Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Jan 09 - 15, 2024

Report Summary:

- **New Threat Detection Added** – 6 (Winter Vivern APT, DarkRadiation Ransomware, GoBruteforcer Malware, RisePro Stealer, Andariel APT and FalseFont Backdoor)
- **New Threat Protections - 24**
- **New Ransomware Victims Last Week - 43**

Newly Detected Threats Added

1. Winter Vivern APT

The Winter Vivern Advanced Persistent Threat (APT) is a lesser-known group with pro-Russian goals. Named after a URL string, they have remained low-profile but resurfaced targeting Ukraine recently. Initially detected in 2021, their activities across Lithuania, India, the Vatican, and Slovakia have increased. They have now attacked Poland, Ukraine, Italy, and Indian government agencies, along with telecom firms backing Ukraine. They craft deceptive documents from real government data and fake government domains for malicious downloads. Their tactics evolve, mimicking official websites to deceive visitors.

Threat 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: Execution T1064/T1129/T1203 - Persistence T1137 - Privilege Escalation T1055 - Defence Evasion T1027/T1036/TT1055/T1064/T1202/T1497 - Discovery T1010/T1082/T1083/T1497 - Command-and-Control T1071/T1095/T1573

2. DarkRadiation Ransomware

A new Bash ransomware named DarkRadiation caught our attention recently. It is a bash script-based attack, showing signs of ongoing development. Targeting Red Hat, CentOS, and sometimes Debian-based Linux systems, it uses Telegram's API for communication. The attack's components have low detection rates in VirusTotal. The "downloader.sh" worm spreads through weak passwords or keys, allowing the attacker to download and run ransomware. This ransomware deletes users, keeps the root user, and creates an account for the attacker. It encrypts files using OpenSSL's AES algorithm.

Threat Protected: 04
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: Execution T1064 - Persistence T1543.002 - Privilege Escalation T1055 - Defence Evasion T1055/T1064/T1070 - Discovery T1518.001 - Exfiltration T1048

3. GoBruteforcer Malware

GoBruteforcer is a newly discovered botnet malware written in Golang, designed to target web servers with services like phpMyAdmin, MySQL, FTP, and Postgres. It employs Classless Inter-Domain Routing (CIDR) block scanning to target multiple IP addresses within a network, providing the threat actor access to a broader range of hosts. After identifying a host, GoBruteforcer attempts to gain access through brute force and deploys an IRC bot with the attacker's URL upon successful entry. The malware also uses a PHP web shell to query the victim system, which is already present on the compromised server.

Threat 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: Execution T1059/T1064 - Persistence T1543.002 - Privilege Escalation T1543.002 - Defence Evasion T1027/T1064/T1070/T1564.001 - Discovery T1082/T1083 - Command-and-Control T1071/T1095

4. RisePro Stealer

RisePro, an information stealer similar to Vidar, operates by gathering sensitive data, including login credentials, credit card details, and personal information. Written in C++, it is distributed by threat actors using the PrivateLoader malware downloader, available for sale on Telegram. Cybercriminals commonly employ information stealers to extract valuable data through methods like keylogging and recording keyboard inputs. The infection typically starts with victims downloading PrivateLoader, often distributed through deceptive emails, malicious links, cracked software, or fake updates. This underscores the importance of cautious online behaviour to avoid falling victim to such malware threats.

Threat Protected: 10
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: Execution T1053 - Persistence T1053/T1547.001 - Privilege Escalation T1053/T1547.001 - Defence Evasion T1036/T1112/T1497/T1562.001 - Credential Access T1003/T1056 - Discovery T1010/T1012/T1016/T1018/T1057/T1082/T1083/T1497/T1518.001 - Collection T1005/T1056/T1114 - Command-and-Control T1071/T1571/T1573

5. Andariel APT

Recent research reports reveal the Lazarus Group's new campaign, dubbed "Operation Blacksmith," showcasing a shift in tactics. The North Korean APT group employs three new DLang-based malware families, including the Telegram-based RAT "NineRAT" and non-Telegram-based RAT "DLRAT," along with the DLang-based downloader "BottomLoader." This marks a notable evolution, with Lazarus Group adopting various uncommon technologies in RAT development over the past year and a half. The campaign, linked to the Andariel (PLUTONIUM) APT subgroup, targets enterprises globally, focusing on those exposing vulnerable infrastructure to exploits like CVE-2021-44228 (Log4j), impacting industries like manufacturing, agriculture, and physical security.

Threat Protected: 04
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: Execution T1064/T1129/T1569.002 - Persistence T1543.003/T1574.002 - Privilege Escalation T1543.003 - Defence Evasion T1027/T1027.005/T1036/T1064/T1202/T1497/T1497.001/T1574.002 - Discovery T1018/T1057/T1082/T1083/T1497 - Collection T1560 - Command-and-Control T1560/TA0011/T1071/T1095/T1102/T1573

6. FalseFont Backdoor

Recently a new campaign has been discovered targeting organisations in the Defence Industrial Base sector, carried out by an Iranian threat actor known as Peach Sandstorm (APT33, Elfin). The campaign introduces a new backdoor named FalseFont which was found in early November 2023. FalseFont enables remote access, file launches, and data transmission to command-and-control servers. This aligns with Peach Sandstorm's past activities, evolving its tactics. This group was previously linked to password spray attacks on global organisations from February to July 2023. The campaign seeks to aid Iranian state interests through intelligence collection, targeting sectors like defence, satellite, and pharmaceuticals.

Threat Protected: 03
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: Execution T1129 - Persistence T1543 - Privilege Escalation T1543.003 - Defence Evasion T1036/T1202/T1497/T1574.002 - Discovery T1018/T1497 - Collection T1560 -Command-and-Control T1560 /T1071 /T1573

Known exploited vulnerabilities (Week 2 January 2024):

Vulnerability	CVSS	Description
CVE-2023-23752	5.3 (Medium)	Joomla Improper Access Control Vulnerability
CVE-2016-20017	9.8 (Critical)	D-Link DSL-2750B Devices Command Injection Vulnerability
CVE-2023-41990	7.8 (High)	Apple Multiple Products Code Execution Vulnerability
CVE-2023-27524	9.8 (Critical)	Apache Superset Insecure Default Initialisation of Resource Vulnerability
CVE-2023-29300	9.8 (Critical)	Adobe ColdFusion Deserialisation of Untrusted Data Vulnerability
CVE-2023-38203	9.8 (Critical)	Adobe ColdFusion Deserialisation of Untrusted Data Vulnerability
CVE-2023-29357	9.8 (Critical)	Microsoft SharePoint Server Privilege Escalation Vulnerability
CVE-2023-46805	8.2 (High)	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability
CVE-2024-21887	9.1 (Critical)	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability

Updated Malware Signatures (Week 2 January 2024)

Threat	Description
Zeus	Also known as Zbot and is primarily designed to steal banking credentials.
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.
Trojan Miner	This malicious software installs and runs cryptocurrency mining applications.
XtremeRAT	A remote access trojan interacts with the infected machine via a remote shell, uploads/downloads files, and records from a webcam/microphone.

New Ransomware Victims Last Week: 43

Red Piranha proactively gathers information about organisations impacted by ransomware attacks through various channels, including the Dark Web. In the past week, our team identified a total of 43 new ransomware victims or updates in the few past victims from 19 distinct industries across 12 countries worldwide. This highlights the global reach and indiscriminate nature of ransomware attacks, which can affect organisations of all sizes and sectors.

LockBit3.0 ransomware group has affected the largest number of victims (9) spread across various countries. Akria and Alphv ransomware groups updated 6 victims each last week. Below are the victim counts (%) for these ransomware groups and a few others.

Name of Ransomware Group	Percentage of new Victims last week
8Base	6.98%
Akira	13.95%
Alphv	13.95%
Bianlian	4.65%
Black Suit	2.33%
Cactus	9.30%
Cloak	2.33%
Dragonforce	2.33%
Everest	2.33%
Inc Ransom	2.33%
Knight	2.33%
Lockbit3	20.93%
Medusa	4.65%
Play	2.33%
Qilin	6.98%
Rhysida	2.33%

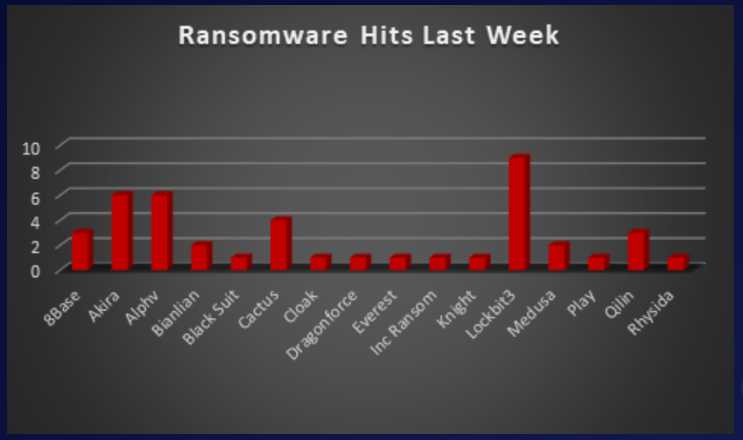

Figure 1: Ransomware Group Hits Last Week

When we examine the victims by country out of 12 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 23 victims updates last week. The list below displays the number (%) of new ransomware victims per country.

Name of the affected Country	Number of Victims
Australia	2.33%
Belgium	2.33%
Canada	18.60%
France	4.65%
Germany	2.33%
Malaysia	2.33%
Norway	2.33%
Singapore	2.33%
South Africa	4.65%
Spain	2.33%
Switzerland	2.33%
USA	53.49%

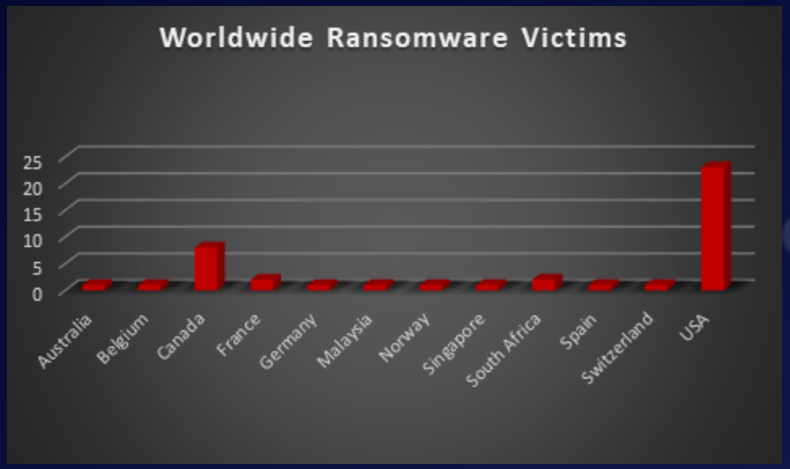

Figure 2: Ransomware Victims Worldwide

After conducting additional research, we found that ransomware has impacted 19 industries globally. Last week, the Manufacturing and Business Services sectors were hit particularly hard, with 18% and 11% of the total ransomware victims belonging to each of those sectors, respectively. The table below presents the most recent ransomware victims sorted by industry.

Industry	Victims Count (%)
Agriculture	2.33%
Business Services	11.63%
Construction	2.33%
Consumer Services	2.33%
Education	4.65%
Finance	4.65%
Government	2.33%
Healthcare	9.30%
Insurance	2.33%
IT	2.33%
Legal Services	6.98%
Manufacturing	18.60%
Media & Internet	2.33%
Metals & Mining	2.33%
Organisations	4.65%
Real Estate	2.33%
Retail	9.30%
Transportation	6.98%
Utilities & Waste Treatment	2.33%

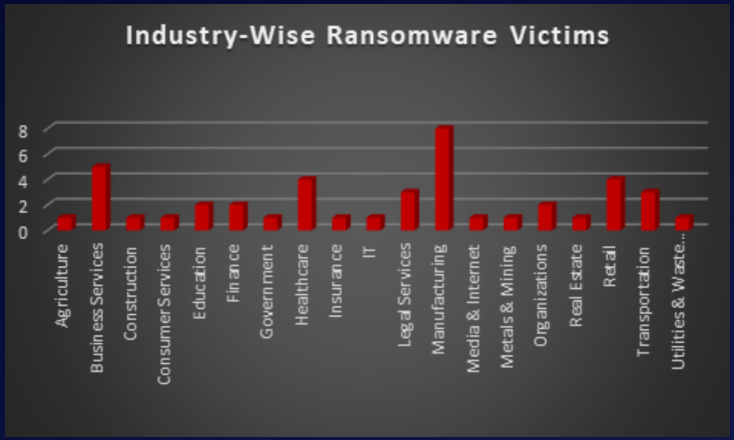

Figure 3: Industry-wise Ransomware Victims