Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Aug 13 - 19, 2024

Report Summary:

- **New Threat Detection Added** – 2 (Oyster Backdoor and Sidewinder APT)
- **New Threat Protections - 91**

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

1. Oyster Backdoor

Oyster is a relatively new backdoor malware that emerged in 2023. Initially delivered through a loader called Broomstick, it has evolved to be deployed directly. This malware is capable of data exfiltration, remote code execution, and persistent system control. Associated with the Russia-linked ITG23 group, Oyster has been observed in malvertising campaigns, where it is disguised as popular software installers. Its modular structure and ability to evade detection make it a growing threat to individuals and organisations.

Threats Protected: 16
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	Link function
	T1059	Command and Scripting Interpreter
Persistence	T1574.002	DLL Side Loading
Privilege Escalation	T1574	Hijack Execution Flow
	T1574.002	DLL Side Loading
Defence Evasion	T1027	Obfuscated Files or Information
	T1562.001	Disable or Modify Tools
Credential Access	T1003	OS Credentials Dumping
	T1539	Steal Web Session Cookie
	T1552	Unsecured Credentials
Discovery	T1010	Application Window Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1497	Virtualization/Sandbox Evasion
Collection	T1005	Data from the Local System
Command-and-Control	T1071	Application Layer Protocol
	T1573	Encrypted Channel

2. Sidewinder APT

Sidewinder APT, also known as Razor Tiger, Rattlesnake, or T-APT-04, is a persistent threat actor believed to originate from India. Active since 2012, they have targeted government, military, and business entities primarily in South Asia. Sidewinder's arsenal includes spear-phishing, document exploitation, and DLL side-loading to deliver malicious payloads. Their recent shift to server-side polymorphism to obfuscate their attacks highlights their adaptability. While primarily focused on espionage, the group's tactics pose a significant threat to various sectors.

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	T1059	Command and Scripting Interpreter
Persistence	T1547	Boot or Logon AutoStart Execution
	T1547.009	Shortcut Modification
	T1574.002	DLL Side Loading
Privilege Escalation	T1547	Boot or Logon AutoStart Execution
	T1547.009	Shortcut Modification
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
	T1056.001	Keylogging
	T1115	Clipboard Data
Command-and-Control	T1071	Application Layer Protocol

Known exploited vulnerabilities (Week 3 August 2024):

Vulnerability	CVSS	Description
CVE-2024-38107	7.8 (High)	Microsoft Windows Power Dependency Coordinator Privilege Escalation Vulnerability
CVE-2024-38106	7.0 (High)	Microsoft Windows Kernel Privilege Escalation Vulnerability
CVE-2024-38193	7.8 (High)	Microsoft Windows Ancillary Function Driver for WinSock Privilege Escalation Vulnerability
CVE-2024-38213	6.5 (Medium)	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability
CVE-2024-38178	7.5 (High)	Microsoft Windows Scripting Engine Memory Corruption Vulnerability
CVE-2024-38189	8.8 (High)	Microsoft Project Remote Code Execution Vulnerability
CVE-2024-28986	9.8 (Critical)	SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-august-2024/499

Updated Malware Signatures (Week 3 August 2024)

Threat	Description
HawkEye	A trojan and keylogger used to steal various account credentials
Nanocore	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.
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.
Remcos	Remcos functions as a remote access trojan (RAT), granting unauthorised individuals the ability to issue commands on the compromised host, record keystrokes, engage with the host's webcam, and take snapshots. Typically, this malicious software is distributed through Microsoft Office documents containing macros, which are often attached to malicious emails.

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 20 industries spanning 26 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

Hunters ransomware group stands out as the most prolific, having updated a significant number of victims (15%) distributed across multiple countries. In comparison, LockBit3.0 ransomware updated 14% 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	0.78%
Akira	0.78%
Bianlian	5.43%
Black Suit	0.78%
Brain Cipher	0.78%
Cicada3301	1.55%
Ciphbit	0.78%
Dan0N	1.55%
Darkvault	2.33%
Dispossessor	1.55%
Everest	0.78%
Fog	0.78%
Handala	0.78%
Helldown	6.98%
Hunters	15.50%
Inc Ransom	0.78%
Killsec	0.78%
Lockbit3	13.95%
Lynx	6.20%
Meow	5.43%
Metaencryptor	0.78%
Mydata	0.78%
Play	6.20%
Qilin	4.65%
Ransomexx	0.78%
Ransomhouse	1.55%
Ransomhub	11.63%
Rhysida	4.65%
Trinity	0.78%

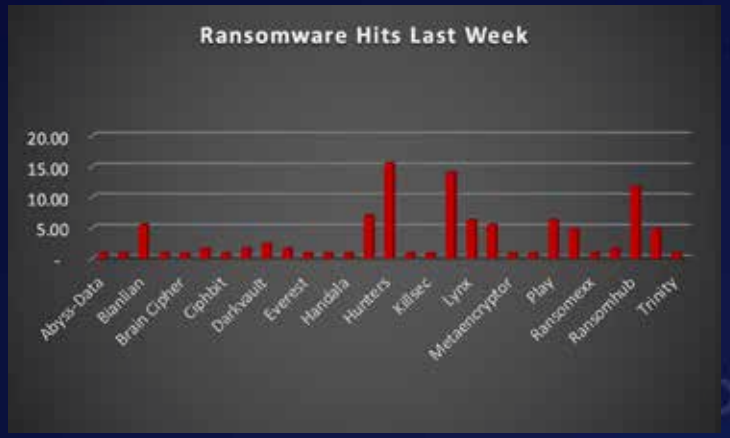

Figure 1: Ransomware Group Hits Last Week

Helldown Ransomware

Emerging in the early months of 2023, Helldown ransomware rapidly established itself as a formidable threat in the cybercrime landscape. This malicious software employs a double extortion tactic, encrypting victims' data and threatening to leak it on the dark web unless a ransom is paid. While the exact origins of Helldown 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 Helldown a particularly dangerous adversary.

TTPs:

Helldown ransomware doesn't rely solely on brute force. It possesses a diverse arsenal of tactics, techniques, and procedures (TTPs) to infiltrate and compromise systems. 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 Vulnerabilities: Helldown 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, Helldown 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: Helldown 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, Helldown 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, Helldown 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: Helldown 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.

Ransom Note

```
ATTENTION!

Don't worry, you can return all your files!
All your files like pictures, databases, documents and other important are encrypted with strongest encrypti
unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
hxxps://we.tl/t-1j5qINGbTc
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.


To get this software you need write on our e-mail:
support@fishmail.top

Reserve e-mail address to contact us:
datarestorehelp@airmail.cc
```

A Global Reach with Focused Targets

Helldown 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 Helldown, 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 Helldown 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. Here are some crucial steps organisations can take to mitigate the risk of Helldown 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 RansomHouse 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.

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxp://onyxcgfg4pjevvp5h34zvhaj45kbft3dg5r33j5vu3nyp7xic3vrzvad.onion/	URLs (Onion)	Leak Site

In a comprehensive analysis of ransomware victims across 26 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 60% of 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	1.55%
Brazil	0.78%
Canada	5.43%
China	1.55%
Cyprus	0.78%
Czech Republic	0.78%
Denmark	1.55%
France	0.78%
Germany	0.78%
India	2.33%
Italy	2.33%
Japan	2.33%
Mexico	0.78%
Netherlands	0.78%
New Zealand	0.78%
Peru	1.55%
Poland	2.33%
Portugal	0.78%
Romania	0.78%
South Africa	3.10%
Spain	2.33%
Sweden	0.78%
Turkey	0.78%
UK	3.88%
Ukraine	0.78%
USA	59.69%

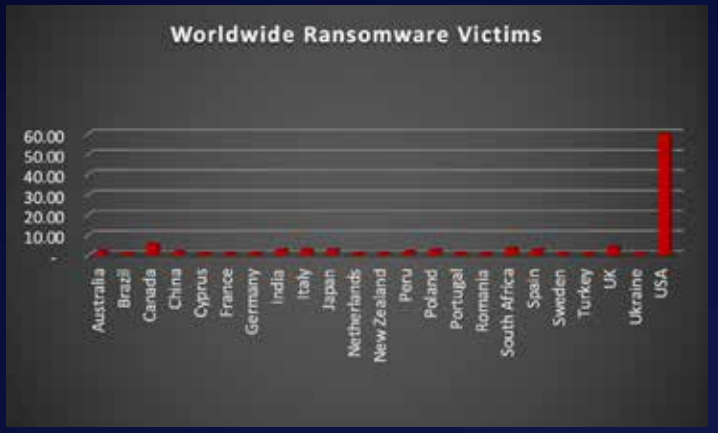

Figure 4: Ransomware Victims Worldwide

Upon further investigation, it has been identified that ransomware has left its mark on 20 different industries worldwide. Notably, Manufacturing bore the brunt of the attacks in the past week, accounting for 19% of victims each.

Industry	Victims Count (%)
Business Services	10.85%
Construction	11.63%
Consumer Services	2.33%
Education	2.33%
Energy, Utilities & Waste Treatment	0.78%
Finance	6.98%
Government	2.33%
Healthcare	8.53%
Hospitality	3.88%
Insurance	1.55%
IT	2.33%
Legal Services	2.33%
Manufacturing	19.38%
Media & Internet	1.55%
Metals & Mining	3.10%
Organisations	1.55%
Real Estate	1.55%
Retail	11.63%
Telecom	2.33%
Transportation	3.10%

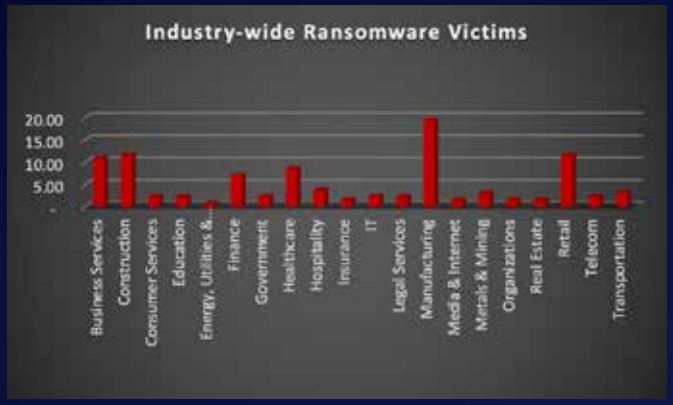

Figure 5: Industry-wide Ransomware Victims