Date of Publication
December 26, 2022

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Actors, Attacks, and Vulnerabilities

19 to 25 DECEMBER 2022

Summary

Threat Actors

Hive Pro has discovered two actors that have been active in the last week. The first, **Gamaredon Group**, is a famous Russian threat actor known for information theft and espionage. The second, **Vice Society**, is a popular ransomware gang known for financial crimes. For further details, see the key takeaway section for actors.

Attacks

We also discovered seven new malware strains that have been active over the last week. **Agenda** is the latest strain of ransomware to use the cross-platform programming language Rust. **SiestaGraph** tends to make use of a .NET API package that can be used in place of the Microsoft Graph API. **RisePro** is a type of malware designed to steal sensitive information from infected computers and send it back to the attacker. A zero-day supply chain attack called "**aioconsol**" was discovered in the Python Package Index (PyPI). **Nokoyawa 2.0** is a 64-bit Windows-based ransomware family that was revised in late September 2022. **Ekipa** is a remote access trojan (RAT) used in targeted attacks that can be purchased on underground forums for the high price of $3,900. **PolyVice**, a ransomware variant developed by Vice Society, uses a strong encryption technique based on the NTRUEncrypt and ChaCha20-Poly1305 algorithms. For further details, see the key takeaway section for attacks.

Vulnerabilities

Last week, we discovered **30** vulnerabilities that organizations should prioritize. Of these, **four** were zero-days that were addressed by Microsoft. The remaining **26** vulnerabilities were addressed by their 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

Gamaredon Group (unattributed)

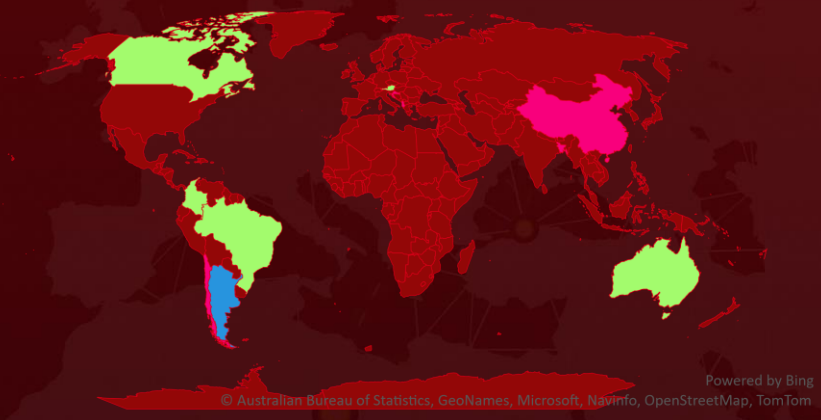
Gamaredon Group has employed fast flux DNS to improve its operational effectiveness. Fast flux DNS involves frequently pivoting through multiple IPs, using each for a brief time to make it difficult to block malicious domains using IP-based lists. Threat actors often hijack legitimate services to query IP addresses in order to avoid DNS logging for malicious domains.

Vice Society (PolyVice)

Vice Society has employed a new custom-designed ransomware called "PolyVice" to gain initial access to a network. To do this, the gang uses compromised credentials and exploits known vulnerabilities like PrintNightmare.

Actor Map

Color	Targeted By
	Gamaredon Group
	Vice Society
	Vice Society; Gamaredon Group



Actor Details

ICON	NAME	ORIGIN	MOTIVE
	Gamaredon Group(Winterflounder, Primitive Bear, BlueAlpha, Blue Otso, Iron Tilden, Armageddon, SectorC08, Callisto, Shuckworm, Actinium, DEV-0157, UAC-0010)	Russia	Information theft and espionage
	Vice Society	Unknown	Financial crime

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

Key Takeaways

Attacks

Agenda Ransomware (unattributed)

Agenda is the latest strain of ransomware to use the cross-platform programming language Rust. The ransomware-as-a-service (RaaS) group Agenda, attributed to an operator named Qilin, has been linked to a number of attacks mainly targeting the manufacturing and IT industries.

SiestaGraph (unattributed)

SiestaGraph tends to make use of a .NET API package that can be used in place of the Microsoft Graph API. After gaining initial access, the threat actor gathers information on domain users and groups, and exports and archives victim mailboxes as PST files. A customized version of the IIS backdoor called DoorMe, with enhanced capabilities, was used to allocate shellcode and load additional implants.

RisePro (unattributed)

RisePro is a type of malware designed to steal sensitive information from infected computers and send it back to the attacker. It was first seen being sold on the illegal Russian online marketplace on December 13. The fact that RisePro is being sold on the Russian market may suggest that it is gaining popularity among cybercriminals.

Aioconsol (unattributed)

A zero-day supply chain attack called "aioconsol" was discovered on December 9, 2022, in a Python package published on the Python Package Index (PyPI) on December 6, 2022. All three versions of the package were published on the same day and contain malicious code that writes a binary file called "test.exe“ and executes it as part of the installation process.

Nokoyawa 2.0 ransomware (unattributed)

Nokoyawa is a 64-bit Windows-based ransomware family that first appeared in early February 2022. The threat group behind Nokoyawa conducts double-extortion ransomware attacks, first stealing data from companies and then encrypting files and demanding a ransom payment. The 2.0 version of the Rust-based Nokoyama ransomware was revised in late September 2022

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

Key Takeaways

Ekipa RAT (unattributed)

Ekipa is a remote access trojan (RAT) used in targeted attacks that can be purchased on underground forums for the high price of $3,900. It primarily spreads and operates using Microsoft Office and Visual Basic for Applications. The trojan also comes with a control panel and tools for creating malicious macros in MS Word, Excel add-ins, and MS Publisher.

PolyVice ransomware (Vice Society)

Vice Society is a well-established ransomware group that has successfully targeted a range of enterprises. They aim to maximize their financial gain by using the standard double extortion strategy. In recent attacks, the group has employed a new custom-designed ransomware called "PolyVice," which uses a strong encryption technique based on the NTRUEncrypt and ChaCha20-Poly1305 algorithms.

TOP MITRE ATT&CK TTPS:

T1190 Exploit Public-Facing Application	**T1203** Exploitation for Client Execution	**T1204** User Execution	**T1059** Command and Scripting Interpreter	**T1036** Masquerading
T1588 Obtain Capabilities	**T1102** Web Service	**T1574** Hijack Execution Flow	**T1078** Valid Accounts	**T1552** Unsecured Credentials
T1497 Virtualization/ Sandbox Evasion	**T1027** Obfuscated Files or Information	**T1047** Windows Management Instrumentation	**T1547** Boot or Logon Autostart Execution	**T1053** Scheduled Task/Job
T1560 Archive Collected Data	**T1055** Process Injection	**T1021** Remote Services	**T1068** Exploitation for Privilege Escalation	**T1564** Hide Artifacts

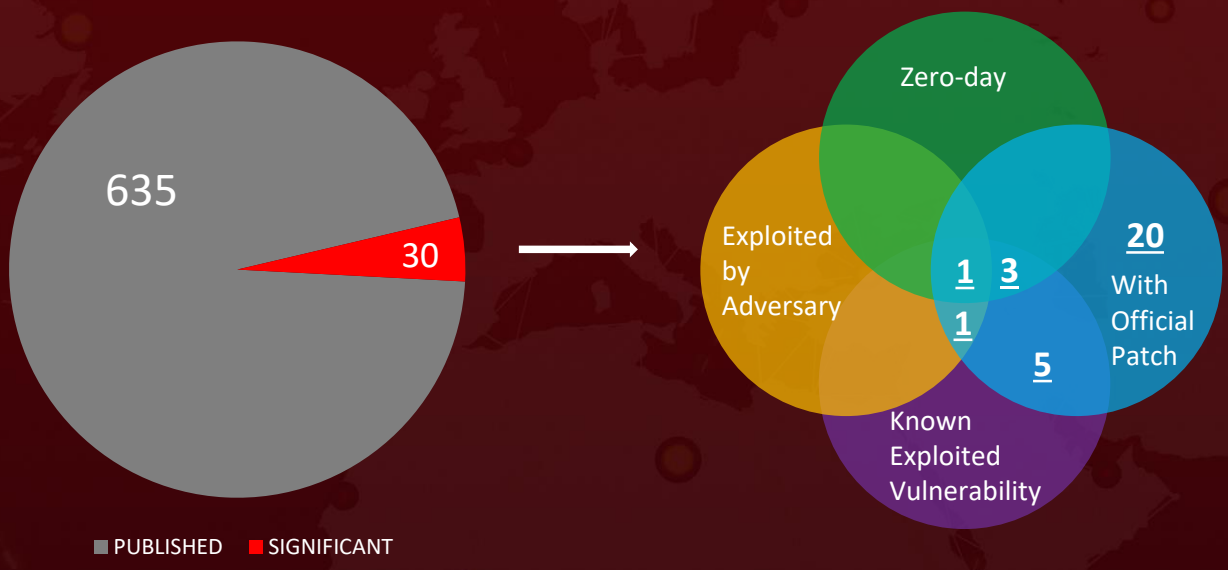
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Vulnerabilities

Four Zero-Days & 20 Notable Mentions

Two of these vulnerabilities, ProxyNotShell (CVE-2022-41082 and CVE-2022-41040), have been patched in December but remain under active exploitation. The third zero-day vulnerability is the well-known PrintNightmare vulnerability (CVE-2021-34527) that is being exploited by Vice Society. The fourth zero-day is the CVE-2017-0144 vulnerability, which affected the SMB protocol and, like the CVE-2022-37958 vulnerability, can affect a wide range of protocols to cause remote code execution. Additionally, Apple, Samba, Cisco, and Microsoft addressed multiple security issues 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 used as a guide to help security teams prioritize the **30 significant vulnerabilities** and block the indicators related to the threat actors **Gamaredon**, **Vice Society** as well as the malware **Agenda Ransomware**, **SiestaGraph**, **RisePro**, **Aioconsol**, **Nokoyawa 2.0 Ransomware**, **Ekipa RAT** and **PolyVice Ransomware**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, who can get comprehensive insights into their threat exposure and take action easily through the HivePro Uni5 dashboard by:

- Running a scan to discover the assets impacted by the **30 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to **Agenda Ransomware**, **SiestaGraph**, **RisePro**, **Aioconsol**, **Nokoyawa 2.0 Ransomware**, **Ekipa RAT** and **PolyVice Ransomware** in Breach and Attack Simulation(BAS)

Threat Advisories

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

Ekipa RAT: A High-Priced and Evolving Threat for Targeted Attacks

Nokoyawa 2.0: A Reworked Rust-Based Ransomware

Two Zero-day Supply Chain Attacks Found in the Python Package Index

Apple addresses macOS Dirty Cow, Achilles, and other flaws

Outlining a new SiestaGraph backdoor

Agenda ransomware made its return with a Rust variant

Samba addressed a series of severe vulnerabilities

Multiple Old Vulnerabilities actively exploiting in Cisco Products

RisePro: A New Threat Emerges on the Russian Online Marketplace

New Exploit Method that Bypasses ProxyNotShell Mitigations

Gamaredon APT cyber feud strikes Ukrainian entities

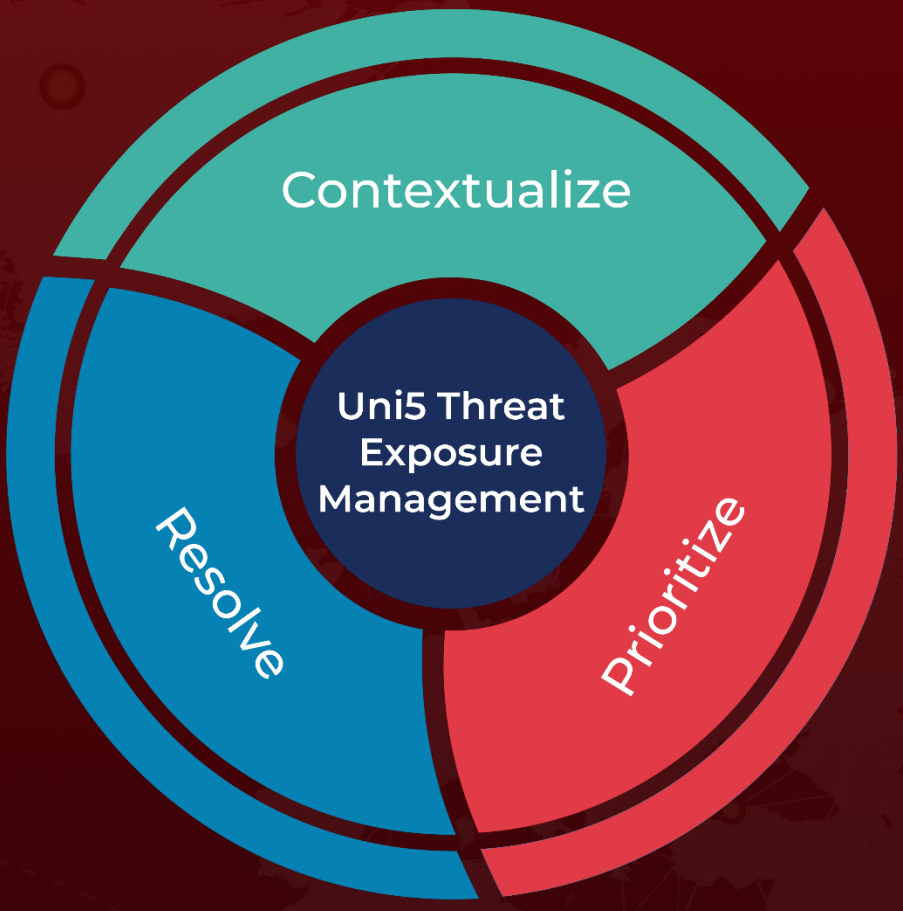
Microsoft Rolled Out SPNEGO NEGOEX Critical Vulnerability

Vice Society gang switches to new custom ransomware

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 26, 2022 • 3:00 AM

More at www.hivepro.com