Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

TA402's Covert Operation Takes Aim at the Middle East

Date of Publication	Admiralty Code	TA Number
November 15, 2023	A1	TA2023461

Summary

Attack Began: July 2023
Threat Actor: TA402 (aka Extreme Jackal, Molerats, Gaza Cybergang, Gaza Hackers Team, Aluminum Saratoga, ATK 89, TAG-CT5)
Malware: IronWind, SharpSploit
Attack Region: Middle East
Targeted Industries: Government, Foreign Affairs
Attack: TA402 (aka Extreme Jackal) launched sophisticated phishing campaigns targeting government entities in the Middle East. The objective was to deploy a newly developed initial access downloader called IronWind, employing an economic-themed social engineering lure.

Attack Regions

Attack Details

#1 Between July and October 2023, TA402, also known as Extreme Jackal, initiated phishing campaigns targeting government entities in the Middle East. These campaigns aim to deploy a novel initial access downloader named IronWind. Employing an economic-themed social engineering lure, TA402 utilized a compromised Ministry of Foreign Affairs email account to target Middle Eastern government bodies.

#2 TA402 has been active since 2012 and exhibits tactical similarities with a pro-Hamas hacking group known as **Arid Viper** (APT-C-23). TA402 consistently updates its malware delivery methods, employing Dropbox links, XLL file attachments, and RAR archives to disseminate IronWind.

#3 The downloader is designed to connect with a server controlled by the attacker to retrieve additional payloads. These payloads include a post-exploitation toolkit named SharpSploit, which is a .NET post-exploitation library written in C#. This process follows a multi-stage sequence. Notably, TA402 employs geofencing techniques to complicate detection efforts.

#4 Operating in alignment with Palestinian espionage goals and emphasizing intelligence gathering, TA402 remains a persistent and innovative threat actor. The group routinely adapts its attack methods and malware to support its cyber espionage manifest.

Recommendations

Email Security Measures: Utilize robust email security solutions to identify and block malicious attachments and links. Explore the implementation of advanced threat protection (ATP) and email filtering technologies to sandbox suspicious or untrusted URLs.

Strengthen Endpoint Security: Fortify endpoint security measures to detect and prevent the execution of malicious payloads, such as IronWind and its associated post-exploitation toolkit, SharpSploit. This involves utilizing advanced endpoint protection solutions and keeping them updated.

User Awareness Training: Conduct regular phishing awareness training for employees to educate them about common phishing tactics and how to recognize suspicious emails. Simulated phishing exercises can be particularly effective in reinforcing security awareness.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery
TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control	T1059 Command and Scripting Interpreter
T1072 Software Deployment Tools	T1083 File and Directory Discovery	T1082 System Information Discovery	T1047 Windows Management Instrumentation
T1560 Archive Collected Data	T1105 Ingress Tool Transfer	T1041 Exfiltration Over C2 Channel	T1543 Create or Modify System Process
T1204 User Execution			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	9b2a16cbe5af12b486d31b68ef397d6bc48b2736e6b388ad8895b588f1831f47, 5d773e734290b93649a41ccda63772560b4fa25ba715b17df7b9f18883679160, 19f452239dadcd7544f055d26199cb482c1f6ae5486309bde1526174e926146a, a4bf96aee6284effb4c4fe0ccfee7b32d497e45408e253fb8e1199454e5c65a3, 26cb6055be1ee503f87d040c84c0a7cacb245b4182445e3eee47ed6e073eca47, cbb89aac5a2c93a02305846f9353b013e6703813d4b6baff8eb89ee938647af3, c98dc0b930ea67992921d9f0848713deaa5bba8b4ba21effd0b00595dd9ed28c, ac227dd5c97a36f54e4fa02df4e4c0339b513e4f8049616e2a815a108e34552f, 6ab5a0b7080e783bba9b3ec53889e82ca4f2d304e67bd139aa267c22c281a368,

TYPE	VALUE
SHA256	e2ba2d3d2c1f0b5143d1cd291f6a09abe1c53e570800d8ae43622426c1c4343c, d8cde28cf2a5884daddf6e3bc26c80f66bc3737e426b4ba747d49d154999fbc1, 81fc4a5b1d22efba961baa695aa53201397505e2a6024743ed58da7bf0b4a97f, 3b2a6c7a39f49e790286185f2d078e17844df1349b713f278ecef1defb4d6b04, 7bddde9708118f709b063da526640a4132718d3d638505aafce5a20d404b2761, 883e035f893483b9921d054b3fa014cef90d90b10dcba7d342def8be2e98ce3c, 4b0a48d698240504c4ff6275dc735c8162e57f92224fb1d2d6393890b82a4206, 4018b462f2fcf1b0452ecd88ab64ddc5647d1857481f50fa915070f5f1858115, 3d80ea70b0c00d12f2ba2c7b1541f7d0f80005a38a173e6962b24f01d4a2a1de
Domains	theconomics[.]net, inclusive-economy[.]com, healthcaption[.]com
IPv4	191.101.78[.]189
File Paths	C:\Users\Win\Desktop\Reno\NewTor\27-07-2023\tornado\tornado\Payloads\BAR_33\I.A\out\IA.pdb, C:\Users\User\Desktop\tornado\Payloads\WKS_10\I.A\out\stagerx64.pdb, C:\Users\Win\Desktop\Reno\NewTor\27-07-2023\tornado\tornado\Payloads\BAR_38\I.A\out\IA.pdb, C:\Users\Win\Desktop\Reno\NewTor\NewIA-Tornado-WithStealer\Payloads\KIL_03\I.A\out\stagerx64.pdb, K:\prj\WIP\C# - Payload\Client-Side\https\client-Divided\KALV\obj\Release\KALV.pdb

References

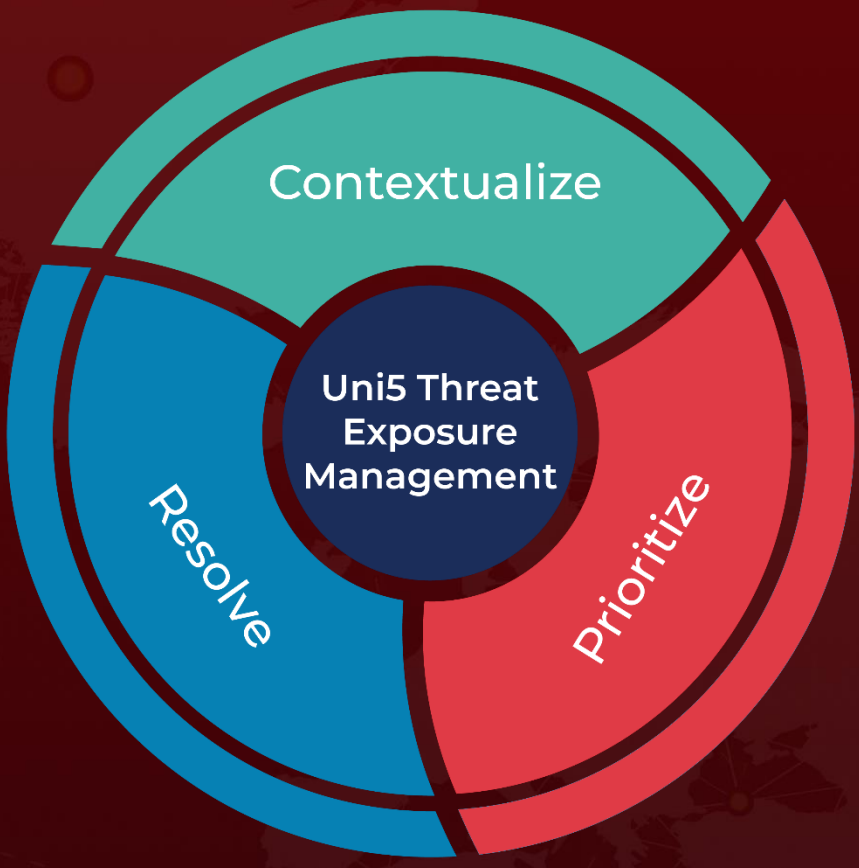
https://www.proofpoint.com/us/blog/threat-insight/ta402-uses-complex-ironwind-infection-chains-target-middle-east-based-government

https://www.hivepro.com/threat-advisory/hamas-israel-conflict-goes-digital/

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 15, 2023 . 4:30 AM

More at www.hivepro.com