ITsMine™

Encryption-less Ransomware:

A New Era of Cyber Threats and How CISOs Can Defend Their Organizations

Encryption-less Ransomware:

A New Era of Cyber Threats and How CISOs Can Defend Their Organizations

When it comes to cyber attacks, prevailing wisdom had it that the #1 threat that CISOs need to be aware of is ransomware. While this is still true, it's the nature of ransomware that has changed, driven by a new generation of ransomware, and it's imperative for CISOs to understand this new threat.

The rise of encryption-less ransomware means that the traditional tools and tactics used to defend organizations are to a large extent no longer relevant.

An encryption-less ransomware attack is when the attacker does not try to encrypt the data. They will demand a ransom for not publishing the stolen information.

Double extortion is when the attacker steals the files and encrypts the files in the file storage of the company – however the files they take are not encrypted. Organizations can restore from a backup cloud to overcome the encryption element, but cannot do anything about the data that is now out there.

For example, if attackers steal a company's sensitive data and threaten to release it on the dark web, then having a backup of that data is irrelevant.

This encryption-less form of ransomware represents a shift from traditional attacks, where the primary threat was data encryption, to a scenario where sensitive information is exfiltrated and held for ransom. This shift necessitates a reevaluation of defense strategies to protect organizational data effectively.

We'll help CISOs ensure:

1. **They are prepared for these attacks**
2. **They have this in their playbook, and will test it like they do for backup and restore solutions**

First, let's start with a deeper understanding of the problem:

The Problem

1. The Rise of Encryption-less Ransomware

The MOVEit Transfer software hack, disclosed by Progress in May 2023, rapidly became the most significant cybersecurity event of last year, marking a notable instance of encryptionless ransomware. Unlike traditional ransomware attacks that encrypt victim's data to demand ransom, this incident involved the Clop ransomware and extortion gang stealing sensitive data from MOVEit Transfer servers. The attackers then threatened to publish the stolen data unless they received payment, leveraging the threat of exposure as their primary weapon of extortion.

The numbers from this attack highlight the danger modern CISOs face:

1,000 victims

More than 1,000 known victims of the MOVEit breach, making it one of the largest hacks in recent history.

83.9 %

83.9% of known corporate victims are U.S.-based, with Germany, Canada, and the United Kingdom also significantly affected.

$65 billion

Estimated total cost of the MOVEit mass-hacks so far is approximately $9.92 billion, with potential to reach at least $65 billion.

$100 million

Clop could earn up to $100 million from the MOVEit mass-hacking campaign, showcasing the lucrative nature of ransomware and data extortion.

60 million

Over 60 million individuals impacted, a number that continues to rise as more organizations confirm related data breaches.

11 million

Maximus, a U.S. government services contractor, emerged as the largest known victim, with up to 11 million individuals' sensitive information accessed.

$10 million bounty

$10 million bounty offered by the U.S. State Department for information on the Clop ransomware group.

A similar incident happened to Deloitte.

The global professional services firm experienced a significant cybersecurity incident where, unlike traditional ransomware attacks that encrypt data, this attack involved the unauthorized access and theft of sensitive data from Deloitte's email platform. The attackers then threatened to release the stolen data unless a ransom was paid, embodying the characteristics of an encryptionless ransomware attack.

This incident did not follow the more common ransomware model of encrypting victim data and demanding payment for decryption keys. Instead, it leveraged the threat of public disclosure of sensitive information as leverage for extortion.

40% Increase

Recent years have seen **a 40% increase in encryption-less attacks**, highlighting a significant change in the tactics of cybercriminals. These attackers no longer rely solely on encryption to paralyze their victims but instead threaten to release sensitive data unless a ransom is paid. This form of attack not only puts the confidential information at risk but also exposes organizations to regulatory fines, reputational damage, and the potential loss of business

75% Spike

CrowdStrike research shows that **75% of attacks were malware-free**. There has also been a 76% spike in data theft victims named on the dark web.

These statistics show how urgent and prevalent this issue is.

What's more, encryption-less ransomware poses a multifaceted problem that extends beyond the immediate threat of data exposure. The psychological impact on organizations, knowing their sensitive data could be exposed at any moment, cannot be overstated. This form of cyber extortion creates a perpetual state of insecurity and fear, making it a potent weapon in the arsenal of cybercriminals.

The consequences of falling victim to encryption-less ransomware are severe:

Reputational damage:

The public exposure of sensitive data can severely tarnish an organization's reputation, eroding trust with customers, partners, and the market at large. Rebuilding this trust can take years and may require significant investment.

Regulatory penalties:

Many industries are subject to strict data protection regulations. The unauthorized release of sensitive information could result in substantial fines and penalties, further compounding the financial impact of an attack.

Operational disruption:

The theft of proprietary information or sensitive operational data can disrupt business operations, leading to loss of revenue and potentially giving competitors an undue advantage.

Strategic vulnerabilities:

The exposure of strategic plans, financial information, or intellectual property can have long-term impacts on an organization's competitive position and market value.

Moreover, the rise of encryption-less ransomware represents a sophisticated evolution in cybercriminal strategies, exploiting the interconnected nature of modern business operations. Cybercriminals are increasingly aware that data is not just a digital asset but a cornerstone of trust, operational integrity, and competitive advantage. The threat of releasing stolen data into the public domain or selling it to the highest bidder on dark web marketplaces introduces a complex risk landscape that traditional cybersecurity measures are ill-equipped to address.

This era of encryption-less ransomware calls for a paradigm shift in how organizations approach cybersecurity. It underscores the inadequacy of relying solely on perimeter defenses or traditional data protection strategies, which may be effective against ransomware that encrypts data but are ineffective against threats that exfiltrate data.

2. Why Traditional Defenses Are No Longer Sufficient

The shift towards encryption-less ransomware has rendered traditional security measures, such as backups and endpoint detection and response (EDR) systems, less effective. These solutions are designed to counteract the effects of encryption, but they offer little protection against the theft and extortion of sensitive data.

For example:

Data exfiltration before detection:

Encryption-less ransomware operates by stealthily exfiltrating sensitive data before any demands are made. By the time the breach is detected, the data may already be in the hands of cybercriminals, making preemptive defenses like firewalls and antivirus insufficient as standalone solutions.

Ineffectiveness of backups:

Backups are essential for recovering encrypted data without paying a ransom. However, in the case of encryption-less ransomware, the threat isn't the inability to access data but rather the unauthorized release of stolen data. Backups do not mitigate the risk of data exposure and the ensuing reputational damage, regulatory penalties, and potential operational disruptions.

Endpoint detection and response (EDR) limitations:

EDR systems are designed to detect and respond to malicious activities on endpoints. While they play a crucial role in identifying and mitigating ransomware attacks, their effectiveness is diminished in scenarios where data is silently exfiltrated. Without clear indicators of ransomware encryption activity, these systems may not trigger alerts or responses in time to prevent data theft.

Insider threat oversight:

Traditional security measures often focus on external threats, neglecting the potential for insider threats. encryption-less ransomware can exploit this vulnerability, either through direct insider collusion or by manipulating insider credentials, bypassing many conventional security measures that fail to monitor for unusual internal activities.

Lack of protection and control when data resides with third parties:

For example, Blackbaud, one of the world's largest providers of fundraising, financial management, and educational software, experienced a cyber attack where cybercriminals managed to access and exfiltrate data from Blackbaud's systems. The stolen data included sensitive information related to the donors, alumni, and other stakeholders of the institutions that rely on Blackbaud's services. This positioned the attackers to potentially extort not only Blackbaud but also its clients and partners by threatening to release the stolen data unless a ransom was paid. Once companies share data, this data leaves their control.

What Should The Solution Be?

To effectively counter the nuanced and evolving threat of encryption-less ransomware, organizations must adopt a cybersecurity attitude that is comprehensive yet flexible, capable of addressing not only the current threat landscape but also adaptable to future threats.

This should include the following capabilities:

Proactive data surveillance & anomaly detection:

Leveraging machine learning and AI, the system should automatically detect and alert on anomalous behavior that deviates from established patterns, indicating potential unauthorized data access or exfiltration attempts. This should include non-authorized persons accessing sensitive data.

Make exfiltrated data unusable:

Should sensitive data be exfiltrated, there should exist the ability to instantly render data unreadable, thus neutralizing the threat posed by data theft.

Full forensic capabilities:

In the event of an encryption-less attack, security teams should be able to instantly know what data was affected.

Ability to safeguard data:

Organizations should have the ability to specifically safeguard sensitive data, a virtual "Fort Knox."

Solution to collaborative environment:

With employees sharing sensitive data with third parties, a winning solution should enable organizations to retain control of their data even when it is with that third party – meaning if the third party has a breach, the original organization's data is still safe.

Education and empowerment of the workforce:

An ideal solution should promote a culture of security awareness through regular, ongoing training, including best practices when it comes to accessing, storing, and sharing data.

What ITsMine Can Do For You

In response to this evolving threat, ITsMine has developed a comprehensive solution designed to empower CISOs and their teams to defend against encryption-less ransomware attacks.

This ITsMine encryption-less protection solution gives CISOs:

Alerts when the data was used outside the organization

The **list of the files** that the attacker took (to limit the potential exposure)

The ability to **kill the most important data**, even if the attacker holds it on an external, offline system

The ability to **present evidence to regulators** that important data was not used and cannot be used after it has been killed

This ITsMine encryption-less protection solution gives CISOs:

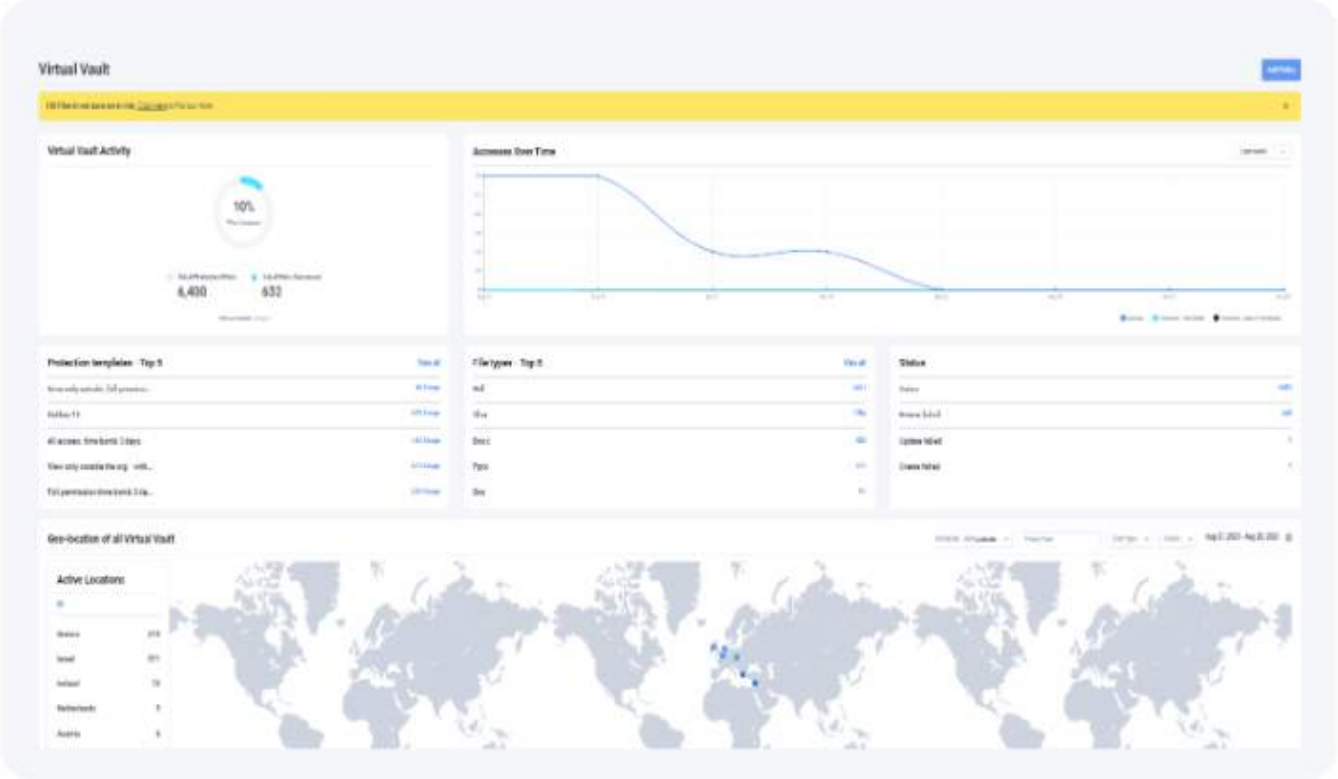
ITsMine SoftwareMines™:

An ideal solution should promote a culture of security awareness through regular, ongoing training, including best practices when it comes to accessing, storing, and sharing data.

ITsMine Virtual Vault™ & File-GPS™:

provides the ability to kill files even if the attacker holds them in an external isolated environment.

ITsMine's Virtual Vaults in action



In summary, ITsMine offers a comprehensive data protection and response solution that includes:

Alerts

for unauthorized external use of data.

Inventory tracking

of compromised files to minimize exposure.

Sanitization capabilities

to neutralize critical data even on external, offline systems

Assurance tools

to prove to regulators that vital data has not been misused and is beyond reach post-incident

A Call to Action for CISOs

As encryption-less ransomware becomes an increasingly common threat, CISOs must adapt their cybersecurity strategies to protect their organizations. This involves not only deploying the right technologies, such as ITsMine's comprehensive solution, but also raising awareness about the changing nature of ransomware attacks.

Specifically, it should now be clear that CISOs must ensure they are prepared for these encryption-less attacks, and that their playbook includes a robust response including testing and simulations much like is done for other common threats.
By understanding the nuances of encryption-less ransomware and implementing robust defense mechanisms, CISOs can safeguard their organizations against this evolving threat.

ITsMine offers a solution that empowers CISOs to be alerted, stay in control, and defend against these sophisticated attacks, ensuring that sensitive information remains secure.