Microsoft

Protecting Point of Sale Devices from Targeted Attacks

1-Apr-14

Version 1.0 Final

Prepared by

Sean Finnegan, Cybersecurity Director

Michael Howard, Principal Cybersecurity Architect

Microsoft

Microsoft

Table of Contents

1 Introduction

Recent attacks on major retailers have resulted in an increased focus on the security of Point of Sale (POS) devices. These devices are typically the front line for processing both customer payment data as well as loyalty programs that can include customer Personally Identifiable Information (PII). As a result any compromise of these devices at scale can yield an attacker not just credit card information but also a wealth of other customer information to include names, phone numbers, e-mail, and physical addresses.

While the motivation for these attacks appears to be financial gain many of the techniques used share similarities with targeted attacks designed to steal intellectual property. Like "Advanced Persistent Threat" or APT attacks the retail breaches have involved lateral movement to get broad access to backend systems, implanting custom malware, and exfiltrating data. As a result, many of the same recommendations that the Microsoft Cybersecurity Team regularly provides to customers when responding to an APT attack can also be applied to POS devices.

This paper will focus solely on major attack vectors designed to provide wide-scale access to POS devices. A related whitepaper, titled *A Systematic Method to Understand Security Risks in a Retail Environment,* looks more broadly at retail systems using the STRIDE methodology to encompass backend systems such as retail ERP and e-commerce systems.

2 Hardening the Point of Sale Device

While the Point Of Sale terminal is a fixed purpose device it still has an underlying operating system and applications that a would-be attacker could try to exploit to gain access to the system. Many of the same recommendations that apply to desktop and server systems apply equally to point of sale devices and the relative uniformity, in the application of these recommendations, should make some mitigations easier to manage.

First, you should keep the software and operating system on your POS device up to date. This includes applying critical software updates for both the OS and applications in a timely fashion as well as running the most modern version of the operating system available for your POS device. As we will discuss below the updating mechanism must be deployed so as not to introduce its own lateral traversal threat.

With each successive release of the Windows operating system Microsoft has not only worked to eliminate vulnerabilities but to add additional protections designed to make it more difficult to exploit new vulnerabilities. This includes memory protections such as DEP, ASLR, HTOC, and

SEHOP[1], as well as techniques such as running select applications in "low rights" mode. Running the most recent version of the OS available for your device ensures you have these additional protections against compromise.

In addition, each POS device should have a form of anti-malware running on it and the signatures should be kept up to date. Many POS vendors will offer a recommended AV solution as part of their solution and depending on the version of Windows running on the POS device it may already include Windows Defender. For POS devices that do not currently have AV software Microsoft also offers the Systems Center Endpoint Protection anti-malware that can be applied to most types of Windows POS devices.

As fixed purpose devices POS terminals are excellent candidates for application whitelisting solutions. An application whitelisting solution is able to detect when a program is being launched and then determine whether or not is should be allowed based on a predefined list. There are multiple 3rd party whitelisting solutions as well as the Microsoft AppLocker or Software Restriction Policies that are built in to Windows. While it will likely require some testing to verify it does not impact the operations of the POS device a whitelisting solution will restrict the device to just running the desired Point of Sale application.

Finally, given that the POS device has a fixed purpose and a fixed configuration, consider using a technology to regularly reset the device configuration back to a known trusted state. One solution would be the use of the Windows Enhanced Write Filter (EWF) that is available on Windows Embedded and POSReady platforms. The EWF is a file system filter that redirects any attempted writes to the protected disk partition into volatile memory but makes the write appear to have succeeded to the requesting application. As a result, an application – including malware or an attacker – that attempts to permanently change the configuration of the device would appear to succeed but at next reboot those changes would disappear. However, if the attacker or malware is EWF aware and has sufficient privileged access to the OS it is possible to disable this as well as other protections.

In summary, the following are suggested measures to protect the POS device from compromise:

1. Keep the POS operating system and application up to date with security patches.
2. Run the most current POS operating system you are able.
3. Use an application whitelisting solution to restrict applications.
4. Deploy a form of anti-virus to the POS device and keep the signatures up to date.
5. Use a technology to prevent unwanted changes to the POS device such as the Enhanced Write Filter or network boot.

[1] http://msdn.microsoft.com/en-us/library/bb430720.aspx

3 Protecting Data At the Endpoint

It is difficult to protect sensitive data on a device where the attacker has complete control of the operating system. However, dedicated hardware devices that never expose unencrypted data to the terminal can provide a safeguard provided that the encryption key is never shared with the terminal. Through the use of encrypting card reader hardware or cards that have a built in cryptographic processor the card data can be encrypted so that it is inaccessible to attacker malware running on the POS device.

This assumes that no customer PII is visible to the terminal either in the initial card swipe, or in the authorization data returned to the POS terminal from the payment system. In addition, many retailers have separate loyalty programs that may contain customer PII although typically not credit card data. While this may be of less interest to an attacker this data still could be stolen by malware on the POS device and as a result just encrypting the credit card data at the swipe is not a panacea to preventing the theft of customer PII.

4 Mitigating Lateral Traversal to Devices

Some attackers may choose to attack one or more POS devices over the network using exploits or even using a physical attack[2] on a device in a store. However, it is difficult to compromise hundreds or thousands of devices using these methods and in the recent retail attacks it is likely that the attacker leveraged some sort of lateral traversal using stolen but legitimate privileged credentials to compromise a large number of devices.

Microsoft has extensive experience in countering these types of attacks as they are often used by APT groups to quickly gain access to information throughout the enterprise after compromising a small number of systems. Microsoft has previously published general guidance on countering these threats in the white paper *Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques*[3]. In this section will we focus on some specific scenarios likely to allow the broad compromise of POS devices.

[2] The discussion of protection against physical attacks on POS devices is out of scope for this paper.
[3] http://www.microsoft.com/en-us/download/details.aspx?id=36036

Active Directory

Many retailers join their Windows POS devices to an Active Directory (AD) in order to gain the many benefits such as centralized configuration management, account management, and easy authentication to network resources. While this is something that we continue to recommend, customers should also be aware that a compromised Active Directory would also become an avenue for an attacker to spread malware throughout the enterprise – including to POS devices. If an attacker gets privileged access to Active Directory such as through the theft of Doman Admin or Enterprise Admin credentials he or she has almost limitless access to systems joined to that AD forest. This includes being able to push programs to run on systems, change security settings on systems, and modify the membership of local groups on systems such as the local administrators group.

Fortunately, the methods by which an Active Directory are typically compromised are well understood and consist primarily of very flat AD designs and administrative practices that put credentials at risk. The previously mentioned PtH white paper describes these attacks and mitigations in great detail and we encourage customers to implement those recommendations to secure not just their POS devices but their entire network.

Another consideration is whether POS devices should be part of retailer's production Active Directory forest or joined to a domain in a separate forest. In Active Directory a separate forest provides a security boundary between systems. This would prevent a compromise of AD in one forest from also compromising resources in the other forest[4]. Cross-forest trust relationships can be established between the forests to allow controlled access to resources across the forest boundaries. This allows similar functionality to a single forest while providing better containment in the event of a compromise.

Shared Service Accounts

In Windows a "service" is a process that is automatically started by the operating system and runs in the background to provide a desired function. Many parts of the operating system function as services as well as applications that need to stay running even when no user is active on the system. On POS devices this can include applications such as security scanners, systems management software, and even part of the POS application itself. When a service is created it

[4] Shared userid and passwords in both forests could still allow a compromise across forest boundaries.

must be set to run as some user account that can include the machine[5] account, a local user, or a domain user account.

In some cases a service will be installed across POS devices using the same Active Directory account or using a common local account created on each system. This is typically done to simplify access to network resources or for the server side of an application to authenticate to the POS device. If this service account is also configured on non-POS systems - such as when the same systems management service account is configured on desktop, servers, and POS systems - the result is a single credential that if compromised has broad access to the network.

Unless using the machine account, the userid and password for this service must be entered and stored encrypted by the operating system for use at system startup. It is important to recognize that while a regular user cannot obtain these logon credentials a local administrator or an attacker who has obtained local administrator access can through the use of common attacker tools. As a result, the compromise of a single system configured with this service account can expose credentials that are valid for access across a large number of devices. Furthermore, in many cases these accounts are members of the local administrators group across devices in order to facilitate privileged access.

Retailers should review their POS devices for services that are running as accounts other than LocalSystem, NetworkService, and LocalService. Where possible, reconfigure these services to use one of these machine accounts. Both LocalSystem and NetworkService can access network resources as the machine account in Active Directory but are unique to each device.

If a common domain or local user account must still be used consider limiting its usage to just POS devices or better yet using multiple accounts with a different account for various POS device communities (e.g. per store, per region, per business). This will not only limit the exposure of the account to attackers but also limit the usefulness to a subset of systems should the account become compromised.

Also, try to limit the privileges assigned to the service account on POS devices in order to make it less useful to an attacker.

[5] There are actually multiple forms this machine account can take including the Local System, Local Service, and Network Service. More information is available at http://msdn.microsoft.com/en-us/library/windows/desktop/ms686005(v=vs.85).aspx

This includes not making the account a member of the local administrators group but also avoid granting the account unnecessary and sensitive user rights such as:

- Allow log on locally
- Access this computer from the network
- Allow logon through Remote Desktop Services
- Act as part of the operating system
- Backup files and directories
- Restore files and directories

The goal is to limit both how widely a single stolen account can be used across devices as well as to limit the amount of damage an attacker can do to a device with the account. Most of the current POS malware require administrator or sensitive user rights to steal customer PII.

Shared Local Administrators

Previously we mentioned how shared local accounts will sometimes be created to support a shared service across systems. We also discussed how administrator or privileged accounts are often necessary for attackers to succeed in stealing customer PII from POS devices. In addition to these scenarios, we need to consider local accounts that are created as part of the OS installation as well as for the terminal operator.

During installation of the operating system at least one local administrator is always created and it is common during scripted deployments to use the same password for this account on all deployed systems. Like with service accounts an attacker that has obtained privileged or admin access to a device can obtain the passwords for local accounts. This compromise of the userid and password for a shared account on one system can then be used to logon to any other system that uses the same userid and password.

Microsoft recommends that customers use unique random passwords for local administrator accounts, disable those accounts, or at a minimum restrict how those accounts can be used in network connections. Details on these mitigations and how to implement them are provided in the referenced *Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques* white paper.

Other Shared Local Accounts

It is common in retail environments to use shared local user accounts to logon to POS devices even though these devices are joined to an Active Directory domain. This is to ensure that the operator can access the terminal even if there is a network connection issue and is also because

it is not considered practical to create and maintain user accounts for retail associates where there are a very large number of users and high personnel turnover.

Such trade-offs need to be made for business reasons but care should also be taken to limit the potential for abuse of these shared local accounts. First, these accounts should only be given the privilege to log on locally and not as a service, via the network, or via Remote Desktop Services. These accounts should also never be local administrator accounts or given sensitive user privileges such as the below.

- Allow log on as a service
- Access this computer from the network
- Allow logon through Remote Desktop Services
- Act as part of the operating system
- Backup files and directories
- Restore files and directories

Where possible, different passwords should be used in order to limit the systems on which this shared account is valid.

5 Conclusion

Point Of Sales devices are prime targets for attackers because they are the front line for collecting information from customers and are often less well protected than backend systems. Recent large scale compromises have required the ability to compromise these systems at scale and often use the same techniques used in targeted attacks designed to steal intellectual property. As a result, applying the same techniques of limiting the ability for attackers to move laterally in a compromise can dramatically reduce the damage from an attack. In addition, there are a number of measures you can take to specifically protect POS devices from compromise as well as securing customer credit card data as it is collected.

We strongly encourage all retail customers to review and implement the measures in this paper as a first step towards mitigating the risk of the wide scale theft of customer information. In addition, we recommend customers read the whitepaper *A Systematic Method to Understand Security Risks in a Retail Environment* to look at other threats to your retail infrastructure. This paper will outline a typical retail threat model and show how to use this as a structured approach to implementing mitigations to other systems in your environment such as e-commerce platforms and back of the house systems.