COMODO

Whitepaper

September 9, 2014

Unsecure Endpoints Threaten Financial Transactions

Secure Your Application Not Just Your Endpoint

SECURE BOX

COMODO ENTERPRISE™

Scenario

A financial institution provides a web site where employees, customer's or other third parties can login and perform financial transactions.

Problem

A user attempts to perform a financial transaction on a web site using a computer that has already been compromised, where hackers can establish a remote session and use key logger and screen capture software.

The user is about to be the victim of financial fraud.

Why is the Endpoint Vulnerable?

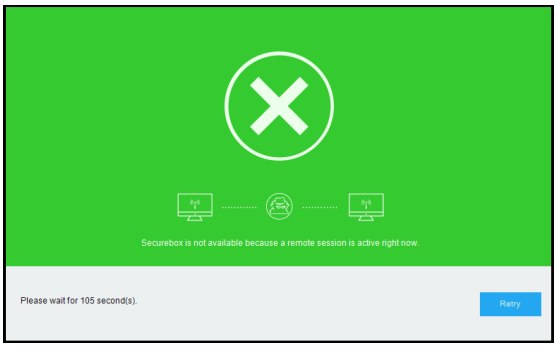
Most endpoints are desktop computer running the Windows operating system. Windows is a well understood and high profile target for hackers. Increasingly, financial institutions allow employees and customers to perform transaction on computers outside the network, including user owned device. The computer may not even have the standard endpoint protection of antivirus and personal firewall.

The traditional approach to protecting endpoints focuses on detecting threats. The leaves most endpoint 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.

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.

Solution:

Require users to connect using Comodo SecureBox. With patent pending technology, SecureBox provides a contained environment where keylogging will be disabled and the form capture will be blocked. Hackers with a remote session will only see the message shown to the right, and can go no further!



How does Comodo SecureBox do it?

The Comodo SecureBox does the following to protect the user:

1. Performs a rapid cloud scanning to detect all running viruses and terminate them.
2. Creates a secure container that the browser will run safely in.
3. Defeats key loggers using keyboard virtualization technology.
4. Defeats remote desktop management tools using Comodo's patent pending application agnostic screen capturing detection technology.

Example: Defeating a Banking Trojan

The following is a typical scenario that the Comodo SecureBox is designed to address:

Part 1—In a World Without SecureBox

A computer user is the victim of a drive by download that infects their computer with a Trojan virus designed for financial fraud. For example, a variant of the infamous Zeus banking trojan. This often occurs when the victim clicks on a link in a phishing email, sent by hackers but appearing to be from a familiar source.

The Trojan is then downloaded to the user's computer and it launches a "Man-the-Browser" (MitB) attack. The Trojan uses common browser features such as Internet Explorer's Browser Helper Objects, browser extensions and JavaScript plus key logger and screen capture programs it install on the user's computer.

- The key logger program allows hackers to capture the user's key strokes. The hacker's know what urls the user visits and capture their login credentials at secure sites
- The screen capture allows the hackers to see what displays on the user's monitor and know exactly what they are doing.

The hackers are sent the information required to create a remote session and they establish a remote connection. They often use software designed for legitimate purposes, such as for remote support and collaboration.

Our user goes to their online banking site to perform a transaction such as transferring funds. The user sees everything as occurring normally, with the payment information they keyed displayed. However, behind the scenes the hackers alter the transaction and send it to another account with possibly a larger amount. The hackers work with "Money Mules" who establish bank accounts with false credentials and receive a commission for handling ill-gotten gains.

Our computer user is now a victim of financial fraud and your business is disrupted.

Part 2 - Comodo SecureBox Authors a Happier Ending

In an alternate universe our computer user, the hacker's target, is using the Comodo SecureBox. Here, this story will have a very different ending. When the remote connection is detected the browser will run in a secured, contained environment. The key logger program will be disabled and the form capture program will be blocked.

The user can visit their banking site in privacy and perform any financial transaction safely. The hacker's attack has been contained.

Our computer user is not a victim and your business is unaffected!

Why Endpoints are Vulnerable

Most endpoints for financial transactions consist of a desktop computer running the Windows operating system. Windows is a well understood and high profile target for hackers. The 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 endpoint 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.

The APT Challenge

Hackers are increasingly using techniques developed by govenments for cyber espionage known as Advanced Persistant Threats (APT). Most APTs use widely understood and available techniques such as Brute Force hacking, Phishing and SQL Injection to obtain access to networks and confidential data.

Of particular concern is the vulnerability of most email systems to phishing, where users are tricked into opening malicious email and downloading malware. According to the 2013 Verizon Data Breach Report, "Most organizations do a poor job of protecting their email systems from email phishing.

Email phishing is a good example of how APTs are similar to but very different from other types of attacks. Spammers use phishing, but cast a very wide net, pun intended. They obtain emails from a variety of sources and send out their spam everywhere with little or no thought about the recipients.

APTs differ in that they target an organization and areas of that organization. They look for specific individuals in that organization who, if compromised, can best be used to advance the goals of the attack. This requires more patience and, as the name implies, persistence than other hackers.

Hackers will compromise email address books to send out malicious email. Most people are not fooled because the messages are very generic and they can tell it did not come from the supposed sender. However, because the hackers send out so many messages it takes only a small percentage of people being fooled to make the effort worth while.

If this was an APT, however, the hackers would go to great lengths to make the subject and message appear plausible. They would analyze your address book information and use any other information they can obtain about you and your organization. For example, if you receive a message from someone you know in your department instructing you sign up for a tradeshow that your company is actually participating in, you could well be fooled into clicking on the link they provide.

And, unlike the common hacker, this is not a one shot attempt. If the tradeshow ruse doesn't work they might identify the high school or college you went to and use that in their next email. They will come back again and again to you or other people in you organization until someone makes the mistake to click on a malicious link.

Targeted phishing is referred to as "spear phishing" because they are aimed at a target. The most high profile example was the compromise of a White House email system by Chinese hackers in 2012. We were assured that nothing important was compromised, but you have to wonder. Afte all, the emails were for the White House Military Office which is in charge of the President's schedule and the codes he can use to order a nuclear attack!

We don't know what the Chinese hackers were looking for exactly, but the lesson for all of us is that if the White House can be hacked then we are all vulnerable.

The SecureBox Solution

Secure Your Application, Not Just Your Endpoint

The safest assumption for protecting your financial application 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 can run safely and communicate securely on a compromised machine. Like a medieval castle, it provides safe harbor in an increasingly hostile landscape.

Features

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 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.

Who Should Use SecureBox?

Although this Whitepaper specifically addresses the needs of Financial Transctions, 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.

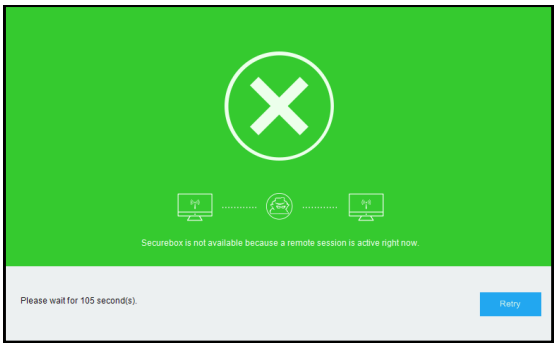
Enterprises

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.

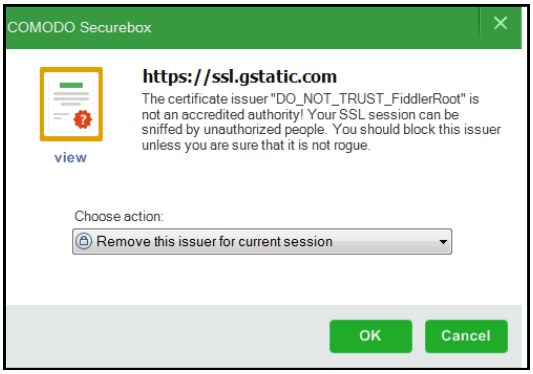


How does SecureBox solve this problem?
When remote takeover is detected, SecureBox blocks the attempt by switching to another desktop that displays warning messages.

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