Date of Publication
March 6, 2023

Hive Pro

Hiveforce Labs

WEEKLY

# THREAT DIGEST

## Actors, Attacks, and Vulnerabilities

27 FEBRUARY to 5 MARCH 2023

# Summary

## Threat Actors

HiveForce Labs discovered **six** actors that have been active in the past week. **TA866**, **APT-C-61**, and **DEV-0569** are cybercrime groups that focus on Financial gain. The other three Chinese-based actors are **Blackfly**, **Iron Tiger**, and **Mustang Panda APT** is well-known for their information theft and espionage capabilities. For further details, see the key takeaway section for Actors.

## Attacks

We also discovered **13** new malware strains that have been active over the past week. One of them was an Information stealer: **Rhadamanthys**. We discovered two new malware strains called **SysUpdate** and **SCARLETEEL**. Additionally, two were classified as backdoors: **Winnkit** and **MQsTTang.** Three Trojans: **AgentTesla**, **An unknown Trojan,** and **ParallaxRAT.** We also identified three strains of ransomware: **Maui** and **H0lyGh0st**, **Royal Ransomware,** and **Exfiltrator-22.** Finally, Two Crypters: **PureCrypter** and **Snip3 Crypter.** For further details, see the key takeaway section for Attacks.

## Vulnerabilities

Last week, we discovered **six** vulnerabilities that organizations should prioritize. **One** Zero-day vulnerability along with **two** other flaws was exploited by Malicious DPRK Actors. The remaining **three** vulnerabilities affected Apple macOS Ventura allowing attackers to elevate privileges and execute unauthorized code execution. For further details, see the key takeaway section on vulnerabilities.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

# Key Takeaways

## Threat Actors

**TA866 (AHKBot and Rhadamanthys Stealer)**
A new financially motivated threat actor named TA866 has been active since October 2022 and targets organizations in the United States and Germany. The attack chain starts with a malicious email containing an attachment or URL, leading to the installation of WasabiSeed and Screenshotter.

**Blackfly (Winnkit)**
The Blackfly Chinese espionage group, which has been active since at least 2010, has been targeting multiple subsidiaries of an Asian conglomerate operating in the materials and composites sector. The group's most recent activity shows that it has been relying on open-source tools rather than its custom malware, which helps it avoid detection and attribution.

**Iron Tiger (SysUpdate)**
Iron Tiger is a widely recognized Chinese APT group that mainly participates in cyber espionage. In 2022, the group enhanced its custom malware, SysUpdate, by adding new features and support for Linux platforms. The loading process of the malware is intricate, which may suggest an effort to avoid detection by security solutions.

**APT-C-61 (unattributed)**
APT-C-61, also known as Tengyun Snake, is an APT group that has been active in South Asia since January 2020. The group utilizes social engineering tactics and spear-phishing emails to disseminate malware onto targeted devices. The Trojan utilized by the group is coded in Python.

**Mustang Panda APT (MQsTTang)**
The Mustang Panda APT group has developed a new custom backdoor known as MQsTTang, used in an ongoing campaign that began in early January 2023. The targets of this campaign appear to be political and governmental organizations. MQsTTang appears to be distinct from most of the group's malware, as it is not based on existing families or publicly available projects.

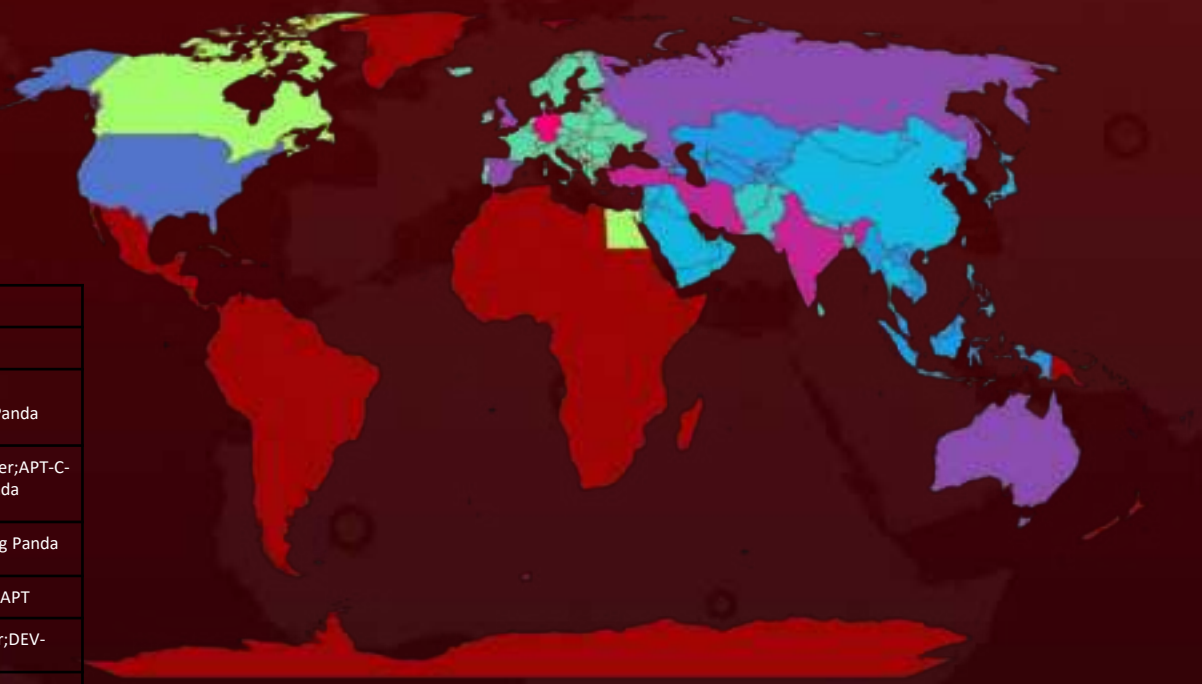
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

# Key Takeaways

**DEV-0569 (Royal Ransomware)**

DEV-0569 threat actors have been utilizing Royal ransomware to attack American and international companies since September 2022. This ransomware is distinct in that it uses a custom-made file encryption tool. Additionally, it employs double extortion tactics, which involve threatening to publicly expose encrypted data if the victim does not pay a ransom in Bitcoin ranging from $1 million to $11 million.

## Actor Map



| Color | Targeted By |
|---|---|
| | Iron Tiger |
| | Blackfly;Iron Tiger;Mustang Panda APT;DEV-0569 |
| | Blackfly;Iron Tiger;APT-C-61;Mustang Panda APT;DEV-0569 |
| | Blackfly;Mustang Panda APT;DEV-0569 |
| | Mustang Panda APT |
| | TA866;Iron Tiger;DEV-0569 |
| | Iron Tiger;Mustang Panda APT;DEV-0569 |
| | TA866;Iron Tiger;Mustang Panda APT;DEV-0569 |

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

# Key Takeaways

## Actor Details

| ICON | NAME | ORIGIN | MOTIVE |
|---|---|---|---|
|  | TA866 | Unknown | Financial gain |
|  | Blackfly (APT 41, Double Dragon, TG-2633, Bronze Atlas, Red Kelpie, Earth Baku, SparklingGoblin ,Grayfly) | China | Information theft and espionage |
|  | Iron Tiger (APT 27, Emissary Panda, LuckyMouse, Bronze Union, TG-3390, TEMP.Hippo, Budworm, Group 35, ATK 15, Earth Smilodon, Red Phoenix, ZipToken) | China | Information theft and espionage |
|  | APT-C-61 (Tengyun Snake) | Unknown | Information Theft and espionage |
|  | Mustang Panda APT (Bronze President, TEMP.Hex, HoneyMyte, Red Lich, EarthPreta) | China | Information theft and espionage |
|  | DEV-0569 | Unknown | Financial gain |

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

# Key Takeaways

## Attacks

**PureCrypter Downloader(unattributed)**

Government institutions have been targeted by an unknown perpetrator who is using Discord to distribute a deceptive threat campaign. This campaign uses PureCrypter downloader and a hacked non-profit organization's domain as Command and Control (C2) to deliver a secondary payload. Various malware, such as RedlineStealer, AgentTesla, Eternity, Blackmoon, and Philadelphia Ransomware, are disseminated through this campaign.

**Exfiltrator-22 Ransomware Framework (unattributed)**

The developers of a new post-exploitation framework called EXFILTRATOR-22, also known as EX-22, are selling it as a subscription-based service. A lifetime subscription costs $5,000, and the monthly subscription fee is $1,000. The threat actors who created the framework have used domain fronting to conceal its command-and-control traffic. Moreover, similarities have been discovered between a LockBit 3.0 sample that has been actively used in LockBit 3.0 campaigns and EX-22.

**AgentTesla Trojan(unattributed)**

Attackers have been using GuLoader to deliver the AgentTesla Trojan in a new round of phishing attacks, as the AgentTesla Trojan has remained active since February of this year. GuLoader is used to load other malicious files and employs various obfuscation and anti-reverse analysis techniques to evade detection by security products. The final payload is the AgentTesla Trojan, which is a commercial .NET-based Trojan that steals secrets through functions such as keylogging, screen capture, and password theft.

**AHKBot and Rhadamanthys Stealer (TA866)**

The attack chain commences with a malevolent email containing an attachment or URL, resulting in the installation of WasabiSeed and Screenshotter. TA866 is a well-organized actor capable of executing attacks on a large scale using custom tools and buying tools and services from other vendors. The threat actor inspects the screenshots manually and installs additional payloads for the WasabiSeed loop to download, such as AHKBot and Rhadamanthys Stealer.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

# Key Takeaways

**Maui and H0lyGh0st Ransomware (DPRK)**
DPRK actors utilize a variety of exploits of common vulnerabilities and exposures (CVE) to obtain access and escalate privileges. They deploy staged payloads with tailored malware to do reconnaissance, upload and download additional files and executables, and run shell commands. They also use ransomware such as Maui and H0lyGh0st, as well as publicly available encryption tools, and demand ransom in cryptocurrency, primarily bitcoin.

**Winnkit Backdoor (Blackfly)**
The current activity of the Blackfly espionage group demonstrates that it has been depending on open-source tools rather than its normal bespoke software Winnkit Backdoor, which helps it evade detection and attribution. The group's technical competence has remained stable, and it has been continually renewing its tool set in order to avoid detection.

**SCARLETEEL attack (unattributed)**
The SCARLETEEL operation was a sophisticated cloud operation that involved stealing sensitive data by exploiting a misconfigured Kubernetes container, gaining access to one AWS account, and attempting to pivot to additional associated AWS accounts.

**ParallaxRAT (unattributed)**
ParallaxRAT is a type of malware that focuses on attacking cryptocurrency organizations via phishing emails. It carries out numerous malicious activities, including keylogging and remote control of affected machines. Specifically, it gains unauthorized access to files, captures keystrokes, and takes control of the remote desktop.

**SysUpdate (Iron Tiger)**
The Iron Tiger APT group modified their malware, SysUpdate, to target Linux platforms and avoid detection. They used a sophisticated loading mechanism and novel C&C communication via DNS TXT queries to precisely target a vulnerability in a Wazuh-signed program.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

# Key Takeaways

**Unknown Trojan (APT-C-61)**
APT-C-61 uses social engineering techniques and spear-phishing emails to infect victim devices. They also use cloud services for C2 infrastructure, load delivery, and stolen data storage. The Trojan used by this gang is a piece of malware written in Python.

**Snip3 Crypter (unattributed)**
Snip3 crypter, a multi-stage remote access trojan (RAT) loader, was recently identified distributing RAT families such as QuasarRAT and DcRAT to target victims across numerous industry verticals, and the crypter has been updated with advanced approaches that allow it to deploy the final Remote Access Trojan (RAT) payload while remaining undetected.

**MQsTTang Backdoor (Mustang Panda APT)**
MQsTTang is a basic backdoor associated with the Mustang Panda APT organization. It communicates over the MQTT protocol and is transmitted via spear phishing through RAR archives with names relating to diplomacy and passports. For C&C communication, this backdoor uses the MQTT protocol. While MQTT is commonly used for communication between IoT devices and controllers, it has not been commonly employed in many publicly reported malware families.

**Royal Ransomware (DEV-0569)**
Royal ransomware is distinct in that it uses a custom-made file encryption tool as well as double extortion tactics. The latter entails threatening to publicly expose encrypted data if the victim does not pay a ransom in Bitcoin. The demanded amount typically spans from $1 million to $11 million.

## TOP MITRE ATT&CK TTPS:

| T1027 | T1055 | T1566 | T1082 | T1057 |
|---|---|---|---|---|
| Obfuscated Files or Information | Process Injection | Phishing | System Information Discovery | Process Discovery |

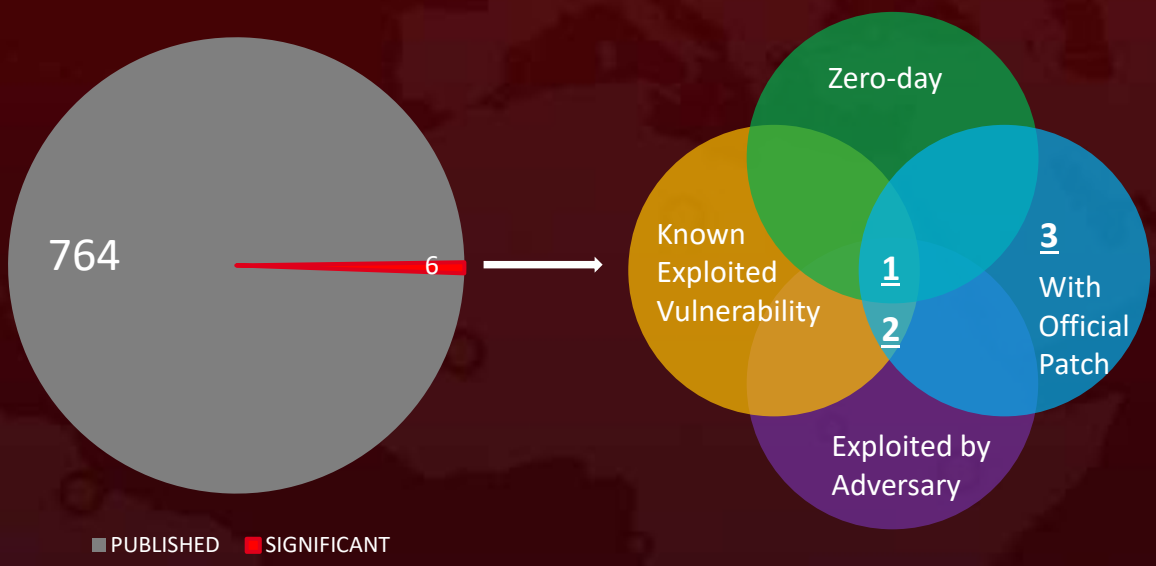
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

# Key Takeaways

## Vulnerabilities

### One Zero-day and Five Notable Mentions

Among these six vulnerabilities, DPRK actors utilized three vulnerabilities to escalate privileges, load Maui and H0lyGh0st Ransomware, and gain access. These vulnerabilities included a zero-day tracked CVE-2021-44228, and the remaining three were found in Apple macOS Ventura, the first vulnerability is related to a race situation that impacts the crash reporter component, which enables an attacker to read any files as root. The other two vulnerabilities impact the 'foundation' component and allow an attacker to execute arbitrary code outside the sandbox or with elevated privileges.




*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

# Recommendations

**Security Teams**

This digest can be utilized as a drive to force security teams to prioritize the **six significant vulnerabilities** and block the indicators related to the threat actor **TA866**, **Blackfly**, **Iron Tiger**, **APT-C-61**, **Mustang Panda APT**, **DEV-0569** and malware **PureCrypter Downloader**, **Exfiltrator-22 Ransomware Framework**, **AgentTesla Trojan**, **AHKBot**, **Rhadamanthys Stealer**, **Maui**, **H0lyGh0st Ransomware**, **Winnkit Backdoor**, **SCARLETEEL**, **ParallaxRAT**, **SysUpdate**, **Unknown Trojan**, **Snip3 Crypter**, **MQsTTang Backdoor**, and **Royal ransomware**.

**Uni5 Users**

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **six significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to malware **PureCrypter Downloader**, **Exfiltrator-22 Ransomware Framework**, **AgentTesla Trojan**, **AHKBot**, **Rhadamanthys Stealer**, **Maui**, **H0lyGh0st Ransomware**, **Winnkit Backdoor**, **SCARLETEEL**, **ParallaxRAT**, **SysUpdate**, **Unknown Trojan**, **Snip3 Crypter**, **MQsTTang Backdoor**, and **Royal ransomware** in Breach and Attack Simulation(BAS).

## Threat Advisories

Check out the links below for more extensive remediation and security precautions.

Apple Discovers Three New Vulnerabilities in macOS Ventura 13.2

Deceptive Discord Campaign Targets Government Entities with PureCrypter Malware

New Post-Exploitation Exfiltrator-22 Ransomware Framework Designed to Evade Detection

AgentTesla Trojan Returns with Phishing Campaigns Using GuLoader to Steal Secrets

TA866 New Financially-Motivated Threat Actor Targeting US and Germany Organizations

Malicious DPRK Actors Target the Healthcare Industry in the US & South Korea

Blackfly Chinese APT targets Asian conglomerate in materials sector

Highly Sophisticated SCARLETEEL Cloud Attack That Stole Proprietary Data

ParallaxRAT targets cryptocurrency organizations through phishing emails

Iron Tiger APT Group Updates SysUpdate Malware to Target Linux Platforms

A New APT named APT-C-61 Targets South Asia

Snip3 Crypter an Advanced RAT Loader Targeting Multiple Industries

New MQsTTang Backdoor from Mustang Panda Targets Political and Governmental Organizations

Royal Ransomware Targets Organizations with Custom Encryption and Double Extortion Tactics

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**:Threat Exposure Management Platform.


REPORT GENERATED ON

**March 6, 2023 • 2:12 AM**



More at www.hivepro.com