ENSILO GUIDE TO UNDERSTANDING RANSOMWARE

2018 Whitepaper

ENSILO

WHAT IS RANSOMWARE?

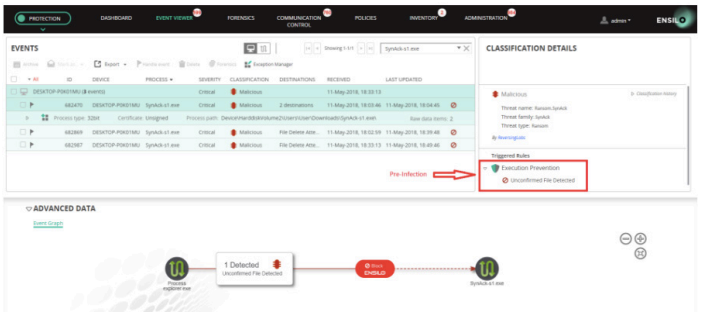
Ransomware is an increasingly popular tactic used to steal data and disrupt a system's operations. Essentially, ransomware is malware used by attackers to infect a device, hijack files on that device and lock them via encryption. These maliciously encrypted files can no longer be accessed by users and are held hostage by the attacker until a ransom is paid.

WHAT IS SYNACK?

SynAck ransomware was first discovered in 2017. The new variant of SynAck that was recently discovered utilizes the Process Doppelgänging technique to bypass detection of antivirus products. This is the first known ransomware that has adopted this sophisticated technique.

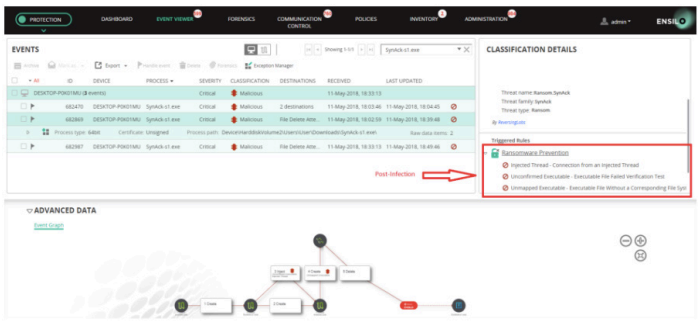
enSilo's protection platform blocks the SynAck on both pre- and post-infection stages during the initial execution process. It also stops the threat chain from advancing.

BLOCKING IN PRE-INFECTION (FIGURE 1)



In order to see our post-infection protection in action, we disabled our pre-execution engine. As shown in figure 2, SynAck is blocked by enSilo's ransomware prevention policy when it attempts to use the Process-Dopplegänging technique in attempt to avoid detection by AV.

ENSILO BLOCKING IN POST-INFECTION (FIGURE 2)



HOW DOES PROCESS DOPPELGÄNGING HIDE MALWARE?

On most Windows computers the files are stored on disks that use NTFS file system. This file system is relatively old, although Microsoft updates it from time to time. In 2007, with the release of Windows Vista, Microsoft introduced a new feature to NTFS—transactions. NTFS transactions allow many file operations to be performed and at the end either accepts those operations or cancels them. Therefore, any application could make changes to multiple files on disk and return all files to their original state if an error were detected. The most common use of transactions is during Windows updates installations. If everything goes well the transaction is accepted or, as it is called in transaction language, committed. If an error occurs, the transaction is canceled or rolled back.

Process doppelgänging utilizes this mechanism to hide the main malware payload by choosing an innocent file, overwriting it and running malware. Just before letting the malware run, it rejects or rolls back all changes, thus preventing antivirus software from scanning the file content that is really being executed. Note: the malware process can still be run in such a case. If opened, the file on disk will contain no suspicious content. Moreover, this file can be a well-known, digitally signed application.

WHO DOES RANSOMWARE AFFECT?

Ransomware can infect a single user and then spread throughout the entire organization, knocking computers offline and forcing employees to use pen and paper to do business while IT and SOC teams scramble to mitigate the infection.

HOW IS A USER AFFECTED?

A user can be infected in a number of ways, such as actively installing the ransomware (i.e., when it appears as an innocuous program), opening a malicious file in an email (such as a phishing attack) or surfing to a compromised website (a drive-by-download attack).

WHAT TRIGGERS RANSOMWARE?

While in certain scenarios the victim had to be active and click on the malicious program, **in most cases the infection is actually seamless to the user**. Ransomware that is triggered should be blocked from encrypting data and spreading through an organization laterally.

HOW DO I RECOGNIZE RANSOMWARE?

Ransomware creators are getting more creative with their attack tactics. Organizations now spend thousands of dollars for cybersecurity public awareness and education for their employees. However, it only takes one employee and one click to trigger a ransomware that could take down an entire organization.

HOW MUCH IS THE DEMAND AMOUNT FROM A RANSOMWARE ATTACKER?

The ransom can range from hundreds of dollars to hundreds of thousands, depending on the type of file and victim. Usually, the extortionists set a deadline for paying the ransom, and when that deadline is not met, a new deadline is set and the ransom rate increases.

CAN I STILL WORK ON MY COMPUTER IF RANSOMWARE IS TRIGGERED?

The most advanced attacks can crawl across organizational networks and traverse file shares looking for data. What it finds, it encrypts. Confused users have perfectly functioning computer systems, but no data. Or at least no data that they can read.

WHAT HAPPENS IF I ACCIDENTALLY CLICK ON A RANSOMWARE FILE?

Some ransomware encrypts files, while others lock out the user. After ransomware is triggered, a file appears in a pop-up format and it is often a friendly message from the attacker explaining exactly how the user can regain access to their files – and how much it's going to cost them. "Of course, there's no guarantee that even if a victim pays the demanded amount they will actually get access to their files again, which makes dealing with ransomware somewhat of a tricky issue"

HOW CAN I PREVENT RANSOMWARE ATTACKS?

WannaCry and Petya attacks were the top ransomware attacks fracturing critical infrastructures and causing complete business disruptions in a variety of industries. Many NGAV and AV security products failed to protect against these ransomware attacks because the products lacked a post-infection layer of protection. In addition to protecting against WannaCry and Petya, post-infection protection guards against many unknown variants because it can detect any malicious outbound connections that may occur after they bypass a pre-infection protection barrier such as NGAV or AV.

WHAT IS WANNACRY RANSOMWARE?

WannaCry ransomware was a worldwide cyber attack targeting computers with dated Windows operating systems. WannaCry completely disrupted business operations for many industries because they lacked proper cyber security capabilities that protected systems from a ransomware that used EternalBlue, an NSA exploit.

WHAT IS ENCRYPTION?

Encryption is encoding information in a format that is not legible to unauthorized parties. Encryption is designed to protect the confidentiality of your files. Encrypting your files is generally a good thing. For example, an application like Bitlocker (which has been part of Windows since Vista) uses an algorithm to convert data on your drive to encrypted data. This makes it unreadable to everyone unless you unencrypt the data. Or you can encrypt individual files. In either case, a "key" is used to unencrypt the data.

HOW LONG DOES IT TAKE FOR RANSOMWARE TO ENCRYPT MY FILES?

Encryption time depends on the file extensions that exist on the victim's machine, as well as how many files with these extensions exist.

HOW CAN I PREVENT RANSOMWARE PRE-INFECTION?

Essentially, pre-infection is used to manage cyber hygiene. Pre-infection protection such as NGAV and AV protects users from known ransomware that is signature based or exploits vulnerabilities with a patch or malware that has been seen before.

HOW CAN I PROTECT MY COMPUTER UTILIZING AUTOMATED POST-INFECTION PROTECTION IN REAL-TIME?

Step 1: Conduct a retroactive review in real-time. It starts by seamlessly recording all OS activity.

Step 2: Freeze the action and retrieve all recorded activity only when there's an attempt to take or modify data.

Step 3: Retroactively analyze the retrieved history. This chain of OS activities provides conclusive evidence that you're dealing with an actual threat.

Step 4: Block the action in real-time if it is a real threat, with absolutely no impact on the user's machine.

Step 5: Identify the root cause by tracing malicious activity back to its origin. If you choose to take action, you can also neutralize it.

Learn more about how enSilo can protect your organization's endpoints with automated real-time protection. Visit ensilo.com for more info.

CAN RANSOMWARE BYPASS AV AND NGAV PRE-INFECTION DEFENSES?

Antivirus and NGAV solutions are simply not enough. Traditional antivirus solutions were designed and built before the ransomware epidemic. NGAV claims to defeat ransomware "better" than AV. "The bad guys are still iterating far faster than the antivirus companies can keep up, next-generation or not."

ENSILO GUIDE TO UNDERSTANDING RANSOMWARE

WHAT IS RANSOMWARE AS A SERVICE?

Ransomware as a service (RaaS) is a variant of ransomware designed to be so user-friendly that **anyone with little or no technical knowledge can also easily deploy them to make money**. Ransomware is "the new age robbery" and the risk of getting caught is low.

HOW MUCH CAN A CRIMINAL MAKE FROM RANSOMWARE?

According to a security expert who requested anonymity, **ransomware cybercriminals took in about $1 billion** last year. Victims usually pay anywhere from $200 USD to $10,000 USD, often in Bitcoin.

MY ORGANIZATION HAS BACKUP DATA, SO WE SHOULD BE OK, RIGHT?

Because backing up files is costly, many organizations don't include their most important documents in their backup. So if ransomware hits, these companies don't have the most updated version of their files on hand.

IF MY ORGANIZATION HAS ALREADY BEEN HIT WITH RANSOMWARE, CAN WE GET HIT AGAIN?

Ransomware exploits human and technical vulnerabilities to gain access to an organization's technical infrastructure. It then denies the organization access to its own data by encrypting that data. Chances are if the organization has been hit with ransomware, **the infections will only increase**, unless the organization deploys a solution with post-infection protection.

WHAT IS THE BEST DEFENSE AGAINST RANSOMWARE?

To prevent ransomware from infecting your devices, invest in the best endpoint protection with an efficient endpoint security solution. The best ransomware protection provides two separate layers of endpoint protection.

The first layer of defense is **NGAV or pre-infection protection**, which is essentially used to clean up known security vulnerabilities by maintaining a better cyber hygiene.

The second layer of defense occurs **post-infection**, similar to an EDR, but in real-time. This post-infection layer protects an organization from any malicious outbound activity that usually occurs during a data breach. It also protects the organization from any suspected malicious activity that bypassed the pre-infection layer. It is the last line of defense that allows a CISO to sleep better at night.

HOW CAN RANSOMWARE SPREAD AND INFECT MY ENTIRE ORGANIZATION?

Ransomware can spread in three ways:

1. Implementing the lateral movement capability on its own.
2. Using other Trojans that are considered "stealers" by design.
3. Finding vulnerabilities that allows it to propagate.

IF MY ORGANIZATION IS PARALYZED BY RANSOMWARE, SHOULD WE PAY THE REQUESTED AMOUNT?

Paying a ransom doesn't guarantee an organization that it will get its data back. We've seen cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals.

HOW SEVERE IS THE RANSOMWARE THREAT TO ORGANIZATIONS?

Ransomware is a threat for every organization, yet very few organizations implement disaster recovery planning. A recent U.S. government interagency report indicates that, on average, "there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015)."

WHAT IS PETYA RANSOMWARE?

A variant of Petya ransomware was utilized in a second worldwide attack which also targeted Windows operating systems. This cyber attack was framed as a ransomware attack for first responders. It was then discovered that this variant of Petya ransomware was paired with a NSA exploit and was a wiper, later dubbed NotPetya.

WHAT ARE COMMON TYPES OF RANSOMWARE?

The two most common types of ransomware are:

- **Crypto ransomware** which encrypts files or data, preventing access to the user. It has evolved to common variants, such as CryptoLocker, which generated $3 million USD before authorities took it down. CryptoWall had generated $18 million USD by June 2015.
- **Locker ransomware**, which locks the device from being accessed.

ARE ORGANIZATIONS REQUIRED BY LAW TO REPORT A RANSOMWARE INFECTION?

Yes, if it's health data. The U.S. Department of Health and Human Services (HHS) Office of Civil Rights recently stated that according to Ransomware Fact Sheet "the newly released guidance from the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR), ransomware is now considered a data breach and healthcare organizations are required by U.S. law to report ransomware attacks. The HHS has also developed guidance to help healthcare organizations better understand and respond to ransomware threats.

WILL RANSOMWARE ATTACKS DIE DOWN?

The proliferation of ransomware is predicted to only get worse. According to McAfee Labs, there were twice as many ransomware samples in 2015 Q1 than in other any other quarter, and the FBI recently issued an alert on the uptick of ransomware, citing CryptoWall as "the most current and significant ransomware targeting US individuals and businesses."

HOW IS RANSOMWARE EVOLVING?

In the past couple of years, we have seen ransomware growing from a nickel-and-dime operation targeting individual computers to a **multimillion-dollar criminal operation** targeting organizations that can afford to pay enterprise-level payments.

FIVE WAYS TO PROTECT AGAINST RANSOMWARE

The best way to protect against ransomware is by using an efficient **endpoint security solution like enSilo's**. This solution provides the following:

1. DETECTION

Blocks attacks in real-time by stopping malicious activity that results from exploited vulnerabilities.

2. CONTAINMENT

Identifies security concerns with a single product that can maximize investigation and sustain business continuity without isolating an infected device.

3. INVESTIGATION

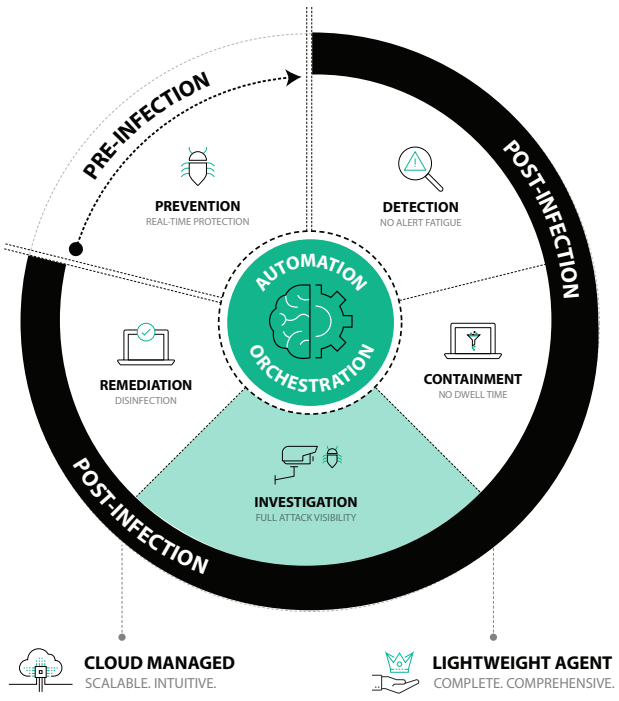
Eliminates remediation latency and reduces alert overload by virtual patching to mitigate cyber threats.

4. REMEDIATION

Unifies a 24-hour-a-day incident monitoring with both pre- and post-infection protection, allowing visualization of the entire environment.

5. PREVENTION

Rectifies ransomware prevention by blocking malicious outbound communication in real-time.



ABOUT ENSILO

enSilo delivers the first complete endpoint security platform providing pre- and post-infection protection in real-time, defending endpoint devices from data tampering and breaches caused by advanced malware. enSilo provides security operators with an intuitive way to manage, orchestrate and automate prevention, detection, response and remediation tasks. A single lightweight agent combines enSilo's Next Generation AntiVirus (NGAV) and automated Endpoint Detection and Response (EDR) with real-time blocking to deliver a multi-layered defense strategy that can be managed from the cloud. enSilo strives to make self-defending endpoint security cost-effective so virtually any enterprise can ensure business continuity. To learn more, visit www.ensilo.com.

CONTACT ENSILO

enSilo is headquartered at 182 Second Street, Suite 210 San Francisco, CA 94105
Email us at contact@ensilo.com or call us at 800.413.1782 2018

REQUEST A DEMO

https://info.ensilo.com/schedule-demo

Sources: Healthcareitnews.com, Businessinsider.com, ZDNet.com, TheRegister.co.uk, CSOOnline.com

ENS18-000-06012018