Check Point®
SOFTWARE TECHNOLOGIES LTD

# Ransomware

## A NEW APPROACH TO IDENTIFYING, BLOCKING AND REAL-TIME REMEDIATION

MAY 17, 2017

# TABLE OF CONTENTS

©2017 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

## The Ransomware Challenge

If your organization has not yet been hit by ransomware, the chances are it soon will be. Ransomware has become the cybercriminal's weapon of choice, locking organizations large and small out of their own files and data with the aim of extorting a ransom in exchange for unscrambling them.

Now a global epidemic, ransomware attacks targeting companies have escalated 300% since January 2016; attacks are occurring every 40 seconds. Check Point's H2 2016 Global Threat Intelligence Trends showed that ransomware attacks doubled during the period July – December.

Just some of the recent high-profile victims of ransomware:

- The UK's National Health Service, US delivery company FedEx, car manufacturer Renault in France and telecommunications company Telefonica in Spain were among 200,000 businesses across 150 countries that fell victim to the high profile WannaCry attack in May 2017.
- Netflixfell victim to an extortion attack in May 2017 (technically, this was not a ransomware attack because the data was not encrypted when it was stolen). Hackers posted unreleased episodes of the upcoming season of the Netflix show *Orange Is the New Black* online.
- The San Francisco Municipal Transit Authority had to open its fare gates in November 2016 when a ransomware attack took down its payment and email systems, demanding 100 Bitcoins ($73,000).
- Hosted desktop and cloud provider VESK handed over approximately $22,800 in BitCoins in September 2016, as a result of a ransomware attack.
- Kansas Heart Hospital, which was attacked in May 2016, learned a hard lesson when it paid the ransom but didn't get all its data back.

Check Point's recent ransomware defense survey found that 36% of respondents said they had been a victim of ransomware, causing problems including system downtime, loss of productivity and data loss. And the problem is getting worse. Criminals are accelerating the development and introduction of new, stealthy ransomware attacks and variants, which are purpose-made to evade detection by conventional defenses using new attack techniques – such as spreading via images on social media sites. Furthermore we are seeing increasing levels of sophistication with 'file-less' variants of ransomware that utilise admin tools such as PowerShell to evade detection. These advances leave many organizations dangerously exposed to new and emerging types of ransomware.

In this document, we will examine the current, conventional approaches to ransomware prevention and the shortcomings of these traditional methods against new, zero-day variants. Then we will look at a new approach to detecting, blocking and mitigating the impact of even brand-new, unknown ransomware variants, to better protect your organization's assets and minimize damage and disruption.

## Conventional Ransomware Prevention

The risk of ransomware penetration and the business impact of a ransomware infection can both be reduced by implementing several conventional best practices. These can be split into two categories, general good practice and security best practice; these baseline protections are strongly recommended to any organization.

©2017 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

## GENERAL GOOD PRACTICE

- **Education:** Training users on how to identify and avoid potential ransomware attacks is crucial. As many of the current cyber-attacks start with a targeted email that does not even contain malware, but only a socially-engineered message that encourages the user to click on a malicious link, user education is often considered as one of the most important defenses an organization can deploy.
- **Continuous data backups:** Maintaining regular backups of data as a routine process is a very important practice to prevent losing data, and to be able to recover it in the event of corruption or disk hardware malfunction. Functional backups can also help organizations to recover from ransomware attacks.
- **Patching:** Patching is a critical component in defending against ransomware attacks as cyber-criminals will often look for the latest uncovered exploits in the patches made available and then target systems that are not yet patched. As such it is critical that organizations ensure that all systems have the latest patches applied to them as this reduces the number of potential vulnerabilities within the business for an attacker to exploit.

## SECURITY BEST PRACTICE

- **Endpoint protections:** Conventional signature-based anti-virus is a highly efficient solution for preventing known attacks and should definitely be implemented in any organization, as it protects against a majority of the malware attacks an organization faces.
- **Network protections:** Advanced protections in the enterprise network such as IPS, Network Anti-Virus and Anti-Bot are also crucial and efficient in preventing known attacks. Advanced technologies such as sandboxing have the capability to analyze new, unknown malware, execute it in real time, look for signs that it is malicious code and as a result block it and prevent it from infecting endpoints and spreading to other locations in the organization. As such, sandboxing is an important prevention mechanism that can protect against evasive or zero-day malware, and defend against many types of unknown attacks on the organization.

# Analyzing the Gaps in Traditional Prevention Techniques

Unfortunately, despite the importance of these conventional ransomware prevention best practices, even implementing all of them together does not guarantee protection. Many organizations that deployed some, or even all, of those best practices have fallen victim to ransomware mainly due to coverage gaps such as roaming users, removable media, failing to inspect SSL connections and usage of encrypted media. Let's take a look at the shortcomings of these approaches in turn to understand why.

- While education is critical, it lacks enforcement capabilities. Employees are only human, they make mistakes and they can be manipulated by fairly simple social engineering methods, even when educated about potentially malicious emails. All it takes is a moment's inattention from a user, and an attack can be triggered.
- While backups are critical to recovering after a ransomware attack, they can fail at the moment of truth. The backup may not always be up to date and the process to restore the files from the repository can be long and tedious – introducing delays and loss of productivity while data is being restored. New generations of ransomware are also specifically targeting backups and try to encrypt or delete them to maximize the ability to collect a ransom. In addition, backing up central file servers may be a relatively easy task but backing up all of the organization's endpoints is much more challenging: a great deal of valuable data is actually distributed on endpoint machines, and may not be regularly copied to a central data repository.

©2017 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

- While regularly patching systems goes a long way to reducing the number of potential exploits, many operating systems and application security vulnerabilities are being discovered every day. The OS and application vendors are releasing patches and updates to fix those vulnerabilities but many times users are failing to install those in a timely manner. Moreover, when those patches are released, attackers are made aware of those vulnerabilities and deliberately exploit those systems that are yet to be patched. And while organizations should strive to have their systems 100% patched, in real life there will always be a gap between the release of the patch and its deployment. This time window is the attackers' chance to attack.
- For all the protection that endpoint signature-based defenses provide, they are easily bypassed by obfuscated malware and ransomware and are highly dependent on regular updates. Despite blocking many basic attacks, AV solutions are bypassed every day by advanced attacks.
- While they are a crucial component of an organization's defenses, network-based protections, such as sandboxes, can only beneficial when users are connected to the network, and can also be occasionally evaded by malwares using sophisticated evasion techniques.

With ransomware becoming ever more sophisticated and only requiring a single weakness in an organization's defenses to take hold of the IT infrastructure, these gaps clearly need to be closed. As such, ransomware protection needs a new approach to prevent more businesses suffering the disruption and damage of a successful attack.

## Taking Ransomware Head-On

Ransomware has a lot in common with other malware: It infiltrates the organization through email attachments, web downloads or removable media, uses social engineering tricks, and leverages vulnerability exploitation tactics to gain a foothold on its target systems.

But ransomware also has unique characteristics. As the SANS Institute pointed out in its 2016 Incident Response survey, ransomware attacks highlights the need for rapid response, with minimum delay. With other types of malware, the criminals' objective is stay hidden from detection for as long as possible to enable lateral movement on the target network over periods of days or weeks.

In contrast, the objective of a ransomware attack is to quickly prevent users' access to files, and then encrypt as many files as possible, in the shortest possible time. The faster that ransomware can infect and spread through the target network, the greater the chance that the organization will agree to pay the ransom.

So an effective anti-ransomware solution has to be able to detect the earliest possible signs of infection and indicators of compromise, and then block the infection at source (whether on the endpoint or on the corporate network) before it can start to spread.

Check Point's malware analysis and threat research teams thoroughly studied thousands of real-world ransomware variants, from hundreds of different ransomware families, all collected in the wild with a simple goal in mind: to understand their fundamental characteristics, such as deleting shadow copies, preparing and displaying ransom notes, the dynamics of file encryption and many more. Building on this understanding, we have defined and developed a dedicated solution that tackles ransomware head-on.

Here are the underlying principles of the solution:

- **Implemented on the endpoint:** The endpoint – whether a desktop, laptop or server – is the first target in ransomware attacks. By compromising a single endpoint, the ransomware can then look for and spread to network shares, online backups and other resources. Also, as we mentioned earlier, the endpoint is often where new, valuable user data resides. So it is critical that the anti-ransomware solution protects on the endpoint itself, to identify the first indicators of compromise and block the potential spread of ransomware.
- **Built on behavior analysis:** Many new ransomware variants are found in the wild which have not yet been classified, and for which no signatures have been developed. These variants can bypass signature-based methods of detection, and may not even be detected by sandboxing due to various anti-sandbox evasion techniques such as virtual machine detection, delayed execution and human behavior sensors. However, those evasions will not be used on the target system, hence, the endpoint, as this is where attack should run. As such, code that is suspected of being ransomware should be detected and blocked by tracing its steps in runtime and looking for signs of suspicious behavior.
- **Can remediate attacks:** It is never enough to merely detect and deliver an alert about an attack or infection attempt – ransomware is designed to operate quickly, and could encrypt thousands of files before the alert is noticed and acted on. The anti-ransomware solution should have the capability to detect the attack at the earliest possible stage, ideally before any files are encrypted, completely remove all elements of the infection and remediate the attack.
- **Restores encrypted data:** Although the behavioral analysis capability is capable of detecting ransomware attacks at a very early stage, as more sophisticated and complex attacks are developed, detection may well take more time. During that time, ransomware may already begin encrypting a number of files on the machine it first infects. The optimal solution should be able to automatically restore any encrypted data and "roll back" the infection to the exact status the endpoint was before it.
- **Connectivity independent:** When dealing with ransomware, it is not safe to assume that the endpoint device will be connected to the corporate network. The optimal anti-ransomware solution should work effectively in the very likely event that the endpoint is not connected to the network, which means that it cannot use a sandbox inspection and is not receiving regular updates from a centralized threat intelligence feed.

## How Check Point Anti-Ransomware Works

SandBlast Anti-Ransomware protects organizations against all types of ransomware attacks, not only blocking infections at the first contact, but also quickly remediating their actions.

The Anti-Ransomware technology utilizes an advanced security engine and algorithms to automatically detect, block and remove the most sophisticated and evasive ransomware infections. By using predictive behavior-based technologies which do not rely on signature updates, Anti-Ransomware is able to identify and remediate zero-day ransomware, and to restore any data or files encrypted during an attack almost immediately, minimizing business disruption.

Anti-Ransomware utilizes a multi-layered architecture to provide a comprehensive solution in the fight against ransomware:

©2017 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]

## LAYER 1: RANSOMWARE BEHAVIORAL ANALYSIS

**Real-time behavioral analysis identifies ransomware before it can begin encrypting data**

- Purpose-built algorithms perform ongoing inspection of all activities in the OS, looking for ransomware-specific behavior patterns.
- In addition to ransomware, our analysis engine also detects and blocks other types of malware that may have characteristics similar to ransomware .

## LAYER 2: ILLEGITIMATE DATA ENCRYPTION IDENTIFICATION

**Identifies ransomware that evades initial behavioral analysis and begins encrypting data**

- An independent file-tracking engine looks for evidence that data files, such as documents and images, are being illegitimately and systematically encrypted.
- The file-tracking engine keeps close track of any change to files, checking which processes are modifying data files, and the nature of the modification. The engine is designed to differentiate between legitimate and illegitimate activities.
- If ransomware is actively encrypting data, the algorithms will pick this up immediately, typically before more than a few dozen files have been encrypted.

## LAYER 3: AUTOMATED FORENSIC ANALYSIS AND MALWARE QUARANTINE

**Automatically analyzes and quarantines any detected ransomware**

- Ransomware (or other types of malware) detected by the engines described above (layers 1 & 2) automatically triggers forensic analysis.
- The analysis begins with the detected indicator of compromise (IOC) being used as the basis for the investigation.
- The forensic analysis uses SandBlast Agent's powerful ability to automatically trace the attack activity and analyze all its elements, in order to identify the full ***attack model***.
- The generated attack model includes identification of the malicious elements and activities of the ransomware.
- Using SandBlast Agent's malware removal capability, all malicious components of the malware – as identified by the generated forensic attack model - are terminated and quarantined, stopping the ransomware from encrypting any further files, and from spreading to other drives or network shares.

## LAYER 4: DATA RESTORATION

**Restores data immediately in the event where encryption starts before ransomware is identified or blocked**

- The solution automatically takes ongoing snapshots of data files, before the files can be modified.
- Several factors help minimize and reduce the storage required for snapshots to 1GB (default setting):
  — A file snapshot is taken only when we suspect an attempt to modify the file might be illegitimate (from layer 2 detection).
  — Users typically modify very few data files during the course of day-to-day work.
  — Maintaining a short file history is sufficient. File snapshots need to be maintained only until a determination is made on the nature of the modification. If it isn't ransomware, then the snapshots can be discarded.
- The data-file snapshots are stored on the endpoint file system and protected from tampering by Check Point Endpoint's self-protection kernel drivers.
- After malware is quarantined by layer 3 of the solution architecture (as described above), data files are automatically restored from the snapshots, to quickly remediate any ransomware actions and to minimize business disruption.

©2017 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]
May 17, 2017

## Anti-Ransomware Effectiveness

Using cutting-edge research and dedicated advanced technology is obviously a must in order to combat modern sophisticated ransomware. But how effective is the final product? Answering this question requires constant and rigorous testing with an ongoing stream of current real world ransomware samples.

Anti-Ransomware technology is being rigorously tested in Check Point daily against a continually-updated, extensive range of fresh, real-world ransomware samples found in the wild.

We have devised the following methodology in order to continuously validate the effectiveness of our anti-ransomware solution. Each day, a set of new ransomware samples are gathered from the Internet, and are executed in our research laboratory on a virtualized endpoint that imitates a typical end-user's physical PC. The only security technology installed and activated on this endpoint is Check Point's Anti-Ransomware technology; all other endpoint and network security technologies (such as firewalling, IPS, anti-virus, anti-bot, threat emulation, etc.) are disabled. We monitor the malware's execution to see whether our Anti-Ransomware technology was able to detect the infection and quarantine it before it could start encrypting files. If the ransomware was an advanced, sophisticated variant that was able to start encrypting files before it was identified and blocked, we check that the solution was able to successfully restore the encrypted files to their original state.

Using this process, we test an average of 250 ransomware samples daily. During the 6 months since we started testing, the malware catch rate has exceeded 99%, and is improving every day as the behavioral analysis detection engine is enhanced based on testing. In addition, the false positive rate we are seeing is negligible when compared to the impact of an undetected ransomware attack on the organization and also in terms of the impact of everyday operation on the organization. In real life scenarios, where the security protections that were disabled for this testing would have been enabled, the catch rate will be even higher, reaching as close as you can get to full protection.

## Summary

Ransomware has become a major threat to business and individuals around the world. The inability to effectively counter ransomware attacks can cause significant losses and major disruptions to organizations. Implementing conventional best-practices and anti-malware protections can defend against some well-known, older variants of ransomware, but given the sophistication and ongoing evolution of modern ransomware, are not enough on their own to identify and block new, zero-day attacks.

Check Point's Anti-Ransomware technology uses a purpose-built engine that defends against the most sophisticated, evasive zero-day variants of ransomware and safely recovers encrypted data, ensuring business continuity and productivity. The effectiveness of this technology is being verified every day by our research team, and consistently demonstrating excellent results in identifying and mitigating attacks.

SandBlast Agent, Check Point's leading endpoint prevention and response product, includes Anti-Ransomware technology and provides protection to web browsers and endpoints, leveraging Check Point's industry-leading network protections. SandBlast Agent delivers complete, real-time threat prevention and remediation across all malware threat vectors, enabling employees to work safely no matter where they are, without compromising on productivity.

To learn more about threat prevention and how Check Point Anti-Ransomware, SandBlast Zero-Day Protection and SandBlast Agent can help protect your company against ransomware, please visit our website at www.checkpoint.com/sandblast.

# Frequently Asked Questions on Anti-Ransomware

### Our AV has successfully stopped ransomware previously, why do I need Anti-Ransomware?

Traditional AV can be effective in detecting attacks by known ransomware. However, ransomware is constantly evolving, mutating and incorporating new evasion tricks. Many ransomware attacks are capable of evading AV detection, as evident by the numerous infections suffered by businesses globally – virtually all of which are utilizing conventional AV solutions. Moreover, signature-less and behavioral-analysis based Anti-Ransomware can automatically recover encrypted files from infected users' endpoints, even if those machines are offline.

### If I use Anti-Ransomware, do I still need my endpoint AV?

We recommend using endpoint AV on all endpoints – it is still an important part of an effective, multi-layered approach to security, and it is still an effective means for preventing basic malware attacks that are still very prevalent. SandBlast Agent can be deployed alongside any third party AV solution, or as a single unified product with Check Point Anti-Malware or with Check Point's full endpoint suite for an integrated solution with a single agent and management.

### How much storage is required for Anti-Ransomware's file snapshots?

We recommend allocating 1GB of storage for file snapshots. The storage capacity can be custom-configured by the customer.

### Do I still need my conventional backups if I use the Anti-Ransomware feature?

Yes. Anti-Ransomware focuses only on recovering data and files that have been encrypted by ransomware in the first stages of infection, not on general purpose backup. In order to ensure data recovery in the event of other situations, such as disk failure, a conventional backup is always highly recommended.

### How are file snapshots protected?

File snapshots are protected by the SandBlast Agent self-protection kernel driver, which prevents any attempt to access the data by processes that are not part of SandBlast Agent and signed by Check Point.

### What is an IT organization required to do when Anti-Ransomware detects an event?

An IT organization is usually not required to be involved when Anti-Ransomware treats an incident. Anti-Ransomware automatically recovers files affected by the attack. It keeps user notified at all steps. The self-service interactive process enables users to independently review and restore files.

©2017 Check Point Software Technologies Ltd. All rights reserved. Classification: [Protected]
May 17, 2017