Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

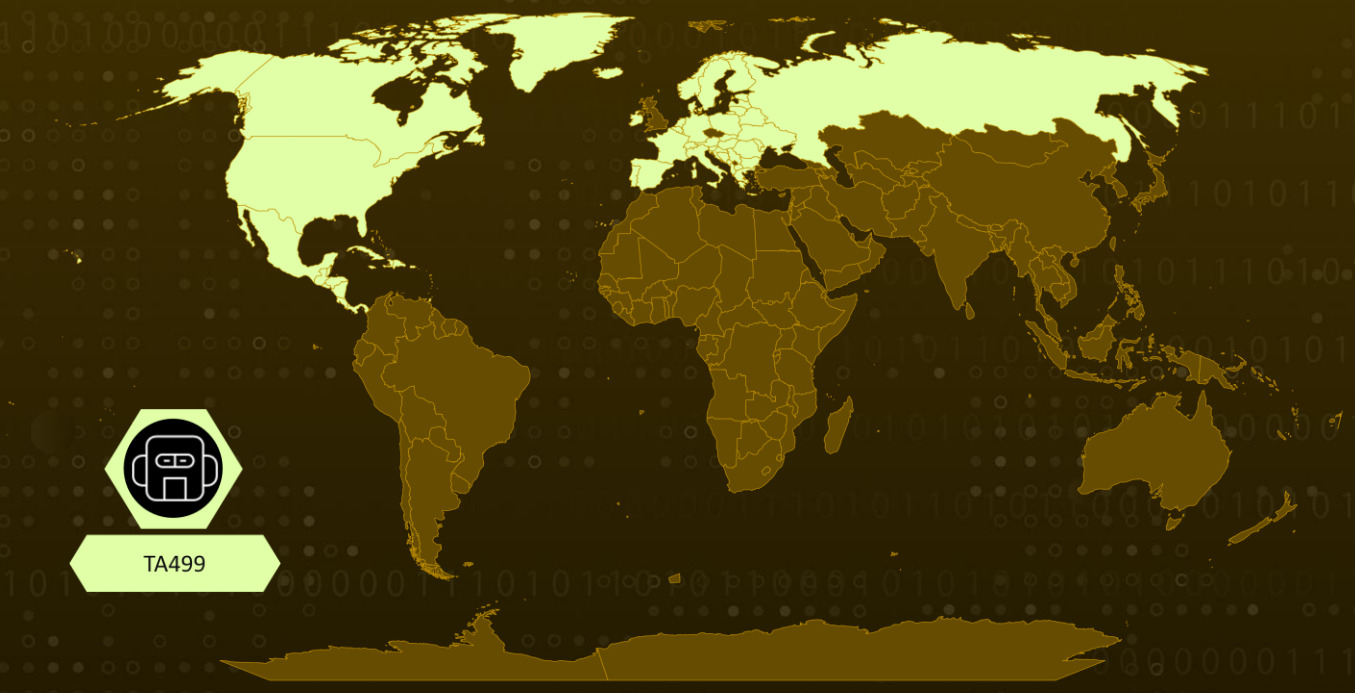
Tracking the Malicious Email Campaigns of Russia-Aligned TA499

Date of Publication	Admiralty Code	TA Number
March 9, 2023	A1	TA2023125

Summary

First Appearance: Early 2021
Actor Name: TA499
Target Region: North America and Europe
Target Sectors: Government

Actor Map



Actor Details

#1

TA499 is a group of threat actors aligned with the Russian state that engages in impersonation-based, patriotically motivated misinformation campaigns. They use email to target high-profile individuals, including government officials, businesspeople, and celebrities, who have made public statements in favor of sanctions against Russia, against the detainment of Alexei Navalny, or in support of Ukraine.

#2

The emails are designed to solicit information or entice the targets into further contact via phone calls or remote video. The group has been tracked by researchers since early 2021, and their campaigns intensified in late January 2022, after Russia invaded Ukraine. TA499 has not used malware in its emails, relying instead on social engineering techniques to achieve its goals.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
TA499(Vovan; Lexus)	Russia **MOTIVE** Sabotage and Espionage	North America and Europe	Government

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0011 Command and Control	T1566 Phishing	T1204 User Execution	T1547 Boot or Logon Autostart Execution
T1036 Masquerading	T1102 Web Service		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	office@oleksandrmerezhko[.]com secretary.mfa@gmail[.]com embassy.usa@ukr[.]net embassy.us@ukr[.]net s.dorenko@ukr[.]net embassy.chernysh@ukr[.]net office@iaea[.]co[.]uk iaea[.]com[.]uk oleksandrmerezhko[.]com navalny[.]team office@oleksandrmerezhko[.]com lvolkov@navalny[.]team julia@navalny[.]team

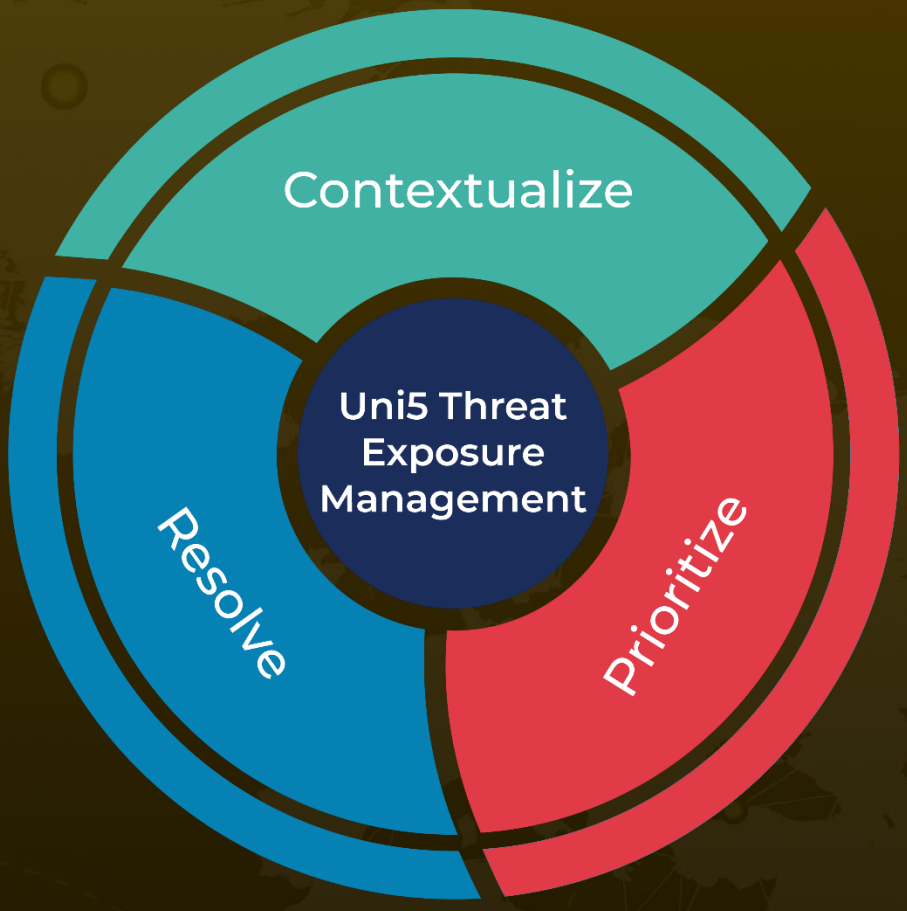
References

https://www.proofpoint.com/us/blog/threat-insight/dont-answer-russia-aligned-ta499-beleaguers-targets-video-call-requests

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

March 9, 2023 • 3:20 AM

More at www.hivepro.com