Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Oct 8 - 14, 2024

Report Summary:

- **New Threat Detection Added** – 2 (FleshStealer Malware and AhMyth RAT)
- **New Threat Protections - 197**

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

1. FleshStealer Malware

FleshStealer is a potent information-stealing botnet that has emerged as a significant threat in the cyber landscape. This botnet leverages compromised devices to harvest sensitive data, including login credentials, credit card information, cryptocurrency wallet details, and personal files. FleshStealer'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, FleshStealer poses a significant risk to both individuals and organisations.

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	T1106	Native API
Persistence	T1574	Hijack Execution Flow
	T1574.002	DLL Side Loading
Privilege Escalation	T1055	Process Injection
Defence Evasion	T1027	Obfuscated Files or Information
	T1027.002	Software Packing
	T1055	Process Injection
Credential Access	T1056	Input Capture
Discovery	T1082	System Information Discovery
	T1083	Files and Directory Discovery
Collection	T1056	Input Capture
	T1560	Archive Collected Data
Command-and-Control	T1071	Application Layer Protocol
	T1095	Non-Application Layer Protocol

2. AhMyth RAT

AhMyth RAT is a sophisticated Remote Access Trojan (RAT) that has emerged as a significant threat in the cyber landscape. This malware grants attackers extensive control over compromised systems, enabling them to steal data, execute commands, and establish persistent backdoors. AhMyth's advanced features, including encryption and anti-analysis techniques, make it difficult to detect and mitigate. The malware has been linked to various cyberattacks targeting government, military, and critical infrastructure sectors. Its ability to evade detection, combined with its affiliation with a well-resourced threat actor, makes AhMyth a significant concern for organisations worldwide.

Threats Protected: 04
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	T1518 T1518.001	Software Discovery Security Software Discovery
Command-and-Control	T1071 T1573	Application Layer Protocol Encrypted Channel
Defence Evasion	T1406	Obfuscated Files or Information
Discovery	T1430	Location Tracking
Collection	T1429 T1430	Audio Capture Location Tracking

Known exploited vulnerabilities (Week 2 October 2024):

Vulnerability	CVSS	Description
CVE-2024-43573	8.1 (High)	Microsoft Windows MSHTML Platform Spoofing Vulnerability
CVE-2024-43572	7.8 (High)	Microsoft Windows Management Console Remote Code Execution Vulnerability
CVE-2024-43047	7.8 (High)	Qualcomm Multiple Chipsets Use-After-Free Vulnerability
CVE-2024-9380	7.2 (High)	Ivanti Cloud Services Appliance (CSA) OS Command Injection Vulnerability
CVE-2024-9379	7.2 (High)	Ivanti Cloud Services Appliance (CSA) SQL Injection Vulnerability
CVE-2024-23113	9.8 (Critical)	Fortinet Multiple Products Format String Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-october-2024/512

Updated Malware Signatures (Week 2 October 2024)

Threat	Description
Zeus	Also known as Zbot, this malware is primarily designed to steal banking credentials.
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.
Vidar	A stealer designed to collect sensitive data from infected machines. It usually targets Windows-based machines and is spread through email attachments or downloads from compromised websites.

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 21 industries in 32 countries. This highlights the pervasive nature of ransomware, demonstrating its ability to target organisations of all sizes and sectors worldwide.

The Sarcoma ransomware group has claimed 20% of victims this week. This surge solidifies its position as the ransomware group with the highest number of victims reported this week. Play ransomware updated its victim count by 12% during the same period. 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	0.71%
8Base	9.29%
Abyss-Data	0.71%
Akira	2.14%
Bianlian	0.71%
Black Suit	0.71%
Cactus	2.86%
Ciphbit	0.71%
Clop	2.14%
El Dorado	1.43%
Everest	0.71%
Handala	2.14%
Hunters	5.71%
Inc Ransom	1.43%
Killsec	5.71 %
Lockbit3	0.71%
Lynx	2.14%
Medusa	5.00%
Meow	7.86%
Monti	1.43%
Orca	0.71%
Play	11.43%
Qilin	1.43%
RansomHouse	1.43%
RansomHub	7.86%
Rhysida	0.71%
Sarcoma	20.00%
Stormous	1.43%
Team Underground	0.71%

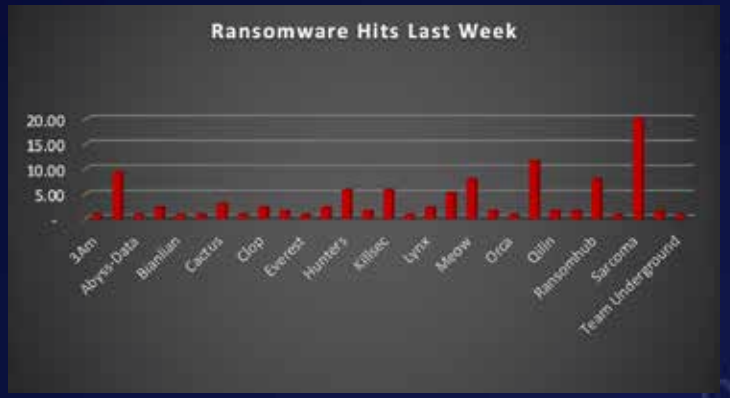

Figure 1: Ransomware Group Hits Last Week

Sarcoma Ransomware

Sarcoma ransomware, a formidable adversary in the cybercrime landscape, first emerged in late 2023, quickly establishing itself as a significant threat. This ransomware, known for its aggressive tactics and devastating impact, employs a double extortion model, encrypting victims' data and threatening to leak it on the dark web if ransom demands aren't met. While the exact origins of Sarcoma 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 Sarcoma a particularly dangerous threat.

TTPs:
Sarcoma 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**: Sarcoma 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**: Similar to other ransomware strains, Sarcoma 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**: Sarcoma 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, Sarcoma 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, Sarcoma 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: Sarcoma 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 2: Screenshot of Leak Site used by Sarcoma Ransomware

A Global Reach with Focused Targets

Sarcoma 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 worldwide have fallen victim to Sarcoma, 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 Sarcoma 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	T1190 T1566	Exploit Public-Facing Application Phishing
Execution	T1059.001 T1129	Command and Scripting Interpreter: PowerShell T1129
Persistence	T1053.003 T1546.011	Server Software Component: Web Shell Event-Triggered Execution: Application Shimming
Privilege Escalation	T1068	Exploitation for Privilege Escalation
Defence Evasion	T1055 T1070 T1574.002	Process Injection Indicator Hijack Execution Flow: DLL Side-Loading
Discovery	T1018	Remote System Discovery
Command-and-Control	T1071 T1105	Application Layer Protocol Ingress Tool Transfer

A recent analysis of ransomware victims across 32 countries reveals the United States as the most heavily impacted nation, with a staggering 54% increase in victim reports over the past week. Notably, Canada has also experienced a significant rise once again, with victim reports of 7% last week. 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 (%)
Albania	0.71%
Algeria	0.71%
Australia	2.86%
Belgium	0.71%
Bolivia	0.71%
Brazil	0.71%
Bulgaria	0.71%
Canada	7.14%
China	0.71%
France	2.86%
Germany	2.86%
India	2.14%
Indonesia	0.71%
Israel	0.71%
Italy	0.71%
Japan	1.43%
Lithonia	0.71%
Mexico	0.71%
Netherlands	0.71%
New Zealand	0.71%
Philippines	0.71%
Poland	0.71%
Qatar	0.71%
Saudi Arabia	0.71%
Serbia	0.71%
South Africa	2.86%
Spain	5.00%
Sweden	2.14%
Switzerland	0.71%
UK	1.43%
USA	54.29%
Vietnam	0.71%

Figure 3: Ransomware Victims Worldwide

Further analysis reveals that ransomware has impacted 21 industries worldwide. The manufacturing sector remains a significant target, accounting for 20% of victims in the past week. Retail and Business Services sectors got 16% of victims each in the past week.

Industry	Victims Count (%)
Agriculture	0.71%
Business Services	11.43%
Construction	8.57%
Consumer Services	2.14%
Education	2.14%
Energy, Utilities & Waste Treatment	0.71%
Finance	5.00%
Government	0.71%
Healthcare	4.29%
Hospitality	3.57%
Insurance	2.14%
IT	5.00%
Legal Services	4.29%
Manufacturing	20.71%
Media & Internet	2.86%
Metals & Mining	2.14%
Organisations	2.14%
Real Estate	2.14%
Retail	15.71%
Telecom	0.71%
Transportation	2.86%

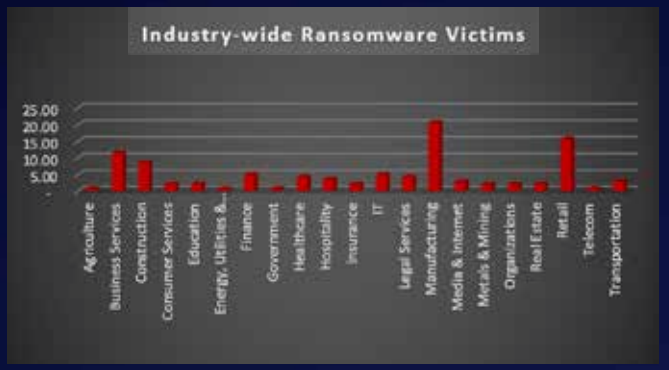

Figure 4: Industry-wide Ransomware Victims

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.