Date of Publication
February 20, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Actors, Attacks, and Vulnerabilities

13 to 19 FEBRUARY 2023

Summary

Threat Actors

HiveForce Labs identified seven active actors over the past week. There were three prominent Russian actors, namely **TA505**, **Nodaria**, and **KillNet**. Additionally, three Chinese actors, **Tonto Team**, **DEV-0147**, and **Dalbit**, were also identified. It should be noted that **Red Eyes** is a threat actor from North Korea. For more information, please refer to the key takeaway section on Actors.

Attacks

Last week, five new active malware strains were identified. Three of these were ransomware: **Clop Ransomware**, **DarkBit ransomware**, and **MortalKombat ransomware**. Additionally, a **ProxyShellMiner** was discovered exploiting Microsoft Exchange Server vulnerabilities. Another new malware found was **GlobeImposter**. For more information, please refer to the key takeaway section on Attacks.

Vulnerabilities

Last week, we found a total of 32 vulnerabilities that organizations should prioritize. Specifically, Apple had **three** vulnerabilities addressed, Microsoft had **17** vulnerabilities addressed, and Citrix had **four** flaws identified. Additionally, there were seven zero-day vulnerabilities that were actively exploited last week. 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

TA505

The GoAnywhere MFT attacks have been linked to the TA505 threat group, known for deploying Clop ransomware in the past while investigating an attack where the TrueBot malware downloader was deployed. However, the claims have not been independently confirmed and Fortra has not responded to inquiries.

Nodaria

A cyber espionage group linked to Russia, known as Nodaria, has been spotted deploying a newly created information-stealing malware named Graphiron in attacks aimed at Ukraine. The malware, coded in Go, can gather a significant amount of information from compromised computers, including system details, credentials, and files.

KillNet

Killnet, a Russian hacker group, disrupted relief efforts for the Turkey-Syria earthquake by carrying out DDoS attacks, taking down the websites of NATO Special Operations Headquarters and Strategic Airlift Capability.

Tonto Team

The Tonto Team threat actors pretended to be employees of a reputable organization and utilized a GMX Mail-created phony email. The enclosed file is a malicious Rich Text Format (RTF) document developed with the Royal Road RTF Weaponizer. The tool enables the threat actor to construct malicious RTF exploits with realistic decoy content for the Microsoft Equation Editor vulnerabilities CVE-2017-11882, CVE-2018-0802, and CVE-2018-0798.

DEV-0147

The China-based cyber espionage group DEV-0147 has expanded its data exfiltration operations to include diplomatic targets in South America, in addition to targeting government agencies and think tanks in Asia and Europe. The group uses tools like ShadowPad and QuasarLoader for persistent access and deploying malware and employed post-exploitation activities to abuse identity infrastructure and use Cobalt Strike for command and control and data exfiltration.

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

Key Takeaways

Threat Actors

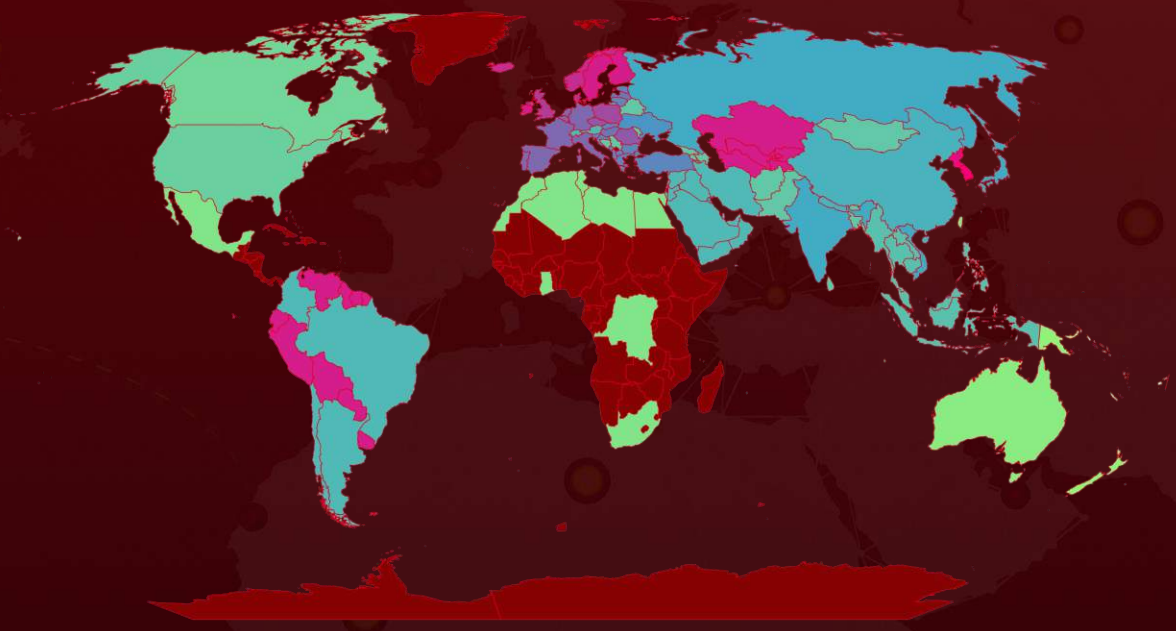
Red Eyes

The Red Eyes is responsible for stealing personal information from both PCs and mobile phones, and in this specific attack, they utilized the Hangul EPS vulnerability and a steganography technique to spread malicious code. The vulnerability used in the attack is an old one that has already been patched, but the attackers were able to exploit it because the target was using an outdated version of the software.

Dalbit

Dalbit is a threat actor group that has been active since at least 2022. They have been targeting Korean companies, with more than 50 confirmed attack attempts so far. The group relies on open-source tools and has lacked any distinct characteristics to profile them.

Actor Map



Color	Targeted By
	Dalbit;DEV-0147;Red Eyes;TA505;Tonto Team
	Dalbit;DEV-0147;Tonto Team
	DEV-0147
	DEV-0147;KillNet
	DEV-0147;KillNet;Red Eyes;TA505
	DEV-0147;KillNet;Red Eyes;TA505;Tonto Team
	DEV-0147;KillNet;Red Eyes;Tonto Team
	DEV-0147;KillNet;TA505
	DEV-0147;KillNet;TA505;Tonto Team

Color	Targeted By
	DEV-0147;KillNet;Tonto Team
	DEV-0147;Nodaria;Tonto Team
	DEV-0147;Red Eyes;TA505
	DEV-0147;Red Eyes;TA505;Tonto Team
	DEV-0147;Red Eyes;Tonto Team
	DEV-0147;TA505
	DEV-0147;TA505;Tonto Team
	DEV-0147;Tonto Team
	KillNet;Red Eyes;TA505;Tonto Team

Color	Targeted By
	Red Eyes;Tonto Team
	TA505
	TA505;Tonto Team
	Tonto Team

*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
	TA505(Graceful Spider, Gold Evergreen , Gold Tahoe, TEMP.Warlock, ATK 103, SectorJ04, Hive0065, Chimborazo)	Russia	Financial crime, Financial gain
	Nodaria(SaintBear, Ember Bear, TA471, UNC2589, Lorec53, UAC-0056)	Russia	Information theft and espionage
	KillNet	Russia	Hacktivist
	Tonto Team(HeartBeat, Karma Panda, CactusPete, Bronze Huntley, LoneRanger)	China	Information theft and espionage
	DEV-0147	China	Data Exfiltration
	Red Eyes (Reaper, APT 37, Ricochet Chollima, ScarCruft, Thallium, Group 123, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10)	North Korea	Information theft and espionage
	Dalbit	China	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

Clop ransomware (TA505)

The Clop ransomware claims responsibility for recent cyber attacks that exploited a zero-day vulnerability in the GoAnywhere MFT secure file transfer tool. The group claims to have stolen data from over 130 organizations but refused to provide proof or details about the attacks and extortion.

ProxyShellMiner (Unattributed)

ProxyShellMiner exploits Windows Exchange servers' vulnerabilities, which are used to gain unauthorized access and compromise an organization, leading to the installation of cryptocurrency miners.

DarkBit ransomware (Unattributed)

DarkBit ransomware is a newly emerged threat in the cybersecurity scene that has targeted Technion - Israel Institute of Technology. The attackers behind this assault are opposed to prejudice, fascism, and apartheid and have adopted the hashtag "#HackForGood" to promote their cause. The hackers demanded a ransom of 80 Bitcoin (BTC) valued at approximately USD $1,869,760.

MortalKombat ransomware & Laplas Clipper (Unattributed)

An unidentified actor using the MortalKombat ransomware and a GO variant of the Laplas Clipper malware to steal cryptocurrency from victims. This campaign aims to steal or demand ransom payments in cryptocurrency, which offers anonymity, decentralization, and a lack of regulation.

GlobeImposter (Unattributed)

GlobeImposter, first observed in 2016, has multiple versions and variations that have appeared over the years, and it is most often delivered via phishing emails as an attachment or a link to a malicious attachment. GlobeImposter can delete volume shadow copies, and its delivery methods and functionalities are consistent with those of the new variant TZW.

TOP MITRE ATT&CK TTPS:

T1082 System Information Discovery	**T1547** Boot or Logon Autostart Execution	**T1203** Exploitation for Client Execution	**T1105** Obfuscated Files or Information	**T1059** Command and Scripting Interpreter

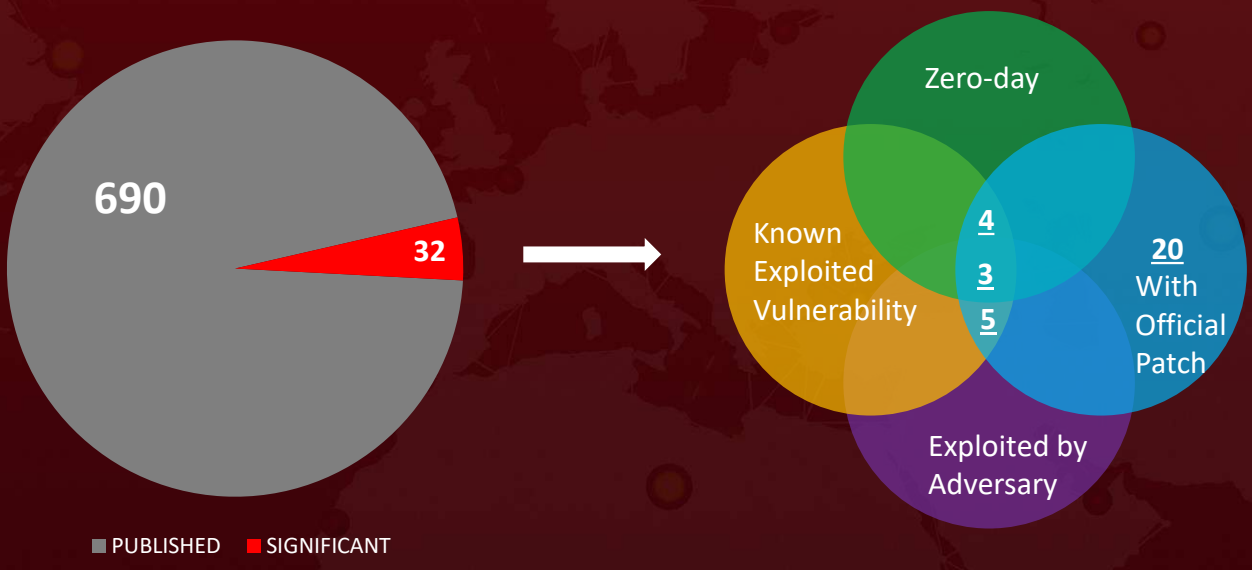
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Vulnerabilities

Seven Zero-days and Twenty-five Notable Mentions

There are seven zero-day vulnerabilities. One of these vulnerabilities, identified as CVE-2023-23529, is related to the MacOS Ventura operating system and allows arbitrary code execution. The second vulnerability, known as CVE-2017-8291, has been exploited by a group called Red Eyes. The third vulnerability, CVE-2018-0802, has been used by a group known as Tonto Team. The fourth vulnerability(CVE-2023-0669) was exploited by a group called TA505 to deploy the Clop ransomware. The last three vulnerabilities, identified as CVE-2023-21823, CVE-2023-21715, and CVE-2023-23376, were addressed by Microsoft as part of their Patch Tuesday updates. Other vulnerabilities have also been addressed by companies such as Microsoft, Apple, and Citrix.



*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 **32 significant vulnerabilities** and block the indicators related to the threat actor **TA505, Nodaria, KillNet, Tonto Team, DEV-0147, Red Eyes, Dalbit** and malware, **Clop ransomware, ProxyShellMiner, DarkBit ransomware, GlobeImposter, MortalKombat ransomware & Laplas 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 **32 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to malware **Clop ransomware, ProxyShellMiner, DarkBit ransomware, GlobeImposter, MortalKombat ransomware & Laplas Clipper** in Breach and Attack Simulation(BAS).

Threat Advisories

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

Clop Ransomware Group Claims Responsibility for GoAnywhere MFT Attacks

Russia-linked Nodaria group employs Graphiron information stealer

Russian Hacker Group Disrupts Relief Efforts for Turkey-Syria Earthquake with DDoS Attacks

Apple Addressed A Zero-day Vulnerability With An Emergency Security Update

Revealing the Tonto Team's Latest Hacks and Menaces

Emerging MortalKombat Ransomware and Laplas Clipper Malware Targeting Cryptocurrency

New China-based Group Expands Operations to Compromise Diplomatic Targets in South America

Microsoft tackles three actively exploited zero-day vulnerabilities and several other bugs

Red Eyes Exploits Hangul EPS Vulnerability and Steganography to Spread Malware

Citrix Resolves Vulnerabilities in Virtual Apps and Workspace Apps

Dalbit Threat Actor Launches APT Attack Campaign Against Multiple Korean Organizations

New Ransomware Campaign "TZW" Linked to GlobeImposter Targets South Korean Organizations

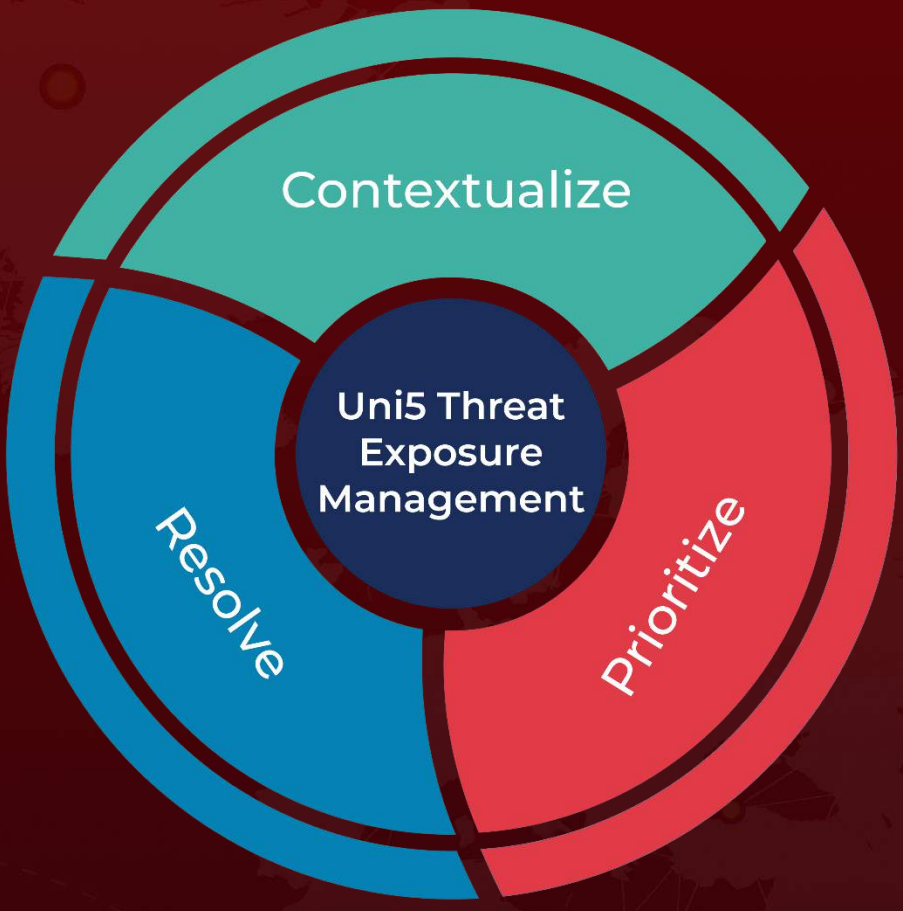
ProxyShellMiner Exploits Windows Exchange Server Vulnerabilities for Cryptocurrency Mining

Israel's Technion Targeted by DarkBit Ransomware's Campaign

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 20, 2023 . 5:00 AM

More at www.hivepro.com