Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Sept 24 - 30, 2024

Report Summary:

- **New Threat Detection Added** – 2 (FoggyWeb Backdoor and DNSBin Malware)
- **New Threat Protections - 241**

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

1. FoggyWeb Backdoor

FoggyWeb Backdoor 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. FoggyWeb'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 FoggyWeb a significant concern for organisations worldwide. 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: 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
Initial Access	T1566	Phishing
	T1566.001	Spear Phishing
Execution	T1059	Command and Scripting Interpreter
	T1204.002	Malicious File
	T1064	Scripting
Defence Evasion	T1027	Obfuscated Files or Information
Discovery	T1082	System Information Discovery
	T1083	Files and Directory Discovery
Collection	T1113	Screen Capture
	T1005	Data from Local System
	T1048	Exfiltration on Alternative Protocol
Command-and-Control	T1071	Application Layer Protocol
	T1095	Non-Application Layer Protocol
	T1573	Encrypted Channel

2. DNSBin Malware

DNSBin is not a standalone malware but a service used by cybercriminals to exfiltrate data and establish command-and-control (C2) infrastructure. DNSBin provides a platform for attackers to send and receive data through DNS requests, making it difficult to detect and block traditional security measures. While not a malware itself, DNSBin is frequently leveraged by various threat actors to facilitate malicious activities, including malware distribution, data theft, and botnet management. Organisations should be aware of DNSBin and implement robust security measures to protect against its potential misuse. This includes monitoring network traffic for suspicious DNS requests, implementing DNS filtering, and educating employees about the risks of clicking on malicious links or downloading attachments from unknown sources.

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
Initial Access	T1091	Replication Through Removable Media
Execution	T1059 T1059.002	Command and Scripting Interpreter AppleScript
Persistence	T1547.001	Registry Run Keys / Startup Folder
Privilege Escalation	T1055 T1134	Process Injection Access Token Manipulation
Defence Evasion	T1070 T1070.004 T1564 T1564.001	Indicator Removal File Deletion Hide Artifacts Hidden Files and Directories
Discovery	T1082	System Information Discovery
Command-and-Control	T1071 T1095	Application Layer Protocol Non-Application Layer Protocol

Known exploited vulnerabilities (Week 3 September 2024):

Vulnerability	CVSS	Description
CVE-2024-7593	9.8 (Critical)	Ivanti Virtual Traffic Manager Authentication Bypass Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-september-2024/508

Updated Malware Signatures (Week 3 September 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 20 industries in 17 countries. This highlights the pervasive nature of ransomware, demonstrating its ability to target organisations of all sizes and sectors worldwide.

RansomsHub ransomware group has continued significantly increasing its attacks recently, claiming a 17% increase in victims this week alone. This surge solidifies its position as the group with the highest number of victims reported this week. Play ransomware also updated its victim count by 14% 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
Abyss-Data	2.86%
Akira	10.00%
Arcus Media	5.71%
Bianlian	2.86%
Black Suit	4.29%
Brain Cipher	1.43%
Cactus	5.71%
Cicada3301	10.00%
Everest	1.43%
Fog	1.43%
Hunters	1.43%
Inc Ransom	1.43%
Killsec	1.43%
Lynx	2.86%
Play	14.29%
Qilin	10.00%
RansomHub	17.14%
Rhysida	4.29%
Trinity	1.43%

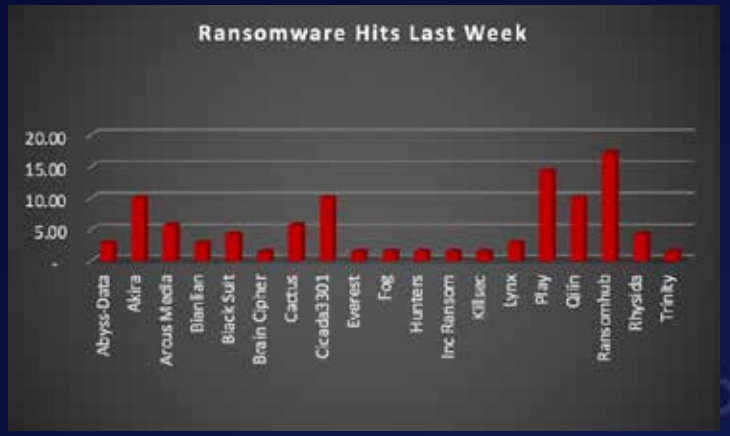

Figure 1: Ransomware Group Hits Last Week

Rhysida Ransomware

Emerging in the latter half of 2022, Fog 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 aren't met. While the exact origins of Fog 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 Fog a particularly dangerous adversary.

TTPs:

Rhysida ransomware, a formidable adversary in the cybercrime landscape, first emerged in late 2022. 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 Rhysida 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 Rhysida a particularly dangerous threat.

- **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**: Rhysida 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, Rhysida 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**: Rhysida 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, Rhysida 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, Rhysida 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: Rhysida 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 Fog Ransomware

Ransom Note

Rhysida ransomware, a notorious cyber threat, employs a deceptive tactic in its ransom notes. Rather than demanding a ransom outright, it presents itself as a "CriticalBreachDetected.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'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.

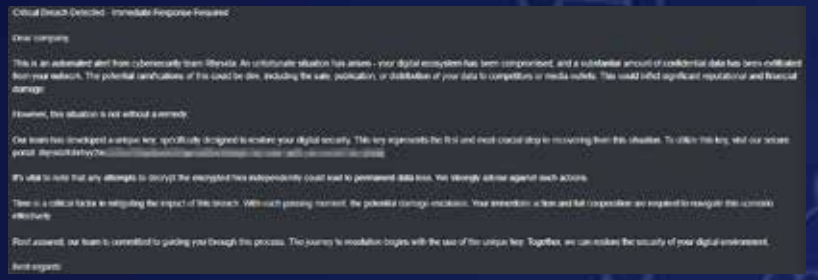

Figure 3: Screenshot of Ransom Note used by Rhysida Ransomware

A Global Reach with Focused Targets

Rhysida 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 Rhysida, 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 financial losses.

The emergence of Rhysida 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	T1133	External Remote Services
Persistence	T1053.005	Scheduled Task/Job: Scheduled Task
Defence Evasion	T1070.004 T1222.002	Indicator Removal: File Deletion File and Directory Permissions Modification
Discovery	T1083 T1082	File and Directory Discovery System Information Discovery
Impact	T1486	Data Encrypted for Impact

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxp://rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7cad.onion/ hxxp://rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7cad.onion/archive.php hxxp://rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7cad.onion/archive.php?auction hxxp://rhysidafc6lm7qa2mkiukbezh7zuth3i4wof4mh2audkymscjm6yegad.onion/	URLs (Onion)	Leak Site
69b3d913a3967153d1e91ba1a31ebed839b297ed 338d4f4ec714359d589918cee1adad12ef231907 b07f6a5f61834a57304ad4d885bd37d8e1badba8 39649fa040a3c6894758016a65afec7b6acd4017 4947cf015875b169b6509a279941e854b022dd8e c27a865b3ab1f0bd2ea1e8f7298b5ef9348c5ac 96dc78c00a622c3df5e038b8ed41b2de68e6c350 df96143540d36edf1b9d9d25d91778855cafa8a6 a1034cdc499b4c551e43bc259d10928d75293214 de52c40ca449c7285660541c84ac5d6fe78a6bff e14ee9ad241517ef72a4c6561fb848f6d659e764	Hash	Malicious Files

A recent analysis of ransomware victims across 17 countries reveals the United States as the most heavily impacted nation, with a staggering 57% increase in victim reports over the past week. Notably, Canada has also experienced a significant rise once again, with victim reports 9% of 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 (%)
Argentina	1.43%
Australia	1.43%
Belgium	1.43%
Brazil	5.71%
Canada	8.57%
Denmark	1.43%
France	1.43%
Germany	2.86%
Greece	1.43%
Japan	2.86%
Poland	1.43%
Portugal	1.43%
Spain	1.43%
Sweden	2.86%
Turkey	1.43%
UK	5.71%
USA	57.14%

Figure 4: Ransomware Victims Worldwide

Further analysis reveals that ransomware has impacted 20 industries worldwide. The manufacturing sector remains a significant target, accounting for 13% of victims in the past week Retail and Business Services sectors got 11% of victims each in the past week.

Industry	Victims Count (%)
Agriculture	2.86%
Business Services	11.43%
Construction	10.00%
Consumer Services	4.29%
Education	4.29%
Energy, Utilities & Waste Treatment	1.43%
Finance	4.29%
Government	2.86%
Healthcare	5.71%
Hospitality	4.29%
Insurance	1.43%
IT	1.43%
Legal Services	5.71%
Manufacturing	12.86%
Media & Internet	2.86%
Metals & Mining	2.86%
Organisations	2.86%
Real Estate	1.43%
Retail	11.43%
Transportation	5.71%

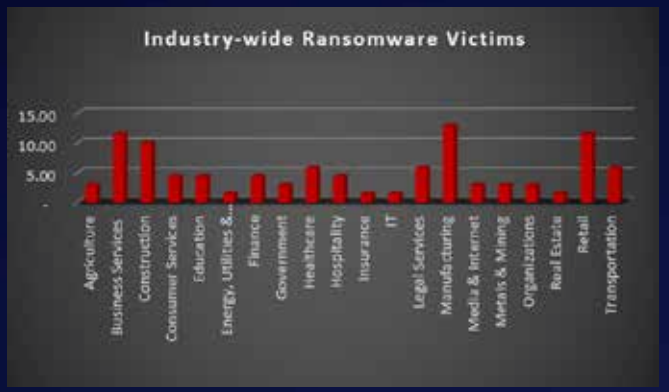

Figure 5: Industry-wide Ransomware Victims

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.