ultraviolet

THREAT REPORT:

# ‘MuddyWater’ adds ‘BugSleep’ backdoor to toolkit

**Services Performed By:**
UltraViolet Cyber
Johnathon Moyer
(443) 351-7630
info@uvcyber.com

**Published Date:**
July 15, 2024

# Contents



# 1 Executive Summary

MuddyWater, the Iranian cyber espionage group associated with Iran's Ministry of Intelligence (MOIS) has leaked part of their new backdoor tool, dubbed 'BugSleep'. This advanced persistent group (APT) is known for exploiting compromised enterprise environments to send phishing emails to compromise other environments. The group has been more active after the October 2023 conflict between Israel and Hamas. While MuddyWater is still developing this new backdoor tool, researchers have already documented command and control tactics within the currently available sample.

# 2 Technical Analysis

MuddyWater, also known as 'Earth Vetala', 'MERCURY', and 'Static Kitten', is believed to have started operations as far back as 2017. The group primarily targets Israel, with other notable activity within the Middle East, Asia, North America, Europe and Africa. Much of their work focuses on cyberespionage, with their targets aligning with government and private organizations of interest to the state of Iran.

Check Point researchers recently shared a change in attack pattern associated with MuddyWater (MW). Previously, MW would send a spear phishing email to targets within a specific industry to prompt the recipient to download the Atera remote management tool from an Egnyte-hosted page. MW now added a variation where the spear phishing email contains a PDF with an embedded link to download the BugSleep backdoor.

Once downloaded, the backdoor sleeps for a period. This is a common tactic to avoid detection within researcher sandboxes. The payload then extracts the encrypted configuration file and calls out every 30 minutes to the command and control (C2) server for further instructions. The communications to the C2 server are also encrypted, further increasing the difficulty of detection from security tools.

A variant of the custom loader injected encrypted shellcode into the running memory of Edge, Chrome, Opera, AnyDesk, OneDrive and Powershell to further avoid detection. MuddyWater has used Telegram APIs to establish encrypted C2 communications in the past, with their 'Small Sieve' Python backdoor back in late 2021. Other encrypted channels may be added to BugSleep in future iterations.

# 3 What UltraViolet Cyber is Doing

- We regularly update our Indicators of Compromise (IoC) databases
- Network monitoring tools to alert on traffic to known malicious sites
- Monitoring for commands associated with malicious activity from threat actors

# 4 What Customers Can Do

- Ensure your endpoint security tools are up to date with the latest malware signatures
- Train users to double-check meeting invites from organizations they are unfamiliar with
- End users should not download unsolicited applications from untrusted email domains or senders
- If possible, whitelist the remote management tools authorized within your organization and block unapproved tools from running

# 5 References


Gatlan, S. (2024, July 15). New BugSleep malware implant deployed in MuddyWater attacks. BleepingComputer. Retrieved from https://www.bleepingcomputer.com/news/security/new-bugsleep-malware-implant-deployed-in-muddywater-attacks/

(2024, July 15). New BugSleep Backdoor Deployed in Recent MuddyWater Campaigns. Check Point Research. Retrieved from https://research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/

(2024, July 15) MuddyWater. MITRE | ATT&CK. Retrieved from https://attack.mitre.org/groups/G0069/

(2022, January 27). Small Sieve. National Cyber Security Centre. Retrieved from https://www.ncsc.gov.uk/files/NCSC-Malware-Analysis-Report-Small-Sieve.pdf

(2024, July 15). Manage approved apps for Windows devices with App Control for Business policy and Managed Installers for Microsoft Intune. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-app-control-policy