DEFENCE TECH
Terra, Cielo, Mare, Spazio, Spazio cibernetico.
PROTEGGIAMOLI

Multi-extortion Ransomware and encryption-less attacks

Threat Intelligence Report

Summary

1

Our Malware Lab

1. Our Malware Lab

Defence Tech Malware Lab daily performs dissection of malware with the aim of timely understanding the technological evolutions of attacks, consolidating the knowledge of necessary to make more effective and faster the process of incidents responding, contributing to spreading information about emerging threats into the expert's community and among its clients.

Malware Lab analysts are continuously engaged in searching and experimenting new analysis tools, for increasing accuracy and scope of action with regard to the proliferation of new evasion and anti-analysis techniques adopted by malwares.

The Malware Lab is also committed to the development of proprietary tools for malware analysis and supporting the management and response of incidents.

Besides malware analysis, Malware Lab ideated and implemented an automatic process of extraction of **Indicators of Compromise (IOC)** that is daily run on dozens of new malwares, intercepted in the wide for populating our Knowledge Base.

CORRADO AARON VISAGGIO
Group Chief Scientist Officer & Malware Lab Director
a.visaggio@defencetech.it

2

Executive Summary

2. Executive Summary

We will discuss the evolving trends in ransomware attacks, specifically focusing on two strategies: multi-extortion tactics and encryption-less attacks.

Multi-extortion is a sophisticated approach employed by cybercriminals. In addition to exfiltrating the victim's data, the attacker also encrypts the files, making them inaccessible to the victim. Furthermore, the attackers may resort to additional coercive measures, such as launching distributed denial-of-service (DDoS) attacks and directly contacting the victim's customers or business partners. These tactics increase the pressure on the victims to comply with the ransom demands.

On the other hand, encryption-less attacks are a strategy that does not rely on file encryption but instead involves the unauthorized extraction of sensitive data, which is then used as leverage to demand a ransom. In these attacks, the threat actor gains access to the victim's files and exfiltrates them, creating a significant risk of data exposure and potential harm to the victim's reputation.

The emergence of encryption-less and multi-extortion strategies demonstrates a concerning evolution in ransomware attacks, as cybercriminals continuously adapt their methods to maximize their chances of financial gain. It is crucial for individuals and organizations to be aware of these evolving threats and take appropriate measures to protect their valuable data and systems.

3

Threat intelligence

3. Threat intelligence

Based on our extensive research, it is evident that cybercriminal groups are actively refining their methods to maximise their operational efficiency: some groups are enhancing their extortion techniques by incorporating double or multi extortion attacks within the RaaS (Ransomware-as-a-Service) model, while others are shifting towards encryption-less attacks. A considerable amount of information published on various cybersecurity journal websites stems from ThreatLabz in the 2023 State of Ransomware report[1].

According to their report, the occurrence of double extortion attacks in industries has witnessed a significant surge from April 2022 to April 2023 (see figure 1). However, it is crucial to note that many attacks may remain unreported or undetected.

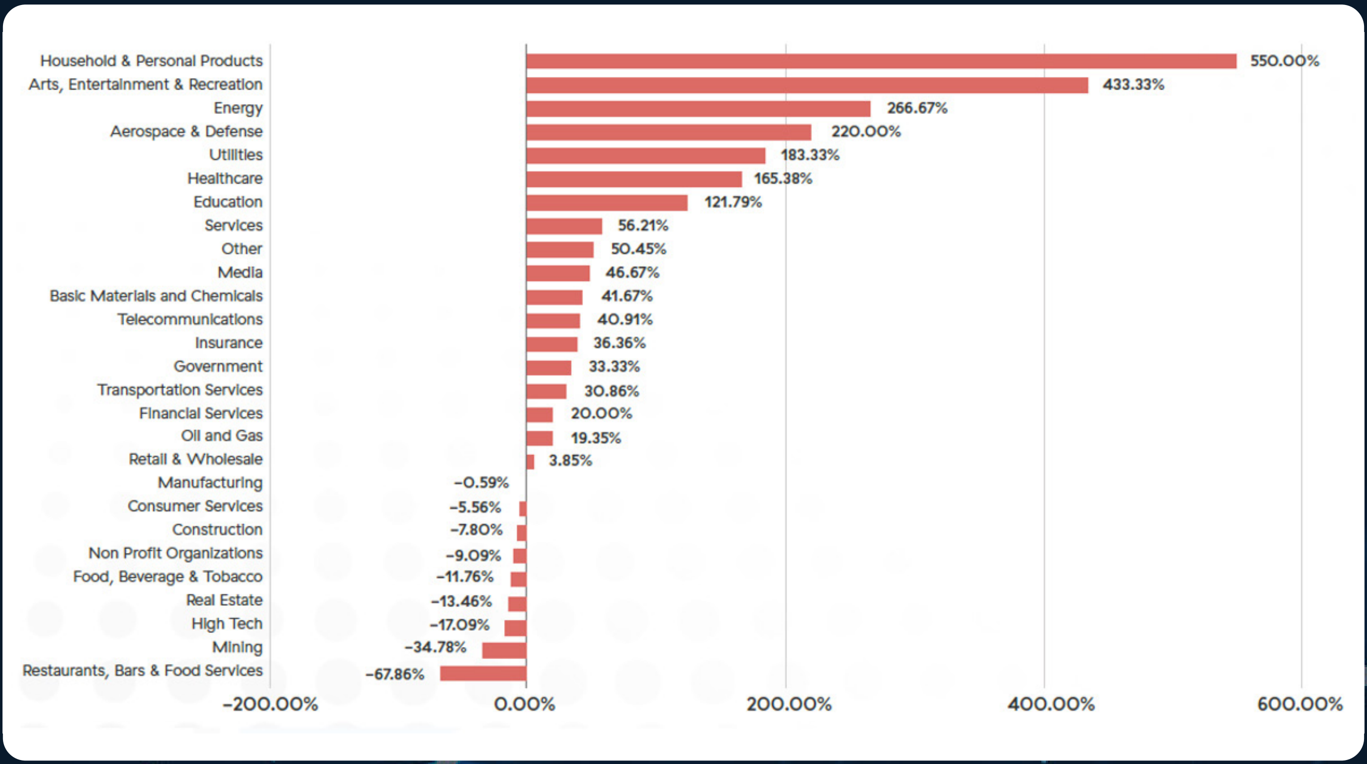


Figure 1. Percentage of growth

[1] *https://info.zscaler.com/resources-industry-reports-2023-threatlabz-ransomware-report*

3.1 Multi-extortion methods

Ransomware attacks mainly rely on encryption to deny access to files, accompanied by a ransom note providing instructions for payment. However, as file encryption alone became insufficient to get ransoms, threat actors began to weaponize the information within the files by improving their extortion methods.

The first notable evolution observed by analysts was the rise of the double extortion strategy[2], where the threat actors started exfiltrating files before encrypting them. For instance, a case that came under our analysis involved a ransomware which exfiltrated data before encrypting: DJVU/Stop Ransomware deploys Vidar Stealer[3]. In this analysis DJVU downloaded a second piece of malware named Vidar, which can steal both company documents and stored credentials, later used to attack partners or the same target again. Following the data exfiltration, the ransomware would proceed to encrypt the files. This example perfectly illustrates the concept of double extortion, as the attackers possess the victim's files, potentially containing sensitive information.

To exert maximum pressure on the victim, cybercriminals commonly employ countdown timers on leak sites before exposing the stolen data. Nevertheless, there are situations where organizations, despite having backup data, refuse to pay the ransom, choosing to risk the exposure of their sensitive data to the public.

In response to such cases, threat actors have developed triple and quadruple extortion strategies, constituting a multi-extortion tactic. Alongside exfiltration and encryption, attackers have started utilizing DDoS attacks to overload servers and disrupt the victim's services. These DDoS attacks are typically aimed at critical infrastructures within industries like healthcare or government organizations, where service interruptions directly impact public order.

Furthermore, threat actors have incorporated an additional phase into the attack process, whereby they directly contact the customers and business partners of the victim, notifying them of the stolen sensitive information. In certain instances, they may go even further by approaching competitors, offering to sell the stolen trade secrets. These new tactics serve to further exploit the impact of the attack by directly involving stakeholders beyond the victim organization.

[2] *https://www.zscaler.com/resources/security-terms-glossary/what-is-double-extortion-ransomware*

[3] *https://www.linkedin.com/posts/defence-tech-holding_report-djivustop-ransomware-deploys-vidar-activity-7067403444185182208-NGCE?utm_source=share&utm_medium=member_desktop*

3.2 Encryption-less ransom attacks

Threat actors consistently employ advanced techniques, tactics, and procedures (TTPs) to target critical infrastructure of organizations. However, developing a malicious program that bypasses anti-malware solutions and effectively encrypts victims' files requires significant financial resources, extensive effort, and advanced technical skills. As a result, several threat actors are now evolving their strategies to minimize the need for extensive skills, effort, and financial investment.

By embracing encryption-less tactics, these threat actors can achieve their objectives through alternative means. Rather than employing traditional file encryptio, certain cyber attackers adopt a different approach by prioritizing the data exfiltration phase. They exploit the stolen files as leverage to demand a ransom from the victim. This approach allows them to circumvent the complexities and costs associated with developing and maintaining sophisticated encryption mechanisms.

Early encryption-less attacks date back to 2021 from groups like Babuk[4] and SnapMC[5], as the model proved profitable more and more threat actors have been switching to it in recent times. We compiled a list of a few other well-known cases of threat actors who have been involved in encryption-less attacks:

- **BianLian:**

BianLian has been formerly known to use a double-extortion model, which involves both exfiltrating and encrypting victims' sensitive data to allow the extortion. However, in January 2023, the FBI and ACSC (Australian Cyber Security Centre) observed that BianLian shifted to purely exfiltration-based extortion, removing the encryption part of the attack[6]. This coincides with the release of a free decryption tool for the BianLian ransomware in January 2023 developed by the antivirus company Avast[7].

[4] *https://www.bleepingcomputer.com/news/security/babuk-quits-ransomware-encryption-focuses-on-data-theft-extortion/*

[5] *https://www.bleepingcomputer.com/news/security/snapmc-hackers-skip-file-encryption-and-just-steal-your-files/*

[6] *https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a*

[7] *https://decoded.avast.io/threatresearch/decrypted-bianlian-ransomware/*

LAPSUS$:

They are primarily focused on data extortion and have targeted a wide range of organizations, including Nvidia[8], Samsung[9], Microsoft[10], Uber[11] and more. Lapsus$ employs various cyberattack techniques, including breaches, ransomware campaigns and social engineering tactics. They have been known to exploit vulnerabilities, steal credentials, and gain unauthorized access to internal systems. The group has been active in posting stolen data on public forums and using it as leverage for extortion. Lapsus$ has been linked to multiple incidents where they have successfully exfiltrated sensitive data and demanded ransom payments.

Cl0p:

The Cl0p Ransomware Group poses a significant threat as they employ the notorious Clop ransomware and employ a range of double-extortion tactics. Notably, they operate a blog named CLOP Leaks[12], where they employ the strategy of threatening to leak stolen data to pressure their victims into paying the demanded ransom. Their targets span across several industries, including law, banking, insurance, manufacturing, software, and IT services. In a concerning incident at the end of May 2023, the Cl0p group exploited vulnerabilities found in the MOVEit Transfer web applications, including the CVE-2023-34362 vulnerability[13]. This allowed the group to infiltrate the compromised systems using a stealer. Moreover, Cl0p is actively publishing data stolen from their victims on their extortion website, with new victims being added to their list on a regular basis.

Undoubtedly, this list is not exhaustive, and researchers have observed a rising trend in encryption-less attacks. With ransomware already being a considerable threat to businesses and encryption-less attacks further lowering the barrier of entry we expect these kinds of attacks becoming more common and widespread as ever.

[8] *https://www.malwarebytes.com/blog/news/2022/03/nvidia-the-ransomware-breach-with-some-plot-twists*

[9] *https://www.bleepingcomputer.com/news/security/samsung-confirms-hackers-stole-galaxy-devices-source-code/*

[10] *https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/*

[11] *https://www.bleepingcomputer.com/news/security/uber-links-breach-to-lapsus-group-blames-contractor-for-hack/*

[12] *https://www.ransomlook.io/screenshots/clop-ekbgzchl6x2ias37onion.png*

[13] *https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a*

4

Conclusions

4. Conclusions

The extortion may be the most crucial stage of a ransom attack, with threat actors continuously striving to improve their TTPs and going as far as providing a true “customer support”-like experience to their victims.

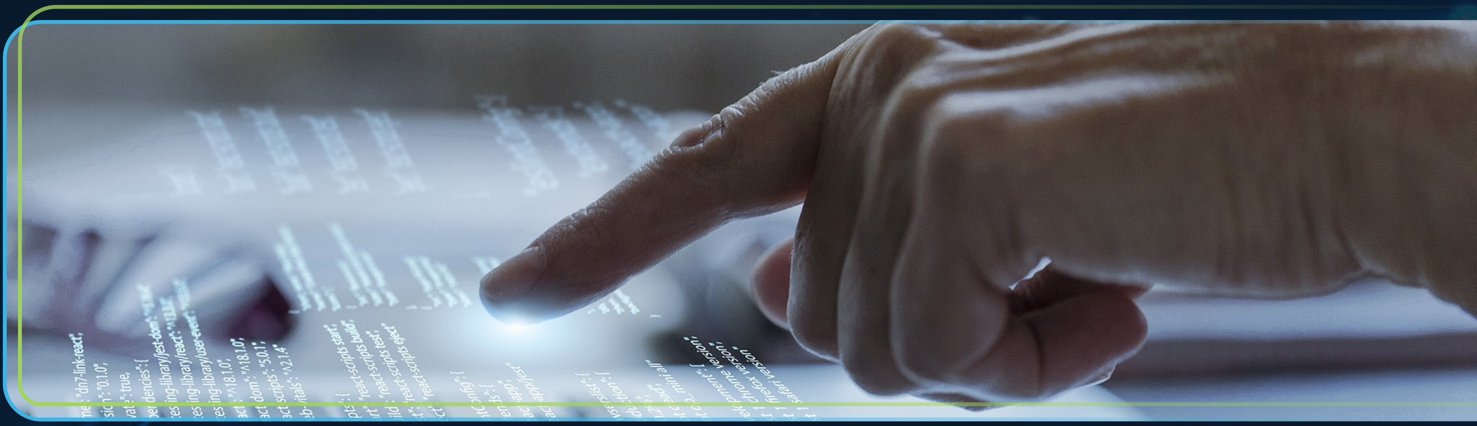
The traditional recommendation to mitigate ransomware attacks is to consistently perform data backups into an isolated environment for data recovery. There are many freely available resources about best practice regarding prevention and handling of ransomware incidents, such as CISA’s guide[14].

Considering this new trend of focusing on the information of a specific target, the organizations need to improve their approach to information management and protection.

A starting point can be the least privilege approach: give each user the minimum amount of privilege needed to achieve their task, isolate development and production environments and avoid internally freely accessible file shares. In this configuration a compromised endpoint could only exfiltrate data it would normally access rather than company-wide documents.

From this point of view, it would be also appropriate to adopt strong authentication mechanisms such as multi-factor authentication (MFA) to reduce the risk of credential reuse-based attacks.

So, in summary, having proper authentication and authorization management is a best practice to considerably reduce the risk of malicious access to crucial information.



[14] https://www.cisa.gov/stopransomware/ransomware-guide

DEFENCE TECH

Terra, Cielo, Mare, Spazio, Spazio cibernetico.
PROTEGGIAMOLI

DONEXIT
IT SECURITY

NEXT
INGEGNERIA DEI SISTEMI

FORAMIL
RADAR TECHNOLOGIES & DEFENCE SYSTEMS

INNODESI
electronic systems

Defence Tech Holding S.p.A Società Benefit
Via Giacomo Peroni, 452 - 00131 Roma
tel. 06.45752720 - fax 06.45752721
info@defencetech.it - www.defencetech.it