COMODO

Whitepaper

September 22, 2014

Point of Sale Vulnerability Threatens Retail

Comodo SecureBox provides a safe harbor that turns POS into a Point of Security

SECURE BOX

COMODO ENTERPRISE™

Point of Sale in Crisis

Over the past year, there have been an alarming number of high profile data breaches of customer cardholder and personal information through compromises of retail Point-of-Sale (POS) systems. In December 2013, retail giant Target revealed that a breach of their Point-of-Sale systems in the early weeks of the holiday shopping season had compromised the personal data of as many 110 million customers, including the information needed to duplicate credit/debit cards.

Despite heightened awareness of the vulnerability of POS and the impact of POS breaches, 2014 has been a banner year for hacker attacks on POS. As each month has rolled by, the "body count" has piled up: Michaels, Neiman Marcus, PF Chang and Sally Beauty all reporting compromises to their POS and the loss of cardholder and customer personal information.

Then in August, a deluge. After Homeland Security warned of the Backoff malware that targets POS, there has been a flood of high profile POS compromise revelations. The US Secret Service has reported that at least 1,000 retailers have been compromised by Backoff and that the 7 largest makers of Point-of-Sale systems report having their customer systems infected. Breaches at the UPS Store and 2 of the largest owners of Supermarket chains, Supervalu and AB Acquisition are just a few of the large retailers believed compromised by Backoff.

Even as this Whitepaper goes to publication, more high profile retailers are announcing their POS systems may have been breached. Home Depot appears to be the latest victim. The highly respected blog krebsonsecurity.com reports that banks have been investigating suspicious card usage connected to Home Depot. His sources believe a large number of counterfeit credit cards are already available on the black-market that are connected to a breach of Home Depot POS.

Are you going to be next?

Impact to You and Your Business: Target as a Lesson

The Target data breach provides an example of how severe the impact can be of a compromised POS system. In August, Target revealed that it had spent $148 million dollars in the second quarter, on top of $200 million in the first quarter, in cleaning up the immediate problem, such as cleaning the malware from the network, reissuing cards and offering customer's free identity theft services.

While this is offset by a $38 million insurance policy against such events, this does not include Target's exposure to financial losses incurred by the cardholders and the issuing authorities. Target is currently defending itself against numerous law suits claiming billions of dollars in damages from the POS breach.

In the aftermath of the breach, Target experienced a decline in the stock price and in year over year sales. While it is difficult to correlate, a loss of consumer confidence due to the breach is clearly a concern.

Shortly after the breach was revealed, Target's Chief Information Officer resigned. In May, its Chief Executive Officer stepped down, at least partly due to the fallout from the breach. You can only imagine the impact that this incident and the leadership turmoil have had on the rest of Target's Information Technology and Business organization.

Do you want to be dealing with such a situation?

Why POS is Vulnerable

Most POS systems consist of desktop computer running the Windows operating system and several POS devices directly connected. Windows is a well understood and high profile target for hackers. In too many cases, the POS computer is treated like all other desktops on the operator's network, with the standard endpoint protection of antivirus and personal firewall.

The traditional approach to protecting endpoints focuses on detecting threats. The leaves most end-point security vulnerable to zero day malware, where the threat has not yet been discovered by the vendor and their signature files not yet updated. Malware creators are very good at modifying the files of known malware so that, for a time, they will be undetected as a threat.

BlackPOS, the malware used in the Target Data breach, was "in the wild" at least 3 months before being discovered and most antivirus systems could be updated to deal with it.

According to Verizon's 2014 Data Breach Report, 85% of POS intrusions compromised the target for more than 2 weeks before being detected. By the time the malware is discovered it may be too late.

The Solution

Secure Your Application, Not Just Your Endpoint

The safest assumption for protecting your POS system is to assume that detection *will* fail. Your POS application must be able to operate safely in an already infected environment.

Comodo SecureBox is not endpoint protection.
It is a *fortress* where your POS application can run safely and communicate securely on a compromised machine. Like a medieval castle, It provides safe harbor in an increasingly hostile landscape.

SecureBox converts existing POS computers into truly secure Point-of-sale terminals without requiring expensive new infrastructure and needs virtually no down time for implementation.

Far from being the sophisticated consoles some imagine them to be, Point-of-Sales terminals are essentially regular PCs that happen to have software on them that can handle payments. They are just as vulnerable to the same attack vectors as every other computer.

Unfortunately, as the Home Depot and Target attacks so vividly illustrate, the effects of a successful attack on these machines can adversely affect hundreds of thousands of people. The 'traditional' security measures on these terminals, such as antivirus and firewalls, simply weren't good enough. POS systems need several more layers of proactive security in order to offer adequate protection for customer transactions. Indeed, to bring long-term security to POS machines, we need to fundamentally re-think the way we implement security on them.

SecureBox: The New Paradigm in POS security

Unlike existing security solutions that seek to protect POS software by protecting the host system, Comodo SecureBox assumes the host will always be vulnerable and zealously protects the application itself. Secure inverts the traditional security approaches by running critical applications inside a dedicated, security hardened container which cannot be modified by any other processes which are running. The core containerization technology is augmented with key-logger protection, AV scanning, Memory Scraping protection, remote takeover protection and Anti-SSL sniffing to transform existing POS computers into truly secure Point of Sale platform.

Features

Your Point-of-Sale software is run inside an exclusive, security hardened container that cannot be accessed or modified by any other processes that are running on the computer.

By effectively separating the application from the underlying operating system, root kits and exploits such as those used in the Target attack cannot gain the privileges they require.

This is accomplished with the following features.

- **Data Protection:** Secures mission critical data by protecting your application's data in memory and on disk data. POS data is being protected from malware, fraudsters etc., allowing companies to ensure customers connect to their services in a secure manner
- **Keylogger Protection:** Using keyboard virtualization technology, Comodo SecureBox intercepts keystrokes from the keyboard filter driver and encrypts the information, sending it directly to the target window in a customized message. This process bypasses the entire Windows® input sub-system, ensuring that nothing can capture SecureBox-protected keystrokes.
- **Remote Takeover Protection:** With Comodo's application-agnostic screen capture detection technology, Comodo SecureBox defeats remote desktop takeover by intercepting the attempt and switching from the default screen to an isolated desktop screen that displays warning messages, prohibiting the hacker from viewing anything on a user's desktop.
- **Anti-SSL Sniffing:** Comodo SecureBox detects malicious SSL connections and SSL sniffing by intercepting and verifying certificates using Comodo's trusted root certificate list, effectively preventing Man-in-the-Middle attacks. Note: This feature is critical for other types of applications that users access from mobile devices outside the organizations network. However, POS systems may also be vulnerable to Man-in-the-Middle attacks
- **Anti-Memory Scrapping:** Comodo SecureBox prevents memory scraping by prohibiting external applications from accessing the memory of containerized applications.
- **Active Virus Removal:** Before the application opens, Comodo SecureBox performs a rapid cloud-based scan to detect and terminate all active viruses on the host device. The results of the virus scan are sent to Enterprise administrators for robust reporting purposes.

Who Should Use SecureBox?

Although this Whitepaper specifically addresses the needs of POS, SecureBox can secure any application that requires maximum protection. In fact, SecureBox is custom built for your unique security needs and can be specifically tailored for your end users, regardless of the type of industry you're in or the services you offer.

We recommend Secure Box for...

Banking and Finance Institutions

Provide highly secure interactions between you and your employees or customers, reducing the risk of financial liability to cover monetary losses due to fraud.

Point-of-Sale (POS) Systems

Protect credit card information by securing POS systems for retailers, food service companies, healthcare organizations, hotels, etc.

ATM Machines

Prevent ATM machines from being compromised or hacked by securing the application at the operating system level.

Government Agencies

Prevent leakage of highly sensitive data by securing important applications used by government employees and agents.

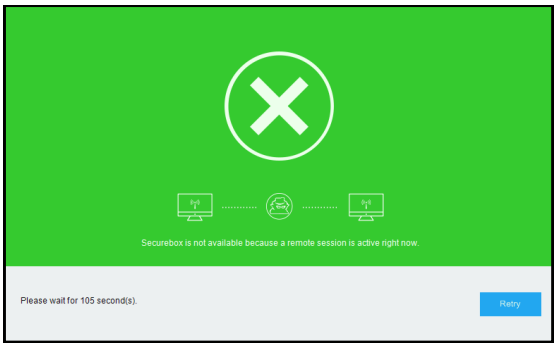
Enterprises

Secure corporate activity on managed and unmanaged desktops to support BYOD and remote work spaces.

Details

Remote Takeover Protection

Hackers use popular remote control software, intended for legitimate purposes, to take control of a target's computer and perform nefarious actions.

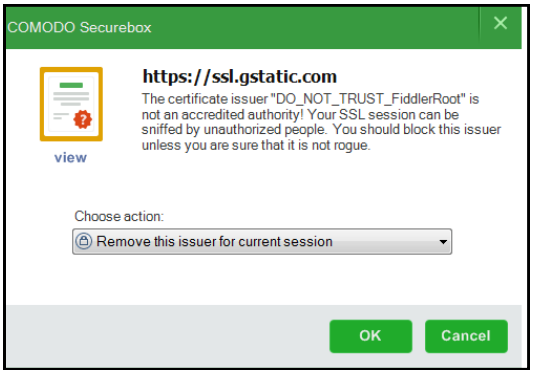


How does SecureBox solve this problem?
When remote takeover is detected, SecureBox blocks the attempt by switching to another desktop that displays warning messages.

Hackers cannot view the user's actions on their screen. User's see the warning displayed and cannot continue to use the application until the remote session has ended (e.g. the hacker ceases the attempt or the user disables the remote sharing tools.

Anti-SSL Sniffing

Malware and fraudsters use certificate root poisoning techniques for "man-in-the-middle" attacks. Browsing form machines not under your control leaves you vulnerable to this threat.



An attacker can break into the SSL connection of a legitimate server and present an invalid certificate to the end user, and if the end user accepts it, then all bets are off and the exfiltration of sensitive data may begin.

How does SecureBox solve this problem?
SecureBox detects malicious SSL connections and SSL sniffing by intercepting and verifying certificates using Comodo's trusted root certificate list, effectively preventing man-in-the middle attacks.

Anti-SSL sniffing is especially important if employees and/or customers are accessing sensitive data while in a café, park, or airport, where the Internet connection is typically unsecured.to another desktop that displays warning messages. Hackers cannot view the user's actions on their screen. Users see the warning displayed and cannot continue to use the application until the remote session has ended (e.g. the hacker ceases the attempt, or the user disables the remote sharing tool.

Anti-Memory Scraping

Memory-scraping malware is typically designed to track data including a cardholder's name, card number, expiration date, and the card's three-digit security code at the place where it's most vulnerable to being intercepted: in memory, where it is in plaintext format.

How does SecureBox solve this problem?
SecureBox prevents memory scraping by prohibiting external applications from accessing the memory of containerized applications.

Anti-Keylogging

Hackers today don't write nuisance viruses to corrupt systems, they write keyloggers that silently capture your keystrokes. It's far more lucrative and less risky. Even worse, eighty percent of all keyloggers are not detectable by antivirus/antispyware software or firewalls.

How does SecureBox solve this problem?
Using keyboard virtualization technology, Comodo SecureBox does intercepts keystrokes from the keyboard filter driver and encrypts the information, sending it directly to the target window in a customized message.

This process bypasses the entire Windows® input subsystem, thus, neither hooks nor monitors in the system input delivery path can capture SecureBox-protected keystrokes.

Benefits

Custom built company-branded application for your unique security needs, specifically tailored for your end users

- A controlled, non-modifiable environment in which users cannot manually introduce other applications, nor can they access websites other than your own, avoiding potential malware.
- Decrease victims of cybercrime when using your company application
- Deeper level of security (complementary to existing solutions) to secure mission critical data in-transit
- Rapid deployment of user-friendly, light software
- Elimination of malware while communicating and transacting online

Getting SecureBox

Learn more about SecureBox or try 30 days with up to 5,000 users for free at *http://securebox.comodo.com/*

If you have a business inquiry and would like to speak directly with a sales representative about Comodo products and services, please contact us at:

Tel: US +U.S. +1-888-256-2608
UK & Europe +44(0)-161-874-7070
International +1-703-637-9361
Email: *enterprisesolutions@comodo.com*

About Comodo

Comodo is a leading provider of trust-based, Internet security products for organizations of every size. Comodo's offerings range from SSL certificates and antivirus software to endpoint security, mobile device management, and PCI compliance. Clients utilizing Comodo security products include Morgan Stanley, Comcast, Sears, Time Warner, and Merck among others.

Comodo Group Inc.
1255 Broad Street
Clifton, NJ 07013
United States
+1 (888) 256 2608

Comodo CA Limited
3rd Floor, 26 Office Village, Exchange Quay,
Trafford Road, Salford, Manchester M5 3EQ,
United Kingdom
Tel: +44 (0) 161 874 7070