Date of Publication
March 13, 2023

Hive Pro

HiveForce Labs

WEEKLY

THREAT DIGEST

Actors, Attacks, and Vulnerabilities

6 to 12 MARCH 2023

Summary

Threat Actors

Last week, HiveForce Labs discovered three threat actors. One of them is a Russian group called **TA499**, which has a history of conducting different cyberattacks such as spear-phishing campaigns and ransomware attacks. The other two are Chinese groups named **Sharp Panda** and **8220 gang**. For more information, please refer to the key takeaway section on Actors.

Attacks

Last week, we discovered nine new active malware strains that pose a significant threat. Three of these malware strains were identified as stealers, which include **RedLine**, **ImBetter**, and **SYS01**. Additionally, two of the new malware strains were RATs, specifically **HiatusRAT** and **AsyncRAT**. Furthermore, we identified other malicious software, such as **LokiBot**, **Formbook**, **BlackSnake** ransomware, and **ScrubCrypt** clipper. For more information on these malware strains, please see the key takeaway section on Attacks.

Vulnerabilities

Last week, we found a total of 20 vulnerabilities that organizations should prioritize. Specifically, Cisco IP Phone was found to have **three** vulnerabilities that have been addressed. In addition, Trusted Platform Module (TPM) 2.0 had **two** vulnerabilities addressed. Lastly, Fortinet had **15 flaws** identified in multiple products, which could potentially lead to unauthorized access to sensitive information. 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

Sharp Panda

Sharp Panda is engaged in a persistent surveillance operation aimed at Southeast Asian government entities. The attackers initiate the attack through spear-phishing emails, which contain government-themed lures in a Word document. These lures utilize a remote template to download and execute a malicious RTF document, which is weaponized with the notorious RoyalRoad kit.

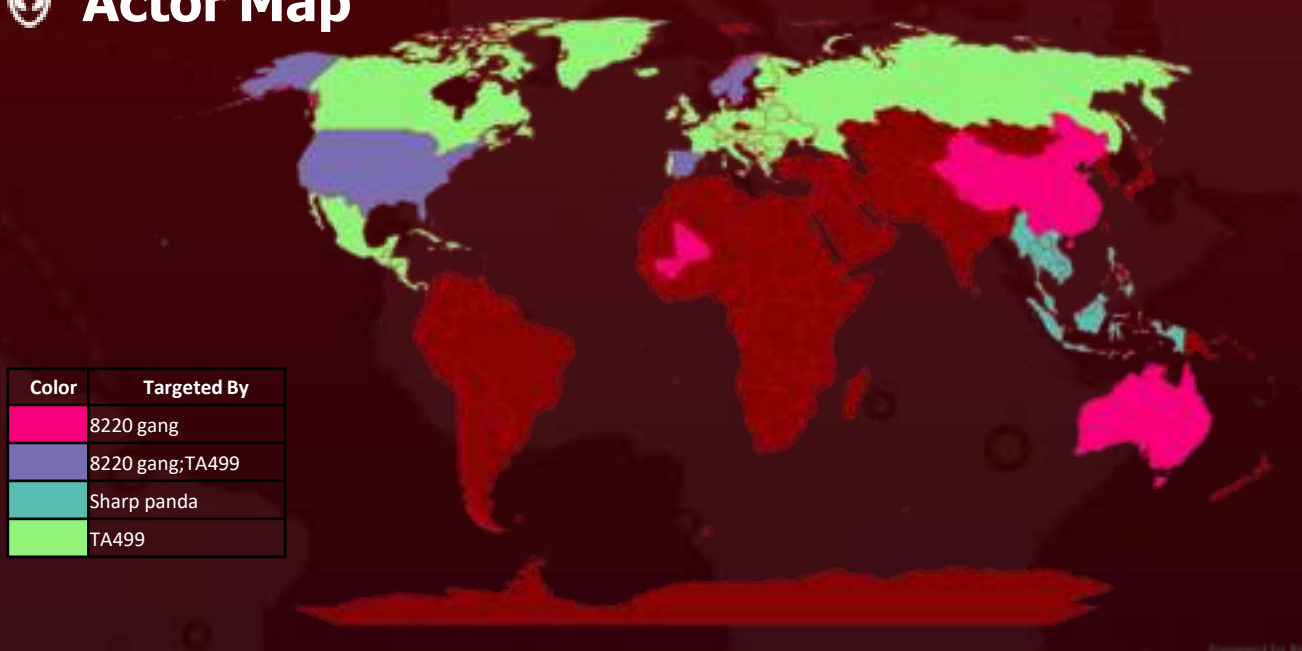
TA499

TA499 is a group of threat actors aligned with the Russian state that engages in impersonation-based, patriotically motivated misinformation campaigns. They use email to target high-profile individuals, including government officials, businesspeople, and celebrities, who have made public statements in favor of sanctions against Russia, against the detainment of Alexei Navalny, or in support of Ukraine.

8220 gang

The 8220 gang has been undertaking crypto-mining operations since 2017. Recently, the gang has begun carrying out crypto-jacking attacks using a new crypter called ScrubCrypt. The assault begins by exploiting unprotected Oracle WebLogic servers in order to download a PowerShell script containing ScrubCrypt.

Actor Map



Color	Targeted By
	8220 gang
	8220 gang;TA499
	Sharp panda
	TA499

*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
	Sharp Panda	China	Information theft and espionage
	TA499(Vovan; Lexus)	Russia	Sabotage and Espionage
	8220 gang	China	Financial gain

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

Key Takeaways

Attacks

LokiBot (Unattributed)

LokiBot is a constantly evolving information-stealing malware that creates a backdoor on infected machines to collect sensitive data, and it uses ISO files and API hashing techniques to bypass detection and inject malicious code.

HiatusRAT (Unattributed)

Hiatus hacking campaign targets DrayTek Vigor routers to steal data and create a covert proxy network. The campaign uses a malicious script, HiatusRAT malware, and tcpdump to capture network traffic, pass commands, and control server traffic through a SOCKS5 proxy.

RedLine Stealer(Unattributed)

A spear-phishing campaign targeting the hospitality industry used subject lines and text to trick hotel staff into clicking on malicious links that led to the download of malware, including the RedLine Stealer, which collected a wide range of data and sent it to its command-and-control server.

ImBetter Stealer (Unattributed)

The ImBetter Stealer malware has been discovered to be capable of stealing sensitive data and cryptocurrency wallets from its victims through phishing websites. These fake sites imitate popular crypto-wallets and online file converters, tricking users into downloading the malware and putting their confidential information at risk.

SYS01 stealer (Unattributed)

The SYS01 stealer has been targeting critical government infrastructure employees, manufacturing companies, and other industries, and using various delivery techniques, including DLL side-loading, to steal and exfiltrate information from victims.

AsyncRAT & Formbook(Unattributed)

AsyncRAT and Formbook are two malware being delivered to users via OneNote documents, which cybercriminals are using to steal data, install ransomware, and perform various malicious activities.

Key Takeaways

Attacks

BlackSnake (Unattributed)

BlackSnake ransomware has been discovered with clipper functionality that intercepts and replaces the cryptocurrency wallet addresses of victims with those of attackers.

ScrubCrypt (8220 Gang)

ScrubCrypt is a crypter used by the 8220 gang that utilizes a distinctive BAT packing mechanism to secure applications. After undergoing Base64 decoding, AES decryption, and unzipping, the regular .NET Reflective Injection code is visible. Before proceeding, the .NET code assesses whether a debugger is attached, updates the extension as null, and verifies the operating system version.

TOP MITRE ATT&CK TTPS:

T1083 File and Directory Discovery	**T1027** Obfuscated Files or Information	**T1204** User Execution	**T1566** Phishing	**T1059** Command and Scripting Interpreter
T1056 Input Capture	**T1140** Deobfuscate/ Decode Files or Information	**T1005** Data from Local System	**T1113** Screen Capture	**T1036** Masquerading
T1560 Archive Collected Data	**T1547** Boot or Logon Autostart Execution	**T1041** Exfiltration Over C2 Channel	**T1055** Process Injection	**T1056** Input Capture
T1562 Impair Defenses	**T1574** Hijack Execution Flow	**T1106** Native API	**T1070** Indicator Removal	**T1040** Network Sniffing

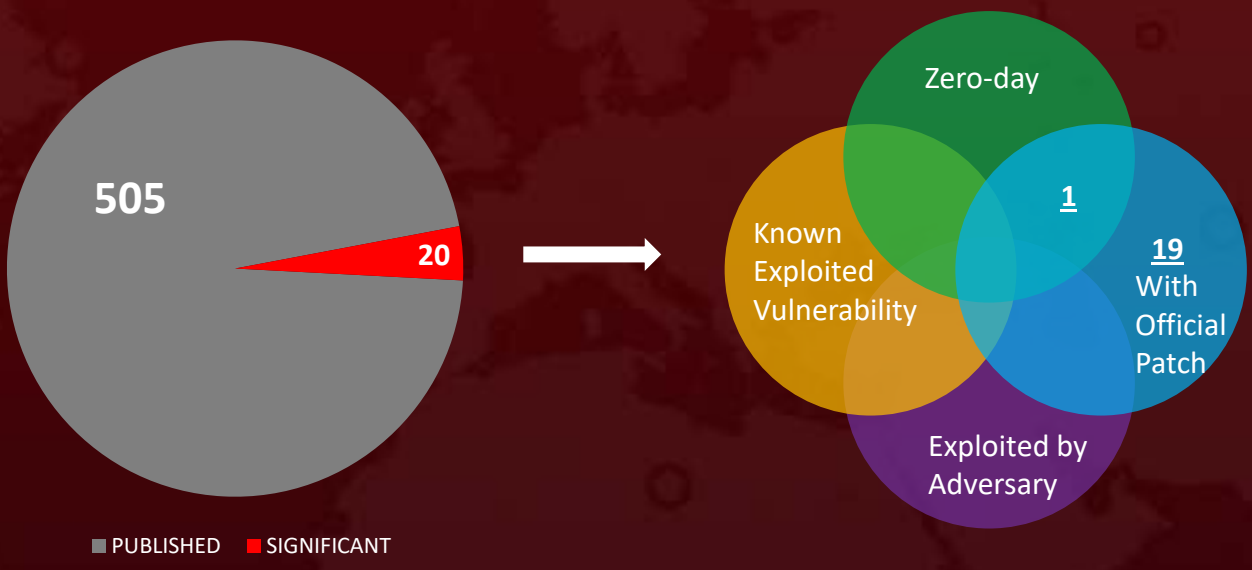
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Vulnerabilities

One Zero-day and Nineteen Notable Mentions

Cisco has disclosed three vulnerabilities in its IP phones, including a zero-day vulnerability in the Cisco IP Phone 7800 and 8800 Series that could allow remote code execution. Additionally, two other vulnerabilities in the phones have been identified, which could result in denial-of-service attacks or remote code execution. Two buffer overflow vulnerabilities have also been found in the Trusted Platform Module (TPM) 2.0 specification, potentially allowing attackers to access or overwrite sensitive data. Furthermore, various Fortinet products, including FortiOS, FortiProxy, FortiAnalyzer, FortiNAC, FortiManager, FortiPortal, FortiSwitch, FortiAuthenticator, FortiDeceptor, FortiMail, FortiSOAR, FortiWeb, and FortiRecorder, have been found to have security vulnerabilities that could result in unauthorized access to sensitive information, denial-of-service attacks, and privilege escalation.



*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 **20 significant vulnerabilities** and block the indicators related to the threat actor **Sharp Panda, TA499, 8220 gang** and malware, **Redline, ImBetter, Sys01, HiatusRAT, AsyncRAT, Lokibot, Formbook, BlackSnake ransomware, and ScrubCrypt clipper.**

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 **20 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to to the threat actor **Sharp Panda, TA499, 8220 gang** and malware, **Redline, ImBetter, Sys01, HiatusRAT, AsyncRAT, Lokibot, Formbook, BlackSnake ransomware, and ScrubCrypt clipper** in Breach and Attack Simulation(BAS).

Threat Advisories

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

Two New Vulnerabilities Discovered in TPM 2.0 Library

Unveiling the Malicious Tactics of LokiBot Malware

Multiple Vulnerabilities Found in Cisco IP Phones Web-Based Management Interface

Hiatus Hacking Campaign Targets DrayTek Vigor Routers to Steal Data

RedLine Stealer Used in Spear-Phishing Campaign Targeting Hospitality Industry

ImBetter Stealer Malware Targets Cryptocurrency Wallets

SYS01 Stealer Targets Government and Manufacturing Industry

Threat Actors Exploit Microsoft OneNote for Malware Delivery via Phishing Attacks

Tracking the Malicious Email Campaigns of Russia-Aligned TA499

Sharp Panda A Sophisticated Cyber-Espionage Campaign Targeting Governments

New BlackSnake Ransomware Performs Clipper Operations on Cryptocurrency Users

8220 Gang leverages ScrubCrypt in Cryptojacking Attacks

Multiple Vulnerabilities in Various Fortinet Products in March 2023

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 13, 2023 • 6:00 AM

More at www.hivepro.com