Corso di Sicurezza delle reti e dei Sistemi Software

UNIVERSITÀ DEGLI STUDI DEL SANNIO
Benevento

CYBER THREAT INTELLIGENCE

Prof. Corrado Aaron Visaggio

Ing. Pietro Melillo

PART 2: RANSOMWARE

Contents

Ransomware

What is Ransomware?

Ransomware Taxonomy

Ransomware Gang

Ransomware Extortion

TTPs

IAB

Data Leak Site

RaaS

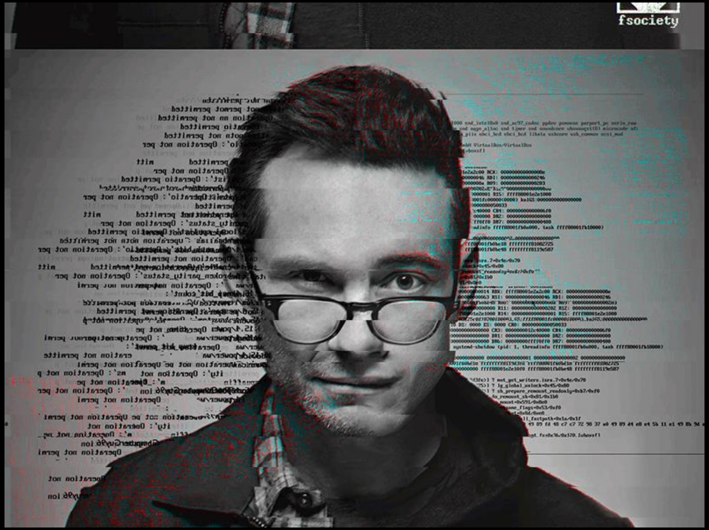
Ransom Note

Ransomware

“Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyberattackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files. Some variants have added additional functionality – such as data theft – to provide further incentive for ransomware victims to pay the ransom.

Ransomware has quickly become the most prominent and visible type of malware. Recent ransomware attacks have impacted hospitals’ ability to provide crucial services, crippled public services in cities, and caused significant damage to various organizations.”

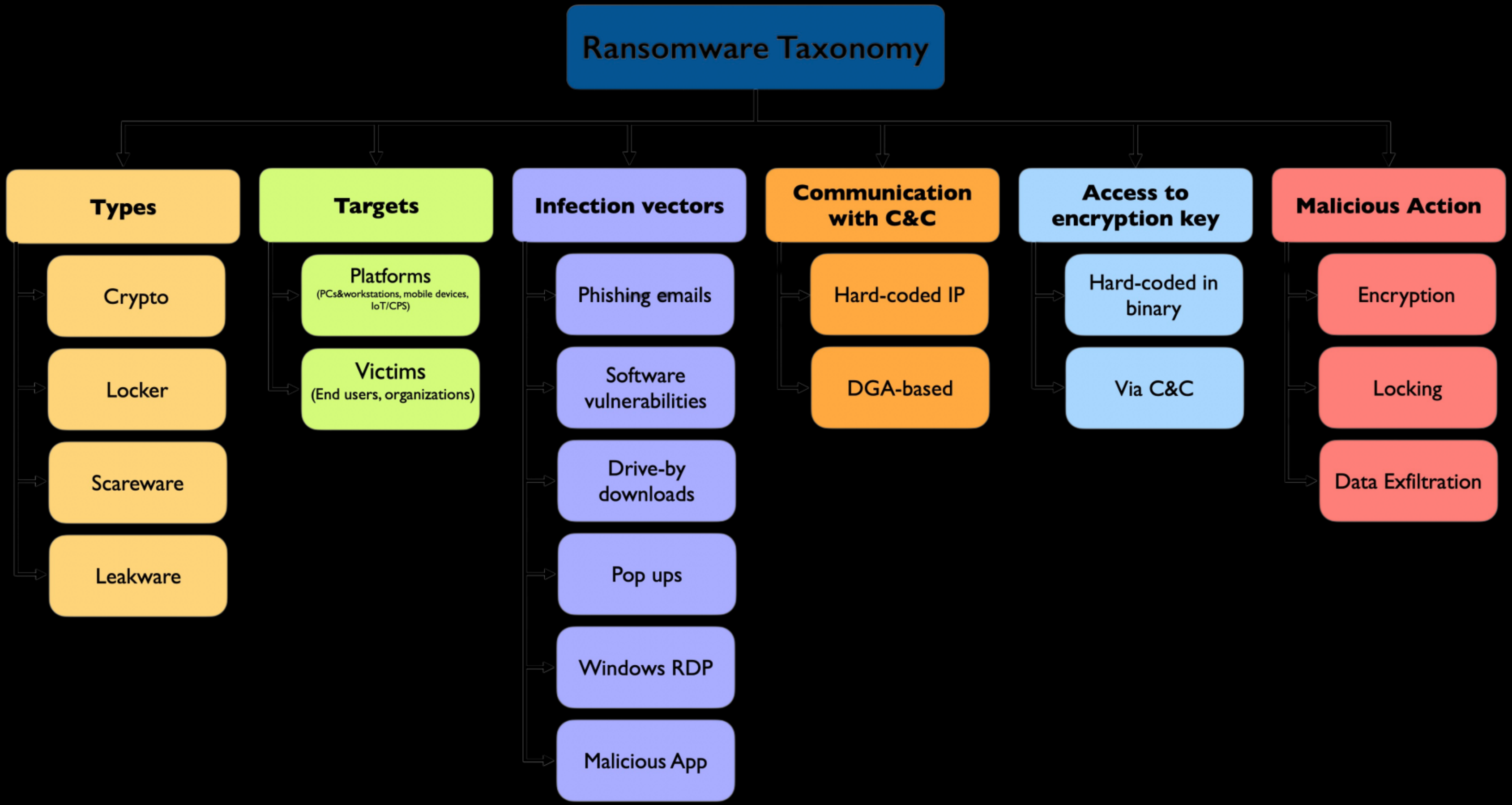
Checkpoint



USD 4.45 million

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.

Ransomware Taxonomy



Ransomware Gang

Ransomware gangs are groups of individuals that work together to carry out ransomware attacks. They often consist of complex networks of numerous cybercriminals with the power to steal tens or hundreds of millions of dollars every year.

LOCKBIT 3.0

Ransomware: Double, Triple, Quadruple Extortion Defined

Single Extortion

Ransomware operators encrypt data, demand payment to provide the decryption key.

Double Extortion

Ransomware operators exfiltrate data, and demand payment from the victim to not release the data. Ransomware operators encrypt data, and demand payment to provide the decryption key.

Ransomware: Double, Triple, Quadruple Extortion Defined

Triple Extortion

Ransomware operators exfiltrate data, and demand payment from the victim to not release the data.
Ransomware operators encrypt data, and demand payment to provide the decryption key.
Some say the third level of extortion is when ransomware operators contact people who would be affected by the release of the stolen data, and demand payment to not release the data. Other say it’s when ransomware operators launch **DDoS** attacks against the victim, and demand payment to stop.

Quadruple Extortion & Beyond

There are several other forms of extortion that ransomware operators have been using. Basically, they add techniques to increase the amount or speed of payment, or to extort other victims.
Ransomware operators threaten greater consequences if the victim involves law enforcement, data recovery experts, or professional negotiators.
Ransomware operators steal credentials from victim’s employees and customers, to sell or use.
Ransomware operators install cryptomining software on victim’s network.
Ransomware operators send phishing emails from the victim’s network, **to compromise additional organizations.**

The anatomy of a ransomware attack

The anatomy of a ransomware attack
Phase 1: Reconnaissance and target selection

Phase 1 of a ransomware attack involves the threat actor researching and selecting organizations to attack. During this phase, threat actors identify potential targets and gather critical information about them.

Identifying potential targets

Threat actors engage in reconnaissance to identify organizations that are more likely to yield a high return on their malicious activities. They carefully assess factors such as the industry, size, financial stability, and the value of the data held by the potential targets. Organizations that heavily rely on their digital infrastructure and are more likely to pay a ransom to regain access to critical systems and data are prime targets.

Techniques used for reconnaissance

Threat actors employ various techniques to gather information during the reconnaissance phase. These techniques may include passive reconnaissance, where they collect publicly available data from websites, social media platforms, and professional networking sites. They may also utilize active reconnaissance, such as scanning for open ports and vulnerabilities, conducting phishing campaigns to gather employee information, or leveraging third-party sources like leaked databases and dark web forums.

The anatomy of a ransomware attack
Phase 1: Reconnaissance and target selection

Vulnerability factors

Several factors can make organizations more vulnerable to targeting during the reconnaissance phase:

- Lack of Security Awareness: Organizations that do not prioritize cybersecurity awareness and training for their employees may inadvertently provide attackers with valuable information through social engineering tactics.
- Inadequate Patch Management: Failure to promptly apply software patches and updates leaves systems vulnerable to known vulnerabilities that threat actors can exploit.
- Weak Access Controls: Poorly managed user accounts, weak passwords, and insufficient access controls increase the likelihood of unauthorized access to sensitive systems and data.
- Absence of Network Segmentation: If an organization's network lacks proper segmentation, a successful initial access point can provide attackers with the opportunity to move laterally within the network and escalate privileges.
- Lack of Monitoring and Detection: Organizations that lack robust monitoring and detection capabilities may not notice the initial signs of a reconnaissance attempt, allowing threat actors to proceed undetected.

The anatomy of a ransomware attack
Phase 2: Initial access

Phase 2 of a ransomware attack is the critical stage where threat actors strive to gain initial access to an organization’s network and systems.

During this stage, threat actors employ a range of techniques to achieve initial access, including:

- Phishing Emails: One of the most common and successful methods, threat actors craft convincing emails designed to deceive recipients into clicking on malicious links or opening infected attachments.
- Exploit Kits: These toolkits contain prepackaged exploits that target vulnerabilities in software, commonly used web browsers, or plugins. By visiting compromised websites, unsuspecting users can unwittingly trigger the exploit kit and grant the attacker initial access.
- Vulnerable Software: Exploiting weaknesses in software, particularly outdated or unpatched applications, is another avenue threat actors may exploit to gain a foothold within an organization’s network. This was recently observed through CLOP’s use of the MOVEit and GoAnywhere MFT vulnerabilities to attack over 100 organizations globally.

The anatomy of a ransomware attack
Phase 3: Lateral movement and privilege escalation

Once threat actors have gained initial access to an organization’s network and systems, they proceed to Phase 3 of a ransomware attack: lateral movement and privilege escalation.

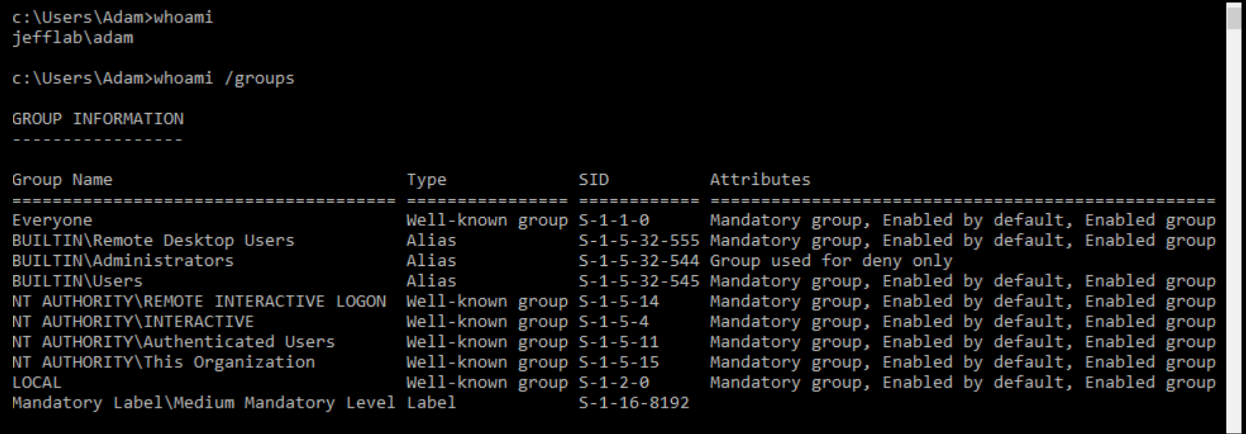
This stage involves the navigation and expansion of their reach within the compromised network. Threat actors explore the compromised network to locate valuable data, critical systems, and potential targets for encryption.

They employ lateral movement, traversing through the network to gain control over multiple machines, servers, or devices, which increases the likelihood of finding and encrypting valuable information while making it challenging for defenders to contain the attack.

Threat actors may use several techniques to achieve lateral movement.

The anatomy of a ransomware attack
Phase 3: Lateral movement and privilege escalation

- Exploiting Misconfigurations: They take advantage of misconfigured network shares, weak or shared passwords, and unsecured remote desktop protocols (RDP) to gain unauthorized access to other systems within the network.
- Credential Theft and Reuse: They employ various tactics to steal or acquire legitimate user credentials, such as using keyloggers, credential harvesting, or compromising administrative accounts. These stolen credentials are then reused to move laterally within the network.
- Pass-the-Hash: This technique involves stealing hashed credentials from compromised systems and using them to authenticate and gain access to other systems without needing to know the plaintext passwords.



```
c:\Users\Adam>whoami
jefflab\adam

c:\Users\Adam>whoami /groups

GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Desktop Users           Alias            S-1-5-32-555 Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                 Alias            S-1-5-32-544 Group used for deny only
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\REMOTE INTERACTIVE LOGON  Well-known group S-1-5-14     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label            S-1-16-8192
```

The anatomy of a ransomware attack
Phase 3: Lateral movement and privilege escalation

Once within the network, threat actors seek to escalate their privileges. By elevating their access rights, they gain increased control over critical systems and can maneuver more freely within the network. Privilege escalation techniques may include:

- Exploiting Vulnerabilities: They identify vulnerabilities in software, operating systems, or network configurations that can be leveraged to elevate their privileges. This may involve exploiting unpatched systems or misconfigured permissions.
- Leveraging Stolen Credentials: If threat actors have successfully stolen credentials during the initial access phase, they can use these credentials to escalate their privileges within the network, gaining administrative or higher-level access.
- Abusing Trusted Applications or Services: They manipulate trusted applications or services that have higher privileges or access rights to gain elevated permissions within the network.

It is important to note that lateral movement and privilege escalation are not necessarily linear processes. Threat actors adapt their tactics based on the network’s topology, security measures, and available targets, maneuvering opportunistically within the network.

The anatomy of a ransomware attack
Phase 4: Deployment of ransomware payload

In Phase 4 of a ransomware attack, threat actors execute their ultimate objective: deploying the ransomware payload. This phase involves the encryption of the victim’s files and the subsequent demand for a ransom payment.

Ransomware comes in various forms, each with its own characteristics and objectives. Some common types include:

- Encryption Ransomware: This type of ransomware encrypts the victim’s files, rendering them inaccessible until a decryption key is obtained by paying the ransom. Examples include notorious strains like WannaCry and Ryuk.
- Locker Ransomware: Locker ransomware locks the victim out of their system or specific applications, denying access to the device or critical functionalities. It often displays a ransom message directly on the victim’s screen, demanding payment to regain access.
- Hybrid Ransomware: Hybrid ransomware combines elements of both encrypting and locker ransomware. It encrypts files while simultaneously locking the victim out of the system, amplifying the impact and urgency of the attack.

The anatomy of a ransomware attack
Phase 4: Deployment of ransomware payload

To deploy the ransomware payload effectively, threat actors may leverage various techniques including:

- Email Attachments and Links: Malicious attachments or links embedded within phishing emails are a common delivery method for ransomware. Opening the attachment or clicking on the link initiates the download and execution of the ransomware payload.
- Drive-by Downloads: By visiting compromised or malicious websites, victims unknowingly trigger the download and execution of ransomware through vulnerabilities in their web browsers or plugins.
- Exploit Kits: Exploit kits can exploit vulnerabilities in software or operating systems to deliver ransomware onto the victim’s system. The kits automatically detect and target vulnerabilities, enabling threat actors to distribute the ransomware payload more efficiently.

The anatomy of a ransomware attack
Phase 5: Encryption and impact

The true consequences of the attack begin to unfold during the encryption and impact phase. During this phase, threat actors encrypt the victim’s files and inflict significant damage on their systems.

Ransomware employs sophisticated encryption algorithms to lock the victim’s files, rendering them inaccessible without the decryption key. The encryption process typically targets a wide range of file types, including documents, images, videos, databases, and more. Threat actors often use strong encryption algorithms like RSA or AES to ensure the victim cannot decrypt the files without the decryption key.

As the encryption process unfolds, the victim’s files become unusable, with each file typically receiving a unique encryption key. The ransomware may also overwrite or modify the original file, making recovery without the decryption key even more challenging. The impact on the victim’s systems can be severe, leading to operational disruption, data loss, financial consequences, and reputational damage.

The anatomy of a ransomware attack
Phase 5: Encryption and impact

The consequences of a successful ransomware attack can be devastating for both organizations and individuals, and often entails many of the following:

- Operational Disruption: Ransomware attacks can cripple an organization’s operations, causing significant disruptions and downtime. Critical systems may become inaccessible, leading to productivity losses, delayed services, and financial repercussions.
- Data Loss and Corruption: If proper backups are not in place, victims may lose access to their valuable data permanently. Ransomware may also corrupt files during the encryption process, making recovery even more challenging.
- Financial Losses: Organizations may face substantial financial losses due to ransom payments, costs associated with recovery and remediation efforts, and potential regulatory penalties. Moreover, there may be indirect financial impacts stemming from reputational damage and customer loss.
- Reputational Damage: Publicly disclosed ransomware attacks can tarnish an organization’s reputation. Clients, partners, and stakeholders may lose trust in the organization’s ability to protect sensitive information, leading to a loss of business opportunities and customer confidence.
- Legal and Regulatory Ramifications: Depending on the nature of the compromised data, organizations may face legal and regulatory consequences, especially if personal or sensitive information is involved. Violations of data protection regulations can result in significant fines and legal liabilities

The anatomy of a ransomware attack
Phase 6: Extortion and communication

In Phase 6 of a ransomware attack, threat actors establish communication with their victims and begin the process of extortion. At this time, they'll demand ransom payments in exchange for providing the decryption keys or access to the victim's systems.

During this phase, threat actors initiate contact with the victim to convey their demands and establish a line of communication. They often use anonymizing technologies, such as the Tor network, to mask their identities and make it difficult to trace their activities. Communication can occur through various channels, including email, instant messaging platforms, or even dedicated ransom negotiation portals set up by the attackers.

The anatomy of a ransomware attack
Phase 6: Extortion and communication

Threat actors employ different methods to demand ransom payments from their victims. These may include:

- Bitcoin or Cryptocurrency Payments: Threat actors typically demand ransom payments in cryptocurrencies, such as Bitcoin, due to the pseudonymous and decentralized nature of these currencies, which makes them difficult to trace.
- Payment Deadlines and Threats: Threat actors often impose strict deadlines for payment, accompanied by threats of permanently deleting the decryption keys or increasing the ransom amount if the deadline is not met. These tactics aim to pressure victims into complying with their demands.
- Proof of Data Exfiltration: In some cases, threat actors may claim to have exfiltrated sensitive data from the victim’s systems and threaten to publicly release it unless the ransom is paid. This adds an additional layer of pressure and urgency for victims to comply.

The anatomy of a ransomware attack
Phase 6: Extortion and communication

Engaging or not engaging with threat actors during the extortion phase raises legal and ethical considerations. Organizations must carefully evaluate their options:

- Legal Considerations: Paying the ransom may be illegal in some jurisdictions or against organizational policies. Additionally, organizations may have legal obligations to report the incident, particularly if personal or sensitive data has been compromised.
- Funding Criminal Activities: Paying the ransom may contribute to funding further criminal activities, as the money can be used to finance future attacks. Supporting cybercriminals through ransom payments perpetuates the ransomware ecosystem.
- No Guarantee of Decryption: There is no guarantee that threat actors will provide the decryption keys or restore access to the victim’s systems even after the ransom is paid. Organizations must consider the risk of paying the ransom and not receiving the promised outcome.
- Cyber Insurance Coverage: Organizations with cyber insurance policies should consult with their insurance providers regarding their coverage and the implications of paying the ransom.

It is crucial for organizations to consult legal counsel, law enforcement agencies, and experienced incident response professionals before making any decisions regarding ransom payment. Each situation is unique, and a thorough evaluation of the risks, legal obligations, and ethical considerations is necessary.

The anatomy of a ransomware attack
Phase 7: Recovery and mitigation

The recovery and mitigation phase of an attack is where organizations focus on restoring systems, recovering encrypted data, and implementing measures to prevent future attacks.

Recovering from a ransomware attack requires a systematic approach. Key strategies for recovering encrypted data and restoring systems include:

- Isolate and Contain: Immediately isolate the affected systems to prevent further spread of the ransomware. Disconnect compromised devices from the network and shut them down to mitigate the risk of re-infection.
- Incident Analysis: Conduct a thorough analysis of the incident to identify the ransomware variant, its impact, and the compromised systems. This analysis can help determine the appropriate recovery strategy.
- Data Restoration: If backups are available, restore data from clean and secure backups. It is crucial to ensure backups are offline or properly protected to prevent them from being compromised by the ransomware.
- Decrypting Data: In some cases, decryption tools may be available from trusted sources, such as law enforcement agencies or security companies. These tools can help decrypt files without paying the ransom. However, this is not always possible, depending on the specific ransomware variant.
- System Rebuilding: In situations where data restoration is not feasible or backups are unavailable,

The anatomy of a ransomware attack
Phase 7: Recovery and mitigation

Effectively responding to ransomware incidents requires a well-defined incident response plan, and may include some of these best practices:

- Incident Response Plan: Develop a comprehensive incident response plan that outlines the steps to be taken in the event of a ransomware attack. This plan should include roles and responsibilities, communication protocols, and predefined actions for different scenarios.
- Rapid Response: Ensure you have the alerting capabilities to act swiftly and decisively to contain the attack, isolate affected systems, and initiate the recovery process. Promptly engage internal IT teams, incident response experts, and relevant stakeholders.
- Communication and Notification: Establish clear lines of communication both internally and externally. Notify appropriate personnel, such as legal, PR, and executive teams, and consider legal and regulatory obligations for disclosing incidents involving compromised data.
- Forensic Investigation: Conduct a thorough forensic investigation to understand the root cause, identify the attack vector, and collect evidence for potential legal actions or future prevention measures.
- Employee Awareness and Training: Continuously educate employees about the risks of ransomware, phishing, and social engineering. Regularly train staff on cybersecurity best practices, including strong password management, recognizing suspicious emails, and reporting incidents promptly.

The anatomy of a ransomware attack
Phase 7: Recovery and mitigation

Prevention is key in mitigating future ransomware attacks. Implementing proactive security measures can significantly reduce the risk and impact of such incidents. Consider these important measures:

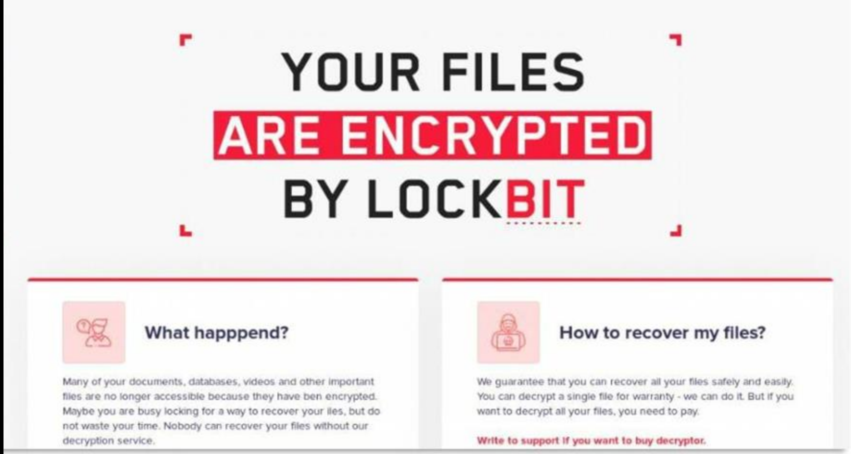
- Patch Management: Regularly apply security patches and updates to operating systems, software, and firmware to address known vulnerabilities that threat actors often exploit.
- Endpoint Protection: Deploy robust antivirus and anti-malware solutions, along with advanced endpoint detection and response (EDR) tools to detect and block malicious activities.
- Network Segmentation: Implement network segmentation to restrict lateral movement and contain the impact of an attack. Separating critical systems from the rest of the network helps prevent the rapid spread of ransomware.
- Least Privilege Access: Enforce the principle of least privilege, granting users only the necessary access rights required to perform their duties. This minimizes the potential damage that can be caused by compromised accounts.
- Regular Data Backups: Maintain regular, encrypted, and secure offline backups of critical data. Regularly test the restoration process to ensure backups are viable for recovery in the event of a ransomware incident.

The anatomy of a ransomware attack
EXTRA: Negotiation

is an interpersonal decision-making process that becomes necessary when it is not possible to achieve one's goals unilaterally.
The negotiator is the entity, for each party, who conducts the negotiation.

The anatomy of a ransomware attack
EXTRA: Negotiation

…during a ransomware attack typically takes place in a restricted-access chat.



YOUR FILES ARE ENCRYPTED BY LOCKBIT

What happpend?

Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Maybe you are busy locking for a way to recover your iles, but do not waste your time. Nobody can recover your files without our decryption service.

How to recover my files?

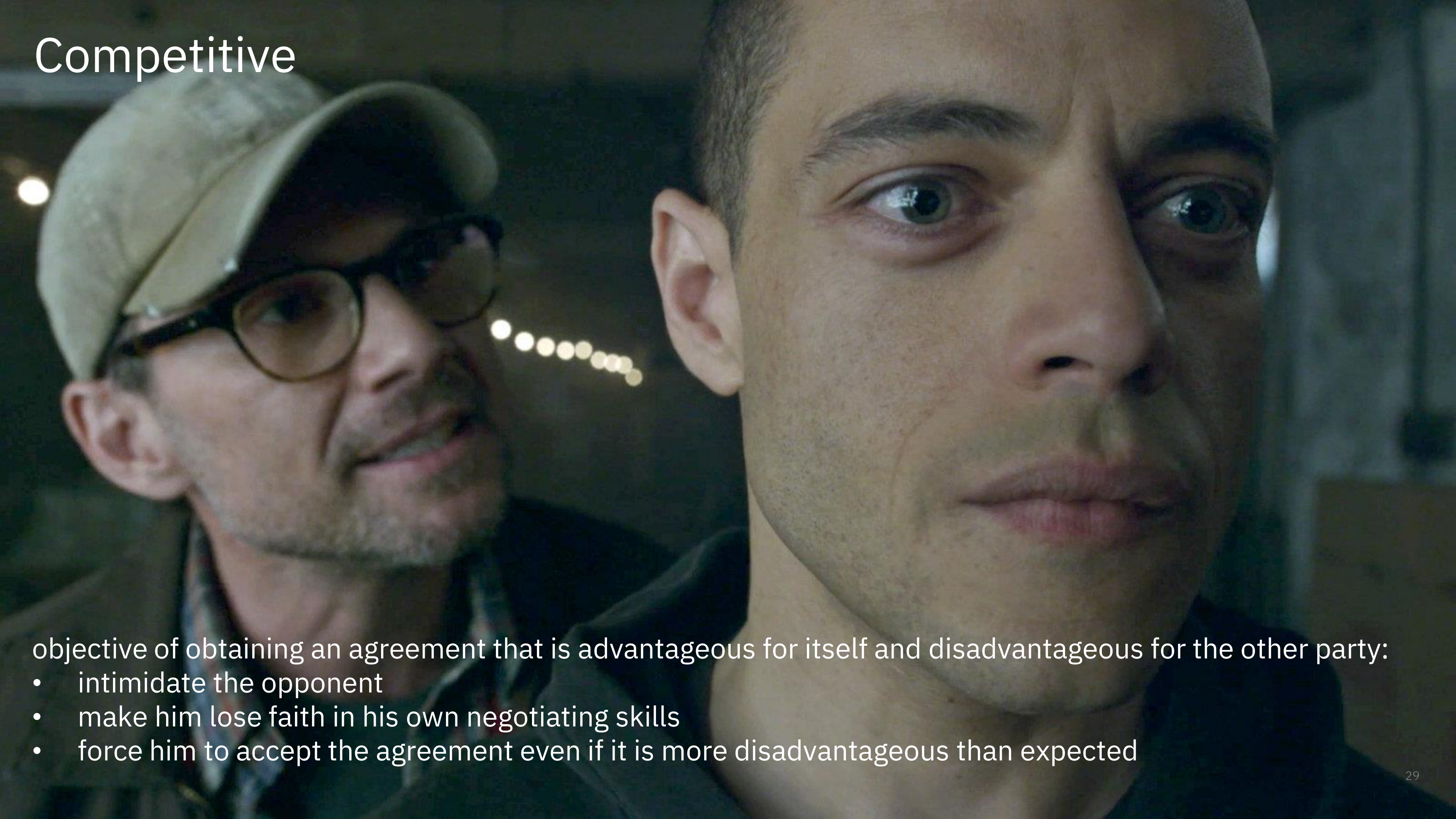
We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

Write to support if you want to buy decryptor.

The anatomy of a ransomware attack
EXTRA: Negotiation

3 types of negotiation

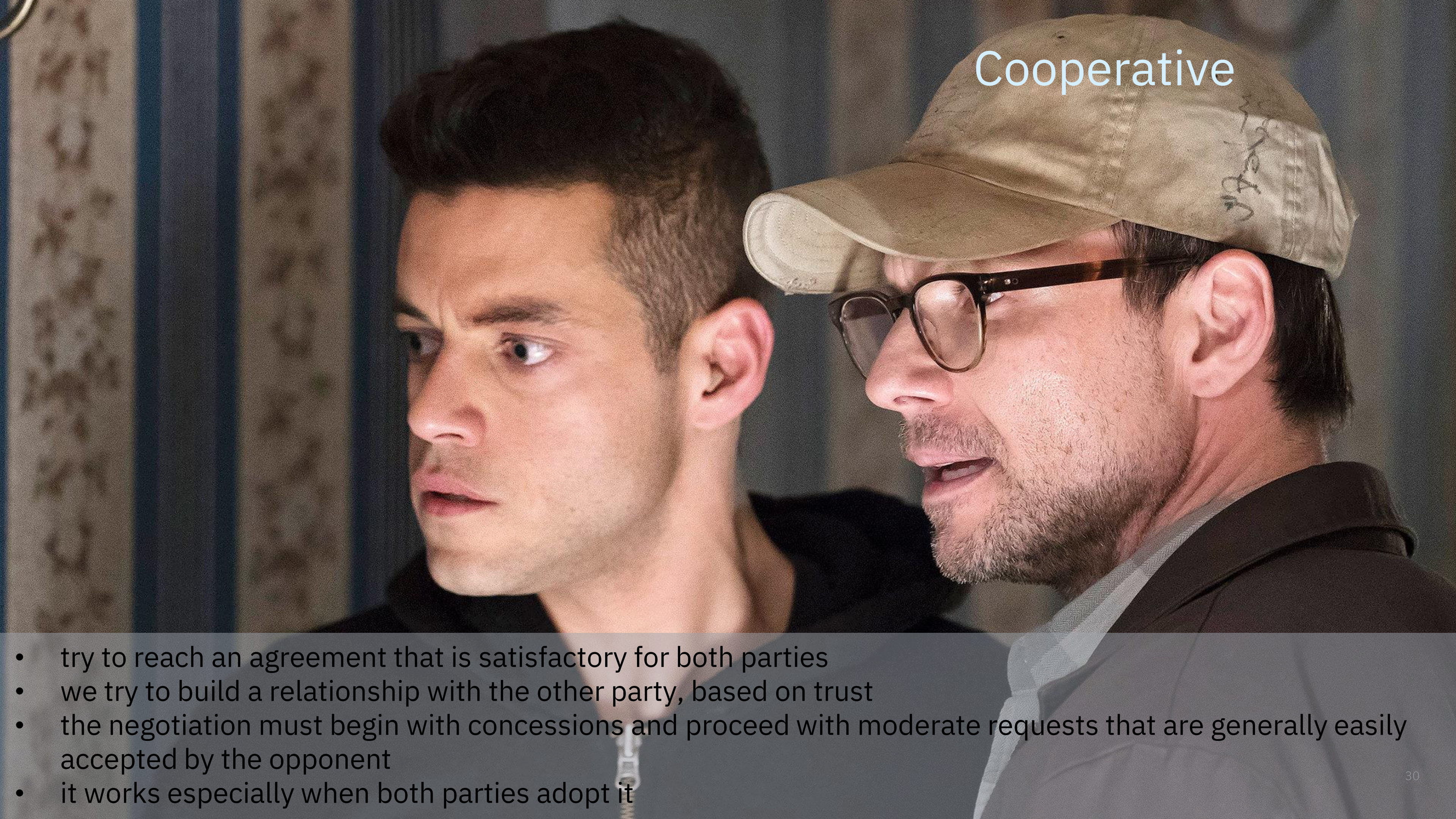
- Competitive
- Cooperative
- Integrative



Competitive

objective of obtaining an agreement that is advantageous for itself and disadvantageous for the other party:

- intimidate the opponent
- make him lose faith in his own negotiating skills
- force him to accept the agreement even if it is more disadvantageous than expected



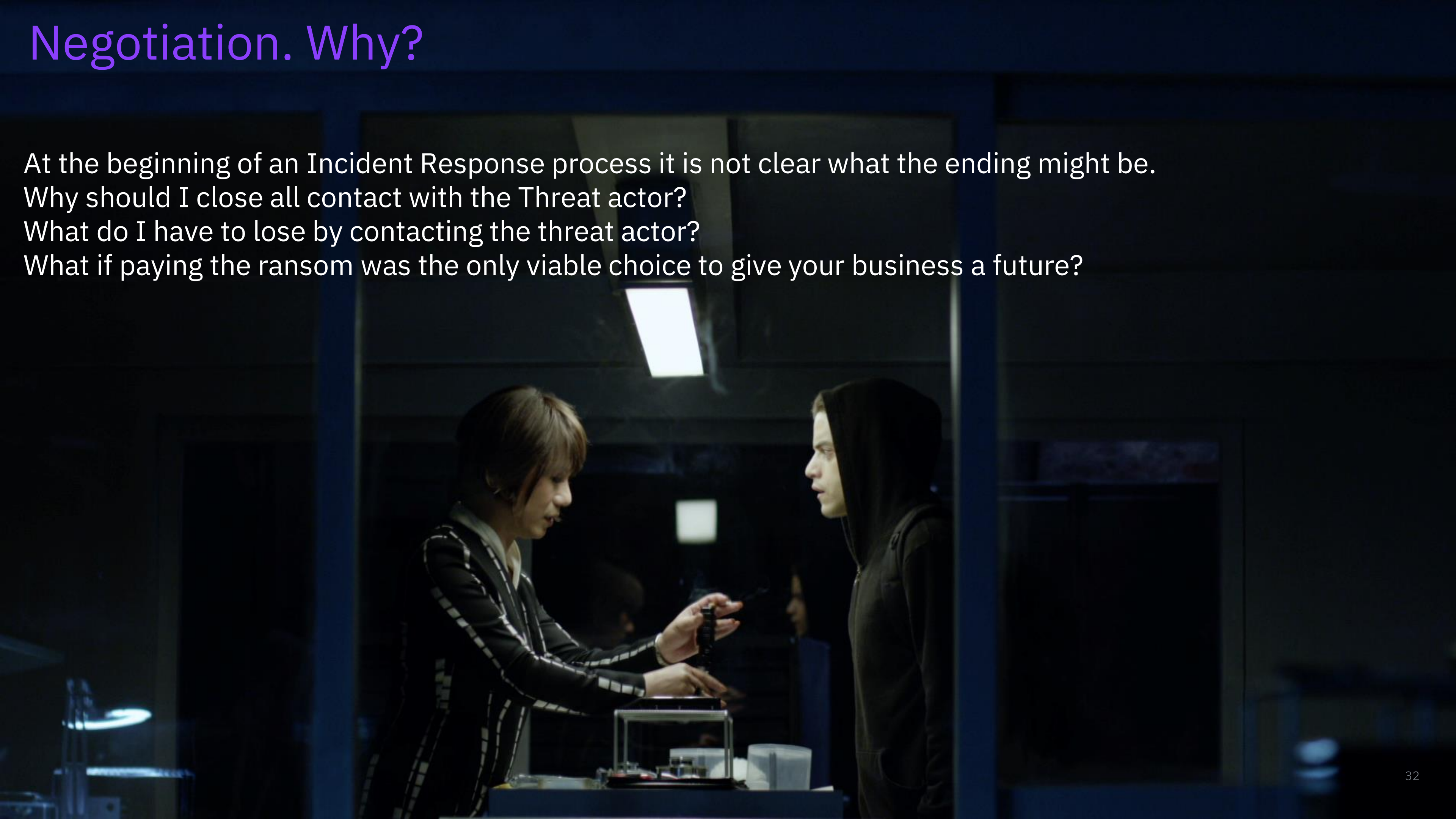
Cooperative

- try to reach an agreement that is satisfactory for both parties
- we try to build a relationship with the other party, based on trust
- the negotiation must begin with concessions and proceed with moderate requests that are generally easily accepted by the opponent
- it works especially when both parties adopt it

Integrative

- combines the 2 approaches
- both parties try to get as many concessions as possible from the other party
- as in the cooperative approach, the litigants attempt to reach an amicable settlement to the dispute

Negotiation. Why?



At the beginning of an Incident Response process it is not clear what the ending might be.
Why should I close all contact with the Threat actor?
What do I have to lose by contacting the threat actor?
What if paying the ransom was the only viable choice to give your business a future?

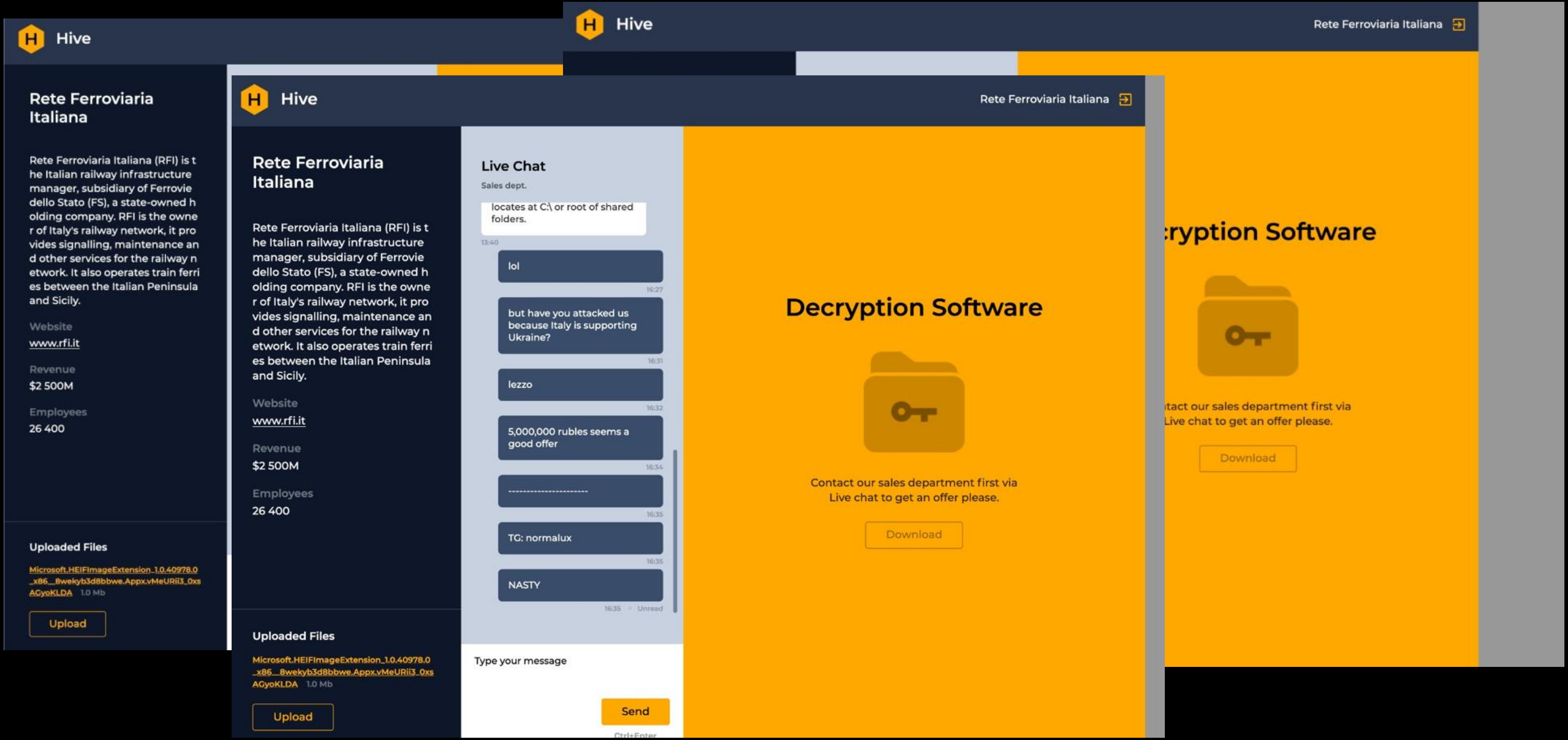
Assumptions

...the ransom amount is not decided randomly

Threat Actor:

- don't like negotiators
- want our money
- invest money to attack
- need our money

RFI got hacked, Hive got trolled



Hive

Rete Ferroviaria Italiana

Rete Ferroviaria Italiana

Rete Ferroviaria Italiana (RFI) is the Italian railway infrastructure manager, subsidiary of Ferrovie dello Stato (FS), a state-owned holding company. RFI is the owner of Italy's railway network, it provides signalling, maintenance and other services for the railway network. It also operates train ferries between the Italian Peninsula and Sicily.

Website
www.rfi.it

Revenue
$2 500M

Employees
26 400

Uploaded Files

Microsoft.HEIFImageExtension_1.0.40978.0_x86__8wekyb3d8bbwe.Appx.vMeURii3_0xsAGyoKLDA 1.0 Mb

Upload

Live Chat

Sales dept.

locates at C:\ or root of shared folders.
13:40

lol
16:27

but have you attacked us because Italy is supporting Ukraine?
16:31

lezzo
16:32

5,000,000 rubles seems a good offer
16:34

16:35

TG: normalux
16:35

NASTY
16:35 · Unread

Type your message

Send
Ctrl+Enter

Decryption Software

Contact our sales department first via Live chat to get an offer please.

Download

Hive

Rete Ferroviaria Italiana

Rete Ferroviaria Italiana (RFI) is the Italian railway infrastructure manager, subsidiary of Ferrovie dello Stato (FS), a state-owned holding company. RFI is the owner of Italy's railway network, it provides signalling, maintenance and other services for the railway network. It also operates train ferries between the Italian Peninsula and Sicily.

Website
www.rfi.it

Revenue
$2 500M

Employees
26 400

Uploaded Files

Microsoft.HEIFImageExtension_1.0.40978.0_x86__8wekyb3d8bbwe.Appx.vMeURii3_0xsAGyoKLDA 1.0 Mb

Upload

Hive

Rete Ferroviaria Italiana

cryption Software

tact our sales department first via Live chat to get an offer please.

Download

Dos

- calm and patience (which is the virtue of the strong!)
- maintain a professional and respectful tone
- show empathy towards the Threat Actor's situation and objectives
- make it clear to the other party that he is talking to the person who(or who is close to whom) can make decisions
- try to establish “tactical empathy” by mirroring the hacker’s language patterns
- look for information on the gang that attacked your organization. You need to know the counterparty's reputation in order to best deal with it
- ask for proof of good functioning of the decryptor, both on small and large files
- make sure the negotiation chat is secure (AKA the private link has not been shared)
- prepares communications (precise, complete, transparent) for the various stakeholders

Don’ts

- don't try to fix the situation on your own. Involve relevant authorities and experts. Negotiation is not a theme to be improvised!
- do not share personal or confidential information with the gang. Just discuss the specific data and ransom situation
- do not name any involvement of insurance companies
- do not threaten or provoke the Threat Actor. This could make the situation even more tense and damaging.

Ransomware: Tactics, Techniques, and Procedures (TTPs)

TTPs stands for tactics, techniques, and procedures. This is the term used by cybersecurity professionals to describe the behaviors, processes, actions, and strategies used by a threat actor to develop threats and engage in cyberattacks.

The ***National Institute of Standards and Technology*** (NIST) describes tactics as being the highest-level description of the behavior. Techniques are a more detailed description of the threat actor's actions within the context of a tactic. Procedures are an even lower level, more detailed description of the activities within the context of a technique.

- **Tactics**–The overall goals behind the attack and the general strategies followed by the threat actor to implement the attack. For example, the threat actor's goal may be to infiltrate a website to steal customer credit card information.

- **Techniques**–The method used by the threat actor to engage in the attack, such as e-skimming, magecart, javascript injection attacks, or cross-site scripting (XSS).

- **Procedures**–The step-by-step description of the attack, including the tools and methods used to orchestrate it. Cybersecurity analysts most often use an attack's procedures to help create a profile or fingerprint for a threat actor or threat group.

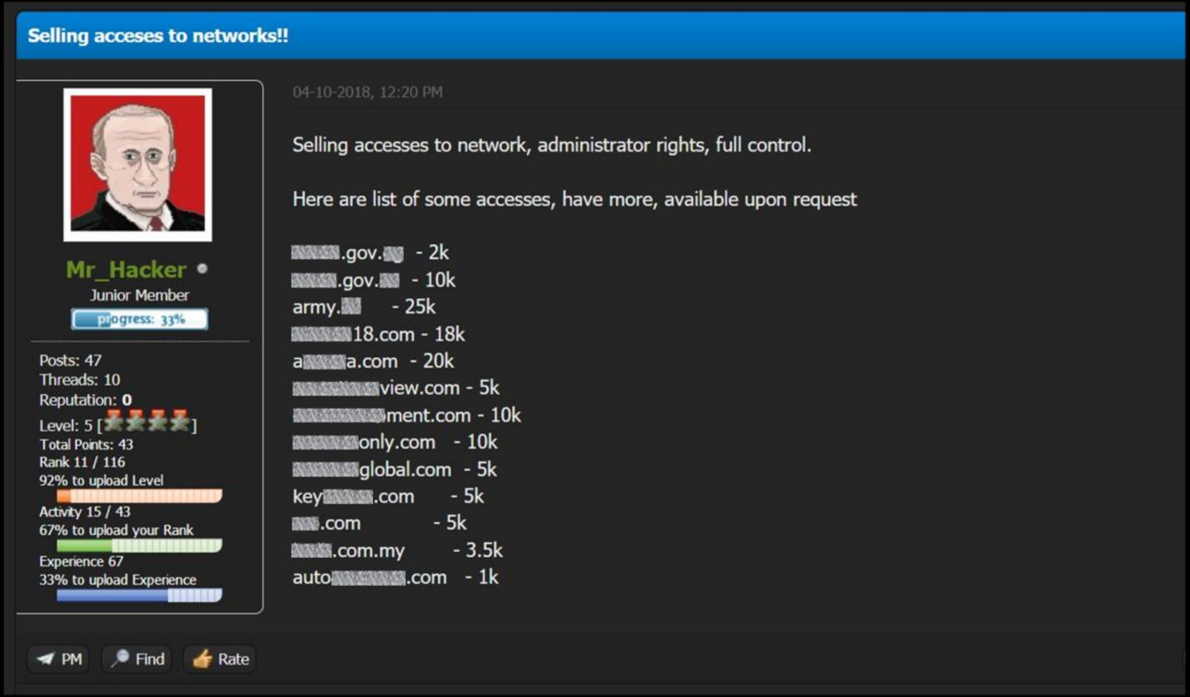
What are TTPs used for?

Security professionals define and analyze the tactics, techniques, and procedures of a threat actor to help them in counterintelligence efforts. TTPs can help security researchers correlate an attack to a known hacker or threat group and better understand an attack framework. TTPs help researchers focus their investigation path, identify threat source or attack vectors, define the severity of the threat, and support incident response and threat mitigation. Security professionals also use TTPs in threat modeling activities.

TTP research also goes beyond basic forensics. By identifying threat actors and groups, security researchers can ascertain relationships that may exist with other attackers. TTPs can also aid in identifying emerging threats and in developing threat and attack countermeasures.

IAB - Initial Access Broker

An Initial Access Broker (IAB) is a threat actor specializing in infiltrating computer systems and networks, then selling that unauthorized access to other malicious actors. IABs are skilled at identifying and exploiting security vulnerabilities, providing services to ransomware groups and other bad actors.



Selling acceses to networks!!

04-10-2018, 12:20 PM

Mr_Hacker
Junior Member
progress: 33%

Posts: 47
Threads: 10
Reputation: 0
Level: 5 [★★★★]
Total Points: 43
Rank 11 / 116
92% to upload Level
Activity 15 / 43
67% to upload your Rank
Experience 67
33% to upload Experience

Selling accesses to network, administrator rights, full control.

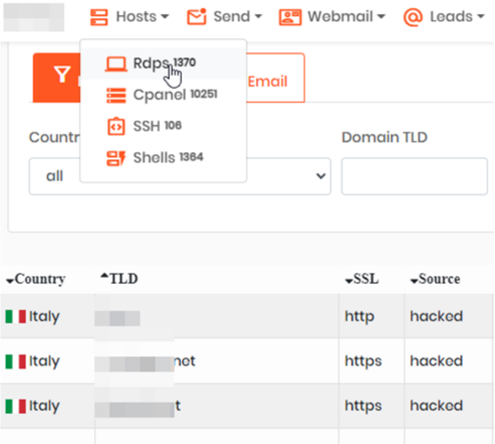
Here are list of some accesses, have more, available upon request

[redacted].gov.[redacted] - 2k
[redacted].gov.[redacted] - 10k
army.[redacted] - 25k
[redacted]18.com - 18k
a[redacted]a.com - 20k
[redacted]view.com - 5k
[redacted]ment.com - 10k
[redacted]only.com - 10k
[redacted]global.com - 5k
key[redacted].com - 5k
[redacted].com - 5k
[redacted].com.my - 3.5k
auto[redacted].com - 1k

IAB - Initial Access Broker

Initial access brokers sell various types of network access:

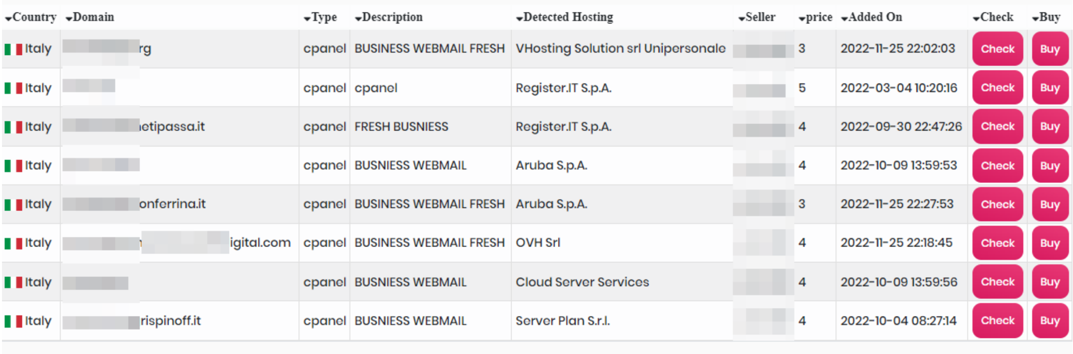
- Remote Desktop Protocol (RDP)
- VPN
- Web Shell Attack
- Remote Monitoring and Management (RMM)
- Active Directory



Countr: all

Domain TLD:

Country	TLD	SSL	Source
Italy	[redacted]	http	hacked
Italy	[redacted]net	https	hacked
Italy	[redacted]t	https	hacked



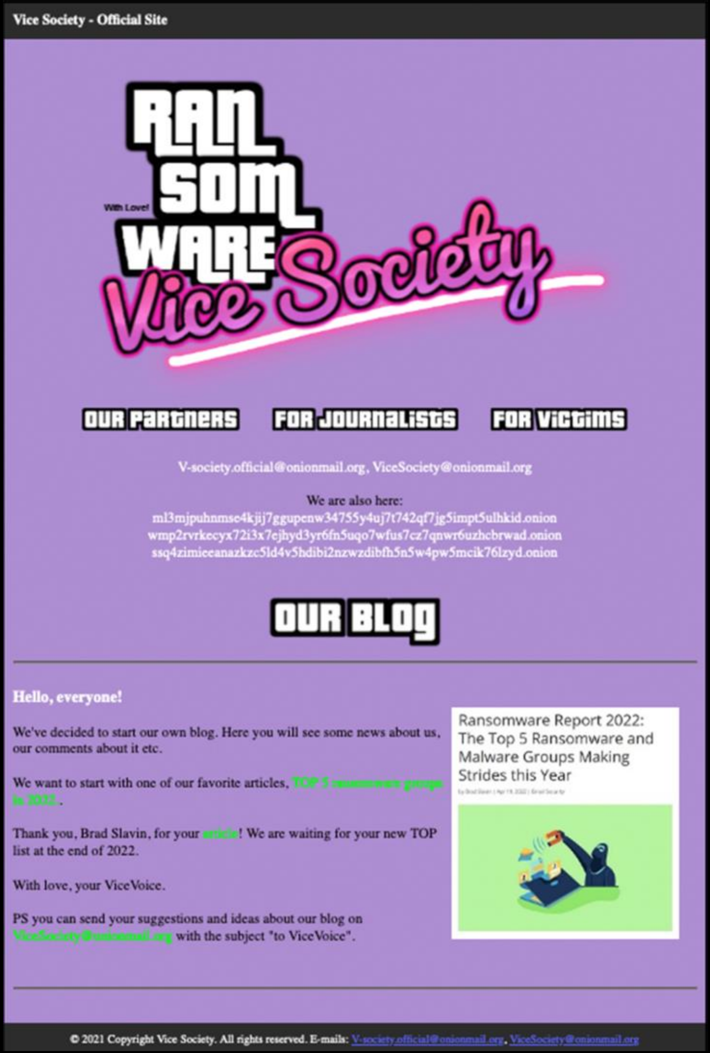
Country	Domain	Type	Description	Detected Hosting	Seller	price	Added On	Check	Buy
Italy	[redacted]rg	cpanel	BUSINESS WEBMAIL FRESH	VHosting Solution srl Unipersonale	[redacted]	3	2022-11-25 22:02:03	Check	Buy
Italy	[redacted]	cpanel	cpanel	Register.IT S.p.A.	[redacted]	5	2022-03-04 10:20:16	Check	Buy
Italy	[redacted]etipassa.it	cpanel	FRESH BUSNIESS	Register.IT S.p.A.	[redacted]	4	2022-09-30 22:47:26	Check	Buy
Italy	[redacted]	cpanel	BUSNIESS WEBMAIL	Aruba S.p.A.	[redacted]	4	2022-10-09 13:59:53	Check	Buy
Italy	[redacted]onferrina.it	cpanel	BUSINESS WEBMAIL FRESH	Aruba S.p.A.	[redacted]	3	2022-11-25 22:27:53	Check	Buy
Italy	[redacted]igital.com	cpanel	BUSINESS WEBMAIL FRESH	OVH Srl	[redacted]	4	2022-11-25 22:18:45	Check	Buy
Italy	[redacted]	cpanel	BUSNIESS WEBMAIL	Cloud Server Services	[redacted]	4	2022-10-09 13:59:56	Check	Buy
Italy	[redacted]rispinoff.it	cpanel	BUSNIESS WEBMAIL	Server Plan S.r.l.	[redacted]	4	2022-10-04 08:27:14	Check	Buy

Data Leak Site

The confidentiality of the data is compromised by threat actors to incentivize the obtained information and extort money from businesses.

These sites can contain sensitive information such as login credentials, intellectual property, personal, and financial data, etc, that puts an organization at risk of security breaches, identity theft, financial fraud, reputational damage, and legal consequences.

Group-IB



V-society.official@onionmail.org, ViceSociety@onionmail.org

We are also here:
ml3mjpuhnmse4kjij7ggupenw34755y4uj7t742qf7jg5impt5ulhkid.onion
wmp2rvrkecyx72i3x7ejhyd3yr6fn5uqo7wfus7cz7qnwr6uzhcbrwad.onion
ssq4zimieeanazkzc5ld4v5hdibi2nzwzdibfh5n5w4pw5mcik76lzyd.onion

Hello, everyone!

We've decided to start our own blog. Here you will see some news about us, our comments about it etc.

We want to start with one of our favorite articles, TOP 5 ransomware groups in 2022.

Thank you, Brad Slavin, for your article! We are waiting for your new TOP list at the end of 2022.

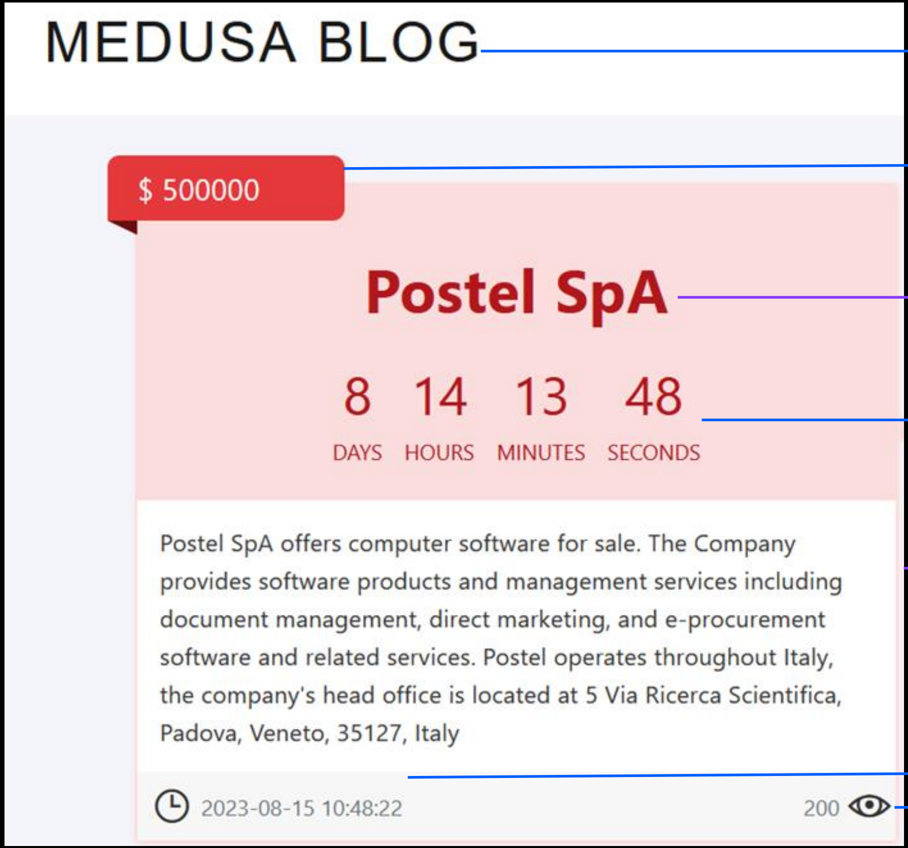
With love, your ViceVoice.

PS you can send your suggestions and ideas about our blog on ViceSociety@onionmail.org with the subject "to ViceVoice".

Ransomware Report 2022: The Top 5 Ransomware and Malware Groups Making Strides this Year

© 2021 Copyright Vice Society. All rights reserved. E-mails: V-society.official@onionmail.org, ViceSociety@onionmail.org

Data Leak Site: Postel SpA



MEDUSA BLOG

$ 500000

Postel SpA

8 DAYS 14 HOURS 13 MINUTES 48 SECONDS

Postel SpA offers computer software for sale. The Company provides software products and management services including document management, direct marketing, and e-procurement software and related services. Postel operates throughout Italy, the company's head office is located at 5 Via Ricerca Scientifica, Padova, Veneto, 35127, Italy

2023-08-15 10:48:22

200

Gang Name

Ransom

Victim Name

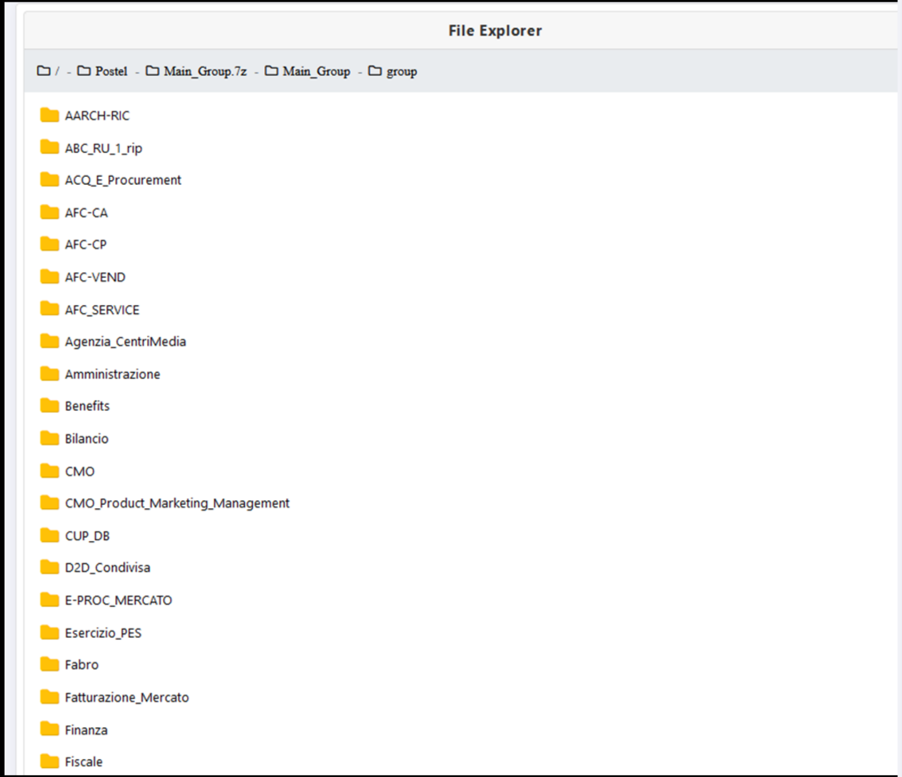
Countdown

Victim Information

Timestamp

Views

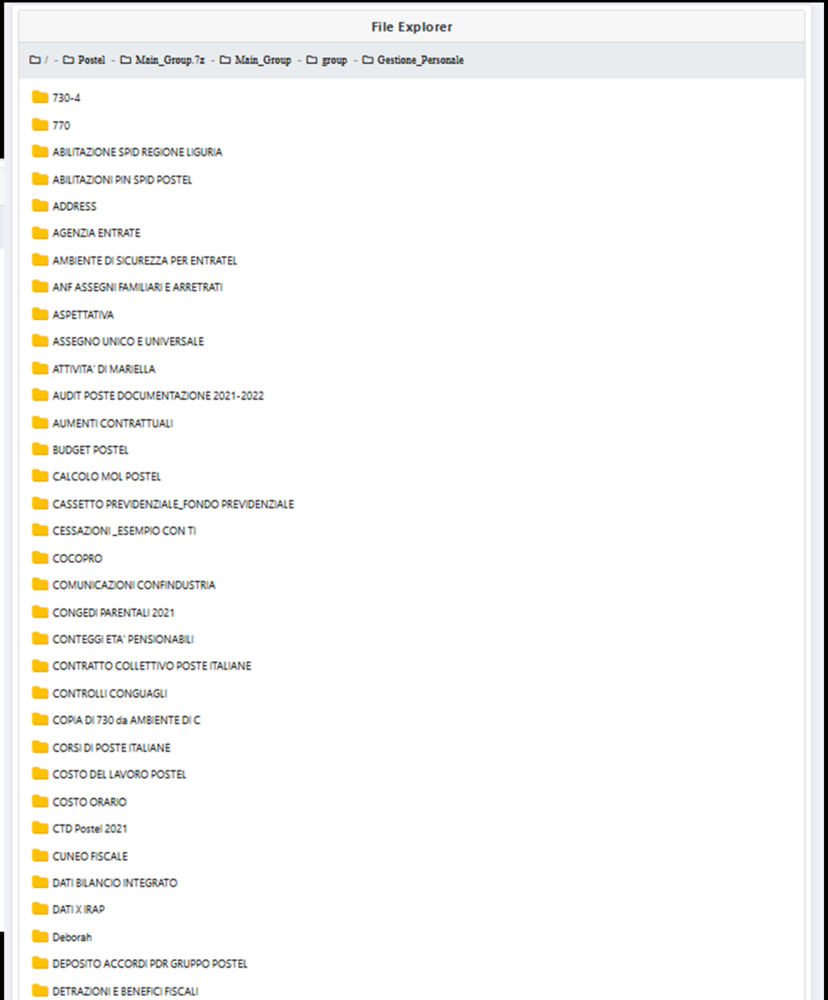
Data Leak Site: Postel SpA



File Explorer

🗀 / - 🗀 Postel - 🗀 Main_Group.7z - 🗀 Main_Group - 🗀 group

- AARCH-RIC
- ABC_RU_1_rip
- ACQ_E_Procurement
- AFC-CA
- AFC-CP
- AFC-VEND
- AFC_SERVICE
- Agenzia_CentriMedia
- Amministrazione
- Benefits
- Bilancio
- CMO
- CMO_Product_Marketing_Management
- CUP_DB
- D2D_Condivisa
- E-PROC_MERCATO
- Esercizio_PES
- Fabro
- Fatturazione_Mercato
- Finanza
- Fiscale



File Explorer

🗀 / - 🗀 Postel - 🗀 Main_Group.7z - 🗀 Main_Group - 🗀 group - 🗀 Gestione_Personale

- 730-4
- 770
- ABILITAZIONE SPID REGIONE LIGURIA
- ABILITAZIONI PIN SPID POSTEL
- ADDRESS
- AGENZIA ENTRATE
- AMBIENTE DI SICUREZZA PER ENTRATEL
- ANF ASSEGNI FAMILIARI E ARRETRATI
- ASPETTATIVA
- ASSEGNO UNICO E UNIVERSALE
- ATTIVITA' DI MARIELLA
- AUDIT POSTE DOCUMENTAZIONE 2021-2022
- AUMENTI CONTRATTUALI
- BUDGET POSTEL
- CALCOLO MOL POSTEL
- CASSETTO PREVIDENZIALE_FONDO PREVIDENZIALE
- CESSAZIONI _ESEMPIO CON TI
- COCOPRO
- COMUNICAZIONI CONFINDUSTRIA
- CONGEDI PARENTALI 2021
- CONTEGGI ETA' PENSIONABILI
- CONTRATTO COLLETTIVO POSTE ITALIANE
- CONTROLLI CONGUAGLI
- COPIA DI 730 da AMBIENTE DI C
- CORSI DI POSTE ITALIANE
- COSTO DEL LAVORO POSTEL
- COSTO ORARIO
- CTD Postel 2021
- CUNEO FISCALE
- DATI BILANCIO INTEGRATO
- DATI X IRAP
- Deborah
- DEPOSITO ACCORDI PDR GRUPPO POSTEL
- DETRAZIONI E BENEFICI FISCALI

RaaS Model

Ransomware as a Service (RaaS) is a business model between ransomware operators and affiliates in which affiliates pay to launch ransomware attacks developed by operators. Think of ransomware as a service as a variation of software as a service (SaaS) business model.

RaaS kits allow affiliates lacking the skill or time to develop their own ransomware variant to be up and running quickly and affordably. They are easy to find on the dark web, where they are advertised in the same way that goods are advertised on the legitimate web.

A RaaS kit may include 24/7 support, bundled offers, user reviews, forums and other features identical to those offered by legitimate SaaS providers. The price of RaaS kits ranges from $40 per month to several thousand dollars – trivial amounts, considering that the average ransom demand in 2021 was $6 million. A threat actor doesn’t need every attack to be successful in order to become rich.

How the RaaS Model Works

The table below outlines the roles operators and affiliates play in the RaaS model:

RaaS Operators	RaaS Affiliates
Recruits affiliates on forums	Pays to use the ransomware Agrees on a service fee per collected ransom
Gives affiliates access to a "build your own ransomware package" panel Creates a dedicated "Command and Control" dashboard for the affiliate to track the package	Targets victims Sets ransom demands Configures post-compromise user messages
	Compromises the victim's assets Maximizes the infection using "living off the land" techniques Executes ransomware
Sets up a victim payment portal "Assists" affiliates with victim negotiations	Communicates with the victim via chat portals or other communication channels
Manages a dedicated leak site	Manages decryption keys

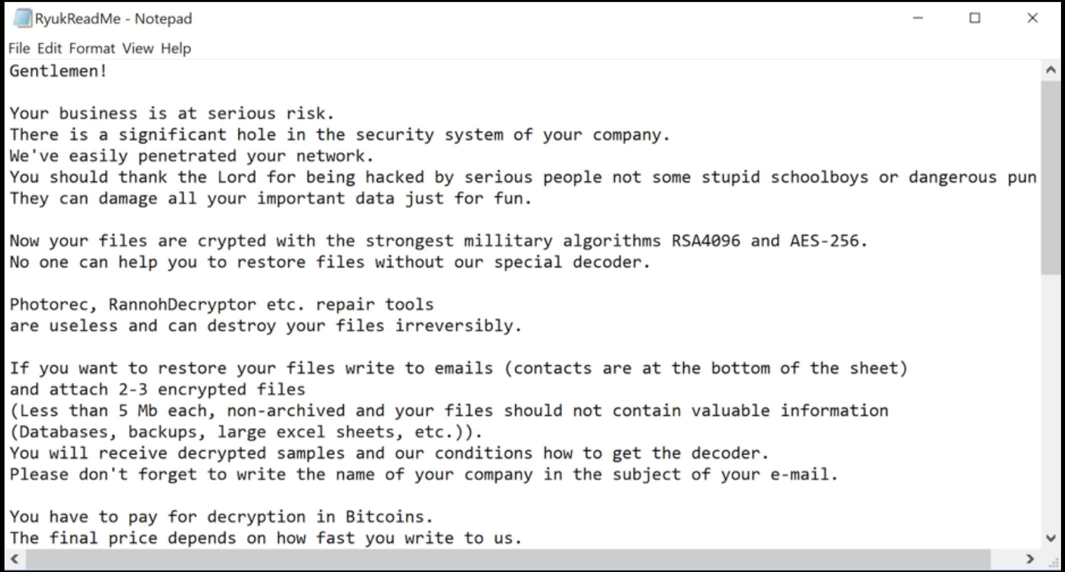
RaaS revenue models

There are 4 common RaaS revenue models:

1. Monthly subscription for a flat fee
2. Affiliate programs, which are the same as a monthly fee model but with a percent of the profits (typically 20-30%) going to the ransomware developer
3. One-time license fee with no profit sharing
4. Pure profit sharing

Ransom Note

A ransom note is tied to the main purpose of why a ransomware virus exists – to hold your data or whole device hostage until you pay the criminals huge amount of money in the form of BitCoin. Usually this note may appear in the form of a wallpaper, text message or an .HTM, .HTML or other forms of files that may lead to an offline web page with the ransom message. Few examples of those can be seen below:



```
Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous pun
They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
```

Paying Cyber Extortion Demands in Cryptocurrency

One of the most common and serious cyber-attacks involves ransomware, in which a threat actor locks an organization’s data with encryption until a ransom demand is met. These attacks are increasing not only in number, but also in severity.

Bitcoin accounts for approximately 98% of ransomware payments. Whether an organization pays the ransom or attempts to recover the data independently, a clear understanding of bitcoin is essential for cyber incident response planning.

Paying Cyber Extortion Demands in Cryptocurrency

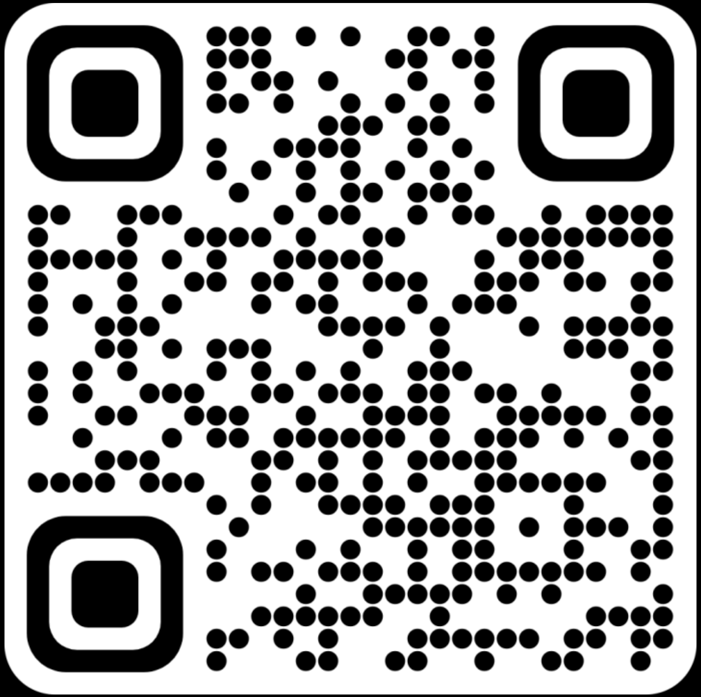
Why Bitcoin?

Anonymity. Speed. Access.

Bitcoin, like other cryptocurrencies, allows cybercriminals to receive funds with a high degree of anonymity, making transactions difficult to track. Bitcoin gained notoriety as the common currency of the Dark Web, where it remains popular. It is seen as the essential cryptocurrency — easy to acquire and use, making threat actors believe victims will be more likely to pay.

Occasionally, cyber threat actors demand other cryptocurrencies, such as Monero and Zcash. These have additional privacy features that make tracking payees more difficult, but are the exceptions to the rule.

Try It



Question and Answer

Sources

Thank You

UNIVERSITÀ DEGLI STUDI DEL SANNIO
Benevento

pimelillo@unisannio.it
pietro.melillo@redhotcyber.com
melillopietro@gmail.com

https://melillopietro.github.io/
https://janaralab.github.io/
https://www.linkedin.com/in/melillopietro/