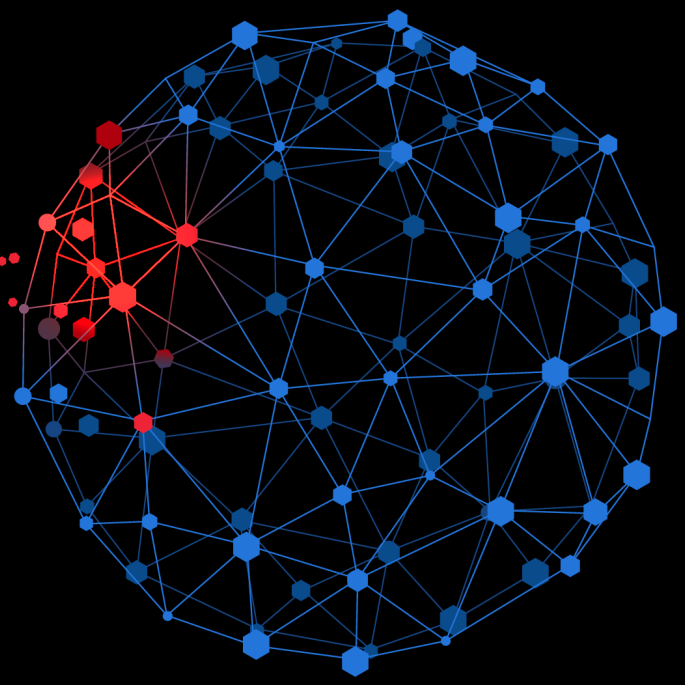
Carbon Black.

Future-Proof Your Ransomware Defenses



An Enterprise Guide to Hardening Your Endpoints Against Future Ransomware Attacks

Table of Contents

Executive Summary 3

An Enterprise Guide to Future-Proofing Ransomware Defenses

History of Ransomware 5

A Brief History, Stats and Timeline

How Ransomware Works 11

Stages of an Attack

Ransomware Attack Anatomy 13

Locky Variant - Shadow Copies 15

Defeating Locky and Volume Shadow Copies

Future-Proof Your Ransomware Defenses 19

Ransomware Defense Cheat Sheet 21

Defense In Depth: 14 Keys to Protecting Against Ransomware

Case Study - Financial Services 23

Taking Preemptive Action Against Ransomware

Conclusion 24

The Future of Next Generation Ransomware Prevention

Executive Summary

AN ENTERPRISE GUIDE TO FUTURE-PROOFING RANSOMWARE DEFENSES

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.

Ransomware attackers are implementing new, innovative techniques that employ unknown binaries and non-malware tactics to evade and bypass traditional defenses. Their encryption techniques go beyond simple files and shares to make it even harder to restore using backups. And their primary targets are increasingly becoming organizations (not just individuals), with much more to lose (and more money to payout).

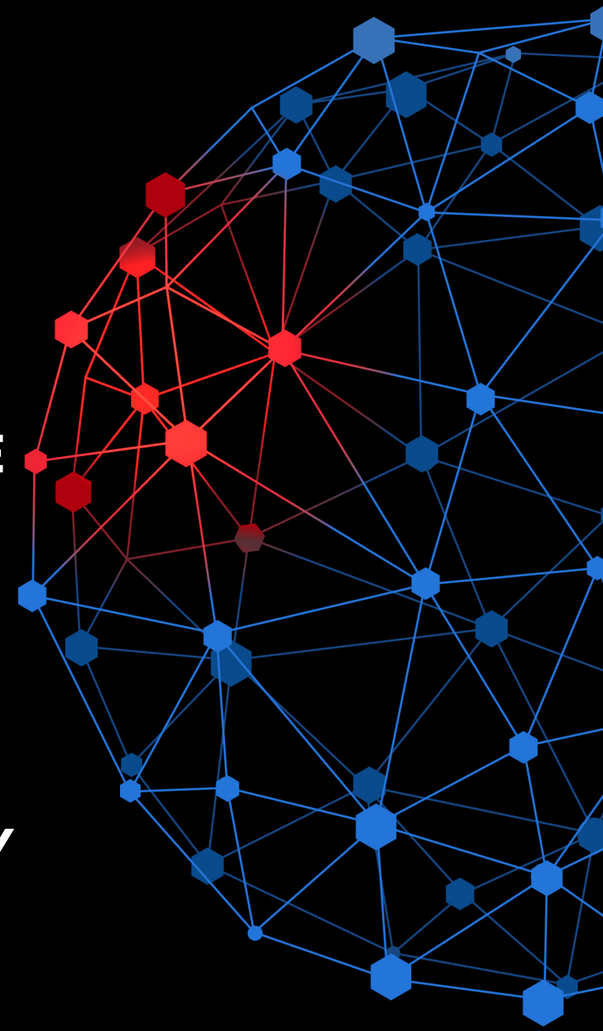
As a result, today's businesses are routinely choosing to pay hefty ransoms rather than lose access to their intellectual property, patient records, credit card information and other valuable business data. Simply put, targeted businesses are paying ransoms in order to avoid significant disruptions to normal 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 fact, according to the 2017 Verizon Data Breach and Incident Report, ransomware has moved from the 22nd most common variety of malware in 2014 to the fifth most common.**

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.

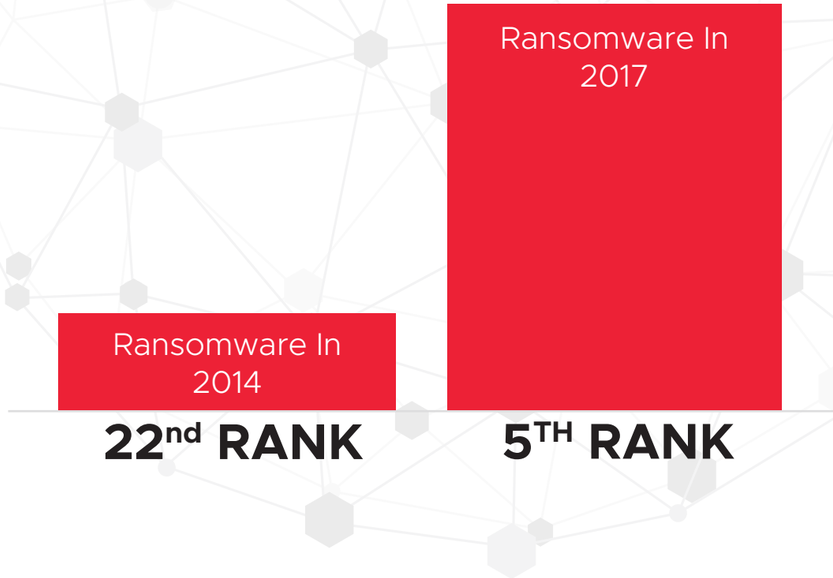
New-age ransomware involves a combination of advanced distribution efforts, such as pre-built infrastructures used to easily and widely distribute new strains, as well as sophisticated development techniques, such as using crypters to ensure reverse-engineering. This combination requires advanced skills 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?

+ 180+ variants of ransomware families have been identified
+ More than 4,000 ransomware attacks happen daily
+ 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 2016, ransomware accounted for 72% of malware incidents in the healthcare industry

ACCORDING TO THE VERIZON DBIR, RANSOMWARE HAS MOVED FROM THE 22ND MOST COMMON VARIETY OF MALWARE IN 2014 TO THE 5TH MOST COMMON IN 2017



THE HISTORY OF RANSOMWARE
1989-2015

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 CryptoAPIs, 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

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

THE HISTORY OF RANSOMWARE
2016-PRESENT

Ransomware32

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

Locky

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

KeRanger

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

Maktub

First to use Crypter to hide and encrypt source code of malware

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

Philadelphia

Very user friendly ransomware-as-a-service released in September but not seen widely until months later

WannaCry

Cryptoworm that used NSA-leaked EternalBlue SMB exploit to infect 23,0000 Windows endpoints in 150+ countries

SambaCry

Continued the trend of using NSA tools to mine cryptocurrency and ransom machines running Linux

2016 2016 2016 2016 2016 2016 2016 2016 2016 2016 2016 2016 2017 2017 2017 2017

7ev3n

Demanded the highest ransom thus far, 13 bitcoins; first to date, to destroy Windows systems if ransom not paid

SamSam (SAMAS)

First to target JBoss servers and include a channel for attackers to communicate in real-time with victims via a .onion website

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

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

CyrptXXX

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

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

Adylkuzz

Leveraged EternalBlue exploit, but focused on mining cryptocurrency instead of demanding ransom

NotPetya

Cyber weapon disguised as Petya that used EternalBlue and Mimikatz to quickly spread from hijacked Ukranian tax software

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

How Ransomware Works

STAGES OF AN ATTACK

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.

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

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."

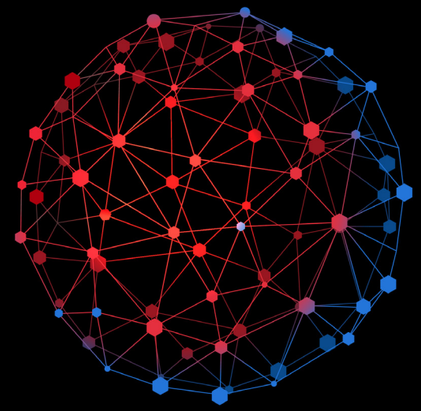
6. The binary also creates a PowerShell executable to propagate copies of itself throughout the filesystem. The executable also searches the filesystem for files of specific extensions and begins to encrypt those files.
7. The powershell.exe child process creates three copies of the originating malware 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 WAS A $1 BILLION CRIME IN 2016



RANSOMWARE ATTACK ANATOMY

PHASE 1

Attacker Sends Spam Email

Bypasses Victim's Spam Filter

Hits User's Inbox

User clicks on malicious link

Antivirus Fails

Malware XYZ.exe is delivered, launches legtimate child processes cmd.exe, PowerShell, VSSasdmin + encryption mechansim

cmd.exe

Copies malware to AppData, Startup, C://

Adds registry entry to run and runonce

PowerShell

PHASE 2

PHASE 3

Encryption

Encrypts Files on victim mounted drives

Connects with attacker's C&C server to deliver info / get instructions

Ransom Note Delivered

Attacker attempts to move laterally across the enterprise

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:

+ Attackers drop malware on the filesystem via whatever infection mechanism they choose
+ Create a volume shadow
+ "Mount" the shadow and execute the malware
+ 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.

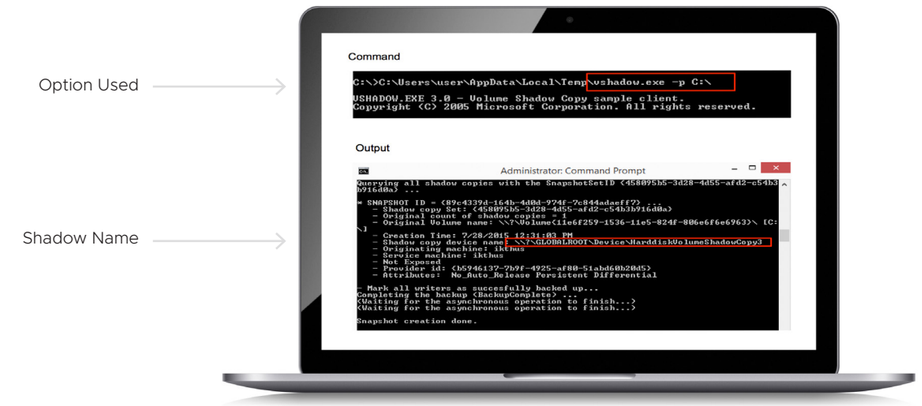


FIGURE 1

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.

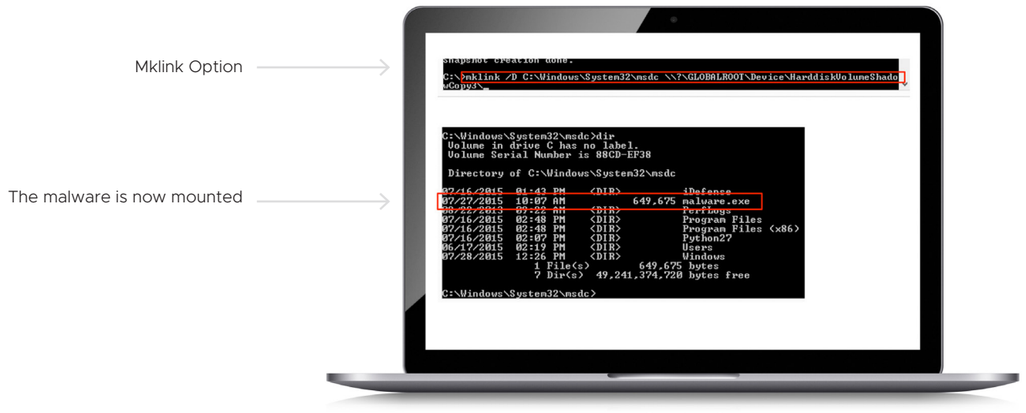


FIGURE 2

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.

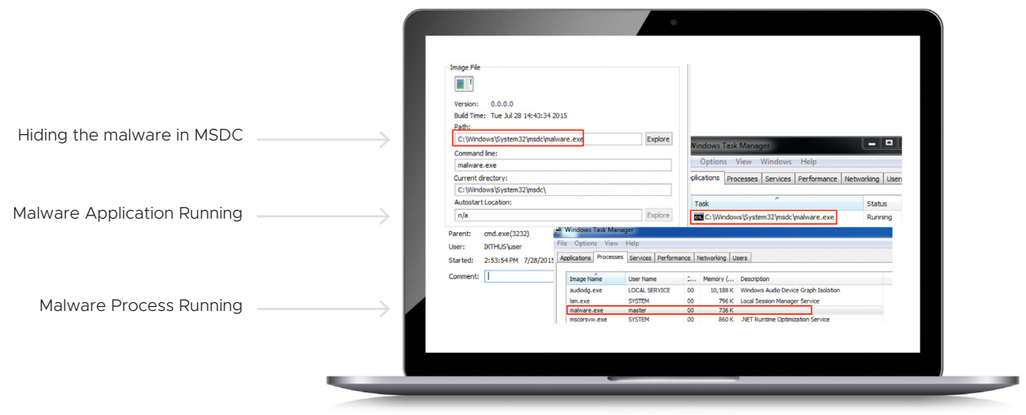


FIGURE 3

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 HAPPEN DAILY
SINCE JANUARY 1, 2016

FIGURE 4

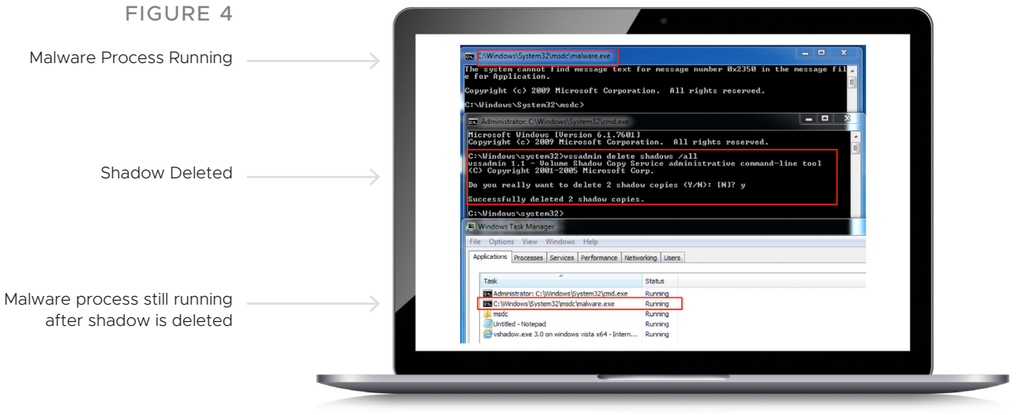


FIGURE 4

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.

Future-Proof Your Ransomware Defenses

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 Carbon Black's breakthrough streaming prevention technology, Cb Defense stops malware and non-malware attacks, using deep analytics to inspect files, connect the dots between events, 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.

DETECT ADVANCED RANSOMWARE EVENT STREAMS

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.

Ransomware itself has evolved in recent years to incorporate some of its own unique behaviors that make its encryption and extortion efforts more effective. To combat this, Cb Defense employs a number of innovative techniques to prevent and disrupt them. To prevent ransomware from destroying backups, a new ransomware technique designed to increase the likelihood of a payout, Cb Defense monitors access and modification attempts to shadow copies and master boot records. In addition, Cb Defense uses "canary files," benign files that sit on the endpoint, as well as other file heuristics to lure evasive and stealthy ransomware variants into a trap that exposes them, allowing active prevention to take over.

BLOCK RANSOMWARE EVEN IF IT'S NEVER BEEN SEEN BEFORE

What makes this approach especially powerful is the fact that it catches ransomware before reputation ever needs to be checked. This means that even if the endpoint is offline and unable to check cloud-based reputation, the stream of events would be detected and automatically blocked by the Cb Defense agent.

However, when connected 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.

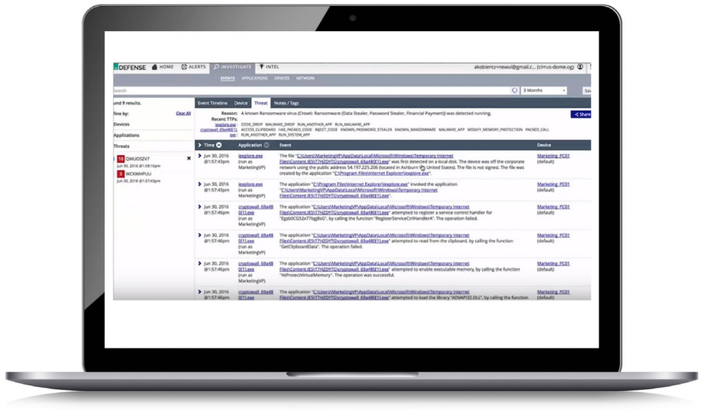


FIGURE 5

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.

Ransomware Defense Cheat

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.

Case Study: Financial Services

TAKING PREEMPTIVE ACTION AGAINST RANSOMWARE

A well-known financial services company needed to protect its servers and workstations from emerging attacks, especially ransomware. Once they realized that traditional antivirus was unsuited for the job, they found Cb Defense was able to give them the insight and protection they need.

GETTING AHEAD OF THE RANSOMWARE THREAT

As new instances of ransomware began popping up throughout their company's environment, it became apparent that a new solution was needed to protect endpoints. Though the instances were isolated, those employees that were affected saw considerable downtime, which impacted their ability to do their jobs.

THE SEARCH FOR A MORE EFFECTIVE PLATFORM

The security team recognized that a small problem today would quickly escalate out of their control if not properly managed. The first step was an internal review of existing security platforms to see if they could be tuned or reconfigured to combat this growing threat. They soon realized that what they had, including their traditional antivirus platform, was just not effective. This initiated an extended search to look into next-generation platforms that could stand up to unknown and evasive variants

INSIGHT AND ADVANCED PREVENTION ARE ESSENTIAL

The security team realized there were two requirements if they were going to effectively combat ransomware - increased insight into advanced techniques, and a powerful prevention engine that could keep threats at bay. Cb Defense proved to be the only platform that could meet both requirements. Because ransomware is constantly evolving, signature-based approaches cannot stop them from infecting machines and causing damage.

ADDED BENEFITS: VISIBILITY INTO ENDPOINT ACTIVITIES

An added benefit with Cb Defense is more visibility into endpoint activities and behavior. Cb Defense can provide process-level visibility at the endpoint, offering an extended view that helped them understand where potential threats were forming before they were able to execute.

Conclusion

THE FUTURE OF NEXT GENERATION RANSOMWARE PREVENTION

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.

In addition, ransomware variants are implementing new, innovative techniques that employ unknown binaries and non-malware tactics to evade and bypass traditional defenses. Their encryption techniques go beyond simple files and shares to make it even harder to restore using backups and their targets are increasingly becoming organizations with much more to lose (and more money to payout) than individuals.

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 antivirus 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 antivirus 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/futureproof-ransomware

Carbon Black.

Carbon Black is the leading provider of next-generation endpoint security. With more than 9 million endpoints under management, Carbon Black has more than 3,000 customers, including 30 of the Fortune 100. These customers use Carbon Black to replace legacy antivirus, lock down critical systems, hunt threats, and protect their endpoints from the most advanced cyberattacks, including non-malware attacks.

1100 Winter Street, Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.carbonblack.com

Ver. 17_0417