Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Sept 10 - 16, 2024

Report Summary:

- **New Threat Detection Added** – 3 (Obsidium Stealer, Spy Keylogger and Enigma Stealer)
- **New Threat Protections - 63**

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

1. Obsidium Stealer

Obsidium Stealer is a potent information-stealing malware that has emerged as a significant threat in the cyber landscape. This malware targets a wide range of sensitive data, including login credentials, credit card information, cryptocurrency wallet details, and personal files. Obsidium Stealer's advanced capabilities, such as keylogging, screen capturing, and file exfiltration, make it a formidable tool for cybercriminals. Often distributed through phishing emails or malicious downloads, Obsidium Stealer poses a significant risk to both individuals and organisations. Effective cybersecurity measures, including vigilant email practices, strong password management, and regular software updates, are essential to protect against this and other malware threats.

Threats Protected: 10

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	T1047	Windows Management Instrumentation
Persistence	T1574 T1574.002	Hijack Execution Flow DLL Side Loading
Privilege Escalation	T1574 T1574.002	Hijack Execution Flow DLL Side Loading
Defence Evasion	T1027 T1027.002 T1497	Obfuscated Files or Information Software Packing Virtualisation/Sandbox Evasion
Credential Access	T1003 T1056	OS Credential Dumping Input Capture
Discovery	T1082 T1083	System Information Discovery Files and Directory Discovery
Collection	T1005 T1056	Data from Local System Input Capture

2. Spy Keylogger

Spy Keylogger is a stealthy malware designed to record keystrokes entered on a compromised system. This type of malware can be used to steal sensitive information such as passwords, credit card numbers, and personal details. Spy Keyloggers often operate in the background, silently capturing keystrokes without the user's knowledge. They can be distributed through various methods, including phishing emails, malicious downloads, or bundled with legitimate software. To protect against Spy Keylogger threats, users should be cautious about opening suspicious emails, downloading files from untrusted sources, and using strong, unique passwords for their online accounts.

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
Initial Access	T1091	Replication Through Removable Media
Execution	T1059 T1129	Command and Scripting Interpreter Shared Modules
Persistence	T1547 T1547.001	Boot or Logon AutoStart Execution Registry Run Keys / Startup Folder
Privilege Escalation	T1055 T1055.003 T1134	Process Injection Thread Execution Hijacking Access Token Manipulation
Defence Evasion	T1027	Obfuscated Files or Information
Collection	T1056 T1113	Input Capture Screen Capture
Command-and-Control	T1071	Application Layer Protocol

3. Enigma Stealer

Enigma Stealer is a potent information-stealing malware that has emerged as a significant threat in the cyber landscape. This malware targets a wide range of sensitive data, including login credentials, credit card information, cryptocurrency wallet details, and personal files. Enigma Stealer's advanced capabilities, such as keylogging, screen capturing, and file exfiltration, make it a formidable tool for cybercriminals. Often distributed through phishing emails or malicious downloads, Enigma Stealer poses a significant risk to both individuals and organisations. Effective cybersecurity measures, including vigilant email practices, strong password management, and regular software updates, are essential to protect against this and other malware threats.

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
Execution	T1047	Windows Management Instrumentation
Persistence	T1547 T1547.001 T1547.008	Boot or Logon AutoStart Execution Registry Run Keys / Startup Folder LSASS Driver
Privilege Escalation	T1055 T1055.003 T1134	Process Injection Thread Execution Hijacking Access Token Manipulation
Defence Evasion	T1027 T1036 T1055	Obfuscated Files or Information Masquerading Process Injection
Collection	T1056 T1114 T1115	Input Capture Email Collection Clipboard Data
Command-and-Control	T1071 T1095	Application Layer Protocol Non-Application Layer Protocol

Known exploited vulnerabilities (Week 2 September 2024):

Vulnerability	CVSS	Description
CVE-2024-40766	9.8 (Critical)	SonicWall SonicOS Improper Access Control Vulnerability
CVE-2017-1000253	7.8 (High)	Linux Kernel PIE Stack Buffer Corruption Vulnerability
CVE-2016-3714	8.4 (High)	ImageMagick Improper Input Validation Vulnerability
CVE-2024-38217	5.4 (Medium)	Microsoft Windows Mark of the Web (MOTW) Protection Mechanism Failure Vulnerability
CVE-2024-38014	7.8 (High)	Microsoft Windows Installer Improper Privilege Management Vulnerability
CVE-2024-43491	9.8 (Critical)	Microsoft Windows Update Use-After-Free Vulnerability
CVE-2024-38226	7.3 (High)	Microsoft Publisher Protection Mechanism Failure Vulnerability
CVE-2024-8190	7.2 (High)	Ivanti Cloud Services Appliance OS Command Injection Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-september-2024/506

Updated Malware Signatures (Week 2 September 2024)

Threat	Description
QuasarRat	A remote access trojan that was made available to the public as an open-source project. Once installed on a victim's machine, it is capable of keylogging, data and screen capturing among other things. It is also known to be highly customisable depending on the threat actor's intended need.
Lumma Stealer Nanocore	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. The Nanocore trojan, built on the .NET framework, has been the subject of multiple source code leaks, resulting in its widespread accessibility.
	Like other remote access trojans (RATs), Nanocore empowers malicious actors with complete system control, enabling activities such as video and audio recording, password theft, file downloads, and keystroke logging.

Ransomware Report

The Red Piranha Team actively monitors the dark web and other sources to identify organisations globally affected by ransomware attacks. In the past week alone, we have uncovered new ransomware victims and updates on existing cases across 18 industries in 16 countries. This highlights the pervasive nature of ransomware, demonstrating its ability to target organisations of all sizes and sectors worldwide.

RansomHub ransomware group significantly increased its attacks this week, claiming a 15% decrease in victims compared to the previous week (31%). It is the most prolific ransomware group, with victims distributed across multiple countries. Play ransomware updated its victim count by 10% in the past week, increasing the number of victims by 3% from the previous 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
3AM	1.33%
Akira	1.33%
Bianlian	9.33%
Black Suit	2.67%
Cactus	5.33%
Dispossessor	1.33%
Dragonforce	8.00%
Everest	1.33%
Fog	2.67%
Hunters	5.33%
Inc Ransom	4.00%
Killsec	2.67%
Lynx	2.67%
Mad Liberator	1.33%
Meow	9.33%
Play	10.67%
Qilin	9.33%
RansomHub	14.67%
Rhysida	4.00%
Space Bears	1.33%
Stormous	1.33%

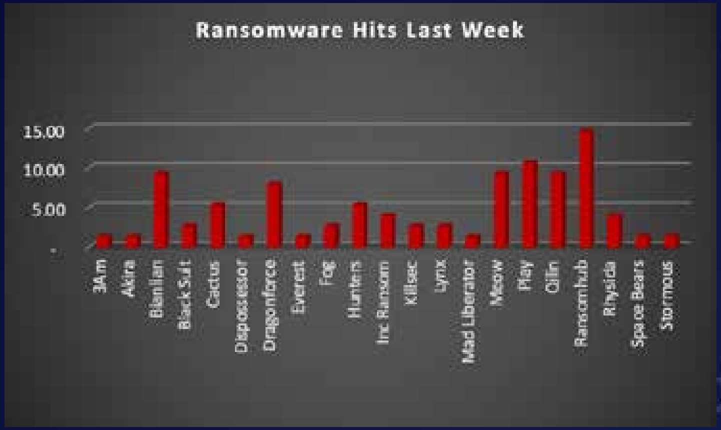

Figure 1: Ransomware Group Hits Last Week

3AM Ransomware

Emerging in the early months of 2023, 3AM ransomware 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 are not met. While the exact origins of 3AM remain shrouded in 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 3AM a particularly dangerous adversary.

TTPs:
3AM ransomware does not rely solely on brute force. It possesses a diverse arsenal of tactics, techniques, and procedures (TTPs) to infiltrate and compromise systems stealthily. Here is 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: 3AM 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, 3AM 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: 3AM 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, 3AM 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, 3AM 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: 3AM ransomware maintains a data leak site on the dark web where they list victims who have not paid the ransom. This serves as a public shaming tactic and adds pressure on compromised organisations.

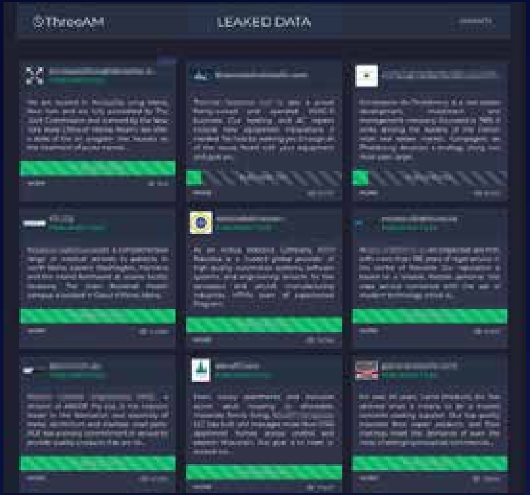

Figure 2: Screenshot of Leak Site used by 3AM Ransomware

Ransom Note

3AM ransomware, a notorious cyber threat, employs a deceptive tactic in its ransom notes. Rather than demanding a ransom outright, it presents itself as a "bidon_readme.txt" or “readme.txt”. 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 is 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.

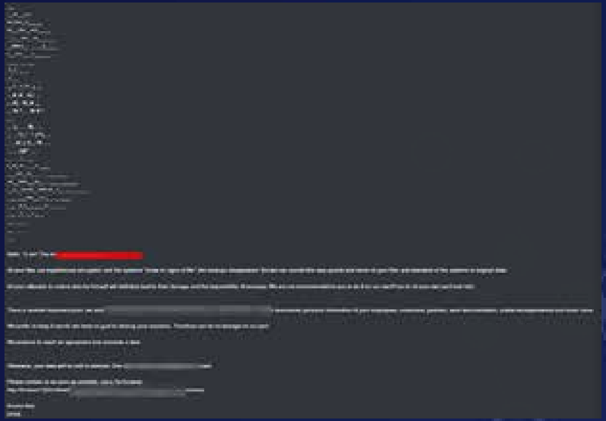

Figure 3: Screenshot of Ransom Note used by 3AM Ransomware

A Global Reach with Focused Targets

3AM 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 3AM, 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 3AM 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
Execution	T1053	Schedule Task/Job
Defence Evasion	T1082	System Info Discovery
	T1140	DE obfuscate/Decode Files or Information
	T1490	Inhibit System Recovery
Discovery	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1518	Software Discovery
Lateral Movement	T1021	Remote Services: SMB/Windows Admin Shares
Collection	T1005	Data from Local System
	T1056	Input Capture
Command-and-Control	T1071	Application Layer Protocol: Web Protocols
Exfiltration	T1041	Exfiltration Over C2 Channel
Impact	T1486	Data Encrypted for Impact
	T1491	Defacement
	T1499	Endpoint Denial of Service

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxp://threeamkelxicjsaf2czjyz2lc4q3ngqkxhhlexyfcp2o6raw4rphyad[.]onion	URLs (Onion)	Leak Site
307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e	Hash	Malicious Files

A recent analysis of ransomware victims across 16 countries reveals the United States as the most heavily impacted nation, with a staggering 56% increase in victim reports over the past week. Notably, UK has also experienced a significant rise, with victim reports jumping from 5% to over 13% in the same period. The following list details the number and percentage of new ransomware victims per country, highlighting the pervasive and concerning nature of ransomware attacks, particularly in the United States.

Industry	Victims Count (%)
Australia	2.67%
Belgium	2.67%
Cameroon	1.33%
Canada	6.67 %
France	2.67%
Germany	1.33%
India	1.33%
Indonesia	1.33%
Israel	1.33%
Italy	4.00%
Japan	1.33%
Malaysia	1.33%
Senegal	1.33%
Thailand	1.33%
UK	13.33%
USA	56.00%

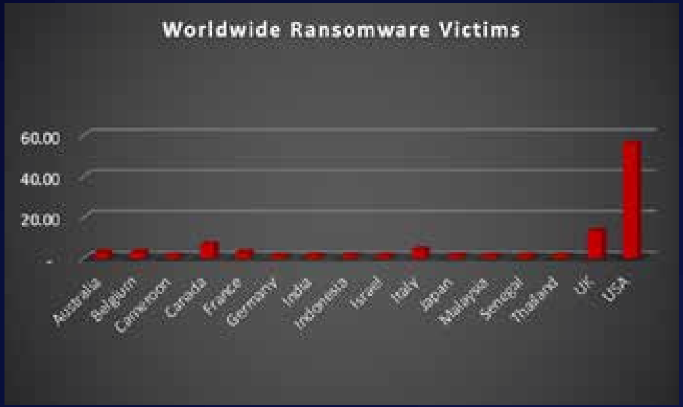

Figure 4: Ransomware Victims Worldwide

Further analysis reveals that ransomware has impacted 18 industries worldwide. The manufacturing sector remains a significant target, accounting for 30% of victims in the past week, increasing victims from 10% in the past week, despite a slight decrease in attacks on business services (11%) which was 15% during the past week.

Industry	Victims Count (%)
Agriculture	1.33%
Business Services	10.67%
Construction	8.00%
Consumer Services	1.33%
Education	5.33%
Finance	6.67%
Government	2.67%
Healthcare	5.33%
Hospitality	5.33%
Insurance	2.67%
IT	4.00%
Legal Services	2.67%
Manufacturing	29.33%
Media & Internet	1.33%
Metals & Mining	4.00%
Organisations	2.67 %
Retail	5.33%
Transportation	1.33%

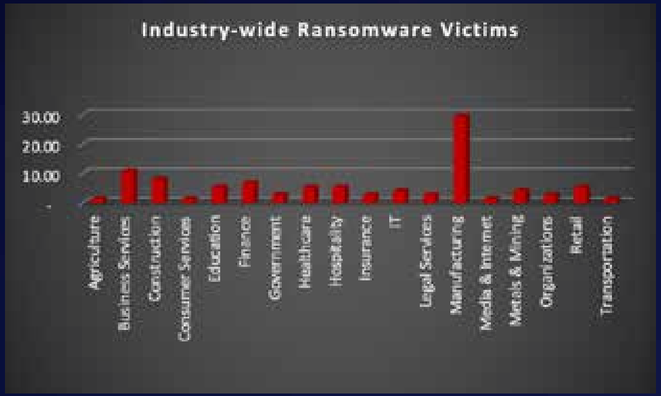

Figure 5: Industry-wide Ransomware Victims

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.