Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

MuddyWater Returns with a New Spear-Phishing Campaign

Date of Publication	Admiralty Code	TA Number
November 03, 2023	A1	TA2023445

Summary

First appeared: 2017
Attack Region: Israel
Actor: MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm)
Attack: MuddyWater, the Iranian nation-state actor, has been identified in a new spearphishing campaign targeting two Israeli entities and deploying a legitimate remote administration tool known as N-able Advanced Monitoring Agent. This agent helps in remote administration and management of workstations and servers. What's particularly noteworthy is that MuddyWater is using a new C2 framework, MuddyC2Go, and N-able remote monitoring system indicating a new technique or tools being employed in their cyber operations.

Attack Regions

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

Attack Details

#1 A recent campaign carried out by the MuddyWater cyber-espionage group has been identified, with two Israeli targets being the focus of their attack. MuddyWater is known for its activities in the realm of cyber-espionage, particularly against entities in the Middle East and other regions. The group's tactics often involve spear-phishing and the deployment of various malware and tools for reconnaissance and data exfiltration.

#2 **MuddyWater** has been conducting spear-phishing campaigns since 2020, typically using emails that contain direct links or attachments such as PDF, RTF, and HTML files. These attachments often include links to archives hosted on different file-sharing platforms. What sets this recent campaign apart is the use of a N-able's remote monitoring software and a new file-sharing service called Storyblok as part of a multi-stage infection vector.

#3 On October 30th, two archives hosted on Storyblok were identified, which are part of a new multi-stage infection vector. The attack is believed to initiate with a spear-phishing email that encourages the victim to download an archive hosted at storyblok[.]com. This archive executes a multi-step process, ultimately resulting in the deployment of the Advanced Monitoring Agent. The infection vector comprises hidden files, an LNK file designed to trigger the infection, and an executable file that reveals a decoy document while executing the Advanced Monitoring Agent.

#4 Once the victim has been infected, the MuddyWater operator will connect to the compromised host using the deployed N-able agent and begin conducting reconnaissance on the target. After the reconnaissance phase, the MuddyWater is likely to execute PowerShell code on the infected host which will make the compromised system communicate with a custom C2 server controlled by the attacker. MuddyWater has previously used the PhonyC2 framework for their C2 infrastructure. However, it has been observed that they are now using a new C2 framework called MuddyC2Go. This indicates a shift in their tactics and tools for their cyber operations.

Recommendations

Remain vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Email Security Measures: Employ robust email security solutions to detect and block malicious attachments and links. Consider using advanced threat protection (ATP) and email filtering technologies to sandbox suspicious or untrusted URLs.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing	T1566.002 Spearphishing Link
T1547 Boot or Logon Autostart Execution	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1105 Ingress Tool Transfer
T1204 User Execution	T1204.002 Malicious File		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	37c3f5b3c814e2c014abc1210e8e69a2, 16923d827a440161217fb66a04e8b40a, 7568062ad4b22963f3930205d1a14df7, 39eea24572c14910b67242a16e24b768, 2e09e53135376258a03b7d793706b70f, 1f0b9aed4b2c8d958a9b396852a62c9d, 065f0871b6025b8e61f35a188bca1d5c, 146cc3a1a68be349e70b79f9115c496b, Dd247ccd7cc3a13e1c72bb01cf3a816d, 8d2199fa11c6a8d95c1c2b4add70373a, 04afff1465a223a806774104b652a4f0,

TYPE	VALUE
MD5	6167f03c8b2734c20eb02d406d3ba651, E8f3ecc0456fcbbb029b1c27dc1faad0, 952cc4e278051e349e870aa80babc755, 34212eb9e2af84eceb6a8234d28751b6, 3c6486dfb691fc6642f1d35bdf247b90, 55b99af81610eb65aabea796130a0462, d7ca8f3b5e21ed56abf32ac7cb158a7e, d3a2dee3bb8fcd8e8a0d404e7d1e6efb, 4a70b1e4cb57c99502d89cdbbed48343, f08aa714fd59b68924843cbfddac4b15, db0e68d7d81f5c21e6e458445fd6e34b, dbcc0e9c1c6c1fff790caa0b2ffc2fe5, e07adc4ee768126dc7c7339f4cb00120, feede05ba166a3c8668fe580a3399d8f, 9894b84916f9264d897fe3b4a83bc608, 9957250940377b39e405114f0a2fe84b, 245c3ed373727c21ad9ee862b767e362, 22971759adf816c6fb43104c0e1d89d6, 5e0cc23a6406930a40696594021edb5f, 79a638b2f2cc82bfe137f1d12534cda5, fc523904ca6e191eb2fdb254a6225577, b867ec1cef6b1618a21853fb8cafd6e1, 57641ce5af4482038c9ea27afcc087ee
URL	ws.onehub[.]com/files/7f9dxtt6, a.storyblok[.]com/f/253959/x/b92ea48421/form.zip, a.storyblok[.]com/f/255988/x/5e0186f61d/questionnaire.zip, a.storyblok[.]com/f/259791/x/94f59e378f/questionnaire.zip, a.storyblok[.]com/f/259837/x/21e6a04837/defense-video.zip, a.storyblok[.]com/f/259791/x/91e2f5fa2f/attachments.zip
IP	146.70.149[.]61, 146.70.124[.]102, 37.120.237[.]204, 37.120.237[.]248, 91.121.61[.]76, 109.201.140[.]103, 162.223.89[.]11, 164.132.237[.]65, 141.95.177[.]130, 91.121.240[.]108, 137.74.131[.]18, 137.74.131[.]20, 45.150.64[.]239, 95.164.46[.]35, 45.67.230[.]91,

TYPE	VALUE
IP	94.131.109[.]65, 185.248.144[.]158, 94.131.98[.]14, 45.150.64[.]23, 45.150.64[.]39, 95.164.38[.]99
SHA1	69f68529e07f2463eb105cfc87df04539e969a56, 81c06183b1bb146f5f1a5f1d03ac44fa9d68d341

References

https://www.deepinstinct.com/blog/muddywater-en-able-spear-phishing-with-new-ttps

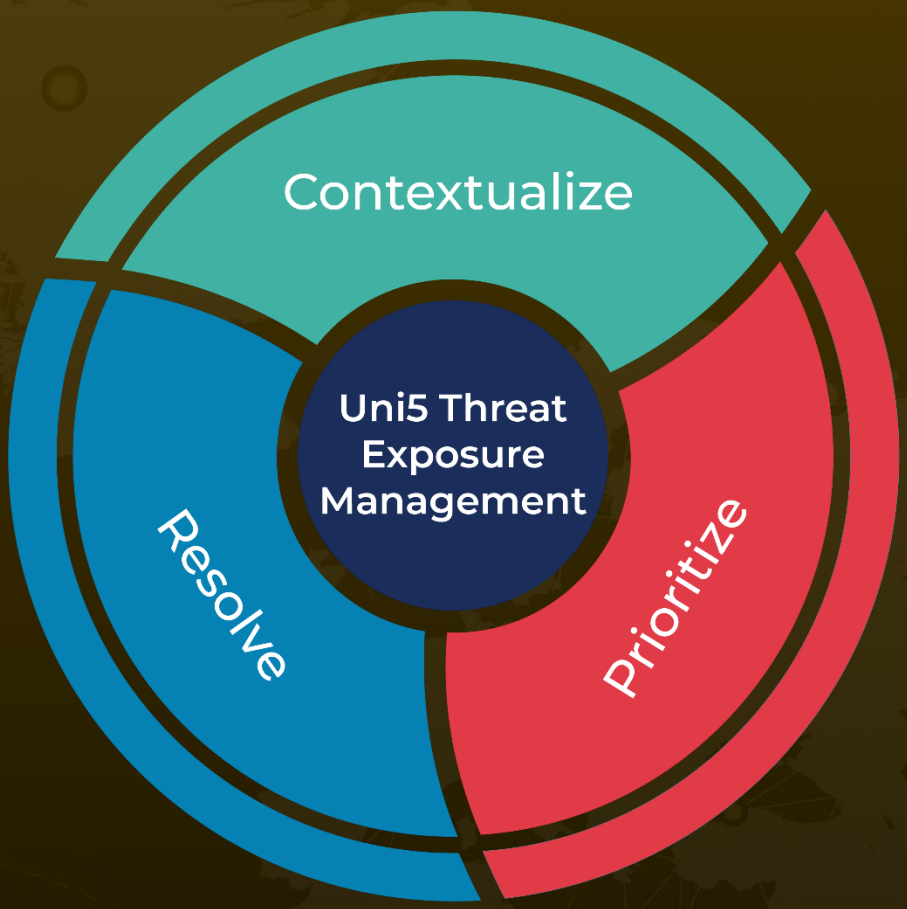
https://twitter.com/GroupIB_TI/status/1719675754886131959

https://www.hivepro.com/muddywater-is-back-with-new-techniques/

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 03, 2023 • 5:10 AM

© 2023 All Rights are Reserved by Hive Pro®

More at www.hivepro.com