Date of Publication
February 13, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Actors, Attacks, and Vulnerabilities

06 to 12 FEBRUARY 2023

Summary

Threat Actors

Hive Pro identified three active actors over the past week. The first, **OilRig**, is a well-known threat actor known for its information theft and espionage activities. The second, **Mustang Panda APT**, is a Chinese-based cybercrime group that focuses on information theft and espionage. The third actor identified is **NewsPenguin**. For more information, refer to the "Actors" section for key takeaways.

Attacks

Last week, seven new active malware strains were identified. Three of these were ransomware: **ESXiArgs Ransomware**, **Cl0p ransomware**, and **Trigona ransomware**. Additionally, two botnets were discovered: **Medusa Botnet** and **Mirai Botnet**. Another new malware found was **PlugX Malware** and one more was **Batloader**. For further details, please consult the "Attacks" section for important highlights.

Vulnerabilities

Last week, we identified 23 vulnerabilities that organizations should be aware of. **Three** vulnerabilities were discovered in VMware ESXi and VMware vCenter Server, granting remote code execution capabilities and the potential for attackers to gain control of the impacted system. The OpenSSL Project has also released fixes for **eight** security flaws that pose a threat to users and could result in malicious attacks. For more information, please refer to 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

OilRig APT

OilRig is a state-sponsored APT group that primarily targets organizations in the Middle East. In a recent intrusion, a threat actor utilized AutoHotkey to launch a keylogger. The initial compromise was initiated with a malicious VBA macro embedded in a Word document.

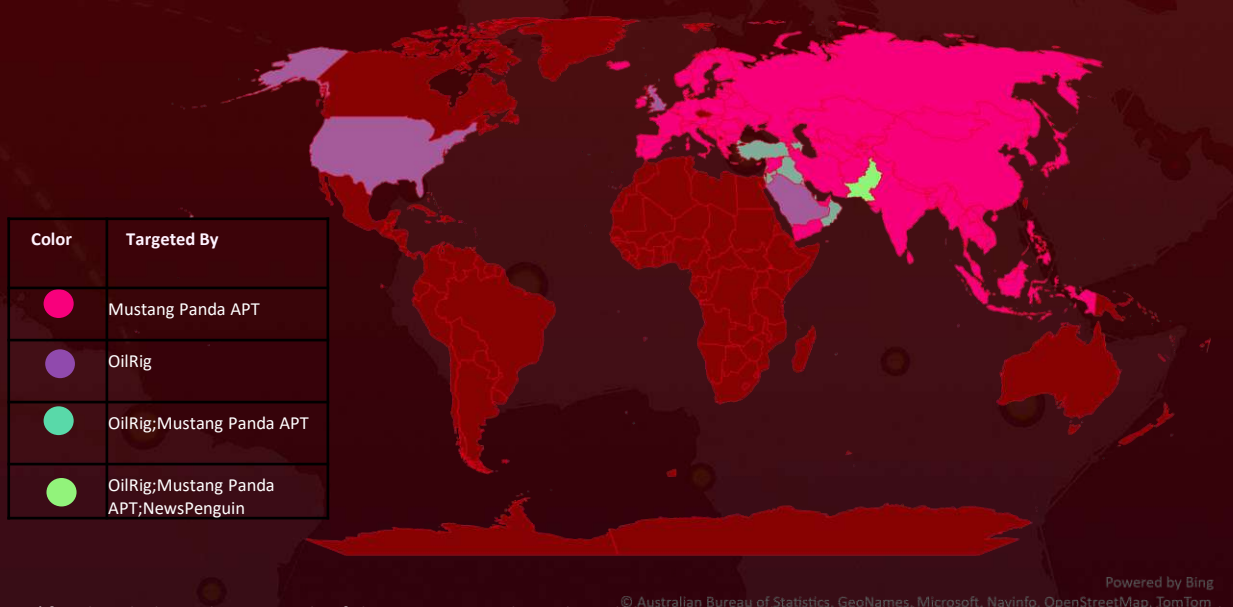
Mustang Panda APT

The Mustang Panda APT group has been targeting government and public sector organizations across Asia and Europe since at least 2019.Recently, the group has shifted from using archive files to using malicious optical disc image (ISO) files to deliver a modified version of the PlugX malware, increasing the group's evasion against anti-malware solutions targeting Europe.

NewsPenguin

NewsPenguin is a known advanced persistent threat (APT) actor group that has been active since at least 2020. The group has been known to target organizations in East Asia, with a focus on the political and media sectors. The group's primary goal is typically to gather intelligence and steal sensitive information, including political, military, and economic information.

Actor Map



*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
	OilRig (APT 34, Helix Kitten, Twisted Kitten, Crambus, Chrysene, Cobalt Gypsy, TA452, IRN2, ATK 40, ITG13)	Iran	Information theft and Espionage
	Mustang Panda APT(Bronze President ,TEMP.Hex ,HoneyMyte,Red Lich,Earth Preta)	China	Information theft and Espionage
	NewsPenguin	Unknown	Information theft and Espionage

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

Key Takeaways

Attacks

Medusa Botnet (unattributed)

Medusa is a type of botnet, which is a network of compromised computers that are remotely controlled by an attacker, without the knowledge or consent of their owners. The computers in a botnet can be used to carry out various malicious activities, such as sending spam, launching denial-of-service (DoS) attacks, or stealing sensitive information.

PlugX malware (Mustang Panda APT)

PlugX is a type of malware that has been used in advanced persistent threat (APT) attacks. It is a remote access trojan (RAT) that allows attackers to gain unauthorized access to a compromised system and steal sensitive information. PlugX is known for its ability to evade detection by security software and its ability to dynamically load modules to extend its functionality.

Cl0p ransomware (Unattributed)

The first-ever ELF variant of Cl0p (also known as Clop) ransomware has been detected in the wild. However, the ELF executable contains a flawed encryption algorithm, allowing for the decryption of locked files without paying the ransom. The Linux version is designed to encrypt specific folders and file types, but it includes a hard-coded master key that can be utilized to retrieve the original files without paying the adversary.

Trigona ransomware (Unattributed)

Trigona ransomware has gained momentum lately due to its utilization of the double-extortion technique of encrypting crucial assets within an organization, including endpoints and infrastructure, and demanding payment of ransom, or else the stolen data from these systems will be publicly released on the internet.

Batloader (Unattributed)

Batloader is a piece of malware that is used to deliver other types of malware to a compromised system. It is typically delivered as an executable file, often masqueraded as a legitimate file, that is executed by the user or by exploiting a vulnerability in the system. Once executed, Batloader downloads additional malware components, such as Trojans or rootkits, which are used to steal sensitive information or to gain unauthorized access to the system.

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

Mirai Botnet(unattributed)

The Mirai botnet is a network of Internet of Things (IoT) devices that have been infected with the Mirai malware. The Mirai malware infects vulnerable IoT devices, such as routers, security cameras, and digital video recorders, and turns them into bots that can be controlled remotely by attackers.

ESXiArgs Ransomware(unattributed)

ESXiArgs is a type of ransomware that specifically targets VMware ESXi servers. ESXi is a popular virtualization platform that allows multiple virtual machines to run on a single physical server. The ESXiArgs ransomware is delivered to the target server through a vulnerability in the server's configuration or through an exploit in the software.

TOP MITRE ATT&CK TTPS:

T1140 Deobfuscate/ Decode Files or Information	**T1204.002** Malicious File	**T1204** User Execution	**T1027** Obfuscated Files or Information	**T1571** Non-Standard Port
T1071 Application Layer Protocol	**T1068** Exploitation for Privilege Escalation	**T1055** Process Injection	**T1082** System Information Discovery	**T1486** Data Encrypted for Impact
T1588.006 Vulnerabilities	**T1083** File and Directory Discovery	**T1036** Masquerading	**T1203** Exploitation for Client Execution	**T1059** Command and Scripting Interpreter
T1518 Software Discovery	**T1518.001** Security Software Discovery	**T1059.001** Power Shell	**T1588** Obtain Capabilities	**T1497** Virtualization/ Sandbox Evasion

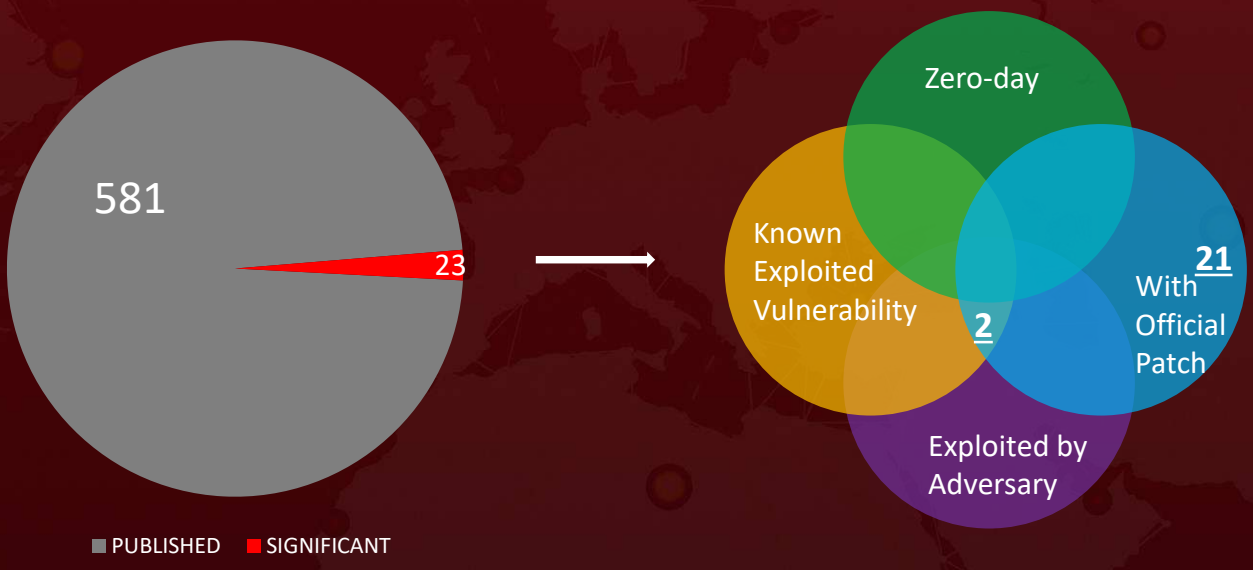
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Vulnerabilities

Twenty-three Notable Mentions

Out of the 23 security vulnerabilities discovered, one (CVE-2023-20076) was found in the Cisco IOx application hosting environment and allows for the execution of arbitrary commands as the root user on the host operating system. Meanwhile, three vulnerabilities were uncovered in VMware ESXi and VMware vCenter Server, enabling remote code execution and the potential takeover of the compromised system. Google Chrome addressed ten issues related to arbitrary code execution that could lead to the exposure of sensitive information. Another vulnerability (CVE-2023-22501) could allow an attacker to impersonate another user and access a Jira Service Management instance in certain scenarios. Furthermore, the OpenSSL Project has released fixes for eight security flaws, with one of them being a high-severity issue (CVE-2023-0286) that could put users at risk from malicious attacks.



*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 **23 significant vulnerabilities** and block the indicators related to the threat actor **OilRig, Mustang Panda APT, NewsPenguin** and malware, **PlugX Malware, Medusa Botnet, Mirai Botnet, Batloader, Cl0p ransomware, ESXiArgs Ransomware,** and **Trigona 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 **23 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to and malware , **PlugX Malware, Medusa Botnet, Mirai Botnet, Batloader, Cl0p ransomware, ESXiArgs Ransomware, and Trigona ransomware** in Breach and Attack Simulation(BAS).

Threat Advisories

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

A critical flaw in Cisco IOx Root Access Threat has been discovered

A new botnet called the "Medusa Botnet" is emerging via Mirai Botnet targeting Linux users

Iranian OilRig Group Strikes with AutoHotkey Keylogger and Malicious Macro

Mustang Panda APT targets Europe with customized PlugX malware

The ESXiArgs ransomware attack is targeting VMware ESXi servers globally

Linux Variant of Cl0p Ransomware Discovered with Flawed Encryption Algorithm

Trigona Ransomware's Rampant Threat to Businesses

The SteelClover Group is Spreading Malware via Google Ads in Japan

Chrome 110 Tackles a Collection of Security Weaknesses

An Authentication Vulnerability Discovered in Jira Service Management Server and Data Center

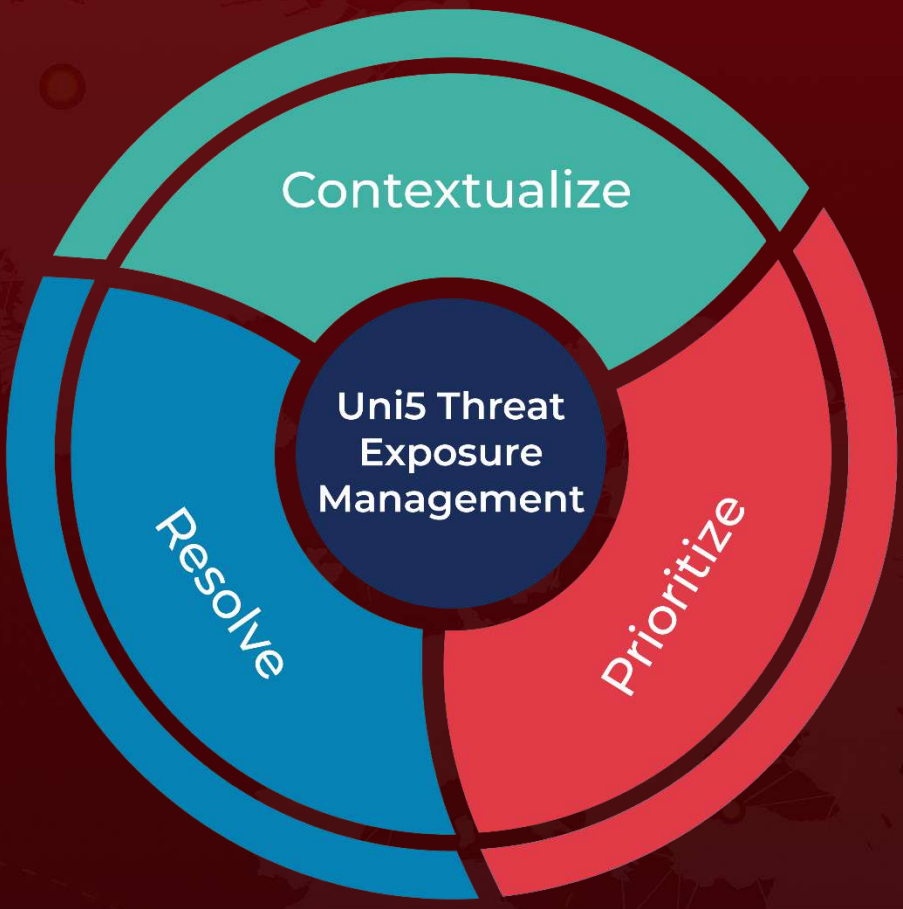
OpenSSL Releases Update to Address Several High-Severity Vulnerabilities

NewsPenguin Threat Actor Unleashes Malicious Attacks on Pakistani Firms

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

February 13, 2023 . 2:00 AM

More at www.hivepro.com