COMODO

Whitepaper

October 27, 2014

Malware Threatens ATMs

A new layer of protection for ATMs is required

SECURE BOX

COMODO ENTERPRISE™

The ATM Myth

It is a commonly held myth that ATM machines are not vulnerable to the type of malware infections that plague other endpoint systems because they are more isolated from their network and end user interactions. While this makes them more difficult to infect, there is ample evidence that determined criminals are able to overcome these obstacles.

ATM Malware Breaches

In 2013, the researchers at the annual Chaos Computing Congress in Hamberg reported that hackers were able to infect cash machines at an unnamed bank by cutting a hole in the machine and transferring malware from a USB into the system. The hackers covered their tracks by patching the holes and the banks only learned of the breach when they discovered that the machines had been emptied of cash.

The software the hackers used did not rely on identifying any specific customer account or account information. It identified the quantities of the various currency denominations and allowed the criminals to simply withdraw the currency by denomination.

In March 2014, malware that targets ATM Machines dubbed Ploutus was identified. Because the hackers need to physically access the machine, it is has been seen primarily on standalone ATM machines, such as found at retail stores. Ploutus allows the hackers to control the machine and withdraw an unlimited amount of cash. A recent version of the malware allows the hackers to control it remotely using text messages. This requires the hackers setting up a mobile phone within the machine.

Not all malware found infecting ATMs requires physical access to the machine. Some get into the machine through vulnerabilities in the institutions network security to deposit the malware on the endpoint itself. In 2013, the malware called "Dump Memory Grabber" was identified as infecting POS and ATMS stealing credit card data. The malware is able to scan the memory of ATMs to obtain the card data

According to the security firm Group-IB the malware may have been use to steal card data at major US banks, including Chase, Capitol One and Citibank. It may be small comfort, but Group-IB believes that "Dump Memory Grabber" was being spread by "insiders" who had authorized access to the targeted endpoints.

How are ATMs Vulnerable?

While organizations attempt to isolate them from their network and limit access via a user interface, an ATM is simply an endpoint computer that is not much different than your common desktop. In fact, most ATMs use the Windows operating system that is the favorite target platform of hackers and fraudster.

When Microsoft discontinued security updates for Windows XP in April of this year, most ATMs were still using the venerable OS first introduced in 2001. Unsupporte operating systems are a prime target for hackers.

No matter how secure you think your ATM is, hackers have proven that they can defeat any conventional approach. As the examples on the prior page indicate, hackers can infect your ATM with malware by:

- Compromising Network Security
- Enlisting conspirators inside your organization
- Physically compromising the machine.

The SecureBox Solution

Secure Your ATM Software, Not Just Your ATM Machine

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

Comodo SecureBox is not endpoint protection. It is a *fortress* where your application software can run safely and communicate securely on a compromised machine.

Like a medieval castle, it provides safe harbor in an increasingly hostile landscape.

Features

The ATM application 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 subsystem, 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.
- **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 Financial Transactions, 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.

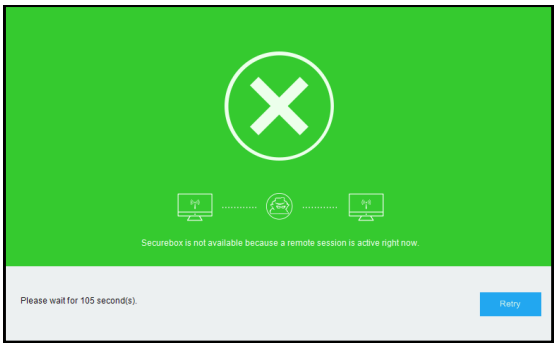
Enterprises

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.

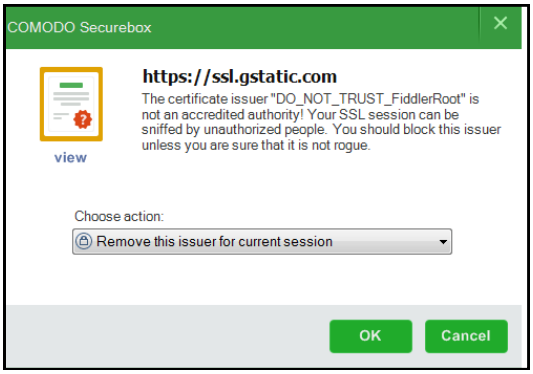


How does SecureBox solve this problem?
When remote takeover is detected, SecureBox blocks the attempt by switching to another desktop that displays warning messages.

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