A Trend Micro White Paper I **October 2017**

Ransomware on Servers:

Detection and Prevention using Trend Micro Deep Security

>> This paper is aimed at information security professionals looking to combat ransomware on their enterprise servers. It provides guidance on how to adopt and implement safeguards to enterprise servers across physical, virtual, and cloud environments leveraging Trend Micro™ Deep Security™.

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice. Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes. Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Table of Contents

INTRODUCTION

Intended Audience

This paper is aimed at information security professionals looking to combat Ransomware on servers. It will provide guidance on how to adopt and implement safeguards to servers leveraging Trend Micro™ Deep Security™. It is expected that the reader is comfortable with common computing, security, and networking terminologies and topics.

About This Paper

This paper will assist in designing a “defense-in-depth” strategy to combat ransomware using Deep Security. We will first discuss the generic and the most effective IT strategies over the years against threats and then provide specific configuration guidance on how to leverage Deep Security modules, such as Intrusion Prevention System (IPS), firewall, application control, integrity monitoring and anti-malware, to help create a “defense-in-depth” strategy against ransomware.

This paper is not intended or claimed to provide a “magic” solution to combat ransomware nor should it be believed that there is a single technology which will prevent all of the bad scenarios or the continued proliferation of ransomware.

An information security professional’s job is to make it harder and increasingly frustrating for adversaries by adopting a “defense-in-depth” or “layered security model”. This model recommends “Detective”, “Preventive”, and “Forensic” defensive layers and we will see where Deep Security can fit into this model.

Help and Support

This paper is not meant to be a substitute for product documentation.

For detailed information regarding installation, configuration, administration and usage of the Deep Security product, please refer to https://help.deepsecurity.trendmicro.com/.

PART I: A BRIEF HISTORY OF RANSOMWARE

Ransomware has become a prominent type of malware, belonging to the class of malware known as "scareware" which takes advantage of people's fear. Its underlining concept is simple: you have something that is valuable to you, so let's hold it hostage and hope the fear of losing it forever will make you pay the ransom to get it back.

It's hard to discuss Information Security without bringing up ransomware as enterprises, Small-Medium Businesses (SMB), and individuals alike are facing continuous battles against it. Though its first occurrence was nearly 28 years ago, it really came to light in 2006 with the release of "Archiveus Trojan" which was the first ever ransomware to use RSA encryption. In 2013, we saw that "CryptoLocker" was able to successfully extort money from victims on a massive scale and the same year when ransomware into a lucrative business model. Since then, ransomware has been creating havoc and attackers have created more improved ransomware variants like CryptoWall, Locky, TeslaCrypt, WannaCry, and Petya to name the few.

Types of Ransomware

There are two primary types of ransomware:

1. **LOCKER RANSOMWARE**
   Locker ransomware, which is also known as Computer lockers, is designed to deny access to a user's computer or device. This type of ransomware simply tries to lock the victim's desktop, without touching the data and files in the file system and request ransom. The main goal of this type of ransomware is to leave the victim's computer with limited capability and functionality so that they can't gain access to their data. The locking procedure involves creating a new desktop for the victim and then making it persistent, and the new presented desktop eliminates unnecessary processes and disables certain keyboard shortcuts and special keys, such as the Esc and Windows keys.

   Ransomware that falls under this category that we see often uses fear techniques to pressure the victims into paying the ransom. It tricks the user with copyright infringements or by claiming to represent a law enforcement authority to issue fines on criminal activities. These types of ransomware are less effective to enterprises, SMBs, and tech-savvy individuals since it lacks the technical complexity required to perform a successful attack to hold victim's resources hostage. They can be removed cleanly and the victim's computer can be restored close to its original state.

2. **CRYPTO RANSOMWARE**
   Crypto ransomware, as the name suggests make use of cryptography, the very same technique that information security professionals use to protect data from unauthorized access. This type of ransomware targets users' data/files and encrypts them using symmetric and asymmetric encryption. Ransomware of this kind targets various types of files from documents, images (photos), and database files. For example, WannaCry targeted 176 file types to ensure it encrypted files that were valuable to variety of its victims, as opposed to a specific kind of victim. This type of ransomware can travel across a user's network and encrypt any files located on both mapped and unmapped network drives.

Crypto ransomware don't use techniques to trick victims into paying a ransom, instead they are upfront with their demands. They send an extortion message to a victim that provides instructions on how to pay the ransom. The message also contains information about how much time the victim has to pay ransom and the consequences for not paying before the set deadline. Crypto ransomware threats are much more effective and technically capable of keeping a victim's resources hostage than locker ransomware is since it adopts stronger operational and encryption procedures. We will discuss more on how the crypto ransomware works in the next section of this paper.

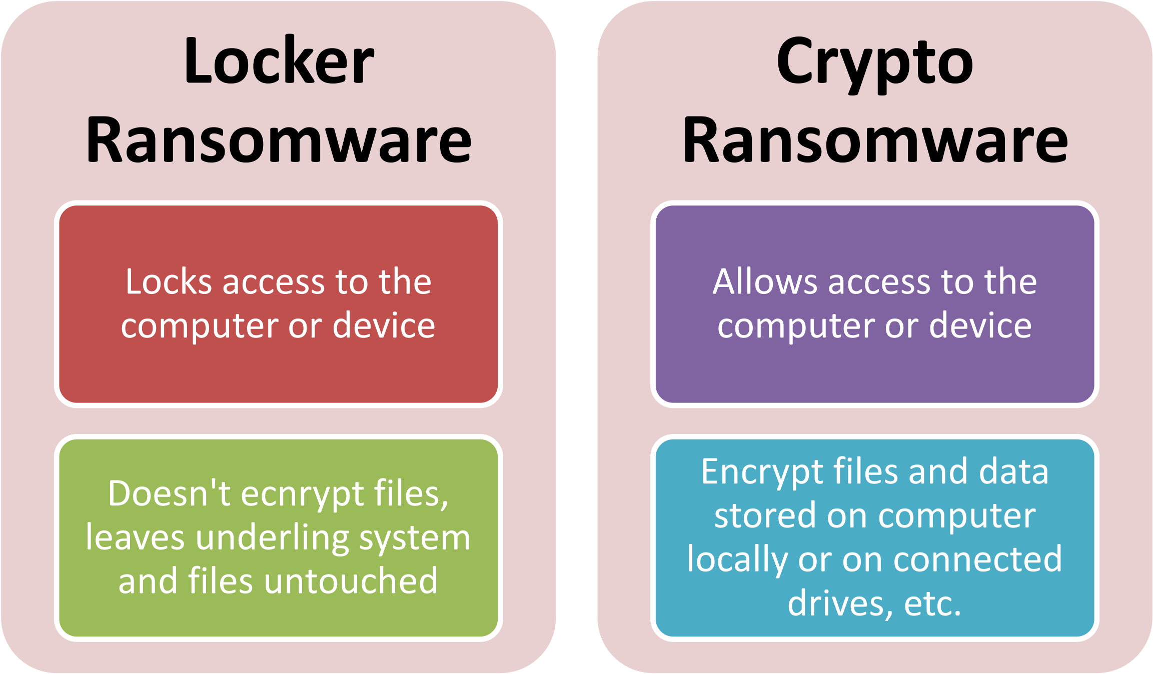

Locker Ransomware
Locks access to the computer or device
Doesn't ecnrypt files, leaves underling system and files untouched
Crypto Ransomware
Allows access to the computer or device
Encrypt files and data stored on computer locally or on connected drives, etc.

FIGURE 1 - TYPES OF RANSOMWARE

The Evolution of Ransomware

The advancements in technology, ease of use, and our reliance on devices has made our lives increasingly digital. We are storing more and more personal data on our computers, laptops, and other hand-held devices. Our adoption of technology has also provided new avenues for our adversaries. The AIDS Trojan, known as the PC Cyborg that Joseph L. Popp created and sent to attendees of the World Health Organization's International AIDS conference in 1989, faced a number of challenges before it was successful. It had problems with the delivery mechanism, the unavailability of a stronger encryption solution at the time, and difficulty gaining untraceable financial benefits out of it. However, the AIDS Trojan set the scene for today's successful ransomware threats.

The figure below shows how ransomware has evolved over time, has become more sophisticated, and has adapted to our digital lives. The era where it was just causing annoyance to its victims is gone—it has now entered into an era where it is providing a business model that offers significant financial gains. The use of advanced encryption technologies and the availability of untraceable crypto-currency (Bitcoins) to receive ransom and anonymity network (TOR) to communicate with victims are arguably the main factors in the rise of ransomware. The adversaries now target victims' computing environments, including personal computers, mobile devices, and servers, regardless if a home user, an enterprise, or even a public agency owns them. As long as attackers can take a user's data hostage and they can receive ransom, there is a target.

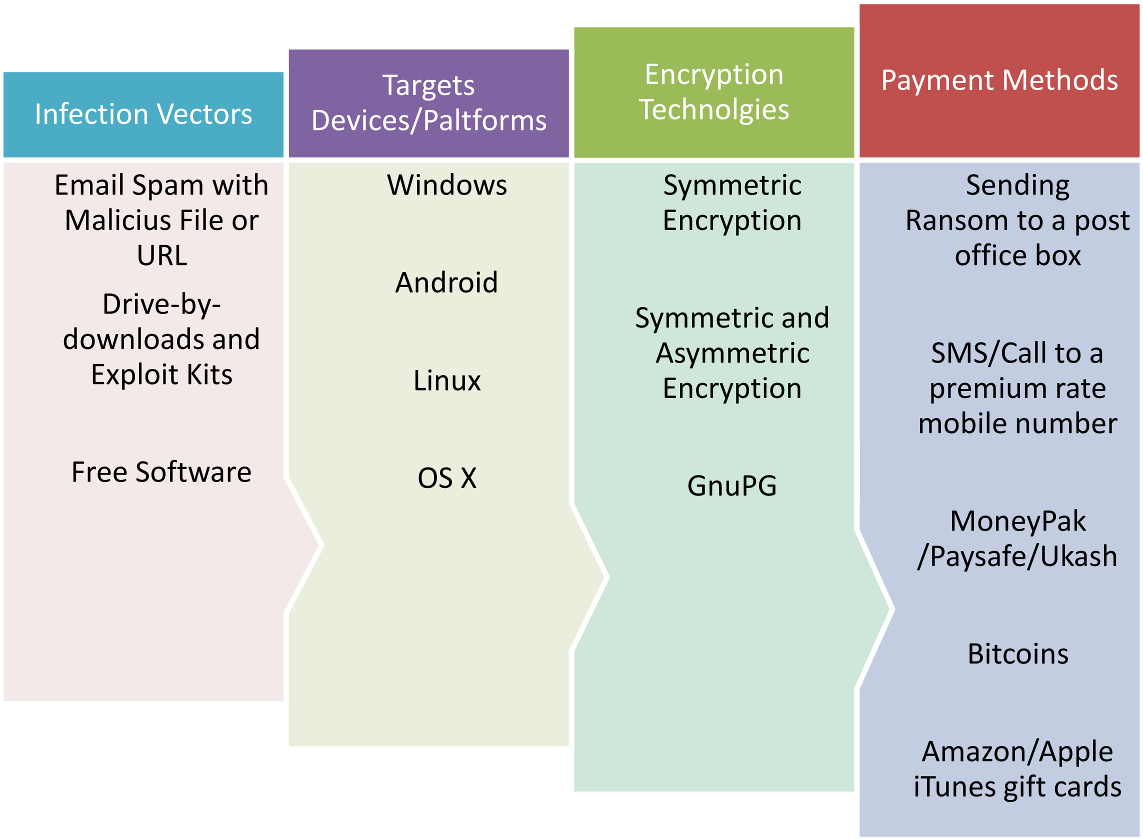

Infection Vectors
Email Spam with Malicius File or URL
Drive-by-downloads and Exploit Kits
Free Software
Targets Devices/Paltforms
Windows
Android
Linux
OS X
Encryption Technolgies
Symmetric Encryption
Symmetric and Asymmetric Encryption
GnuPG
Payment Methods
Sending Ransom to a post office box
SMS/Call to a premium rate mobile number
MoneyPak /Paysafe/Ukash
Bitcoins
Amazon/Apple iTunes gift cards

FIGURE 1 - QUICK VIEW OF THE EVOLUTION OF RANSOMWARE

PART II – HOW CRYPTO RANSOMWARE WORKS

We classified various ransomware into two main types; the locker ransomware and the crypto ransomware. The most effective and current ransomware is crypto ransomware. It is important to understand how this ransomware works. Despite the continuous improvement to their encryption, deletion, and communication methods, it is possible to design a layered defense strategy that can stop a large number of ransomware attacks.

Crypto ransomware operations and technical details vary, and to understand the general operations and high-level technical details of them, it is important to cover the details around which cryptography techniques adversaries use to encrypt files.

Customized Vs. Standard Encryption Cryptosystems

Encryption is the key element of crypto ransomware. We see both customized and standard encryption cryptosystems being used by crypto ransomware. The use of one cryptosystem over the other doesn't necessarily mean that the ransomware is more advanced, complex, or sophisticated. In fact, the adversary's choice to use cryptosystem in their ransomware could simply be a matter of their technical depth, to evade common malware detection techniques, or because they are targeting specific devices/platforms for their ransomware. For example, the CryptoLocker and CryptoWall both used standard Windows functions of Microsoft's CryptoAPI to perform file encryption.

Symmetric Vs. Asymmetric Encryption

Modern crypto ransomware use both symmetric and asymmetric encryption. The main reasons for dual encryption are performance and convenience. With symmetric encryption, the adversaries are able to encrypt victims' files in a reasonable time thus achieving high performance which is essential in staying under the radar. With the use of asymmetric encryption, adversaries can protect the symmetric encryption key, thus leaving the victims no chance to get their hands on the encryption key without requesting the private key from the adversary.

More advanced and successful ransomware use both symmetric and asymmetric encryption. It uses unique public and private key-pairs for each of victim to ensure that the delivery of a private key, once the ransom is paid, to decrypt files on a victim's computer cannot be used to decrypt files on every other computer infected using the same public key.

Key Management

Key management (symmetric key, asymmetric key pair generation, keys delivery and keys protection) is very important in the successful execution of crypto ransomware. The adversaries' goal is to make money and reduce any possibility of recovering the encrypted files without getting the ransom paid. For adversaries, it's equally important to reliably recover and decrypt the encrypted files once the ransom is paid for the attack to be considered successful. For this reason, the ransomware business model must show credibility. If a particular type of ransomware can't decrypt the files despite the ransom being paid, it will look bad on the attacker. News will spread fast and the next victim of the attacker will not pay the ransom. Ransomware is a business and one estimate claims CryptoLocker extorted excess of $300 million USD.

Key Generation & Delivery

Over the years we have seen adversaries enhance their techniques to overcome deficiencies found in previous ransomware in order to successfully execute their ransomware campaign. The two approaches adversaries have taken when it comes to the generation of the cryptography keys is either local (on a victim's computer) or remote (on an adversary's/C&C system).

Looking at modern crypto ransomware, it is observed that the symmetric key (the encryption key which is used for encrypting the files) is generated locally on the victim's computer and then the Public key from the asymmetric key pair is used to protect this encryption key. There are two approaches adversaries take when it comes to the generation of the asymmetric key pair, for example:

- The asymmetric key pair was generated "remotely" on an adversary's command-and-control (C&C) system (CryptoLocker used this approach).

- The asymmetric key pair was generated "locally" on a victim's computer (CryptoDefence used this approach).

In each approach, it was required to communicate with C&C.

In the case of CryptoLocker, the encryption took place only after successful communication with the C&C to retrieve the public key, if C&C communication was blocked the ransomware didn't proceed with the encryption.

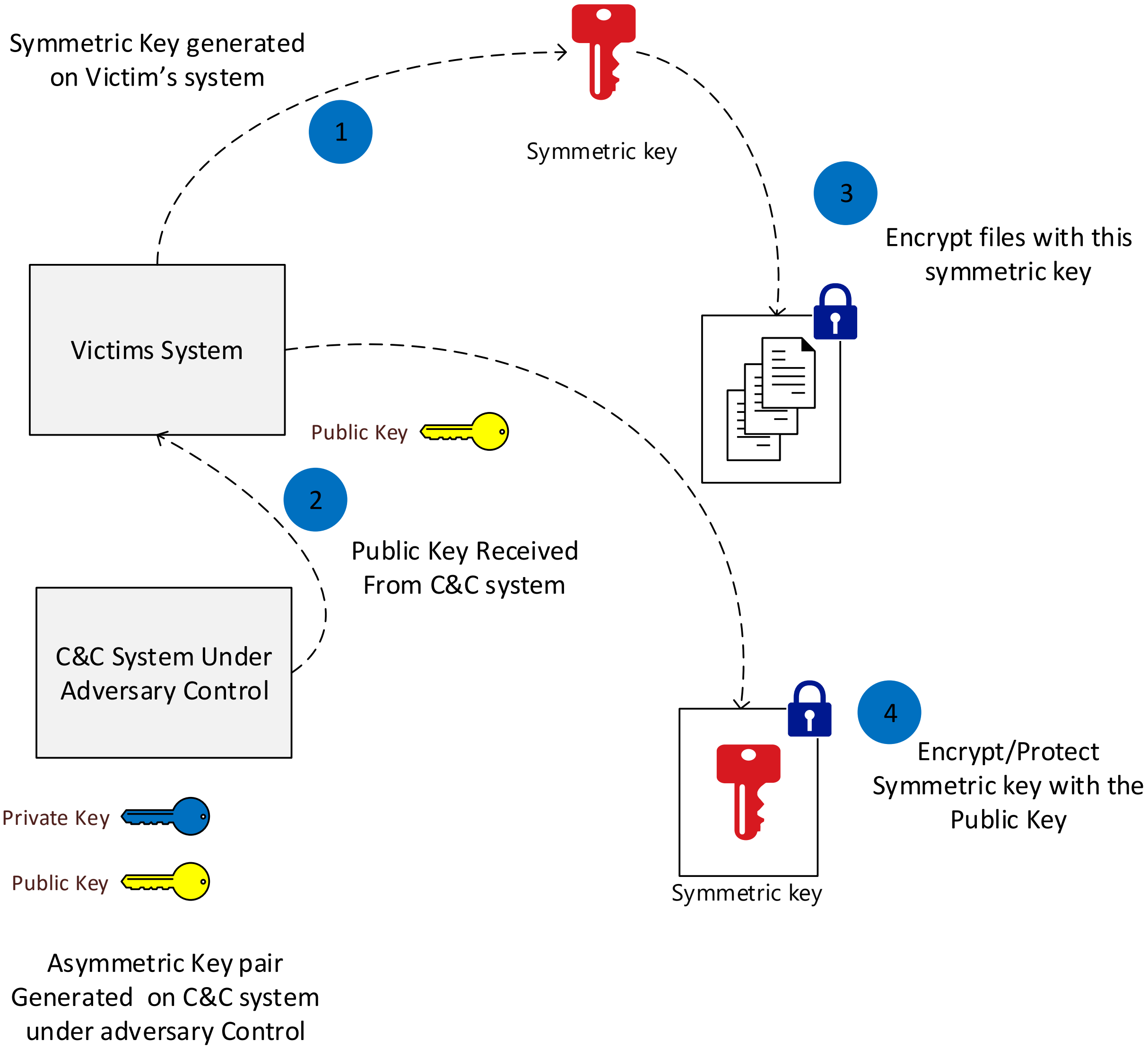

Symmetric Key generated on Victim's system
1
Symmetric key
3
Encrypt files with this symmetric key
Victims System
Public Key
2
Public Key Received From C&C system
C&C System Under Adversary Control
4
Encrypt/Protect Symmetric key with the Public Key
Symmetric key
Private Key
Public Key
Asymmetric Key pair Generated on C&C system under adversary Control

FIGURE 2 - CRYPTOLOCKER SIMPLIFIED KEY MANAGEMENT FLOW

In the case of CryptoDefense, the private key must be sent back to the adversary after the encryption process is done. Though better than CryptoLocker on when the encryption process can start, using this approach means that the private key that the adversary is holding to make decryption possible is also left behind on the victim's computer after its transmission to the adversary.

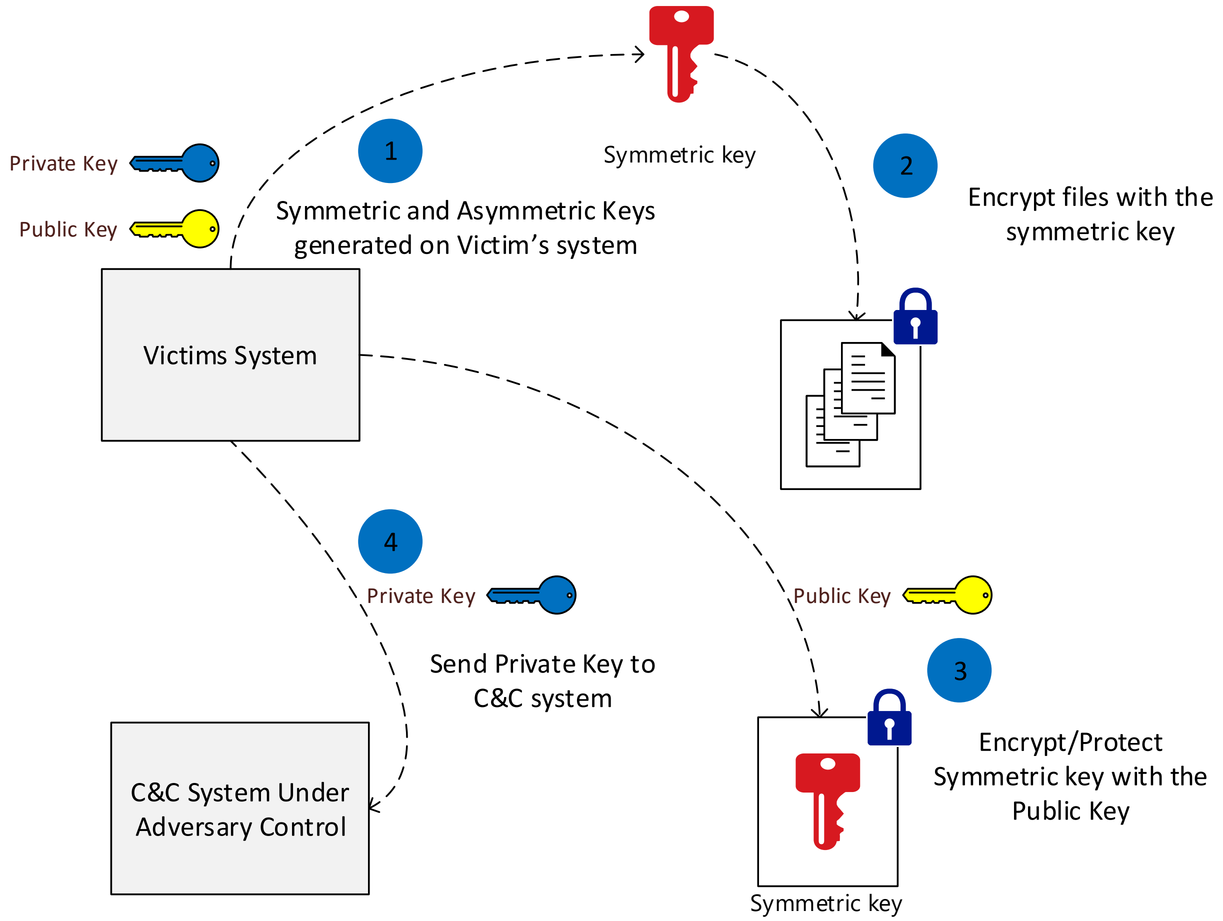
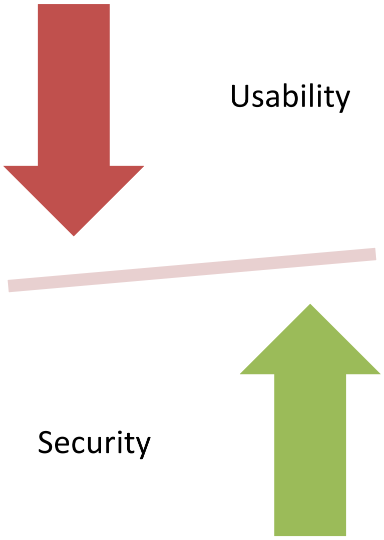

Private Key
Public Key
1
Symmetric and Asymmetric Keys generated on Victim's system
Symmetric key
2
Encrypt files with the symmetric key
Victims System
4
Private Key
Send Private Key to C&C system
Public Key
3
Encrypt/Protect Symmetric key with the Public Key
C&C System Under Adversary Control
Symmetric key

FIGURE 3 - CRYPTODEFENCE SIMPLIFIED KEY MANAGEMNET FLOW

Regardless of which approach the adversary takes in their ransomware, their threat is not always air tight. CryptoDefense leaves the keys behind that can be located and used to decrypt the files, so there is always a chance that will leave victims with room to maneuver.

PART III – DEFENCE-IN-DEPTH STRATEGY



The design of a defense-in-depth strategy requires humans and technology to work together. The battle with ransomware is real and we all have to play a role to win this battle whether as a product designer, as a user of the product, or as a security professional implementing security product—we all have to use basic security practices.

Today's adversaries are equipped with advanced technical skills, well resourced, and extremely motivated. They are constantly looking to improve their techniques and have proven that they can move fast and have taken a more aggressive approach in recent years. They have moved from selling misleading software to a pure ransom model which has inarguably become the most dominant form of threats today.

The recommendations we discuss in this section below are structured as follows:

- The general best security practices that are adopted by many organizations around the world in light of the years of analysis by security organizations.
- Specific security controls that are offered by Trend Micro™ Deep Security™ to help deploy layered security controls.

General Best Security Practices

USER AWARENESS TRAINING

User awareness training should be at the top of every organization's security practice, as the weakest link in cybersecurity is the end user. An end user well-trained on basic security practices, like clicking on URLs, opening documents, or executing programs only from trusted sources is vital to the overall strategy of an organization and it can make a huge difference in its success and failure to defend against ransomware and other threats. Although information security professionals know better, end users don't come to work with intention on clicking links and opening unknown attachments in their emails. They need to be taught.

Adversaries are extremely tricky and use social engineering techniques to trick users into acting and responding to opening the door to ransomware. It is also equally important to conduct simulated phishing attacks to gauge a user's ability to identify current threats and encourage users to alert the IT security team of potential suspicious emails and files.

USE HARDENING FOR OS AND APPLICATIONS

Not everyone has the time to understand and master every intricate detail required to ensure their OS and applications are configured securely. The OS and applications are designed and shipped to keep a wide audience in mind and the use of such application varies greatly from user to user. This is why application and OS vendors face the dilemma of finding a balance between “usability” and “security”.

The system hardening approach is a very good foundation to build an overall defense-in-depth strategy, even though it sometimes creates more work. Not hardening it means having an insecure system that can be broken by anybody with sufficient knowledge and motivation. There are plenty of resources available, such as the National Checklist Program (NCP) and CIS benchmarks to name a few, that can help harden systems and applications. This means adding an additional layer of difficulty that adversaries must go through even if they manage to go through the other
lines of defense.

Hardening is critical. Don’t provide another avenue for adversaries to explore when it can be avoided altogether. For example, the authors of WannaCry ransomware used a previously-fixed vulnerability in SMBv1.0 to spread it like a worm. This particular version should have been disabled in users’ systems and even if they did have a legitimate reason to leave it enabled on their systems, the OS patch that addresses this vulnerability should have been applied.

STAY CURRENT ON PATCHES – CONSIDER VIRTUAL PATCHING SOLUTIONS

Effective patch management is difficult to achieve given the never-ending vulnerabilities in OS and applications (in-house as well as off-the-shelf applications). It is not just a case of patch availability from the vendor and applying patches to the system. The business operations continuity is very critical when new patches are released. Each new patch needs to be validated by the IT team to ensure that the risks are actually addressed without breaking existing applications. If something breaks, it puts organizations in catch-up mode and provides an exposure window to adversaries to carry out attacks.

A modern approach to the old dilemma is to use virtual patching solutions, a non-disruptive vulnerability shield that protects OS and applications during the risk window—and beyond. This information on Shielding End of Support Systems describes how Trend Micro™ Deep Security™ shields vulnerabilities in critical systems until a patch is available and deployed, in place of a future patch that may never materialize, or to protect systems that are not patchable. In each instance, the user gets a timely, cost-effective complement to traditional patching processes that can significantly lower costs, reduce disruptions, and provide greater control over the scheduling of patches.

ADOPT LEAST PRIVILEGE MODEL TO CONTROL ACCESS

Hardening the OS and applications and staying up-to-date on patches ensures a trusted computing base, and now all of the services and functionality that is exposed is required to run the business. However, having a “shell” access available to all users of the system may not be needed to run the business. For example, the ability to install new software on the system should be restricted to specific job functions. The principle of least privilege (also known as the principle of minimal privilege or the principle of least authority) requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose. Consider deploying Privilege Access Management security products that offer a time-based secure way to access a system as a super-user and provide ability to authorize and monitor all privileged users’ interactions with the systems.

IMPLEMENT REGULAR BACKUPS WITH TESTED RESTORE PROCEDURE

The last line of defense when everything fails against ransomware is how good the backup and restore policies are. The whole notion of ransomware is “you have something that is valuable to you, let’s hold it hostage and the fear of losing it forever will make you pay the ransom to get it back.” When organizations have a good back up policy, it removes the leverage adversaries have.

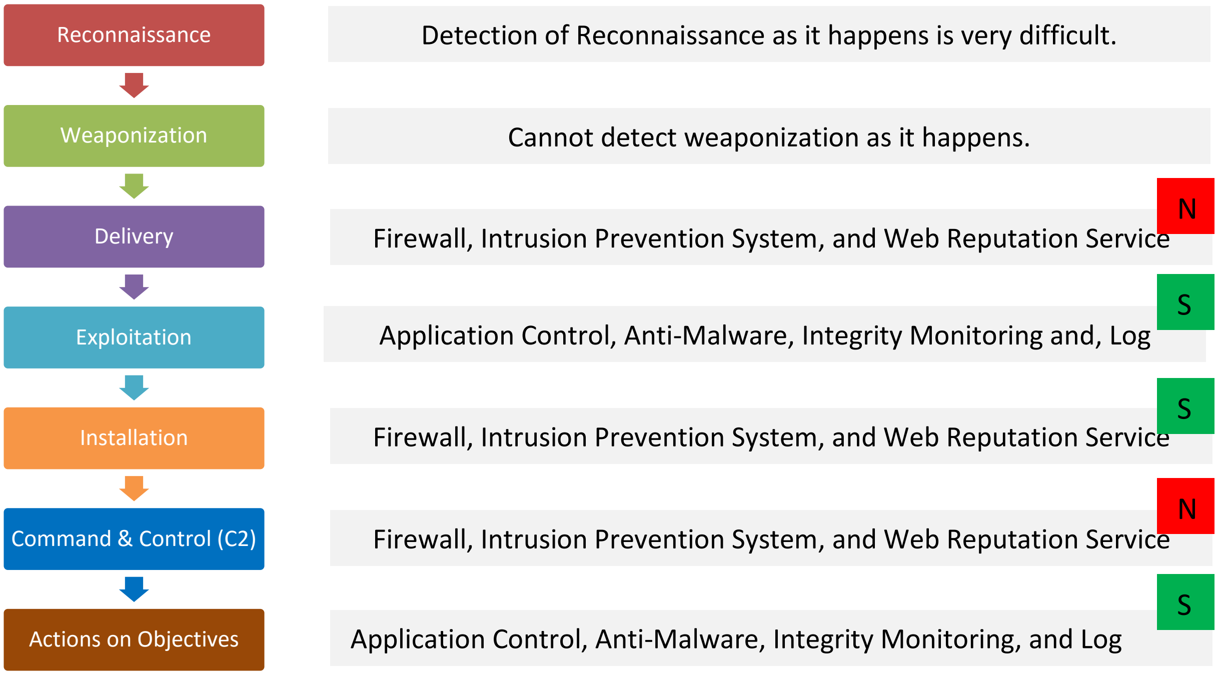
This blog outlines the 3-2-1 rule when doing backups: create 3 backup copies on 2 different media with 1 backup offsite. Some ransomware variants have been known to go after backup data found on a shared network drive, which makes it important to set up a backup on a separate location, such as drives on a system that isn't connected to the company network.

Deploy Layered Security Controls Using Deep Security

The Lockheed Martin Cyber Kill Chain framework is a great resource to understand what adversaries must do in order to achieve their objectives. This framework can also outline how to deploy the layered security controls available through Deep Security.

For any attack (ransomware or others) the adversaries must complete 1 to 6 stages. If adversaries are stopped at any stage of their attack then it is considered successful. The first two stages (Reconnaissance and Weaponization) are hard to defend against and beyond the scope of this paper, however the security controls available with Deep Security™ are mapped against the next five stages of this chain to help create a defense-in-depth strategy.

In the diagram below on the right each stage is labelled with either N (network level) or S (system level) which represents the opportunity area and segment to defend against ransomware attacks.



Reconnaissance	Detection of Reconnaissance as it happens is very difficult.	
Weaponization	Cannot detect weaponization as it happens.	
Delivery	Firewall, Intrusion Prevention System, and Web Reputation Service	N
Exploitation	Application Control, Anti-Malware, Integrity Monitoring and, Log	S
Installation	Firewall, Intrusion Prevention System, and Web Reputation Service	S
Command & Control (C2)	Firewall, Intrusion Prevention System, and Web Reputation Service	N
Actions on Objectives	Application Control, Anti-Malware, Integrity Monitoring, and Log	S

FIGURE 4 - LOCKHEED MARTIN CYBERKILL CHAIN STAGES MAPPED TO DEEP SECURITY CONTROLS

Network Security Controls

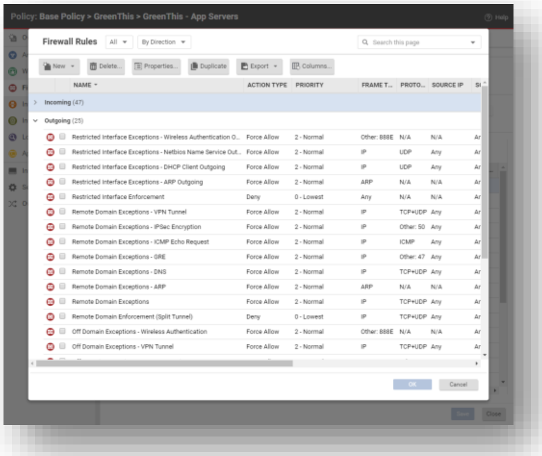
CREATE NETWORK SEGMENTATION

Network segmentation is an effective security practice that can help prevent adversaries from carrying out their ransomware attacks. When an adversary gains access to a system, the network segmentation or as we call it "zones" will limit their further movement across the network. There are industry standards available which provide guidance on creating a clear separation of data within the network. Splitting the network into multiple zones, with specific security requirements, and then enforcing firewall policy on what is allowed to move from zone to zone makes the adversary's job extremely difficult. The Deep Security Firewall control creates logical network segments at the host level without requiring rewiring and touching network devices.

Deep Security: Firewall Recommendations >>

PROHIBITIVE MODE VS. PERMISSIVE MODE

The Deep Security Firewall control is a host-based stateful firewall which can be used in either "Prohibitive mode" when "allow rules" are used in the policy or "Permissive mode" when "deny rules" are used exclusively in the policy. Using Firewall in "Permissive mode" is not recommended since any traffic that is not matching a "deny rule" will be allowed. It is recommended to create a firewall policy with "allow rules" for the traffic that is needed for the system to function properly and let the implicit "deny rules" restrict all the other traffic not matching the "allow" firewall rules.



	NAME	ACTION TYPE	PRIORITY	FRAME T...	PROTO...	SOURCE IP	SI
Incoming (47)							
Outgoing (25)							
	Restricted Interface Exceptions - Wireless Authentication O...	Force Allow	2 - Normal	Other: 888E	N/A	N/A	Ar
	Restricted Interface Exceptions - Netbios Name Service Out...	Force Allow	2 - Normal	IP	UDP	Any	Ar
	Restricted Interface Exceptions - DHCP Client Outgoing	Force Allow	2 - Normal	IP	UDP	Any	Ar
	Restricted Interface Exceptions - ARP Outgoing	Force Allow	2 - Normal	ARP	N/A	N/A	Ar
	Restricted Interface Enforcement	Deny	0 - Lowest	Any	N/A	N/A	Ar
	Remote Domain Exceptions - VPN Tunnel	Force Allow	2 - Normal	IP	TCP+UDP	Any	Ar
	Remote Domain Exceptions - IPSec Encryption	Force Allow	2 - Normal	IP	Other: 50	Any	Ar
	Remote Domain Exceptions - ICMP Echo Request	Force Allow	2 - Normal	IP	ICMP	Any	Ar
	Remote Domain Exceptions - GRE	Force Allow	2 - Normal	IP	Other: 47	Any	Ar
	Remote Domain Exceptions - DNS	Force Allow	2 - Normal	IP	TCP+UDP	Any	Ar
	Remote Domain Exceptions - ARP	Force Allow	2 - Normal	ARP	N/A	N/A	Ar
	Remote Domain Exceptions	Force Allow	2 - Normal	IP	TCP+UDP	Any	Ar
	Remote Domain Enforcement (Split Tunnel)	Deny	0 - Lowest	IP	TCP+UDP	Any	Ar
	Off Domain Exceptions - Wireless Authentication	Force Allow	2 - Normal	Other: 888E	N/A	N/A	Ar
	Off Domain Exceptions - VPN Tunnel	Force Allow	2 - Normal	IP	TCP+UDP	Any	Ar

INGRESS AND EGRESS FIREWALL RULES

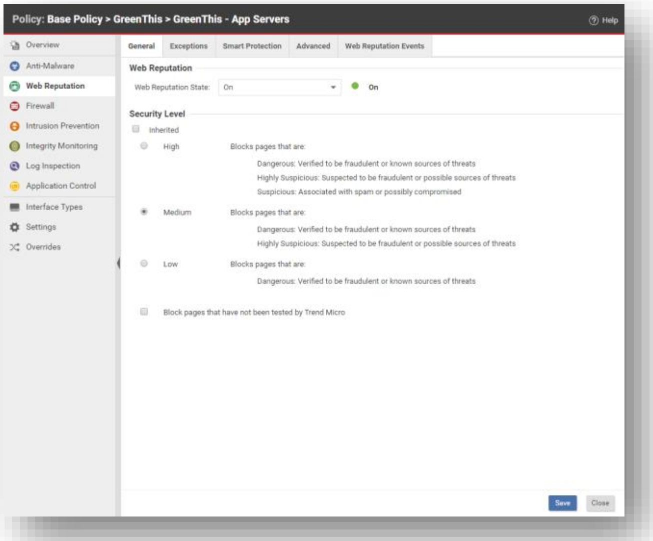
Once a system is infected with ransomware, it needs to reach out to a command and control (C&C) server under adversary control to receive more instructions or download payload. This is where the Deep Security Firewall control can be used to implement egress firewall rules to detect and block C2 traffic. It is a common practice to have an "ingress" firewall policy and restrict allowed ports and communication protocols to reduce the attack surface. It is equally important to create an "egress" firewall policy, especially for servers. For example, if an "egress" firewall rules policy is created for servers that limits the ports, protocols, and communications in the network, any ransomware that tries to use protocols like IRC, NTP, FTP, ICMP etc., to communicate back with C&C servers will be blocked automatically if they're not specifically covered by the "allow" firewall rules. The objective of the firewall policy should be to block open ports and services that are not needed and this will help weed out some ransomware families relying on such protocols and services.

Filter Out Malicious Web Urls

Adversaries must drop ransomware to the victims and one of the infection vectors they use is “drive-by-downloads”. A lot of ransomware infects through drive-by downloads, where visiting a compromised website with an unpatched or outdated browser or software plug-in can infect a machine. These compromised website hosts the exploit kit which in turn runs malicious code when a user visits the website, and checks for known vulnerabilities in the system. This is how adversaries can discover a vulnerability that can be exploited and drops the ransomware.

Deep Security: Web Reputation Service Recommendations >>

By enabling a Web Reputation Service Module in Deep Security, protection can be added against web threats by blocking access to malicious URLs. Deep Security uses Trend Micro's web security threat intelligence from the Trend Micro ™ Smart Protection Network™ to check the reputation of websites. The website's reputation is correlated with the specific Web reputation policy enforced on the computer.



Web Reputation

Web Reputation State: On ● On

Security Level

□ Inherited

○ High Blocks pages that are:
Dangerous: Verified to be fraudulent or known sources of threats
Highly Suspicious: Suspected to be fraudulent or possible sources of threats
Suspicious: Associated with spam or possibly compromised

● Medium Blocks pages that are:
Dangerous: Verified to be fraudulent or known sources of threats
Highly Suspicious: Suspected to be fraudulent or possible sources of threats

○ Low Blocks pages that are:
Dangerous: Verified to be fraudulent or known sources of threats

□ Block pages that have not been tested by Trend Micro

Depending on the Web Reputation Security Level being enforced, Deep Security will either block or allow access to the URL.

Furthermore, on servers, where outbound communication to specific URLs is typically known or put together with much less effort than an end user system, access can be restricted to specific domains that the server is allowed to talk to. For example, specific updates to servers receive patches etc., by using an “Allowed” and “Blocked” list exception in combination, which supports wild cards to make filtering string easier.

Use Network Intrusion Prevention and Detection System

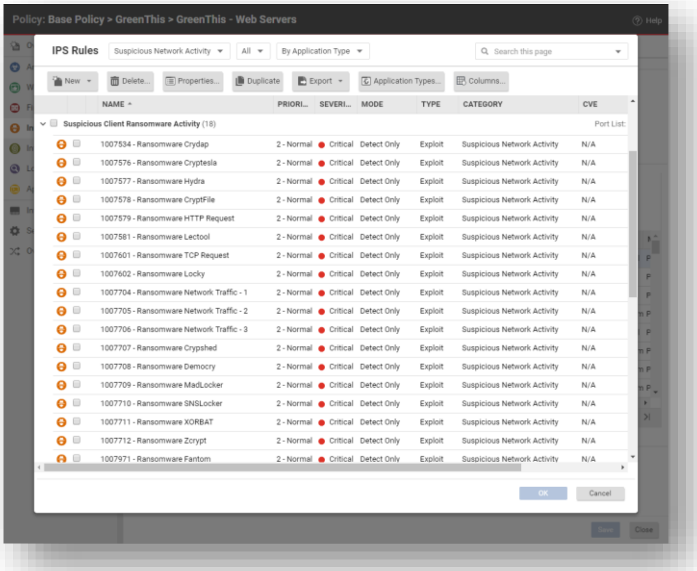
To add further difficulty for adversaries, it is recommended to use an Intrusion Prevention System and inspect the allowed traffic for vulnerabilities and exploits before they reach applications. Traffic allowed for business operations to continue must be confirmed and the application is expected to receive and this is where Deep Security Intrusion Prevention System can be used, which inspects and blocks inbound, outbound, and lateral network traffic in real-time for known, unknown, and zero-day vulnerabilities. For example, any HTTPS packet that comes in on port 443 can be allowed, but if a non-HTTPS packets like SSH comes over this allowed port it can be blocked by Deep Security IPS control since it violates the protocol, hence enforcing protocol behavior.

Deep Security: Intrusion Prevention System Recommendations >>

Run Recommendation Scan Regularly

Figuring out what Intrusion Prevention Rules must be assigned to the system can be a daunting task even for a security professional. We recommend leveraging the Deep Security Recommendation Scan feature which help extract the complexity. During a Recommendation Scan, Deep Security will scan operating system details, such as installed applications on the system, running processes, and services and correlate this information with the vulnerabilities that the system is exposed to. Then, it can either assign the recommended rules automatically or let then be reviewed and assigned. This process should be automated to ensure the context-aware and appropriate protection is assigned. There are two ways to achieve this:

- Leverage the scheduling feature which allows for defining a schedule
- Use “on-going recommendation” scan feature



Policy: Base Policy > GreenThis > GreenThis - Web Servers

IPS Rules — Suspicious Network Activity — All — By Application Type

Suspicious Client Ransomware Activity (18) — Port List:

NAME	PRIORI...	SEVERI...	MODE	TYPE	CATEGORY	CVE
1007534 - Ransomware Crydap	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007576 - Ransomware Cryptesla	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007577 - Ransomware Hydra	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007578 - Ransomware CryptFile	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007579 - Ransomware HTTP Request	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007581 - Ransomware Lectool	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007601 - Ransomware TCP Request	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007602 - Ransomware Locky	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007704 - Ransomware Network Traffic - 1	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007705 - Ransomware Network Traffic - 2	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007706 - Ransomware Network Traffic - 3	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007707 - Ransomware Crypshed	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007708 - Ransomware Democry	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007709 - Ransomware MadLocker	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007710 - Ransomware SNSLocker	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007711 - Ransomware XORBAT	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007712 - Ransomware Zcrypt	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A
1007971 - Ransomware Fantom	2 - Normal	● Critical	Detect Only	Exploit	Suspicious Network Activity	N/A

This blog shows how recommendation scan works.

Note: It is also important to understand that not all IPS rules will be auto-assigned or recommended, so in some cases the administrator must assign rules manually. The exceptions are:

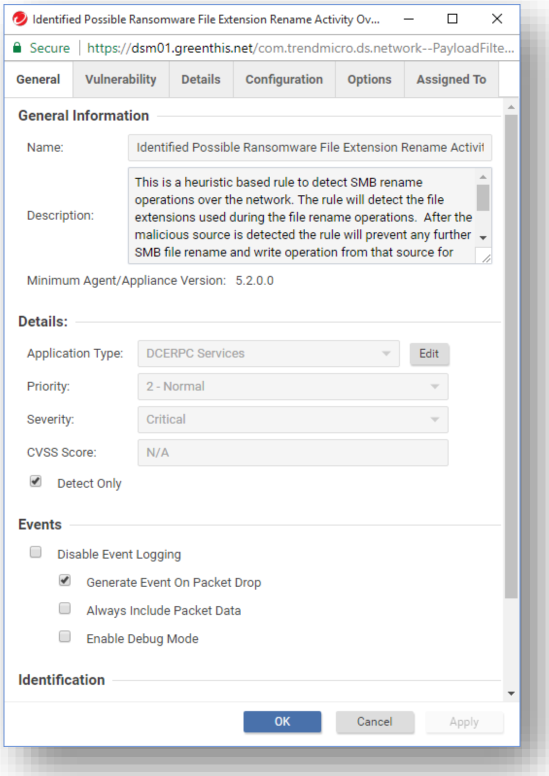
- Rules that require configuration before they can be applied.
- Rules that have been automatically assigned or unassigned based on a previous recommendation scan but which a user has overridden. For example, if Deep Security automatically assigns a rule and then it subsequently gets unassigned, the rule will not get reassigned after the next recommendation scan.
- Rules that have been assigned at a higher level in the policy hierarchy cannot be unassigned at a lower level. A rule assigned to a computer at the policy level must be unassigned at the policy level.
- Rules that Trend Micro has issued but which may pose a risk of producing false positives. (This will be addressed in the rule description.)

Assign Ransomware Rules for Command & Control, Network Share Protection, and Suspicious Network Activity

To detect ransomware activity, ransomware rules should be assigned to detect command-and-control traffic (C&C), identify lateral movement activity with suspicious network activity rules, and further protect network shares from getting infected when ransomware tries to reach out from a victim's system to file shares. Trend Micro™ Deep Security™ provides the following Intrusion Prevention rules which specifically address the ransomware technique of encrypting files on mounted shares (Windows or Linux – Samba).

- Rule name: 1007596 - Identified Suspicious File Extension Rename Activity Over Network Share

This rule provides visibility into ransomware activity but in most cases does not prevent ransomware encryption activity. This rule monitors for known techniques that ransomware uses in changing file extensions (e.g. .zzz, .encryptedRSA, .crypt etc.). There's a check for ~50 file extensions in the rule. The rule also provides an option to exclude and include certain file extensions to maximize the benefits of this rule.


Identified Possible Ransomware File Extension Rename Activity Ov...
Secure
https://dsm01.greenthis.net/com.trendmicro.ds.network--PayloadFilte...
General
Vulnerability
Details
Configuration
Options
Assigned To
OK
Cancel
Apply
Edit

General Information

Name: Identified Possible Ransomware File Extension Rename Activit

Description: This is a heuristic based rule to detect SMB rename operations over the network. The rule will detect the file extensions used during the file rename operations. After the malicious source is detected the rule will prevent any further SMB file rename and write operation from that source for

Minimum Agent/Appliance Version: 5.2.0.0

Details:

Application Type: DCERPC Services

Priority: 2 - Normal

Severity: Critical

CVSS Score: N/A

☑ Detect Only

Events

☐ Disable Event Logging

☑ Generate Event On Packet Drop

☐ Always Include Packet Data

☐ Enable Debug Mode

Identification

Malware Prevention & System Security Controls

Use Definition and Behavior Based Anti-Virus

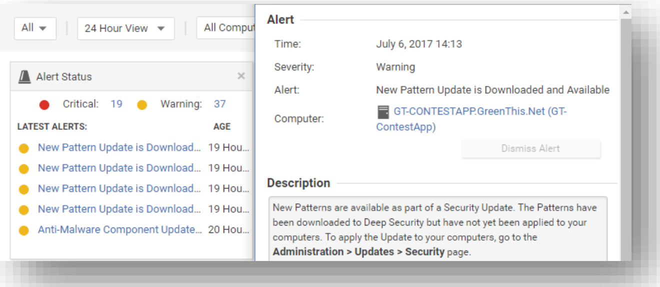
Definition-based or signature-based anti-malware solutions can help identify the ransomware when it is known and stop the ransomware attack at the time of delivery.

What about the zero-day attacks where the signature is not known or adversaries use techniques like polymorphic or encrypted code segments, difficult to detect and create a hashed signature for? This is where a "behavior-based" anti-malware solution can help and stop the ransomware at the time of exploitation. Exploitation is the next stage the adversary will take to successfully conduct the ransomware attack. The behavior-based anti-malware solutions looks for characteristics of malware execution against a list of known malicious behaviors. For example, a document being opened in an email that invokes JavaScript or Adobe Flash could be viewed as "highly suspicious behavior."

Deep Security: Anti-Malware Recommendations >>

Ensure Patterns and Deep Security Rules are Current

The effectiveness of any security solution is only as good as the update it has, so keeping the anti-malware patterns and Deep Security rule updates current is very critical. Using the Deep Security Scheduling feature, schedules can be defined to check and roll out updates to the system. The speed at which the system will receive updates is also important to ensure the exposure window is kept to a minimum. It's critical to carefully plan the number of Deep Security relay deployments and their assignment to agents to provide quick roll outs.



Alert Status

● Critical: 19 ● Warning: 37

LATEST ALERTS:	AGE
● New Pattern Update is Download...	19 Hou...
● New Pattern Update is Download...	19 Hou...
● New Pattern Update is Download...	19 Hou...
● New Pattern Update is Download...	19 Hou...
● Anti-Malware Component Update...	20 Hou...

Alert

Time: July 6, 2017 14:13
Severity: Warning
Alert: New Pattern Update is Downloaded and Available
Computer: GT-CONTESTAPP.GreenThis.Net (GT-ContestApp)

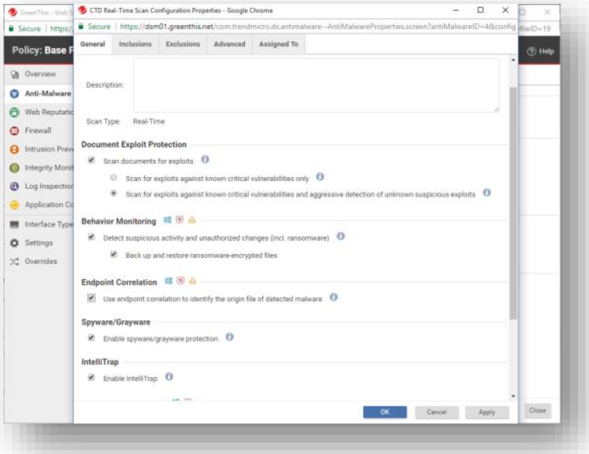
Description

New Patterns are available as part of a Security Update. The Patterns have been downloaded to Deep Security but have not yet been applied to your computers. To apply the Update to your computers, go to the **Administration > Updates > Security** page.

In addition, Deep Security provides dashboard widget, alerts, and reporting capabilities to help identify where in the environment the protection status is out of date and requires immediate attention.

Enable Behavioral Monitoring

As previously discussed, the role of behavior-based anti-malware solutions is critical to defending against ransomware attacks when other lines of defense have been compromised. Malware writers can use malicious code to hook into user mode processes in order to gain privileged access to trusted processes and to hide the malicious activity.



CTD Real-Time Scan Configuration Properties - Google Chrome

Secure | https://dsm01.greenthis.net/com.trendmicro.ds.antimalware--AntiMalwareProperties.screen?antiMalwareID=4&config fileID=19

Description:

Scan Type: Real-Time

Document Exploit Protection

☑ Scan documents for exploits
○ Scan for exploits against known critical vulnerabilities only
● Scan for exploits against known critical vulnerabilities and aggressive detection of unknown suspicious exploits

Behavior Monitoring

☑ Detect suspicious activity and unauthorized changes (incl. ransomware)
☑ Back up and restore ransomware-encrypted files

Endpoint Correlation

☑ Use endpoint correlation to identify the origin file of detected malware

Spyware/Grayware

☑ Enable spyware/grayware protection

IntelliTrap

☑ Enable IntelliTrap

Malware writers inject code into user processes through DLL injection, which calls an API with escalated privileges. They can also trigger an attack on a software exploit by feeding a malicious payload to trigger code execution in memory. In Deep Security, the behavior monitoring functionality monitors for processes that may be performing actions that are not typically performed by a given process. Using a number of mechanisms, including Data Execution Prevention, Structured Exception Handling Overwrite Protection, and heap spray prevention, Deep Security can determine whether a process has been compromised and then terminate the process to prevent further infection.

Configure Network Sandboxing (Optional)

Though this is marked as optional, it is highly recommended to combat techniques to bypass malware detection attacks that are targeted specifically at an organization. Deep Security provides enhanced malware protection for new and emerging threats through its Connected Threat Defense feature, where it uses heuristic detection to analyze files on the protected computer and determines whether they are suspicious. Please note, the Connected

Threat Defense feature would require additional components, such as Trend Micro Control Manager and Trend Micro™ Deep Discovery™ Analyzer.

Implement Application Whitelisting

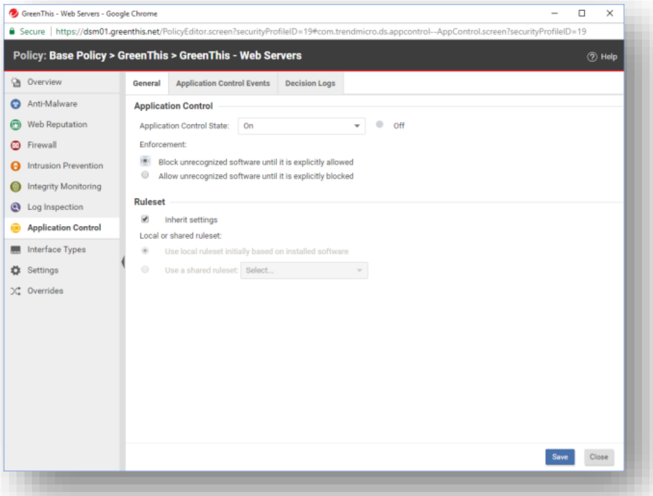
Behavior monitoring keeps "anomalies" or unusual system activities at bay, while application control only allows a list of non-malicious routines, files, and processes to run on the system. This helps to determine which application and programs are allowed to function and operate within the organization's network. Deep Security's application control security module looks for software files when examining the initial installation and monitors for change. There is a vast list of software that includes windows applications (.exe, .dll, .com etc.), linux applications (.so and other compiled binaries) the compiled byte code (.jar, .class) scripts (phython, shell and php etc.,) and windows scripts (Powershell, .vbs, .js etc.,). Adding application control to a defense-in-depth strategy will greatly reduce adversaries' ability to execute malware on the system.

Deep Security: Application Control Recommendations >>

Deploy in "Block Mode" for Best Protection

The application control security module in Deep Security offers two modes of operation, each mode tracks for changes and reports it back, but whether to allow or block the execution of the specific software depends on what mode it is set for, either "Allow" or "Block." It is recommended to switch to block mode once initial vetting is done and the system is promoted to production.

After that, the Deep Security Agent continuously monitors the computer for changes. Application control is integrated with the kernel (on Linux computers) and file system, so it has permissions to monitor the whole computer, including software installed by root or administrator accounts.



GreenThis - Web Servers - Google Chrome

Secure | https://dsm01.greenthis.net/PolicyEditor.screen?securityProfileID=19#com.trendmicro.ds.appcontrol--AppControl.screen?securityProfileID=19

Policy: Base Policy > GreenThis > GreenThis - Web Servers

Application Control

Application Control State: On ○ Off

Enforcement:

● Block unrecognized software until it is explicitly allowed

○ Allow unrecognized software until it is explicitly blocked

Ruleset

☑ Inherit settings

Local or shared ruleset:

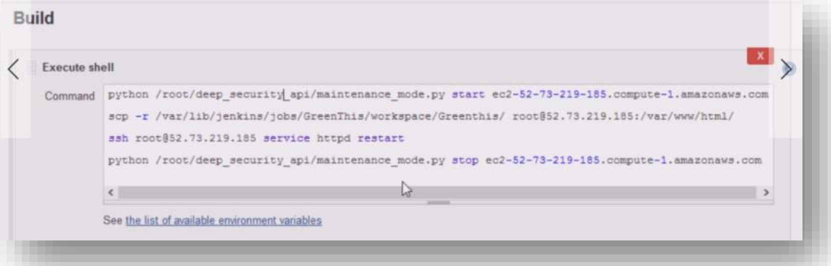
● Use local ruleset initially based on installed software

○ Use a shared ruleset: Select...

The agent watches for disk write activity on executable files, and for attempts to execute software. To determine if the software is new or has changed, it compares the file with the hashes of the initially installed software.

Leverage the "Maintenance Mode" Capabilities of Application Control

When patches are installed, software is upgraded, or web applications are deployed, application control will detect them. Depending on the setting for how to handle unrecognized software, this could block that software until it is specifically allowed from the web console. For mission-critical software, this service interruption may not be acceptable.



```
python /root/deep_security_api/maintenance_mode.py start ec2-52-73-219-185.compute-1.amazonaws.com
scp -r /var/lib/jenkins/jobs/GreenThis/workspace/Greenthis/ root@52.73.219.185:/var/www/html/
ssh root@52.73.219.185 service httpd restart
python /root/deep_security_api/maintenance_mode.py stop ec2-52-73-219-185.compute-1.amazonaws.com
```

See the list of available environment variables

To avoid extra down time and alerts during deployment and maintenance windows, application control can be put into a mode designed for maintenance windows. While maintenance mode is enabled, application control will continue to block blacklisted software, but it will allow new or updated software to run and automatically add it to the allow rules.

The maintenance mode feature of application control is available via rest APIs to allow Deep Security functionality to be integrated with other applications or in the CICD pipeline. At the time of update, maintenance mode can be switched on via a simple API call and then turned off, achieving a balance between security and usability.

Look for Indicators of Compromise Using Integrity Monitoring

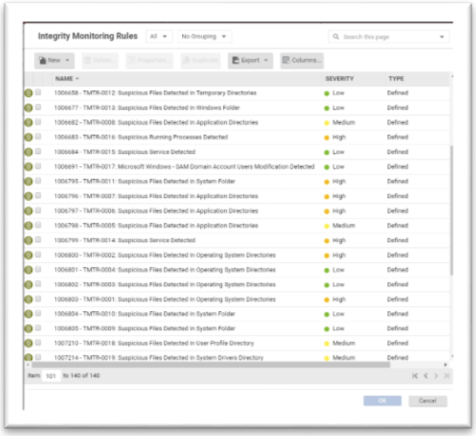
To continue to ensure the integrity of the system is not compromised from the "trusted computing base" that has been created by hardening the system and deploying other security controls, it is equally important to deploy integrity monitoring to detect changes to files and critical system areas like the Windows registry that could indicate suspicious activity.

Deep Security: Integrity Monitoring Recommendations >>

Deep Security's integrity monitoring module can monitor various areas of the system, such as file, software, port, process, registry, services, users, and WQL. Ransomware and other malware typically infects a system by modifying certain registry keys and various system files. The default Deep Security rules allow for monitoring of the integrity of a machine by observing what is most commonly changed by malware in an infected system.

It is recommended to:

- Leverage the Recommendation Scan feature as discussed earlier to discover the recommended integrity monitoring rules for the system.



NAME	SEVERITY	TYPE
1006658 - TMTR-0012: Suspicious Files Detected In Temporary Directories	● Low	Defined
1006677 - TMTR-0013: Suspicious Files Detected In Windows Folder	● Low	Defined
1006682 - TMTR-0008: Suspicious Files Detected In Application Directories	● Medium	Defined
1006683 - TMTR-0016: Suspicious Running Processes Detected	● High	Defined
1006684 - TMTR-0015: Suspicious Service Detected	● Low	Defined
1006691 - TMTR-0017: Microsoft Windows - SAM Domain Account Users Modification Detected	● Low	Defined
1006795 - TMTR-0011: Suspicious Files Detected In System Folder	● High	Defined
1006796 - TMTR-0007: Suspicious Files Detected In Application Directories	● High	Defined
1006797 - TMTR-0006: Suspicious Files Detected In Application Directories	● High	Defined
1006798 - TMTR-0005: Suspicious Files Detected In Application Directories	● Medium	Defined
1006799 - TMTR-0014: Suspicious Service Detected	● High	Defined
1006800 - TMTR-0002: Suspicious Files Detected In Operating System Directories	● High	Defined
1006801 - TMTR-0004: Suspicious Files Detected In Operating System Directories	● Low	Defined
1006802 - TMTR-0003: Suspicious Files Detected In Operating System Directories	● Low	Defined
1006803 - TMTR-0001: Suspicious Files Detected In Operating System Directories	● High	Defined
1006804 - TMTR-0010: Suspicious Files Detected In System Folder	● Low	Defined
1006805 - TMTR-0009: Suspicious Files Detected In System Folder	● Low	Defined
1007210 - TMTR-0018: Suspicious Files Detected In User Profile Directory	● Medium	Defined
1007214 - TMTR-0019: Suspicious Files Detected In System Drivers Directory	● Medium	Defined

Item 101 to 140 of 140

- Assign rules that are written to detect specific known malicious indicators of an attack or a compromise. Ex: Rule with TMTR-xxxx string in the name that are written to provide IOC.

Unless new software or a security patch is installed, there is no reason why any of these files should be modified. If such an event is raised, the administrator can check what is happening on the machine to determine whether or not it is compromised.

It is also possible to create custom rules to monitor specific threats. If a user knows the behavior of a particular virus they are trying to contain in an environment, they can create a special monitoring rule that checks for certain registry keys or files created by the virus. This can determine if the spread of the virus is being contained.

CONCLUSION

This paper covered a brief history and evolution of ransomware. It highlighted how crypto ransomware works and creates a successful revenue-generated business model for adversaries. It outlined how our adversaries have moved from selling misleading software to a pure ransom model, which is inarguably the most dominant threat these days. It discussed what steps an adversary needs to execute to successfully conduct an attack based on the Lockheed Cyber Kill Chain framework. It then discussed, that despite the continuous improvement in its encryption, deletion, and communication methods, it is possible to design a layered defense strategy that can stop a large number of ransomware attacks. It also outlined general best practices for security and listed specific security controls and the recommendations around them that Deep Security can offer to help design a defense-in-depth strategy.

Find out more about how Deep Security can help secure your enterprise servers:
www.trendmicro.com/hybridcloud

REFERENCES

- https://help.deepsecurity.trendmicro.com/Deep_Security_10_0_Best_Practice_Guide.pdf
- https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-all-in-one-solutions-guide
- https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-101-what-it-is-and-how-it-works
- https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/
- http://blog.trendmicro.com/trendlabs-security-intelligence/world-backup-day-the-3-2-1-rule/
- https://www.trendmicro.de/cloud-content/us/pdfs/business/white-papers/wp_lower-security-risks-costs-with-virtual-patching.pdf
- http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/Gaining_the_Advantage_Cyber_Kill_Chain.pdf
- https://nvd.nist.gov/ncp/repository
- https://learn.cisecurity.org/benchmarks
- https://en.wikipedia.org/wiki/Principle_of_least_privilege

Securing Your Journey to the Cloud

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.