Date of Publication
December 19, 2022

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Actors, Attacks, and Vulnerabilities

12 to 18 DECEMBER 2022

Summary

Threat Actors

Hive Pro discovered six Actors that have been active in the last week. Two of them (TA505 and Silence Group)are famous for financial crimes. Three of them (MuddyWater, Cloud Atlas , and APT5) are popularly known for Information theft and Espionage. Lastly, MirrorFace is a Chinese threat actor group popular for data exfiltration and espionage. For further details, see the key takeaway section for Actors.

Attacks

We also discovered five new malware strains that have been active over the last week. TrueBot malware is a downloader malware that spreads through infected systems, collects information on targets, and deploys malicious payloads. A PowerShell-based backdoor PowerShower is placed on disk via simple base64-encoding and string concatenation obfuscation. GoTrim is a new botnet written in go programming language and has been scanning and brute-forcing on the four content management systems. Mallox ransomware is operational, propagating rapidly, and infecting entities around the world. Another backdoor, LODEINFO was dropped as a part of a spearphishing campaign. For further details, see the key takeaway section for attacks.

Vulnerabilities

We discovered 24 Vulnerabilities last week that organizations should Prioritize. Among these 24, there were four zero-day, two of which were addressed by Microsoft, one by Fortinet, and one by Citrix. the remaining 20 vulnerabilities were addressed by respective vendors. For further details, see the key takeaway section for Vulnerabilities.

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

Key Takeaways

Threat Actors

TA505 & Silence Group (Truebot)
In 2017, Truebot was discovered to be linked to the Silence group and has affected more than 1,500 systems worldwide with shellcode, Cobalt Strike beacons, Grace malware, the Teleport tool, and Clop ransomware. A recent study has linked it to TA505.

MuddyWater (unattributed)
MuddyWater used Dropbox links and document attachments with URLs redirected to ZIP archives as lures in its recent campaign, which also utilized compromised corporate email accounts.

CloudAtlas (PowerShower)
CloudAtlas intrusion is typically a PowerShell-based backdoor called PowerShower, which is placed on disk via simple Base64-encoding and string concatenation obfuscation. It makes use of the proxy when sending requests to the C&C server.

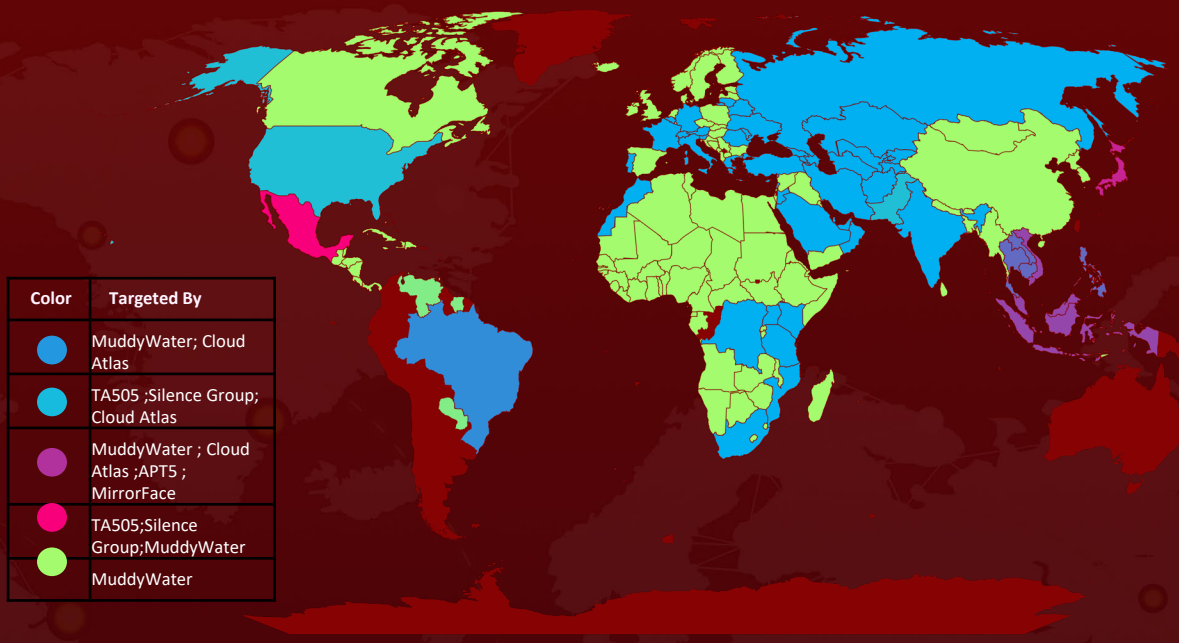
APT5 (unattributed)
The China-based APT5 (aka Bronze Fleetwood, Keyhole Panda, Manganese, UNC2630) threat actors have been actively exploiting a zero-day vulnerability that presents in Citrix Application Delivery Controller (ADC) and Citrix Gateway to gain charge on compromised systems.

MirrorFace (LODEINFO)
A Chinese-speaking APT group named MirrorFace has started its attacks by spearphishing a campaign with a LODEINFO backdoor, targeting Japanese political entities since June 29, 2022, and this campaign operation is named as LiberalFace. The main motive of the MirrorFace threat actor group is the exfiltration of data and espionage.

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

Key Takeaways

Actor Map



Actor Details

ICON	NAME	ORIGIN	MOTIVE
	TA505 Group (aka Graceful Spider, Gold Evergreen, Gold Tahoe, TEMP.Warlock, ATK 103, SectorJ04, Hive0065, Chimborazo)	Russia	Financial crime, Financial Gain
	Silence Group (aka Contract Crew, Whisper Spider, TEMP.TruthTeller, ATK 86,TAG-CR8)	Russia	Financial crime
	MuddyWater	Iran	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

ICON	NAME	ORIGIN	MOTIVE
	CloudAtlas	Russia	Information theft and Espionage
	APT5 (aka Keyhole Panda ,TEMP.Bottle, Bronze Fleetwood, TG-2754, Poisoned Flight, Manganese)	China	Information theft and espionage
	MirrorFace	China	Exfiltration of data and espionage.

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

Key Takeaways

Attacks

Truebot (TA505, Silence Group)
Truebot malware is a downloader malware that spreads through infected systems, collects information on targets, and deploys malicious payloads. The attacker's command and control (C2) receives the collected data.

PowerShower (Cloud Atlas)
PowerShower is placed on disk via simple Base64-encoding and string concatenation obfuscation. It makes use of the proxy when sending requests to the C&C server.

GoTrim Botnet (unattributed)
GoTrim is a new botnet written in Go Programming language and has been scanning and brute-forcing on the four Content Management Systems (WordPress, DataLife Engine, Joomla!, and OpenCart) websites.

Mallox Ransomware (unattributed)
Mallox ransomware strains have been spotted in the wild, indicating that the ransomware is operational, propagating rapidly, and infecting entities. A .Net-based loader downloads and encrypts data on the victim's device with Mallox ransomware from a remote source.

LODEINFO Backdoor (MirrorFace)
LODEINFO backdoor is been dropped by MirrorFace, a Chinese-speaking APT group in its spearphishing campaign. After gaining initial access, LODEINFO delivers additional malware, later it exfiltrates the credentials, documents, and emails of the victims.

TOP MITRE ATT&CK TTPS:

T1190	T1203	T1210	T1059	T1083
Exploit Public-Facing Application	Exploitation for Client Execution	Exploitation of Remote Services	Command and Scripting Interpreter	File and Directory Discovery

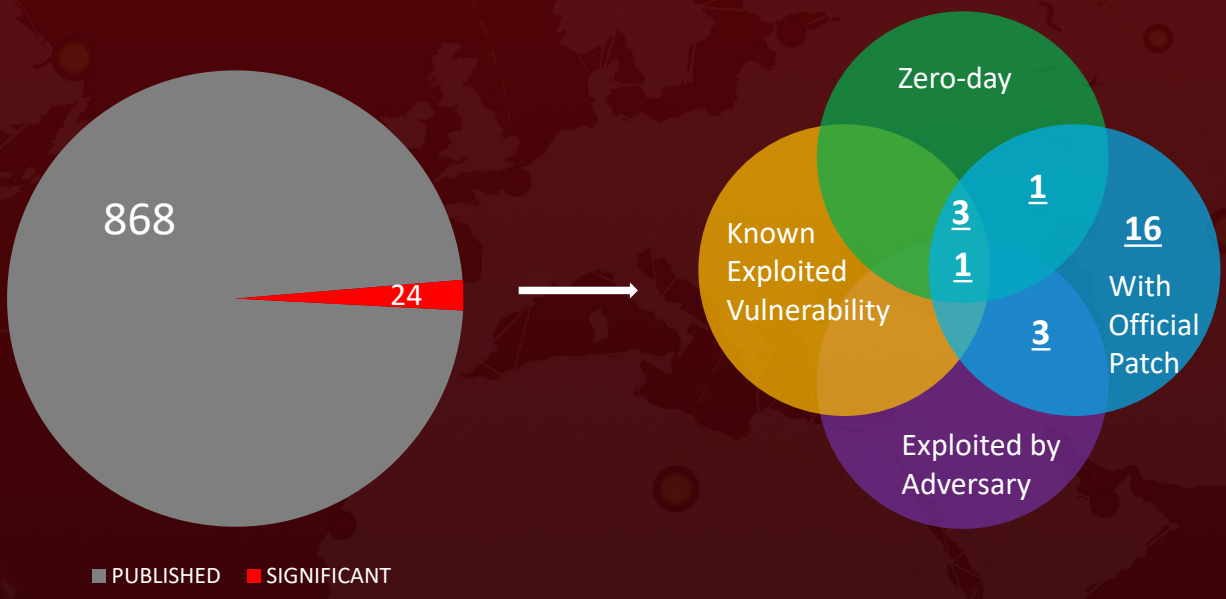
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Vulnerabilities

Four Zero-Days & 16 Notable Mentions

One of the four zero-days, CVE-2022-44698, is a Windows SmartScreen security feature bypass vulnerability. The second zero-day vulnerability, CVE-2022-44710 is a vulnerability in the DirectX graphics kernel that could result in remote code execution, the elevation of privilege (EoP), security feature bypass, and spoofing, both have been patched as part of the Microsoft patch Tuesday release. Third, CVE-2022-27518 was leveraged by APT5 in Citrix Application Delivery Controller (ADC) and Gateway. Lastly, CVE-2022-42475 is a critical vulnerability actively exploited wildly in the FortiOS SSL-VPN product. Also, VMware and Microsoft further addressed multiple security in several products.



*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 **24 significant vulnerabilities** and block the indicators related to the threat actor **TA505, Silence, MuddyWater, CloudAtlas, APT5, MirrorFace** and malware**, Truebot, PowerShower, GoTrim, Mallox Ransomware,** and **LODEINFO Backdoor.**

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 **24 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to and malware **Truebot, PowerShower, GoTrim, Mallox Ransomware,** and **LODEINFO Backdoor** in Breach and Attack Simulation(BAS)

Threat Advisories

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

A New GoLang Botnet named GoTrim BruteForcing multiple CMS

MuddyWater is back with new techniques

Citrix ADC and Gateway Zero-Day Vulnerability Exploited by APT5

VMware tackles security flaws in ESXi and vRealize

China-based MirrorFace APT group targeting Japanese Political

Microsoft addresses actively exploited zero-day and numerous critical flaws

Mallox Ransomware is Ramping up its Operation

The Cloud Atlas Perpetual Threat aims to persuade entities in Russia

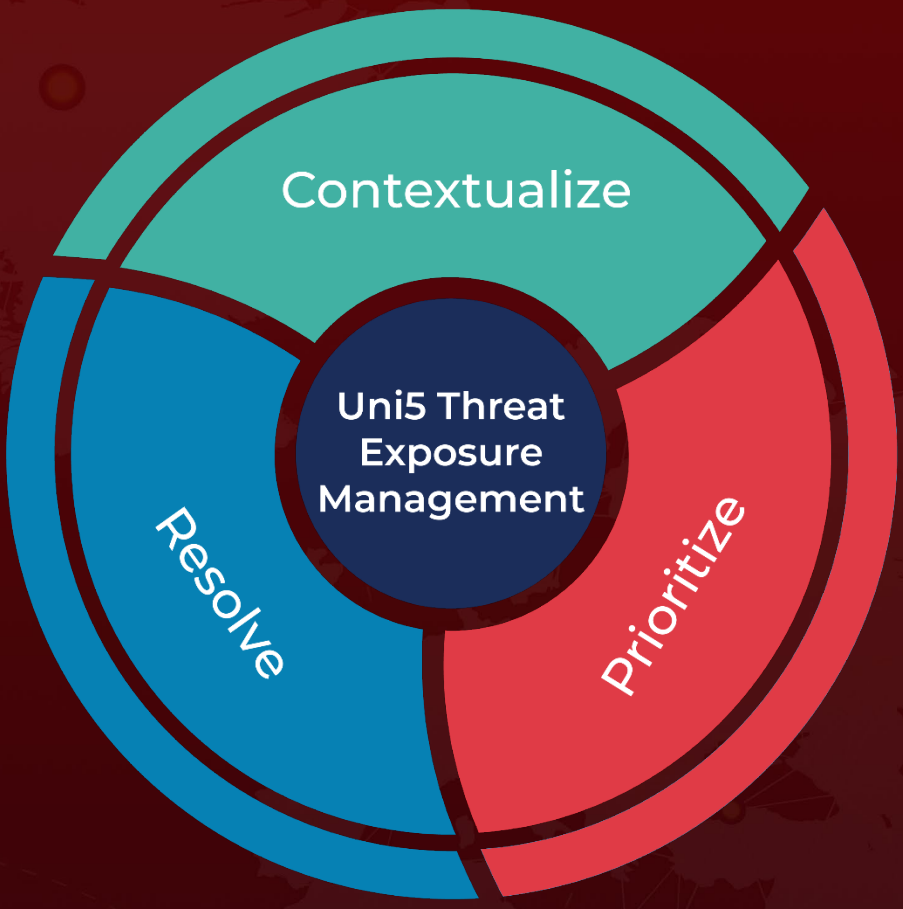
Truebot exploits vulnerability in Netwrix to deploy Clop Ransomware

Active exploitation of the Fortinet pre-auth RCE vulnerability

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

December 19, 2022 • 7:00 AM

© 2022 All Rights are Reserved by Hive Pro

More at www.hivepro.com