Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

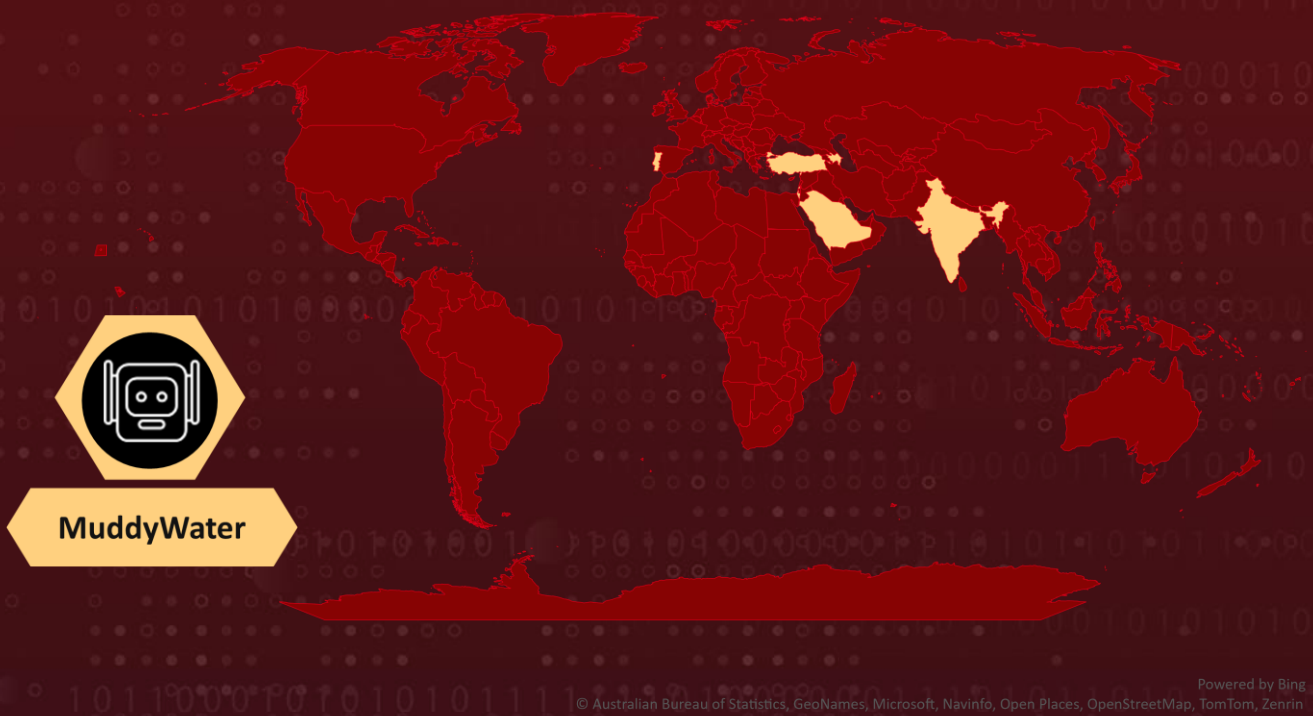
MuddyWater Expands Its Arsenal with BugSleep Malware

Date of Publication	Admiralty Code	TA Number
July 16, 2024	A1	TA2024273

Summary

Attack Discovered: October 2023
Attack Region: Saudi Arabia, Turkey, Azerbaijan, India and Portugal
Affected Industries: Israeli Municipalities, Airlines, Travel Agencies, Journalists, Education, Logistics, Healthcare
Malware: BugSleep Backdoor
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, an Iranian threat group, has substantially escalated its operations in Israel since the onset of the Israel-Hamas conflict in October 2023. The group employs phishing campaigns to target various organizations. Recently, MuddyWater campaigns have led to the deployment of a new, undocumented backdoor known as BugSleep, which executes commands from the threat actors and facilitates the transfer of files between compromised machines and C&C servers. This backdoor is continuously undergoing development and enhancement.

Attack Regions



Attack Details

#1 MuddyWater, an Iranian threat group active since 2017, has intensified its phishing campaigns in the Middle East, notably targeting Israel with increased activity since October 2023. They exploit compromised email accounts to infiltrate various organizations, often deploying legitimate Remote Management Tools (RMM) such as Atera Agent or Screen Connect. Recently, they introduced a custom backdoor known as BugSleep.

#2 The group sends large volumes of emails across diverse sectors, focusing on specific industries like Israeli municipalities, airlines, travel agencies, and journalists. Since February 2024, they have launched over 50 spear-phishing campaigns targeting more than 10 sectors. These campaigns typically feature tailored lures sent to multiple targets within the same industry.

#3 In recent operations, MuddyWater has shifted towards using more generic-themed lures, such as webinars and online courses. While targeting Saudi Arabia and Israel identical lures were sent to the targets, differing primarily in email addresses and final payloads. Saudi targets received RMM payloads, while Israeli targets were exposed to the BugSleep backdoor.

#4 BugSleep, a novel malware introduced in MuddyWater's phishing campaigns since May 2024, has evolved through multiple versions, showcasing continuous refinements in its operations. It evades sandbox detection by invoking the Sleep API, decrypts configurations to extract C&C addresses, and schedules tasks for regular execution.

#5 The latest variant from MuddyWater has successfully circumvented detection and response (EDR) solutions by leveraging flags like MicrosoftSignedOnly and ProhibitDynamicCode. These flags restrict processes to load only Microsoft-signed images, preventing unauthorized DLL injections by other processes. Enabling ProcessDynamicCodePolicy enhances protection against EDR solutions analyzing program behavior through userland API hooks.

#6 BugSleep supports 11 different commands. Its core functionality includes sending file content to its C&C server, writing content into files, and running commands through a command pipe. MuddyWater's evolving tactics, integrating the BugSleep backdoor into its operations, have transitioned from highly customized lures to broader themes aimed at a larger victim pool. This shift, combined with an increased use of the English language for communications, indicates the group's expansion into large-scale operations.

Recommendations

Exercise Caution with Unsolicited Emails: Always exercise caution when receiving unexpected or urgent emails, especially those from unknown sources. Avoid downloading attachments from unsolicited emails to mitigate the risk of malware infections.

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
TA0007 Discovery	TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing
T1566.002 Spearphishing Link	T1036 Masquerading	T1053 Scheduled Task/Job	T1204 User Execution
T1082 System Information Discovery	T1105 Ingress Tool Transfer	T1027 Obfuscated Files or Information	T1059 Command and Scripting Interpreter
T1133 External Remote Services	T1574 Hijack Execution Flow	T1497 Virtualization/Sandbox Evasion	T1070 Indicator Removal
T1033 System Owner/User Discovery	T1132 Data Encoding	T1132.002 Non-Standard Encoding	T1041 Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	kinneretacil.egnyte[.]com, salary.egnyte[.]com, gcare.egnyte[.]com, rimonnet.egnyte[.]com, alltrans.egnyte[.]com, megolan.egnyte[.]com, bgu.egnyte[.]com, fbcsoft.egnyte[.]com, cnsmportal.egnyte[.]com, alkan.egnyte[.]com, getter.egnyte[.]com, ksa1.egnyte[.]com, filecloud.egnyte[.]com, nour.egnyte[.]com, airpazfly.egnyte[.]com, cairoairport.egnyte[.]com, silbermintz1.egnyte[.]com, smartcloudcompany[.]com, onlinemailerservices[.]com, smtpcloudapp[.]com, softwarehosts[.]com, airpaz.egnyte[.]com, airpazflys.egnyte[.]com, fileuploadcloud.egnyte[.]com, downloadfile.egnyte[.]com
URLs	hxxps[:]//shorturl[.]at/NCxJk, hxxps[:]//shorturl[.]at/bYqUx, hxxps[:]//ws.onehub[.]com/files/bbmiio1c, hxxps[:]//ws.onehub[.]com/files/zgov9aqy
IPv4	146[.]19[.]143[.]14, 91[.]235[.]234[.]202, 85[.]239[.]61[.]97, 95[.]164[.]32[.]69, 5[.]252[.]23[.]52, 194[.]4[.]50[.]133, 193[.]109[.]120[.]59, 89[.]221[.]225[.]81, 45[.]150[.]108[.]198, 200[.]200[.]200[.]248,

TYPE	VALUE
IPv4	169[.]150[.]227[.]230, 169[.]150[.]227[.]205, 185[.]248[.]85[.]20, 141[.]98[.]252[.]143, 31[.]171[.]154[.]54, 146[.]70[.]172[.]227, 198[.]54[.]131[.]36
SHA256	73c677dd3b264e7eb80e26e78ac9df1dba30915b5ce3b1bc1c83db52b9c6b30e, 960d4c9e79e751be6cad470e4f8e1d3a2b11f76f47597df8619ae41c96ba5809, b8703744744555ad841f922995cef5dbca11da22565195d05529f5f9095fbfca, 94278fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7130c472, 5df724c220aed7b4878a2a557502a5cefee736406e25ca48ca11a70608f3a1c0, 39da7cc7c627ea4c46f75bcec79e5669236e6b43657dcad099e1b9214527670e, c23f17b92b13464a570f737a86c0960d5106868aaa5eac2f2bac573c3314eb0f, fb58c54a6d0ed24e85b213f0c487f8df05e421d7b07bd2bece3a925a855be93a, 7e6b04e17ae273700cef4dc08349af949dbd4d3418159d607529ae31285e18f7, ff2ae62ba88e7068fa142bbe67d7b9398e8ae737a43cf36ace1fcf809776c909, e2810cca5d4b74e0fe04591743e67da483a053a8b06f3ef4a41bdabee9c48cf7, 90f94d98386c179a1b98a1f082b0c7487b22403d8d5eb3db6828725d14392ded, 20aaeac4dbea89b50d011e9becdf51afc1a1a1f254a5f494b80c108fd3c7f61a, 55af6a90ac8863f27b3fcaa416a0f1e4ff02fb42aa46a7274c6b76aa000aacc2, f925d929602c9bae0a879bb54b08f5f387d908d4766506c880c5d29986320cf9, 424a9c85f97aa1aece9480bd658266c366a60ff1d62c31b87ddc15a1913c10e4, c80c8dd7be3ccf18e327355b880afb5a24d5a0596939458fb13319e05c4d43e9, c88453178f5f6aaab0cab2e126b0db27b25a5cfe6905914cc430f6f100b7675c, 31591fcf677a2da2834d2cc99a00ab500918b53900318f6b19ea708eba2b38ab,

TYPE	VALUE
SHA256	a0968e820bbc5e099efd55143028b1997fd728d923c19af03a1ccec34ce73d9b, 88788208316a6cf4025dbabbef703f51d77d475dc735bf826b8d4a13bbd6a3ee, 4064e4bb9a4254948047858301f2b75e276a878321b0cc02710e1738b42548ca, e7896ccb82ae35e1ee5949b187839faab0b51221d510b25882bbe711e57c16d2, 1c0947258ddb608c879333c941f0738a7f279bc14630f2c8877b82b8046acf91, 8fbd374d4659efdc5b5a57ff4168236aeaab6dae4af6b92d99ac28e05f04e5c1, 7e14ca8cb7980e85aff4038f489442eace33530fd02e2b9c382a4b6907601bee, 02060a9ea0d0709e478e2fba6e9b71c1b7315356acc4f64e40802185c4f42f1c, 53b4a4359757e7f4e83929fba459677e76340cbec7e2e1588bbf70a4df7b0e97, 0ab2b0a2c46d14593fe900e7c9ce5370c9cfbf6927c8adb5812c797a25b7f955

References

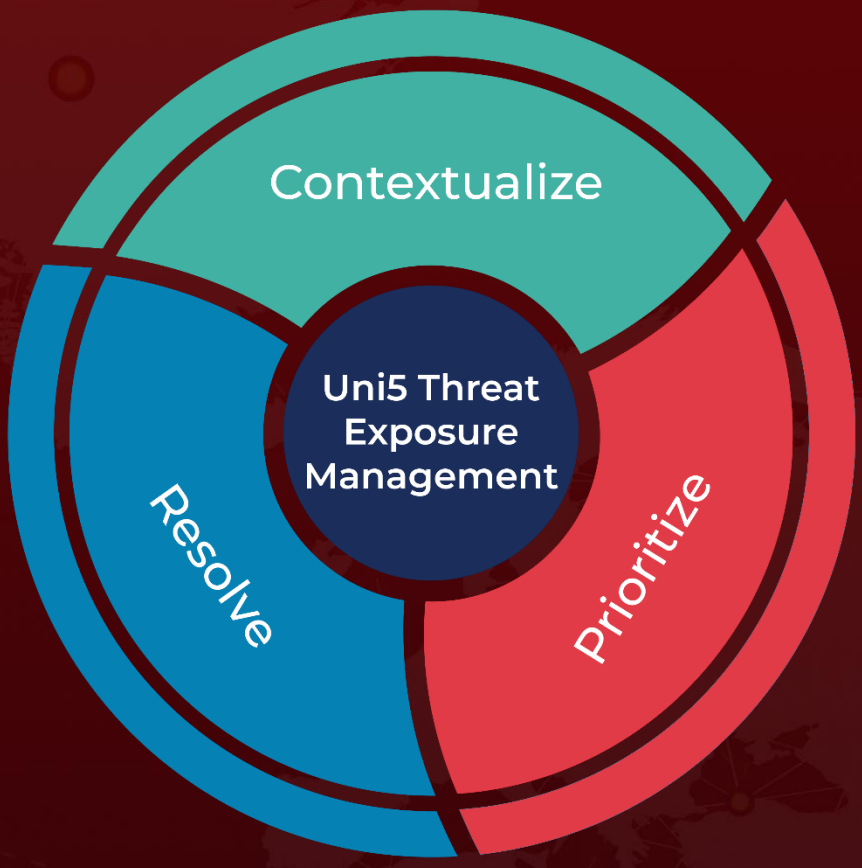
https://research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/

https://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

July 16, 2024 • 6:45 AM

More at www.hivepro.com