Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Nov 26 - Dec 02, 2024

Report Summary:

- **New Threat Detection Added** – 2 (SAP BusinessObjects Authentication Vulnerability (CVE-2024-41730) and Glove Stealer)
- **New Threat Protections - 189**

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

1. SAP BusinessObjects Authentication Vulnerability (CVE-2024-41730)

A critical authentication vulnerability, identified as CVE-2024-41730, has been discovered in SAP BusinessObjects Business Intelligence Platform. This flaw allows unauthorised attackers to obtain a logon token via a REST endpoint, potentially leading to full system compromise. The vulnerability affects versions ENTERPRISE 430 and ENTERPRISE 440, with a CVSS v3.0 Base Score of 9.8, indicating its severity. SAP has released patches to address this issue, and it is strongly recommended that all affected organisations apply these patches promptly to mitigate potential risks.

Threats Protected: 1
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

2. Glove Stealer

Glove Stealer is a .NET-based information-stealing malware that targets sensitive data from browsers, cryptocurrency wallets, two-factor authentication (2FA) applications, password managers, and email clients. It employs the IElevator service to bypass Chrome's App-Bound Encryption, enabling it to access encrypted browser data. The malware is typically distributed through phishing emails that mimic troubleshooting tools, deceiving users into executing malicious scripts.

Threats Protected: 06
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Spearphishing Attachment
Execution	T1059.001	PowerShell
Persistence	T1547.001	Registry Run Keys / Startup Folder
Defence Evasion	T1027	Obfuscated Files or Information
Credential Access	T1555	Credentials from Password Stores
Collection	T1119	Automated Collection
Exfiltration	T1041	Exfiltration Over C2 Channel

Known exploited vulnerabilities (Week 4 November 2024):

Vulnerability	CVSS	Description
CVE-2023-28461	9.8 (Critical)	Array Networks AG and vxAG ArrayOS Missing Authentication for Critical Function Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-november-2024/527

Updated Malware Signatures (Week 4 November 2024)

Threat	Description
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 conducts ongoing surveillance of the dark web and other channels to identify global organisations impacted by ransomware attacks. In the past week, our monitoring revealed multiple ransomware incidents across diverse threat groups, underscoring the persistent and widespread nature of these cyber risks. Presented below is a detailed breakdown of ransomware group activities during this period.

Ransomware Group	Overall Percentage of total attack coverage
Inc Ransom	13.39%
Killsec3	14.29%
Hunters	6.25%
RA Group	2.68%
Eraleign (APT73)	2.68%
BlackSuit	2.68%
SafePay	6.25%
Lynx	5.36%
Dispossessor	0.89%
Everest	1.79%
Handala	0.89%
RansomHouse	1.79%
Ransomware Blog	0.89%
Fog	9.82%
RansomHub	12.5%
Bianlian	0.89%
Kairos	1.79%
Space Bears	1.79%
Lockbit3	1.79%
Argonauts Group	8.93%
Rhysida	1.79%
Qilin	0.89%

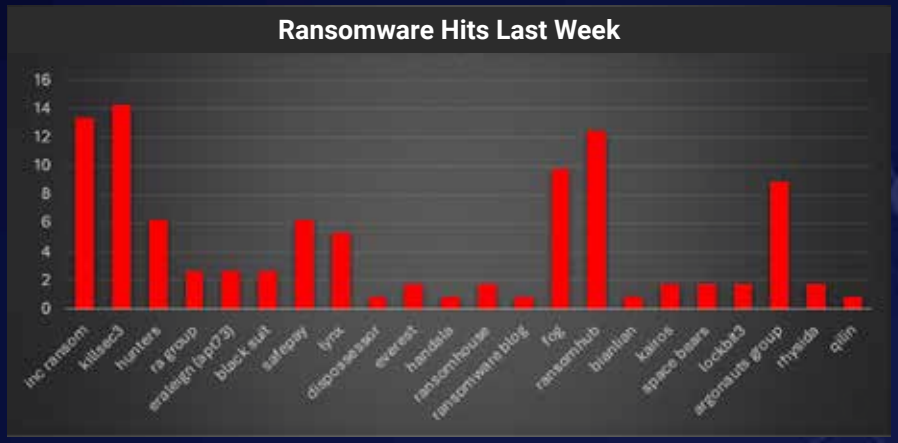


Figure 1: Ransomware Group Hits Last Week

Inc. Ransomware Group

Based on the latest analysis conducted in July 2023, researchers identified a novel ransomware variant named Inc. ransomware, marking its entry into the threat landscape. This extortion-focused operation leverages a unique approach by presenting itself as a service aimed at aiding victims. Threat actors claim that paying the ransom not only helps victims "save their reputation" but also provides insights into vulnerabilities, ostensibly making the victim's environment more secure.

Inc. ransomware employs a multi-extortion strategy, exfiltrating sensitive data and threatening public exposure if demands are unmet. The group's dual focus on reputational and operational leverage underscores a sophisticated tactic to compel compliance. Key characteristics of Inc. ransomware include its emphasis on victim-shaming through reputation damage and its operational rhetoric of security enhancement post-payment.

Detailed TTPs
Initial access methods for Inc. ransomware vary and include spear-phishing emails and exploiting vulnerable services, such as CVE-2023-3519 in Citrix NetScaler. Once access is established, the threat actors leverage a range of Commercial Off-The-Shelf (COTS) tools and Living-Off-The-Land Binaries (LOLBINs) for internal reconnaissance and lateral movement. Tools commonly associated with Inc. ransomware operations include:

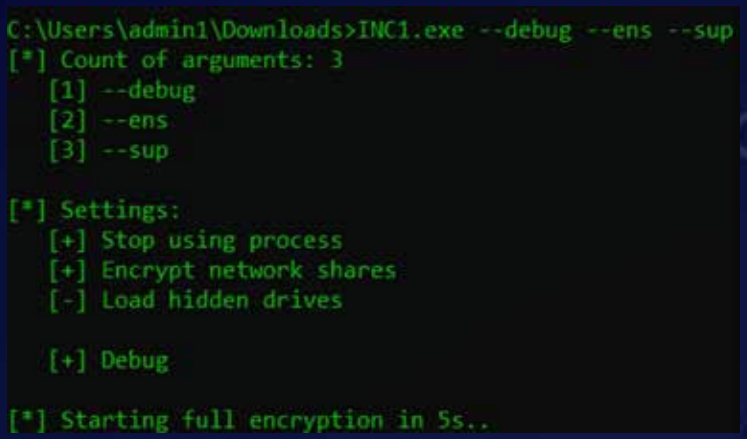
- NETSCAN.EXE: A multi-protocol network scanning and profiling utility.
- MEGAsyncSetup64.EXE: A desktop application for file sharing and synchronisation via the MEGA cloud platform.
- ESENTUTL.EXE: A Microsoft utility for managing and recovering databases.
- AnyDesk.exe: A remote desktop application used for remote management and access.

The Inc. ransomware payload supports several command-line arguments, enabling targeted operations:

Argument	Function
–file	Encrypts a specific file by path.
–dir	Encrypts all files within a specified directory.
–sup	Terminates specified processes.
–ens	Encrypts network shares.
–lhd	Encrypts local hidden drives, including hidden boot and recovery volumes, rendering the device non-bootable.
–debug	Outputs console-style debug logs for detailed monitoring.

These functionalities reflect the ransomware's flexibility and its capacity to cause significant disruption across compromised environments.

If the attacker skips specifying any command-line arguments, the Inc. ransomware payload defaults to encrypting the entire local system. This includes all accessible files and storage volumes, maximising the damage to the compromised device. This approach ensures that even without fine-tuned targeting, ransomware can cause significant disruption.



Inc. ransomware leaves ransom notes in every folder containing encrypted files. These notes are created in both .TXT and .HTML formats, named "INC-README.TXT" and "INC-README.HTML," respectively. Beyond local storage, the ransomware attempts to broadcast the HTML version of the note to any connected printers or fax machines, further amplifying its reach and impact.

Interestingly, Inc. ransomware also appears designed to delete Volume Shadow Copies (VSS) to hinder recovery efforts. However, this behaviour could not be consistently replicated during testing, indicating variability in its implementation or execution.
The debug strings are present in of Inc. ransomware payloads.

C:\source\INC Encryptor\Release\INC Encryptor.pdb

Here's the TTP chart for Inc. ransomware, including MITRE ATT&CK IDs where applicable:

Tactic	Technique/Procedure	ATT&CK ID
Initial Access	Spear-phishing emails with malicious attachments or links	T1566
Initial Access	Exploitation of known vulnerabilities (e.g., CVE-2023-3519 in Citrix NetScaler)	T1190
Execution	Ransomware payload execution using command-line arguments or default settings	T1059
Execution	Uses LOLBINs (e.g., ESENTUTL.EXE) for execution	T1218
Persistence	Deployment of remote management tools like AnyDesk.exe	T1133
Privilege Escalation	Exploitation of system vulnerabilities to escalate privileges	T1068
Defence Evasion	Deletes Volume Shadow Copies to prevent recovery (though inconsistent in testing)	T1490
Credential Access	Potential use of credential-stealing methods to expand access	T1555
Discovery	Network scanning using tools like NETSCAN.EXE	T1046
Lateral Movement	Encryption of network shares via --ens argument	T1210
Collection	Identification of sensitive files and directories for encryption	T1530
Exfiltration	Threats to leak stolen data to compel victim compliance	T1537
Impact	Encryption of local devices, hidden drives, and network shares	T1486
Impact	Broadcasting ransom notes to connected printers or fax machines	T1010

Indicator Of Compromise (IOCs)

Hexadecimal Patterns:

1. $h0: 6A 00 6A 00 6A 18 8D [3-4] 5? 68 28 C0 53 00
2. $h1: 6A 00 68 80 00 00 00 6A 03 6A 00 6A 03 [0-16] 68 9F 01 12 00 [0-8] C7 44 24 ?? 2E 00 5C 00
3. $h2: 6A 20 FF 35 [4] FF 15 [8-12] 8A 4? 1F 80 2? F8 24 3F 0C 40 88 4? 1F

Textual Patterns (Strings):

1. $s0: "\x00Q:\\\x00W:\\\x00E:\\\x00R:\\\x00T:\\\x00Y:\\\x00U:\"
2. $s1: "PGh0bWw+DQoJPGhlYWQ+DQoJCTx0aXRsZT5JbmMuIFJhbnNvbXdhcmU8" (Base64 encoded HTML content)
3. $s2: "\\background-image.jpg\x00"
4. $s3: "\x00–lhd\x00"
5. $s4: "\x00–ens\x00"
6. $s5: "\x00–sup\x00"
7. $s6: " delete shadow copies from %c:/ "
8. $s7: "\x00[+] Start encryption of"
9. $s8: "[+] Encrypting: %s\n"
10. $s9: "[+] Found drive: %s"
11. $s10: " [+] Mounted %s\n"
12. $s11: " [-] Failed to mount %s Error: %d\n"
13. $s12: "[*] Count of arguments: %d\n"
14. $s13: "[-] Please, add \"/\" to the end of directory!\n"
15. $s14: "[*] Settings:\n"
16. $s15: " [%s] Stop using process\n"
17. $s16: " [%s] Encrypt network shares\n"
18. $s17: " [%s] Load hidden drives\n\n"
19. $s18: "[*] Loading hidden drives...\n"
20. $s19: "[*] Starting full encryption in 5s"
21. $s20: "[+] Start sending note to printers...\n"
22. $s21: "[+] Count of printers: %d\n"

Command-Line Arguments:

1. –file: Encrypt a specific file
2. –dir: Encrypt a directory
3. –sup: Stop using a process
4. –ens: Encrypt network shares
5. –lhd: Encrypt local hidden drives (resulting in non-bootable device)
6. –debug: Output console-style debug logs

File Names for Ransom Notes:

- INC-README.TXT
- INC-README.HTML

Here is the yara.rule for the inc ransomware malware.

Mitigation:

1. Educate Employees: Train employees on phishing risks, how to identify malicious attachments and links, and encourage reporting suspicious emails.
2. Implement Strong Passwords: Enforce strong, unique passwords for all accounts and rotate them regularly.
3. Enable Multi-Factor Authentication (MFA): Use MFA for all accounts, especially critical systems, through apps or hardware tokens.
4. Regular Updates and Patching: Regularly patch systems and applications, closing known vulnerabilities such as CVE-2023-3519 in Citrix NetScaler.
5. Backup and Disaster Recovery: Implement regular backups and offsite storage, with verified restoration processes for disaster recovery.
6. Network Segmentation and Least Privilege Access: Segment networks and implement least privilege access to limit lateral movement within the organisation.
7. Endpoint Protection and Network Monitoring: Deploy advanced endpoint protection to detect ransomware activity and monitor for suspicious network traffic.
8. Block Command-and-Control (C2) Communication: Use threat intelligence to block C2 server IPs and domains associated with the ransomware.
9. Disable SMB and Remote Desktop Services: Disable unnecessary SMB and restrict RDP access to prevent lateral movement.
10. File Integrity Monitoring: Implement file integrity monitoring to detect unauthorised changes, like encryption or ransom notes.
11. VSS and Shadow Copy Protection: Protect and back up VSS and shadow copies to prevent deletion by ransomware.
12. Printer and Fax Protection: Limit printer access, secure configurations with strong passwords, and disable unnecessary protocols.

Ransomware Victims Industry-wise

Based on the analysis of ransomware attacks across various industries, the data highlights some notable trends in attack distribution:

- Healthcare (10.71%) and Retail (10.71%) industries were among the most targeted, both covering a significant portion of the total attacks. This underscores the continued focus on sectors handling sensitive personal information, such as patient data and customer details.
- Business Services (13.39%) also stands out as a major target, reflecting the broader threat landscape impacting organisations offering a range of professional services.
- Manufacturing (12.5%) saw a considerable percentage of attacks, which is typical given its critical infrastructure and the potential impact of supply chain disruptions.
- Construction (9.82%) and Healthcare (10.71%) show that industries traditionally less reliant on digital services are becoming increasingly susceptible to cyber threats, as digital transformation and IoT adoption grow.
- Smaller sectors like Telecommunications (1.79%) and Consulting (1.79%) also experienced some impact, reflecting the cross-industry nature of these attacks.
- Certain sectors such as Energy (0.89%), Electronics (0.89%), and Agriculture (0.89%) were less targeted, though they remain important in the broader attack landscape due to critical infrastructure dependencies.

This data highlights the growing threat of ransomware across a broad range of sectors, with particular emphasis on industries managing sensitive data, infrastructure, and business services.

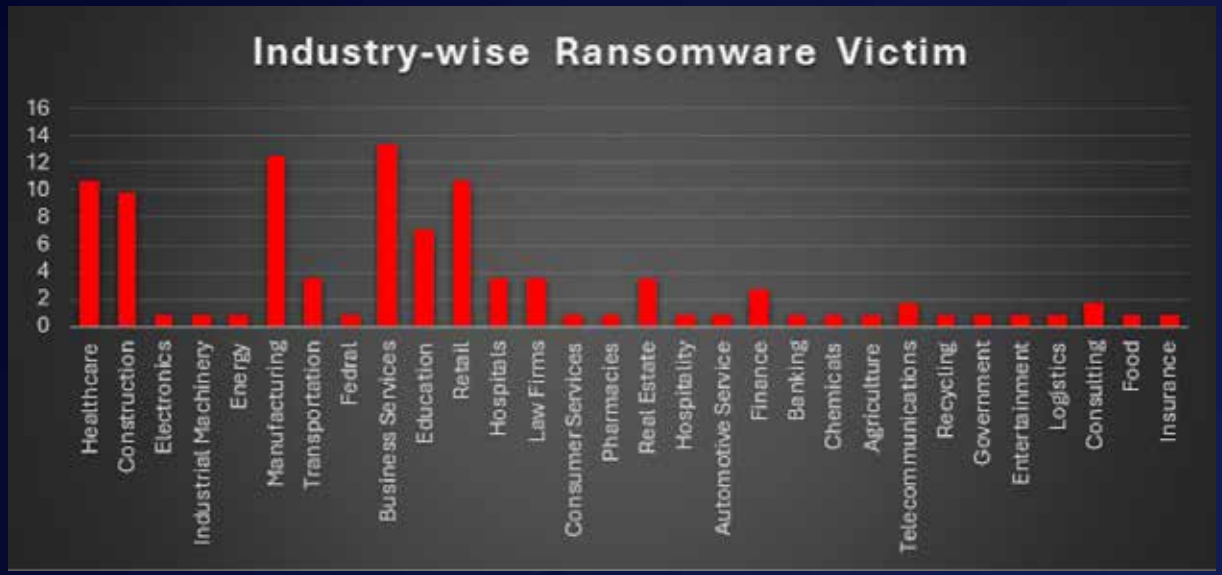


Figure 5: Industry-wise Ransomware Victims

Ransomware Victims Worldwide

A recent ransomware analysis reveals a striking 41.96% of global incidents targeted the United States, making it the hardest-hit country by far. Trailing behind, the United Kingdom experienced 5.36% of attacks, while Canada reported 2.68%. Australia and Italy faced 6.25% of the attacks each, reflecting notable vulnerabilities in these regions.

Germany, Brazil, and Taiwan each experienced 3.57% of incidents, highlighting significant exposure in these countries. Meanwhile, countries such as Argentina, Saudi Arabia, and Malaysia were less impacted, each contributing 0.89% of total incidents.

This analysis demonstrates the widespread nature of ransomware attacks, with North America and Europe bearing the brunt of these persistent threats. These numbers emphasise the urgent need for enhanced cybersecurity measures across these heavily targeted regions, especially in the U.S., which remains the prime focus of attackers.

Figure 6: Ransomware Victims Worldwide