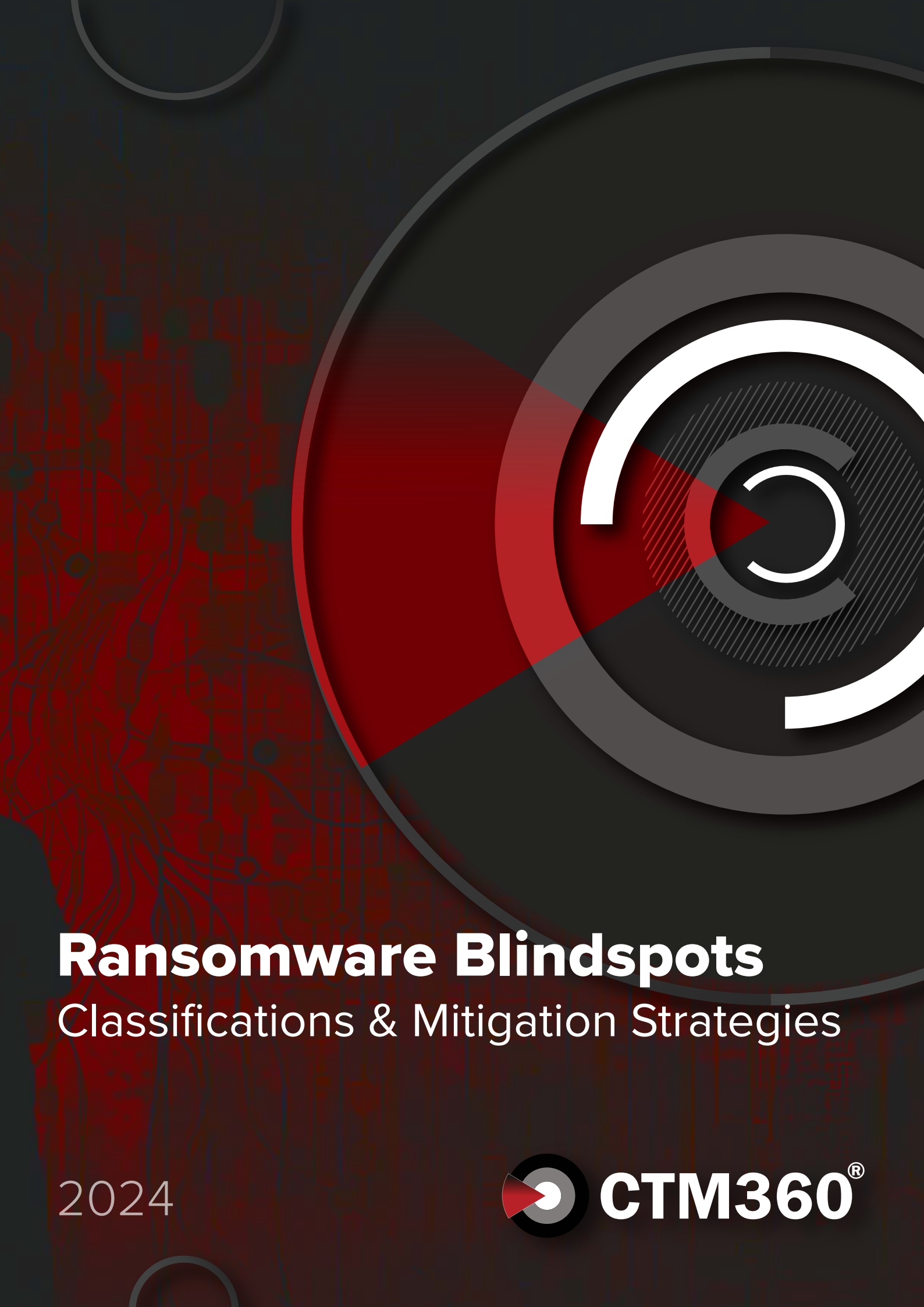


Ransomware Blindspots

Classifications & Mitigation Strategies

2024

CTM360®

TABLE OF CONTENTS

Introduction

Ransomware remains one of the top cybersecurity threats faced by organizations worldwide. While many organizations rely on traditional security methods and policies, ransomware groups have evolved, employing new strategies.

CTM360's analysis in this report aims to shed light on the classification of ransomware, providing an understanding of ransom strategies employed by threat actors, their repeatable aspects, and actionable mitigations.

Key Highlights

Ransomware Classifications

- Single Extortion (Encryption)
- Double Extortion (Encryption + Exfiltration)
- Triple Extortion (Includes DDoS)
- Quadruple Extortion (Extorting Third-Parties)
- Encryption-Less Ransomware (Data Exfiltration)

(Page 5-9)

Other Ransom Strategies

- Fake Ransomware
- Ransom demand without any Hack
- Ransomware Targeting Individuals Rather Than Organization

(Page 9-10)

Post Ransomware Policies

- Ransomware Policy - To Pay Or Not To Pay?
- Cyber Insurance

(Page 12-13)

Top Ransomware Groups

- Lockbit
- Clop
- Alphv (Blackcat)

(Page 15)

Top Repeatable Techniques

- T1059 - Command & Scripting Interpreter
- T1566 - Phishing
- T1027 - Obfuscated Files or Information

(Page 15)

Data Exfiltration Tools

- Rclone
- Cobalt Strike
- RDP

(Page 17)

Common Binaries

- Powershell.exe
- Cmd.exe
- Reg.exe

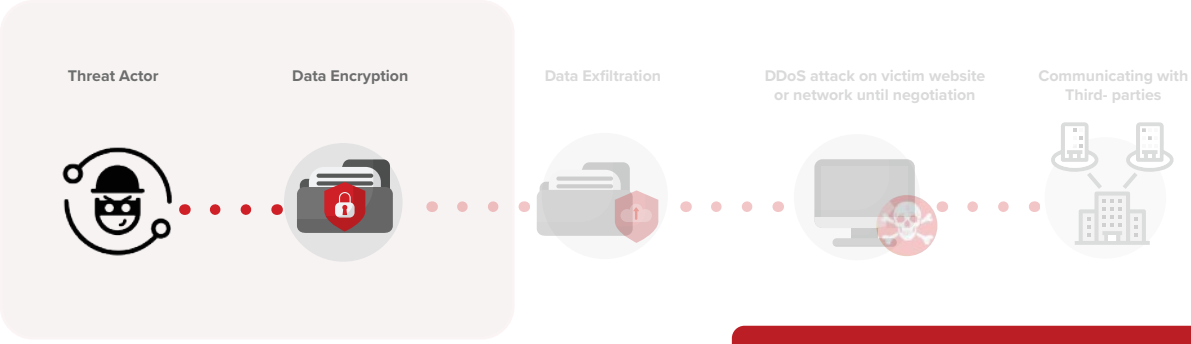
(Page 20)

Understanding Ransomware CLASSIFICATIONS

Ransomware comes in various forms, each with distinct characteristics and strategies. From Single extortion ransomware to complex schemes involving data theft and extortion, the following classifications explore the diverse landscape of ransomware attacks:

SINGLE EXTORTION
(Encryption)

Conventional ransomware typically operates by encrypting a victim's data, rendering it inaccessible, and subsequently demanding a ransom payment from the victim in exchange for the decryption key needed to decrypt the files. This method represents the traditional approach to ransomware also known as Single extortion.



Some single extortion cases:


Jonathan Greig
July 17th, 2024

Furniture giant shuts down manufacturing facilities after ransomware attack

One of the largest U.S. furniture companies, Bassett Furniture Industries, halted production due to a ransomware attack that compromised its IT systems. The incident led to data encryption and the activation of the company's incident response plan, forcing a shutdown of manufacturing facilities to contain the breach. (Source: Securityweek)


Massive ransomware infection hits computers in 99 countries

US National Health staff shared screenshots of the WannaCry ransomware, which demanded a payment of $300 in Bitcoin to unlock the encrypted files on each affected computer. This attack focused solely on data encryption, requiring the payment for decryption without threatening to leak sensitive data—a classic case of single extortion. (Source: BBC)

Interesting Fact:

ONE OF THE FIRST RANSOMWARE ATTACKS ever documented was the AIDS trojan (PC Cyborg Virus) that was released via floppy disk in 1989.

Victims needed to send $189 to a P.O. box in Panama to restore access to their systems, even though it was a simple virus that utilized symmetric cryptography. *(Source: University of Tulsa)*

DOUBLE EXTORTION

(Data Exfiltration & Encryption)

Double extortion ransomware combines data theft with file encryption, demanding payment for both the stolen data and encrypted files. This tactic increases pressure on victims to pay the ransom to prevent data exposure or misuse.

Some double extortion cases:

Cyberattack on Indonesia's national data centre paralyses government services

By Muchamad Azhar Jun 25, 2024

Hackers encrypted systems at Indonesia's National Data Center with Brain Cipher ransomware, disrupting critical services. In addition to encryption, the attackers exfiltrated sensitive data and threatened to release it online unless the ransom was paid. However, it was reported that the groups later apologized for the attack and provided the decryption key for free. (Source: GovInsider)

Ransomware, Breach, Privacy

2.7M medical records exposed in double-extortion ransomware attack

December 21, 2023 Share

ESO Solutions, a medical software company, faced a ransomware breach targeting 2.7 million U.S. patients' sensitive data. Attackers encrypted and exfiltrated data, employing double extortion tactics for financial leverage. (Source: SC Magazine)

Chipmaker Nexperia confirms breach after ransomware gang leaks data

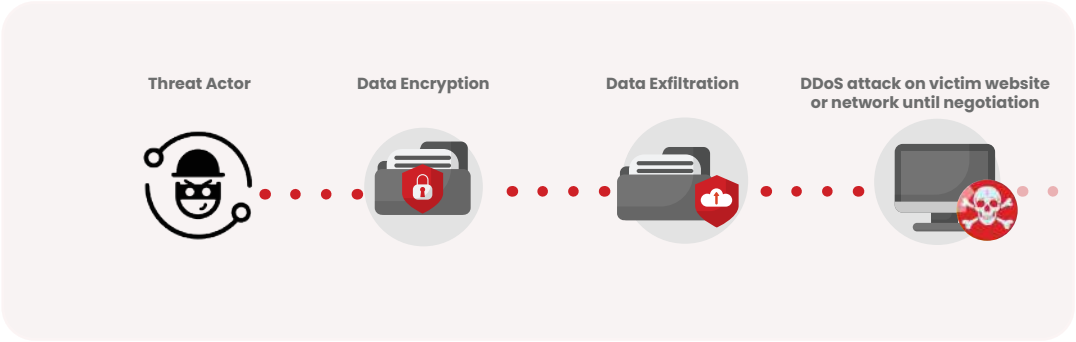
By Bill Toulas

Nexperia, a major silicon processor manufacturer, was targeted by ransomware. The attack involved encrypting and exfiltrating over 1TB of sensitive data, including chip designs, R&D files, employee details, and customer information.
(Source: Bleeping computer)

TRIPLE EXTORTION

(An additional demand)

Triple extortion ransomware goes beyond data theft and encryption by adding an extra layer of threat through DDoS attacks to persuade payment for file decryption.



Triple extortion case:

AvosLocker, a ransomware-as-a-service operator, targeted CHRISTUS Health in an attack involving data theft and disclosure on the dark web. This breach included sensitive patient information and possibly utilized DDoS attacks.
(Source: Govinfosecurity)

QUADRUPLE EXTORTION

(Extorting Third-Parties)

Quadruple extortion ransomware adds an additional layer of extortion. It not only involves encrypting data and other threats but also includes targeting third parties with ransom demands.

Quadruple extortion case:

In 2021, after the hardware supplier Quanta did not pay the ransom demanded by the REvil ransomware group, the attackers shifted their focus to Apple, a client of Quanta.
(Source: Bloomberg)

ENCRYPTION-LESS RANSOMWARE (Data Exfiltration)

Encryption-less ransomware steals data skipping the encryption process, using the threat of data exposure to extort payment from victims.

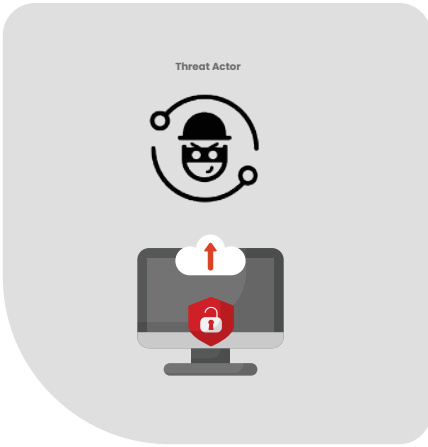
There is an observable **shift** towards encryption-less ransomware attacks.

REASONS FOR THE SHIFT

1. Ransomware groups are now exploiting global data and privacy protection regulations such as GDPR and similar data protection laws to their advantage in attacks. Ransomware groups leverage on the perceived liability that the target organization may face legal consequences from their customers, partners or third parties if data gets publically exposed.

2. Organizations have improved their backup and recovery procedures and they are less likely to pay ransom to decrypt the data.

3. Data exfiltration requires minimal effort and tools from threat actors while still causing significant harm to the targeted organization.



The most prominent ransomware group **LockBit** is continually enhancing its data exfiltration capabilities and also offering Ransomware as a Service (RaaS),

"MAKE RANSOMWARE GREAT AGAIN." *Latest slogan by LockBit*

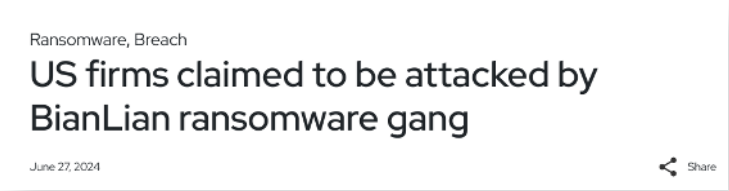
Some encryption-less cases:


RANSOMWARE

Ransomware Attack Cost Keytronic Over $17 Million

Keytronic says the recent ransomware attack resulted in expenses and lost revenue totaling more than $17 million.

Keytronic disclosed a significant impact, with operations disrupted in the US and Mexico due to a ransomware attack by the Black Basta group. The breach, resulting in a two-week suspension, led to the theft of over 500 GB of sensitive data, including financial documents, engineering files, and HR information. (Source: Securityweek)


Ransomware, Breach

US firms claimed to be attacked by BianLian ransomware gang

June 27, 2024 Share

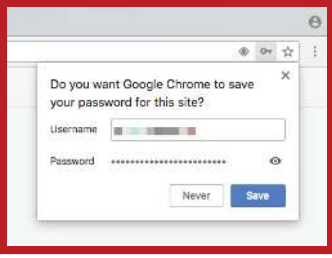
BianLian allegedly exfiltrated 1.2 TB of sensitive data from Better Business Bureau systems, transitioning to exfiltration-based extortion. U.S. Dermatology Partners had 300 GB of data exfiltrated, including personal and financial details, in line with BianLian's new attack approach. (Source: SC Magazine)

Rise in Data Exfiltration using Malware Logs

Malware logs facilitate data exfiltration, allowing threat actors easy access to sensitive information. These logs contain login details of their potential target users, which in the hands of a threat actor makes it easy for them to exfiltrate data from the organization.

What are Malware logs?

Malware logs are data stolen using info-stealing malware designed to capture sensitive information which is saved in the browser such as passwords, cookies, credentials, financial data, or personal details from an infected machine, which is then sent back to the attacker's server for exploitation.



Other RANSOM STRATEGIES

1. FAKE RANSOMWARE

Fake ransomware is a fear-mongering technique that does not encrypt data. Instead of encrypting files, fake ransomware sends email alerts and demands for money, making victims think their data is at risk. These attacks use fear to get money from people and organizations, tricking them without using any ransomware.

Fake ransomware case:

Fake Ransomware Infection Hits WordPress Sites

WordPress sites are hit by fake ransomware warnings with a deceptive countdown clock, demanding Bitcoin payments; investigations reveal these alerts to be a mere hoax generated by a fake plugin. (Source: Threatpost)

2. RANSOM DEMAND WITHOUT ANY HACK

Threat actors may seek ransom payments through methods that do not involve ransomware. Few of them are listed below:

SIMPLE DATA LEAK
Threat actors may steal data from exposed buckets, directories, or unprotected storage systems and demand a ransom. Instead of using ransomware to lock files, they threaten to release the stolen data publicly if their demands aren't met. In some cases, threat actors may also reuse information that has already been leaked or is publicly available through websites or public forums.

SHORT SELLING STOCK ANNOUNCEMENT
This tactic involves threatening to publicly disclose a victim organization's name, which could lead to a drop in its stock price. Traders with insider knowledge are then positioned to profit by short-selling the stock before the information is released.

R-DDOS (RANSOM DDOS)
Ransom DDoS (RDDoS) is a cyberattack where attackers threaten to launch a DDoS attack unless a ransom is paid. They might first conduct a small-scale attack as a warning and demand payment to prevent a larger one, aiming to extort money by exploiting fear of downtime and revenue loss.

SEXTORTION
In sextortion, victims are pressured/Blackmailed to pay in order to prevent the sharing of fake but convincing content, exploiting fear even without actual data possession, and demanding a ransom. AI-generated content enhances these schemes by creating realistic yet fabricated videos to manipulate and intimidate victims.

3. RANSOMWARE TARGETING INDIVIDUALS RATHER THAN ORGANIZATIONS

Ransomware specifically aimed at individuals rather than organizations focuses on extorting money by encrypting personal data, often demanding payment for decryption. In some cases, threat actors have also been observed targeting organization executives or top management.

Ransomware targeting individuals case:


This unusual ransomware attack targets home PCs, so beware

A ransomware campaign is using sneaky techniques to infect individual users with ransomware - and demands thousands for the decryption key.

A ransomware campaign, Magniber was targeting individual users in 2022, using deceptive methods to trick victims into downloading malicious updates that encrypt files and demand ransom payments. This approach, focused on extracting smaller payments from home users, utilizes innovative techniques like distributing the ransomware via JavaScript files to evade detection, posing significant risks to unsuspecting individuals. (Source: Zdnet)

Navigating Post-Ransomware
POLICIES & STRATEGIES

In the wake of a ransomware attack, the organization's response is crucial to mitigating damage and ensuring a swift recovery. This section discusses key considerations that should guide the development and implementation of post-ransomware policies and strategies.

RANSOMWARE POLICY

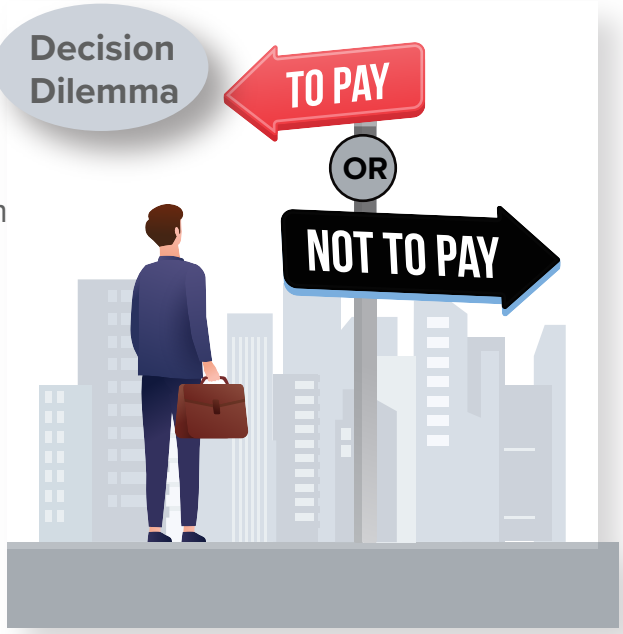
Organizations must decide whether to pay the ransom during a ransomware attack. While the general policy is against it due to supporting criminal activities and no data recovery guarantee, each case requires a careful evaluation of ethical concerns, business impact, and stakeholder interests.

Organizations should also determine if payment of the ransom is permitted under applicable laws, or else the company could find themselves facing another major incident if they unwittingly violate international sanctions by making a ransom payment. *(Source: Cybereason)*

According to veeam survey

47%
of organizations leaned towards paying the ransom to recover their data.

25% of the organizations could not recover data even after paying.



36%
of organizations had a policy against paying the ransom.

In 2023, only **17%** of organizations did not have a policy on whether to pay a ransom or not.

81% of organizations ended up paying the ransom, regardless of whether they had a policy or not.

(Source: Veeam)

IT IS HIGHLY ADVISABLE TO NOT PAY THE RANSOM OR ENGAGE WITH THREAT ACTORS, AS THERE IS NO GUARANTEE THAT YOUR DATA WILL BE FULLY RECOVERED OR DELETED.

Cyber INSURANCE

Cyber insurance can play a vital role in an organization's risk management plan. These policies typically cover expenses related to business disruptions, data recovery and in some cases **ransom payments**. However, the effectiveness of these policies varies, so it's important for organizations to fully understand what their insurance covers and the financial implications.

65% of Organizations Paid Their Ransom with Insurance.

21% chose **not to use** the insurance paying the ransom without making a claim.

73% of organizations experienced an increase in their insurance premium.

44% had their deductible increased.

14% saw their coverage benefits reduced.

(Source: Veeam)

These figures highlight the need for careful consideration when selecting and relying on cyber insurance.

Other Important ASPECTS OF POST-RANSOMWARE

Managing Internal Communication in case of a Third-Party Ransomware Attack

When a third-party vendor or partner is affected by a ransomware attack, prompt and clear internal communication is crucial to reduce risks.

The key actions include:

- **Check Affected Services/Systems:** Identify which services or systems are impacted by the third-party breach and how they are linked to your operations.
- **Review Data Exposure:** Assess what type of data has been leaked, focusing on whether it includes sensitive information such as customer or financial data.
- **Communicate with the Third-Party:** Maintain close communication with the third-party vendor to receive timely updates and relay critical information to your internal teams such as IT/infosec and senior management.
- **Contain the Breach:** Collaborate with the third party to contain the breach and prevent further damage by isolating compromised systems or suspending affected services.

Contractual Disclosures with Third Parties

Contracts with third-party vendors should include clauses requiring immediate notification in case of a ransomware/cyber attack. This ensures transparency and allows your organization to respond quickly and minimize risks.

Organization's Communication Plan

A strong communication plan is essential for handling ransomware incidents. This should include communicating with both internal & external parties.

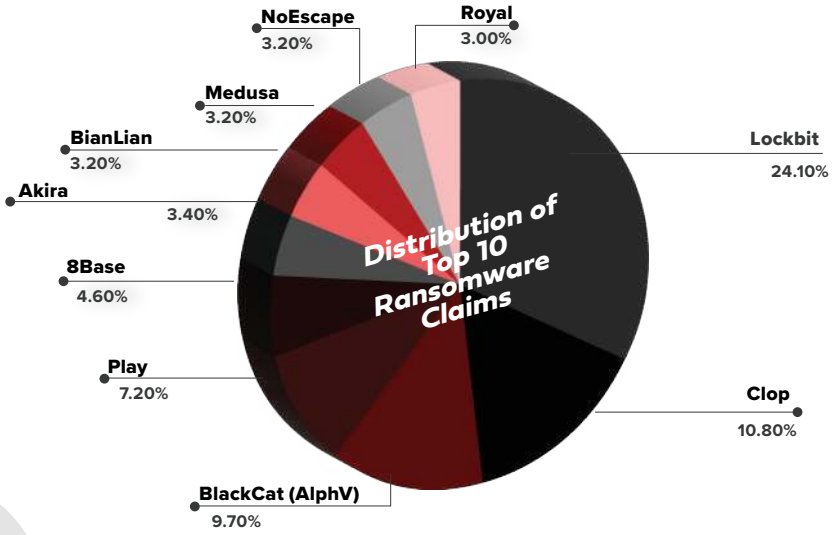
- **Management & Staff:** Immediately notify leadership and staff with clear instructions to secure systems and prevent further harm.
- **Customers:** Be transparent with customers if their data is compromised, explaining the actions being taken to resolve the issue and protect their information.
- **Authorities:** Report the incident to relevant regulatory bodies or authorities promptly to ensure compliance and receive necessary support.

CTM360®

Leading Ransomware Groups & THEIR ARSENAL

Based on the analysis of threat actor claims in **CTM360 2023-24 Threatscape Report**, the top 10 ransomware groups that had the highest number of victims were identified.
(Source: CTM360)

Ransomware groups often reuse successful attack techniques but frequently alter their IP addresses, domains and hosts to evade detection. While security teams typically concentrate on updating Indicators of Compromise (IOCs), they should put more emphasis on addressing the repeatable techniques used by threat actors.



"In my opinion, the frequent changes in IoCs are up to 10 times a day, while the Tactics, Techniques, and Procedures (TTPs) have not changed over the past 10 years."

Mirza Asrar Baig
CEO & Founder | CTM360

Among the various techniques employed by ransomware groups, **5 of the most used techniques are listed below.** These techniques were found to be common across the Ransomware malware type.

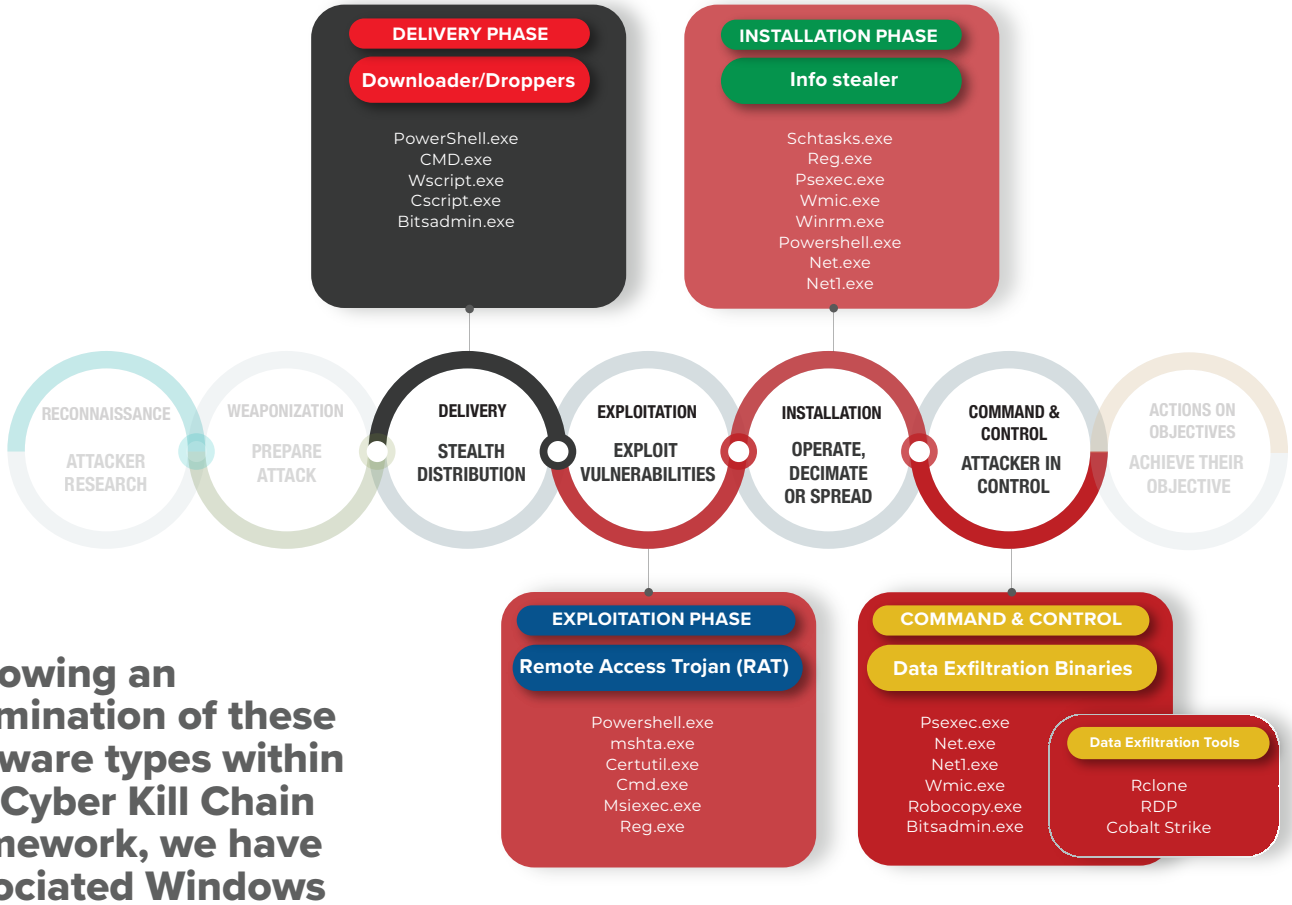
- T1059 - Command and Scripting Interpreter
- T1566 - Phishing
- T1027 - Obfuscated Files or Information
- T1036 - Masquerading
- T1140 - Deobfuscate/Decode Files or Information

As mentioned in the CTM360 2023-24 Threatscape Report, diving deeper into the strategies employed by ransomware groups, an analysis of the recurring playbook used by these groups revealed that many of them employ similar techniques. Hardening against one technique used by a ransomware group not only defends against that specific ransomware but also hardens the environment against other ransomware that may utilize the same technique.

T1059 - Command & Scripting interpreter technique stands out as the most commonly used technique by ransomware groups and may function as a **Kill Switch** for multiple ransomware groups. This technique has the capacity to disrupt malware operations and can be effectively mitigated by implementing appropriate controls. Organizations are advised to gain an understanding of this technique and proactively take measures to reduce its impact on their systems and networks.

Mapping of Windows Binaries WITH KILL-CHAIN

In **CTM360 2023-24 Threatscape Report**, we identified four prominent malware types (Dropper/Downloader, Remote Access Trojan (RAT), Info-Stealer, and Tools/Data Exfiltration), each distinguished by their role in the attack process. Utilizing the Cyber Kill Chain framework by Lockheed Martin, which breaks down a cyber attack into seven stages, ranging from initial reconnaissance to the final stage of Action on Objectives, we were able to map four distinct stages (Delivery, Exploitation, Installation, Command & Control) of the Cyber Kill Chain framework specific to these four malware types.



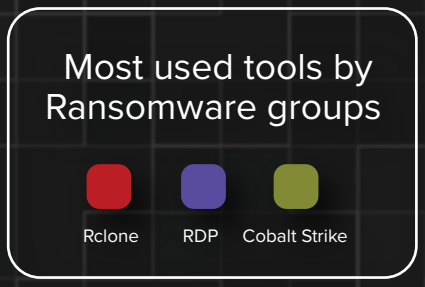
Following an examination of these malware types within the Cyber Kill Chain framework, we have associated Windows binaries linked to each malware type with various stages of the kill chain. This mapping highlights some binaries that are executed in these phases and could be hardened against.

Most frequently seen

Data Exfiltration Tools

Various ransomware groups utilize a range of sophisticated data exfiltration tools to carry out their malicious activities. Below are some of the tools mapped with the ransomware groups utilizing them.

Akira	Rclone, WinRAR
Lockbit	AnyDesk, RDP, Cobalt Strike, ScreenConnect, Rclone, Atera, Pandora RC, TightVNC
Play	Rclone, WinSCP
Royal Ransomware	Rclone, CobaltStrike, ScreenConnect, Atera, Chisel
Blackcat	Exmatter, Rclone, Cobalt Strike, RDP
Medusa	AnyDesk, Teamviewer
8Base	Rclone
No Escape	RDP, MegaSYNC
Bianlian	Rclone, RDP
Clop	Cobalt Strike



It is strongly recommended not to use these tools in any environment to prevent potential data breaches and protect organizational security.

CTM360®

Mitigation CHEATSHEET

After a thorough analysis of common malware types across the different Kill-Chain phases, CTM360 has mapped common Windows binaries used by Malware/Ransomware along with their respective mitigation strategies.

The below mitigation cheat sheet may help organizations to better understand and protect their infrastructure against binaries exploited in the attacks

Kill Chain Phase

DELIVERY

BINARIES	MITIGATION
Powershell.exe	PowerShell can be disabled by creating a new path rule and blocking the paths that lead to its execution in the software restriction policy.
Wscript.exe lCscript.exe	To prevent malicious scripts from running, set "Disable Windows Script Host" to "Enable" under Windows Script Host.
Bitsadmin.exe	Prevent the execution of bitsadmin.exe by disabling the BITS service through Group Policy.
Cmd.exe	Block the use of the command prompt by enabling the "Prevent access to the command prompt" policy under System policies in GPO (Group Policy Object). Consider also disabling the command prompt script processing policy.

Kill Chain Phase

EXPLOITATION

BINARIES	MITIGATION
Powershell.exe	PowerShell can be disabled by creating a new path rule and blocking the paths that lead to its execution in the software restriction policy.
mshta.exe	Mshta.exe can be disabled by blocking the paths that lead to its execution in the software restriction policy.
Reg.exe	Enable and enforce "Prevent access to registry editing tools" under System policies to restrict access to registry editing tools.
Certutil.exe	Prevent access to Certutil.exe by creating a GPO (Group Policy Object) to restrict its execution path through the software restriction policy.
Cmd.exe	Block the use of the command prompt by enabling the "Prevent access to the command prompt" policy under System policies in GPO (Group Policy Object). Consider also disabling the command prompt script processing policy.
Msiexec.exe	Prevent certutil.exe from executing scripts by enabling the "Prevent msiexec.exe from installing software for non-administrators" Group Policy setting

Kill Chain Phase

INSTALLATION

BINARIES	MITIGATION
Lsass.exe	To block credential stealing, enable the appropriate ASR rules under Attack surface reduction in Microsoft Defender Exploit Guard.
Reg.exe	Enable and enforce "Prevent access to registry editing tools" under System policies to restrict access to registry editing tools.
Schtasks.exe	To prevent unauthorized scheduling of tasks, use "Disable New Task Creation" or "Disable Task Deletion" under Task Scheduler.
Takeown.exe	Restrict the execution of Takeown.exe by creating a GPO (Group Policy Object) and use the software restriction policy to block the paths that lead to its execution.
icacls.exe	icacls.exe can be restricted or blocked through the software restriction policy by creating a new path rule and blocking the paths that lead to its execution.
Psexec.exe	Restrict the execution of Psexec.exe by creating a GPO (Group Policy Object) and use the software restriction policy to block the paths that lead to its execution.
Wmic.exe	Restrict the execution of Wmic.exe by creating a GPO (Group Policy Object) and use the software restriction policy to block the paths that lead to its execution.
Winrm.exe	Restrict the execution of Winrm.exe by creating a GPO (Group Policy Object) and use the software restriction policy to block the paths that lead to its execution.
powershell.exe	PowerShell can be disabled by creating a new path rule and blocking the paths that lead to its execution in the software restriction policy.
Net.exe | Net1.exe	Restrict the execution of Net.exe and Net1.exe by creating a GPO (Group Policy Object) and use the software restriction policy to block the paths that lead to their execution.
Sc.exe	Restrict the execution of Sc.exe by creating a GPO (Group Policy Object) and use the software restriction policy to block the paths that lead to its execution.

Kill Chain Phase

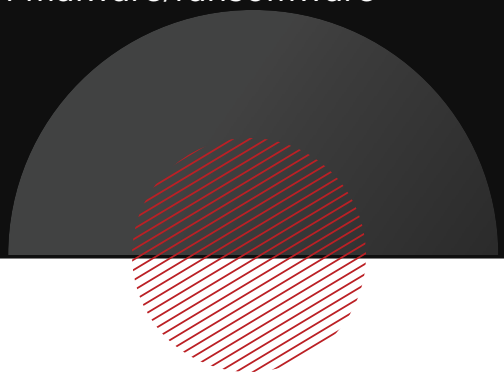
COMMAND & CONTROL

BINARIES	MITIGATION
Bitsadmin.exe	Prevent the execution of bitsadmin.exe by disabling the BITS service through Group Policy.
Ftp.exe	Ftp.exe can be restricted through the software restriction policy by creating a new path rule and blocking the paths that lead to its execution.
Net.exe | Net1.exe	Restrict the execution of Net.exe and Net1.exe by creating a GPO (Group Policy Object) and use the software restriction policy to block the paths that lead to their execution.
Robocopy.exe	Restrict the execution of Robocopy.exe by creating a GPO (Group Policy Object) and use the software restriction policy to block the paths that lead to its execution.
Certutil.exe	Prevent access to Certutil.exe by creating a GPO (Group Policy Object) to restrict its execution path through the software restriction policy.

Common Binaries in KILL CHAIN PHASES

Bitsadmin.exe, Certutil.exe, Net.exe, Net1.exe, Powershell.exe, Cmd.exe, Reg.exe

By mitigating the potential misuse of common Windows binaries, you can strengthen your defenses against multiple types of malware/ransomware making you a harder target for attackers.



Ransomware continues to evolve, posing significant risks to organizations worldwide. Understanding the different types of ransomware, common techniques used by attackers, and best practices for prevention and response is critical for minimizing impact. A well-defined post-event policy and communication strategy ensures that organizations can effectively manage ransomware incidents, protect their data, and maintain stakeholder trust. By staying informed and prepared, organizations can better defend against the ever-growing threat of ransomware and ensure resilience in the face of cyber adversities.

REFERENCES:

1. https://online.utulsa.edu/blog/famous-ransomware-attacks-in-history/
2. https://www.securityweek.com/ransomware-attack-disrupts-bassett-furniture-manufacturing-facilities/
3. https://www.bbc.com/news/technology-39901382
4. https://govinsider.asia/intl-en/article/cyberattack-on-indonesias-national-data-centre-paralyses-government-services
5. https://www.scmagazine.com/news/eso-solutions-says-2-7m-medical-records-exposed-in-oct-ransomware-attack
6. https://www.bleepingcomputer.com/news/security/chipmaker-nexperia-confirms-breach-after-ransomware-gang-leaks-data/
7. https://www.govinfosecurity.com/avoslocker-claims-data-theft-from-another-healthcare-entity-a-19083
8. https://www.bloomberg.com/news/articles/2021-04-21/apple-targeted-in-50-million-ransomware-hack-of-supplier-quanta
9. https://www.securityweek.com/ransomware-attack-cost-keytronic-over-17-million/
10. https://www.scmagazine.com/brief/us-firms-claimed-to-be-attacked-by-bianlian-ransomware-gang
11. https://www.zdnet.com/article/this-unusual-ransomware-attack-targets-home-pcs-so-beware/
12. https://threatpost.com/fake-ransomware-infection-wordpress/176410/
13. https://www.cybereason.com/blog/what-are-the-legal-implications-from-a-ransomware-attack
14. https://www.veeam.com/resources/wp-2024-ransomware-trends-executive-summary-global.html
15. https://www.ctm360.com/threatscape-report/

ACRONYMS:

1. *EASM: External Attack Surface Management*
2. *DRP: Digital Risk Protection*
3. *CTI: Cyber Threat Intelligence*
4. *DMARC: Domain-based Message Authentication, Reporting and Conformance*

View your attack surface and digital frauds in
CTM360's COMMUNITY EDITION.

SIGN UP NOW!

The platform is pre-populated with your data, including hosts, technologies, look-alike domains, leaked credentials, and much more.

You get **3 takedowns for FREE,** as well as access to our community edition of the DMARC platform, all at **NO** cost!

ADDITIONALLY, YOU'LL RECEIVE :
Cyber News Alerts & advisories along with threat actor TTPs and mitigation guidelines to help make yourself a harder target in cyberspace.

CTM360®

ENABLING ORGANIZATIONS TO PROTECT THEMSELVES AND THEIR SUPPLY CHAIN AGAINST EXTERNAL RISKS AND THREATS.

INFO@CTM360.COM | WWW.CTM360.COM