Red Piranha
unified threat management

# THREAT INTELLIGENCE REPORT

Dec 26, 2023 - Jan 01, 2024

# Report Summary:

- **New Threat Detection Added** – 3 (TFlower Ransomware, YoroTrooper APT and BigLock Ransomware)
- **New Threat Protections - 9**
- **New Ransomware Victims Last Week - 47**

# Newly Detected Threats Added

## 1. TFlower Ransomware

The newly discovered TFlower ransomware is making waves in corporate environments by exploiting vulnerabilities in exposed Remote Desktop services. Unleashed in early August, TFlower takes advantage of the lucrative ransomware landscape targeting businesses. Attackers infiltrate networks through compromised Remote Desktop services, infecting local machines or attempting lateral movement using tools like PowerShell Empire or PSExec. The ransomware, while encrypting files without adding extensions, leaves a *tflower marker and seemingly encrypted encryption key. It disables Windows 10 repair features, terminates Outlook.exe, and demands the victim's contact through an email. The ransom amounts remain unknown.

**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/T1129 - Persistence T1547.001 - Privilege Escalation T1547.001 - Defence Evasion T1027/T1070/T1070.004 - Discovery T1057/T1083/T1518 - Impact T1490

## 2. YoroTrooper APT

YoroTrooper, an advanced persistent threat (APT) actor, has been active since June 2022, targeting government entities in Azerbaijan, Kyrgyzstan, Tajikistan, and other Commonwealth of Independent States (CIS) countries. Reports reveal the threat actor's likely origin in Kazakhstan, evidenced using the Kazakh currency and languages. Despite primarily targeting institutions in CIS countries, YoroTrooper seems motivated by Kazakh state interests. The APT employs various tactics, including compromising websites, spear-phishing, and utilizing custom-built Python and Rust-based implants.

**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 T1047/T1059/T1106/T1129 - Persistence T1574.002 - Privilege Escalation T1055 - Defence Evasion T1027/T1036/T1055/T1497 - Credential Access T1003 - Discovery T1016/T1018/T1082 - Lateral Movement T1080 - Collection T1005 - Command-and-Control T1071/T1095/T1102.

## 3. BigLock Ransomware

BigLock, also known as 'corona-lock,' is a ransomware discovered in 2020. It employs chacha and AES encryption to encrypt files, appending the extension '.corona-lock' to all affected files. The ransomware capitalizes on the COVID-19 pandemic, spreading through malicious documents with names like 'CORONA TREATMENT.doc,' distributed via email attachments with subject lines such as 'Corona Virus Cure for China or Italy.' Upon execution, the malware modifies registry entries, injects malicious code into boot-up files, and drops a ransom note named 'README_LOCK.txt' on the desktop and other folders.

**Threat Protected:** 05
**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:** Initial Access T1059 - Execution T1204 - Persistence T1547/T1112 - Defence Evasion T1497/T1055 - Discovery T1082 - Impact T1486

## Known exploited vulnerabilities (Week 4 December 2023):

| Vulnerability | CVSS | Description |
|---|---|---|
| CVE-2023-49070 | 9.8 Critical | Apache OFBiz Remote Code Execution vulnerability |

## Updated Malware Signatures (Week 4 December 2023)

| 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: 47

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 47 new ransomware victims or updates in the few past victims from 19 distinct industries across 15 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 14 victims' updates spread across various countries. Alphv and Cactus ransomware groups updated 7 and 6 new victims, respectively. Below are the victim counts (%) for these ransomware groups and a few others.

| Name of Ransomware Group | Percentage of new Victims last week |
|---|---|
| 8Base | 4.26% |
| Akira | 2.13% |
| Alphv | 14.89% |
| Bianlian | 4.26% |
| Black Suit | 2.13% |
| Blackbasta | 2.13% |
| Cactus | 12.77% |
| Dragonforce | 2.13% |
| Lockbit3 | 29.79% |
| Malek Team | 8.51% |
| Meow | 2.13% |
| Play | 2.13% |
| Qilin | 2.13% |
| Rhysida | 4.26% |
| Stormous | 2.13% |
| Werewolves | 4.26% |

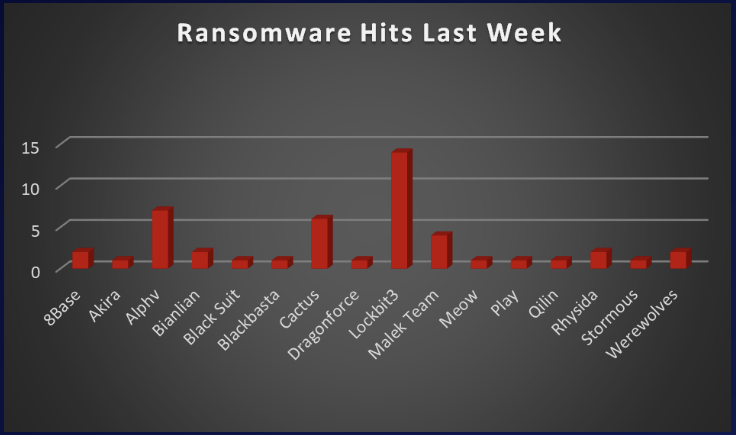

*Figure 1: Ransomware Group Hits Last Week*

When we examine the victims by country out of 15 countries around the world, we can conclude that the USA was once again the most ransomware-affected country, with a total of 26 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 | 2.13% |
| Canada | 8.51% |
| France | 2.13% |
| Israel | 6.38% |
| Jordan | 2.13% |
| Mexico | 4.26% |
| Netherlands | 2.13% |
| Romania | 2.13% |
| Russia | 4.26% |
| Serbia | 2.13% |
| South Africa | 2.13% |
| Switzerland | 2.13% |
| UK | 2.13% |
| USA | 55.32% |
| Uzbekistan | 2.13% |

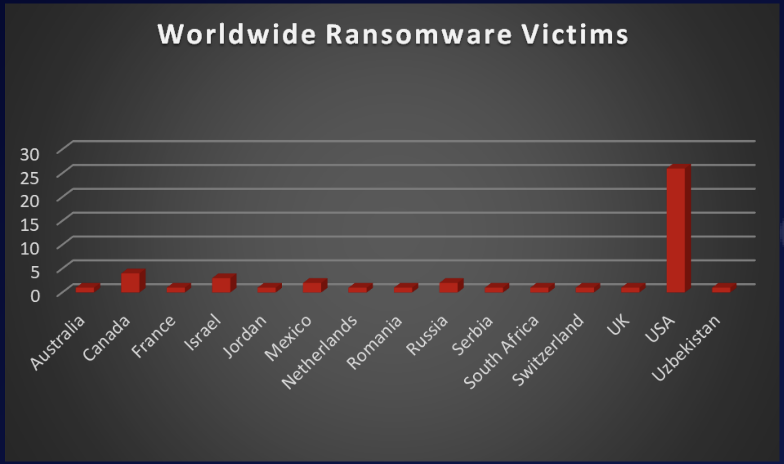

*Figure 2: Ransomware Victims Worldwide*

After conducting additional research, we found that ransomware has impacted 19 industries globally. Last week, the Manufacturing and Retail sectors were hit particularly hard, with 14% and 10% 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 | 2.13% |
| Business Services | 8.51% |
| Cities, Towns & Municipalities | 2.13% |
| Construction | 8.51% |
| Consumer Services | 6.38% |
| Education | 6.38% |
| Energy, Utilities & Waste Treatment | 2.13% |
| Finance | 2.13% |
| Government | 4.26% |
| Healthcare | 6.38% |
| Hospitality | 4.26% |
| IT | 4.26% |
| Legal Services | 6.38% |
| Manufacturing | 14.89% |
| Media & Internet | 4.26% |
| Organisations | 2.13% |
| Real Estate | 2.13% |
| Retail | 10.64% |
| Telecom | 2.13% |

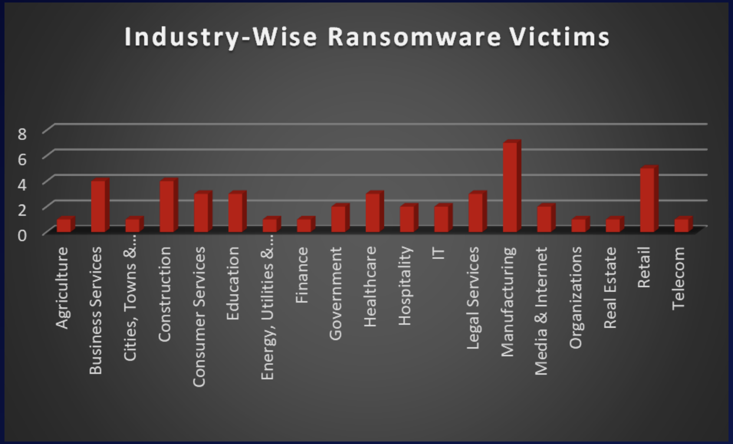

*Figure 3: Industry-wise Ransomware Victims*