuel pumps in the U.S. are often targeted because many don't support chip transactions. In November 2019, VISA published details about attacks at fuel pumps that it investigated in August and September of 2019. Unlike previous attacks that involved criminals installing card-skimming devices inside fuel pumps, the attacks saw hackers get access to the merchant's internal network before gathering credit card data from POS. VISA says that the attacks were successful because of the lack of support for chip transactions and the failure to comply with PCI DSS regulations. Like the Target attack, email phishing was used to initially infect merchants' networks.

DMSniff hits small and medium-sized businesses in the food, hospitality, and entertainment industries

Discovered in 2019 but thought to be active since 2016, DMSniff differs from older forms of POS malware because it can create command-and-control domains on the fly. That means hackers can continue to send captured card data even if a service provider or law enforcement agency shuts down a command-and-control center.

DMSniff can be delivered in a variety of ways. Security researchers believe that criminals distribute DMSniff by using brute-force attacks against Secure Shell (SSH) connections or by looking for operating system vulnerabilities that can be exploited.

Internet game brings POS malware to small and medium-sized companies

2019 saw hackers target small and medium-sized companies with a completely new form of POS malware called GlitchPOS. Delivered as a game containing pictures of cats, the package also has a memory scraper. The main code includes just a few functions, like the ability to send data back to a command-and-control center. GlitchPOS can also receive commands so that criminals can update the software, create scheduled tasks, download other malware, and even wipe itself from infected devices.

HOW TO PREVENT POS MALWARE INFECTIONS

Much of the POS malware in circulation relies on organizations using outdated software that isn't kept up to date with security patches. But as POS devices are not usually the initial entry point for the malware that eventually infects them, businesses should look at protecting all vulnerable systems to prevent malware from spreading device to device.

Here are six ways that you can prevent malware infecting POS devices and other systems on your network.

1. Block Office macros for users who don't need them

Macros are often used to distribute malicious payloads to Windows systems. The best way to prevent malware spreading to Windows and POS devices through macros is to disable the feature completely in Office applications. Most users will never need to use a macro.

Employees who need macros can be protected by running the latest versions of the Office desktop applications. The default Trust Center settings in Office 2016, and later versions, turn on a safety feature called Protected View. Documents with macros downloaded from untrusted sources run in a sandbox when Protected View is enabled. Users are required to manually click Enable Content before macros can run. Protected View is a safety feature, but it relies on users to decide whether a document is safe.

Tip: Use Group Policy to configure the Office Trust Center to block content with macros for most users.

2. Implement Microsoft's Active Directory security best practices

Not all malware contains a 'spreader' or, in other words, a means to propagate from one device to another. Hackers are increasingly weaponizing Windows Server Active Directory for reconnaissance to identify targets. And in some cases, hackers move laterally and gain privileged credentials to further infect systems after the initial compromise.

Microsoft recommends keeping the number of domain administrators, and other privileged groups, in Active Directory to a minimum. Organizations can delegate privileges so that IT staff can perform everyday administration tasks without issuing domain admin rights. Tasks like managing users, groups, resetting passwords, and accessing devices for remote support can all be carried out without domain administrative access to AD.

Tip 1: Delegate rights using the Delegation of Tasks Wizard in Active Directory Users and Computers.

Tip 2: Using a unique local administrator password on each domain-joined device makes it harder for hackers to spread malware to devices.

3. Limit exposure to the Remote Desktop Protocol from the Internet

Remote Desktop is commonly used to administer and manage servers remotely. But it isn't the most secure way to manage Windows Server. Rarely a month goes by where Microsoft doesn't patch a critical flaw in Remote Desktop.

Tip: Consider deploying the Windows Admin Center (WAC) for remote administration and close RDP port 3389 inbound access from the Internet.

4. Use Application Control to block unwanted processes and apps

Windows Defender Application Control and AppLocker are two features built into Windows and Windows Server that can be used to block malicious apps. Windows Defender Application Control was introduced in Windows 10, and it provides more robust protection than AppLocker.

Windows Defender Application Control is the preferred solution if security is the primary reason for implementing Application Control. It can protect Windows even in situations where the OS kernel has been compromised. But it is less flexible and more complicated to set up than AppLocker.

Tip: AppLocker is a good way to get started with Application Control. AppLocker can scan reference systems to automatically create whitelists of apps and processes that are allowed to run. You can test AppLocker in audit only mode before setting it to actively block unauthorized code.

5. Update devices to Windows 10 and keep them current with security patches

Windows 10 IoT Core and Enterprise SKUs replace Windows Embedded editions, including Windows Embedded POSReady 7. Windows 10 IoT Enterprise is designed for fixed devices, like ATM machines and POS terminals.

Fixed devices are locked down to a single application, or set of applications, that are launched through Assigned Access or Shell Launcher. Assigned Access and Shell Launcher are both features for creating locked-down environments that restrict user access to applications.

Windows 10 is more secure than Windows 7. It contains technologies like Windows Defender Credential Guard and built-in antivirus that make it easier for organizations to protect clients and prevent malware spreading to POS systems.

Windows Update for Business and Microsoft Intune can be used to manage how updates are applied to Windows 10. And while keeping current with the latest fixes from Microsoft is important, other defenses, like Application Control, should be used to provide complete protection.

Migrating from Windows Embedded to Windows 10 IoT Enterprise on POS devices brings better management and security. But migration isn't easy to perform, and it might not be possible if your POS vendor doesn't support Windows 10.

6. Segregate and protect network traffic

POS devices are particularly vulnerable to attack, so it makes sense to isolate them from the rest of your network as much as possible. For example, segregate POS from end-user systems that have access to the Internet (Figure 3).

You can also analyze network traffic to and from POS devices. Products from network vendors like Cisco allow you to set up zones for different types of devices. If traffic flow rules between zones are broken, you will be alerted. Deep inspection of network traffic can also reveal malware on your network.

Figure 3 – POS network segmentation

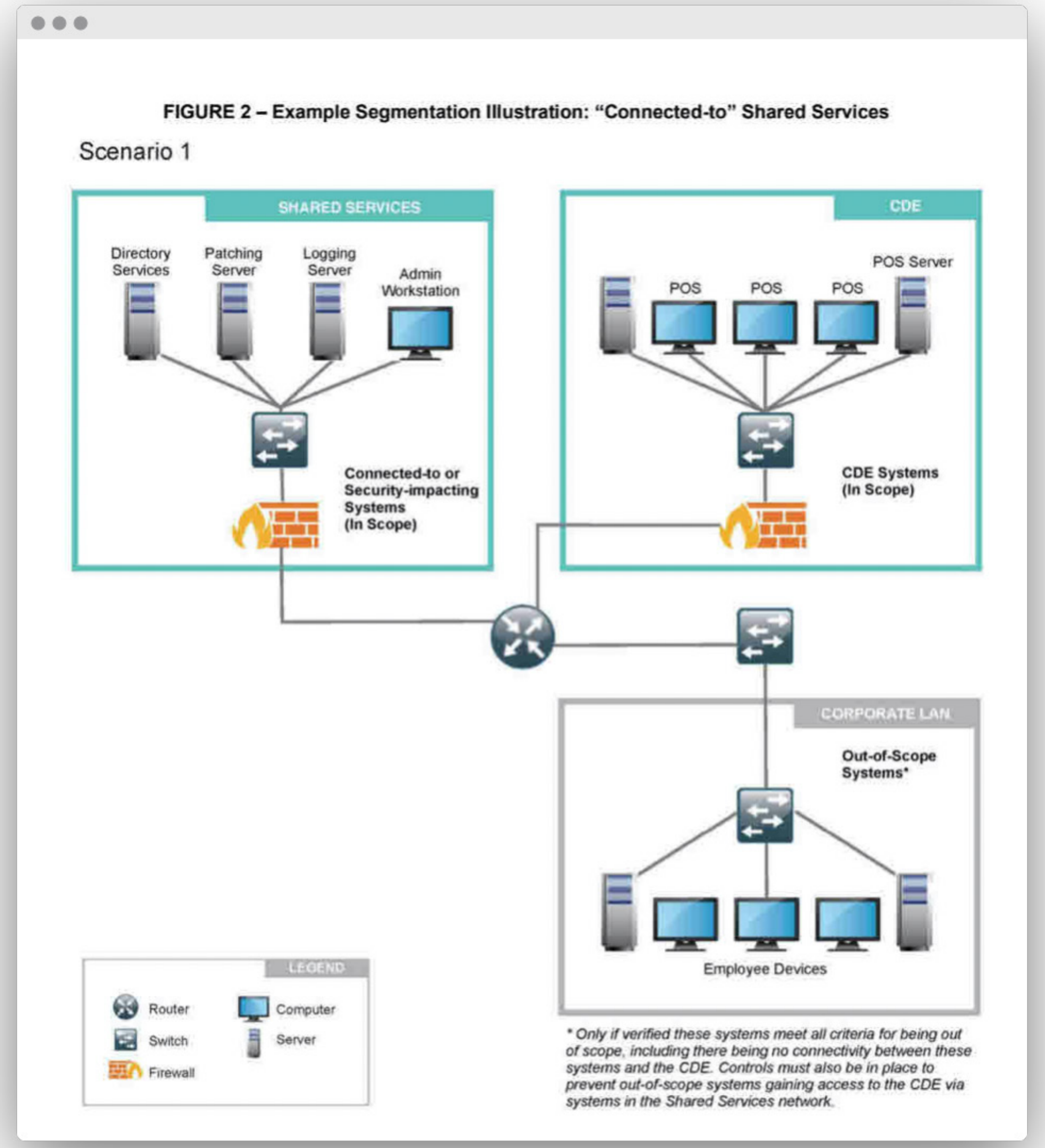


FIGURE 2 – Example Segmentation Illustration: "Connected-to" Shared Services

* Only if verified these systems meet all criteria for being out of scope, including there being no connectivity between these systems and the CDE. Controls must also be in place to prevent out-of-scope systems gaining access to the CDE via systems in the Shared Services network.

ALSID: STOP MALWARE INFECTING POS DEVICES

Implementing Microsoft's security best practices for Active Directory makes it harder for hackers to compromise networks and eventually infect POS systems. But Microsoft's tools don't allow you to monitor AD threats in real time. The Windows Event Log records a lot of useful information. But even if the logs are centralized and collected using a Security Information and Event (SIEM) solution, you might discover an attack when it is already too late.

Alsid can identify security issues with AD before attackers exploit them to spread malware. Built-in attack path technology and real-time alerts help organizations mitigate issues and remediate threats. Alsid integrates with SIEM and security tools to proactively improve AD security, providing dynamic dashboards to give you a level of insight that isn't possible with the tools available out-of-the-box in Windows Server.

ALSID

EPISODE 12

POS: PREVENTING MALWARE IN POINT-OF-SALE SYSTEMS

ALSID ACADEMY