Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

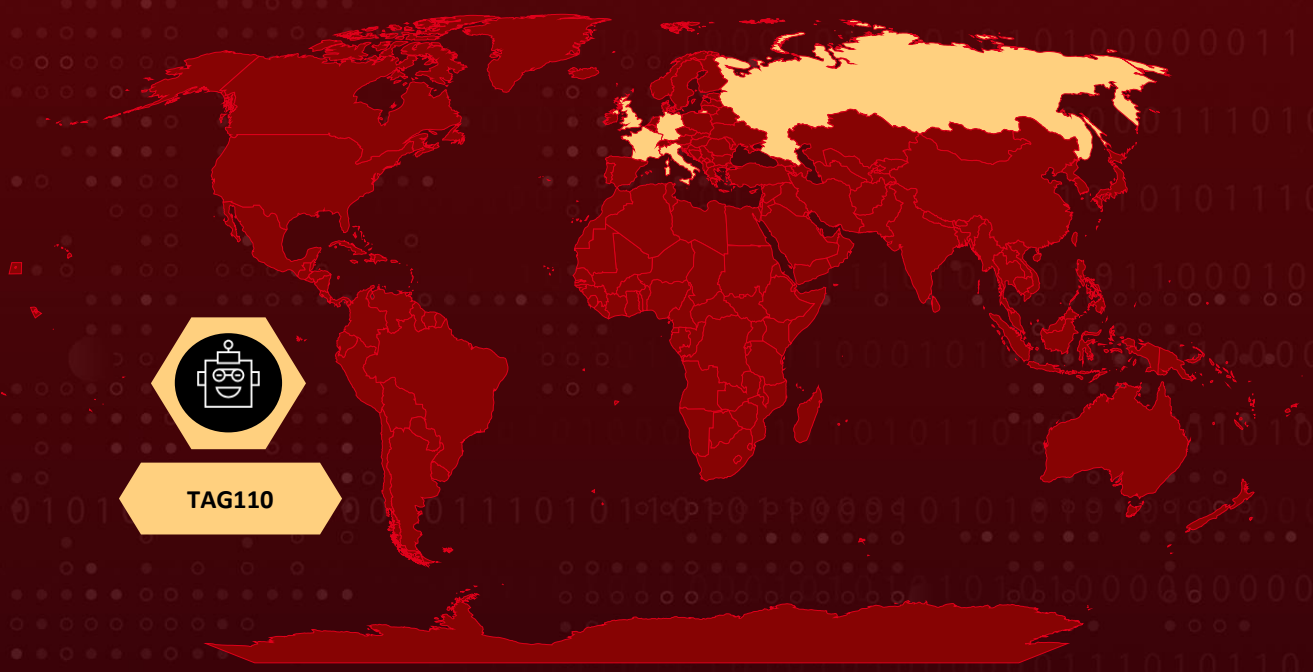
TAG-110: A Persistent Threat to Asia and Europe

Date of Publication	Admiralty Code	TA Number
November 26, 2024	A1	TA2024444

Summary

First Appearance: July 2024
Malware: HATVIBE and CHERRYSPY
Threat Actor: TAG110 (UAC-0063)
Targeted Countries: Central Asia, Europe, and East Asia
Targeted Industries: Government entities, Human rights groups, and Educational institutions
Affected Platforms: Windows
Attack: TAG-110, a Russia-aligned threat group linked to APT28, is conducting a cyber-espionage campaign targeting government, human rights, and educational institutions in Central Asia, East Asia, and Europe. Using custom malware HATVIBE and CHERRYSPY, the group infiltrates systems via phishing and exploits, focusing on data exfiltration and intelligence gathering. These activities align with Russian geopolitical objectives, particularly in maintaining influence in post-Soviet states.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-23692	Rejetto HTTP File Server Template Injection Vulnerability	Rejetto HTTP File Server	✗	✓	✗

Attack Details

#1

A new cyber-espionage campaign by Russian-linked hacking group TAG-110 (aka UAC-0063) is targeting government, NGO, and educational institutions across Europe, Central Asia, and East Asia. This campaign employs custom malware tools, specifically HATVIBE and CHERRYSPY, which have been deployed against government entities, human rights organizations, and educational institutions. Since its inception in July 2024, the campaign has identified 62 unique victims across eleven countries, with a notable concentration in Central Asia.

#2

The malware employed in this campaign serves distinct functions; HATVIBE acts as a loader that facilitates the deployment of CHERRYSPY, a Python-based backdoor designed for espionage and data exfiltration. Initial access to target systems is often gained through phishing emails or by exploiting vulnerabilities in web applications. The sophisticated nature of the malware allows it to evade detection through layers of obfuscation and encryption, complicating efforts to identify and neutralize the threat.

#3

TAG-110's activities appear to align closely with Russian geopolitical interests, particularly in maintaining influence over post-Soviet states amid ongoing tensions following Russia's invasion of Ukraine. The intelligence gathered through these cyber operations is likely intended to bolster Russia's military strategies and inform its understanding of regional dynamics. The group’s tactics and objectives align with those of TAG-110, linked to the Russian APT group BlueDelta (aka APT28), though the direct connection between the two remains moderately confident.

#4

As the threat landscape evolves, TAG-110 is expected to continue its operations with a focus on Central Asia and Ukraine's allies. Organizations are urged to remain vigilant and proactive in strengthening their defenses against such sophisticated cyber threats.

Recommendations

Patch Vulnerabilities: Prioritize patching known vulnerabilities in web-facing services such as Rejetto HTTP File Server, which TAG-110 exploits. Implement a robust vulnerability management program to address critical and high-severity flaws promptly.

Enhance Email Security: Implement advanced email filtering solutions to detect and block phishing attempts. Use technologies like DMARC, DKIM, and SPF to authenticate incoming emails and reduce the risk of spoofing.

Implement Robust Access Controls: Enforce the principle of least privilege, restricting access to critical systems and data, and closely monitor user permissions to prevent lateral movement by attackers.

Enhance Incident Response Capabilities: Develop and regularly test a proactive incident response plan that includes scenarios involving sophisticated malware, persistence mechanisms, and data exfiltration techniques.

Network Segmentation: Segment networks to limit the lateral movement of attackers within the organization. This can help contain potential breaches and minimize damage in case of an attack.

Advanced Threat Detection and Response: Deploying advanced threat detection and response solutions is essential for identifying and mitigating sophisticated attacks. This includes using Endpoint Detection and Response (EDR) tools, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS). These tools can detect unusual activity and provide alerts on potential intrusions, allowing for quicker response times.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0011 Command and Control	T1583 Acquire Infrastructure	T1583.003 Virtual Private Server
T1190 Exploit Public-Facing Application	T1566 Phishing	T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter
T1059.005 Visual Basic	T1204 User Execution	T1204.002 Malicious File	T1053 Scheduled Task/Job

T1053.005 Scheduled Task	T1027 Obfuscated Files or Information	T1027.013 Encrypted/Encoded File	T1218 System Binary Proxy Execution
T1218.005 Mshta	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1573 Encrypted Channel
T1573.001 Symmetric Cryptography	T1573.002 Asymmetric Cryptography		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	trust-certificate[.]net, experience-improvement[.]com, telemetry-network[.]com, shared-rss[.]info, game-wins[.]com, internalsecurity[.]us, errorreporting[.]net, lanmangraphics[.]com, retaildemo[.]info, tieringservice[.]com, enrollmentdm[.]com
IPv4	5[.]45[.]70[.]178, 45[.]136[.]198[.]18, 45[.]136[.]198[.]184, 45[.]136[.]198[.]189, 46[.]183[.]219[.]228, 84[.]32[.]188[.]23, 185[.]62[.]56[.]47, 185[.]158[.]248[.]198, 185[.]167[.]63[.]42, 194[.]31[.]55[.]131, 212[.]224[.]86[.]69
SHA256	332d9db35daa83c5ad226b9bf50e992713bc6a69c9ecd52a1223b81e992bc725

Patch Link

https://www.rejetto.com/hfs/

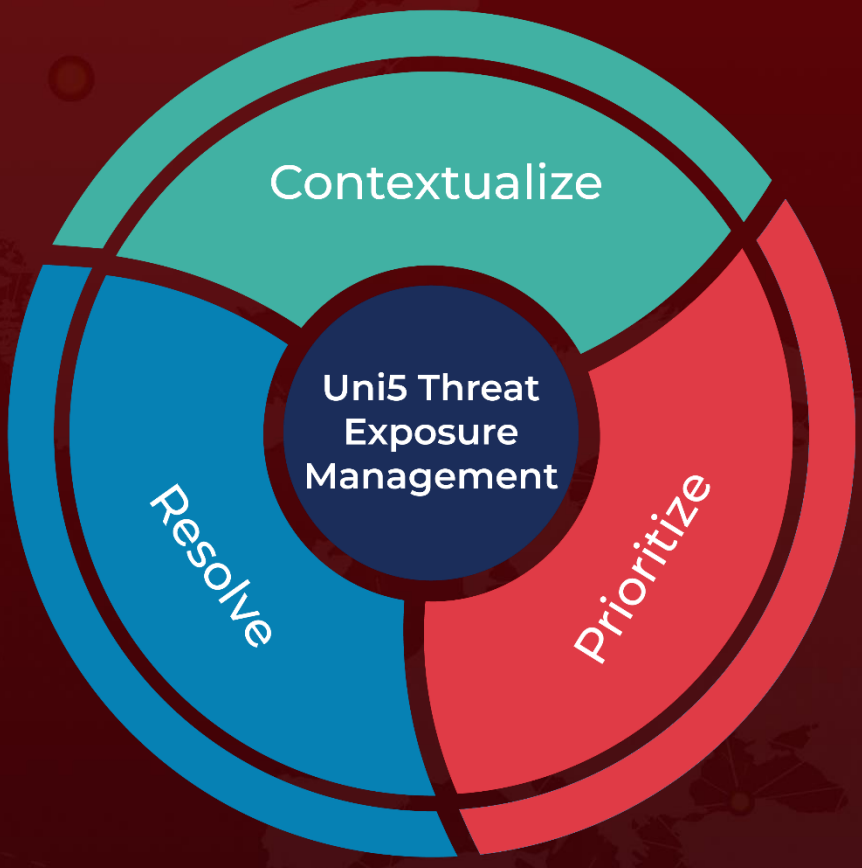
References

https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-1121.pdf

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

November 26, 2024 . 6:30 AM

More at www.hivepro.com