Contents

[**G0069 Muddy Water** 2](#_Toc179356267)

[**I. Introduction** 2](#_Toc179356268)

[**II. Tactics** 2](#_Toc179356269)

[**III. Techniques** 2](#_Toc179356270)

[**IV. Procedures** 3](#_Toc179356271)

[**V. Summary** 5](#_Toc179356272)

[**References** 6](#_Toc179356273)

## **G0069 Muddy Water**

## **I. Introduction**

Muddy Water, also known as TEMP.Zagros, Seedworm, and Static Kitten, is an Iranian state-sponsored advanced persistent threat group that has been active since at least 2017. The group primarily focuses on cyber espionage operations whereby they target government entities, telecommunications, and oil and gas sectors in the Middle East, with occasional attacks into targets in Europe and North America.

## **II. Tactics**

Muddy Water's tactical approach is described by

1. ***Targeted Espionage***

The group focuses on collecting sensitive information related to geopolitical interests and critical infrastructure.

1. ***Social Engineering***

Heavy reliance on social engineering techniques, particularly through spear-phishing campaigns.

1. ***Living off the Land***

Extensive use of legitimate tools and scripts to blend in with normal system operations.

1. ***Continuous Evolution***

Regular updates to their toolset and techniques to evade detection and improve efficacy.

1. ***Persistence***

Emphasis on maintaining long-term access to compromised networks for ongoing intelligence gathering.

## **III. Techniques**

Muddy Water employs a range of techniques in their operations

|  |  |
| --- | --- |
| Spear-phishing Campaigns (T1566) | Use of carefully crafted emails with malicious macro-enabled documents (T1566.001).  Leveraging of geopolitical themes and impersonation of legitimate organizations. |
| PowerShell and VBA Macros | Extensive use of PowerShell scripts for payload execution and data exfiltration (T1059.001).  Employment of VBA macros in Office documents for initial compromise (T1204.002). |
| Custom Malware Deployment | Use of custom backdoors such as POWERSTATS and SHARPSTATS.  Deployment of open-source tools modified for their specific needs. |
| Command and Control (C2) Infrastructure | Use of compromised websites for C2 communication (T1102.002).  Leveraging of cloud services like GitHub and Pastebin for payload hosting and data exfiltration (T1102.002). |
| Lateral Movement | Use of compromised websites for C2 communication (T1102.002).  Leveraging of cloud services like GitHub and Pastebin for payload hosting and data exfiltration (T1102.002). |
| Defense Evasion | Obfuscation of PowerShell scripts and payloads (T1027).  Use of legitimate services and tools to blend malicious activities with normal operations (T1036). |

## **IV. Procedures**

Muddy Water's typical attack chain follows this sequence

***1. Initial Access***

a. Spear-phishing emails are sent to targeted individuals, often containing macro-enabled Office documents.

b. The lures typically relate to geopolitical themes or impersonate trusted organizations.

***2. Execution***

a. When the malicious document is opened and macros are enabled, it typically executes a PowerShell script.

b. This script downloads and executes the main payload, often a variant of POWERSTATS backdoor.

***3. Persistence and Privilege Escalation***

a. The malware establishes persistence through various methods, including scheduled tasks and registry modifications.

b. Privilege escalation is attempted using both custom and publicly available tools.

***4. Discovery and Lateral Movement***

a. Network reconnaissance is conducted to identify valuable systems and data.

b. Lateral movement is achieved using stolen credentials and by exploiting network vulnerabilities.

***5. Collection and Exfiltration***

a. Sensitive documents and data are identified and collected.

b. Data is often exfiltrated using legitimate cloud services or through custom C2 channels.

***6. Operational Maintenance***

a. Muddy Water regularly updates their tools and infrastructure to evade detection.

b. They maintain long-term access for continuous intelligence gathering.

## **V. Summary**

An analysis of Muddy Water’s operations provides a fascinating snapshot into what Iran is up to with regards to cyber espionage. Its target and interests in the Middle Eastern region are nearly identical to those of Iran’s geopolitical goals, especially with regards to its government and energy infrastructure targets.

One can highlight that, for example, Muddy Water’s tactics include numerous instances of using what is called ‘living off the land.’ They use real system administration tools, and scripting languages such as PowerShell, and thus integrate their actions with normal operations within the system, tweaking it in a manner that can be extremely onerous to identify. As for this approach it also helps to avoid security measures while minimizing the effectiveness of Custom Malware. Furthermore, the technical sophistication of the tools and techniques employed by the group also include exploiting open source tools and frequently changing them further solidifies the groups advantage in terms of timely modification of their toolsets without having to spend time in developing new and different ones, while also making it harder to track and identify them.

That Muddy Water main target the telecommunication companies suggest that this actor intend to gather intelligence that may be useful to them in future activities, or keep tab on certain persons of interest. Their spear-phishing campaigns show geopolitics knowledge, and the attackers commonly use low geographic environments’ political structures to formulate precise, unique, and plausible messages to include in the lure messages. As the situation in the Middle East changes, Muddy Water operates as Iran’s ‘digital thermometer,’ allowing for analysis of the country’s operational priorities and key concerns throughout the region.

## **References**

1. Kaspersky Lab. (2018). "MuddyWater expands operations." <https://securelist.com/muddywater/88059/>

2. Symantec Threat Hunter Team. (2019). "Seedworm: Group Compromises Government Agencies, Oil & Gas, NGOs, Telecoms, and IT Firms." <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/seedworm-espionage-group>

3. ClearSky Cyber Security. (2018). "Muddy Water Activities in the Middle East." <https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanon-and-Oman.pdf>

4. MITRE ATT&CK. (2024). "Muddy Water, G0069." <https://attack.mitre.org/groups/G0069/>