A note on different types of ransomware attacks

Mihail Anghel, Andrei Racautanu, email: racautanu.andrei.nicolae@info.uaic.ro
Computer Science Faculty, “Al. I. Cuza” University, Iasi, Romania

Abstract

Ransomware are malware whose purpose is to generate income for the attacker. The first of these malware made intense use of cryptography, specifically for file encryption. They encrypt some or most files on the computer before asking a ransom for the decryption. Since they appeared, however, ransomware have evolved into different types which fulfill their task in different ways. Some encrypt files and data from the hard drive, others block access to the OS or use private user data to blackmail the user, some aren’t even a real threat, but they scare the user into paying for some fake service or software. The software security industry is well aware of these threats and is constantly analyzing the new versions and types to determine how dangerous they are and to provide an updated protection solution. This article tries to investigate and compare the way these malware work and how they affect the victims computer. Our analysis will provide interesting insight into how they work, it will highlight the particularities of ransomware and will give some information about why some of these malware are more dangerous than others.

Keywords: *ransomware, analysis, infection, crypto-ransomware, locker-ransomware*

1. Introduction

Ransomware is the name of a class of malware. The name is made out of two words, ransom and malware, thus following the way they work: they are malware that demand payment for stolen functionality, stolen personal data/information or data that the user’s access has been restricted to. The first ransomware relied on encrypting information on the victim’s computer to demand payment for the key or software to decrypt the data. Today, these malware have diversified in the way they extort money from the victim. One could argue that ransomware is a simple form of blackmail that is used for mass extortion, being wild-spread to many users and it is only made more efficient by the growing popularity and adoption of cryptocurrencies, which warrant the anonymity of transactions. What are the differences in the behaviors of the different classes of ransomware? What do they change on the victim computer? What means do they use to extort money and what makes them efficient? These are some of the points that will touch in this article. The first section will cover the main types of ransomware, section 2 will explain what happens during an attack and point out ransomware families that operate in that manner and section 3 will go over ways that can help mitigate ransomware. The paper is concluded in section 4.

1.1. Encrypting ransomware

This class of malware, once executed, silently searches for and encrypts valuable files on the victim’s machine. After the first step is completed, a message is displayed to the user that asks for a ransom in return of the hidden files. Detailed instructions are presented to the user, sometimes, even a call center number is provided.

After the ransom is payed, the victim will be given either a key or code for the decryption of the files, or an executable file that is created specifically to decrypt the files on that victim’s machine. Examples of typical crypto-ransomware include CryptoWall, CryptoLocker, WannaCry and Locky.

1.2. Non-encrypting ransomware

Typically, these types of ransomware use means of locking or locking access to the target machine and demanding a ransom or asking for a user action that ends up costing money to unlock.

To make the users pay the ransom, some of these malware either ask their victims for payment up front, while others rely on deceit (ex. Ask the user to call a high rate phone number and presenting the call as free.). Examples of typical locker-ransomware include Winlocker and Reveton.

1.3. Leakware (also called Doxware)

This class of malware differ from the ones presented above in that they don't block access to the victim's machine or any information that it is stored on it. Rather, it silently collects sensitive information from the machine and uses it to blackmail the victim.

The information gathered is stored on servers or other infected machines and the attacker threatens the victim that the data will be published if payment is not made.

1.4. Mobile ransomware

These ransomware target mobile devices (phones, tablets, etc). Because, usually, the information is easy to back up and restore to and from the cloud or any back-up solution, these malware act as blockers, with little incentive to encrypt data. Thus, unlike regular locker malware, they rely on the value of the mobile device rather for the ransom, rather than on the information that is saved on it.

Once these malware are installed or ran on the victim machine, some attempt to display a blocking message on top of the UI, while others use a form of click high-jacking to cause the user to allow it higher privileges.

2. Analysis of a ransomware attack

2.1. Ransomware Behavior

Ransomware have been classified as a malware subcategory. As such, they have a number of common traits to other malware. These traits can be organized under six categories:

- Payload persistence – the attack is carried out all the way; usually done through placing an executable in the startup folder, scheduling a task on startup or registering a startup item in the registry
- Anti-system restore – prevent system restore from rolling back the changes; usually done by deleting shadow copy saves
- Stealth techniques – malware will try to run in a stealthy manner to avoid detection; usually done by injecting code into legitimate processes, running from AppData or naming executables after other Windows processes
- Environment mapping – some ransomware analyze the system they infected; this is done to determine the value of the target, other possible targets (over the network) and if it's running on a real computer or on a sandbox environment that could be attempting to analyze it
- Network traffic – most ransomware require an internet connection; they use it for downloading the payload related files and/or for the communication of the encryption key
- Privilege elevation – using elevated privileges carry out the attack; sometimes, simply asking for administrator access may work or other privilege escalation techniques may be used, like click high-jacking

2.2 Components of a ransomware attack

2.2.1. The start of the infection

The first phase of a ransomware attack is the installation of the components that are used to infect, encrypt, or lock the system. For the malware files to get to the victim computer, a few methods are used:

drive-by download – occurs when a system automatically downloads a piece of malware or spyware without the end user's knowledge

strategic web compromise (subset of a drive-by download) **–** strategic web compromises are also called *watering-hole attacks*. These rely on strategic reconnaissance of the end users, and are often reserved for more specific targeted attacks

phishing emails – may be spam or specially crafted to specific an organization or industry. These emails can include attachments or provide links to malicious websites

exploiting vulnerabilities in internet or network accessible systems – scanning networks or scanning the internet for vulnerable systems and infecting them without any need for user input

Table 1: Different ransomware families, their propagation strategy(deployment), date appeared, cryptographic techniques used to encrypt files and the command and control methods. [1]

Families	Deployment	Date Appeared	Cryptographic Techniques	Command and Control
Reveton	Drive-by downloads	2012	RSA and DES	MoneyPak
GpCode	Email Attachments	2013	660-bit RSA and AES	Tor Network
CryptoLocker	Compromised websites and Email Attachments	2013	2048-bit RSA	Tor Network
CryptoWall	Compromised websites and Email Attachments	2013	2048-bit RSA	Tor Network
FileCrypto	Compromised websites and Email Attachments	2013	2048-bit RSA	Tor Network
TeslaCrypt	Compromised websites and Email Attachments	2013	2048-bit RSA	Tor Network
CTB-Locker	Email Attachments	2014	ECC	Onion Network
Shade	Spam Email	2015	RSA-3072 and AES-256	Fixed Server
Jigsaw	Word Document with Javascript	2016	RSA and AES	Onion Network
WannaCry	Samba Vulnerability	2017	RSA and AES	Onion Network

2.2.2. Installation

Once the malicious payload has been delivered to the victim system, the infection begins. The infection is delivered in a variety of ways, no matter what the target system is. In many cases, the effective modern variants of crypto-ransomware first will leverage some form of macro virus or exploited PDF to get onto the system; they also have been known to use JS, Java and Adobe Flash. Once the malware has been downloaded to the system, it will execute its embedded code and then begin to analyze the system to determine if it is running on a real machine or in a virtual sandbox.

The second stage begins if the ransomware determines that it is in a machine worth infecting. Often disguised as a standard Windows process, the malware will chose a unique identifier like a Mac address to be easily identified by its server.

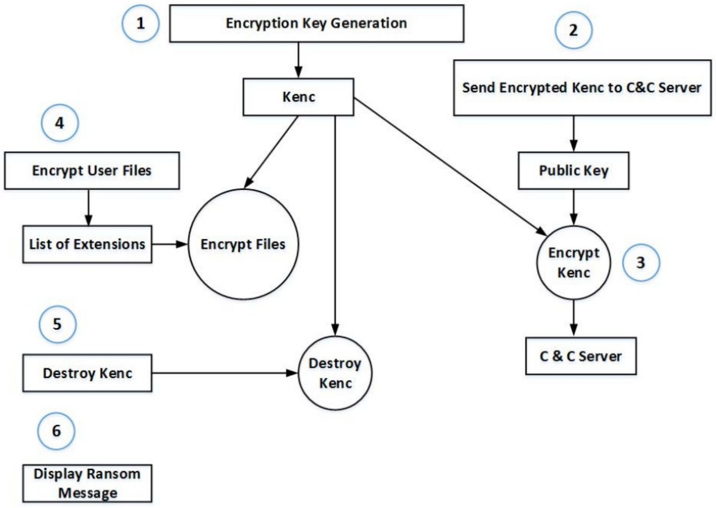
The next stage begins once the ransomware has established itself in a common Windows process like svchost.exe or lsass.exe and it will begin the command-and-control phase.

2.2.3. Command-and-Control

After the malicious code is fully deployed, it will try to contact its command servers, asking for instructions. These instructions can include everything from identifying the types of files they should target for encryption, to how long they should wait to begin the process and whether they should continue to spread prior to beginning the process. Some ransomware variants will also report back a significant amount of system information, including IP address, domain name, operating system, installed browsers and anti-malware software.

Handshake and key exchange

Fig. 1: General crypto-ransomware key lifecycle [1]



The malicious code that is now running on the victim's computer is a client that is commanded by a server operated by the criminal attacker. The client will ensure it is communicating with the correct server through a preset handshake protocol. Once the client and server have authenticated to each other, the next step is the key generation and exchange. Some ransomware use weak cyphers while others use complex ones like 4.096-bit RSA. In the case of asymmetric algorithms, only the public key is sent to the client, the private key remains on the attacker's server.

2.2.4.Destruction

This is the moment when the ransomware begins to make significant changes to the target machine, either locks it or starts encrypting the files (Fig 1). In the latter case, all the files that have been identified for encryption after the command stage (can be documents, images, sound files etc) are now getting encrypted. Some malware encrypt not only the files, but also the filenames, making it even more difficult for the victim to know how far the attack has gone or what has been encrypted.

Locking Procedure

In case of a locking ransomware, the success of the attack depends on the locking of the system. This is typically done by creating a new desktop and making it persistent. Ransomware samples simply create a new Desktop environment and eliminate unnecessary processes. The new desktop is the instance that receives input from the victim. Most locking ransomware use similar approaches to establish a persistent desktop lock. Only a small number of malware used a lock banner that is simply downloaded as a HTML page with corresponding images based on the victim's geographical location and is then displayed in full screen in a browser window (typically IE) with hidden controls. The banner plays a law enforcement warning or asks for a payment in the language used in the victim's location. The warning usually says that the operating system is locked due to some law infringement (ex. Windows doesn't have a valid license). Disabling certain keyboard shortcuts such as toggling is automatically done once a new desktop, system key shortcuts are disabled by installing hook procedures that monitor keyboard input events.

Deletion Mechanisms

In this part, we specifically discuss file deletion mechanisms that are unique to ransomware attacks. Some ransomware families do not perform any encryption. Instead, they delete the user's files if the user does not pay the ransom. Certain samples in Gpcode and Filecoder families deleted the original unencrypted file's data after the encryption occurred [2]. They accomplish this by modifying the MFT(Master File Table) to set its non-system file records as being unallocated.

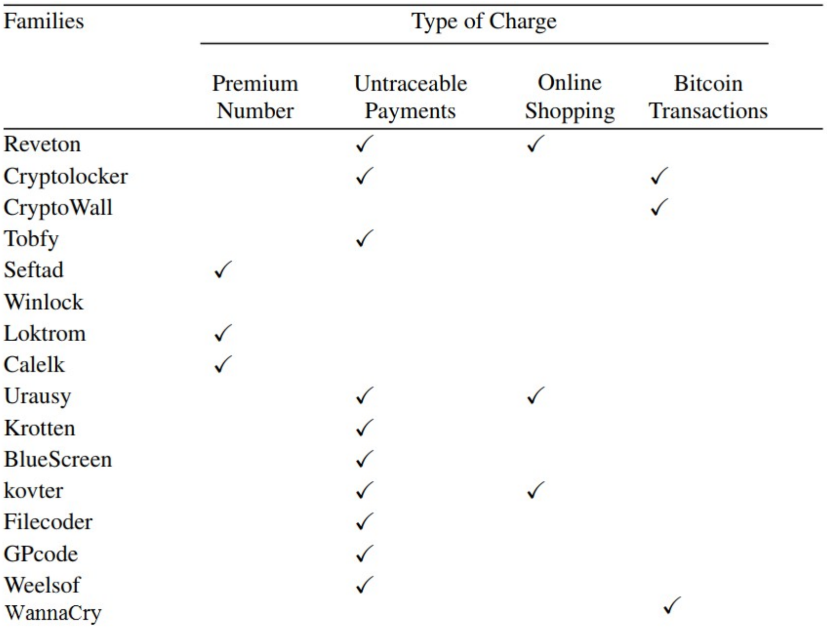
Changing Master Boot Records

Some ransomware families like Seftad or Petya were developed to attack the Master Boot Records (MBR) which contains the executable boot code and the partition table. The MBR is located on the first sector of a hard disk, and it is loaded into memory at boot time when the system transfer control to the code stored in the MBR. Samples that target the MBR prevent the infected system from loading the boot code in the active partition by simply replacing it with a bogus MBR that displays a message asking for a ransom.

2.2.5. Extortion

After the files have been encrypted or the system has been locked, the victim is shown a message that tells them how they have been compromised. The extortion payment can be done in various ways. Also, some ransomware variants will allow the victim to decrypt one file for free to prove that there is a key to the system. Other variants have escalating payments, where the price increases with time.

Table 2: Types of charge used by different ransomware families [2]



Families	Type of Charge			
	Premium Number	Untraceable Payments	Online Shopping	Bitcoin Transactions
Reveton		✓	✓	
Cryptolocker		✓		✓
CryptoWall				✓
Tobfy		✓		
Seftad	✓			
Winlock				
Loktrom	✓			
Calelk	✓			
Urausy		✓	✓	
Krotten		✓		
BlueScreen		✓		
kovter		✓	✓	
Filecoder		✓		
GPcode		✓		
Weelsof		✓		
WannaCry				✓

3. Mitigation Strategies

While ransomware infections are not entirely preventable due to the effectiveness of phishing emails and drive-by downloads from otherwise legitimate sites, users can drastically reduce this risk by implementing cybersecurity strategies and improving threat awareness and security practices. The most effective strategy to mitigate the risk of data loss resulting from a successful ransomware attack is having a comprehensive data backup process in place, however, backups must be stored off the network and their integrity tested regularly. Here is a comprehensive list of recommendations to reduce the risk posed by ransomware infections:

Data Protection

- Off site backups with regular consistency checks
- Online file backup

System Management

- Anti-virus software that is up-to-date
- Automatic updates for the SO, software, plugins, and browsers

- Good user access control
- Application whitelisting
- Turn off unused wireless connections.
- Disable macros on Microsoft Office software.
- Use ad blocking extensions in browsers to prevent “drive-by” infections
- Disable Windows Script Host and Windows PowerShell
- Disable Remote Desktop Protocol, Telnet, and SSH connections. Block inbound traffic to associated ports.
- If remote access is needed, audit access, ensure that login credentials are complex, and implement a 2FA solution to prevent unauthorized access.
- Configure systems by modifying the Group Policy Editor to prevent executables (.exe, .rar, .pdf, exe, .zip) from running in places like appdata, localappdata, temp and the Recycle Bin. CryptoPrevent is a free tool that can help automate this process and prevent ransomware from executing.
- Use web and email protection to block access to malicious websites and scan all emails, attachments, and downloads and configure email servers to proactively block emails containing suspicious attachments such as .exe, .vbs, and .scr.
- Implement a behavior blocker to prevent ransomware from executing or making any unauthorized changes to systems or files.
- Consider utilizing a free or commercially available anti-ransomware tool by leading computer security vendors.

Network Management

- Ensure the firewall is enabled and properly configured
- Close and monitor unused ports
- Block known malicious Tor IP addresses

Mobile Device Management

- For Apple iOS devices: ensure data is backed up on iCloud and two-factor authentication is enabled, only download media from the official stores, and avoid “jailbreaking” the device
- For Android devices: disable the “unknown sources” option in the Android security settings menu, only install apps from the official Google Play store, and avoid "rooting" the device

4. Conclusions

Over the past years, ransomware attacks have become increasingly popular among cybercriminals. This type of malware demands payment for stolen functionality, stolen personal data/information or data that the user’s access has been restricted to, through money extortion from its victims using online payment services or cryptocurrency. In this article, we have presented the main types of ransomware, their behavior and way of installing themselves on a computer host, have included comparisons between popular ransomware families and documented methods for mitigating or dealing with a ransomware attack.

Bibliography

[1] Awareness Education as the Key to Ransomware Prevention - Xin Luo, Qinyu Liao

[2] Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks - Amin Kharraz , William Robertson , Davide Balzarotti , Leyla Bilge , Engin Kirda

[3] A behavioural-based approach to ransomware detection - Daniel Nieuwenhuizen

[4] Comparative analysis of various ransomware virii - Alexandre Gazet

[5] Forensic Analysis of Ransomware Families using Static and Dynamic Analysis - Kul Prasad Subedi, Daya Ram Budhathoki, Dipankar Dasgupta, University of Memphis

[6] Ransomware. Defending Against Digital Extortion – Timothy Gallo, Allan Liska