Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

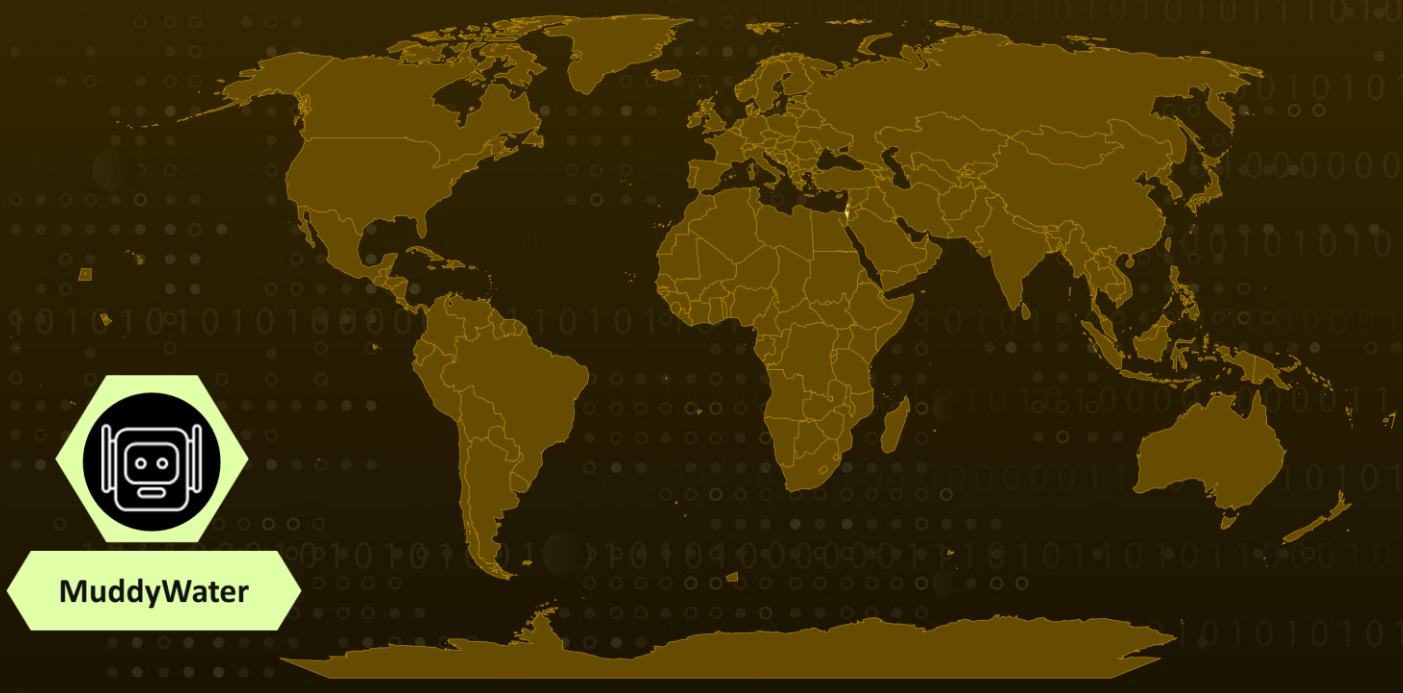
MuddyWater Enhances Its Arsenal with DarkBeatC2 Framework

Date of Publication	Admiralty Code	TA Number
April 15, 2024	A1	TA2024145

Summary

Attack Discovered: April 2024
Attack Region: Israel
Malware: DarkBeatC2
Actor: MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm, Boggy Serpens, Yellow Nix)
Attack: MuddyWater, the Iranian threat actor, has added a new C2 infrastructure named DarkBeatC2 to its arsenal. Despite occasionally switching to different remote administration tools or changing their C2 framework, MuddyWater's overall methods and tactics remain consistent.

Attack Regions



Attack Details

#1 MuddyWater, the Iranian threat actor, active since at least 2017, they have been active in orchestrating spear-phishing attacks, which result in the deployment of various legitimate Remote Monitoring and Management (RMM) solutions on compromised systems. Recently, MuddyWater has been associated with a new C2 infrastructure named DarkBeatC2, adding to its array of tools. Despite occasional changes in RATs or C2 frameworks, MuddyWater's overall methods and tactics remain consistent.

#2 MuddyWater deployed a phishing campaign, leveraging PDF attachments sent from an email account compromised within an Israeli company. These PDFs contained links to web hosting services where recipients could download archives containing RAT. Notably, one of the hosting providers, "Egnyte," was newly identified as being used by MuddyWater, indicating an expansion of their tactics. Additionally, a similar campaign utilizing a different subdomain which points to an Israeli higher education college.

#3 The use of compromised email accounts suggests MuddyWater exploited the trust recipients had in familiar and credible organizations to disseminate their malicious links. Furthermore, another archive hosted on Sync and OneHub, indicating a potential targeting of victims within the education sector.

#4 MuddyWater has been observed utilizing the DarkBeatC2 framework in conjunction with other tools, including IP addresses 185.236.234[.]161 and 185.216.13[.]242, which host the "reNgine" open-source reconnaissance framework. These domains are linked to "Stark-Industries," a known hosting provider associated with malicious activities. MuddyWater has a track record of utilizing various open-source tools, with reconnaissance playing a vital role in their operations.

#5 The DarkBeatC2 framework acts as a central hub for managing infected computers, with threat actors typically establishing connections through manual execution of PowerShell code, wrapping a connector, or sideloading a malicious DLL. This demonstrates MuddyWater's adaptability and sophistication in orchestrating cyberattacks, utilizing a combination of open-source tools and custom frameworks to achieve their objectives.

#6 Once a connection is established with an infected host, it enables the reception of PowerShell responses that retrieve two additional scripts from the same server. The first script extracts the contents of a file and transmits them to the C2 server using HTTP POST. Meanwhile, the second script conducts regular checks on the server for supplementary payloads and records the execution outcomes in "SysInt.log." Although the nature of the subsequent payload remains undisclosed, PowerShell continues to be the primary tool within MuddyWater's C2 frameworks.

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.

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.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0011 Command and Control	T1566 Phishing	T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1036 Masquerading	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading
T1071 Application Layer Protocol			

Indicators of Compromise (IOCs)

TYPE	VALUE
IP	185.236.234[.]161, 185.216.13[.]242, 45.66.249[.]226, 137.74.131[.]19, 164.132.237[.]68, 95.164.61[.]64, 95.164.46[.]54, 91.225.218[.]210, 95.164.38[.]68, 45.140.147[.]81, 80.71.157[.]130, 103.35.190[.]203, 95.164.46[.]253
MD5	353b4643ec51ecff7206175d930b0713, 3dd1f91f89dc70e90f7bc001ed50c9e7, Bede9522ff7d2bf7daff04392659b8a8, 32bfe46efceae5813b75b40852fde3c2, b7d15723d7ef47497c6efb270065ed84

References

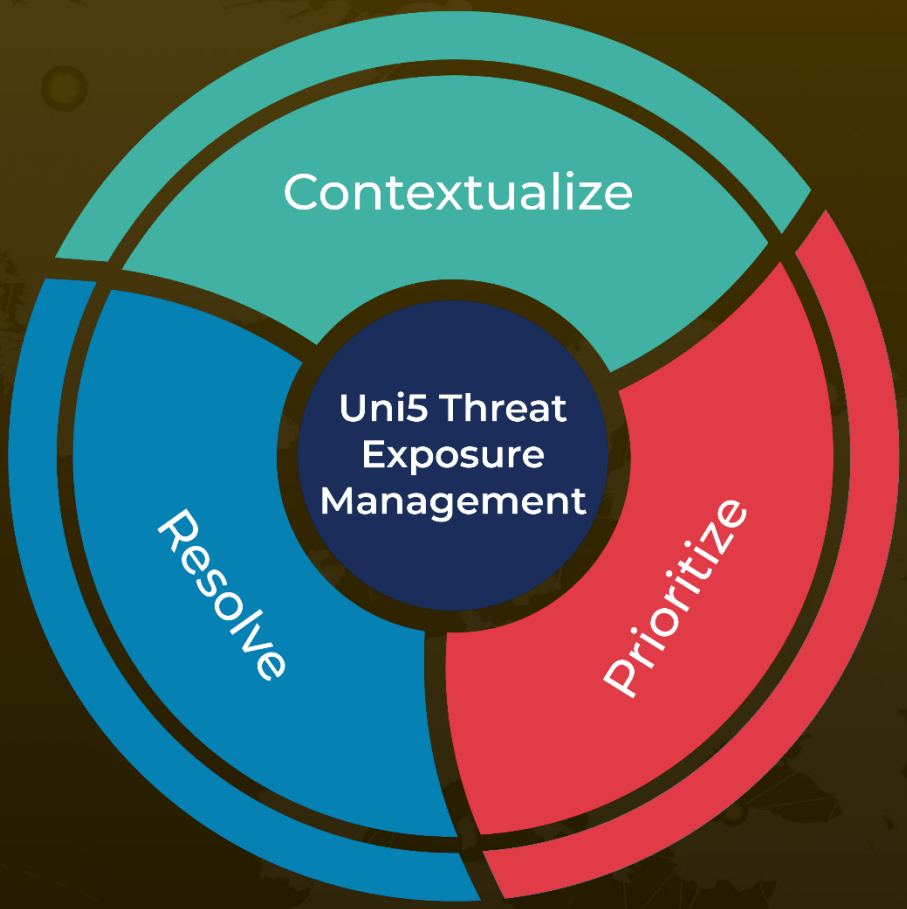
https://www.deepinstinct.com/blog/darkbeatc2-the-latest-muddywater-attack-framework

https://www.hivepro.com/threat-advisory/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

April 15, 2024 • 6:00 AM

More at www.hivepro.com