Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

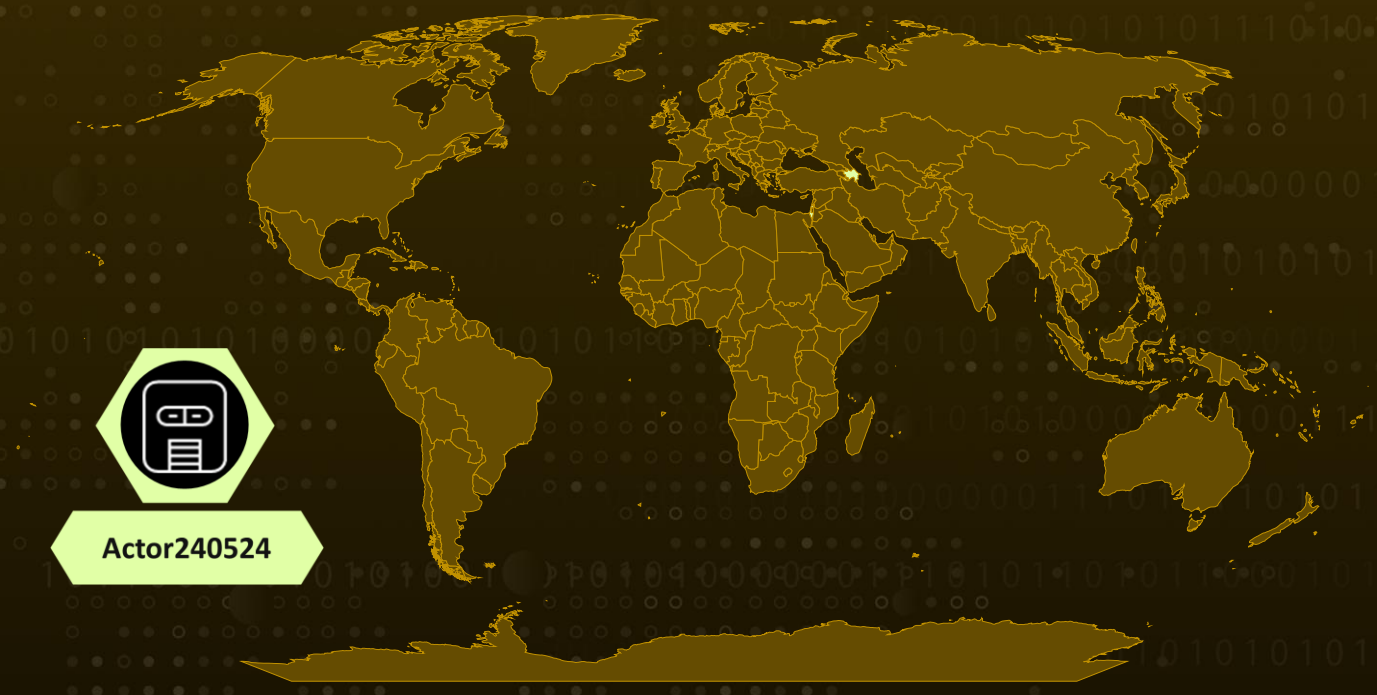
Actor240524 the New Face of Geopolitical Cyber Espionage

Date of Publication	Admiralty Code	TA Number
August 16, 2024	A1	TA2024313

Summary

Attack Commenced: July 2024
Threat Actor: Actor240524
Malware: ABCloader, ABCsync
Targeted Countries: Azerbaijan, Israel
Targeted Industries: Government, Diplomats
Attack: A newly discovered cyber threat group, Actor240524, has launched a series of targeted cyberattacks against diplomatic entities in Azerbaijan and Israel. These cyberattacks primarily targeted government diplomats and officials, underscoring the strategic and geopolitical significance of these nations.

Attack Regions



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

Attack Details

#1 A recent surge in cyberattacks linked to a newly identified threat group, known as Actor240524, has attracted significant attention due to its highly targeted operations against diplomatic entities in Azerbaijan and Israel. The nation-state behind these attacks remains unknown. The primary targets were government diplomats and officials in both countries, underscoring a focus on the geopolitical and strategic interests of these nations.

#2 The attack chain executed by Actor240524 was intricate and meticulously planned. It began with a spear-phishing campaign, where the attackers tricked their targets with emails that seemed legitimate and highly relevant.

#3 The phishing emails contained a Word document embedded with VBA macros, which delivered a novel Trojan called ABCloader upon execution. ABCloader then decrypted and loaded an ABCsync DLL, enabling communication with the command-and-control (C2) server for remote command execution. The malware employed advanced anti-sandbox and anti-debugging techniques to evade detection.

#4 The motive behind these attacks appears to be espionage, with the primary goal of gathering intelligence on the diplomatic communications and strategic plans of Azerbaijan and Israel. By targeting government officials and diplomats, the attackers aimed to access sensitive information that could potentially influence geopolitical dynamics in the region.

Recommendations

Enhance Email Security: To enhance email security, deploy advanced email filtering solutions that leverage machine learning and threat intelligence to effectively filter out phishing emails and malicious attachments. Additionally, conduct regular training for employees to help them recognize and understand the risks associated with opening suspicious email attachments or links.

Use Network Monitoring Tools and Conduct Regular Audits: Deploy network monitoring tools such as IDS and IPS to detect unusual traffic patterns and communications with command-and-control (C2) servers. Implement Network Traffic Analysis (NTA) solutions to monitor for abnormal behavior and perform routine network audits to identify and address potential security gaps, including network segmentation to limit the lateral movement of attackers.

Encrypt Sensitive Data: Ensure that all sensitive diplomatic communications and strategic data are encrypted using strong encryption algorithms, both in transit and at rest. Implement end-to-end encryption for email and messaging services and employ data encryption solutions for storage and backup systems to protect against unauthorized access.

Verify Software Sources and Monitor Third-Party Risks: Implement strict software supply chain management practices, including verifying the authenticity and integrity of software and updates before installation. Use code signing and checksum verification to ensure software integrity. Assess and monitor third-party vendors and partners for potential security risks and include supply chain security in vendor management policies.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**TA0010** Exfiltration	**T1059.005** Visual Basic
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1204** User Execution	**T1204.002** Malicious File
T1059 Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1574** Hijack Execution Flow	**T1036** Masquerading
T1070 Indicator Removal	**T1082** System Information Discovery	**T1497** Virtualization/Sandbox Evasion	**T1041** Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
File Name	iden.doc, MicrosoftWordUpdater.log
File Path	C:\Users\Public\Documents\MicrosoftWordUpdater.log, C:\Users\AppData\Local\Microsoft\Edge\User Data\Synchronize, C:\Windows\System32\Windows.UI.FileExplorer.dll
MD5	1ee73b17111ab0ffb2f62690310f4ada
SHA1	3d3e2e367fe9b358bbb91e5cbcbe90250c220648
SHA256	31300645371f90f83ca6aa058503fa7c2ba386f496ac181a6b287ba7ba1ea10e, a250740948aba579462397ac95ff10e6b0ee952c2af7d9d726cbfde9da1eaaff, 6fa56ab1ce0d4fc9db6422bff8caa38bea1bdb9abbe4a48ecfb364eb20c7ac1a
IPv4:Port	185[.]23[.]253[.]143[:]36731

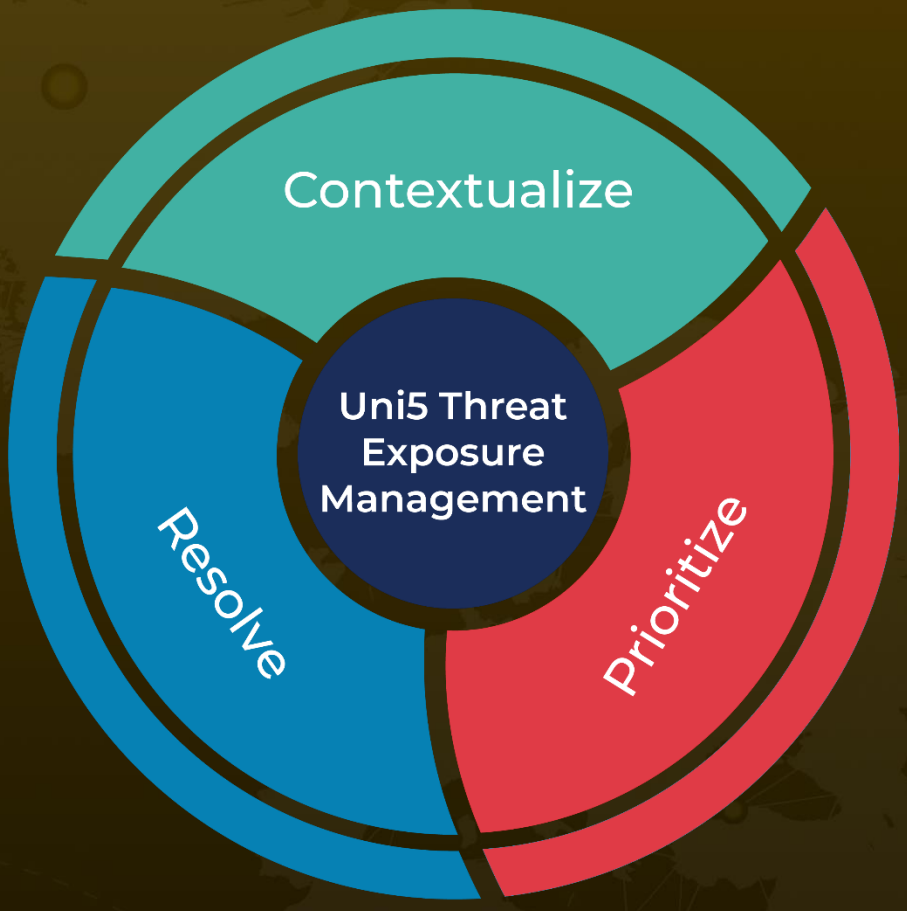
References

https://nsfocusglobal.com/new-apt-group-actor240524-a-closer-look-at-its-cyber-tactics-against-azerbaijan-and-israel/

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

August 16, 2024 • 4:30 AM

© 2024 All Rights are Reserved by Hive Pro

More at www.hivepro.com