

Date of Publication
January 30, 2023



HiveForce Labs

WEEKLY

THREAT DIGEST

Actors, Attacks, and Vulnerabilities

23 to 29 JANUARY 2023

Summary



Threat Actors

Hive Pro discovered **four** actors that have been active in the past week. The first, **APT40 and Tick**, are well-known Chinese threat actors known for information theft and espionage. The second, **BlueNoroff**, is a well-known North Korean state-sponsored threat group that specializes in financial cyber operations. The third **Vice Society** ransomware group is known for Financial gain. The fourth **Cobalt Sapling** is a well-known Iranian state-sponsored threat group that specializes in Sabotage and destruction. For further details, see the key takeaway section for Actors.



Attacks

We also discovered **eight** new malware strains that have been active over the past week. The source code for the **CrySIS ransomware** family has been publicly disclosed, exposing it for anyone to access and modify. **Vidar** is a subscription-based information-stealer that utilizes Russian VPN gateways to evade detection. **Album Stealer** uses DLL side loading and data masking to evade detection and exfiltrate information to a C2 server. Chinese threat actors are deploying the **Remcos RAT and GuLoader** through phishing attacks. DragonSpark campaigns leverage the open-source **SparkRAT** to target businesses in East Asia. **Titan Stealer** is a cross-platform information-stealing malware that is actively spread by a threat actor. **CryptBot** is a malware that steals data from Windows-based computers for system configuration information. New **Mimic ransomware** uses the APIs of a legitimate tool called Everything to encrypt target files. For further details, see the key takeaway section for Attacks.



Vulnerabilities

Last week, we discovered **nine** vulnerabilities that organizations should prioritize. **Four** of these vulnerabilities were security flaws in VMware, and **four** were in Google Chrome. 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

APT40 & TICK (Remcos RAT and GuLoader)

APT40 and TICK are well-known Chinese threat actors who deployed the Remcos RAT and GuLoader via phishing campaigns. These campaigns' motivations include exploiting system flaws, lateral movement within organizations, and deploying malware/trojan implants to target governments and organizations in order to exfiltrate sensitive information and achieve maximum benefit with minimal effort.

Vice Society (unattributed)

The Vice Society ransomware gang is a highly flexible and persistent threat that targets many industries with diverse tools and techniques and is suspected of planning a Ransomware-as-a-Service operation. The attack vector of the group is most likely to entail the exploitation of a public-facing website or the use of compromised remote desktop protocol (RDP) credentials.

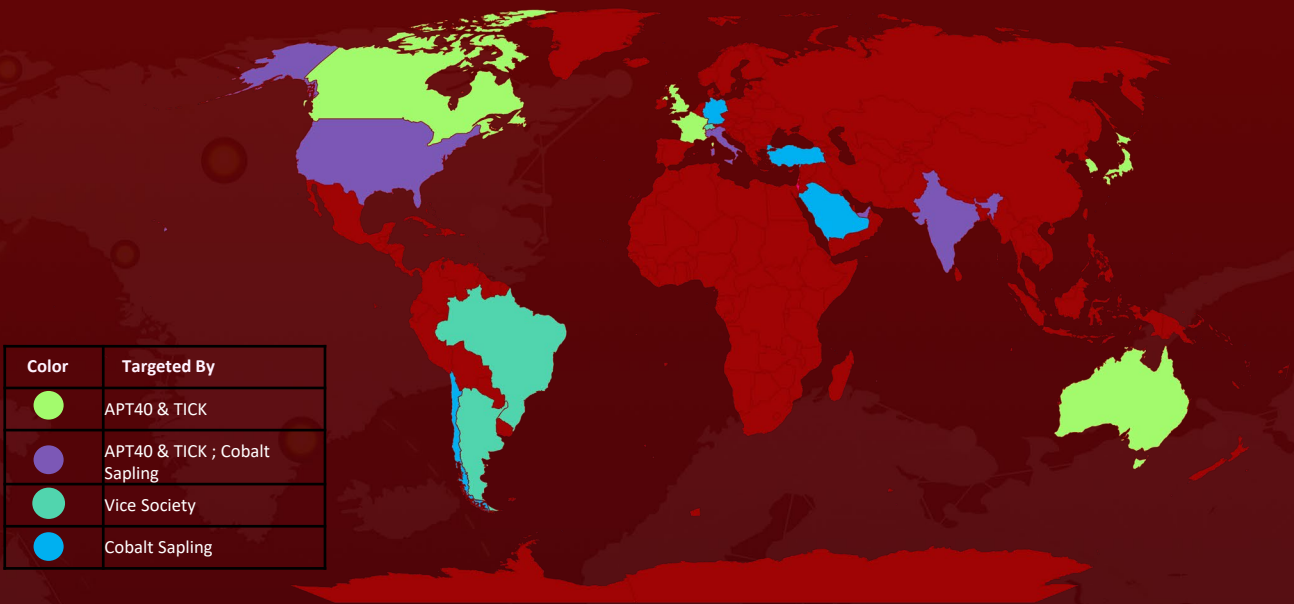
Cobalt Sapling (unattributed)

Cobalt Sapling is a threat actor group believed to be of Iranian origin. The group has been known to use various hacktivist group aliases, including Moses Staff and Abraham's Ax. The group operates its leak sites on WordPress blogs and supports multiple languages. As of December 2, the group has posted 16 "actions" on its website, primarily consisting of data sets obtained from Israeli companies.

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


Key Takeaways

Actor Map



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Actor Details

ICON	NAME	ORIGIN	MOTIVE
	<u>APT 40,Leviathan,Kryptonite Panda,TEMP.Periscope,TEMP.Jumper,Bronze Mohawk,Mudcarp,Gadolinium,ATK 29,ITG09,TA423,Red Ladon</u>	China	Information theft and espionage
	<u>Tick,CTG-2006,Bronze Butler,TEMP.Tick,RedBaldNight,Stalker Panda</u>	China	Information theft and espionage
	<u>Vice Society</u>	Unknown	Financial Crime
	<u>Cobalt Sapling Moses Staff, DEV-0500, Abraham's Ax</u>	Iran	Sabotage and destruction

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

Key Takeaways

Attacks

CrySIS Ransomware (unattributed)

The CrySIS (also known as Dharma) ransomware operates as a ransomware-as-a-service (RaaS). Notably, the source code of a version was made public, making it available for purchase and repurposing. The malware's operators penetrate systems using vulnerable Microsoft Remote Desktop Protocol (RDP) servers and encrypt data using AES-256 encryption with RSA-1024 asymmetric encryption.

Vidar Info-stealer malware (unattributed)

Vidar is a formidable information-stealing malware notable for its ability to evade detection by using Russian VPN gateways, relocating to the Tor network, and extending its infrastructure. It operates on a conventional business model in which consumers pay between \$130 and \$750 for a subscription, with the option to tailor the targeted information types.

Album Stealer (unattributed)

Album Stealer can circumvent detection in numerous phases by using vulnerable legitimate apps via the technique of DLL side loading. The malware masks critical strings and data using the ConcurrentDictionary class and delivers the information gathered from an infected system to a command-and-control server.

Remcos RAT and GuLoader (APT40, TICK)

APT40 and TICK, two Chinese threat actors, are launching phishing attempts to distribute the Remcos RAT and GuLoader. GuLoader is a sophisticated malware downloader that uses a versatile shellcode loader to evade detection by conventional protection solutions. Static analysis is difficult as the shellcode is encrypted and obfuscated. GuLoader installs the Remcos RAT on the victim's device.

SparkRAT (unattributed)

The DragonSpark attack campaigns utilize open-source SparkRAT and Golang-written malware to evade detection by interpreting its source code at runtime. They target firms in East Asia using infiltrated infrastructure in China and Taiwan to transmit SparkRAT and other tools and malware.

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

Key Takeaways

Titan Stealer (unattributed)

Titan Stealer is a cross-platform information-stealing malware that is actively spread by a threat actor through a Telegram channel. It is capable of capturing various data from compromised Windows devices, giving the attacker access to victims' login activity and data. The stealer can steal a range of information, including browser credentials and cryptocurrency wallets, from compromised Windows devices.

CRYPTBOT malware (unattributed)

CryptBot is a data stealer that targets Windows-based computers. By traversing the 'Uninstall' registry tree, the malware checks the system for installed software. It looks for particular registry keys in order to identify the collection of system configuration data.

Mimic ransomware (unattributed)

Mimic ransomware was discovered in June 2022. It encrypts files using the APIs of a product called Everything and has features such as removing shadow copies, terminating apps and services, and deactivating Windows Defender. Mimic has multiple threads that use the CreateThread function to speed up encryption and complicate analysis for security researchers.

TOP MITRE ATT&CK TTPS:

T1027

Obfuscated
Files or
Information

T1082

System
Information
Discovery

T1071

Application
Layer Protocol

T1547

Boot or Logon
Autostart
Execution

T1070

Indicator
Removal

T1083

File and
Directory
Discovery

T1059

Command and
Scripting
Interpreter

T1518

Software
Discovery

T1574

Hijack
Execution
Flow

T1087

Account
Discovery

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

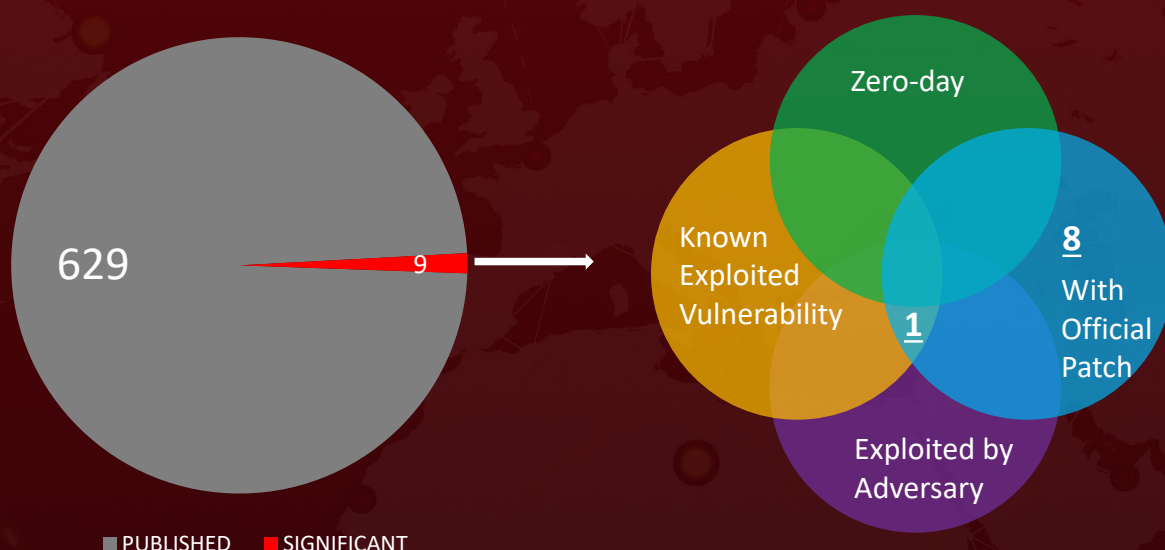
Key Takeaways



Vulnerabilities

Nine Notable Mentions

Among the nine vulnerabilities, one was discovered in a Kerberos Distribution Center (KDC) that was being used by threat actors to spoof connected certificates in various ways. This is because certificate-based authentication was not handled properly, leading to an elevation of privilege flaws. VMware has fixed four security vulnerabilities in vRealize Log Insight, known as Aria Operations for Logs, which could lead to remote code execution attacks. Unauthenticated malicious actors can insert files into compromised products' operating systems. Finally, four flaws allow a remote attacker to access potentially sensitive information, causing type confusion and a use-after-free error.



*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 **nine significant vulnerabilities** and block the indicators related to the threat actor **APT40, TICK, Vice Society, Cobalt Sapling** and malware **CrySIS Ransomware, Vidar Info-stealer, Album Stealer, Remcos RAT, GuLoader, SparkRAT, Titan Stealer, CRYPTBOT**, and **Mimic 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 **nine significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to malware **CrySIS Ransomware, Vidar Info-stealer, Album Stealer, Remcos RAT, GuLoader, SparkRAT, Titan Stealer, CRYPTBOT**, and **Mimic ransomware** in Breach and Attack Simulation(BAS).



Threat Advisories

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

[CrySIS Ransomware A Long-Standing Threat with a New Twist](#)

[Tracking the Stealthy Movements of Vidar Info-Stealer Malware](#)

[A New Malware Called Album Stealer is Targeting Facebook Users](#)

[Unpatched Systems Vulnerable to Spoofed Linked Certificates in KDC](#)

[Chinese Threat Actors Leverage Phishing and GuLoader to Distribute Remcos RAT](#)

[DragonSpark Attacks Targeting East Asian Countries Using SparkRAT Malware](#)

[VMware addresses Security Flaws in vRealize Log Insight](#)

[Brazil's manufacturing industry under attack by Vice Society ransomware group](#)

[Chrome 109 addresses an array of security flaws](#)

[Titan Stealer – A Cross-Platform Information Stealer Malware Distributed by Threat Actors](#)

[CRYPTBOT Information-Stealing Malware Targeting Your Browser and Crypto-Wallet](#)

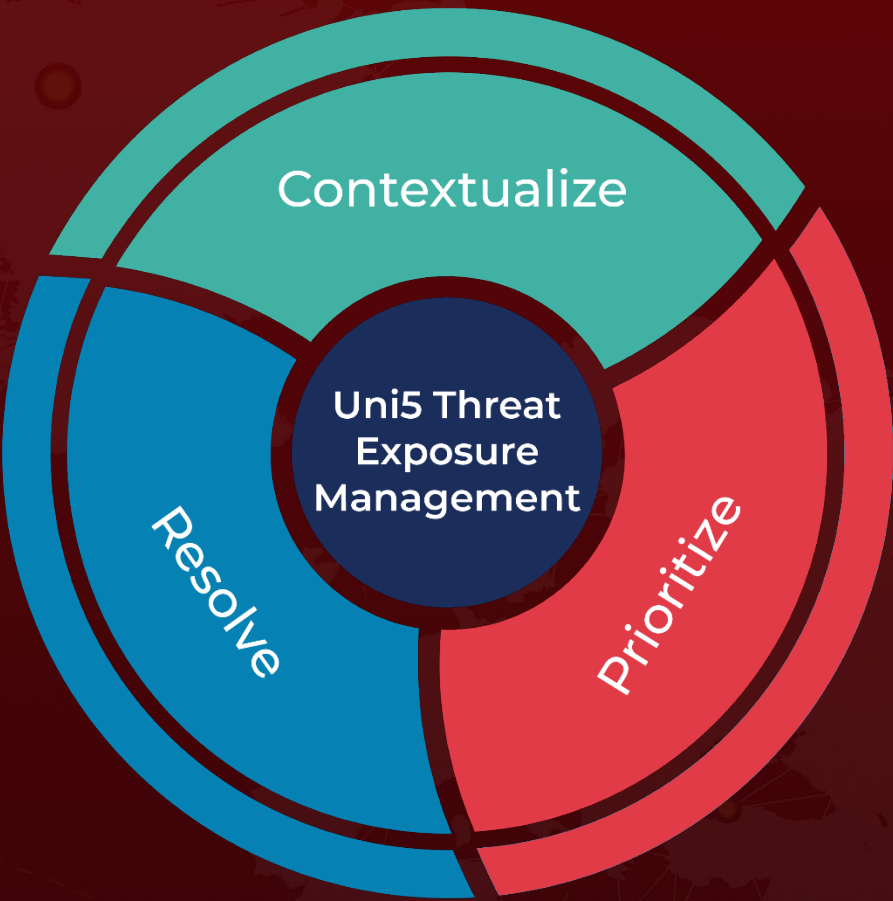
[Similarities between hacktivist groups reveal Iranian connection](#)

[New Ransomware Mimic Emerges in the Wild, Abusing Legitimate Tool for Faster Encryption](#)

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
January 30, 2023 • 4:44 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com