Date of Publication
January 2, 2023

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Actors, Attacks, and Vulnerabilities

26 DECEMBER 2022 to 2 JANUARY 2023

Summary

Threat Actors

Hive Pro discovered two actors that have been active in the past week. The first, **SideCopy**, is a well-known Pakistani threat actor 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. For further details, see the key takeaway section for Actors.

Attacks

We also discovered four new malware strains that have been active over the past week. Several campaigns have been launched to distribute unknown **infostealer malware**. The latest version of **GuLoader** employs new anti-analysis measures as well as code injection redundancy. The undisclosed **Conti ransomware** source code has facilitated the emergence of new ransomware strains. **ArkeiStealer** is a malware family designed by threat actors for enumerating confidential information. For further details, see the key takeaway section for Attacks.

Vulnerabilities

Last week, we discovered **six** vulnerabilities that organizations should prioritize. **Five** of these vulnerabilities were security flaws in the Linux kernel, and **one** was in a WordPress plugin. 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

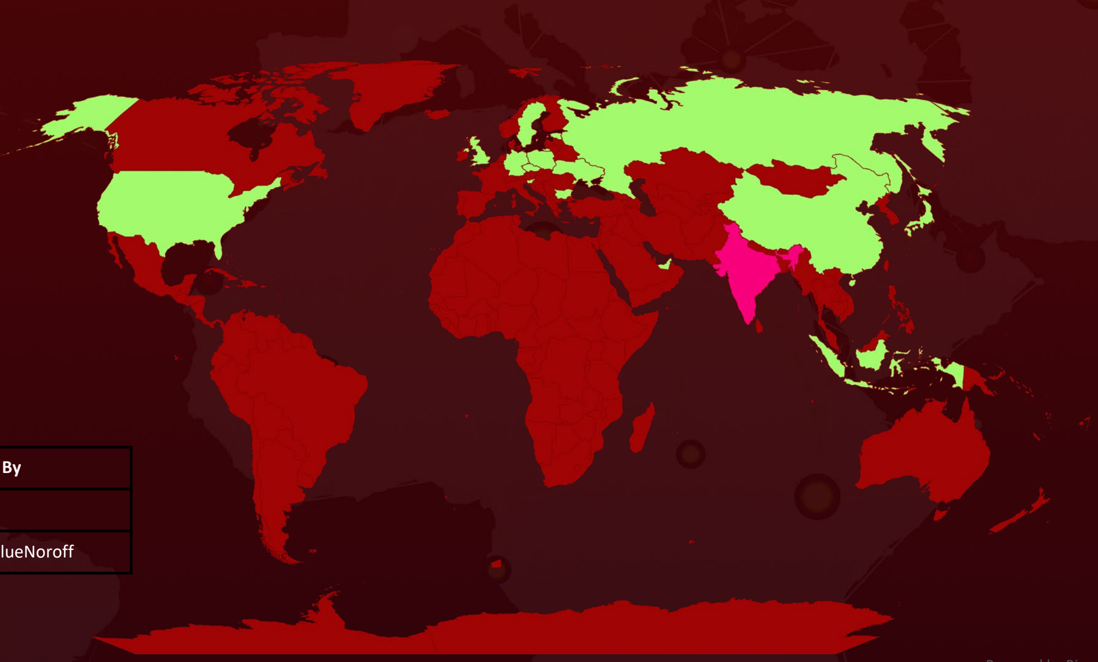
SideCopy (unattributed)

SideCopy threat actors have been linked to the attack campaign STEPPY#KAVACH, which was prominent in 2021 and was first linked to Pakistan. This new SideCopy attack campaign involves dropping LNK files with Remote Access Trojans (RATs) via phishing to target a two-factor authentication solution called Kavach, which is used by Indian officials.

BlueNoroff (unattributed)

BlueNoroff threat actors have been known to circumvent Microsoft Windows' Mark of the Web (MotW) security feature, primarily targeting Japanese enterprises. The Bluenoroff group has used a variety of methods to bypass MotW in order to send malware to its targets, including leveraging trustworthy third-party websites to host malicious information and pivoting domains (names that are identical to or connected to existing domains).

Actor Map



Color	Targeted By
🟢	BlueNoroff
🩷	SideCopy; BlueNoroff

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

*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
	SideCopy	Pakistan	Information theft and Espionage
	BlueNoroff(APT 38, Stardust Chollima, CTG-6459, Nickel Gladstone, T-APT-15, ATK 117)	North Korea	Financial Crime

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

Key Takeaways

Attacks

Unknown InfoStealer Malware (unattributed)

Several efforts have been conducted to distribute InfoStealer malware, which is written in the .NET programming language. In some instances, it has been recognized as PureLogs, a commercial infostealer. Based on the tactics, techniques, and procedures (TTPs) and data gathered, it appears that the attacks were carried out by the same adversary (internally called AUI001). Based on a GitHub account used as a drop point, several vendors refer to this actor as Alibaba2044.

GuLoader (unattributed)

GuLoader is a sophisticated malware downloader that first appeared in 2019 and employs polymorphic shellcode to circumvent typical security solutions. All embedded DJB2 hash values in GuLoader are mapped against every API used by the malware. GuLoader has many anti-analysis measures, making detection and defense difficult. GuLoader uses a multi-stage deployment strategy that involves a VBS dropper file, a bundled payload in the registry, and a PowerShell script.

Putin Team, ScareCrow, BlueSky, and Meow ransomware (unattributed)

New strains of ransomware have been developed using the disclosed source code of the Conti ransomware, which include Putin Team, ScareCrow, BlueSky, and Meow, are being delivered through a variety of methods, including email phishing campaigns and exploit kits. Ransomware attacks can be disruptive and expensive for businesses because they can result in the loss of access to critical data and payment of a ransom to regain access.

ArkeiStealer (unattributed)

ArkeiStealer is an information stealer that was originally discovered in May 2018 and is currently being distributed via Windows Installer packages disguised as trading software. Upon execution, this installer displays a graphical user interface (GUI) that imitates the trading application and drops a SmokeLoader DLL, which starts beaconing out to its C2 at the IP address and a few infiltration tools.

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

Key Takeaways

TOP MITRE ATT&CK TTPS:

- **T1041** Exfiltration Over C2 Channel
- **T1105** Ingress Tool Transfer
- **T1204.001** Malicious Link
- **T1566** Phishing
- **T1059.003** Windows Command Shell
- **T1027** Obfuscated Files or Information
- **T1204** User Execution
- **T1055** Process Injection
- **T1204.002** Malicious File
- **T1059** Command and Scripting Interpreter
- **T1082** System Information Discovery
- **T1071** Application Layer Protocol
- **T1497.001** System Checks
- **T1070.004** File Deletion
- **T1071.001** Web Protocols
- **T1518.001** Security Software Discovery
- **T1564.001** Hidden Files and Directories
- **T1070** Indicator Removal
- **T1059.001** PowerShell
- **T1497** Virtualization/ Sandbox Evasion
- **T1566.002** Spearphishing Link
- **T1518** Software Discovery
- **T1036** Masquerading
- **T1564** Hide Artifacts
- **T1190** Exploit Public-Facing Application
- **T1055.002** Portable Executable Injection
- **T1566.001** Spearphishing Attachment
- **T1083** File and Directory Discovery
- **T1574** Hijack Execution Flow
- **T1588** Obtain Capabilities
- **T1027** Obfuscated Files or Information
- **T1547** Boot or Logon Autostart Execution
- **T1134** Access Token Manipulation
- **T1055** Process Injection
- **T1189** Drive-by Compromise

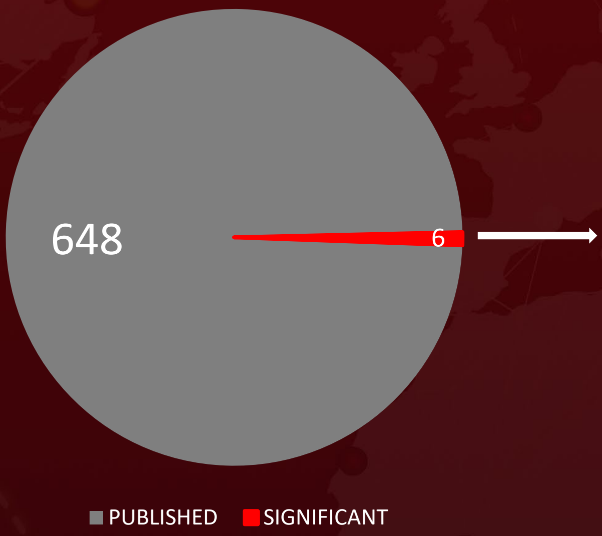
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

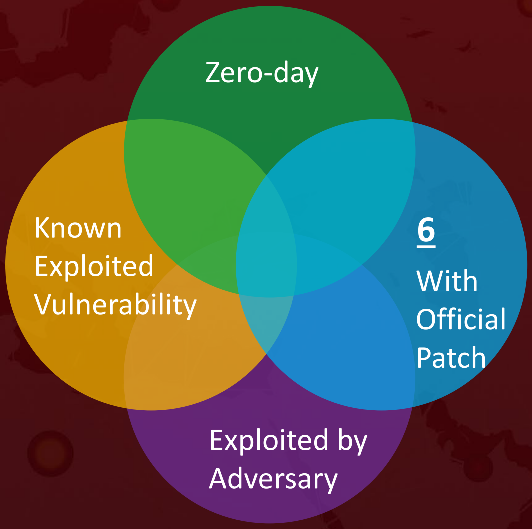
Key Takeaways

Vulnerabilities

Six Notable Mentions

Among the six vulnerabilities, one was found in a WordPress plugin named Yith WooCommerce Gift Cards Premium. Upon exploitation of CVE-2022-45359, unauthenticated attackers can upload files to vulnerable sites. Over 50,000 websites continue to use vulnerable versions of the plugin, enabling threat actors to exploit the bug and plant a backdoor to perform remote code execution attacks. The other five impact the Linux kernel, and by exploiting these vulnerabilities, an unauthenticated remote user can trigger an out-of-bounds read error and read the contents of memory, execute code, and cause a denial-of-service condition on the system.





*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 **six significant vulnerabilities** and block the indicators related to the threat actor **SideCopy**, **BlueNoroff** and malware **Unknown InfoStealer Malware, GuLoader, Putin Team ransomware, ScareCrow ransomware, BlueSky ransomware, Meow ransomware**, and **ArkeiStealer**.

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 **6 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to malware **Unknown InfoStealer Malware, GuLoader, Putin Team ransomware, ScareCrow ransomware, BlueSky ransomware, Meow ransomware**, and **ArkeiStealer** in Breach and Attack Simulation(BAS).

Threat Advisories

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

GuLoader's Advanced Anti-Analysis Techniques

Campaigns Spread InfoStealer Malware Targeting Italy, Germany, and Turkey

SideCopy APT Launches Phishing Campaign Against Indian Government

Bluenoroff Bypasses MoTW to Target Japanese Organizations

The Linux kernel has several security flaws

New Ransomware Variants Created Using Leaked Conti Source Code

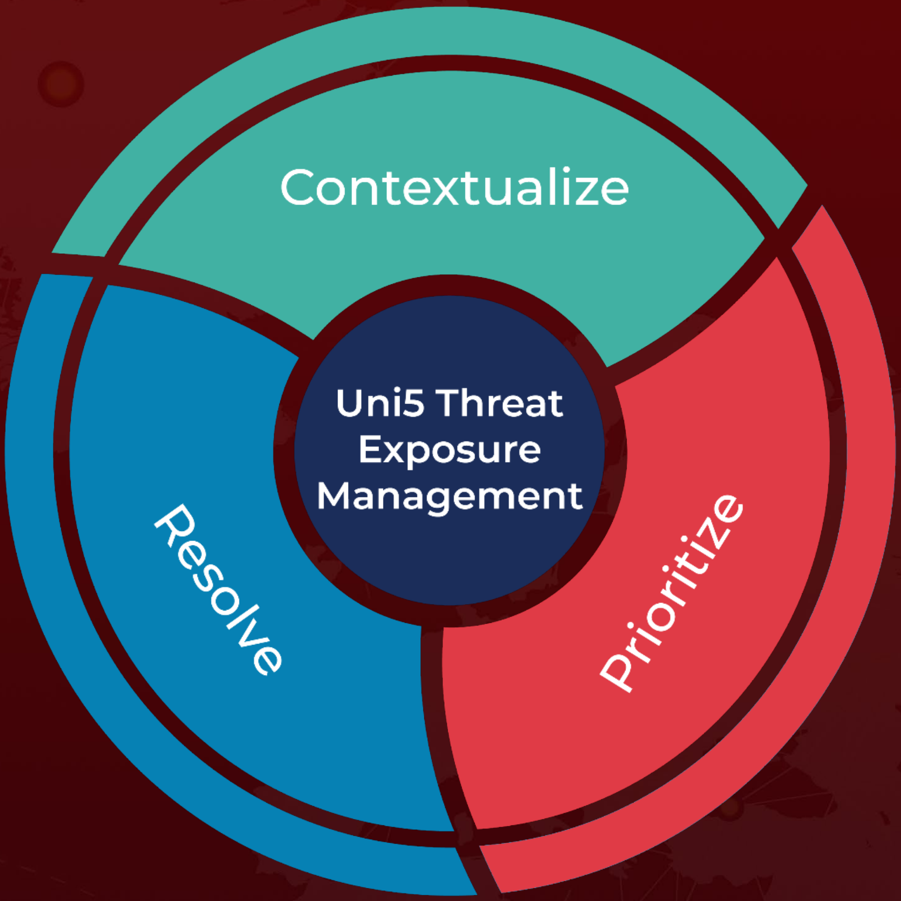
Trading platforms are in jeopardy due to ArkeiStealer

WordPress plugin has been exploited in the wild to mount backdoors

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 2, 2023 • 12:12 AM

More at www.hivepro.com