Red Piranha
unified threat management

# THREAT INTELLIGENCE REPORT

Jan 23 - 29, 2024

# Report Summary:

- **New Threat Detection Added** – 4 (KEKW Python Stealer, Atomic Stealer, ScarCruft APT and Atlassian Confluence CVE-2023-22527)
- **New Threat Protections - 237**
- **New Ransomware Victims Last Week - 111**

# Newly Detected Threats Added

## 1. KEKW Python Stealer

PyPI (Python Package Index) serves as a vital hub for Python developers globally, enabling code sharing and distribution. Unfortunately, its popularity makes it an attractive target for Threat Actors (TAs). TAs exploit PyPI by uploading malicious packages, disguising them as legitimate software or mimicking well-known projects. Recently, Researchers identified malicious Python .whl files distributing a new malware named KEKW. This malware not only steals sensitive information but also engages in clipper activities, potentially hijacking cryptocurrency transactions.

**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:**

| Tactic | Technique ID | Technique Name |
|---|---|---|
| Execution | T1204 | User Execution |
|  | T1047 | Windows Management Instrumentation |
| Persistence | T1547 | Registry Run Keys / Startup Folder |
| Defence Evasion | T1497 | Virtualisation/Sandbox Evasion |
|  | T1562 | Disable or Modify Tools |
| Credential Access | T1056 | Credential API Hooking |
| Discovery | T1057 | Process Discovery |
|  | T1012 | Query Registry |
|  | T1082 | System Information Discovery |
|  | T1083 | File and Directory Discovery |
| Collection | T1005 | Data from Local System |
| Command-and-Control | T1071 | Application Layer Protocol |

## 2. Atomic Stealer

Atomic Stealer (AMOS), a popular Mac-targeting stealer, underwent an update introducing payload encryption to evade detection. Prolific in malvertising and compromised sites, AMOS developers justified its $3000/month rental fee with continuous enhancements. A January 2024 malvertising campaign revealed the updated version, potentially accessed by customers through software cracks. Despite a holiday slowdown in malvertising, a renewed campaign featured AMOS's updated variant. As Mac users face persistent threats, caution in downloading software from reputable sources is crucial, given the deceptive nature of malicious ads. Reported incidents to relevant parties aim for prompt mitigation.

**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:**

| Tactic | Technique ID | Technique Name |
|---|---|---|
| Execution | T1059.002<br>T1064 | AppleScript<br>Scripting |
| Persistence | T1547.011 | Plist Modification |
| Privilege Escalation | T1547.011 | Plist Modification |
| Defence Evasion | T1064<br>T1070<br>T1070.004<br>T1564.001 | Scripting<br>Indicator Removal<br>File Deletion<br>Hidden Files and Directories |
| Discovery | T1082 | System Information Discovery |
| Command-and-Control | T1071<br>T1095<br>T1573 | Application Layer Protocol<br>Non-Application Layer Protocol Performs DNS lookups.<br>Encrypted Channel Uses HTTPS |

## 3. ScarCruft APT

ScarCruft, also known as APT37 and InkySquid, is a suspected North Korean cyber threat group. They are currently in the planning and testing stages, using a technical threat research report on Kimsuky as a decoy. ScarCruft focuses on gathering insights from technical threat intelligence consumers, aiming to refine their operational approaches. Their use of oversized Windows Shortcut files in infection chains, delivering the RokRAT backdoor, demonstrates their advanced tactics. By targeting high-profile North Korean affairs experts, ScarCruft aligns with its goal of strategic intelligence gathering, contributing to North Korea's decision-making. The group's interest in mimicking cybersecurity professionals suggests a growing threat landscape with potential implications for specific targets and brand impersonation.

**Threat Protected:** 32
**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<br>T1203 | Scripting<br>Exploitation for Client Execution |
| Defence Evasion | T1036<br>T1064 | Masquerading<br>Scripting |
| Discovery | T1082<br>T1083 | System Information Discovery<br>File and Directory Discovery |
| Command-and-Control | T1071<br>T1095<br>T1105 | Application Layer Protocol<br>Non-Application Layer Protocol Performs DNS lookup<br>Ingress Tool Transfer |

## 4. Atlassian Confluence RCE (CVE-2023-22527)

A template injection vulnerability present in earlier versions of Confluence Data Center and Server enables an unauthorised attacker to execute remote code on a compromised instance.  The most recent supported iterations of Confluence Data Centre and Server remain unaffected, as the vulnerability was successfully addressed in routine version updates. Nevertheless, Atlassian advises customers to prioritise installing the latest version to safeguard their instances against non-critical vulnerabilities highlighted in the January Security Bulletin.

**Threat Protected:** 1
**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 January 2024):

| Vulnerability | CVSS | Description |
|---|---|---|
| CVE-2023-34048 | 9.8 (Critical) | VMware vCenter Server Out-of-Bounds Write Vulnerability |
| CVE-2023-22527 | 9.8 (Critical) | Atlassian Confluence Data Centre and Server Template Injection Vulnerability |

## Updated Malware Signatures (Week 4 January 2024)

| Threat | Description |
|---|---|
| Valyria | A Microsoft Word-based malware which is used as a dropper for second-stage malware. |
| LokiBot | An information-stealer malware used to gather data from victims' machines such as stored account credentials, banking information and other personal data. |
| CoinMiner | This malicious software installs and runs cryptocurrency mining applications. |
| 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: 111

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 111 new ransomware victims or updates on previous victims across 21 different industries spanning 21 countries. This underscores the widespread and indiscriminate impact of ransomware attacks, emphasising their potential to affect organisations of varying sizes and sectors worldwide.

LockBit 3.0 ransomware group stands out as the most prolific, having updated a significant number of victims (27) distributed across multiple countries. In comparison, Blackbasta and Akira ransomware groups updated 13 and 9 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 |
|---|---|
| 0Mega | 0.90% |
| 8Base | 7.21% |
| Abyss data | 0.90% |
| Akira | 8.11% |
| Alphv | 6.31% |
| Bianlian | 4.50% |
| Blackbasta | 11.71% |
| Cactus | 1.80% |
| Cuba | 0.90% |
| Hunters | 6.31% |
| Inc Ransom | 1.80% |
| Lockbit3 | 24.32% |
| Medusa | 5.41% |
| Meow | 0.90% |
| Money Message | 0.90% |
| Monti | 0.90% |
| Mydata | 7.21% |
| Play | 0.90% |
| Qilin | 2.70% |
| Ransomhouse | 1.80% |
| Trigona | 4.50% |

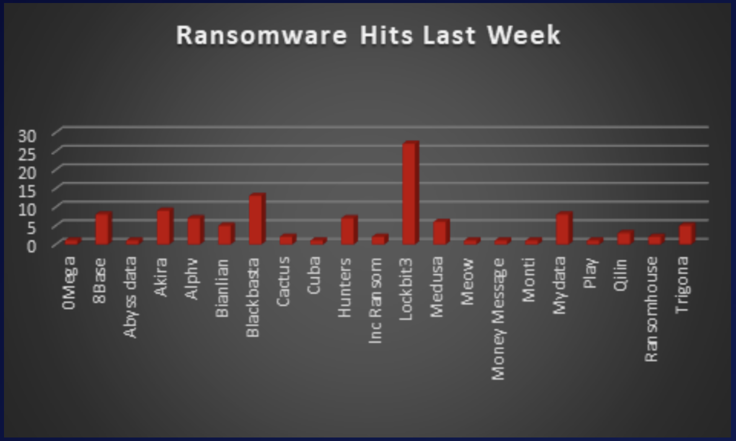

*Figure 1: Ransomware Group Hits Last Week*

As you read above, LockBit3.0 has emerged as one of the most dangerous ransomware strains, affecting the highest number of victims globally. Take a moment to delve into the dark history and the profound impact that the LockBit3.0 ransomware group has had:

LockBit3.0, also known as LockBit Black, stands out as a highly dangerous ransomware that has inflicted widespread damage on a global scale. Its history unfolds with the emergence of the original LockBit in 2016, initially a basic but effective ransomware. By 2019, LockBit 2.0 arrived, featuring enhanced encryption and a focus on larger organisations.

A significant shift occurred in 2020 when LockBit transformed into a Ransomware-as-a-Service (RaaS) model, allowing anyone to launch ransomware attacks through its platform. This evolution marked a turning point, granting widespread access to LockBit and amplifying its threat level. In 2022, LockBit3.0, or LockBit Black, made its debut, introducing increased modularity, evasion tactics, and customisation, making detection and prevention more challenging.

LockBit3.0 has left a trail of disruption across critical sectors, impacting hospitals, schools, and government agencies. In 2021, it notably crippled the Colonial Pipeline, leading to significant fuel disruptions in the US. Even manufacturing giants like CISA and Samsung have fallen victim to LockBit's powerful encryption.

Efforts are underway globally to dismantle LockBit and its operators, with companies investing heavily in defence measures. Despite these endeavours, LockBit3.0 remains a persistent threat. Its RaaS model ensures constant evolution, posing an ongoing challenge for the cybersecurity community. Staying vigilant and implementing robust security practices are crucial to confront this ever-growing and evolving cyber threat.

In a comprehensive analysis of ransomware victims across 21 countries, the United States emerges as the most heavily impacted nation, reporting a staggering 56 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 | 2.70% |
| Austria | 0.90% |
| Bavaria | 0.90% |
| Belgium | 1.80% |
| Brazil | 0.90% |
| Canada | 4.50% |
| France | 7.21% |
| Germany | 1.80% |
| Indiana | 0.90% |
| Indonesia | 0.90% |
| Italy | 2.70% |
| Japan | 0.90% |
| Malaysia | 0.90% |
| Mexico | 0.90% |
| New Zealand | 0.90% |
| Sweden | 0.90% |
| Taiwan | 3.60% |
| Thailand | 2.70% |
| UAE | 2.70% |
| UK | 10.81% |
| USA | 50.45% |

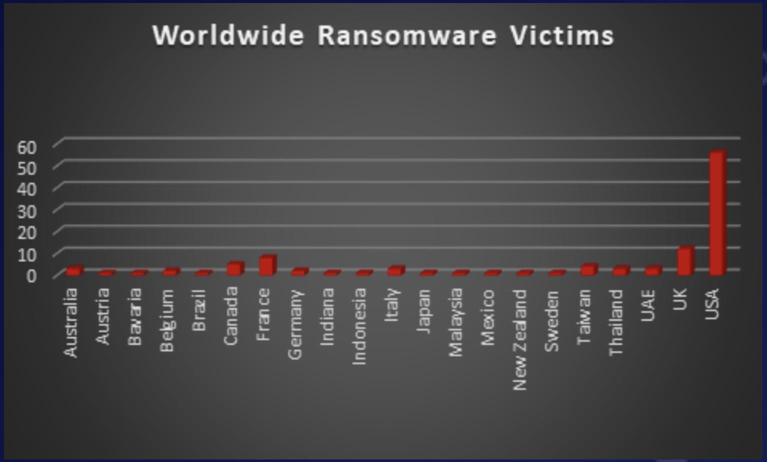

*Figure 2: Ransomware Victims Worldwide*

Upon further investigation, it has been identified that ransomware has left its mark on 21 different industries worldwide. Notably, the Manufacturing and Retail sectors bore the brunt of the attacks in the past week, accounting for 21% and 10% of the total ransomware 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 (%) |
|---|---|
| Agriculture | 0.90% |
| Business Services | 8.11% |
| Construction | 8.11% |
| Consumer Services | 2.70% |
| Education | 3.60% |
| Energy, Utilities & Waste Treatment | 3.60% |
| Finance | 6.31% |
| Government | 0.90% |
| Healthcare | 4.50% |
| Hospitality | 6.31% |
| Insurance | 1.80% |
| IT | 1.80% |
| Legal Services | 4.50% |
| Manufacturing | 21.62% |
| Media & Internal | 1.80% |
| Metals & Mining | 0.90% |
| Organisations | 5.41% |
| Real Estate | 0.90% |
| Retail | 10.81% |
| Telecom | 0.90% |
| Transportation | 4.50% |

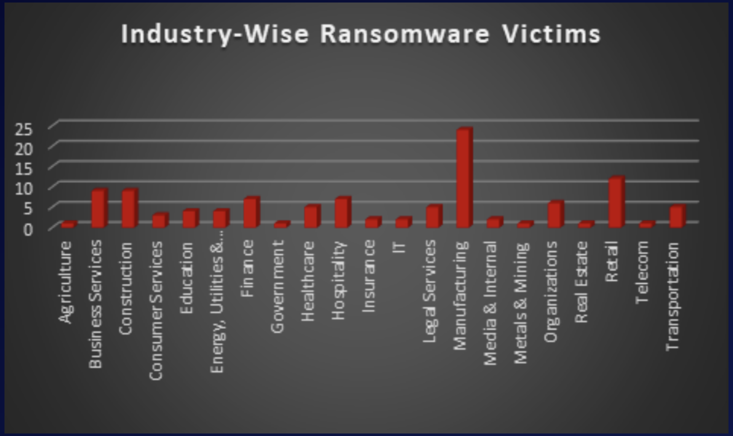

*Figure 3: Industry-wise Ransomware Victims*