Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Oct 1 - 7, 2024

Report Summary:

- **New Threat Detection Added** – 2 (S400 RAT Malware and Cosa Nostra Botnet)
- **New Threat Protections - 232**

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

1. S400 RAT Malware

S400 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. S400'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 S400 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
Initial Access	T1091	Replication Through Removable Media
Execution	T1106	Native API
Persistence	T1542 T1542.003	Pre-OS Boot Boot kit
Privilege Escalation	T1055	Process Injection
Defence Evasion	T1027 T1027.002 T1055	Obfuscated Files or Information Software Packing Process Injection
Credential Access	T1056	Input Capture
Discovery	T1082 T1083	System Information Discovery Files and Directory Discovery
Lateral Movement	T1091	Replication Through Removable Media
Collection	T1056 T1560	Input Capture Archive Collected Data

2. Cosa Nostra Botnet

Cosa Nostra v.1.2 is a sophisticated HTTP botnet capable of orchestrating large-scale distributed attacks. This botnet leverages compromised devices as zombie nodes to execute malicious actions under the control of a central Command-and-Control (C2) server. Cosa Nostra v.1.2 can be used for various attacks, including denial-of-service (DoS), spam campaigns, and malware distribution. Its ability to evade detection and operate discreetly makes it a significant threat 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	T1047	Windows Management Instrumentation
Persistence	T1547 T1547.001	Boot or Logon Autostart Execution Registry Run Keys / Startup Folder
Privilege Escalation	T1055 T1134	Process Injection Access Token Manipulation
Defence Evasion	T1027 T1027.002 T1036 T1055	Obfuscated Files or Information Software Packing Masquerading Process Injection
Discovery	T1010 T1012 T1016 T1018	Application Window Discovery Query Registry System Network Configuration Discovery Remote System Discovery
Command-and-Control	T1071 T1095	Application Layer Protocol Non-Application Layer Protocol

Known exploited vulnerabilities (Week 1 October 2024):

Vulnerability	CVSS	Description
CVE-2019-0344	9.8 (Critical)	SAP Commerce Cloud Deserialization of Untrusted Data Vulnerability
CVE-2021-4043	5.5 (Medium)	Motion Spell GPAC Null Pointer Dereference Vulnerability
CVE-2020-15415	9.8 (Critical)	DrayTek Multiple Vigor Routers OS Command Injection Vulnerability
CVE-2023-25280	9.8 (Critical)	D-Link DIR-820 Router OS Command Injection Vulnerability
CVE-2024-29824	8.8 (High)	Ivanti Endpoint Manager (EPM) SQL Injection Vulnerability
CVE-2024-45519	9.8 (Critical)	Synacor Zimbra Collaboration Command Execution Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-october-2024/509

Updated Malware Signatures (Week 1 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 19 industries in 26 countries. This highlights the pervasive nature of ransomware, demonstrating its ability to target organisations of all sizes and sectors worldwide.

El Dorado ransomware group has claimed 15% of victims this week. This surge solidifies its position as the ransomware group with the highest number of victims reported this week. LockBit3.0 ransomware updated its victim count by 9% 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	3.05%
Akira	6.11%
Black Suit	0.76%
Blackbyte	0.76%
Blackout	0.76%
Cactus	4.58%
Cicada3301	0.76%
Ciphbit	0.76%
Cloak	1.53%
Clop	0.76%
El Dorado	14.50%
Embargo	0.76%
Handala	1.53%
Hunters	1.53%
Inc Ransom	3.05%
Killsec	4.58%
Lockbit3	9.16%
Mad Liberator	0.76%
Medusa	7.63%
Meow	6.11%
Nitrogen	6.87%
Play	8.40%
Qilin	3.82%
RansomHub	7.63%
Rhysida	0.76%
Stormous	1.53%
Trinity	1.53%

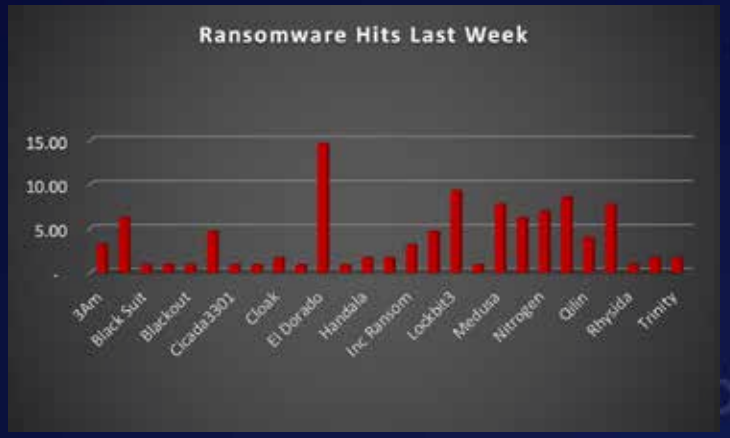

Figure 1: Ransomware Group Hits Last Week

Clop Ransomware

Clop ransomware, a formidable threat in the cybercrime landscape, 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 Clop 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 Clop a particularly dangerous adversary.

TTPs:

Clop 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**: Clop 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, Clop 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**: Clop 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, Clop 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, Clop 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: Clop 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.

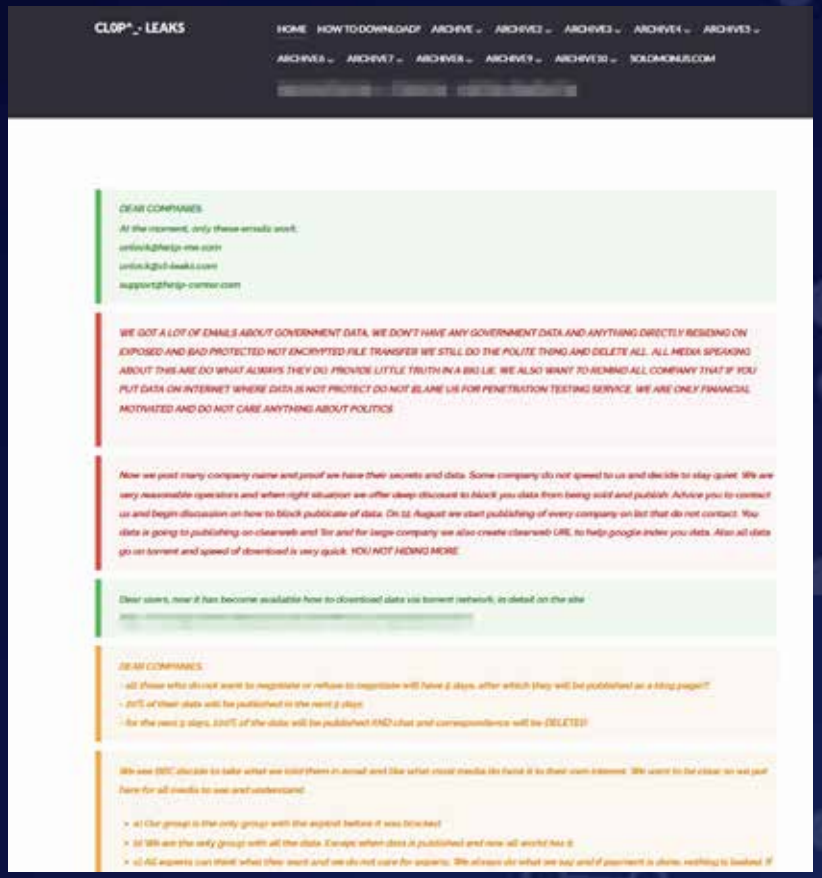

Figure 2: Screenshot of Leak Site used by Clop Ransomware

Ransom Note

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

A Global Reach with Focused Targets

Clop 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 Clop, 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 Clop 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 26 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 of 8% 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 (%)
Afghanistan	0.76%
Australia	1.53%
Belgium	0.76%
Brazil	3.82%
Canada	8.40%
Colombia	0.76%
Costa Rica	0.76%
Czech Republic	0.76%
France	2.29%
Germany	2.29%
India	2.29%
Israel	2.29%
Italy	0.76%
Lebanon	0.76%
Mexico	1.53%
Montana	0.76%
Netherlands	0.76%
Norway	1.53%
Philippines	0.76%
Singapore	1.53%
South Korea	0.76%
Spain	0.76%
Sweden	0.76%
UAE	0.76%
UK	4.58%
USA	57.25%

Figure 4: Ransomware Victims Worldwide

Further analysis reveals that ransomware has impacted 19 industries worldwide. The manufacturing sector remains a significant target, accounting for 22% of victims in the past week Retail and Business Services sectors got 12% of victims each in the past week.

Industry	Victims Count (%)
Business Services	14.50%
Construction	0.76%
Consumer Services	11.45%
Education	5.34%
Energy, Utilities & Waste Treatment	0.76%
Finance	1.53%
Government	3.82%
Healthcare	1.53%
Hospitality	6.11%
Insurance	5.34%
IT	3.05%
Legal Services	4.58%
Manufacturing	17.56%
Media & Internet	1.53%
Metals & Mining	5.34%
Organisations	2.29%
Real Estate	12.21%
Retail	1.53%
Transportation	0.76%

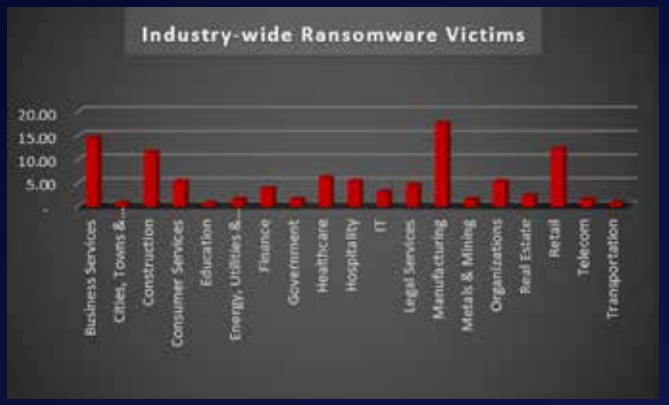

Figure 5: Industry-wide Ransomware Victims

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.

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
hxxp://ekbgzchl6x2ias37.onion hxxp://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad.onion/ hxxp://3ws3t4uo7fehnn4qpmadk3zjrxta5xlt3gsc5mx4sztrsy7ficuz5ayd.onion/ hxxp://amnwxasjtjc6e42siac6t45mhbkgtycrx5krv7sf5festvqxmnchuayd.onion/ hxxp://qahjimrublt35jlv4teesicrw6zhpwhkb6nhtonwxuqafmjhr7hax2id.onion/	URLs (Onion)	Leak Site
0b3220b11698b1436d1d866ac07cc90018e59884e91a8cb71ef8924309f1e0e9 0ea05169d111415903a1098110c34cdbbd390c23016cd4e179dd9ef507104495 110e301d3b5019177728010202c8096824829c0b11bb0dc0bff55547ead18286 1826268249e1ea58275328102a5a8d158d36b4fd312009e4a2526f0bfbc30de2 2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5 2ccf7e42afd3f6bf845865c74b2e01e2046e541bb633d037b05bd1cdb296fa59 348e435196dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d 387cee566aedbafa8c114ed1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a 38e69f4a6d2e81f28ed2dc6df0daf31e73ea365bd2cfc90ebc31441404cca264 3a977446ed70b02864ef8cfa3135d8b134c93ef868a4cc0aa5d3c2a74545725b 3ab73ea9aebf271e5f3ed701286701d0be688bf7ad4fb276cb4fbe35c8af8409	Hash	Malicious Files
http://hiperfdhaus[.]com http://jirostrogud[.]com http://qweastradoc[.]com http://qweastradoc[.]com/gate.php http://connectzoomdownload[.]com/download/ZoomInstaller.exe https://connectzoomdownload[.]com/download/ZoomInstaller.exe http://zoom[.]voyage/download/Zoom.exe http://guerdofest[.]com/gate.php http://zoom[.]voyage/download/Zoom.exe http://guerdofest[.]com/gate.php	Malicious Domain	C&C
unlock@rsv-box[.]com unlock@support-mult[.]com rey14000707@gmail[.]com gagnondani225@gmail[.]com	Email Address	CL0P communication email CL0P communication email Login/Download Email