Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Aug 20 - 26, 2024

Report Summary:

- **New Threat Detection Added** – 3 (Numozylod Malware, Cobalt Strike Malleable C2 and Meimaii Malware)
- **New Threat Protections - 117**

The following threats were added to Crystal Eye XDR this week:

1. Numozylod Malware

Numozylod is a relatively new malware family that has emerged as a growing threat in the cyber landscape. NUMOZYLOD is characterised by its advanced evasion techniques and modular architecture. This malware is capable of a wide range of malicious activities, including data exfiltration, remote code execution, and persistent system control. Associated with a threat actor believed to be of Russian origin, NUMOZYLOD has been observed in various cyberattacks targeting critical infrastructure and government entities. The malware's sophisticated capabilities and affiliation with a well-resourced threat actor make it a significant concern for organisations worldwide.

Threats Protected: 02
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1059	Command and Scripting Interpreter
	T1059.001	PowerShell
	T1064	Scripting
Persistence	T1547	Boot or Logon AutoStart Execution
	T1574.002	DLL Side Loading
Defence Evasion	T1027	Obfuscated Files or Information
	T1112	Modify Registry
Discovery	T1010	Application Window Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
Collection	T1056	Input Capture
	T1115	Clipboard Data
Command-and-Control	T1071	Application Layer Protocol

2. Cobalt Strike Malleable C2

Cobalt Strike Malleable is a powerful post-exploitation framework used by both legitimate security professionals and malicious actors. Its flexibility allows attackers to customise their operations, making it a versatile tool for a variety of cybercrime activities. While Cobalt Strike itself is legitimate, its misuse by malicious actors has led to its association with high-profile cyberattacks. Malleable's capabilities include lateral movement, privilege escalation, data exfiltration, and command-and-control (C2) infrastructure management. Its popularity and effectiveness have made it a persistent threat to organisations worldwide.

Threats Protected: 05
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1129	Shared Module
Defence Evasion	T1497 T1497.003	Virtualisation/Sandbox Evasion Time-Based Evasion
Credential Access	T1539	Steal Web Session Cookie
Discovery	T1082 T1083	System Information Discovery File and Directory Discovery
Command-and-Control	T1071	Application Layer Protocol

3. Meimaii Malware

Meimaii is a sophisticated malware family known for its advanced evasion techniques and persistence. Initially detected in 2018, Meimaii has been linked to various cyberattacks targeting government, military, and industrial sectors. This malware's modular architecture allows attackers to tailor its capabilities to specific objectives, including data exfiltration, remote code execution, and system control. Meimaii's ability to evade detection, combined with its affiliation with a well-resourced threat actor, makes it a significant threat to organisations worldwide.

Threats Protected: 01
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Discovery	T1018	Remote System Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
Command-and-Control	T1071	Application Layer Protocol
	T1095	Non-Application Layer Protocol
	T1105	Ingress Tool Transfer

Known exploited vulnerabilities (Week 4 August 2024):

Vulnerability	CVSS	Description
CVE-2024-23897	9.8 (Critical)	Jenkins Command Line Interface (CLI) Path Traversal Vulnerability
CVE-2021-31196	7.2 (High)	Microsoft Exchange Server Information Disclosure Vulnerability
CVE-2022-0185	8.4 (High)	Linux Kernel Heap-Based Buffer Overflow
CVE-2021-33045	9.8 (Critical)	Dahua IP Camera Authentication Bypass Vulnerability
CVE-2021-33044	9.8 (Critical)	Dahua IP Camera Authentication Bypass Vulnerability
CVE-2024-39717	6.6 (Medium)	Versa Director Dangerous File Type Upload Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-august-2024/500

Updated Malware Signatures (Week 4 August 2024)

Threat	Description
Glupteba	A malware dropper that is designed to download additional malware on an infected machine.
Qwerty Stealer	A QWERTY malware stealer, also known simply as QWERTY, is a type of malicious software designed to steal sensitive information from an infected computer. This information can include passwords, login credentials, financial details, and other personal data.
Lumma Stealer	A type of malware classified as an information stealer. Its primary purpose is to steal sensitive information from infected systems, including but not limited to credentials, financial information, browser data, and potentially other personal or confidential information.
BlankGrabber Stealer	BlankGrabber stealer malware is a type of malicious software designed to steal sensitive information from an infected system. This information can include login credentials, passwords, browser cookies, stored credit card information, and other personal data. The malware typically operates by extracting this data from web browsers, applications, and system files where such information is commonly stored.

Ransomware Report

The Red Piranha Team actively collects information on organisations globally affected by ransomware attacks from various sources, including the Dark Web. In the past week alone, our team uncovered new ransomware victims and updates on previous victims across 19 industries spanning 27 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

RansomHub ransomware group stands out as the most prolific, having updated a significant number of victims (20%) distributed across multiple countries. In comparison, Play ransomware updated 06% of victims, in the past week. The following list provides the victim counts in percentages for these ransomware groups and a selection of others.

Name of Ransomware Group	Percentage of new Victims last week
Abyss-Data	1.03%
Akira	4.12%
Bianlian	2.06%
Black Suit	3.09%
Blackout	1.03%
Brain Cipher	1.03%
Cicada3301	3.09%
Ciphbit	1.03%
Cloak	5.15%
Darkvault	1.03%
Dragonforce	5.15%
Eraleign (Apt73)	3.09%
Handala	1.03%
Helldown	6.19%
Hunters	4.12%
Inc Ransom	2.06%
Killsec	3.09%
Lockbit3	2.06%
Lynx	3.09%
Mad Liberator	1.03%
Medusa	2.06%
Meow	4.12%
Metaencryptor	2.06%
Play	6.19%
Qilin	4.12%
Ransomhouse	1.03%
RansomHub	19.59%
Rhysida	4.12%
Space Bears	1.03%
Stormous	1.03%
Trinity	1.03%

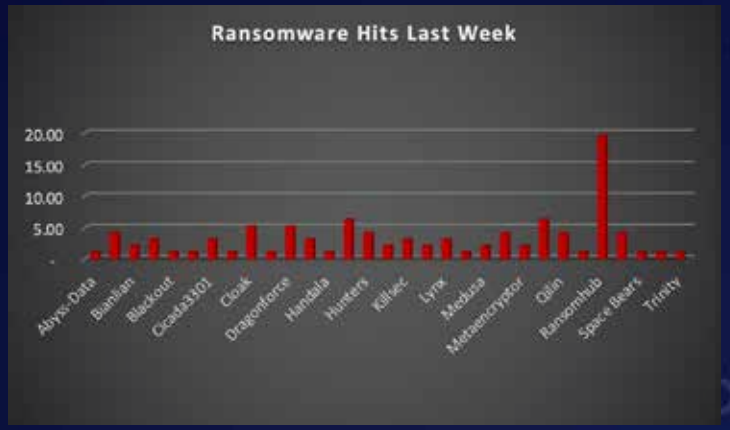

Figure 1: Ransomware Group Hits Last Week

Cloak Ransomware

Cloak ransomware, first detected in late 2022, quickly established itself as a formidable threat in the cybercrime landscape. This stealthy malware employs a double extortion tactic, encrypting victims' data and threatening to leak it on the dark web if ransom demands aren't met. While the exact origins of Cloak remain shrouded in some mystery, security researchers believe it may be linked to a cybercriminal group operating out of Eastern Europe. This group's previous activities suggest a level of sophistication in malware development and deployment, making Cloak a particularly dangerous adversary.

As previously mentioned, Cloak Ransomware began compromising victims in late 2022. Throughout 2023, it claimed to have successfully attacked 32 organisations worldwide. Germany and the United States were among the countries most heavily affected by Cloak Ransomware during this period.

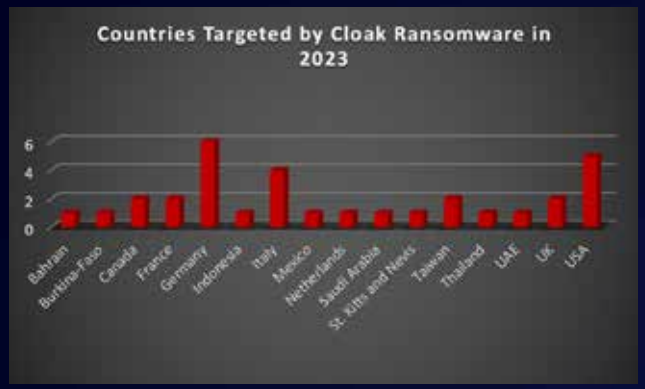

Figure 2: Countries hit by Cloak Ransomware in 2023

However, as of the date, we are writing this report, Cloak Ransomware has already claimed to have attacked 32 countries in 2024. Following the trend from the previous year, the United States and Germany remain the primary targets.

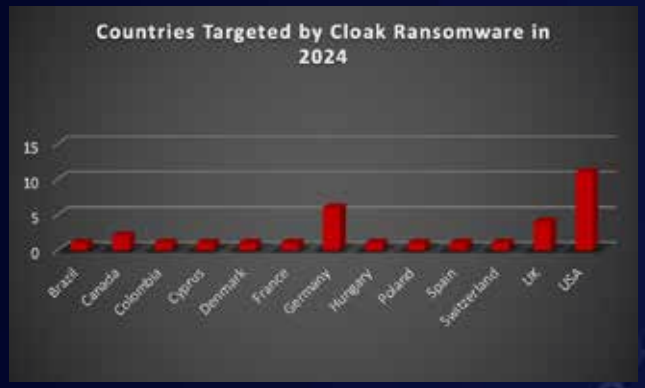

Figure 3: Countries hit by Cloak Ransomware in 2024

TTPs:

Cloak ransomware doesn't rely solely on brute force. It possesses a diverse arsenal of tactics, techniques, and procedures (TTPs) to infiltrate and compromise systems stealthily. Here's a glimpse into its malicious toolkit:

- Phishing Attacks: Deceptive emails designed to trick users into clicking malicious links or downloading infected attachments are a common entry point. These emails often mimic legitimate business communications, making them more likely to be clicked.
- Exploiting Unpatched Vulnerabilities: Cloak actively seeks out unpatched vulnerabilities in software and operating systems to gain unauthorised access to networks. This underscores the importance of keeping all software and systems updated with the latest security patches.
- Remote Desktop Protocol (RDP) Exploitation: Like other ransomware strains, Cloak can exploit weaknesses in RDP configurations to gain access to a system. RDP allows remote access to a computer, and misconfigured settings can create a vulnerability for attackers.
- Supply Chain Attacks: Cloak has shown a preference for targeting supply chains, compromising vendors and suppliers to gain access to a wider network of victims. This tactic allows attackers to reach a larger number of victims with a single intrusion.
- Lateral Movement: Once a foothold is established on a single system, Cloak can utilise various tools to move laterally across a network. This allows it to infect additional devices, escalate privileges, and potentially compromise critical systems.
- Data Exfiltration: Before encryption, Cloak often exfiltrates sensitive data like financial records, personal information, and intellectual property. This stolen data serves as additional leverage in extortion attempts, putting pressure on victims to pay the ransom.
- Strong Encryption: The malware utilises robust encryption algorithms to render files inaccessible. Decrypting them without the attacker's key is extremely difficult, if not impossible. This effectively cripples a victim's operations until a decision is made.

Data Leak Site: Cloak ransomware maintains a data leak site on the dark web where they list victims who haven't paid the ransom. This serves as a public shaming tactic and adds pressure on compromised organisations.

Figure 4: Screenshot of Leak Site used by Cloak Ransomware

Ransom Note

Cloak ransomware, a notorious cyber threat, employs a deceptive tactic in its ransom notes. Rather than demanding a ransom outright, it presents itself as a "data recovery service." This facade aims to manipulate victims into believing they have a chance to recover their encrypted data for a fee.

However, this is a deceptive ploy. Once a victim pays the ransom, there's no guarantee that their data will be decrypted. In many cases, victims are left with no option but to rebuild their systems and data from backups.

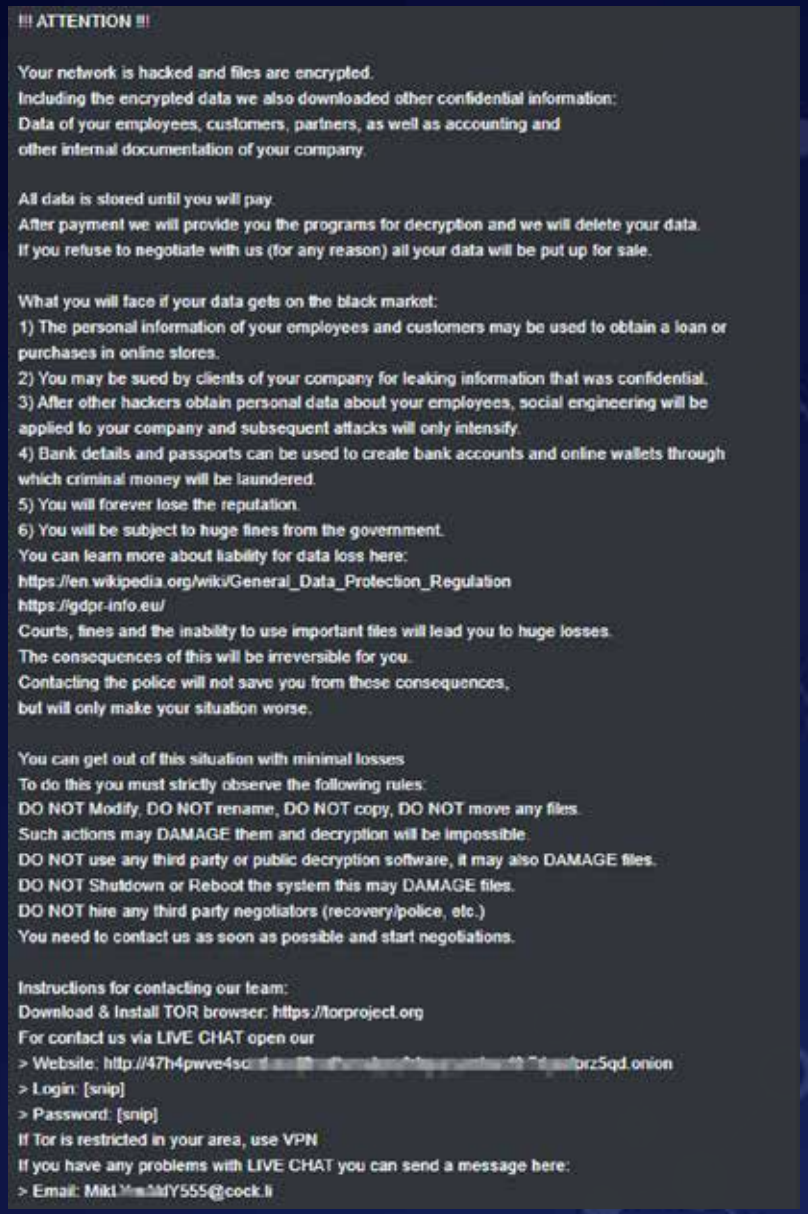

Figure 5: Screenshot of Ransom Note used by Cloak Ransomware

A Global Reach with Focused Targets

Cloak ransomware has demonstrated a global reach, targeting victims across various industries and geographies. Here are some examples of its operations and the impact it has caused:

- Healthcare Organisations: Hospitals and other healthcare providers have been frequent targets due to the sensitive nature of patient data and the potential disruption to critical services.
- Manufacturing Disruptions: Manufacturing companies across the globe have fallen victim to Cloak, experiencing data breaches, operational disruptions, and potential production delays.
- Financial Institutions: The financial sector has also been targeted, with banks and credit unions facing potential data breaches and economic losses.

The emergence of Cloak ransomware underscores the ever-evolving threat landscape of cybercrime. Its focus on supply chain attacks and the potential for significant disruptions highlights the need for organisations to prioritise robust cybersecurity measures.

Tactic	Technique ID	Technique Name
Initial Access	T1195	Supply Chain Compromise
	T1566.002	Spearphishing Link
	T1190	Exploit Public-Facing Application
	T1566.001	Spearphishing Attachment
	T1078	Valid Accounts
Execution	T1059.001	PowerShell
	T1569.002	Service Execution
	T1059.003	Windows Command Shell
Persistence	T1547.009	Shortcut Modification
	T1547.001	Registry Run Keys / Startup Folder
	T1078	Valid Accounts
Privilege Escalation	T1078	Valid Accounts
	T1547.001	Registry Run Keys / Startup Folder
	T1547.009	Shortcut Modification
Defence Evasion	T1027.001	Binary Padding
	T1036.005	Match Legitimate Name or Location
	T1078	Valid Accounts
Discovery	T1016.001	Internet Connection Discovery
Collection	T1114.001	Local Email Collection
Exfiltration	T1537	Transfer Data to Cloud Account
	T1567	Exfiltration Over Web Service
Impact	T1486	Data Encrypted for Impact

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxp://47h4pwve4scndaneljfnxdhzoulgsyfzbgayyonbwztfz74gsdprz5qd.onion hxxp://cloak7jpvcb73rtx2ff7kaw2kholu7bdiivxpzbhlny4ybz75dpxckqd.onion	URLs (Onion)	Leak Site
MikLYmAklY555@cock.li	Email	

In a comprehensive analysis of ransomware victims across 27 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 50% victim updates in the past week. The following list provides a breakdown of the number and percentage of new ransomware victims per country, underscoring the persistent and concerning prevalence of ransomware attacks, with the USA particularly susceptible to these cybersecurity threats.

Industry	Victims Count (%)
Australia	2.06%
Austria	1.03%
Belgium	1.03%
Brazil	1.03%
Bulgaria	1.03%
Canada	3.09%
China	2.06%
Czech Republic	1.03%
Denmark	2.06%
Germany	3.09%
Ireland	1.03%
Israel	1.03%
Italy	1.03%
Jersey	1.03%
Lebanon	3.09%
New Zealand	1.03%
Philippines	1.03%
Poland	1.03%
Saudi Arabia	1.03%
South Africa	2.06%
South Korea	1.03%
Spain	1.03%
Sweden	1.03%
Switzerland	2.06%
Taiwan	1.03%
UK	12.37%
USA	50.52%

Figure 6: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 19 different industries worldwide. Notably, Manufacturing bore the brunt of the attacks in the past week, accounting for 26% of victims each. There are a few key reasons why the manufacturing sector is a prime target for ransomware groups:

- High Disruption Potential: Manufacturing relies heavily on interconnected systems and just-in-time production. A ransomware attack can grind operations to a halt, causing significant financial losses due to production delays and lost revenue. This pressure to get back online quickly can make manufacturers more willing to pay the ransom.
- Vulnerable Legacy Systems: Many manufacturers use legacy control systems (OT) that haven't been updated for security. These older systems often lack robust security features, making them easier targets for attackers to exploit.
- Limited Cybersecurity Investment: Traditionally, cybersecurity might not have been a top priority for some manufacturers compared to production efficiency. This lack of investment in security awareness training and robust security protocols leaves them exposed.
- Valuable Data: Manufacturing facilities often hold valuable intellectual property (IP) and trade secrets. Ransomware groups may not only disrupt operations but also threaten to leak this sensitive data if the ransom isn't paid.
- Success Breeds Success: The high payout potential from past attacks on manufacturers incentivises ransomware groups to continue targeting them.

Industry	Victims Count (%)
Agriculture	2.06%
Business Services	10.31%
Cities, Towns & Municipalities	1.03%
Construction	6.19%
Education	6.19%
Energy, Utilities & Waste Treatment	2.06%
Finance	8.25%
Healthcare	5.15%
Hospitality	4.12%
Insurance	1.03%
IT	5.15%
Legal Services	3.09%
Manufacturing	25.77%
Media & Internet	2.06%
Organisations	5.15%
Real Estate	1.03%
Retail	5.15%
Telecom	4.12%
Transportation	2.06%

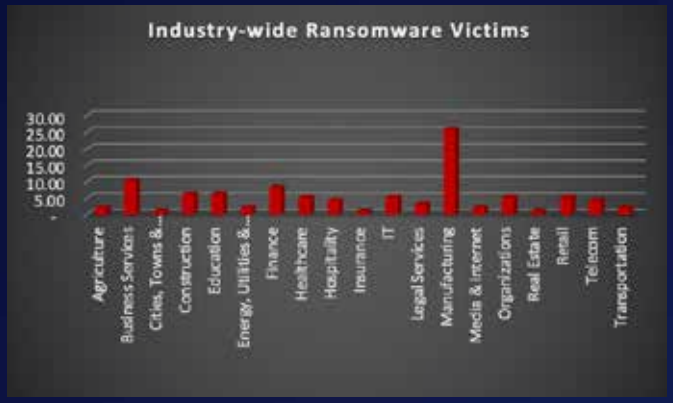

Figure 7: Industry-wide Ransomware Victims

According to recent data, the manufacturing industry was the most heavily targeted by ransomware groups in 2024, followed by business services and hospitality.

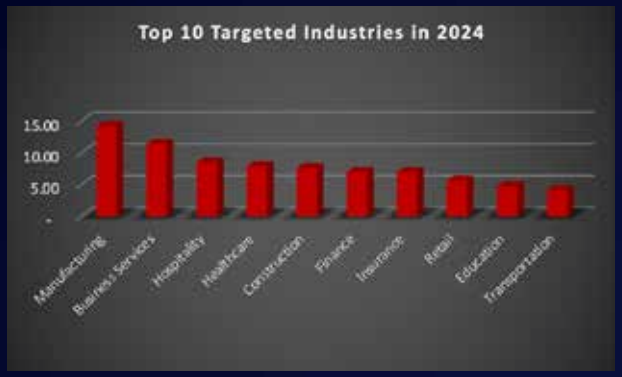

Figure 8: Top 10 Targeted Industries in 2024

Here are some crucial steps organisations can take to mitigate the risk of ransomware and similar threats:

- Third-Party Risk Management: Implement a comprehensive third-party risk management program to assess and monitor the security posture of vendors and suppliers.
- Supply Chain Visibility: Maintain visibility into your supply chain to identify potential risks and vulnerabilities.
- Regular Backups: Maintain secure, offline backups of critical data to facilitate recovery in case of a ransomware attack.
- Patch Management: Implement a rigorous patch management system to ensure all software and operating systems are updated with the latest security patches.
- Security Awareness Training: Educate employees on identifying phishing attempts and other social engineering tactics used by attackers. Regular training can significantly reduce the risk of human error leading to breaches.
- Endpoint Security Solutions: Deploy endpoint security solutions that can detect and prevent malware infections at the device level. These solutions can act as a first line of defence against Cloak and other malware threats.
- Network Segmentation: Segmenting your network can limit the lateral movement of ransomware, potentially preventing it from spreading throughout your entire infrastructure.
- Incident Response Planning: Develop and regularly test an incident response plan to effectively respond to a ransomware attack and minimise damage. Having a plan in place ensures a more coordinated and efficient response during a crisis.