Red Piranha
unified threat management

# THREAT INTELLIGENCE REPORT

Feb 20 - 26, 2024

# Report Summary:

- **New Threat Detection Added** – 4 (TFlower Ransomware, Java Rat Malware, Havex RAT and ConnectWise ScreenConnect (CVE-2024-1709, CVE-2024-1708))
- **New Threat Protections - 180**
- **New Ransomware Victims Last Week - 66**

# Newly Detected Threats Added

## 1. TFlower Ransomware

The TFlower ransomware has become a notable threat within corporate environments, particularly exploiting vulnerabilities found in exposed Remote Desktop services. Launched in early August 2023, TFlower capitalises on the profitable landscape of ransomware attacks targeted at businesses. The modus operandi involves infiltrating networks through compromised Remote Desktop services, subsequently infecting local machines. The attackers may also attempt lateral movement using tools such as PowerShell Empire or PSExec. Notably, the ransomware encrypts files without adding extensions but leaves behind a distinct *tflower marker and an apparently encrypted encryption key. TFlower takes additional measures to disrupt systems, disabling Windows 10 repair features and terminating Outlook.exe. The attackers then demand the victim's contact through an email for further communication. As of now, the specific ransom amounts remain unknown, adding an element of uncertainty to the severity of the threat. Organisations are advised to remain vigilant and take necessary precautions to safeguard against this evolving ransomware menace.

**Rules Created:** 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:**

| Tactic | Technique ID | Technique Name |
|---|---|---|
| Execution | T1059<br>T1129 | Command and Scripting Interpreter<br>Shared Modules |
| Persistence | T1547.001 | Registry Run Keys / Startup Folder |
| Privilege Escalation | T1547.001 | Registry Run Keys / Startup Folder |
| Defence Evasion | T1027<br>T1027.005<br>T1070<br>T1070.004 | Obfuscated Files or Information<br>Indicator Removal from Tools<br>Indicator Removal<br>File Deletion |
| Discovery | T1057<br>T1082 | Process Discovery<br>System Information Discovery |
| Impact | T1490 | Inhibit System Recovery |

## 2. Java Rat Malware

Java Rat is a sophisticated remote administration tool implemented in Java, enabling the rapid extraction of information from a large array of computers. This program not only serves as a means to enhance our foundational comprehension of network programming but also results in the creation of a powerful tool with practical applicability in real-world scenarios. Specifically designed as a Remote Administration Tool (RAT), Java Rat establishes a connection with a Command-and-Control Server (CNC Server). Through this centralised server, users gain the capability to dispatch commands or requests to individual clients and receive corresponding responses. These commands could range from requesting files, querying the operating system version, or soliciting other pertinent information. Functioning as a two-way communication channel, the RAT executes designated actions on the host machine and subsequently transmits the acquired data back to the CNC server upon completion. This robust tool not only facilitates efficient remote administration but also showcases the potential for versatile applications in diverse operational environments.

**Rules Created:** 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:**

| Tactic | Technique ID | Technique Name |
|---|---|---|
| Execution | T1064 | Scripting |
| Persistence | T1543.002 | Systemd Service |
| Privilege Escalation | T1543.002 | Systemd Service |
| Defence Evasion | T1064<br>T1070<br>T1564.001 | Scripting<br>Indicator Removal<br>Hidden Files and Directories |
| Discovery | T1082<br>T1083 | System Information Discovery<br>File and Directory Discovery |
| Command-and-Control | T1071<br>T1095 | Application Layer Protocol<br>Non-Application Layer Protocol |

## 3. Havex RAT

Havex, a remote access trojan (RAT) identified in 2013, emerged within a broad-reaching espionage initiative aimed at industrial control systems (ICS). Attributed to the hacking groups "Dragonfly" and "Energetic Bear," Havex left a significant impact, affecting numerous infrastructure sites, particularly in Europe and the United States. Focusing on the energy sector, it targeted energy grid operators, major electricity generation firms, petroleum pipeline operators, and industrial equipment providers. Beyond energy, its reach extended to aviation, defence, pharmaceutical, and petrochemical industries. Upon infiltration, Havex systematically scanned infected systems for Supervisory Control and Data Acquisition (SCADA) or ICS devices, transmitting the acquired data to command-and-control servers. Leveraging the Open Platform Communications (OPC) standard, a universal protocol in ICS, and utilising the Distributed Component Object Model (DCOM) to connect to OPC servers, Havex gathered critical information such as CLSID, server details, Program ID, OPC version, vendor specifics, running state, group count, and server bandwidth. Despite being an intelligence-collection tool for espionage, Havex did not disrupt or destroy industrial systems. Instead, the harvested data served to inform and enhance the design of targeted attacks against specific entities or industries.

**Rules Created:** 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:** Attempted-Admin

**Kill Chain:**

| Tactic | Technique ID | Technique Name |
|---|---|---|
| Execution | T1129 | Shared Modules |
| Persistence | T1547.001 | Registry Run Keys / Startup Folder |
| Defence Evasion | T1027<br>T1070 | Obfuscated Files or Information<br>Indicator Removal |
| Discovery | T1057<br>T1082 | Process Discovery<br>System Information Discovery |

## 4. ConnectWise ScreenConnect (CVE-2024-1709, CVE-2024-1708)

CVE-2024-1709 enables anonymous attackers to leverage an authentication bypass vulnerability for the creation of admin accounts on publicly accessible instances. This vulnerability could allow malicious actors to impersonate system administrators, eliminate all other users, and seize control of the instance.

**Rules Created:** 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:** Attempted-admin
**Kill Chain:**

| Tactic | Technique ID | Technique Name |
|---|---|---|
| Initial Access | T1190 | Exploit Public-Facing Application |

## Known exploited vulnerabilities (Week 4 February 2024):

| Vulnerability | CVSS | Description |
|---|---|---|
| CVE-2024-1709 | 10.0 (Critical) | ConnectWise ScreenConnect Authentication Bypass Vulnerability |

## Updated Malware Signatures (Week 4 February 2024)

| Threat | Description |
|---|---|
| Bifrost | A remote access trojan that enables its operator to take control of a victim machine and steal data. It is usually distributed through spam and phishing emails. |
| CoinMiner | This malicious software installs and runs cryptocurrency mining applications. |
| Nanocore | The Nanocore trojan, built on the .NET framework, has been the subject of multiple source code leaks, resulting in its widespread accessibility. Similar to other remote access trojans (RATs), Nanocore empowers malicious actors with complete system control, enabling activities such as video and audio recording, password theft, file downloads, and keystroke logging. |
| 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. |

## New Ransomware Victims Last Week: 66

The Red Piranha Team actively collects information on organisations globally affected by ransomware attacks from various sources, including the Dark Web. In the past week alone, our team uncovered a total of 66 new ransomware victims or updates on previous victims across 19 different industries spanning 17 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

Hunters ransomware group stands out as the most prolific, having updated a significant number of victims (12) distributed across multiple countries. In comparison, Black Basta and Alphv ransomware groups updated 9 and 7 victims, respectively, in the past week. The following list provides the victim counts in percentages for these ransomware groups and a selection of others.

| Name of Ransomware Group | Percentage of new Victims last week |
|---|---|
| 3Am | 4.55% |
| 8Base | 6.06% |
| Akira | 7.58% |
| Alphv | 10.61% |
| Bianlian | 4.55% |
| Blackbasta | 13.64% |
| Cactus | 7.58% |
| Dragonforce | 3.03% |
| Everest | 1.52% |
| Hunters | 18.18% |
| Lockbit3 | 9.09% |
| Medusa | 3.03% |
| Meow | 1.52% |
| Mogilevich | 1.52% |
| Qilin | 1.52% |
| Snatch | 1.52% |
| Stormous | 1.52% |
| Trisec | 3.03% |

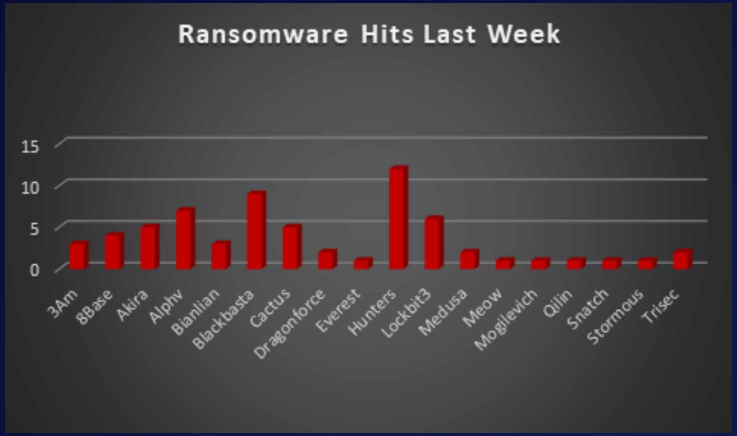

*Figure 1: Ransomware Group Hits Last Week*

In a comprehensive analysis of ransomware victims across 17 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 40 victim updates in the past week. The following list provides a breakdown of the number and percentage of new ransomware victims per country, underscoring the persistent and concerning prevalence of ransomware attacks, with the USA particularly susceptible to these cybersecurity threats.

| Name of the affected Country | Number of Victims |
|---|---|
| Australia | 3.03% |
| Belgium | 1.52% |
| Brazil | 1.52% |
| Canada | 3.03% |
| Chile | 1.52% |
| Florida | 1.52% |
| France | 3.03% |
| Germany | 1.52% |
| Ireland | 3.03% |
| Italy | 3.03% |
| Poland | 1.52% |
| Spain | 1.52% |
| Sweden | 1.52% |
| Switzerland | 1.52% |
| UAE | 1.52% |
| UK | 7.58% |
| USA | 62.12% |

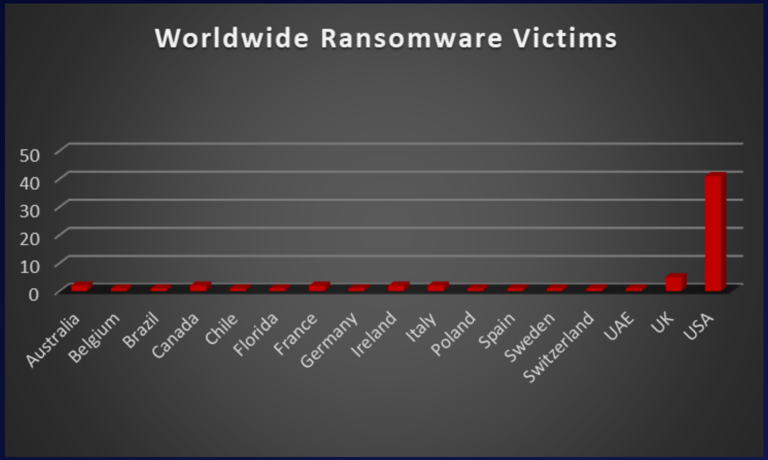

*Figure 2: Ransomware Victims Worldwide*

Upon further investigation, it has been identified that ransomware has left its mark on 19 different industries worldwide. Notably, the Manufacturing and Retail sectors bore the brunt of the attacks in the past week, accounting for 16 and 7 victims respectively. The table below delineates the most recent ransomware victims, organised by industry, shedding light on the sectors grappling with the significant impact of these cyber threats.

| Industry | Victims Count (%) |
|---|---|
| Business Services | 9.09% |
| Construction | 7.58 % |
| Consumer Services | 7.58% |
| Education | 6.06% |
| Energy, Utilities & Waste Treatment | 1.52% |
| Finance | 6.06% |
| Government | 1.52% |
| Healthcare | 6.06% |
| Hospitality | 1.52% |
| Insurance | 1.52% |
| IT | 3.03% |
| Legal Services | 1.52% |
| Manufacturing | 24.24% |
| Media & Internet | 1.52% |
| Organisations | 1.52% |
| Real Estate | 4.55% |
| Retail | 10.61% |
| Telecom | 3.03% |
| Transportation | 1.52% |

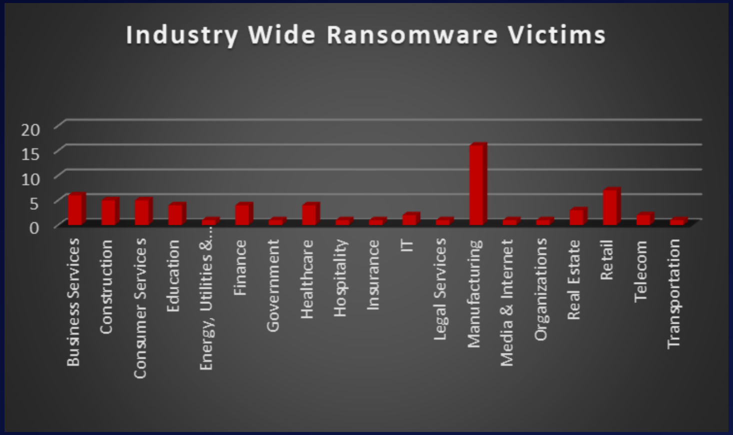

*Figure 3: Industry-wide Ransomware Victims*