RANSOMWARE ON THE RISE

An Enterprise Guide to Preventing Ransomware Attacks

CARBON BLACK

Table of Contents

Executive Summary

AN ENTERPRISE GUIDE TO PREVENTING RANSOMWARE ATTACKS

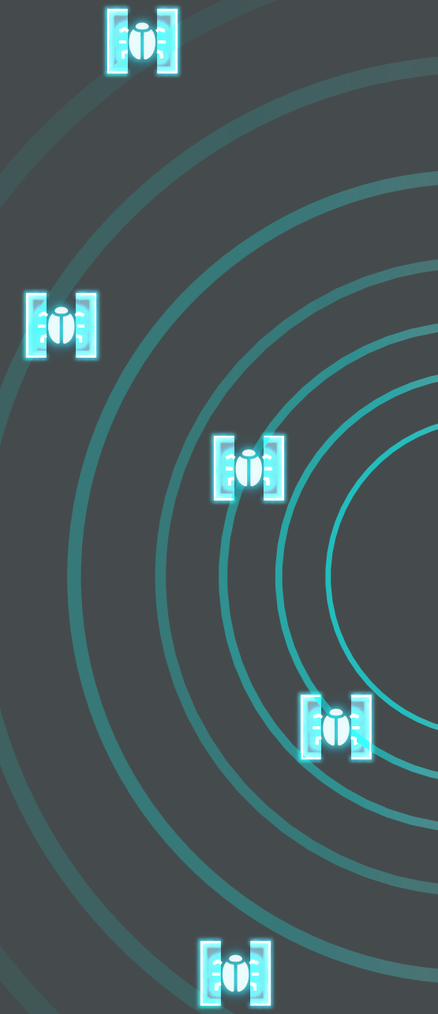
Ransomware isn't new. In fact, it's 30-years-old. What **IS** new is ransomware's sudden rise as a favored attack by cyber criminals. Cyber crime has become a lucrative business and, unfortunately, ransomware has become an integral attack method that many organizations are fighting a losing battle against.

Today's businesses are routinely choosing to pay hefty ransoms rather than lose access to their intellectual property, patient records, credit card information and other valuable business data. Simply put, targeted businesses are paying ransoms in order to avoid significant disruptions to every-day operations.

Ransomware's rise in popularity parallels the development of fileless attack methods that traditional antivirus (AV) simply cannot stop. Cyber criminals are quick learners and eager to make fast money. Whether extorting $300 per user from a small business or $30 million from a multinational enterprise, the level of effort is often similar.

While ransomware isn't going away any time soon (if ever), you **CAN** defend your organization - if you're properly prepared.

In this eBook, we answer the questions: **"What is ransomware?," "How does it work?"** and **"What can I do to better protect my organization?"** We also dive into a recent variant of ransomware - "Locky" - and review case studies from Carbon Black customers that have stopped ransomware in its tracks.



"WHILE RANSOMWARE ISN'T GOING AWAY ANY TIME SOON (IF EVER), **YOU CAN DEFEND YOUR ORGANIZATION** - IF YOU'RE PROPERLY PREPARED."

A Brief History

HISTORY & STATS

Ransomware attacks date back to 1989 and have been the most pervasive cyber threat since 2005, with a dramatic spike in recent years. The resulting costs to targeted businesses are soaring. **In the U.S. alone, victims lost $209 million due to ransomware in the first three months of 2016, compared with $24 million in all of 2015, according to the FBI.**

Two distinct varieties of ransomware have remained consistent in recent years: Crypto- and Locker-based. Crypto-ransomware variants encrypt files and folders, hard drives, etc. Locker-ransomware - most often seen with Android based ransomware - only locks users out of their devices.

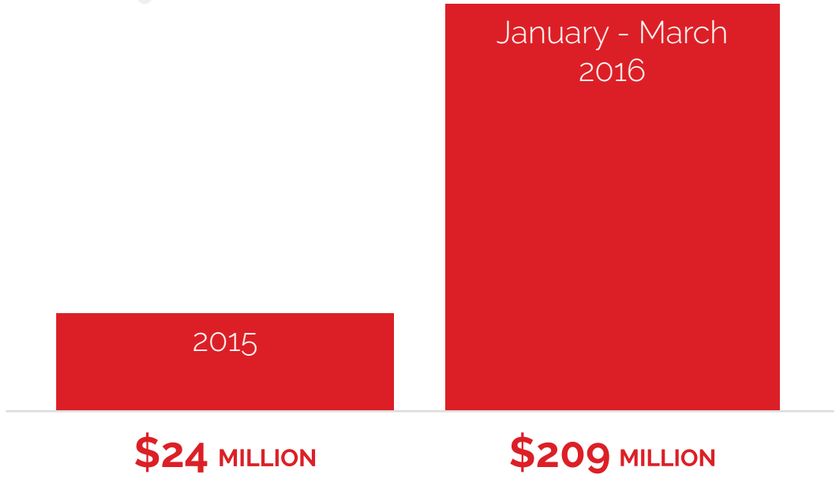
New-age ransomware involves a combination of advanced distribution efforts, such as pre-built infrastructures used to easily and widely distribute new strains, as well as sophisticated development techniques, such as using crypters to ensure reverse-engineering. This combination requires advanced skills on the part of the attacker. But because the ROI is high, attackers are continually investing in these advanced forms of ransomware.

Offline encryption methods are also becoming popular. These attacks exploit legitimate system features, such as Microsoft's CryptoAPI, eliminating the need for Command and Control (C2) communications.

DID YOU KNOW?

- Ransomware is on track to be a $1 billion crime in 2016
- 25+ variants of ransomware families have been identified
- 4,000+ ransomware attacks happened daily since January 1, 2016
- Phishing is the most popular ransomware attack vector
- The top-5 variants in the U.S. are: CryptoWall, CTB-Locker, TeslaCrypt, MSIL/Samas, Locky

> IN THE U.S. ALONE, **VICTIMS LOST $209 MILLION DUE TO RANSOMWARE** IN THE FIRST THREE MONTHS OF 2016, COMPARED WITH $24 MILLION IN ALL OF 2015



Ransomware Timeline

Top 5 ransomware variants in U.S.

1989 — AIDS Trojan
Infected 20k diskettes distributed at AIDS conference; symmetric cryptography; set in motion three decades of ransomware attacks

2005 — Archievus
First ransomware to use asymmetric encryption; encrypted everything in 'My Documents' and required users to make purchases from websites to obtain passwords to decrypt files

2011 — Unnamed Trojan
First ransomware to leverage mainstream adoption of anonymous payment services

2012 — Reveton
Spawned 'police-based' ransomware including Urausy and Tohfy

2013 — CryptoLocker
First cryptographic malware spread by downloads from a compromised website and/or business professionals in the form of email attachments

2014 — CryptoDefense
Used Windows' built-in encryption CryptoAPI's, 2048-bit RSA encryption & Tor/Bitcoin for anonymity

2014 — CryptoWall
New and improved ransomware from creators of CryptoDefense; first to establish persistence by adding registry keys and copying itself to startup folders; netted $325 million for the threat actor

2014 — Sypeng
First Android-based ransomware

2014 — Koler
Considered first 'Lockerworm'

2014 — CTB-Locker
First ransomware to communicate directly with a C2 server in Tor as well as delete Volume Shadow Copies on Windows machines

2014 — SimplLocker
First 'crypto-based' ransomware for Android devices that encrypted files on simply locked phones

2015 — LockerPin
First ransomware able to reset PIN on Android phones; $500 ransom to unlock phone

2015 — TeslaCrypt
First ransomware to allow resiliency and persistence on victim machines

2015 — Chimera
First 'doxing' ransomware that threatened to publish sensitive or private files online

2015 — LowLevel04
First ransomware to be carried out manually by attackers by remoting into servers, mapping internal systems and drives before distributing ransomware; attackers were observed deleting application, security and system logs

2016 — 7ev3n
Demanded the highest ransom thus far, 13 bitcoins; first to destroy Windows systems if ransom not paid

2016 — Ransomware32
First ransomware written in JavaScript; first to work on multiple OS including Linux, Windows and MacOS X

2016 — SamSam (SAMAS)
First to target JBoss servers and include a channel for attackers to communicate in real-time with victims via a .onion website

2016 — Locky
Spread via aggressive phishing campaigns and leveraged Dridex infrastructure; used to target hospitals in Kentucky, California and Kansas; started ransomware-in-healthcare trend

2016 — Petya
Delivered via Dropbox; overwrote Master Boot Record (MBR) of infected machines and encrypted physical drive; ransom doubled if payment not received in seven days

2016 — KeRanger
First MacOS X ransomware; signed with MAC development certificate allowing it to bypass Apple's Gatekeeper security software

2016 — Jigsaw
First to use ransom note containing characters from the movie series "Saw"; deleted files every 60 minutes if ransom not paid; restarting a machine resulted in 1,000 files being deleted

2016 — Maktub
First to use Crypter to hide and encrypt source code of malware

2016 — CyrptXXX
Research suggests CyrptXXX is connected to the Reveton ransomware variant; typically observed after Bedep infections

2016 — PowerWare
A new instance of ransomware utilizing native tools, such as PowerShell on operating systems, discovered by Cb Threat Research team in April; asks PowerShell, a core utility of current Windows systems, to do the dirty work; attempts to avoid writing new files to disk and tries to blend in with legitimate computer activity

2016 — ZCryptor
One of the first 'crypto-worms' that self-propagates to infect external devices and other systems on the network, while also encrypting every machine and shared drive

Source: "The history of ransomware," PC World, July 20, 2016

How Ransomware Works

STAGES OF AN ATTACK

>> *HERE'S AN EXAMPLE OF THE STAGES OF A "LOCKY" ATTACK ORIGINATING FROM A SPEAR-PHISHING EMAIL*

Ransomware is similar to other malware in that it installs itself on a computer and runs in the background without the user's knowledge. But unlike malware that hides and steals valuable information, ransomware doesn't hide. As soon as ransomware has locked a user's machine and/or encrypted files, it notifies the user of its presence to make the ransom demand.

1. End user receives an email that appears to be from their boss. It contains a URL to a SaaS application such as Salesforce, Workday or ZenDesk.
2. The link opens a browser window and directs the user to a website that seems legitimate. It's actually a landing page for an exploit kit hosted in a .co.cc top level domain (TLD).
3. Upon loading the page, the web server hosting the exploit kit begins communicating with the victim machine. The server sends requests about versions of software such as Java to find a vulnerable version for which the kit has an exploit.
4. When a vulnerable version is confirmed, the kit attempts to exploit the vulnerability. Once successful, the exploit kit pushes down a malicious .EXE file - let's call it "ransomware.exe." The malicious binary on the victim machine then attempts to execute.
5. From this beachhead, the binary spawns child processes, including vssadmin.exe (shadow copy), to delete existing shadows on the victim machine and create new ones to hide in. The attacker does this to limit the possible recovery of files by the victim using Shadow Copies that Windows stores on a system.

NOTE: The inclusion of a child process containing Volume Shadow Copy processes is a behavior of a new Locky variant. A diagram and screenshots of this attack and how to detect it are provided in the section below, "Locky Variant - Shadow Copies."

6. The binary also creates a powershell executable to propagate copies of itself throughout the filesystem. The executable also searches the filesystem for files of specific extensions and begins to encrypt those files.
7. The powershell.exe child process creates three copies of the originating malware binary, first in the AppData directory, next in the Start directory, and finally in the root C:\ directory. These copies are used in conjunction with the registry modifications to restart the malware upon reboot and login events.
8. After encrypting the victim's files, the malware sends the encryption key and other host- specific information back to the command-and-control server.
9. The server then sends a message to the victim. This could be a simple "alert user of encryption and directions on paying us." It could also include directions that result in downloading additional malware, which enables the attacker to steal credentials from the victim as well.

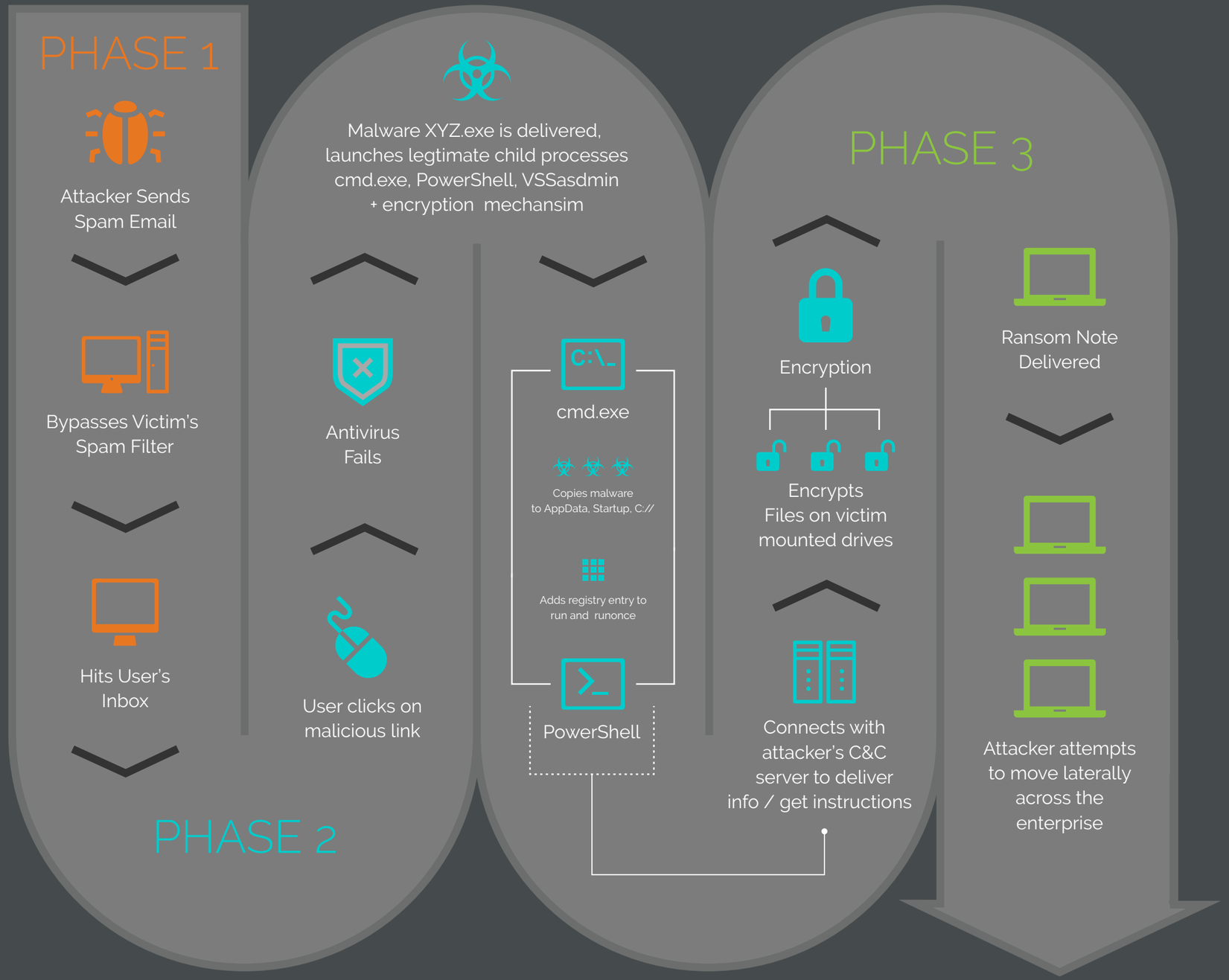
To amplify the victim's distress, ransomware often includes a countdown clock with a deadline for paying the ransom - or else the decrypt key will be destroyed, eliminating any chance of recovery.

Paying the ransom often means the attacker will unlock the victim's machine or provide the key to decrypt files. However, it rarely means the originating malicious binary, "ransomware.exe" in the case above, has been removed. That will require IT and SecOps support.

And the attack doesn't necessarily end there. Attackers often load additional malware on a user's machine, allowing them to harvest personal information, intellectual property, and credentials to sell for additional revenue.

"RANSOMWARE IS ON TRACK TO BE A **$1 BILLION CRIME** IN 2016"

Ransomware Attack Anatomy



Locky Variant - Shadow Copies

DEFEATING LOCKY AND VOLUME SHADOW COPIES

Ransomware is becoming increasingly sophisticated. Comparing today's ransomware to yesterday's malware is like comparing a computer to an abacus. One advanced example is "Locky," a CryptoLocker variant that deletes all "Volume Shadow Copies" to prevent restoring from backup, and then encrypts the files for ransom. This can be a terrible - and *expensive* - headache for unprepared IT and security teams.

Shadow Copy is a Microsoft Windows technology that allows the capture of backup copies (snapshots) of computer files or volumes. Backups can be taken even when the files are in use. It's implemented as a Windows service called the "Volume Shadow Copy Service." Shadow copies can be created on local and external volumes by any Windows component that utilizes it, such as when creating a scheduled Windows backup or automatic system restore point.

Carbon Black has observed various ransomware techniques utilizing volume shadows. Lately, it's been used for avoiding detection and for anti-analysis. A specific attack we've seen consists of the following steps:

1. Attackers drop malware on the filesystem via whatever infection mechanism they choose
2. Create a volume shadow
3. "Mount" the shadow and execute the malware
4. Unmount the shadow and delete it

What's unique about this technique is that even after unmounting and deleting the shadow, the executed malware will still run. On Windows XP, the vssadmin tool isn't able to create persistent shadows. Starting with the Windows Vista SDK, Microsoft supplied a binary called Vshadow to allow this.

FIGURE 1

In the above example, the attackers create a persistent shadow of the full C: drive. This will run for a few seconds and end with the output seen above.

Note the "Shadow copy device name." (\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3) - it will be used to mount the shadow in the attack.

Once the shadow has been created, it must be mounted, which is done using the "mklink" command. In the image below, the attackers create a symbolic link directory in System32 to a directory called "msdc." The symlink directory points to the shadow copy of the C drive created earlier.

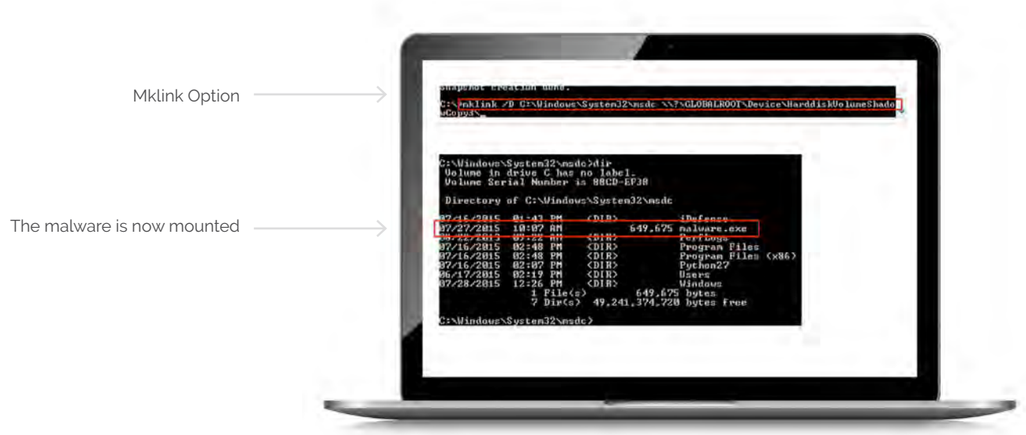


FIGURE 2

The malware is placed at the root of the shadow after it was created. A directory listing of C:\Windows\System32\msdc reveals the malware on the normal filesystem but living inside the shadow filesystem. Once the symlink has been created the contents of the shadow are accessible via normal filesystem operations like the directory listing seen above.

Once the file system setup is in place, the malware is started just like any other executable.

When the malware is started and shown in a tool like process explorer it shows that it is running from C:\Windows\System32\msdc.

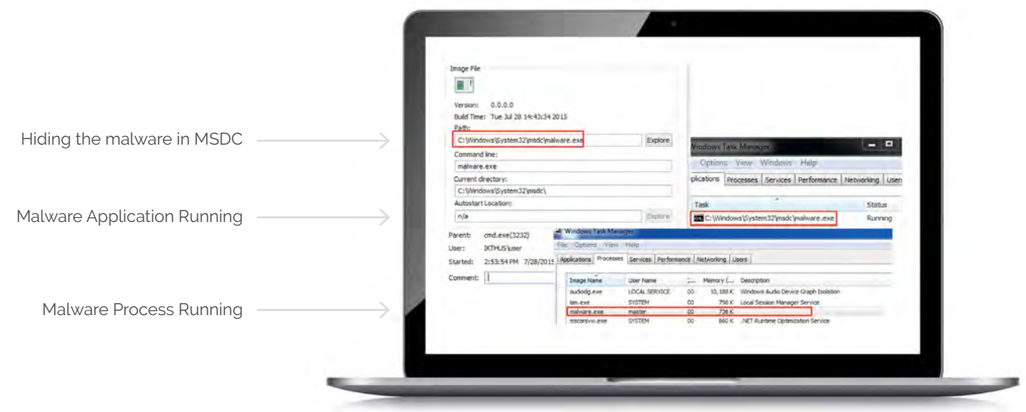


FIGURE 3

At first glance, that path doesn't look too suspicious.

Once the malware is started, the attackers can unmount and delete the shadow and the malware continues to run. To remove as much forensic evidence as possible, the attacker would unmount the directory and delete the shadow with vssadmin.

"4,000+ RANSOMWARE ATTACKS HAPPENED DAILY SINCE JANUARY 1, 2016"

FIGURE 4

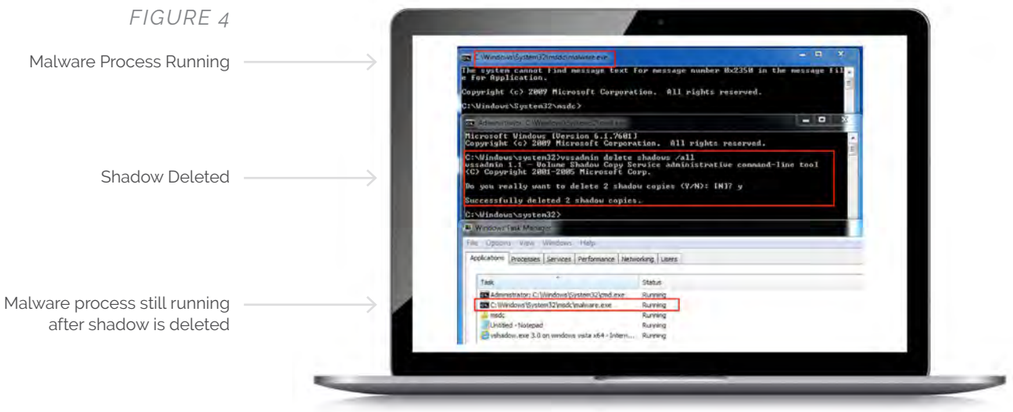


FIGURE 4

This technique is an effective hiding mechanism that throws in a little anti-forensics, demonstrating how ransomware is evolving.

Ransomware can be dangerously effective. Recent additions of features such as removing shadow copies makes it even more dangerous. Visibility is a key requirement for detecting and preventing such ransomware.

Cb Endpoint Security Platform

STOP RANSOMWARE BEFORE IT STARTS WITH CB DEFENSE

Even the most educated end users, well versed in security best practices such as never clicking on email attachments, can become victims of drive-bys and other sophisticated exploit kits that can deliver ransomware.

Traditional, signature-based antivirus can sometimes protect an organization's endpoints from existing, known malware. However, there are new variants of ransomware, such as Locky, as well as advanced attacks that leverage PowerShell, scripts, macros, remote shell attacks and memory-based attacks that AV simply cannot stop. These attacks now make up more than 50 percent of the attacks targeting enterprise organizations. The first step every organization can take is to stop relying on AV solutions to defend their endpoints, servers and critical systems.

Cb Defense is the most powerful next-generation antivirus solution available today. Using a combination of endpoint and cloud-based technologies, Cb Defense stops more attacks, sees more threats, and closes more security gaps, using deep analytics to inspect files and identify malicious behavior. This comprehensive approach blocks traditional malware as well as increasingly common malware-less attacks that exploit memory and scripting languages such as PowerShell.

Cb Defense stops ransomware attacks including the Locky variant explained earlier in this eBook more effectively and efficiently than any other solution available. And it does so at multiple points in the infection workflow for layered defense. First, Cb Defense checks the reputation of all executables and binaries downloaded to an endpoint against the Cb Collective Defense Cloud. The Cb Collective Defense Cloud contains reputation scores on more than 8 billion files, adding approximately 200,000 per day, while also leveraging threat intelligence from more than 20 threat partners to determine good software and binaries from malicious.

If the XYZ.exe is a zero-day and has no reputation score on file, Cb Defense would block the execution of the malicious binary based on behavior. In this example, Cb Defense would recognize the attempt on behalf of the executable to inject code into legitimate running processes or the creation of new child processes from packed memory buffers. Cb Defense is able to detect this infection workflow in part because of its focus on patterns of attack versus simply indicators of compromise. Additionally, in this scenario, Cb Defense would also block the attempt of the executable to 'phone home' to the C+C server.

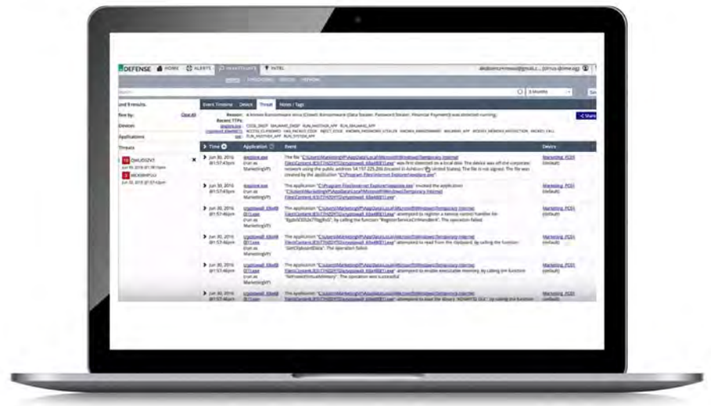


FIGURE 5

Once ransomware is blocked, Cb Defense provides full visibility into how the attack happened. By capturing and analyzing behavior in advance, Cb Defense pinpoints the exploit. Armed with this insight from Cb Defense, IT and SecOps teams can proactively patch the vulnerabilities exploited by the exploit kit. Cb Defense also provides a suite of remediation tools to quarantine machines, blacklist software, and remove unwanted items.

Cb Defense uses a lightweight sensor that installs in less than a minute and consumes less than one percent of the CPU, disk, and network. Once installed, Cb Defense can be completely managed from the cloud through an easy-to-use web-based interface.

CB ENDPOINT SECURITY PLATFORM

Cb Defense is a core component of the Cb Endpoint Security Platform which also including Cb Response and Cb Protection. The Cb Endpoint Security Platform helps organizations of all sizes replace ineffective antivirus, lock down endpoints and critical systems, and arm incident response teams with the most advanced tools to hunt down threats.

Cb Protection provides the most proven application control solution for enterprise endpoints and critical systems. With Cb Protection, IT, compliance, infrastructure, and security teams establish automated software execution controls and protection policies that safeguard corporate and customer data.

Cb Response is the most precise IR and threat hunting solution, allowing you to get the answers you need faster than any other tool. Only Cb Response continuously records and captures all threat activity so you can hunt threats in real time, visualize the complete attack kill chain, and then respond and remediate attacks, quickly.

Case Study Tech Manufacturing

TRACKING DOWN A TESLACRYPT ATTACK

After falling victim to a TeslaCrypt attack that affected 200+ endpoints, a large technology manufacturer needed to remediate the threat and stop future attacks.

ZERO-DAY EXPLOIT EVADES STANDARD ANTIVIRUS (AV)

In the fall of 2015, 300+ employees at this technology manufacturer received an email with a malicious PDF attachment. The phishing email was so deceiving that even security-savvy employees opened the attachment. Although the organization had standard antivirus to scan all executables, the zero-day exploit went undetected. After the file had executed on employees' computers, it began withholding files and instantly stopped business operations.

IDENTIFYING THE ROOT CAUSE OF THE ATTACK WITH CB RESPONSE

The manufacturing firm urgently needed visibility and protection. After quickly implementing Cb Response, the organization's security team was able to unravel the entire attack, discovering that the PDF file made an http call to download two files: one.exe and 76.exe.

FUTURE ATTACKS BLOCKED USING CB PROTECTION: ZERO BREACHES

Leveraging Cb Response's visibility into the executables, the team then deployed Cb Protection to block future execution. After the ban, more employees received the email, but Cb Protection blocked the attack. The company moved all their endpoints into "High Enforcement" for the highest level of protection.

THE SENIOR DIRECTOR OF IT SECURITY SAID, "THE REAL GODSEND HERE WAS CB RESPONSE."

Without Cb Response the organization would not have been able to visualize the attack kill chain, or respond and remediate with the speed and ease that they did. Since implementing Cb Protection, the company has seen zero breaches.

Case Study Oil & Gas

TAKING PREEMPTIVE ACTION AGAINST RANSOMWARE

A well-known oil and gas manufacturer needed to protect its servers and workstations from ransomware attacks. After implementing Cb Protection, the company was able to free up internal resources and block 13 times more security threats per week than other solutions.

GETTING AHEAD OF THE RANSOMWARE THREAT

After a number of other oil and gas companies were hit by ransomware attacks, the company wanted to improve its security posture before it was too late. The security team was looking for a solution that could be applied at scale and would provide the highest level of endpoint protection against ransomware.

STOPPING 13 TIMES MORE THREATS THAN TRADITIONAL AV

The company tested Cb Protection against two traditional security solutions and saw instant value. In the test, Cb Protection stopped 13 times as many threats as traditional AV products. Not long after implementation, the organization had 240 machines targeted by ransomware. Carbon Black protected all 240 machines from the ransomware attack. All devices that weren't running Cb Protection were crippled and the hardware had to be replaced, costing the company a significant amount of money. As a result, the organization recognized it needed to deploy Cb Protection across all systems.

ADDED BENEFITS: COMPLIANCE AND REDUCED RE-IMAGING

The company realized additional value from Carbon Black. Critical Security Control 2.2 had to be met and, as a result of utilizing Carbon Black, the compliance standard was met. The company has also seen a massive reduction in re-imaging machines. In the past, it had to re-image 75-275 machines per month. With Carbon Black, that's down to zero. Since implementing Carbon Black, the company has seen zero breaches, freed up internal resources, and saved significant money.

Ransomware Defense Cheat Sheet

DEFENSE IN DEPTH: 14 KEYS TO PROTECTING AGAINST RANSOMWARE

Ransomware infections can be devastating and recovery efforts threaten to financially cripple an organization. Prevention is the most effective defense. Deploying a next-generation endpoint security product like Cb Defense that can detect and stop ransomware attacks is an obvious first step. Here are 14 additional best practices recommended by the U.S. government and other experts to combat ransomware:

1. **Back up data regularly.** Verify the integrity of those backups and test the restoration process to ensure it's working.

2. **Secure your offline backups.** Backups are essential: if you're infected, a backup may be the only way to recover your data. Ensure backups are not connected permanently to the computers and networks they are backing up.

3. **Configure firewalls** to block access to known malicious IP addresses.

4. **Logically separate networks.** This will help prevent the spread of malware. If every user and server is on the same network newer variants can spread.

5. **Patch operating systems, software, and firmware on devices.** Consider using a centralized patch-management system.

6. **Implement an awareness and training program.** End users are targets, so everyone in your organization needs to be aware of the threat of ransomware and how it's delivered.

7. **Scan all incoming and outgoing emails** to detect threats and filter executable files from reaching end users.

8. **Enable strong spam filters to prevent phishing emails** from reaching end users and authenticate inbound email using technologies such as Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent spoofing.

9. **Block ads.** Ransomware is often distributed through malicious ads served when visiting certain sites. Blocking ads or preventing users from accessing certain sites can reduce that risk.

10. **Use the principle of "least privilege" to manage accounts:** No users should be assigned administrative access unless absolutely needed. If a user only needs to read specific files, the user should not have write access to them.

11. **Leverage next-generation anti-virus technology** to inspect files and identify malicious behavior to block malware and malware-less attacks that exploit memory and scripting languages like PowerShell.

12. **Use application whitelisting,** which only allows systems to execute programs known and permitted by security policy.

13. **Categorize data based on organizational value** and implement physical and logical separation of networks and data for different organizational units.

14. **Conduct an annual penetration test** and vulnerability assessment.

Conclusion

DEFENSE IN DEPTH IS THE BEST SOLUTION

Ransomware is here, and it's not going away. Criminals are making money at an alarming rate with little resistance. There have been more ransomware variants in the last 18 months than all of the 29 previous years. By using ransomware, cyber criminals have had a free run at organizations' critical data. It's time to stem the tide, now.

Stopping ransomware requires a defense-in-depth approach; there is no silver bullet to security. Software alone is not the answer. IT and SecOps teams must build a strategy that combines user training, next-generation endpoint security, and backup operations.

Every strategy should start with the simplest, most immediate risk-mitigation techniques available in order to limit the attack surface, such as next-generation anti-virus and strong spam filtering. Concurrently, user training and backup infrastructures should be evaluated, implemented, and practiced.

Cb Defense is the most effective and easy-to-use next-generation anti-virus solution available - and the only one proven to stop ransomware variants, such as "Locky."

To learn more about Cb Defense, register for a private solution demonstration, or speak with a Cb Solution Architect, visit: carbonblack.com/ransomwareprotection.

CARBON
BLACK

1100 Winter Street, Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499

www.carbonblack.com

ABOUT CARBON BLACK

Carbon Black has designed the most complete next-gen endpoint security platform, enabling organizations to stop the most attacks, see every threat, close security gaps, and evolve their defenses. The Cb Endpoint Security Platform helps organizations of all sizes replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats. Today, Carbon Black has approximately 2,000 worldwide customers, including 25 of the Fortune 100 and more than 600 employees. Carbon Black was voted Best Endpoint Protection by security professionals in the SANS Institute's Best of 2015 Awards.