Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Nov 19 - 25, 2024

Report Summary:

- **New Threat Detection Added** –2 (Palo Alto PAN-OS Vulnerabilities (CVE-2024-0012 and CVE-2024-9474) and LandUpdate808 Fake Update Variant)
- **New Threat Protections - 210**

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

1. Palo Alto PAN-OS Vulnerabilities (CVE-2024-0012 and CVE-2024-9474)

Two critical vulnerabilities have been identified in Palo Alto Networks' PAN-OS, specifically affecting the SSLVPN component. CVE-2024-0012 is an authentication bypass vulnerability in the management web interface, while CVE-2024-9474 pertains to privilege escalation. Exploitation of these vulnerabilities allows attackers to gain unauthorised access and execute arbitrary code with root privileges on the firewall. These issues have been actively exploited in the wild, underscoring the urgency for immediate patching and implementation of recommended mitigations.

Threats Protected: 2
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. LandUpdate808 Fake Update Variant

LandUpdate808 is a sophisticated fake update malware variant that deceives users into downloading malicious payloads by presenting counterfeit software update prompts. Unlike other fake update schemes such as SocGholish, LandUpdate808 employs a unique delivery chain and payload variations. The malware's delivery mechanism involves multiple stages, including the use of obfuscated JavaScript and remote PHP scripts to load deceptive update pages. The final payloads are typically named in the format "update_DD_MM_YYYY_#######" with extensions like .js, .exe, or .msix. This variant has evolved over time, with changes in its delivery infrastructure and obfuscation techniques, making detection and mitigation challenging.

Threats Protected: 04
Rule Set Type:

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

Class Type: Attempted-admin

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566.002	Spearphishing Link
Execution	T1204.002	Malicious File
Discovery	T1082	System Information Discovery
Defence Evasion	T1027	Obfuscated Files or Information
Command-and-Control	T1071.001	Web Protocols

Known exploited vulnerabilities (Week 3 November 2024):

Vulnerability	CVSS	Description
CVE-2024-9474	6.9 (Medium)	Palo Alto Networks PAN-OS Management Interface OS Command Injection Vulnerability
CVE-2024-0012	9.3 (Critical)	Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability
CVE-2024-1212	10.0 (Critical)	Progress Kemp LoadMaster OS Command Injection Vulnerability
CVE-2024-38813	9.8 (Critical)	VMware vCenter Server Privilege Escalation Vulnerability
CVE-2024-38812	9.8 (Critical)	VMware vCenter Server Heap-Based Buffer Overflow Vulnerability
CVE-2024-21287	7.5 (High)	Oracle Agile Product Lifecycle Management (PLM) Incorrect Authorisation Vulnerability
CVE-2024-44309	Ongoing Analysis	Apple Multiple Products Cross-Site Scripting (XSS) Vulnerability
CVE-2024-44308	Ongoing Analysis	Apple Multiple Products Code Execution Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-november-2024/526

Updated Malware Signatures (Week 3 November 2024)

Threat	Description
Qakbot	A malware designed to acquire valuable data such as banking credentials and is also capable of stealing FTP credentials and spreading across a network by utilising SMB.
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 Groups and Attack Coverage:

Name of Ransomware Group	Overall Percentage of total attack coverage
DragonForce	8.13%
Medusa	6.5%
BlackSuit	5.69%
Rhysida	0.81%
RansomHub	13.82%
Lynx	3.25%
Termite	4.88%
Killsec3	7.32%
Money Message	0.81%
Cactus	4.07%
El Dorado	3.25%
Eraleign (APT73)	1.63%
Hunters	0.81%
Meow	0.81%
SafePay	17.07%
Monti	0.81%
Play	0.81%
INC Ransom	3.25%
Arcus Media	4.88%
Bianlian	2.44%
Qilin	4.88%
Fog	1.63%
Handala	0.81%
Chort	0.81%
Lockbit3	0.81%

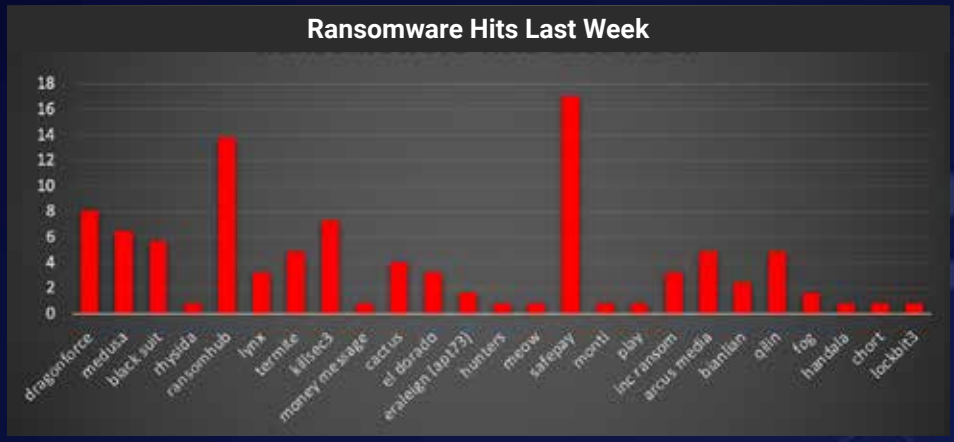


Figure 1: Ransomware Group Hits Last Week

SafePay Ransomware Group

Based on the latest Analysis on 21-Nov-2024, In the latest analysis conducted by Red Piranha, our team has identified a concerning new ransomware variant named SafePay that has emerged in the threat landscape. First observed in October 2024, this previously unreported ransomware strain has been identified in multiple incidents across different business sectors and geographical locations.

Red Piranha analysts documented two distinct SafePay ransomware deployment incidents. These attacks targeted organisations in different business verticals and geographical locations, indicating a potentially widespread campaign. The key identifying characteristics of these attacks include:
•Encrypted files appended with .safepay extension
•Ransom note filename: readme_safepay.txt
•No prior public reporting or documentation of this variant

Detailed TTPs
Initial Access and Defence Evasion:

- Primary access vector: Remote Desktop Protocol (RDP)
- Initial attempt to execute Sparpfinder.ps1 was detected and blocked by Windows Defender
- Threat actors successfully disabled Windows Defender using a series of LOLBin commands
  "C:\Windows\system32\SystemSettingsAdminFlows.exe" Defender DisableEnhancedNotifications 1
  "C:\Windows\system32\SystemSettingsAdminFlows.exe" Defender SubmitSamplesConsent 0
  "C:\Windows\system32\SystemSettingsAdminFlows.exe" Defender SpynetReporting 0
  "C:\Windows\system32\SystemSettingsAdminFlows.exe" Defender RTP 1
- Successfully executed ShareFinder.ps1 after disabling security controls

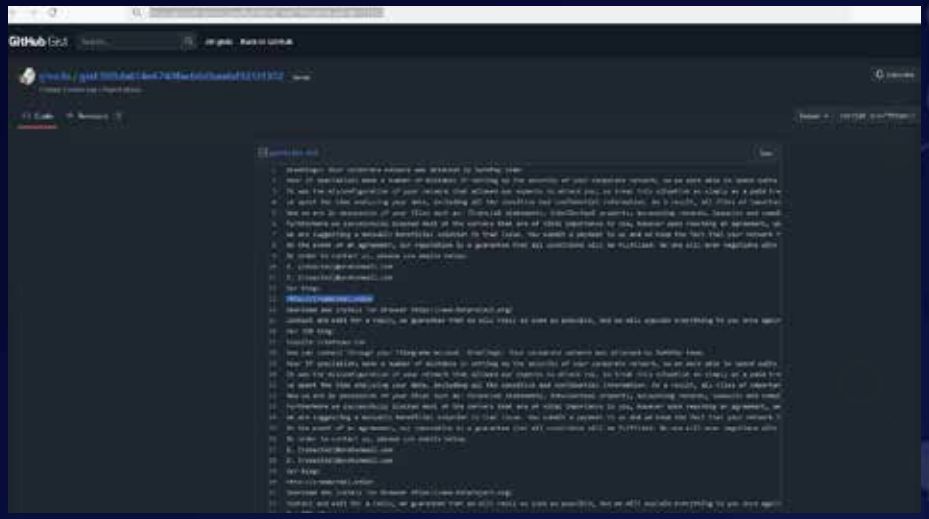
Privilege Escalation Analysis
The adversary likely employed a widely recognised UAC Bypass Privilege Escalation technique, frequently used by ransomware groups such as LockBit and BlackCat/ALPHV. This method involves creating an elevated process via a specified COM Object, enabling the execution of malicious commands or binaries.

In this instance, the parent process observed was DllHost.exe, with the CLSID of the COM Object (CMSTPLUA) visible in the command line. Although such activity may occasionally occur for legitimate reasons, it is uncommon—particularly in scenarios involving:

- Unsigned binaries.
- System binaries leveraged for proxy execution.
- Scripting interpreters (e.g., CMD or PowerShell) as child processes.

This behaviour typically warrants further scrutiny to identify potential misuse or privilege escalation attempts.

Ransomware note: Safeplay Message!



Process Termination
The malware employs ZwTerminateProcess to terminate specific processes, targeting applications and services critical for system operations, databases, and productivity tools. The processes targeted for termination include:

- Database & Sync Services: sql, oracle, ocssd, dbsnmp, synctime, agntsvc, isqlplussvc.
- Backup & Security Services: xfssvccon, mydesktopservice, ocautoupds, encsvc.
- Web & Email Clients: firefox, tbirdconfig, thunderbird, thebat.
- Office Suite & Productivity Tools: excel, infopath, msaccess, mspub, onenote, outlook, powerpnt, visio, winword.
- Miscellaneous Applications: steam, notepad, wordpad, wuauclt, onedrive, sqlmangr.

Service Termination
The ransomware leverages ControlService to stop services, focusing on those related to backups, antivirus software, and system operations, aiming to disable protective mechanisms and hinder data recovery efforts. Targeted services include:

- System & Backup Services: vss, sqlsvc, memtas, backup, GxVss, GxBlr, GxFWD, GxCVD, GxCIMgr.
- Email & Exchange Services: mepocs, msexchange.
- Antivirus & Security Tools: Sophos, Veeam.

This dual strategy of terminating both processes and services ensures the ransomware can maximise its impact while reducing resistance from the system's defences.

Data Exfiltration Phase:

- Approximately 40 minutes after initial access, threat actors began data archiving operations
- Utilised WinRAR.exe with specific command parameters for data collection:

WinRAR.exe a -v5g -ed -r -tn1000d -m0 -mt5 -x*.rar -x*.JPEG -x*.RAW -x*.PSD -x*.TIFF -x*.BMP -x*.GIF -x*.JPG -x*.MOV -x*.pst -x*.FIT -x*.FIL -x*.mp4 -x*.avi -x*.mov -x*.mdb -x*.iso -x*.exe -x*.dll -x*.bak -x*.msg -x*.png -x*.zip -x*.ai -x*.7z -x*.DPM -x*.log -x*.dxf -x*.insp -x*.upd -x*.db -x*.dwg -x*.nc1 -x*.metadata -x*.dg -x*.inp -x*.dat -x*.TIFF -x*.tiger -x*.pcp -x*.rvt -x*.rws -x*.nwc -x*.tif -x*.frx -x*.dyf -x*.rcs -x*.diff C:\[redacted].rar \\[redacted]\C$\Users\

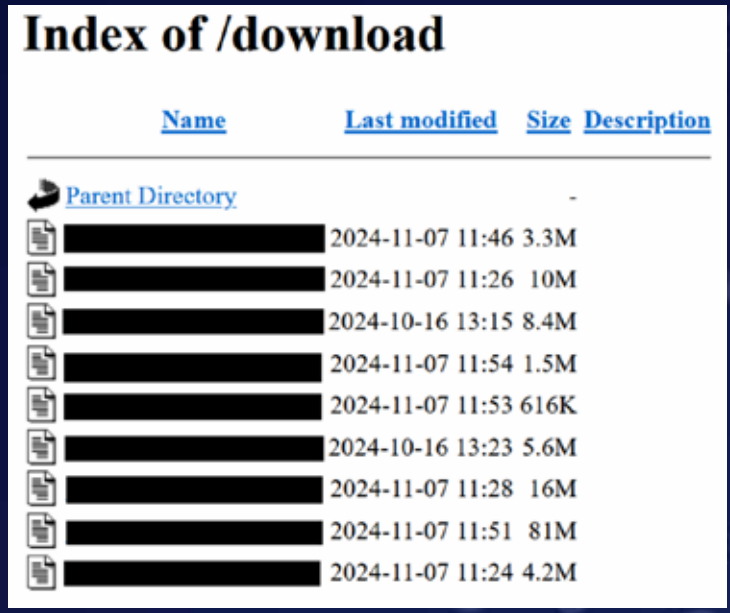
Shortly thereafter, FileZilla was installed using the setup file FileZilla_3.67.1_win64_sponsored-setup.exe. Following the installation, both filezilla.exe and fzsftp.exe were executed. However, the application was promptly uninstalled afterwards.

Most of the strings throughout the binary are obfuscated with a simple three-step XOR loop consisting of a random single-byte key, the index of the character, and the first byte of kernel32.dll ('M').

String Encryption: String_decrypt.py

Tactic	Technique ID	Technique Name
Execution	T1059	Command and Scripting Interpreter
	T1059.001	Powershell
	T1059.003	Windows Command Shell
Privilege Escalation	T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control
Defence Evasion	T1202	System Binary Proxy Execution
	T1070.004	File Removal
	T1562.001	Impair Defences: Disable or Modify Tools
Discovery	T1135	Network Share Discovery
Collection	T1560.001	Archive Collected Data: Archive via Utility
Exfiltration	T1048	Exfiltration Over Alternative Protocol
Impact	T1486	Data Encrypted for Impact
	T1490	Inhibit System Recovery

Indicator of Compromises (IOC's)
SHA256: a0dc80a37eb7e2716c02a94adc8df9baedec192a77bde31669faed228d9ff526
IPv4: 45.91.201.247
IPv4: 77.37.49.40
IPv4: 80.78.28.63
domain iieavvi4wtiuijas3zw4w54a5n2srnccm2fcb3jcrvbb7ap5tfphw6ad.onion
domain qkzxzeabulbbaevqkoy2ew4nukakbi4etnnkcyo3avhwu7ih7cql4gyd.onion



Mitigation:

1.Restrict Remote Desktop Protocol (RDP) Access: Use VPNs, enable multi-factor authentication (MFA), and enforce strong password policies
2.Monitor PowerShell and LOLBins Usage.
3.Monitor UAC Bypass Attempts: Audit and alert on the creation of processes with elevated privileges, especially those leveraging DllHost.exe or COM Objects.
4.Ensure the least privileged access is enforced for all users and processes.

Ransomware Victims Worldwide

A recent ransomware analysis reveals a striking 48.78% of global incidents targeted the United States, making it the hardest-hit country by far. Trailing behind, the United Kingdom experienced 5.69% of attacks, while Canada reported 4.88%. Australia, France, and India each faced 4.07%, reflecting notable vulnerabilities in these regions.

Germany and Italy were also significantly impacted, contributing 3.25% each, followed by Brazil at 2.44%. Other countries like the Netherlands, Spain, and Argentina recorded smaller shares, each at 1.63%.

Meanwhile, a diverse group of nations, including Estonia, Belgium, Oman, China, Egypt, Peru, and Mexico, saw limited impacts, each representing just 0.81% of the total incidents.

This analysis highlights the widespread nature of ransomware attacks, with North America and Europe facing the brunt of these persistent threats. These numbers underscore the urgent need for robust cybersecurity measures worldwide.

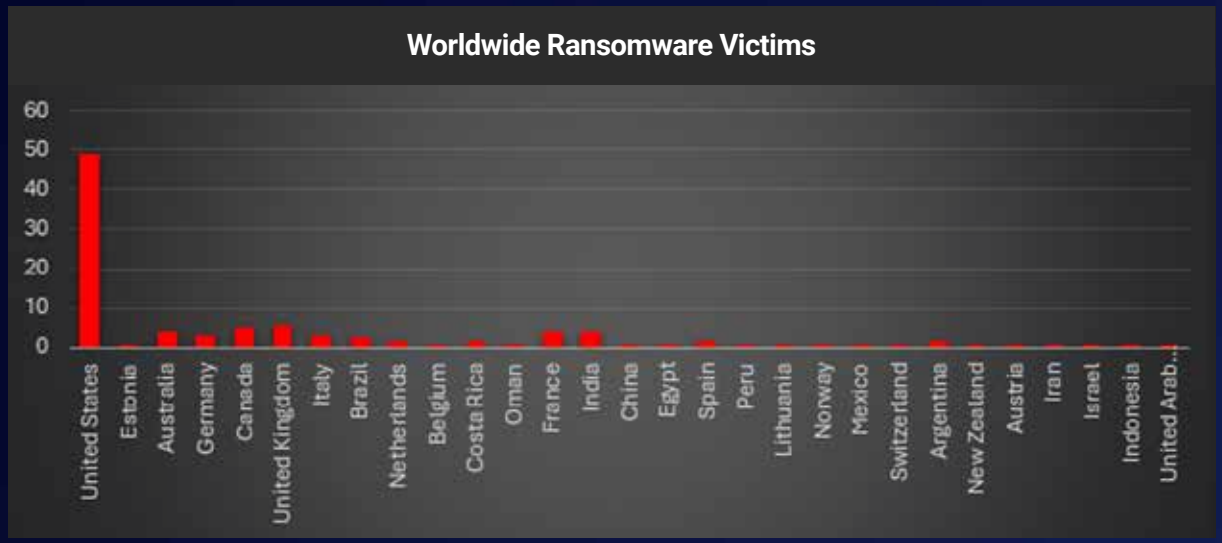


Figure 5: Ransomware Victims Worldwide

Ransomware Victims Industry-wise

Ransomware attacks continue to disrupt industries across the board, with the Retail sector emerging as the hardest hit, making up a significant 13.01% of all incidents. Education, Construction, and Business Services are also high on the radar, each seeing 8.94% of attacks, underlining their growing vulnerability.

The Healthcare and Finance sectors are not far behind, each accounting for 6.5%, while Manufacturing faces its own challenges at 4.88%. Even industries like Software and Energy are feeling the impact, with each recording 3.25% of incidents.

Mid-level impacts were observed in areas like Food & Beverage, Consumer Services, and Architecture, all reporting 2.44% of attacks. Meanwhile, sectors like Automotive Services, Hospitality, and Law Firms experienced smaller yet notable shares of 1.63%.

A wide range of industries, including Fitness, Airlines, Oil, Gambling, and Internet Service Providers, were less affected, each seeing 0.81% of the total incidents.

These numbers paint a clear picture: ransomware isn't just targeting one or two industries. It's spreading across the spectrum, hitting both critical and smaller sectors. This makes it more important than ever for organisations in every field to bolster their cybersecurity strategies and protect against these growing threats.

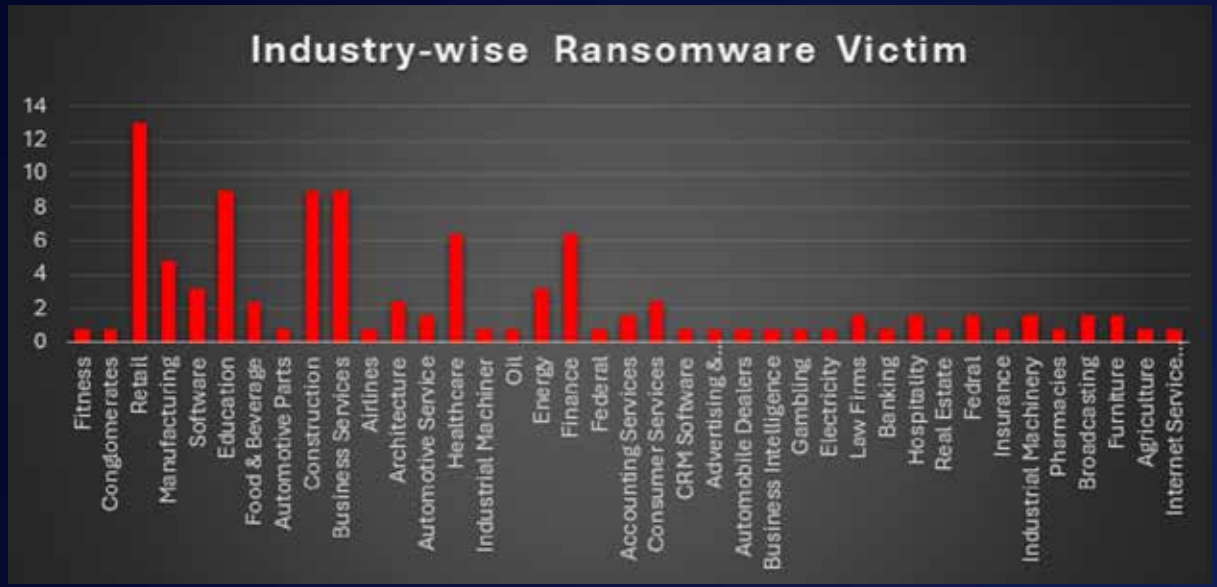


Figure 6: Industry-wise Ransomware Victims