Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Oct 29 - Nov 04, 2024

Report Summary:

- **New Threat Detection Added** – 2 (Ivanti CSA Zero-Day Exploitation and BugSleep Remote Access Tool (RAT))
- **New Threat Protections - 137**

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

1. Ivanti CSA Zero-Day Exploitation

Advanced threat actors have exploited multiple zero-day vulnerabilities in Ivanti's Cloud Services Appliance (CSA), including CVE-2024-8190, CVE-2024-8963, and CVE-2024-9380. These vulnerabilities allow attackers to perform unauthorised actions such as path traversal and command injection, leading to potential system compromise. The exploitation of these flaws underscores the importance of timely patching and robust security measures.

Threats Protected: 01
Rule Set Type:

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

Class Type: Attempted-admin

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Defence Evasion	T1210	Exploitation of Remote Services
Impact	T1499	Endpoint Denial of Service

2. BugSleep Remote Access Tool (RAT)

BugSleep is a sophisticated Remote Access Tool (RAT) that provides attackers with reverse shell capabilities and file input/output operations on compromised endpoints. It employs a custom Command-and-Control (C2) protocol over plain TCP sockets, utilizing a pseudo-Type Length Value (TLV) structure for communication. The malware encrypts payloads by subtracting a static value from each byte, enhancing its stealth. BugSleep's functionalities include reverse shell access, file manipulation, and persistence mechanisms, posing significant risks to affected systems.

Threats Protected: 02
Rule Set Type:

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

Class Type: Attempted-admin

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059.001	PowerShell
Persistence	T1547.001	Registry Run Keys / Startup Folder
Privilege Escalation	T1055	Process Injection
Defence Evasion	T1027	Obfuscated Files or Information
Credential Access	T1056	Input Capture
Command-and-Control	T1071.001	Web Protocols

Known exploited vulnerabilities (Week 5 October 2024):

Vulnerability	CVSS	Description
CVE-2024-51567	10.0 (Critical)	CyberPanel pre-auth remote code execution vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-5th-week-of-october-2024/519

Updated Malware Signatures (Week 5 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, we uncovered numerous ransomware incidents across various groups, highlighting the ongoing and pervasive nature of these cyber threats. Below is the breakdown of ransomware group activities for this period.

Ransomware Groups and Attack Coverage:

Name of Ransomware Group	Overall Percentage of total attack coverage
Play	12.26%
BlackSuit	3.77%
Meow	3.77%
Interlock	1.89%
Donut Leaks	1.89%
Bianlian	1.89%
RA Group	1.89%
RansomHub	12.26%
Brain Cipher	3.77%
Killsec	9.43%
RansomHouse	2.83%
El Dorado	2.83%
Playboy	2.83%
Fog	5.66%
Lynx	0.94%
Handala	1.89%
Arcus	0.94%
Abyss-data	0.94%
Eraleign (APT73)	2.83%
Sarcoma	2.83%
Cactus	0.94%
3AM	5.66%
Qilin	10.38%
Everest	5.66%

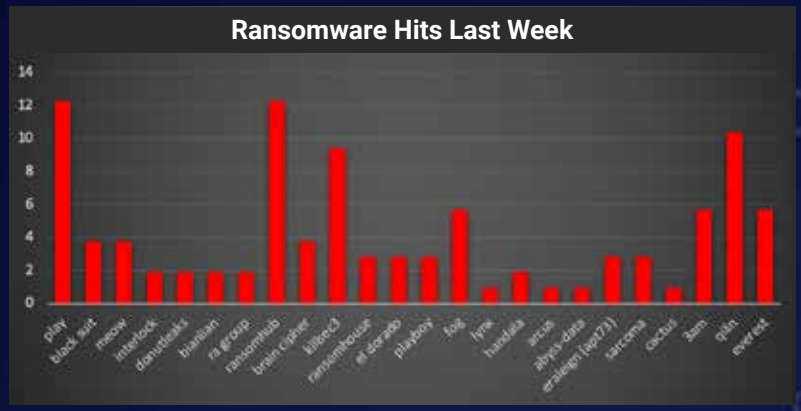

Figure 1: Ransomware Group Hits Last Week

Play Ransomware Analysis

Play ransomware, emerging as one of the most active threat actors with 12.26% of total attacks in our recent analysis, has gained significant attention due to its collaboration with North Korean state-sponsored actors. This partnership marks a concerning evolution in ransomware operations, blending cybercrime with state-sponsored capabilities.

Play Ransomware: North Korean State Actor Connections
Key Connection Points

1. Infrastructure Overlap
   - Shared Command-and-Control (C2) infrastructure with North Korean APT groups
   - Common IP addresses used in attacks (68.235.184[.]54)
   - Identical server configurations and malware deployment patterns
2. Technical Similarities
   - Use of Tactics, Techniques, and Procedures (TTPs) similar to UNC4899
   - Deployment of DPRK-linked malware alongside Play ransomware
   - Common exploitation of vulnerabilities like ProxyNotShell and OWASSRF
3. Attack Pattern Correlations
   - Coordinated targeting healthcare organisations
   - Similar victim selection methodology
   - Synchronised timing of attacks

Detailed TTPs for Play Ransomware with North Korean Connection

1. Initial Access and Exploitation:
   - Exploits Microsoft Exchange vulnerabilities (ProxyNotShell and OWASSRF)
   - Exploits specifically CVE-2022-41082 and CVE-2022-41040
   - Targets healthcare sector organisations predominantly
   - Deploys web shells for persistent access
2. Infrastructure and Operations:
   - Shares C2 infrastructure with IP address 68.235.184[.]54
   - Connects with UNC4899 operations
   - Maintains common Command-and-Control servers
   - Deploys shared malware infrastructure
3. Post-Exploitation Activities:
   - Deploys Cobalt Strike beacons for network control
   - Executes PowerShell commands for system manipulation
   - Implements BitLocker encryption for data impact
   - Performs Volume Shadow Copy Deletion
4. Lateral Movement and Persistence:
   - Modifies Windows Registry for persistence
   - Creates scheduled tasks for maintained access
   - Installs malicious services
   - Abuses admin shares for movement
5. Data Impact and Encryption:
   - Uses BitLocker Drive Encryption for file encryption
   - Targets system backups systematically
   - Deletes volume shadow copies
   - Implements secure data destruction methods
6. Tool Deployment and Usage:
   - Deploys custom web shells for access
   - Uses sophisticated PowerShell scripts
   - Implements Remote Administration Tools
   - Employs shared North Korean malware variants
7. Strategic Operations:
   - Coordinates synchronised attack timing
   - Shares attack infrastructure with DPRK actors
   - Focuses on the healthcare sector targeting
   - Implements common exploitation techniques
8. Command-and-Control:
   - Uses shared hosting providers
   - Maintains overlapping C2 servers with DPRK operations
   - Implements sophisticated proxy mechanisms
   - Deploys coordinated control infrastructure

Figure 2: Screenshot of Leak Site used by Play

Key Characteristics:

- Emergence: Gained prominence in 2022, showing significant evolution in capabilities and reach
- Infrastructure: Maintains sophisticated infrastructure including leak sites and C2 servers
- Partnership Model: Unique collaboration with state-sponsored actors, particularly North Korean APT groups
- Technical Sophistication: Advanced encryption and evasion capabilities

Modus Operandi:

- Target Selection:
  - Focus on high-value organisations
  - Strategic targeting of critical infrastructure
  - Preference for organizations with cyber insurance
- Attack Methodology:
  - Sophisticated initial access techniques
  - Advanced lateral movement capabilities
  - Implementation of multiple pressure points for ransom payment
- Extortion Tactics:
  - Multi-layered extortion approach
  - Sophisticated negotiation strategies
  - Strategic data leakage for maximum impact

Technical Observations:

- Malware Characteristics:
  - Custom-developed encryption algorithms
  - Sophisticated anti-analysis capabilities
  - Advanced process injection techniques
- Network Infrastructure:
  - Distributed Command-and-Control
  - Sophisticated proxy mechanisms
  - Shared infrastructure with state-sponsored actors
- Evasion Capabilities:
  - Advanced anti-debugging features
  - Sophisticated process hiding
  - Complex obfuscation techniques

MITRE ATT&CK-based Kill Chain for Play Ransomware:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application (Exchange Server)
	T1566	Phishing
	T1133	External Remote Services
	T1078	Valid Accounts
Execution	T1059	PowerShell
	T1059	Windows Command Shell
	T1106	Native API
	T1204	Malicious File
Persistence	T1505	Web Shell
	T1543	Create or Modify System Process
	T1547	Registry Run Keys
	T1136	Create Account
Privilege Escalation	T1548	Abuse Elevation Control Mechanism
	T1134	Access Token Manipulation
	T1068	Exploitation for Privilege Escalation
	T1484	Domain Policy Modification
Defence Evasion	T1562	Disable or Modify Tools
	T1070	Indicator Removal
	T1112	Modify Registry
	T1027	Obfuscated Files or Information
Credential Access	T1003	OS Credential Dumping
	T1552	Unsecured Credentials
	T1555	Credentials from Password Stores
	T1558	Steal or Forge Kerberos Tickets
Discovery	T1082	System Information Discovery
	T1087	Account Discovery
	T1083	File and Directory Discovery
	T1018	Remote System Discovery
Lateral Movement	T1021	Remote Desktop Protocol
	T1021	SMB/Windows Admin Shares
	T1091	Replication Through Removable Media
	T1570	Lateral Tool Transfer
Collection	T1560	Archive Collected Data
	T1213	Data from Information Repositories
	T1005	Data from Local System
	T1039	Data from Network Shared Drive
Command-and-Control	T1071.001	Web Protocols
	T1573	Encrypted Channel
	T1090	Proxy
	T1572	Protocol Tunnelling
Exfiltration	T1041	Exfiltration Over C2 Channel
	T1567	Exfiltration Over Web Service
	T1048	Exfiltration Over Alternative Protocol
	T1029	Scheduled Transfer
Impact	T1486	Data Encrypted for Impact
	T1489	Service Stop
	T1490	Inhibit System Recovery
	T1485	Data Destruction

Indicators of Compromise

SHA256 Hashes

- 243ad5458706e5c836f8eb88a9f67e136f1fa76ed44868217dc995a8c7d07bf7
- 2b254ae6690c9e37fa7d249e8578ee27393e47db1913816b4982867584be713a
- f64dab23c50e3d131abcc1bdbb35ce9d68a34920dd77677730568c24a84411c5
- 99e2ebf8cec6a0cea57e591ac1ca56dd5d505c2c3fc8f4c3da8fb8ad49f1527e
- b4f5d37732272f18206242ccd00f6cad9fbfc12fae9173bb69f53fffeba5553f
- b1ac26dac205973cd1288a38265835eda9b9ff2edc6bd7c6cb9dee4891c9b449

Sliver C2 Server Information

- 172.96.137[.]224
- americajobmail[.]site

Code Signing Certificate Details

SHA256 hash:
b4f5d37732272f18206242ccd00f6cad9fbfc12fae9173bb69f53fffeba5553f
Chain: 6e95d94d5d8ed2275559256c5fb5fc6d01da6b46
Issuer: CN=LAMERA CORPORATION LIMITED
NotBefore: 2/10/2022 9:44 PM
NotAfter: 12/31/2039 4:59 PM
Subject: CN=LAMERA CORPORATION LIMITED
Serial: 879fa942f9f097b74fd6f7dabcf1745a
Cert: 6e95d94d5d8ed2275559256c5fb5fc6d01da6b46

SHA256 hash:
f64dab23c50e3d131abcc1bdbb35ce9d68a34920dd77677730568c24a84411c5
Chain: 6624c7b8faac176d1c1cb10b03e7ee58a4853f91
Issuer: CN=Tableau Software Inc.
NotBefore: 5/27/2023 11:15 AM
NotAfter: 12/31/2039 4:59 PM
Subject: CN=Tableau Software Inc.
Serial: 76cb5d1e6c2b6895428115705d9ac765
Cert: 6624c7b8faac176d1c1cb10b03e7ee58a4853f91

This list of IoCs may not be the full list managed by Red Piranha and should only be considered a sample list.

A recent analysis of ransomware impacts across various countries highlights the United States as the most affected, with a dominant 52.83% of incidents. Following are Canada with 7.55% and India with 6.6% of total attacks. The United Kingdom constituted 3.77% of incidents, while Australia, Brazil, and France each recorded 2.83% of total incidents. The United Arab Emirates, Germany, and Israel each experienced 1.89% of attacks. Several other nations including Indonesia, Cyprus, Spain, Czech Republic, Philippines, Poland, Saudi Arabia, Puerto Rico, Guatemala, Mexico, Sweden, Thailand, Bangladesh, Latvia, and Italy observed minimal impacts at 0.94% each. This distribution underscores the global reach and varied impact of ransomware attacks, with a clear concentration in North America, particularly the United States.

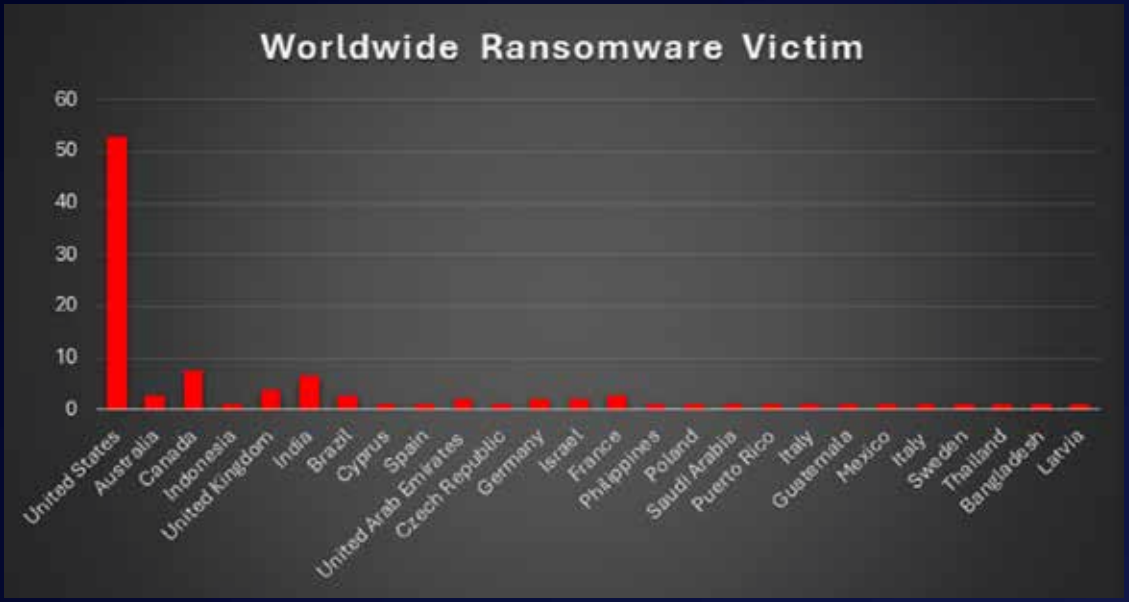

Figure 3: Ransomware Victims Worldwide

Industries	Overall Percentage
Technology & communications	9.43%
Business & professional services	16.04%
Industrial machinery	3.77%
Construction & infrastructure	1.89%
Logistics services	0.94%
Healthcare	8.49%
Retail	3.77%
Manufacturing	4.72%
Transportation	1.89%
Government of Brazil	0.94%
Real estate	1.89%
Transaction processing	0.94%
Financial & legal	4.72%
Aerospace	1.89%
Automotive service	5.66%
Education	1.89%
Logistics services	2.83%
Energy & resources	2.83%
Agriculture	0.94%
Food & beverage	1.89%
Federal	0.94%
Appliances	0.94%
Mining	0.94%
Advertising & marketing	0.94%
Care services	0.94%

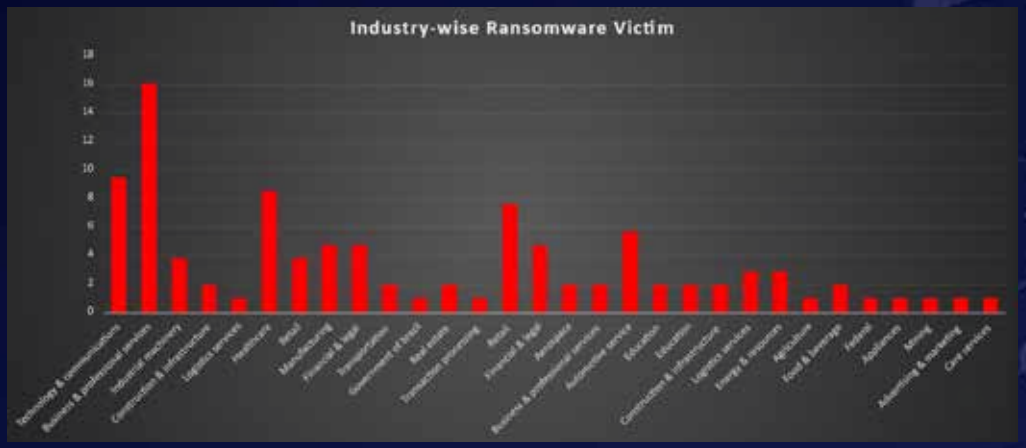

Figure 4: Industry-wise Ransomware Victims

Here are essential measures to mitigate the risk of Play ransomware and similar threats:

1. **Enhanced Exchange Server Security**: Implement robust security measures for Microsoft Exchange servers, including regular patching and monitoring, particularly focusing on CVE-2022-41082 and CVE-2022-41040 vulnerabilities that Play ransomware actively exploits.
2. **Advanced Network Segmentation**: Deploy comprehensive network segregation to isolate critical systems and implement strict access controls between segments, limiting the potential spread of ransomware within the network.
3. **Multi-Factor Authentication**: Enforce strong multi-factor authentication across all remote access points and privileged accounts to prevent unauthorised access and lateral movement commonly used by Play ransomware.
4. **Backup and Recovery Strategy**: Maintain secure, encrypted offline backups with regular testing procedures, implementing a 3-2-1 backup strategy to ensure data recovery capabilities in case of encryption.
5. **Email Security Controls**: Deploy advanced email security solutions with robust phishing protection and attachment scanning, as Play ransomware often initiates attacks through phishing campaigns.
6. **Endpoint Detection and Response**: Implement sophisticated EDR solutions to monitor and detect suspicious activities, particularly focusing on PowerShell abuse and unusual encryption behaviours characteristic of Play ransomware.
7. **Security Awareness Training**: Conduct regular security awareness sessions focusing on ransomware threats, phishing identification, and proper security practices to prevent initial compromise.
8. **Incident Response Planning**: Develop and maintain comprehensive incident response plans specifically addressing ransomware scenarios, including regular testing and updates based on Play ransomware's evolving tactics.