Ransomware Report

By Ellen Hallam
Senior Threat Intelligence Analyst

Created: 1st November 2023

The challenge of Ransomware:

Ransomware attacks have become a pervasive and evolving threat to organisations worldwide. Whilst the concept of ransomware is relatively straightforward, the technical mechanisms and challenges behind them are complex and multifaceted. Ransomware has evolved so rapidly over the past few years, that it now has the power to paralyse organisations and extract large ransoms. Ransomware attacks are sophisticated, well-organised operations carried out by cybercriminal groups. Although figures vary, on average, research collated by US Norton suggests that ransomware attacks have risen by 85% since 2020, with an estimated 4,000 attacks every day. The average ransom payout has risen by nearly 80%, with it costing a business £1.5million, on average, to recover[1].

Ransomware is about leverage. Cybercriminals infiltrate systems, encrypt data, and then demand a ransom for its release. However, the modern ransomware landscape has evolved, taking on more sinister forms, including, "double", "triple" and "quadruple extortion". In Double extortion, attackers not only encrypt data but also exfiltrate it, threatening to expose sensitive information unless their demands are met. Triple extortion adds a further step by contacting "collateral" victims and encouraging them to contact the victimised organisation, to urge them to pay the ransom to "protect their personal data". Quadruple extortion, first seen in 2021, against Racetrac Petroleum[2], goes even further by coordinating other attacks, such as Distributed Denial of Service (DDOS) attacks on the victim's network. This tactic is growing in popularity as attackers seek new ways to ensure and speed up ransom payments. Furthermore, a recent US-led coalition of nations has agreed to end ransomware payments to hackers, which will also start to change the ransomware landscape[3].

To effectively defend against such threats, we must embrace a proactive approach that utilises intelligence derived from Open Source (OSINT, information readily available and accessible on the internet), as well as Closed Source (CSINT) intelligence, such as especially criminal forums, to give us the best understanding of the capabilities and intentions of cyber criminals. Whilst the threat landscape continues to evolve, one indispensable defensive weapon stands out: Cyber Threat Intelligence.

1. 100+ ransomware statistics for 2023 and beyond – Norton
2. Ransom Gangs Emailing Victim Customers for Leverage – Krebs on Security
3. US-led coalition of nations agrees to end ransomware payments to hackers – ITPro

The evolution of Ransomware:

The timeline (below), shows how Ransomware first began in 1989 and how it has changed rapidly over the last 5 years, feeding the billion-dollar global cybercrime industry. With this evolution, any business is a target from any cybercriminal threat.

1989

AIDS

- Spread by floppy disk
- Symmetric encryption

2004

GPCODE

- Spread via phishing emails
- Used asymmetric encryption

2009

LOCKER

- Spread via phishing emails
- Used asymmetric encryption

2010

WINLOCKER

- Spread via phishing emails
- Used asymmetric encryption

2012

FAKE DEFENDER

- Spread via phishing emails
- Used asymmetric encryption

2013

CRYPTO-LOCKER

- Spread via phishing emails
- Used asymmetric encryption

2015

LINUS ENCONDER

- Spread via backdoor in magento CMS
- Used symmetric encryption

2017

WANNACRY

- Spread via a flaw in SMB server
- Used asymmetric encryption

2019

MAZE

- Spread via phishing emails and exploit kits
- Used asymmetric encryption

2021

RANSOMWARE AS A SERVICE

- Spread via phishing emails and exploit kits
- Used asymmetric encryption

2022

REVIL

- Spread via phishing emails and exploit kits
- Used asymmetric encryption

2023

MOVEIT

- Spread using a zero-day vunerability
- Used data-filtration extortion attack

Understanding the Anatomy of a Ransomware attack:

1 Initial Infection:

- The ransomware payload is delivered through various vectors, including malicious email attachments, drive-by downloads from compromised websites, exploit kits, and supply chain attacks.
- Attackers often use social engineering tactics, like phishing emails, to trick users into opening infected files or clicking on malicious links.

2 Execution and Encryption:

- Once executed on the victim's system, the payload seeks vulnerabilities to exploit, including unpatched software, weak passwords, or unsecured network shares, as well as privilege escalation for file encryption or sensitive data access.
- Ransomware uses encryption algorithms to lock victim files, making them inaccessible. Symmetric and asymmetric encryption techniques are often used to encrypt data efficiently while securing the encryption keys.

3 Extortion and Communication:

- After encryption, the ransomware displays a ransom note or message informing the victim of the attack and providing instructions for paying the ransom, including the amount and obtaining decryption keys.
- Ransomware communicates with a remote C2 server controlled by the attackers, which is used to verify the victim's identity, facilitate ransom payment, and, in some cases, deliver decryption keys.

4 Data Exfiltration:

- Attackers can exfiltrate sensitive data before encrypting it, in a double extortion attack. They threaten to release this data unless the ransom is paid, increasing the pressure on victims.

5 Ransom Payment:

- Attackers typically demand payment in cryptocurrency to maintain their anonymity. Victims are often directed to specific cryptocurrency wallets to make payment. Cryptocurrency transactions are difficult to trace, making it challenging for law enforcement to identify and apprehend attackers.

6 Decryption:

- After receipt of the ransom, attackers may provide decryption keys to the victim, though there is no guarantee of this, as this is reliant on the integrity of the ransomware group.

7 Cleanup and Remediation:

- Victims must thoroughly clean and restore their compromised systems to remove the ransomware and associated malware, using Incident Response, Cyber Threat Intelligence and Digital Forensics.
- Effective defence strategies require proactive measures; robust cybersecurity practices, advanced threat detection solutions, threat intelligence, user education and security improvements, such as patching, to reduce the risk of falling victim to these malicious operations.

Threat actors are a serious threat to any organisation, which means companies need to be considering their security posture, tooling, and threat intelligence capabilities, to ensure they can mitigate attacks before they happen. In our Bytes security survey, The State of Cyber Security & Risk in 2023, 40% of those we asked, see 'increased threats' as the biggest challenge of 2023, Ransomware is considered the biggest risk to businesses but only 36% of businesses are using multiple threat sources ingested into an SIEM/SOC, which means 64% of businesses are missing intelligence from their intelligence feeds and not building up a comprehensive threat intelligence picture to protect their assets.

The Power of Cyber Threat Intelligence:

The Power of CTI:

Cyber Threat Intelligence (CTI) is the linchpin of any robust cybersecurity strategy, especially in the face of evolving ransomware threats. It helps provide.

Early Warning:

CTI provides early warning indicators by monitoring the dark web, hacker forums, and other clandestine corners of the internet. It helps organisations stay one step ahead by identifying potential threats before they strike.

Targeted Defence:

Armed with intelligence on the tactics, techniques, and procedures (TTPs) employed by ransomware groups, defenders can develop targeted security measures, helping organisations pre-empt what threats they may face and in what form.

Vulnerability Mitigation:

Threat intelligence can identify vulnerabilities that ransomware actors might exploit. By patching or securing these weaknesses, organisations can reduce their attack surface.

Indicators of Compromise (IoCs):

CTI provides IoCs, such as IP addresses, file hashes, and malware signatures, that can be used to detect and block ransomware attacks in real-time.

Contextual Insights:

Beyond technical indicators, CTI also offers context. It helps organisations understand the motivations, affiliations, and goals of ransomware groups, enabling more informed decision-making at every level.

Incident Response:

When an attack occurs, CTI aids in swift and effective incident response. It guides organisations in containment, eradication, and recovery efforts, minimising the damage inflicted.

The Imperative of Investment:

In an era where cyberattacks are not a matter of "if" but "when," investing in CTI is not a luxury but a necessity. Organisations should allocate resources for threat intelligence platforms, dedicated analysts, and the training of cybersecurity teams. The cost of prevention is always better than the toll ransomware attacks can exact.

Future trend:

The initial attack vector is *likely* to be moving away from the exploitation of public facing mis-figured or vulnerable services, focusing instead on a supply-chain attack model, with the attacker *almost certainly* targeting multiple organisations in one hit. Events like the MOVEit data breach, which compromised the personal data of 64million people, across 2500 different organisations, are *almost certain* to continue[4]. Furthermore, it is *likely* there will be a rise in quadruple extortion and more 'extreme' tactics and techniques, as ending ransomware payments to hackers is *highly likely* to encourage hackers to resort to more extreme and more damaging methods to extort payment from organisations. Although Ransomware will continue to be an existential threat in our digital world, Cybercriminals are not invincible. With the power of Cyber Threat Intelligence at our disposal, we can proactively identify, assess, and mitigate these risks. It is time to embrace intelligence-driven cybersecurity, empower our defences, and turn the tables on those who seek to hold our digital lives hostage. Together, we can chart a future where ransomware is but a fading shadow in the world of cybersecurity.

4. MOVEit data breach exposed personal data of 64M people – 9to5mac.com

Annex A:

The Probability Yardstick

To quantify language, we use the Probability Yardstick, from the Professional Head of Intelligence Assessment. It is a tool used in the UK Government to standardise the way we describe probability and has been used to ensure consistency across the different thematic areas and threats when providing assessments on how likely something is to occur. The Yardstick is displayed across for your information.

Professional Head of Intelligence Assessment

Probability range	Judgement range	Fraction range
>0 - ≤ ≈5%	Remote chance	>0 - ≤ ≈1/20
≈10% - ≈20%	Highly unlikely	≈1/10 - ≈1/5
≈25% - ≈35%	Unlikely	≈1/4 - ≈1/3
≈40% - <50%	Realistic possibility	≈2/5 - <1/2
≈55% - ≈75%	Likely or probably	≈5/9 - ≈3/4
≈80% - ≈90%	Highly likely	≈4/5 - ≈9/10
≥ ≈95% - <100%	Almost certain	≥ ≈19/20 - <1

≈ approximately ≥ is more than or equal to ≤ is less than or equal to > is more than < is less than

Source Evaluation

We also assess our sources using this matrix, but rarely disclose our source, to protect its integrity. We assess sources on how reliable they are and how they access the intelligence. The table here illustrates this:

Source Evaluation	Intelligence Evaluation
1. Reliable	**A.** Known directly to the source
	B. Known indirectly to the source but corroborated
2. Untested	**C.** Known indirectly to the source
	D. Not known
3. Not reliable	**E.** Suspected to be false

Confidence Levels

High Confidence → High confidence indicates judgements based on high-quality information, and/or the nature of the issue makes it possible to render a solid judgment. A "high confidence" judgment is not a fact or a certainty however, and still carries a risk of being wrong.

Moderate Confidence → Moderate confidence means credibly sourced and plausible information, but not of sufficient quality or corroboration to warrant a higher level of confidence.

Low Confidence → Low confidence means questionable or implausible information was used, the information is too fragmented or poorly corroborated to make solid analytic inferences, or significant concerns or problems with sources existed.