Apr 01 2024

NETMANAGEIT

Intelligence Report

New Campaigns After Operation Swords of Iron

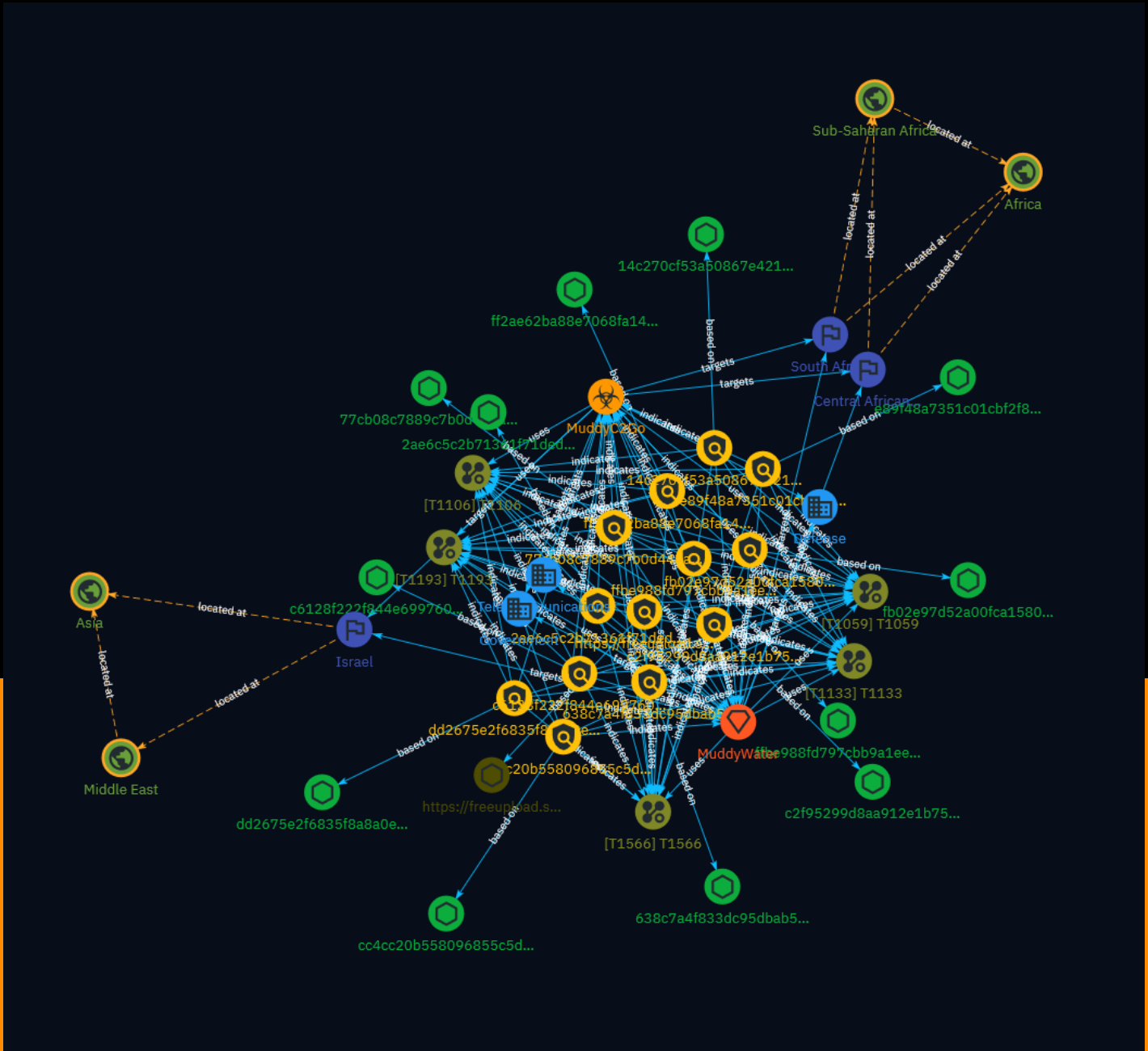

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The MuddyWater APT group has recently launched new attacks in Israel, Africa, and Turkiye using products developed in-house and taking over third-party tools. Phishing attacks use PDF attachments with agents from services like Atera and ConnectWise. Once installed, actors gain privileges to monitor and execute files. MuddyWater is expanding tactics to reduce digital footprint, likely increasing spear-phishing via compromised accounts. Technical analysis shows tailored attack files named for targets. Compromised business accounts used to build agents, increasing victim persuasion. Remote access tools ensure persistence and capabilities like command execution and file operations. MuddyWater aligns attacks with Iran's interests, adding techniques and using legitimate tools for anonymity.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name

https://freeupload.store/rALE7/wIHItUcE08.msi/download

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '10 months ago', 'timestamp': 1685979389, 'iso': '2023-06-05T11:36:29-04:00'} - **IPQS: Domain:** freeupload.store - **IPQS: IP Address:** 51.255.19.181

Pattern Type

stix

Pattern

[url:value = 'https://freeupload.store/rALE7/wIHItUcE08.msi/download']

Name

ff2ae62ba88e7068fa142bbe67d7b9398e8ae737a43cf36ace1fcf809776c909

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ff2ae62ba88e7068fa142bbe67d7b9398e8ae737a43cf36ace1fcf809776c909']

Name

ffbe988fd797cbb9a1eedb705cf00ebc8277cdbd9a21b6efb40a8bc22c7a43f0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ffbe988fd797cbb9a1eedb705cf00ebc8277cdbd9a21b6efb40a8bc22c7a43f0']

Name

fb02e97d52a00fca1580ca71ed152dd28dd5ae28ab0a9c8e7b32cebd7f1998a1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fb02e97d52a00fca1580ca71ed152dd28dd5ae28ab0a9c8e7b32cebd7f1998a1']

Name

dd2675e2f6835f8a8a0e65e9dbc763ca9229b55af7d212da38b949051ae296a5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dd2675e2f6835f8a8a0e65e9dbc763ca9229b55af7d212da38b949051ae296a5']

Name

c2f95299d8aa912e1b753f3f0780a00ea6e8b5dab0245d77fcf3b6499677c328

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c2f95299d8aa912e1b753f3f0780a00ea6e8b5dab0245d77fcf3b6499677c328']

Name

c6128f222f844e699760e32695d405bd5931635ec38ae50eddc17a0976ccefb4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c6128f222f844e699760e32695d405bd5931635ec38ae50eddc17a0976ccefb4']

Name
77cb08c7889c7b0d443aeacfdcbc1cc6745d3e3441f4b42ddbf7fde6113491ae
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '77cb08c7889c7b0d443aeacfdcbc1cc6745d3e3441f4b42ddbf7fde6113491ae']
Name
638c7a4f833dc95dbab5f0a81ef03b7d83704e30b5cdc630702475cc9fff86a2
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '638c7a4f833dc95dbab5f0a81ef03b7d83704e30b5cdc630702475cc9fff86a2']
Name
2ae6c5c2b71361f71ded4ad90bbf6ef0b0f4778caf54078c928e2017302fbe69
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '2ae6c5c2b71361f71ded4ad90bbf6ef0b0f4778caf54078c928e2017302fbe69']

Name

14c270cf53a50867e42120250abca863675d37abf39d60689e58288a9e870144

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '14c270cf53a50867e42120250abca863675d37abf39d60689e58288a9e870144']

Name

e89f48a7351c01cbf2f8e31c65a67f76a5ead689bb11e9d4918090a165d4425f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e89f48a7351c01cbf2f8e31c65a67f76a5ead689bb11e9d4918090a165d4425f']

Name

cc4cc20b558096855c5d492f7a79b160a809355798be2b824525c98964450492

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cc4cc20b558096855c5d492f7a79b160a809355798be2b824525c98964450492']

Malware

Name
MuddyC2Go

Attack-Pattern

Name
T1193
ID
T1193
Name
T1059
ID
T1059
Description
Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries

may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

T1566

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

T1106

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. (Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations.(Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may use assembly to directly or in-directly invoke syscalls in an attempt to subvert defensive sensors and detection signatures such as user mode API-hooks.(Citation: Redops Syscalls) Adversaries may also attempt to tamper with sensors and defensive tools associated with API monitoring, such as unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001).

Name

T1133

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management] (https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Intrusion-Set

Name

MuddyWater

Description

[MuddyWater](https://attack.mitre.org/groups/G0069) is a cyber espionage group assessed to be a subordinate element within Iran's Ministry of Intelligence and Security (MOIS). (Citation: CYBERCOM Iranian Intel Cyber January 2022) Since at least 2017, [MuddyWater] (https://attack.mitre.org/groups/G0069) has targeted a range of government and private organizations across sectors, including telecommunications, local government, defense, and oil and natural gas organizations, in the Middle East, Asia, Africa, Europe, and North America.(Citation: Unit 42 MuddyWater Nov 2017)(Citation: Symantec MuddyWater Dec 2018) (Citation: ClearSky MuddyWater Nov 2018)(Citation: ClearSky MuddyWater June 2019) (Citation: Reaqta MuddyWater November 2017)(Citation: DHS CISA AA22-055A MuddyWater February 2022)(Citation: Talos MuddyWater Jan 2022)

Country

Name
Israel
Name
South Africa
Name
Central African Republic

Region

Name
Middle East
Name
Asia
Name
Sub-Saharan Africa
Name
Africa

Sector

Name
Telecommunications
Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.
Name
Government
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.
Name
Defense
Description
Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations.

StixFile

Value
ffbe988fd797cbb9a1eedb705cf00ebc8277cdbd9a21b6efb40a8bc22c7a43f0
ff2ae62ba88e7068fa142bbe67d7b9398e8ae737a43cf36ace1fcf809776c909
fb02e97d52a00fca1580ca71ed152dd28dd5ae28ab0a9c8e7b32cebd7f1998a1
dd2675e2f6835f8a8a0e65e9dbc763ca9229b55af7d212da38b949051ae296a5
c6128f222f844e699760e32695d405bd5931635ec38ae50eddc17a0976ccefb4
c2f95299d8aa912e1b753f3f0780a00ea6e8b5dab0245d77fcf3b6499677c328
77cb08c7889c7b0d443aeacfdcbc1cc6745d3e3441f4b42ddbf7fde6113491ae
2ae6c5c2b71361f71ded4ad90bbf6ef0b0f4778caf54078c928e2017302fbe69
638c7a4f833dc95dbab5f0a81ef03b7d83704e30b5cdc630702475cc9fff86a2
14c270cf53a50867e42120250abca863675d37abf39d60689e58288a9e870144
e89f48a7351c01cbf2f8e31c65a67f76a5ead689bb11e9d4918090a165d4425f
cc4cc20b558096855c5d492f7a79b160a809355798be2b824525c98964450492

Url

Value
https://freeupload.store/rALE7/wIHItUcE08.msi/download

External References

- https://www.malwation.com/blog/new-muddywater-campaigns-after-operation-swords-of-iron
- https://otx.alienvault.com/pulse/660a7dd1dcc267d78c7733e7