Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

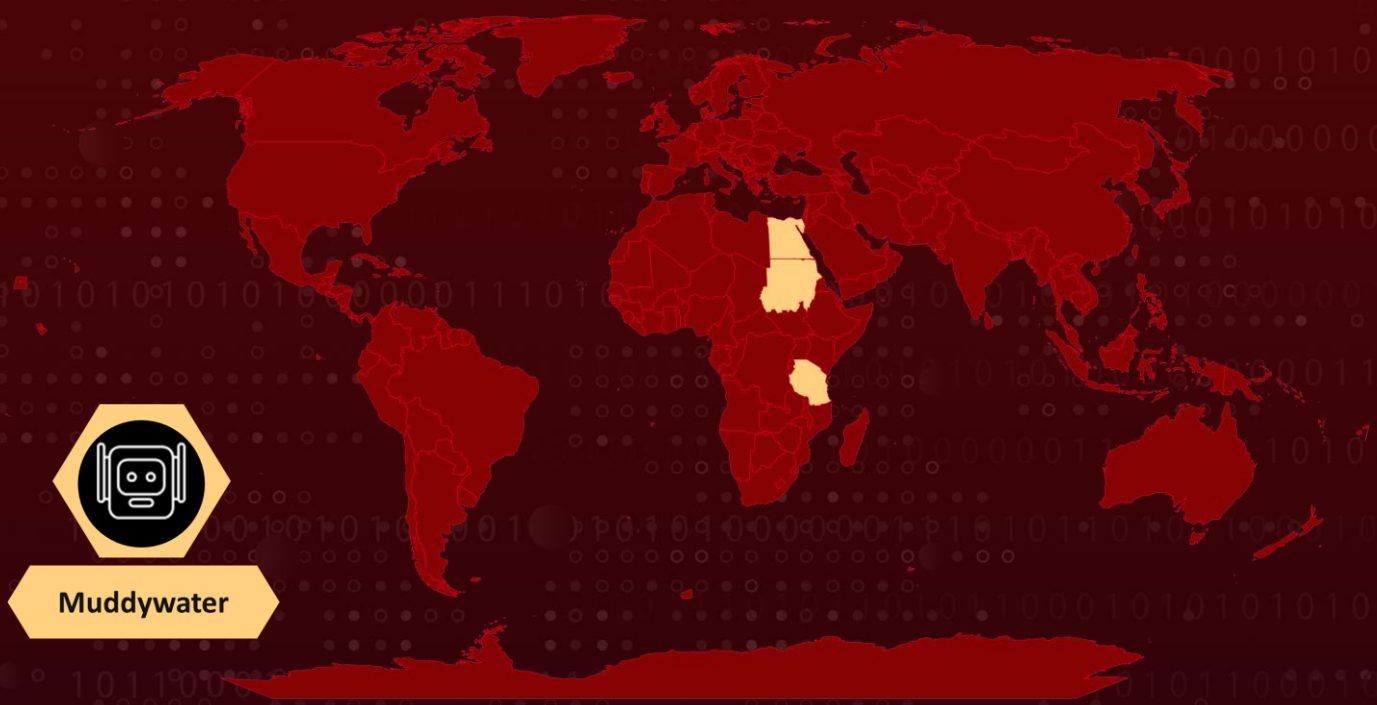
Muddywater Utilizes Custom Tools to Target Telecom Companies

Date of Publication	Admiralty Code	TA Number
December 22, 2023	A1	TA2023517

Summary

Attack Began: November 2023
Affected Industries: Telecommunications organization
Attack Region: Egypt, Sudan, and Tanzania
Actor: MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm)
Malware: MuddyC2Go, Venom Proxy, SimpleHelp
Attack: Iranian espionage group Muddywater, targeted telecommunications companies in Egypt, Sudan, and Tanzania in November 2023. The attackers employed a diverse set of tools for this activity, including leveraging the MuddyC2Go infrastructure. Additionally, they utilized the SimpleHelp remote access tool and Venom Proxy. The attackers also deployed a custom keylogging tool along with other publicly available and living-off-the-land tools as part of their espionage efforts.

Attack Regions



Attack Details

#1 In November 2023, the Iranian cyberespionage group MuddyWater shifted its focus towards telecommunications companies in Egypt, Sudan, and Tanzania. The attack involved various tools, including the MuddyC2Go infrastructure, a custom keylogging tool, the SimpleHelp remote access tool, and the Venom Proxy, all associated with MuddyWater's previous activities.

#2 MuddyWater, active since 2017, has a history of targeting organizations globally, with a particular emphasis on entities in the Middle East. In this recent campaign, the group specifically targeted a telecommunications company, with early signs of malicious activity including the execution of PowerShell commands linked to the MuddyC2Go backdoor.

#3 The MuddyC2Go malware was sideloaded through jabswitch.exe, a legitimate executable from Java Platform SE 8. PowerShell code was then executed to establish a connection with the C&C server, employing techniques to evade security software detection. The attackers initiated the malware using a scheduled task, utilizing commands associated with the Impacket WMIExec hacktool. Additionally, the SimpleHelp remote access tool was deployed.

#4 During the intrusion, the attackers utilized Windows Management Instrumentation (WMI) to execute the SimpleHelp installer within the victim network. Although not conclusively linked to MuddyWater, a group previously targeted another telecommunications and media company, where SimpleHelp was repeatedly used to connect to known MuddyWater infrastructure.

#5 The attackers also executed a custom build of the Venom Proxy hacktool and utilized a newly developed custom keylogger. In another targeted organization, Venom Proxy, AnyDesk, and suspicious Windows Scripting Files (WSF) were used. This consistent pattern of attack activities indicates the involvement of the same threat actor group across multiple incidents.

#6 In a recent **spearphishing campaign**, MuddyWater was identified targeting two Israeli entities. The attackers deployed a legitimate remote administration tool called N-able. This indicates a continuation of MuddyWater's sophisticated tactics, employing both social engineering through spearphishing and the use of legitimate tools to compromise their targets.

Recommendations

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.

Application whitelisting: This security practice that allows only approved applications to run on a system or network, while blocking all others. Create and maintain a comprehensive inventory of all authorized software within your organization. Regularly review and update the list to ensure it reflects the current software requirements.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0009 Collection	TA0011 Command and Control	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1047 Windows Management Instrumentation	T1189 Drive-by Compromise	T1105 Ingress Tool Transfer	T1056 Input Capture
T1566 Phishing	T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1027 Obfuscated Files or Information
T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1a0827082d4b517b643c86ee678eaa53f85f1b33ad409a23c50164c3909fdaca, 25b985ce5d7bf15015553e30927691e7673a68ad071693bf6d0284b069ca6d6a, eac8e7989c676b9a894ef366357f1cf8e285abde083fbdf92b3619f707ce292f, 3916ba913e4d9a46cfce437b18735bbb5cc119cc97970946a1ac4eab6ab39230
IP	146.70.124[.]102, 94.131.109[.]65, 95.164.38[.]99, 45.67.230[.]91, 95.164.46[.]199, 94.131.98[.]14, 94.131.3[.]160

References

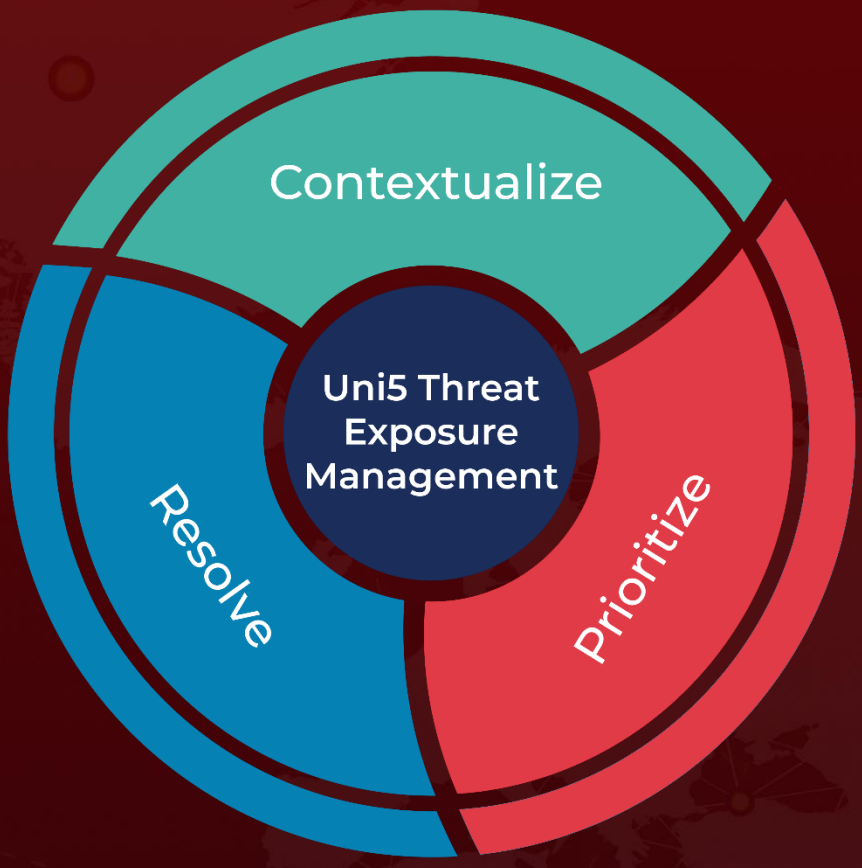
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/iran-apt-seedworm-africa-telecoms

https://www.hivepro.com/threat-advisory/muddywater-returns-new-spear-phishing-campaign/

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

December 22, 2023 . 3:50 AM

More at www.hivepro.com