

Part 1 - Ransomwares

Feb 5 2025



How ? Via Ransomwares

1. Introduction: why have we gone so far in the threat?
2. Cryptocurrency, RaaS, and the Extortion Ecosystem
3. Can cyberinsurance cope with ransomware prevalence ?
4. Back ups , the ultimate protection, ransomware-proof ?
5. Anatomy of a ransomware attack

Introduction

History of Ransomwares:

Ransomwares becomes open source

- **Release of ransomware source code**
 - a security group published the source code for Hidden Tear on GitHub in August 2015 for helping other security teams
 - Bad guys quickly seized upon the source code + made improvements
 - As recently as July 2020, almost five years later, new variants of ransomware were traced to the Hidden Tear source code

Governments Do Ransomware Too: WannaCry and NotPetya

- **The WannaCry ransomware was launched on May 12, 2017, and spread around the world, infecting 230,000 computers in 150 countries.**
 - WannaCry was a worm that spread via the EternalBlue Server Message Block (SMB) vulnerability (exploit stolen from the NSA).
 - Ransom payment of \$300 USD in Bitcoin but no encryption key was available.
 - Attributed to North Korea.
- **NotPetya: distributed through a trojanized update to the M.E.Doc accounting software.**
 - This software is used by business in Ukraine: Attackers managed to gain access to M.E.Doc's update server and replace the legitimate update with the malicious code.
 - Not Petya attributed to Russia

Introduction

History of Ransomwares:

Ransomware as a Service

- RaaS Value proposition: Inexperienced cybercriminals...or cybercriminals with experience in other areas can jump into ransomware: RaaS lowers the barrier of entry for ransomware
- The RaaS customer got only an executable and still has to manage much of the attack such as initial access and collecting and processing payments (dangerous and difficult, for newer cybercriminals)
- Typical Turnkey RaaS offering with back-end portal that affiliates (RaaS customers) could use to follow the status of an attack + RaaS handles payments and then issue a payout to the affiliates (minus a cut, of course).

History of Ransomwares

Wrap Up:

- Ransomware is constantly evolving and will continue to do so into the foreseeable future.
- Ransomware started via malware delivered via floppy disk to large-scale campaigns that exploit previously unknown vulnerabilities.
- Ransomware has gone from demanding payment in check or money to gift cards and millions of dollars in cryptocurrency.
- Ransomware groups have gone from one person sitting behind a computer to large, complex organizations with specialized roles.
- Ransomware is the most profitable type of cybercriminal activity, and with that kind of money to be made it is not going to disappear easily

Ransomware sophistication is like innovation in IT: incremental.

Nobody can foresee what the profile of ransomware will be in 2025



RANSOMWARE

- Introduction: why are we so far in the threat?
- **Cryptocurrency, RaaS, and the Extortion Ecosystem**
- Can cyberinsurance cope with ransomware prevalence ?
- Back ups , the ultimate protection, ransomware-proof ?
- Anatomy of a ransomware attack

Follow the money to stop ransomwares ?

Regulate cryptocurrencies/cryptocurrencies exchanges in the hope of stopping ransomware ?

- Could ransomware actors go back to other forms of payment? Probably not !
- In 2020, Palo Alto: average ransomware payment was \$312,000(Q1 2021: \$850,000) but it is not unusual to see ransom payments in the millions of dollars

Follow the money to stop ransomwares ?

Regulate cryptocurrencies exchanges maybe better thanks to KYC and without cryptocurrencies exchanges, cryptocurrencies are useless for the real world (for the moment....)

- There will always be exchanges that don't comply and don't care they can't do business in certain KYC-severe countries
- But enforcing KYC laws would limit the number of exchanges ransomware actors could use to launder their money + easier for governments and private companies to more effectively track their transactions

The Commoditization of Ransomware

- Operations usually involve contracting cybercriminals with specialized roles having nothing to do with ransomware:
- Development, gaining initial access, processing the ransoms paid, and handling negotiations.
- Independent contractors + sometimes on the “payroll”.
- Negotiators deal with the ransomware actors + facilitate payment when organizations can’t quickly source hundreds of thousands or millions of dollars in cryptocurrency.
- Ransomware groups prefer working with negotiators, dispassionate and reasonable
- Ransomware negotiators provide help to ransomware victims to navigate through the ransomware process, not just the ransom payment

The Ransomware Value Chain: Initial Access Broker

Initial Access Brokers (IAB)

65,000 hands-on-keyboard ransomware attacks in 2020: That's simply too much without split of tasks

Gain access, steal files from, deploy ransomware,... = too much to do for one actor.

There is a business model for Initial Access Brokers (IABs)

- IABs specialize in credential stuffing (attempts to log in with common username/password combinations, using brute force or credential reuse of username/password combinations on underground markets)
- IAB's role : gain and maintain the initial foothold + sell the access to ransomware actors for an average price of \$5,400
- IABs also exploit vulnerabilities (e.g. Pulse Secure VPN, Citrix, Fortinet VPN, SonicWall Secure Mobile Access, Palo Alto VPN, F5 VPN)
- IABs operate independently or work as contractors for specific ransomware groups (If the expected payoffs don't happen, IABs retaliate: dumping sensitive information about the ransomware group for the world to see)

The Ransomware Value Chain: Money Launderers

Money laundering is difficult for ransomware group

- There is a difference between trying to move thousands of dollars versus millions of dollars at a time: how to clean up millions of dollars in collected ransoms ?
- Most of the victims' funds go to mainstream exchanges, high-risk exchanges (meaning those with loose to non-existent compliance standards) and mixers.

Ransomware laundering activity is concentrated on a few platforms but ransoms groups may also hire professional launderers

Laundering use advanced obfuscation techniques (“chain hopping” = conversion from one cryptocurrency to another to blur investigators to lose their trail) before cashing out

The Ransomware Value Chain: Exploit Brokers

Ransomware actors buy exploits:

- Ransomware groups target well-known vulnerabilities for exploitation, rather than zero-days (Ransomware groups and IABs are counting on the slow patch cycle of many organizations)
- Ransomware groups compete with nation-state actors to acquire exploits
- Ransomware groups rely on exploit brokers to produce exploits for well-known vulnerabilities (gain administrative access to Windows systems)
- Exploit brokers are paid by the exploit or are contracted to the ransomware groups

The Ransomware Value Chain: Ransomware As A Service (RaaS)

Ransomware actors operating alone can complete 1 or 2 attacks a week.

Gaining administrative access, finding and exfiltrating files, getting access to the Domain Controller and deploying the ransomware takes time, even in heavily scripted operations, takes time.

- Most attempted attacks fail (area of study: no one is collecting statistics on ransomware group failures)
- RaaS operators have affiliates = criminals who subscribe to their service as “affiliates.”
- RaaS offerings require an initial buy-in, then affiliates pay for the service and the RaaS operator takes money off the top of each ransom paid.
- Some ransomware groups have even been known to pay affiliates who recruit new affiliates (friends get friends)
- Like ads for Multi-Level-Marketing schemes, RaaS ads advertise the money that affiliates can make and post news articles showing the amounts paid by the victims.

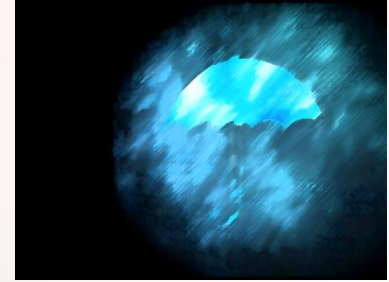
RANSOMWARE

1. Introduction: why are so far in the threat?
2. Cryptocurrency, RaaS, and the Extortion Ecosystem
3. Can cyberinsurance cope with ransomware prevalence ?
4. Back ups , the ultimate protection, ransomware-proof ?
5. Anatomy of a ransomware attack

Cyber insurance in the context of ransomwares

Why is covering cyber attacks so difficult ?


- Damages of cyberattacks are vast in scope not only in scale: regulatory fines, lost turn over, fraud (if the intruder hijacks the payment systems), data leaks, loss of intellectual property !
- In case of flooding or fire, things are more simple.... The damage to compensate is only what has been destroyed: If an insurance covers the loss of turn over, the claim can only come as a result of the destruction of the asset not its stop due to a cyber attack



Not all industries are impacted in the same way by cyberattacks

- Manufacturing companies have “just” delays in supplying the customer
- Financial services loose transactions for ever and must pay damages to the customer + distrust up to runoff may arrive






Cyber insurance in the context of ransomwares

Not all industries are impacted in the same way by cyberattacks

- Manufacturing companies have “just” delays in supplying the customer
- Financial services loose transactions for ever and must pay damages to the customer + distrust up to runoff may arrive
- Cyber silent insurances are stopped or adapted



Cyber insurance in the context of ransomwares

Cyberattacks are very special

- This is a risk whose materialization is under control by the (future) victim ! For ransomware, maybe the victim will be able to contain it, to stop it, to limit the damages. The customer may negotiate the ransom...
- This diversity make it difficult to build actuarial models: to better control the risk, the insurance company will want to intervene in the crisis response.
- The customer is expected to call the insurance company when the attack begins
- The customer is expected to fill in a questionnaire, to prove it has a good in house security, maybe he will be obliged to pass certification/exams in the future to still be covered by a cyberinsurance (This is the practice for covering industrial risks)

RANSOMWARE

1. Introduction: why are so far in the threat?
2. Cryptocurrency, RaaS, and the Extortion Ecosystem
3. Can cyberinsurance cope with ransomware prevalence ?
4. Back ups, the ultimate protection, ransomware-proof ?
5. Anatomy of a ransomware attack

Back up

Reliable and well-tested backups give a ransomware victim options

If an organization has confidence in its ability to restore from backups, they're empowered to make a more nuanced decision

Victims must determine the sensitivity of the data exfiltrated by the ransomware actor

Offline backups are backups that aren't connected to the network but could be stored on:

- ✓ Tape
- ✓ A DR network
- ✓ A cloud provider
- ✓ An offline backup storage facility



| Back up

3-2-1 Rule

Three copies of
backed up data

Stored on at least
two different media
types

One of the
copies is
offsite

Backup professionals don't like tape backups as an alternative to drives, but no ransomware group has figured out how to encrypt or delete files backed up to tape, especially tape that's not in the loader (in other words, truly offline)

Back up

Gold Images need to be stored too

- Gold images = preconfigured versions of the operating system and all installed applications on those servers. They allow organizations to quickly rebuild systems in the event of a ransomware attack (or other disaster)
- This precaution also helps DR teams move through the restoration process a lot faster, because they don't have to
- install the OS and necessary software for every critical server

Precautions for Gold Images

- They must be properly maintained : when IT team updates the OS and different applications, a new gold image has to be made.
- Keep identical spare versions of the most critical servers too: then a ransomware attack, the gold image can be installed on the spare server and the data backed up on to that.

Back up

Immutable Cloud Backups

- Cloud storage providers <> cloud backup provider (for protections in place)
- Advantages of cloud backup providers:
 - Versioning
 - The ability to leave the file structure in place
 - Scheduling
 - More encryption options for file transfer
 - Immutability
- Immutable file storage is not a good option when backup solution is often used for day-to-day restoration and may change more frequently. But it is good for intermittent copies (e.g. weekly full backups).
- Immutable solution adds resiliency to the backup solution and serves as an additional layer of protection against ransomware

Back up

Testing Backups with Ransomware in Mind

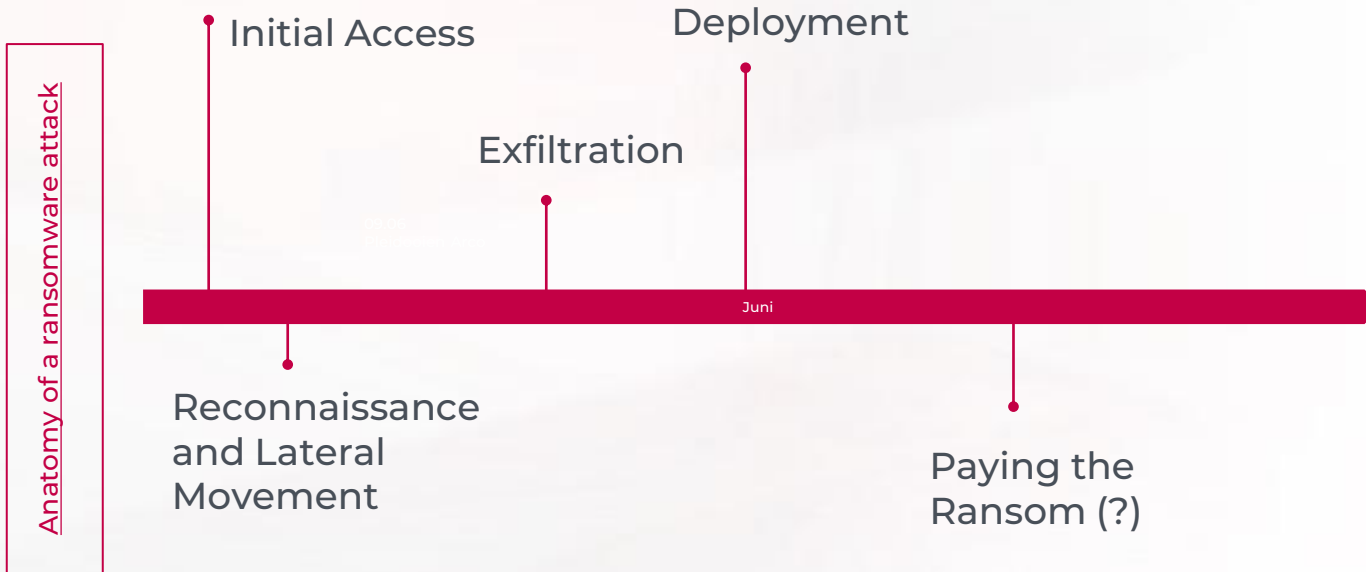
- Let's say that backups are conducted hourly: an organization should never lose more than an hour of data, correct? Not necessarily.
- Let's say it takes four hours to back up a server. That means you could lose as much as five hours of data
- Ideally, the backups are pulled from the backup server:
 - What if the ransomware actor manages to encrypt the backup server?
 - Pull the backup from the tape drive, but what if the tape is corrupted and no one noticed?
 - If that fails, the restoration has to come from the cloud backup provider, but the organization isn't backing up the cloud provider hourly, just a few times a week

RANSOMWARE

- Introduction: why are we so far in the threat?
- Cryptocurrency, RaaS, and the Extortion Ecosystem
- Can cyberinsurance cope with ransomware prevalence ?
- Back ups , the ultimate protection, ransomware-proof ?
- Anatomy of a ransomware attack

11.05.2022

Anatomy of a Modern Ransomware Attack



Anatomy of a Modern Ransomware Attack

Initial Access

- Four ways that ransomware groups gain access to victim networks:
 1. Phishing
 2. Credential stuffing/reuse (especially through Remote Desktop Protocol)
 3. Vulnerability exploitation
 4. Trojanized software (less frequent, based on fake downloads)
 5. Exploit kits (has declined because they were relying on flaws in Adobe Flash and Microsoft Internet Explorer, fallen out of use)
 - *Delivered primarily through banner ads and other web-based mechanisms.*
- Initial payload is injected into memory to avoid detection + performs a few basic reconnaissance commands.
- Commands such as whoami (note: whoami is native to every major operating system), net, and nltest allow to understand the system on which it's installed without raising any alerts in the SOC
- Using commands native to the operating system, as opposed to third-party tools, means that ransomware groups are less likely to be detected by defenders

Initial Access

Anatomy of a Modern Ransomware Attack

Reconnaissance and Lateral Movement

- The ransomware actor maps the victim network
- It establish footholds on systems beyond the initial access machine, to ensure they don't lose access to the victim's network.
- Cobalt Strike is often used (it is initially a penetration testing tool but several cracked versions have been released on underground forums, - is widely adopted by all types of cybercriminals from nation-state actors to ransomware groups).

Reconnaissance and Lateral Movement

Anatomy of a Modern Ransomware Attack

Reconnaissance and Lateral Movement

The ransomware actors are attempting to gain administrative credentials to facilitate moving around the network.

Disable any security programs that may hinder their ability to move around

Once done, use gathered credentials to start moving around the network

- Ransomware actors look for credentials that allow them to log in to Linux and ESXi (i.e., VMware) servers.
- This is made easier by administrators' common practice of keeping spreadsheets with username and password information for these servers on their endpoints.

Reconnaissance and Lateral Movement

Anatomy of a Modern Ransomware Attack

Exfiltration

- The ransomware actors look for interesting files to exfiltrate:
 - Finance documents
 - Accounting information
 - Client data
 - Project data
- The ransomware actors look for keywords like: Cyber , policy, insurance, endorsement, supplementary, underwriting, terms, bank, 2021
- To get the data out of the cloud, use common tools as: Rclone, WinSCP, StealBIT, MegaSYNC (if these tools are commonly used, they will not raise alarm in the SOC or are not flagged by security tools)
- Open an account on file-sharing services + limit the number of streams (simultaneous upload to limit detection)

Exfiltration

Deployment

Anatomy of a Modern Ransomware Attack

Deployment

- first step = find and encrypt or destroy any backups
- next step = deploy the ransomware on one or two systems to ensure that everything works as advertised to ensure that the malware can encrypt network machines (+ disabling all known security tools) without raising alerts or having their executable blocked.
- last step = deploy the ransomware across the network. (PsExec, to execute the ransomware after pushing it to all the different machines via SMB)