Date of Publication
January 16, 2023

Hive Pro

Hiveforce Labs

WEEKLY
THREAT DIGEST

Actors, Attacks, and Vulnerabilities

9 to 15 JANUARY 2023

Summary

Threat Actors

Hive Pro discovered four actors that have been active in the past week. The first, **Turla**, is a well-known Russian threat actor known for information theft and espionage. The second, **Saaiwc Group**, is a well-known Southeast Asian threat group that specializes in Information Theft and espionage. The third, **PatchWork**, is a well-known Indian threat actor known for information theft and espionage. The fourth, **NoName057(16)**, is a well-known Russian threat actor known for Hacktivist 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 **LummaC2** is an information stealer being marketed on a Russian website. The Turla Group is delivering the KOPILUWAK reconnaissance software and the QUIETCANARY backdoor to **ANDROMEDA** malware victims in Ukraine. The Saaiwc Group employs a PowerShell backdoor known as **PowerDism**, as well as other custom tools. Patchwork's most recent campaign featured a variant of the **BADNEWS** (Ragnatela). The **Emotet** banking Trojan used the EtterSilent malicious document builder. A new dropper strain called **NeedleDropper** leveraged the CVE-2017-11882 vulnerability to mount intricate payloads. The **Gootkit** loader targets the Australian healthcare industry via SEO poisoning. A new malware called **PoweRAT** combines stealer and RAT capabilities. For further details, see the key takeaway section for Attacks.

Vulnerabilities

Last week, we identified **31** vulnerabilities that organizations should be aware of. Two of these are zero-day vulnerabilities, **one** being in Microsoft Windows Advanced Local Procedure Call, and another being actively exploited by the **Saaiwc group**. 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

Turla (KOPILUWAK, QUIETCANARY, and ANDROMEDA)
The Turla Team operation began profiling victims in September 2022 in order to selectively implant KOPILUWAK, QUIETCANARY, and ANDROMEDA malware transmitted via infected USB sticks. The one-of-a-kind approach of claiming expired domains is used by extensively deployed, financially motivated malware.

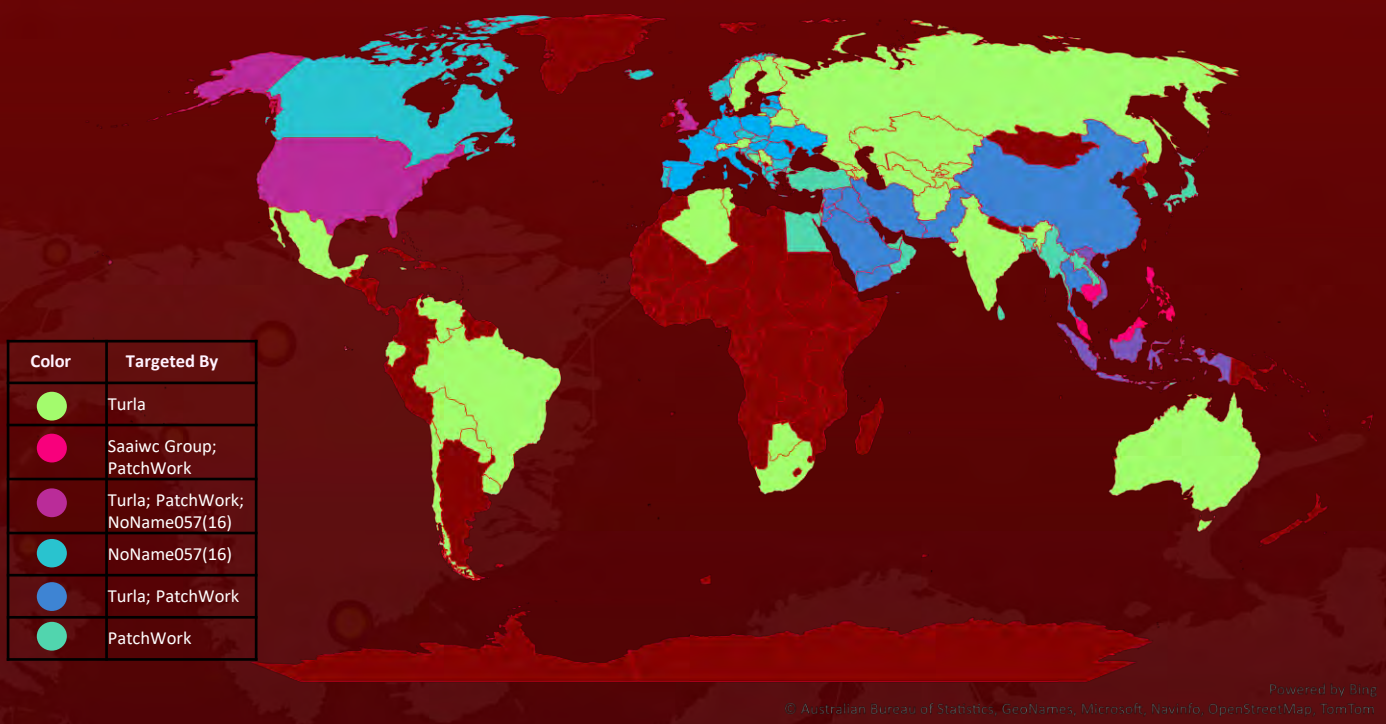
Saaiwc Group (PowerDism)
The Saaiwc Group is a newly discovered APT group that is thought to be a conglomeration of nation-state threat actors from China, North Korea, Iran, and Pakistan. They primarily use an ISO file as a malicious payload, which, when executed, injects a PowerShell command into the local registry after exploiting the vulnerability CVE-2017-0199 and deploying PowerDism, a proprietary PowerShell backdoor.

PatchWork (BADNEWS)
Patchwork is an Indian threat actor that has been active since December 2015. They typically target Pakistan via spear-phishing attacks. In their most recent attack, they used a variation of the BADNEWS (Ragnatela) Remote Administration Trojan, which utilized malicious RTF files.

NoName057(16) (unattributed)
NoName057 (16) is a pro-Russian hacktivist group that has been waging a DDoS attack campaign against Ukraine and NATO organizations. On January 11, 2016, the group targeted the websites of the 2023 Czech presidential election candidates. The gang operates through Telegram channels, a volunteer-fueled DDoS payment program, a multi-OS-supported toolkit, and GitHub.

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

Actor Map



Actor Details

ICON	NAME	ORIGIN	MOTIVE
	Turla(Waterbug,Venomous Bear,Group 88,SIG2,SIG15,SIG23,Iron Hunter,CTG-8875,Pacifier APT,ATK 13,ITG12,Makersmark,Krypton,Belugasturgeon,Popeye,Wraith,TAG-0530)	Russia	Information theft and espionage
	Saaiwc Group (APT-LY-1005, Dark Pink)	China, North Korea, Iran, and Pakistan	Information Theft & espionage
	Patchwork(Dropping Elephant,Chinastrats,APT-C-09,Monsoon,Quilted Tiger,TG-4410,Zinc Emerson,ATK 11,Confucius,EHDevel,Manul,Operation Hangover,Viceroy Tiger,Mahabusa)	India	Information theft and espionage
	NoName057(16)[NoName05716, 05716nnm , Nnm05716]	Russia	Hacktivist & Destruction

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

Key Takeaways

Attacks

LummaC2 Information stealer (unattributed)

LummaC2 Stealer is an information stealer that focuses on Chromium and Mozilla-based browsers. Its purpose is to steal sensitive information, such as cryptocurrency wallets and two-factor authentication (2FA) extensions, from a victim's device. Prices for the malware range from $250 to $200,000 on a Russian website.

KOPILUWAK, QUIETCANARY, and ANDROMEDA malware (Turla)

The Turla Team operation began profiling victims in order to selectively deploy KOPILUWAK, a JavaScript-based reconnaissance utility distributed to victims as a first-stage malicious email attachment; QUIETCANARY, a lightweight .NET backdoor that was primarily used to collect and exfiltrate data from the victim; and ANDROMEDA malware, which remained present by installing another version of itself on the device and spreading through infected USB thumb drives.

PowerDism (Saaiwc Group)

The Saaiwc Group is a new APT group that injects a PowerShell command into the local registry and launches the PowerShell backdoor PowerDism. This allows them to steal information and execute arbitrary commands on targeted systems. They employ custom and self-created tools such as TelePowerBot, KamiKakaBot, Cucky, and Ctealer stealers, as well as the public PowerSploit/Get-MicrophoneAudio utility. In addition, the group is known to leverage the PowerDism Backdoor to exploit the vulnerability CVE-2017-0199 in their attack attempts.

BADNEWS Trojan (PatchWork)

Patchwork's latest campaign employed a variant of the BADNEWS RAT, known as Ragnatela, which was spread through malicious RTF files. The RAT is capable of running commands, collecting directory lists on the victim's device, and downloading additional payloads. The BADNEWS Trojan, the final payload, is embedded as an OLE object within the RTF document and uses a stolen digital signature.

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

Key Takeaways

Attacks

Emotet (unattributed)

Emotet employs the EtterSilent malware document builder and has incorporated a new social engineering method via an Excel attachment instructing how to avoid Microsoft's "Mark-of-the-Web" detection. Emotet is a modular malware variation that acts as a downloader for other malware variants such as TrickBot and IcedID. It has primarily been operated by a Russian-based, financially motivated threat group, though this may no longer be the case in recent campaigns.

NeedleDropper (unattributed)

A new dropper strain called NeedleDropper is being used by attackers to conceal malicious payloads. The dropper is typically delivered through spam email attachments, and it consists of an Excel sheet that takes advantage of the CVE-2017-11882 vulnerability to initiate the vbc.exe (NeedleDropper) script. This script then releases its payload into a temporary folder.

Gootkit loader (unattributed)

Gootkit, also referred to as Gootloader, is a type of malware that is spread through search engine optimization (SEO) poisoning. It is frequently used in advanced persistent threat (APT) operations. Additionally, the malware installs malicious DLLs by utilizing a commonly used legitimate program called VLC Media Player.

PoweRAT (unattributed)

PoweRAT, a newly discovered malware, combines a stealer and a RAT (remote access tool). The malware is distributed via the Python Package Index (PyPI), a software repository for the Python programming language. The malware is found in several packages, including pyrologin, easytimestamp, discorder, discord-dev, style.py, and pythonstyles, all of which start with the setup.py file.

TOP MITRE ATT&CK TTPS:

T1547 Boot or Logon Autostart Execution	**T1059** Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1083** File and Directory Discovery	**T1566** Phishing

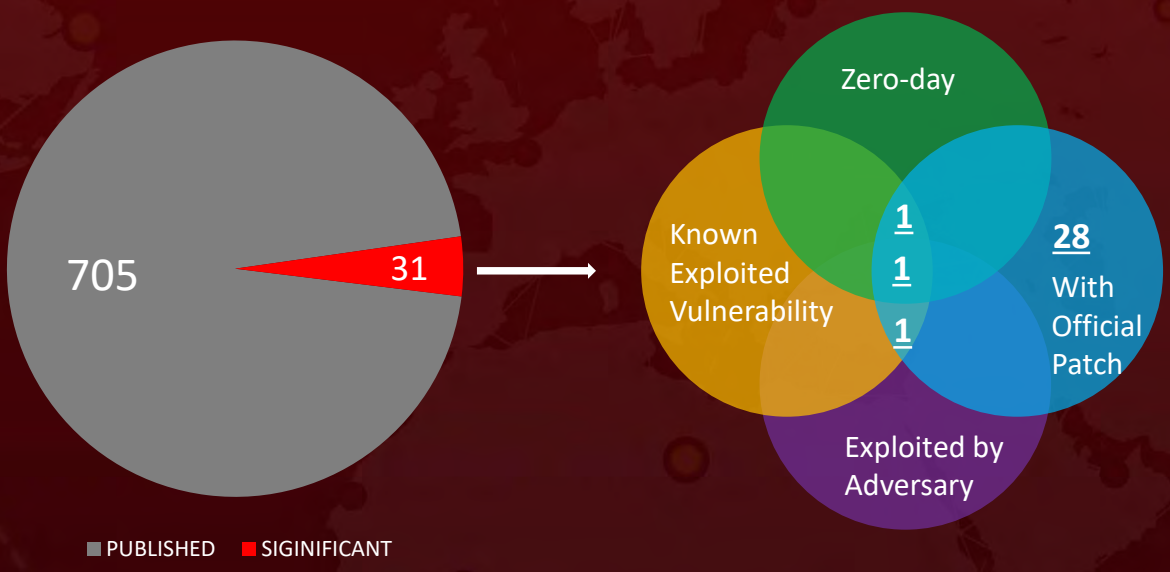
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Vulnerabilities

Two Zero-day and 29 Notable Mentions

Out of the 31 vulnerabilities identified, a zero-day exploit (CVE-2017-0199) is currently being used by the Saaiwc group. Additionally, a zero-day vulnerability in the Windows Advanced Local Procedure Call (ALPC) and 13 other critical vulnerabilities were addressed in the latest Microsoft patch. Among these, the CVE-2022-23529 vulnerability enables attackers to execute remote code on servers that process a maliciously crafted JSON web token (JWT) request. Furthermore, 14 bugs were fixed in the stable channel for Windows, Mac, and Linux in the latest update of Google Chrome 109.



*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 **31 significant vulnerabilities** and block the indicators related to the threat actor **Turla**, **Saaiwc Group**, **PatchWork**, **NoName057(16)** and malware **LummaC2**, **KOPILUWAK**, **QUIETCANARY**, **ANDROMEDA**, **PowerDism**, **BADNEWS**, **Emotet**, **NeedleDropper**, **Gootkit**, and **PoweRAT**.

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 **31 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to malware **LummaC2**, **KOPILUWAK**, **QUIETCANARY**, **ANDROMEDA**, **PowerDism**, **BADNEWS**, **Emotet**, **NeedleDropper**, **Gootkit**, and **PoweRAT** in Breach and Attack Simulation(BAS).

Threat Advisories

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

Information Stealer LummaC2 Targets Browsers and Crypto Wallets

Turla APT used ANDROMEDA malware to infiltrate a variety of industries

Southeast Asian APT Group Saaiwc Targets Military and Financial Departments with Custom Tool

New Vulnerability Found in the JsonWebToken Open-Source Project

PatchWork gang dropped a variant of the BADNEWS Trojan

Google releases Chrome 109 with a range of bug fixes

Microsoft addresses one actively exploited zero-day and numerous critical vulnerabilities

After four months of idleness, Emotet reappears and deploys loaders

NeedleDropper malware leverages a memory corruption flaw in Microsoft to disseminate

GootKit Loader is targeting organizations in the Australian healthcare industry

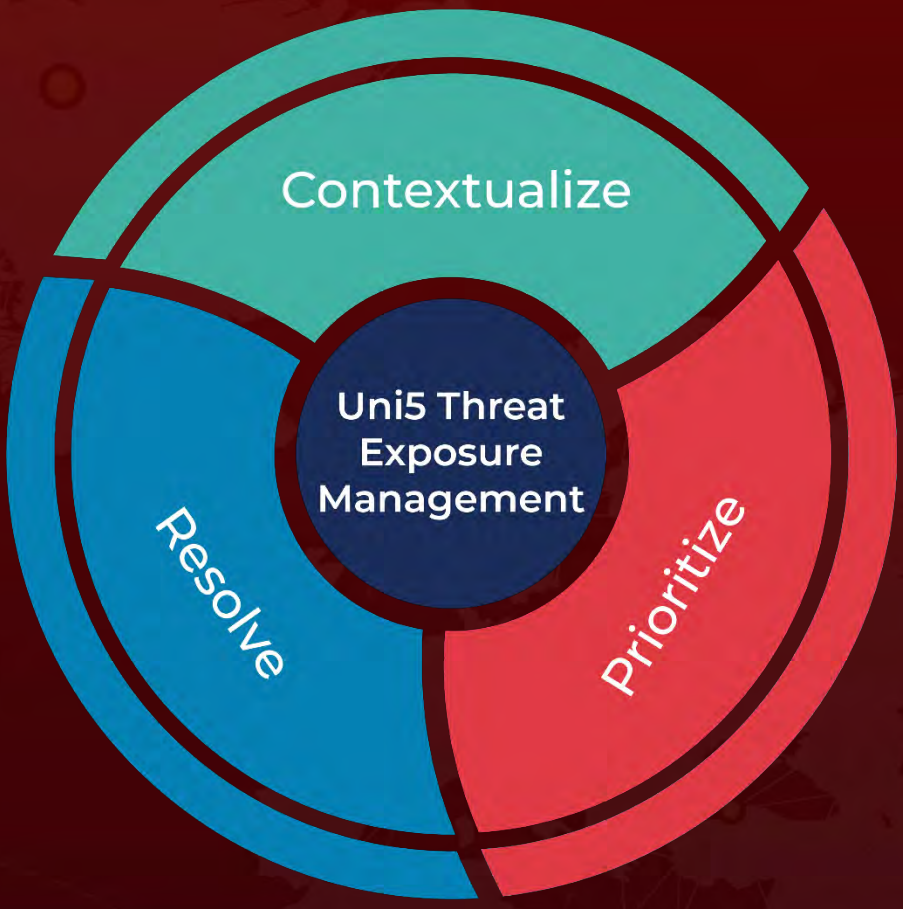
Newly Discovered PoweRAT Malware Distributed through PyPI

Pro-Russian Hacktivist Group NoName057(16) Launches Cyber Attacks on Ukraine and NATO Organizations

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 16, 2023 • 3:00 AM

More at www.hivepro.com