Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Oct 15 - 21, 2024

Report Summary:

- **New Threat Detection Added** – 2 (Ivanti Cloud Services Appliance CVE-2024-8190 and Lumma Stealer)
- **New Threat Protections - 84**

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

1. Ivanti Cloud Services Appliance CVE-2024-8190

Nation-state adversaries exploited zero-day vulnerabilities in Ivanti Cloud Services Appliance (CSA), chaining multiple exploits. A publicly unknown path traversal vulnerability on the resource /client/index.php (CVE-2024-8963, disclosed September 19) allowed unauthorised access to other resources like users.php and reports.php. Additionally, a command injection vulnerability on reports.php (CVE-2024-9380, disclosed October 8) enabled remote command execution. These vulnerabilities allowed attackers to bypass security, gaining control of compromised systems.

Threats Protected: 01
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Reject	Drop
Connectivity	Alert	Alert
OT	Reject	Drop

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059	Command and Scripting Interpreter
Privilege Escalation	T1055	Process Injection
Defence Evasion	T1210	Exploitation of Remote Services
Credential Access	T1078	Valid Accounts
Impact	T1499	Endpoint Denial of Service

2. Lumma Stealer

Lumma Stealer is a sophisticated malware that exploits fake CAPTCHA pages to distribute itself, targeting Windows users. The malware is distributed via phishing sites that trick victims into executing malicious PowerShell commands. Lumma Stealer steals sensitive data like credentials, financial information, and personal files. It leverages various CDN platforms for delivery and evades detection using base64 encoding and clipboard manipulation. This malware is dangerous due to its stealth tactics and the growing trend of fake CAPTCHA attacks.

Threats Protected: 48
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	T1566.002	Spear Phishing Link
Execution	T1059.001	PowerShell
Defence Evasion	T1027	Obfuscated Files or Information
Credential Access	T1115	Clipboard Data
Collection	T1056	Input Capture
Command-and-Control	T1071.001	Web Protocols

Known exploited vulnerabilities (Week 3 October 2024):

Vulnerability	CVSS	Description
CVE-2024-28987	9.1 (Critical)	SolarWinds Web Help Desk Hardcoded Credential Vulnerability
CVE-2024-9680	9.8 (Critical)	Mozilla Firefox Use-After-Free Vulnerability
CVE-2024-30088	7.0 (High)	Microsoft Windows Kernel TOCTOU Race Condition Vulnerability
CVE-2024-40711	9.8 (Critical)	Veeam Backup and Replication Deserialization Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-october-2024/513

Updated Malware Signatures (Week 3 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 and closely monitors the dark web and other sources to track ransomware activities globally. In the past week alone, we have uncovered new ransomware victims and updates on existing cases across 19 industries and 11 countries.

This surge underscores the pervasive and growing reach of ransomware, affecting organisations of all sizes and sectors, from healthcare to manufacturing. These findings highlight the evolving nature of ransomware, posing significant operational and financial risks to businesses in diverse regions globally.

Name of Ransomware Group	Percentage of new Victims last week
RansomHub	33.33%
Cicada3301	12.82%
Meow	7.69%
Play	7.69%
Cactus	7.69%
Sarcoma	5.13%
Hunters	5.13%
Killsec	5.13%
Black suit	2.56%
Interlock	2.56%
Lynx	2.56%
Rhysida	2.56%
Fog	2.56%
Everest	2.56%

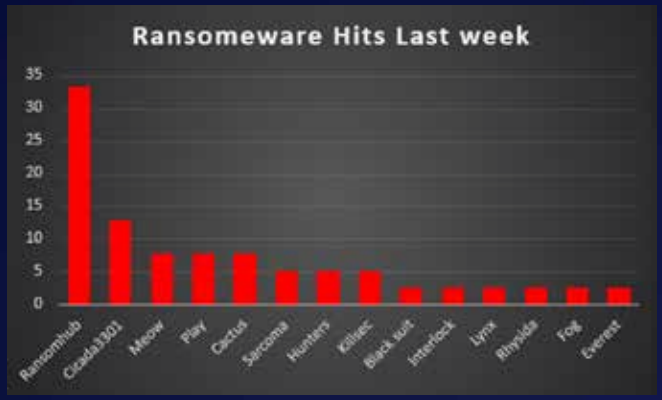

Figure 1: Ransomware Group Hits Last Week

Killsec Ransomware

Killsec ransomware, first identified in October 2023, has quickly gained notoriety for targeting critical industries such as government, finance, and manufacturing. Employing a hybrid extortion model, Killsec not only encrypts data but also defaces websites to further pressure victims. Its ransom demands typically range from €1,500 to $25,000. The ransomware group is notorious for leveraging phishing, exploiting Remote Desktop Protocol (RDP) weaknesses, and utilising double extortion to steal sensitive data before encryption.

Killsec's rise demonstrates the ever-evolving nature of ransomware, emphasising the need for comprehensive cybersecurity strategies, including patch management, regular security audits, and training to identify phishing attacks. By combining traditional encryption-based extortion with new methods such as website defacement, Killsec presents a formidable challenge to modern organisations.

Detailed TTPs:

1. **Command-and-Control (C2)**: Killsec uses encrypted communication channels to maintain stealth. They often communicate via command-and-control servers, which coordinate attacks and issue commands to deploy malware within victims' systems.
2. **Lateral Movement**: Once they gain access through RDP exploitation, Killsec deploys tools such as PowerShell scripts to move laterally across the network, enabling them to compromise additional systems and escalate privileges.
3. **Credential Dumping**: Post-compromise, Killsec frequently engages in credential dumping to harvest login credentials, gaining higher-level access to more critical systems.
4. **Process Injection**: To evade detection, Killsec often injects malicious code into legitimate system processes. This tactic helps them avoid endpoint detection systems while maintaining persistence on the network.
5. **Advanced Encryption**: Killsec leverages robust encryption techniques, making decryption nearly impossible without their private key. The ransomware uses sophisticated algorithms, locking out victims from accessing crucial data unless they pay the ransom.

Data Leak Site: Killsec ransomware operates a data leak site on the dark web where they expose victims who refuse to meet ransom demands. This site lists compromised organisations, leveraging public shaming as an additional extortion tactic. By making sensitive data public, Killsec increases the pressure on victims to pay the ransom to avoid further reputational damage and data exposure. This aggressive approach mirrors the tactics of other ransomware groups, emphasising Killsec's commitment to exploiting both the financial and reputational vulnerabilities of its victims.

Figure 2: Screenshot of Leak Site used by Killsec Ransomware

Extortion Demands and Victim Profiles

Killsec typically demands ransoms ranging from €1,500 to $25,000, depending on the size of the organisation and the value of the compromised data. Industries such as government, banking, and manufacturing have been primary targets, with confirmed cases in the United States, Romania, and India.

Targeted Sectors and Countries:

- **Sectors**: Killsec targets various sectors, but especially government, finance, and manufacturing industries.
- **Countries**: Notable attacks have been identified in the U.S., Romania, India, and Bangladesh.

Known Victims and Impact:

- **Government Institutions**: A primary target, Killsec disrupts operations by encrypting sensitive data and threatening to leak classified information.
- **Banking Sector**: Financial institutions face heavy extortion demands, risking the exposure of client data and financial losses.
- **Manufacturing**: By encrypting critical systems, Killsec has caused operational disruptions and significant production downtime.

The emergence of Killsec ransomware underscores the evolving complexity of ransomware attacks, focusing on double extortion, website defacement, and exploiting weak security configurations in critical sectors. Below is the Kill Chain for Killsec, detailing its attack stages:

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566 T1190	Phishing Exploit Public-Facing Application
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
Persistence	T1053.003	Server Software Component: Web Shell
Privilege Escalation	T1068	Exploitation for Privilege Escalation
Defence Evasion	T1055 T1574.002	Process Injection 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 11 countries shows the United States as the most affected, accounting for 55.26% of incidents reported last week. Canada follows with 13.16%, while countries like Japan, Australia, and India each experienced 5.26% of new attacks. Nations like Bangladesh, Israel, Ghana, Malaysia, the United Kingdom, and Romania recorded 2.63% each. This data highlights the global impact of ransomware, with the United States being disproportionately affected.

Industry	Victims Count (%)
Japan	5.26%
Bangladesh	2.63%
Israel	2.63%
United States	55.26%
Ghana	2.63%
Canada	13.16%
Australia	5.26%
Malaysia	2.63%
India	5.26%
United Kingdom	2.63%
Romania	2.63%

Figure 3: Ransomware Victims Worldwide

Further analysis of ransomware victims across 19 industries reveals that Manufacturing remains a significant target, accounting for 13.16% of all victims in the past week. Business Services follows closely, making up 15.79% of attacks. Sectors such as Hospitality, Healthcare, and Holding Companies each recorded 7.89% of incidents. Other impacted industries include Software, Construction, and Education, each experiencing 5.26%. This highlights the wide range of industries vulnerable to ransomware attacks, emphasising the need for robust cybersecurity across all sectors.

Industry	Victims Count (%)
Hospitality	7.89%
Holding Companies	7.89%
Manufacturing	13.16%
Business Services	15.79%
Telecommunications	2.63%
Oil	2.63%
Healthcare	7.89%
Advertising & Marketing	2.63%
Retail	2.63%
Legal Service	2.63%
Software	5.26%
Food & Beverage	2.63%
Legal Services	2.63%
Construction	5.26%
Education	5.26%
Real Estate	2.63%
Pharmacies	2.63%
Minerals & Mining	5.26%
Consumer Services	2.63%

Figure 4: Industry-wide Ransomware Victims

Here are some crucial steps organisations can take to mitigate the risk of **Killsec ransomware** and similar threats:

- **Third-Party Risk Management**: Implement a robust third-party risk management program to continuously assess and monitor the security posture of vendors and partners. Many ransomware attacks, including Killsec, target vulnerabilities in the supply chain.
- **Website Security and Monitoring**: Given Killsec's tendency to deface websites, ensure regular monitoring of web assets, implement strong web application firewalls (WAF), and conduct regular penetration testing to detect vulnerabilities in public-facing websites.
- **Regular Backups and Data Recovery Plans**: Maintain encrypted, offline backups of all critical data to enable quick recovery in case of a ransomware attack. These backups should be regularly tested for integrity to ensure they can be used for restoration if needed.
- **Patch Management and Vulnerability Scanning**: Conduct continuous vulnerability assessments and patch known vulnerabilities in software and operating systems promptly. Killsec, like other ransomware, exploits outdated or unpatched systems to gain access.
- **Security Awareness Training**: Train employees on recognising phishing attacks, one of Killsec's primary attack vectors. Focus on the importance of avoiding suspicious links and attachments, and conduct regular phishing simulations to enhance employee awareness.
- **Endpoint Detection and Response (EDR)**: Deploy EDR solutions that can detect and respond to malicious activity at the endpoint level. Ensure that EDR solutions are configured to monitor and prevent process injection and other advanced tactics used by Killsec.
- **Network Segmentation and Least Privilege Access**: Segregate critical parts of the network from the rest of the organisation. Implement least privilege access to ensure that users and systems have the minimum access needed to perform their functions, limiting the lateral movement of ransomware.
- **Incident Response and Business Continuity Planning**: Develop and regularly test a detailed incident response plan to contain and respond to ransomware attacks like Killsec. Ensure that key stakeholders know their roles and that critical systems can be restored quickly to minimise downtime.