LEMON SHARK

CYBER SECURITY CONSULTANCY

Ransomware

A MULTI-HEADED MONSTER TO BEAT

ERIK HESKES

MAY 2021

Ransomware

Introduction

Ransomware is a buzzword and a real threat. A sophisticated attack or a script kiddie may lead to this result: a complete lockdown of a company with the associated damages. This damage can be enormous. Not only because the systems are down and no work can be done, but also because restoring the system, either by paying the ransom or by hiring specialists, is very expensive indeed. And then there's reputational damage. When asked how it got to this point, hardly anyone has a good answer....

With the resources available, the attacker has every chance of committing a successful attack. This white paper covers the history of this type of attacks, the reasons for the attacker to carry out such an attack, the various ways of ransomware attacks and, very important, it describes the key protection measures that need to be in place to reduce chances of becoming a victim of these attacks. Understanding the variety in ransomware attacks from the recent past is necessary to be able to determine the best strategy to protect the company's data systems. Although, as you will see, dealing with ransomware is like dealing with a multi-headed monster.

What is Ransomware?

Ransomware can be defined as a type of malware that can infect a system by the encryption of files, folders, or an entire system. The compromised system shows the victim that a ransom needs to be paid, often by means of transferring a set amount of cryptocurrency or a large sum of money to an account or crypto wallet controlled by the attacker. Once the ransom is paid, the victim might be able to regain access to his system or files by following instructions with a decryption key, if the attacker allows it.

Who performs Ransomware attacks?

The culprits behind ransomware attacks are, in most of the occasions, well organized criminals who try to benefit through the financial gain. Russian hacking groups often are blamed for these attacks. For instance, the Russian Evil Corp, who started the Dridex malware back in 2007, has been linked to the latest ransomware Hades. Cozy Bear and Fancy Bear, who are both linked to Russian intelligence agencies have been accused of several attack scenarios in stealing information from SolarWinds, and information regarding COVID-19 research on the Corona-vaccine by making use of APT's (Advanced Persistent Threat) in combination with ransomware attacks.

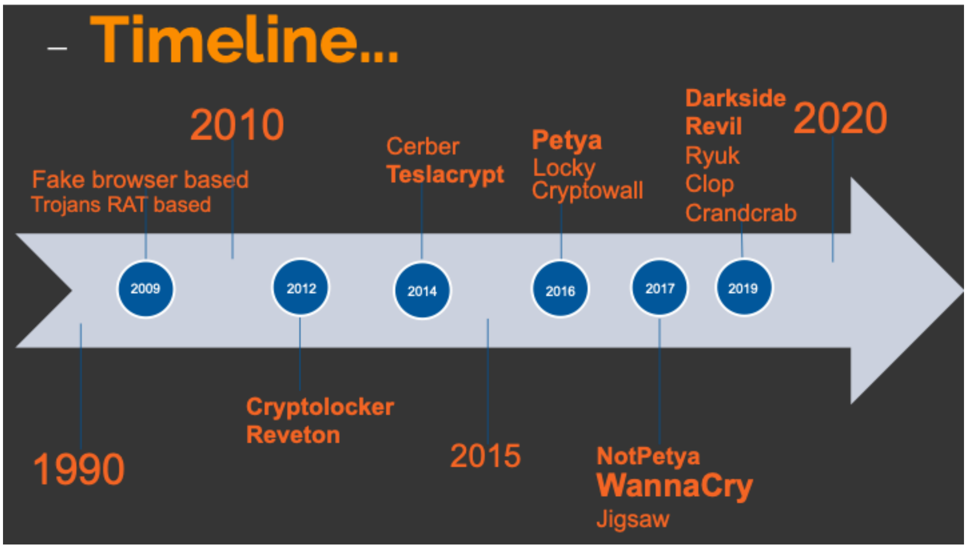
Why are Ransomware attacks performed?

In case of a "traditional" attack the hacker tries to infect a victim's machine, break into the infected system, exfiltrate the desired data, finds a buyer for that data, negotiate a deal, and process the payment. Such an attack can take several weeks or months, assuming anyone is willing to purchase the stolen data.

Ransomware simplifies this process by applying a new business model in launching an attack and getting paid immediately with Bitcoin or any other anonymous crypto currency.

Because of the simplified business model, it's much easier for attackers to raise funds quickly. The money raised can be put back into research and development, and the expansion of ransomware. With many ransomware attacks being reported in the media, this attracts even more groups which get involved in the ransomware business. There is even a RaaS (Ransomware as a Service) offering services to those who want to explore the ransomware business.

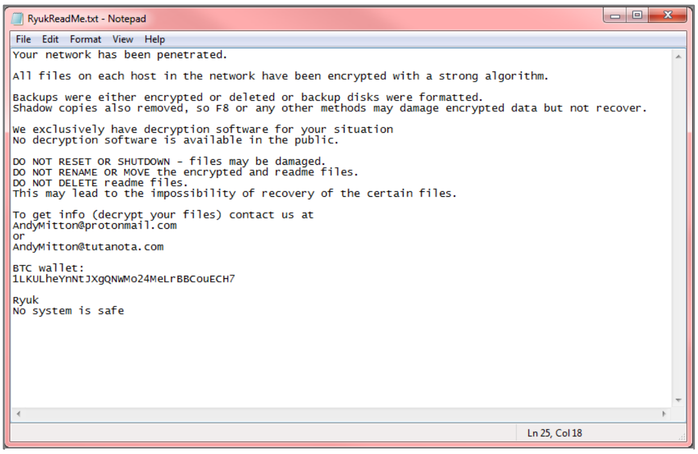
History of Ransomware



Trojan	The first documented example of ransomware is the 1989 AIDS Trojan, also known as the PS Cyborg. This ransomware was created by a biologist J. Popp who handed out infected floppy disks during a WHO AIDS conference.
Fake browser message	The fake browser message or pop-up scam displays a false security warning a ransomware threat has been detected. In some cases, it can also be an extortion message with a threat to report you to the local authorities. This usually is related to malicious advertising (malvertising) and is 9 out of 10 times harmless.
Cryptolocker	The first versions of Cryptolocker are discovered around 2012. With Cryptolockers users click on an executable which initiated the scanning of network drives, renaming of files and folders and decrypting them.
Reveton	Also known as the FBI Virus, Police Trojan and known as Win23/Reveton.A, this ransomware that spread through spam, phishing and websites. It is known to impersonate law enforcement authorities from a variety of countries while preventing victims from accessing their infected systems.

RANSOMWARE

Cerber	With the developments of ransomware came the Ransomware-as-a-service (Raas) called Cerber. Cerber was the first recorded instance of a ransomware family talking to the victims. Cerber offered also a lower ransom to users who paid the ransom sooner rather than later. The Cerber team appears to be based in Russia.
TeslaCrypt	Upon detection in 2015, the ransomware Trojan specifically targeted gamers and their computers by infecting game saves, user profiles, recorded replays etc. Its master key was released by its creators and newer variants also encrypt Word, JPEG, PDF and other files.
Petya	Discovered in 2016, the Petya encrypting malware spreads via email attachments. It infects the master boot record of Microsoft Windows systems by executing a payload that encrypts the hard drive's file system table and prevents the system from booting. The victim is shown a request for a ransom payment in Bitcoin to unlock the hard drive. Petya was eventually superseded by NotPetya.
Locky	Locky, another variant of ransomware spreads mostly via spam emails with attachments such as Microsoft Office document formats like Word and Excel and disguised as invoices. The invoices themselves looked incomplete and force the user to enable macros to make them readable. When this is done, a malicious code is executed and compromises the system of the victim. Next to that, Locky was able to run its encryption process completely offline without any C2 connections.
Cryptowall	With the introduction of Cryptowall a new more harmful type of ransomware emerged. Cryptowall in certain cases makes it impossible for victims to restore their data since Cryptowall finds a file to encrypt, it runs through a series of processes to encrypt and obfuscate the files that is ensnaring for the ransom. Cryptolocker leverages TOR as part of its communication protocols.
NotPetya	After the Petya ransomware came to light, a more dangerous variant called NotPetya was discovered. This ransomware strain spread by means of a backdoor present in accounting software originating in the Ukraine. It encrypted not only the Master File Table, but also other files existing on the hard drive. During the encryption process it could harm data beyond the possibility of recovery, rendering the data useless. In addition, users would not be able to retrieve this data when having paid the ransom.
Wannacry	The most infamous ransomware (cryptoworm) created, named Wannacry, targets the Windows operating system and has affected hundreds of thousands of systems worldwide. Wannacry makes use of phishing emails and the External Blue exploit for the Microsoft OS system to infect user systems and demands ransom in Bitcoin.
Jigsaw	Also known as BitcoinBlackmailer, Jigsaw attacked systems running on the Windows operating system. Jigsaw mostly spread via spam email or adware. When opening a file, the attachment or download was installed and activated. It encrypted files on the compromised device onto which it had downloaded while leaving out the encryption of executables.
Bad Rabbit	The Bad Rabbit ransomware experienced mainly in Ukraine and Russia, is oriented towards users downloading Adobe Flash installers from infected websites that propagate the launch of the execution file and thus infecting their own systems. The Flash downloads are installed on these insecure websites using Javascript injected into the HTML or Java Files of the affected websites. Once the user clicks on the installer, their computer is locked, and ransom is to be paid in Bitcoin.
Darkside	The Darkside ransomware was an uncommon ransomware strain that had been used to target high-value-organizations. With the use of brute force attacks and exploiting known vulnerabilities in the remote desktop protocol, it gained access to the systems of victims.
Clop	The Clop ransomware with its name deriving from the Russian word "klop" meaning "bed bug", was a virus encrypting files while avoiding detection by security solutions. It also forced the victim to pay the ransom within a certain time limit. It is considered a dangerous type of ransomware that can compromise most Windows operating systems.
GandCrab	Initially discovered in 2018, the GandCrab ransomware-as-a-service utilized RIG and Grandsoft exploit kits in order to distribute the ransomware via phishing emails. GandCrab was used along with an affiliates program where those making use of it would pay a certain percentage of their ransom revenues to the GrandCrab creator. In return they would be granted access to technical support and a web panel. Over time, different strains and versions have been identified.



```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
AndyMitton@protonmail.com
or
AndyMitton@tutanota.com

BTC wallet:
1LKULheYnNtJXgQNWMo24MeLrBBCouECH7

Ryuk
No system is safe
```

Ryuk ransomware note (https://threatpost.com/ryuk-ransomware-emerges-in-highly-targeted-highly-lucrative-campaign/136755/)

Nowadays, more elaborate cyber-attacks run the scene in the world of cybercrime which include ransomware and APT's combined. When such a ransomware attack is launched, it encrypts the victim's system and employs APT's to run on the system, collecting and stealing files. The attacker can access the system and can return to cause more harm or gather more data.

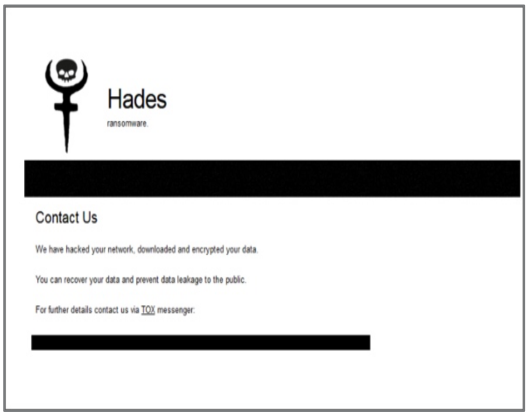
Ransomware and Advanced Persistent Threats (APT's)

Advanced Persistent Threats (APT's), frequently focus on select targets over a longer period to gain access over the victim's system. Sometimes an attacker may analyze a target for years.
Whereas a ransomware attack is evident by the display of a payment demand, APT's tend to manifest themselves on the system of the victim undetected, and meanwhile stealing credentials along with other valuable information. The damages incurred from both types of attacks can be devastating for organizations. Where ransomware aims to encrypt systems and all files, APT's aim to steal and misuse the information gathered during an attack which often goes unnoticed.

Ransomware and supply chain attack (Apple)

A supply chain is basically the chain of components involved to move resources from the vendor to the paying customer. Ransomware can be a part of this multi-staged attack in order to attack one of the delivering vendors. Almost every company is using a third party for their IT OPS management these days. The Ransomware actors will specifically hunt for those third parties to use as a steppingstone to attack larger organizations. For instance, one of the latest reported ransomware attacks on a supplier of Apple is by the Sodinokibi ransomware gang.

Recent Ransomware variants



[redacted]

Contact Us

We have hacked your network, downloaded and encrypted your data.

You can recover your data and prevent data leakage to the public.

For further details contact us via TOX messenger:

[redacted]

https://www.bankinfosecurity.com/hades-ransomware-targets-3-us-companies-a-16268

- **Hades**

In 2020, a new variant of ransomware named Hades was discovered. It affected large enterprises generating billions of revenues in the US. The group behind Hades allegedly has ties to the Chinese nation-state group Hafnium. Hades aimed to infiltrate systems by means of internet facing systems, Remote Desktop Protocol (RDP) or Virtual Private Networks (VPN) setups using credentials, which are likely retrieved via brute-force attacks or data dumps. By duplicating itself and launching itself via the command line, a spare copy is deleted, and an executable file is released in the memory. Consequently, files and folders of relevance are then encrypted and use different extensions. The cybersecurity firm Crowdstrike, focusing on endpoint protection, deems Hades an evolution of the Evil Corp's WastedLocker ransomware. While there is still uncertainty regarding the individuals behind Hades, it is evident that the ransomware is linked to advanced persistent threats.

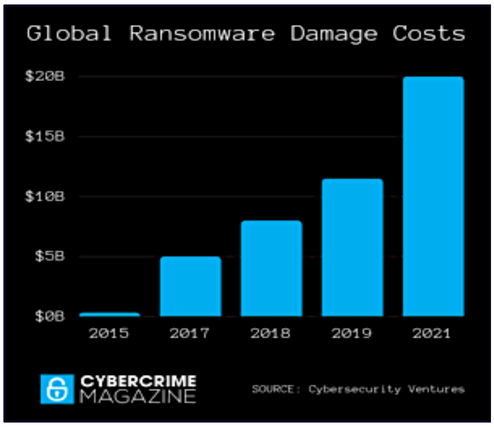
- **Ryuk**

A Russian group called the Wizard Spider has employed their Ryuk ransomware since 2018 to attack larger organizations and demand high ransoms. Using botnets like Trickbot, distributed via spam emails or Emotet, systems are infected. Ryuk can identify and encrypt network drives and delete shadow copies on the network, disabling the Windows System Restore option for users and rendering the encrypted objects lost without external backups.

Costs of Ransomware

A recent article "*Cybercrime to cost the world $10,5 trillion annually by 2025*" published by Cybersecurity Ventures, highlighted the enormous financial impact cybercrime has worldwide. Ransomware is one of the fastest growing categories of cybercrime. Costs of ransomware entail damages, destruction/loss of data, downtime, lost productivity, post disruption, investigation, remediation, reputational harm, training, and global ransom payouts. While quantifying exact costs is troublesome and largely dependent on victim reports to authorities dealing with cybercrime, the overall costs have significantly increased in the recent years.

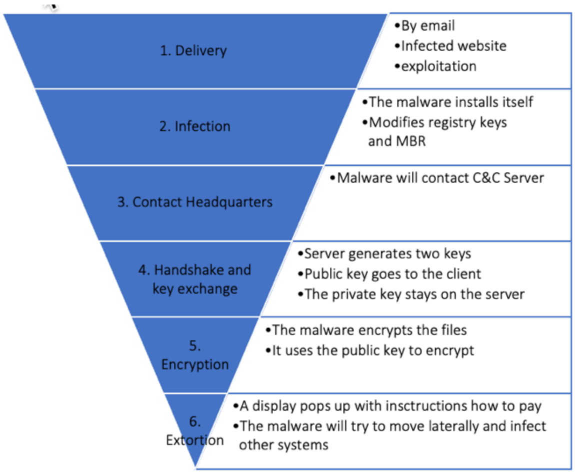
The estimated costs of ransomware in the article have been compiled based on the insights from media outlets, academia, industry experts and cybersecurity firms for these statistics, according to Cybersecurity Ventures. The costs of damages incurred from ransomware attacks between 2015 and 2017 had increased from $325 million dollars in 2015 to an estimated $5 billion dollars in 2017. For the years 2018 an estimation of $8 billion dollars in costs was predicted and 11,5 billion dollars in 2019. The latest prediction alludes to more troubled and dark times ahead for (potential) victims of ransomware with estimated costs stacking to $20 billion by 2021.



Global Ransomware Damage Costs (https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/)

The anatomy of a ransomware attack

A ransomware attack is complex and multi-staged:


1. Delivery
•By email
•Infected website
•exploitation
2. Infection
•The malware installs itself
•Modifies registry keys and MBR
3. Contact Headquarters
•Malware will contact C&C Server
4. Handshake and key exchange
•Server generates two keys
•Public key goes to the client
•The private key stays on the server
5. Encryption
•The malware encrypts the files
•It uses the public key to encrypt
6. Extortion
•A display pops up with insctructions how to pay
•The malware will try to move laterally and infect other systems

After the infection the malware will:

- Change registry entries to control the system, important it will remove registry entries which allows an option to revert
- Make changes to the MBR so that after a reboot the malware will stay active
- It will delete all backup shadow copies and snapshots to prevent a roll-back or revert to known good state
- Changes file extensions of system operation critical files

The world is changing, so is ransomware (type II attack)

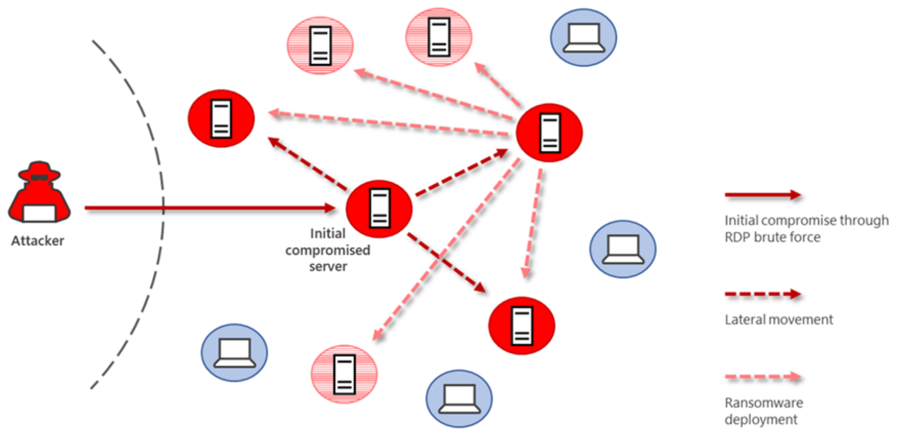

Attacker
Initial compromised server
Initial compromise through RDP brute force
Lateral movement
Ransomware deployment

Figure - https://www.microsoft.com/security/blog/2020/06/10/the-science-behind-microsoft-threat-protection-attack-modeling-for-finding-and-stopping-evasive-ransomware/

With the still ongoing COVID-19 pandemic in 2021, security experts and researchers have observed that ransomware developers and attackers have started to alter their modus operandi. All around the world more people started to work remotely, often from home, and thus changing threat models and network architectures allowing this. Ransomware closely followed this development with a shift towards targeting larger companies with more resources and leverage material. As such, there was an increase in double extortion type of attacks where attackers do not only encrypt files, but also exfiltrate data often containing high value information. This information in its turn is used to threaten an organization by making it publicly available for the world in case the ransom is not paid. In some cases, backups are also compromised and encrypted, causing serious data recovery issues. Trying to exfiltrate this data, attackers need to know where this information is located on a network. By means of stolen credentials retrieved from other systems on the network, attackers can move laterally from one system to another to extract this high value data. With this development, security solutions such as DLP, ERDs and EPPs seem to have difficulties coping with this more corrosive type of ransomware threat. Attackers might use admin credentials and tools to move from system to system while executing malicious commands to steal data, thereby allowing themselves to encrypt the network and initiate the extortion process.

Defense against Ransomware

Often organizations make use of electronic messaging services to exchange information. Email is labeled as one of the most vulnerable for ransomware attacks. Spam, spoofing and (spear)phishing are used to lure victims into clicking on suspicious attachments or links. By checking and monitoring email traffic by authentication procedures such as SPF DKIM and DMARC, an organization can better equip itself against ransomware in a proactive stage. Another way to defend against ransomware attacks is by using Endpoint detection and response (EDR) software in addition to antivirus software.

Sender Policy Framework (SPF)

Employing the Sender Policy Framework allows an organization to recognize unauthorized sender addresses and can prevent the delivery of emails with potentially malicious content. The DNS servers are hardened and limiting anyone from sending emails from the domain used by the organization. It allows the mail server to recognize whether the message originating from the domain it is using. If the domain is not registered in the SPF record, the servers will not be authorized to send emails on behalf of the domain. SPF consists of three components: a framework, an authentication method and specific headers contained in the emails that convey this information.

Domain-keys Identified Mail (DKIM)

DKIM provides an authentication method to apply a signature on any email message being sent. The receiver is able to verify the sender's domain and the content of the message according to this signature. The signature is being provided by the email server which generates a private key to go with the sending message. The receiver receives the public key from DNS through which he can perform the verification.

Domain-based Message Authentication, Reporting and Conformance (DMARC)

DMARC ensures the connection between SPF and DKIM methods by ensuring that the email sender's address matches the body form address. Conventional email programs display the body-from information of an email, while the actual sender information remains masked. DMARC also establishes guidelines for SPF and DKIM procedures and provide instructions for handling of received emails. For instance, for SPF verification must be positive and the email sender's address of the domain needs to match the address stored in the SPF record, while for DKIM the signature needs to be valid, and the domain needs to match the body-from address of the specific email. A positive verification is achieved by linking the sender's domain name with the indexed 'From' header along with mail recipient reports.

Endpoint Detection and Response (EDR)

EDR solutions are a comprehensive centralized approach to manage cyber threats. The use of EDR tools allows an organization to protect their endpoints (connected devices and computers) in their enterprise infrastructure. The protection of endpoints is structured to detect, contain, investigate, and eliminate threats. Furthermore, it enables the monitoring of network and endpoint events, along with analysis and reporting of this information with storage on centralized databases. The protecting of endpoints is carried out by including the collection of data of potential threats for an organization. Prevention, hunting down threats, remediation capabilities, and responding to advanced types of malware is therefore possible. By detecting anomalies and suspicious activities EDR tools are able to stop an attack in its primary stages and can control and contain the spread of malware and ransomware.

Virus vocabulary

Virus	Infects files and in some cases the master boot record (MBR) most classic example and comes in many guises and intents
Worm	Infects other computers over the network, example Iloveyou virus and Melissa
Trojan	Installs a backdoor so that the attacker can take over the computer. Also called Remote Access Trojan (RAT).
Adware	Annoying virus with ad popups.
Malware	Another word for virus.
Dropper	Small piece of malware that starts the infection.
Spyware	Dangerous virus form, looks for passwords, keystrokes, etc.
Ransomware	Virus form where a price is set to undo the infection.
DDOS **(Distributed Denial Of Service)**	Attack with the aim of resource exhausting the target.
Botnet	Virus that turns a computer into a zombie to participate in a DDOS attack.
APT **(Advanced Persistent Threat)**	Very patient attack process to only become active after a long time, often involves the crown jewels.
Drive-by-Download	Infected website with malware targeting the victim.
Phishing	Email with a hidden link to a target website where credentials are extracted from the victim
MITM (Man In The Middle)	A “proxy” that sits invisibly between sender and receiver to receive data or credentials from the victim.