

## Unmasking MuddyWater's New Malware Toolkit Driving International Espionage



### Introduction

Group-IB [Threat Intelligence](#) uncovered a sophisticated phishing campaign orchestrated by the Advanced Persistent Threat (APT) MuddyWater, targeting international organizations worldwide to gather foreign intelligence.

MuddyWater accessed the compromised mailbox through NordVPN(a legitimate service abused by the threat actor), and used it to send phishing emails that appeared to be authentic correspondence. By exploiting the trust and authority associated with such communications, the campaign significantly increased its chances of deceiving recipients into opening the malicious attachments.

The phishing emails contain Microsoft Word documents that prompted recipients (victims) to enable macros in order to view the content. As soon as macros were activated, the Microsoft Word documents executed malicious Visual Basic for Application (VBA) code, ultimately leading to the deployment of version 4 of the Phoenix backdoor on the victim's system.

Group-IB attributes this campaign to the Iran-linked threat actor MuddyWater with high confidence, based on the tools, techniques, and procedures (TTPs) observed. The incident underscores how state-backed Threat Actors continue to exploit trusted channels of communication to evade defenses and infiltrate high-value targets.

### Key Takeaways

- Muddywater is targeting international organizations in an espionage campaign.
- The use of version 4 of the Phoenix backdoor malware in this campaign, featuring a different persistence technique.

- A new Remote Monitoring and Management (RMM) tool and custom browser credential stealer were potentially used in this campaign.

## Attribution Assessment

Group-IB attributes this campaign to MuddyWater with high confidence based on the following indicators observed during the course of our investigation and analysis:

- The dropped malware families, **Fakeupdate injector** and **Phoenix Backdoor**, are custom malware previously observed exclusively in Muddywater operations.
- The malicious macro embedded in the document shares similar logic and matches code with macros used in past MuddyWater campaigns (hash: 40dead1e1d83107698ff96bce9ea52236803b15b63fb0002e0b55af71a9b5e05).
- The command-and-control (C2) server hosts a custom browser credential stealer that employs the same string decoding techniques observed in other MuddyWater-linked malware.
- The same C2 infrastructure also contains PDQ RMM tools, which have been previously used by MuddyWater for remote access and persistence.
- The targeting patterns align with MuddyWater's historical victimology, specifically its focus on the Middle East region.

## Group-IB Threat Intelligence Portal: MuddyWater

Group-IB customers can access our [Threat Intelligence portal](#) for more information about MuddyWater and [Phoenix](#) malware profiles.



# MuddyWater

## Aliases

TEMP.Zagros, Seedworm  
Static Kitten, TA450, Boggy  
Serpens, Earth Vetala

## First seen

2017

## Latest activity

Present

## LANGUAGES

English Persian  
Arabic Hebrew

## GEOGRAPHY

Middle East Turkey  
Azerbaijan Pakistan  
United States  
United Kingdom

## TOP INDUSTRIES TARGETED

Telecommunications  
Government Education  
Energy Aviation  
Information Technology

## MOTIVATION(S)

Espionage  
Intelligence Gathering  
Tactical Disruption

## Skillset

Linux Apache Windows Nginx  
Python Golang AWS PowerShell  
RMM SpearPhishing

## Toolset

StealthCache Phoenix BugSleep  
FakeUpdate LiteInject Fooder  
CannonRat Blackout UDPgangster  
Chromium\_Stealer SilentShell PowerGUI  
Atera PDQ Action1 ScreenConnect  
Level RMM HackBrowserData Yamux  
go-socks5

## Threat Actor Write-up

MuddyWater, also known by aliases TA450 and Seedworm, is a sophisticated threat actor group operating since at least 2017. It is believed to be state-sponsored by the Iranian Ministry of Intelligence and Security (MOIS). The group's primary motivation is espionage and intelligence gathering. MuddyWater targets a variety of industries including government, telecommunications, energy, and critical infrastructure, focusing its efforts in the Middle East, South Asia, and NATO-affiliated countries.

## Modus operandi

MuddyWater primarily relies on phishing to gain initial access to systems belonging to organizations and persons of interest, and maintain long term stealthy access while conducting espionage and information gathering for further operation expansion, serving the interests of the Iranian government. They have also conducted destructive operations during times of conflict as a tactical move against Iranian geopolitical adversaries.



# Phoenix

Type  
Backdoor

Platform  
Windows

First seen  
17 April 2025

Last Discovered  
N/A

## ABOUT

The Phoenix malware is used by MuddyWater to deploy what Group-IB assesses to be a new, minimalistic variant of the BugSleep backdoor by self-injecting the backdoor into its own process. It decrypts an embedded PE file, maps it into its process memory, and transfers execution to its entry point.

We have found two version of the backdoor in the wild and both are used by muddywater, versions are determined from the PDB paths:

### Phoenix Version 3:

- The backdoor begins by copying itself to a new location using PowerShell commands ( powershell.exe -Command "Copy-Item -Path %%malware path%% -Destination 'C:\ProgramData\Logs' -Force").
- then generates a machine GUID by concatenating the username and computer name—similar to the technique used by BugSleep backdoor.
- Next, it registers with the C2 server via the /register endpoint.
- After registration, it enters a C2 communication loop where it periodically sends an /alive beacon to the C2 and retrieves commands from the /request endpoint.

### Phoenix Version 4:

This version has the following behavior:

- Attempts to create a mutex named "sysprocupdate.exe."
- Gather system information, including computer name, domain/workgroup, Windows version, and username.
- Copies itself to C:\ProgramData\sysprocupdate.exe.
- Establishes persistence by modifying the registry key HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon under the Shell value.

Connects to its C2 server via WinHTTP to receive and execute commands.

## FEATURES

- Launch interactive shell
- Persist on the disk
- Upload files to C2
- Download files from C2
- Receive commands from C2

## FORMATS

EXE

## THREAT ACTORS

MuddyWater

## TOP TACTICS

- T1598.002 - Phishing for Information -> Spearphishing Attachment
- T1059.001 - Command and Scripting Interpreter -> PowerShell
- T1059.003 - Command and Scripting Interpreter -> Windows Command Shell
- T1547.001 - Boot or Logon Autostart Execution -> Registry Run Keys / Startup Folder
- T1547.004 - Boot or Logon Autostart Execution -> Winlogon Helper DLL
- T1546.015 - Event Triggered Execution->Component Object Model Hijacking
- T1055.002 - Process Injection -> Portable Executable Injection
- T1055 - Process Injection
- T1140 - Deobfuscate/Decode Files or Information
- T1027.007 - Obfuscated Files or Information -> Dynamic API Resolution
- T1027.009 - Obfuscated Files or Information -> Embedded Payloads
- T1112 - Modify Registry
- T1027.002 - Obfuscated Files or Information -> Software Packing
- T1105 - Ingress Tool Transfer
- T1071.001 - Application Layer Protocol -> Web Protocols

## From Malicious Email to System Compromise

MuddyWater launched the operation by sending malicious email using a compromised account. Based on the email header, MuddyWater accessed the compromised account through NordVPN, and used it to send phishing emails to multiple targets worldwide.

The phishing emails contained a malicious Microsoft Word attachment. When opened, the document displayed blurred content and instructed the recipient to “enable content” to view the text. Once macros were enabled, the embedded VBA code executed functioning as a dropper that decoded and wrote a loader to disk before executing it.

The loader was identified as **FakeUpdate**, which is an injector-style loader that decrypts an embedded second-stage payload using Advanced Encryption Standard (AES) and injects it into its own process. The decrypted second-stage payload was identified as **Phoenix backdoor version 4**. Written to disk under the name sysProcUpdate, Phoenix v4 registered the infected host with the attacker’s command-and-control (C2) infrastructure, initiating continuous beaconing, and polling for commands, and in doing so enabling remote control, data collection, and further post-exploitation activities.

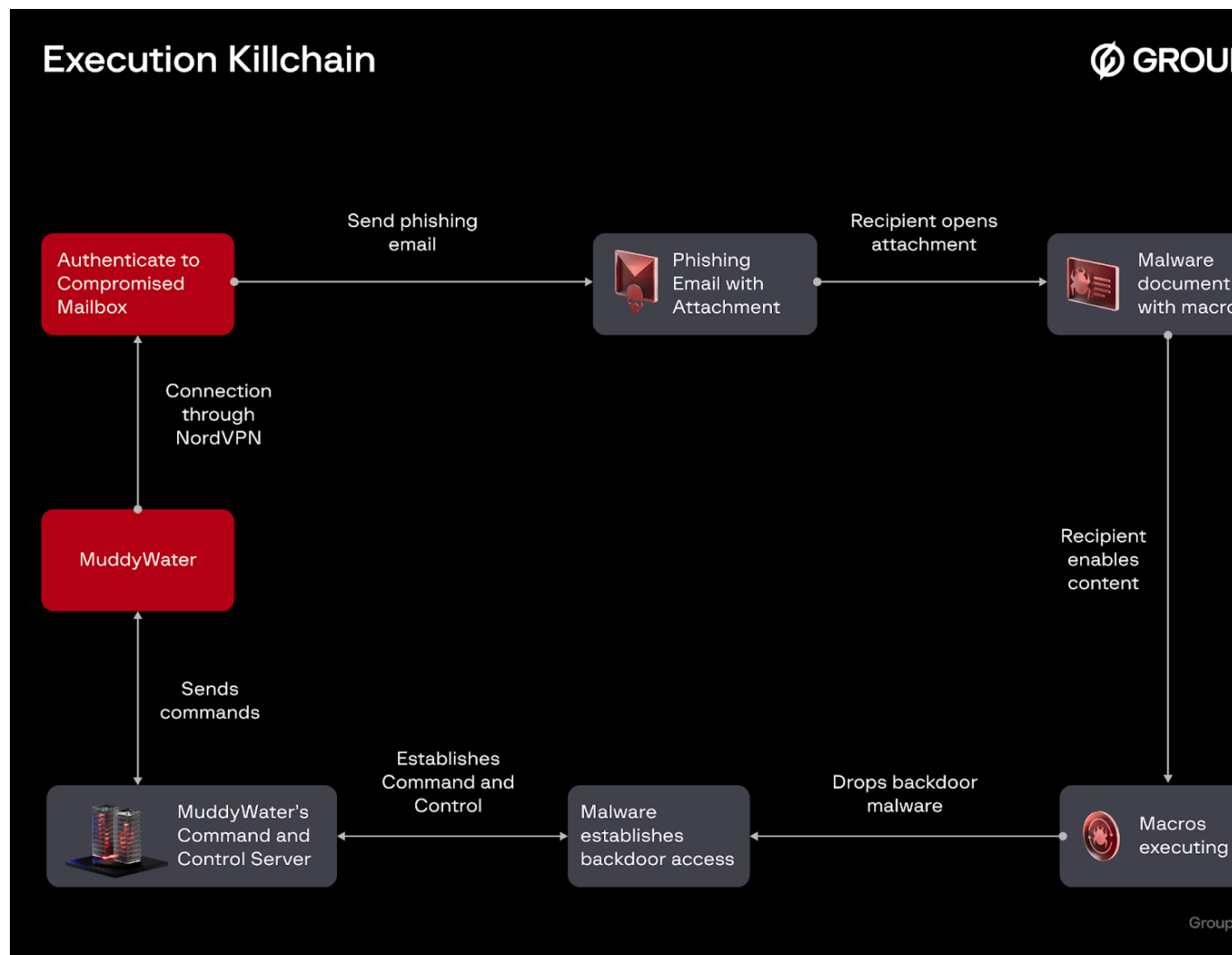


Figure 1. An overview of the execution killchain.

## Targeting Analysis and Campaign Insights

An examination of the recipients from the phishing emails observed by Group-IB reveals several key insights :

### Notable targeting patterns

- **Inclusion of Personal Email Accounts:** The mix of official (.gov) and personal emails (Yahoo, Gmail, and Hotmail) indicates that MuddyWater possesses detailed knowledge of its targets.
- **Targeting of International Organizations:** The campaign’s focus extended to influential global organizations engaged in international cooperation and humanitarian missions, highlighting the actor’s broader geopolitical

motivations.

## Target Types Classification

The diagram below provides a breakdown of the different target categories identified in this espionage campaign, based on Group-IB's analysis of the phishing email recipients.

Several targeted recipients are part of well-known global institutions that focus on international cooperation and humanitarian work. This supports the group's larger geopolitical goals and the purposeful nature of its targeting.

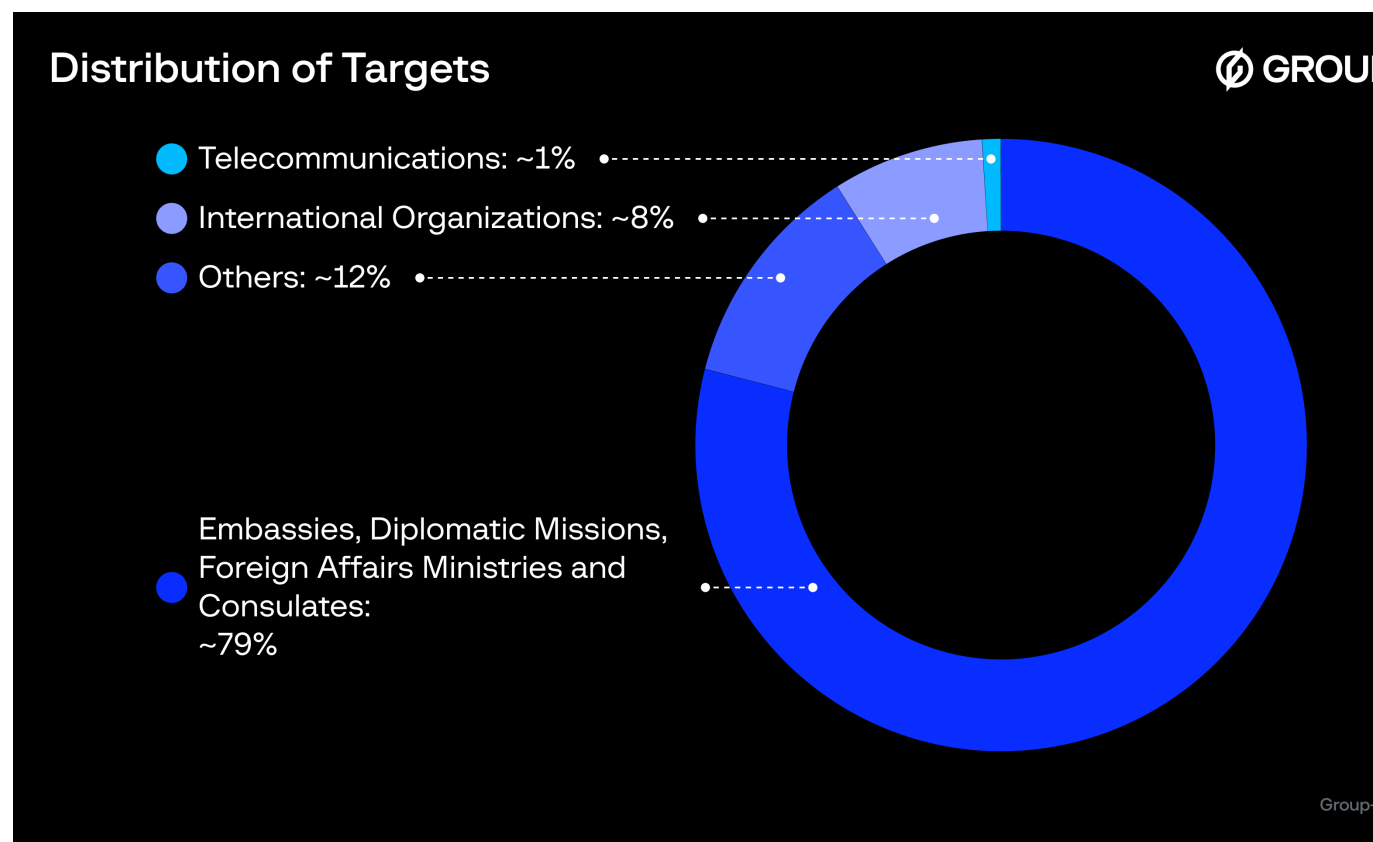


Figure 2. A diagram highlighting the types of targets observed during this MuddyWater campaign.

## Samples Connections and Campaign Overlaps

During extended analysis of artifacts associated with this campaign, Group-IB Threat Intelligence identified additional malicious documents that share technical and infrastructure overlaps with the current operation. These findings suggest continued activity by MuddyWater, potentially involving related or concurrent campaigns.

We identified another malicious document that impersonates a government-organization seminar addressing ongoing geopolitical tensions in the region and mirrors themes seen elsewhere in this campaign. The file contains identical macro code, delivers the same payload, and communicates with the same command-and-control (C2) domain as other samples (screenai[.]online). Given these overlaps — including matching last-editor metadata and edit timestamps — we assess this document as part of the same espionage campaign. Although the exact distribution method remains unconfirmed, phishing via a compromised email account is the most likely vector.

Additionally, we identified another document which targeted the energy sector in the Middle East and North Africa. This file also deployed the FakeUpdate malware injector to deliver Phoenix backdoor version 4, communicating with the same C2 infrastructure (screenai[.]online) used in this Espionage Campaign. The attack was conducted in the same time frame as the campaign mentioned in this blog. However, due to differing target profiles, with this sample

focusing on energy-sector entities rather than diplomatic or international organizations, we assess it to be a separate but concurrent MuddyWater operation reusing the same C2 domain.

## Malware Analysis

### Malicious Mail attachment

When macros are enabled and executed, the malicious document macros retrieves an embedded dropped file and writes C:\Users\Public\Documents\ManagerProc.log ,then executes that file.

On Error GoTo AAAA

```
Dim pth As String
Dim malmal_path As String
```

```
pth = "C:\\Users\\Public\\Documents\\ManagerProc.log"
laylay
```

//Dropped file path

```
Dim app As String
app = dddd(UserForm1.TextBox1.Text)
laylay
```

```
.....
```

```
fileNumber = FreeFile
Open pth For Output As fileNumber
Print #fileNumber, app
Close fileNumber
```

```
RRRR (pth)
```

//starting the dropped file

```
laylay
```

```
AAAA:
```

```
' n
```

```
End Sub
```

Figure 3. A screenshot of the executed macro, as soon as the recipient enables it.

### Dropped Backdoor

The dropped file acts as an injector tracked by Group-IB as FakeUpdate. It decrypts an embedded second-stage payload and injects it into its own process. The injected component is a backdoor which is version 4 of the [Phoenix](#) backdoor used by MuddyWater, which performs the following actions:

- Attempts to create a mutex named sysprocupdate.exe
- Gather system information, including **computer name, domain/workgroup, Windows version, and username.**
- Copies itself to C:\ProgramData\sysprocupdate.exe
- Achieves persistence by modifying the registry key HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon and altering the Shell value.
- Connects to its C2 server via WinHTTP to receive and execute commands.

Command	Description
---------	-------------

## COM-Based Persistence and Overlapping Artifact

A similar DLL (coreglobconfig.dll) was previously observed in the [CannonRat](#) malware, which has also been linked to MuddyWater.



The Mononoke.exe backdoor and its associated DLL were delivered through a malicious document employing the same lure and theme seen in a [recent MuddyWater operation](#) documented by Group-IB Threat Intelligence. This overlap suggests that the developer likely neglected to remove this DLL artifact from the malware used in this campaign.



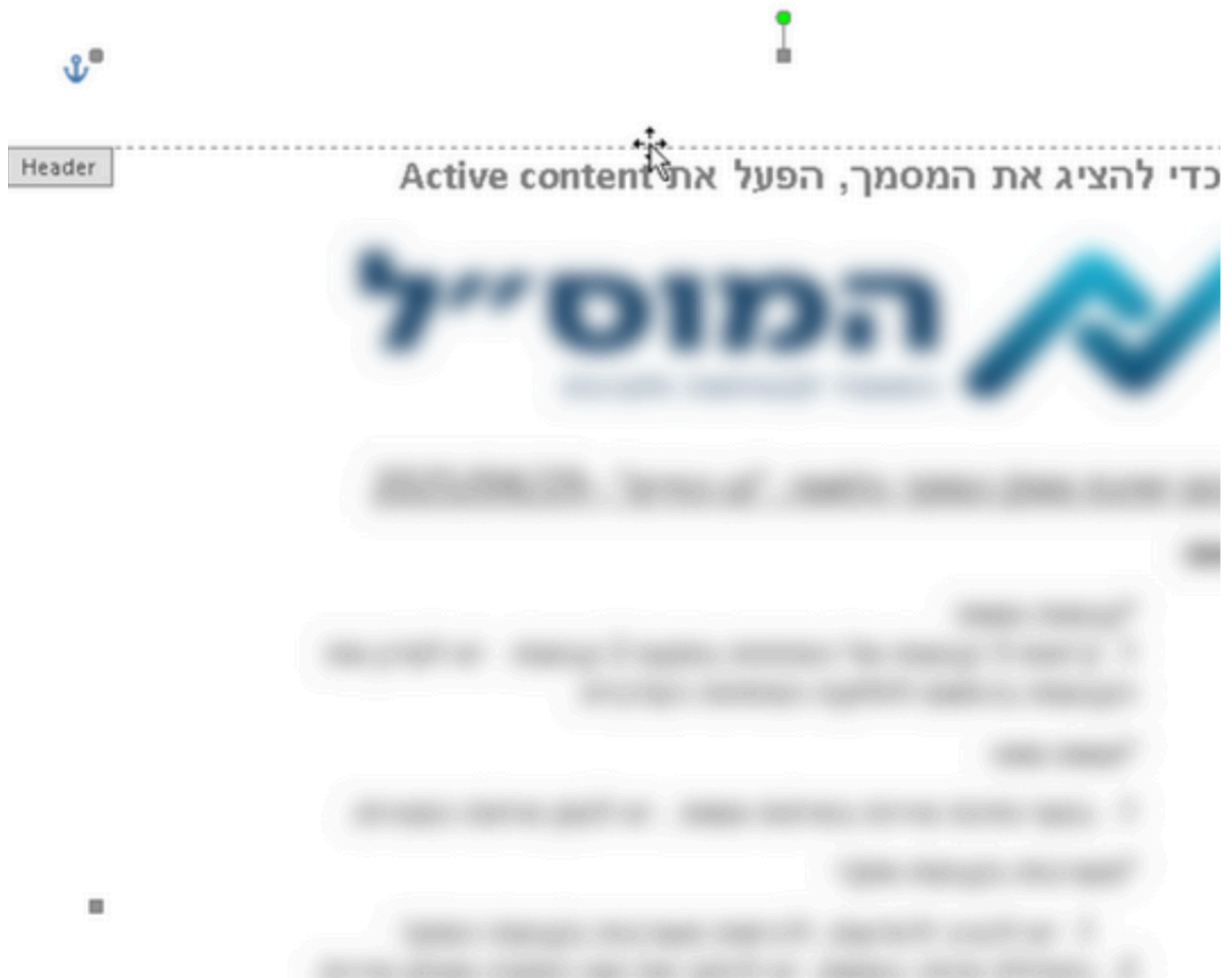


Figure 5. The document dropped the Mononoke.exe, which uses the same theme used in a recent attack.

## Infrastructure Analysis

The value of x-originating-ip in the email header is a NordVPN exit node located in France. The x-originating-ip header reveals the **original IP address of the client or device** that first submitted the email to the mail server. According to IPinfo this IP is located in France:

## IP Geolocation

City	Marseille
State	Provence-Alpes-Côte d'Azur
Country	 France
Postal	13000
Local time	01:13 AM, Wednesday, September 03, 2025
Timezone	Europe/Paris
Coordinates	43.2970,5.3811



### Location Evidence

We have confirmed the location of this IP address with active measurement data

```
$ ping 212.3[REDACTED]  
PING 212.3[REDACTED] (212.3[REDACTED]): 56 data byte  
64 bytes from 212.3[REDACTED]: icmp_seq=0 ttl=58 time=0.366 ms
```




Measurement taken from  IPinfo ProbeNet in Marseille, Provence-Alpes-Cote d'Azur, FR  
On August 25th 2025

Figure 6. NordVPN exit node IP information.

Based on this analysis, we can record the fact that MuddyWater uses NordVPN and possibly other similar VPN services in their operations.

The malware samples contained a hardcoded C2 domain `screenai[.]online` which remained active only for several days after the launch of the phishing campaign. Although available information on this domain is limited, Group-IB Threat Intelligence was able to establish several key details.

The domain `screenai[.]online` was registered via [NameCheap](#) on 17 August 2025 at 16:41:01 hours (UTC) (2025-08-17T16:41:01.00Z), with an expiration date of 17 August 2026 16:41:01 hours (2026-08-17T16:41:01.00Z). The DNS servers were set to CloudFlare as shown in the WHOIS records.

Tech Fax:

Tech Fax Ext:

Tech Email: `64ddb59ab57d4979a09561b48a1db89e.protect@withheldforprivacy.com`

Name Server: `michelle.ns.cloudflare.com`

Name Server: `vick.ns.cloudflare.com`

DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>

>>> Last update of WHOIS database: 2025-10-07T21:34:51.52Z <<<

For more information on Whois status codes, please visit <https://icann.org/epp>

Figure 7. C2 name servers in WHOIS info.

This can be confirmed by looking at the resolved IP addresses that belong to CloudFlare as shown in the image below:

Query	Answer	Answer ASN	First Seen	Last Seen
screenai.online	104.21.19.118	13335	2025-08-18 16:54:31	2025-08-19 01:52:59
screenai.online	172.67.186.35	13335	2025-08-18 16:54:31	2025-08-19 01:52:59
screenai.online	199.59.243.228	16509	2025-04-07 23:42:13	2025-06-19 14:04:36
screenai.online	13.248.169.48	16509	2024-08-30 19:09:37	2025-04-07 14:01:08
screenai.online	76.223.54.146	16509	2024-08-30 19:09:37	2025-04-07 14:01:08
screenai.online	9.44.163.50	16509	2024-04-08 09:03:30	2024-08-30 14:17:44

Figure 8. C2 passive DNS history.

At this stage, further analysis would not be possible unless we obtain the real IP address. However, we were able to uncover it through the Secure Sockets Layer (SSL) certificate, which showed that the real IP of the server was 159[.]198[.]36[.]115 which is registered under NameCheap's Autonomous System Number (ASN), this aligns with the domain registration information.

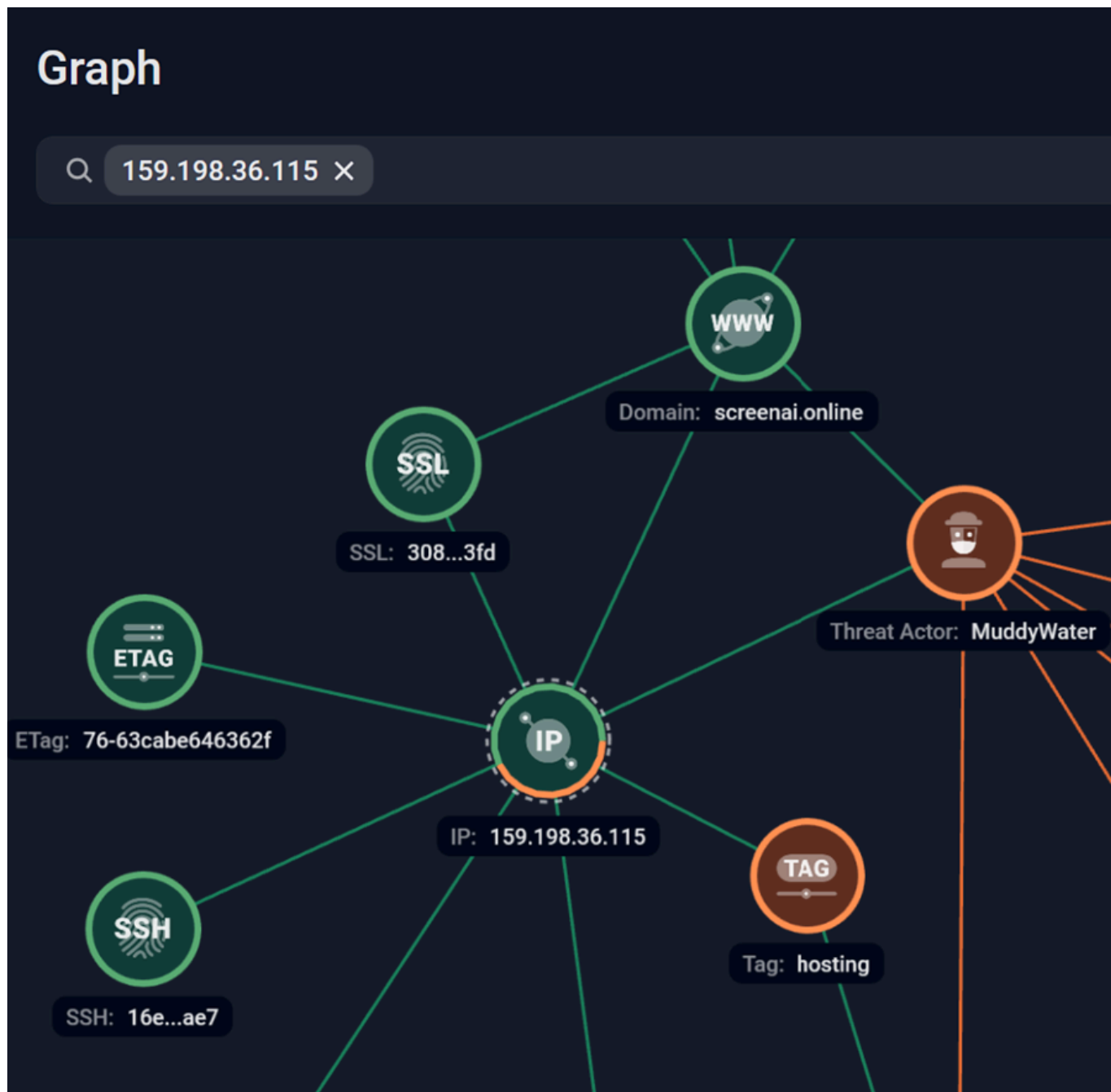


Figure 9. Analysis of the MuddyWater's C2 domain using Group-IB's [Graph](#) solution.

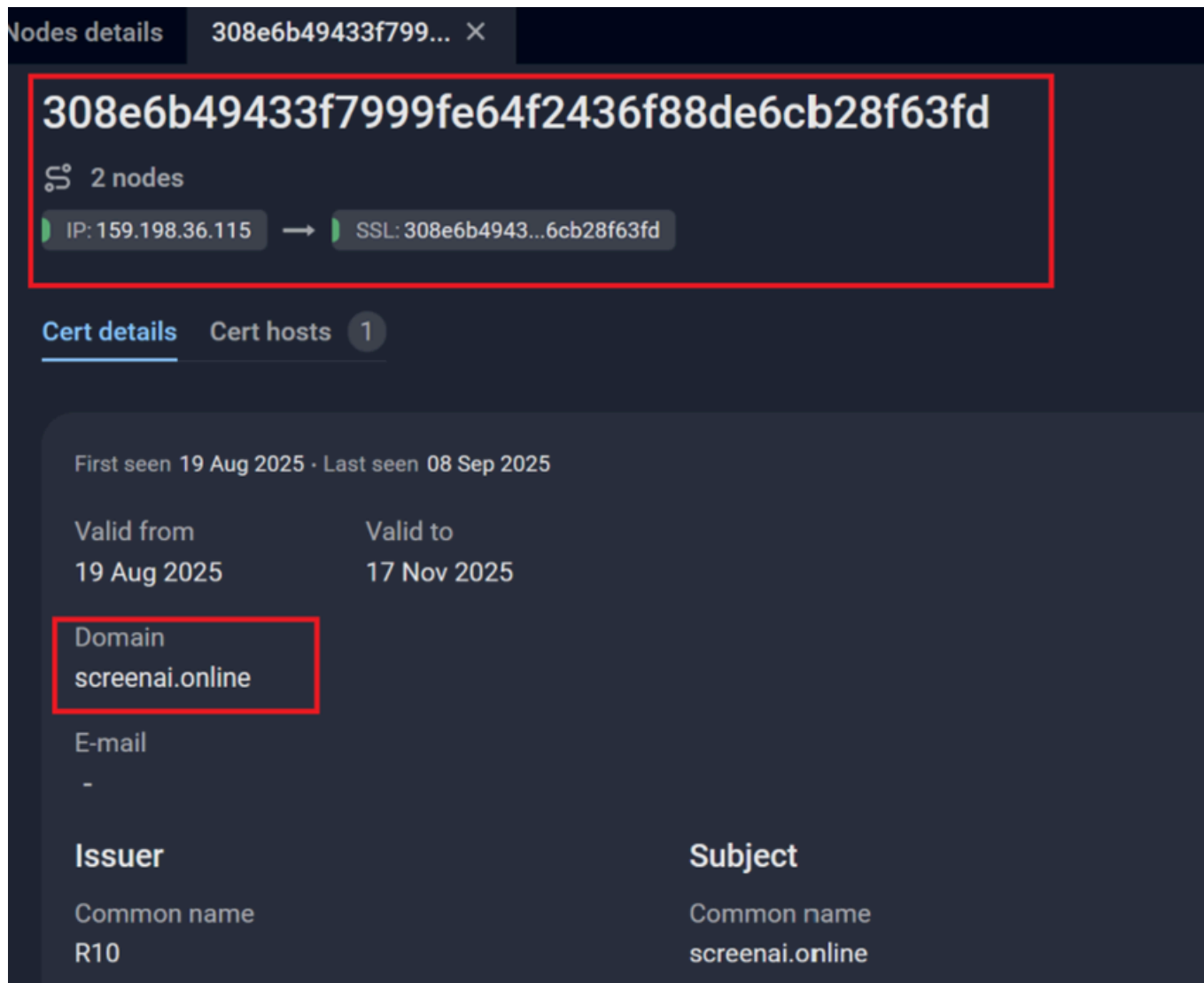


Figure 10. A screenshot of the SSL certificate used by C2 via Group-IB's [Threat Intelligence platform](#).

Analyzing the banners associated with the real IP address reveals several findings:

- The threat actor deployed the server and server-side C2 component on **19 August 2025**, and took it down on **24 August 2025**, indicating an **active attack window of about five days**.
- The C2 component initially ran on **Uvicorn**, until MuddyWater replaced it with **Apache** on 24 August 2025 which had been responding with a "503 service unavailable" message.
- The web page displayed the title "**ScreenAI | Your On-Screen Content Genius**"

<input type="checkbox"/>	<a href="#">159.198.36.115</a> AS 22612	443	<a href="#">HTTP/1.1 503 Service Unavailable</a>	<a href="#">503 Service Unavailable</a>	380 B	2025-08-31
<input type="checkbox"/>	<a href="#">159.198.36.115</a> AS 22612	443	<a href="#">HTTP/1.1 503 Service Unavailable</a>	<a href="#">503 Service Unavailable</a>	380 B	2025-08-26
<input type="checkbox"/>	<a href="#">159.198.36.115</a> AS 22612	443	<a href="#">HTTP/1.1 503 Service Unavailable</a>	<a href="#">503 Service Unavailable</a>	380 B	2025-08-24
<input type="checkbox"/>	<a href="#">159.198.36.115</a> AS 22612	443	<a href="#">HTTP/1.1 200 OK</a>	<a href="#">ScreenAI   Your On-Screen Content Genius</a>	19.198 KB	2025-08-21
<input type="checkbox"/>	<a href="#">159.198.36.115</a> AS 22612	8080	<a href="#">HTTP/1.1 200 OK</a>	<a href="#">ScreenAI   Your On-Screen Content Genius</a>	19.198 KB	2025-08-21
<input type="checkbox"/>	<a href="#">159.198.36.115</a> AS 22612	443	<a href="#">HTTP/1.1 200 OK</a>	<a href="#">ScreenAI   Your On-Screen Content Genius</a>	19.198 KB	2025-08-19
<input type="checkbox"/>	<a href="#">159.198.36.115</a> AS 22612	8080	<a href="#">HTTP/1.1 200 OK</a>		0 B	2025-08-19
<input type="checkbox"/>	<a href="#">159.198.36.115</a> AS 22612	443	<a href="#">HTTP/1.1 200 OK</a>		0 B	2025-08-19

Figure 11. A screenshot of the real IP address of the C2 server.

### HTTPS Request to 443

<https://159.198.36.115:443/>

16d 14h ago  
2025-08-19

[View Full HTML](#)  
Enterprise Only

▼ Response Banner

```

HTTP/1.1 200 OK
Date: Tue, 19 Aug 2025 <redacted> GMT
Server: uvicorn
content-type: text/html; charset=utf-8
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 4697
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

```

### HTTP Request to 8080

<http://159.198.36.115:8080/>

14d 14h ago  
2025-08-21

[View Full HTML](#)  
Enterprise Only

▼ Response Banner

```

HTTP/1.1 200 OK
date: Thu, 21 Aug 2025 <redacted> GMT
server: uvicorn
content-length: 19659
content-type: text/html; charset=utf-8

```

Figure 12. A screenshot of the C2 server's real IP address and installed application on port 443 and port 8080.

Given the short attack timeframe and the fact that disabling the C2 server renders the deployed backdoors inactive, we assess that MuddyWater has probably followed up with additional tools or malware on infected hosts to maintain access and continue intelligence gathering, this assessment is supported by the open directory observed on that IP which has several RMM and post exploitation tools.

The open directory was exposed using a Python simple HTTP server (SimpleHTTP/0.6 Python/3.10.12). It is noteworthy that no similar servers were identified

# Directory listing for /

---

- [.ansible/](#)
  - [.bash\\_history](#)
  - [.bashrc](#)
  - [.cache/](#)
  - [.config/](#)
  - [.launchpadlib/](#)
  - [.lessht](#)
  - [.local/](#)
  - [.profile](#)
  - [.viminfo](#)
  - [47/](#)
  - [a.txt](#)
  - [act.msi](#)
  - [chromium\\_stealer\\_user.exe](#)
  - [config.txt](#)
  - [dell.txt](#)
  - [dq.msi](#)
  - [FMAPP.dll](#)
  - [FMAPP.exe](#)
  - [PDQConnectAgent-5.8.18.msi](#)
  - [snap/](#)
  - [tmp/](#)
- 

Figure 13. Screenshot of the open directory exposed on the C2 server.

## Custom Malware and new Remote Monitoring and Management Tool:

During investigation of the infrastructure tied to this campaign, specifically 159[.]198[.]36[.]115, Group-IB Threat Intelligence identified a custom tool and several remote monitoring and management (RMM) utilities hosted on the attacker C2 server. These components appear to have been used for remote access and credential harvesting on compromised hosts. We believe that those tools and utilities were potentially used in this campaign by Muddywater.

The artifacts observed on the C2 include a custom browser credential stealer and two RMM utilities:

- **Chromium\_Stealer:** Custom browser credential stealer hosted at  
`hxxp://159.198.36[.]115:4444/chromium_stealer_user.exe`, disguised as a calculator application.
- **Action1:** RMM tool identified on the C2, used for remote management and command execution.
- **PDQ RMM:** Additional RMM utility found on the same C2 server, previously observed in MuddyWater operations.

### Chromium\_Stealer — technical summary

**Host URL:** `hxxp://159.198.36[.]115:4444/chromium_stealer_user.exe`

**Disguise:** Appears as a calculator-like user App to reduce suspicion.

**Primary goal:** Harvest credentials stored by browsers and write the harvested data to a local staging file.

#### Observed behavior:

1. Enumerates browsers profile directories to locate the Local State file and profile databases.
2. Extracts the `os_crypt.encrypted_key` from Local State and uses OS crypto APIs to unwrap the master key.
3. Terminates active browser processes mostly to remove file locks on profile databases.
4. Opens Login Data files to extract stored login credentials.
5. Decrypts credentials using the recovered master key and writes the results to a local staging file at

C:\Users\Public\Downloads\cobe-notes.txt(credentials are written in encrypted form).

6. Restores the browser by restarting it from its last state to minimize user suspicion.

#### Affected browsers:

- Google Chrome
- Opera
- Brave
- Microsoft Edge

```
Thread = CreateThread(0LL, 0LL, (LPTHREAD_START_ROUTINE)Fake_calc, 0LL, 0, 0LL);
Sleep_0(dwMilliseconds);
if ( v2 )
    MessageBoxA(0LL, "This program is designed to work in all systems.", "info", 0x40u);
Google_Chrom();
BraveSoftware();
Opera();
Edge_();
TerminateThread(Thread, 0);
CloseHandle_0(Thread);
ExitProcess(0);
```

Figure 14. Entry point of the Chromium stealer.

## Conclusion

MuddyWater remains a persistent Iran-aligned threat actor engaged in long-term espionage and infiltration campaigns targeting high-value governmental, and international organizations across the Middle East, with expanding operations observed in Europe, Africa, and North America.

This campaign highlights MuddyWater's evolving tradecraft and operational maturity. The group leveraged a compromised mailbox to exploit trusted communication channels, a highly effective social engineering vector that bypassed conventional security defenses. By deploying updated malware variants such as the Phoenix v4 backdoor, the FakeUpdate injector, and custom credential-stealing tools alongside legitimate RMM utilities like PDQ and Action1, MuddyWater demonstrated an enhanced ability to integrate custom code with commercial tools for improved stealth and persistence.

Given MuddyWater's sustained focus on governmental targets especially amid the ongoing geo-political tension in the region, Group-IB expects similar campaigns will continue to emerge, leveraging newly compromised accounts and evolving payloads. MuddyWater's consistent pattern of reusing and modifying its custom malware families underscores a long-term strategic intelligence objective rather than pursuit of short-term gain.

## Recommendations

Organizations, particularly those operating within government and critical infrastructure sectors, can strengthen their defenses against MuddyWater and similar state-aligned actors by implementing the following measures:

- **Strengthen Threat Intelligence and Monitoring**
  - Subscribe to trusted [Threat Intelligence feeds](#) to receive up-to-date Indicators of Compromise (IOCs) and Tactics, Techniques, and Procedures (TTPs) related to MuddyWater.
  - Conduct continuous threat hunt for indicators associated with Phoenix, FakeUpdate, and related infrastructure (e.g., screenai[.]online, sysprocupdate.exe).
  - Integrate YARA rules and [Endpoint Detection and Response](#) (EDR) detections for known MuddyWater malware families.
- **Enhance Email and Phishing Defenses**



- Deploy **sandboxing and attachment scanning** for Office documents, flagging those with embedded macros or suspicious VBA code.
- Conduct **regular phishing simulations** and awareness training for personnel, emphasizing “enable content” macro lures.
- **Implement Endpoint and Access Controls**
  - Disable Office macros by default through Group Policy and allow execution only from signed or trusted sources.
  - Deploy and tune [EDR/XDR solutions](#) to detect PowerShell misuse, process injection, and abnormal auto registry modifications.
  - Enforce Multi-Factor Authentication (MFA) across all accounts to prevent unauthorized mailbox access.
- **Strengthen Network and Infrastructure Security**
  - Monitor outbound traffic for unusual beaconing or repeated HTTP(S) requests matching known MuddyWater C2 patterns and domains.
  - Restrict, log, and monitor the use of remote monitoring and management tools (RMMs) such as Action1, PDQ, and ScreenConnect, and only allow the RMM tools needed for the organization.
- **Build Long-Term Strategic Defense**
  - Maintain comprehensive asset visibility and enforce least-privilege principles for all critical systems.
  - Deploy behavioral-based anomaly detection for account logins and email patterns from unexpected regions or VPNs.
  - Periodically review and update incident response and crisis playbooks to address phishing-based intrusions and credential-compromise scenarios.

DISCLAIMER. All technical information, including malware analysis, indicators of compromise and infrastructure details provided in this publication, is shared solely for defensive cybersecurity and research purposes. Group-IB does not endorse or permit any unauthorized or offensive use of the information contained herein. The data and conclusions represent Group-IB’s analytical assessment based on available evidence and are intended to help organizations detect, prevent, and respond to cyber threats.

Group-IB expressly disclaims liability for any misuse of the information provided. Organizations and readers are encouraged to apply this intelligence responsibly and in compliance with all applicable laws and regulations.

## Frequently Asked Questions

### What is the MuddyWater Espionage Campaign?

arrow\_drop\_down

This is a cyber-espionage operation conducted by MuddyWater, an Iran-linked Advanced Persistent Threat (APT) group. During this campaign were sent phishing emails containing Phoenix backdoor malware to over 100 governmental targets worldwide.

### When did this campaign begin?

arrow\_drop\_down

The operation began on 19 August 2025, with evidence indicating that MuddyWater accessed and used an email account through a NordVPN connection to distribute phishing emails.

### How were victims targeted?

arrow\_drop\_down

Victims received phishing emails that appeared to come from legitimate sources. The attached Microsoft Word documents urged recipients to “enable content.” Once enabled, malicious VBA macros executed code that installed the Phoenix v4 backdoor, giving attackers persistent access to the victim’s system.

## What malware families were used in the attack?

arrow\_drop\_down

The primary malware families identified include:

- Phoenix Backdoor (Version 4) — used for persistence, command execution, and data exfiltration.
- FakeUpdate Injector — used to deploy the Phoenix backdoor.
- Chromium\_Stealer — a custom credential stealer disguised as a calculator app.
- Remote Monitoring and Management (RMM) Tools — PDQ RMM and Action1, used for remote control and persistence.

## How does the Phoenix Backdoor work?

arrow\_drop\_down

Version 4 of the Phoenix backdoor works by:

- Creating a mutex (sysprocupdate.exe) for process uniqueness.
- Gathering host and system information.
- Copying itself to C:\ProgramData\sysprocupdate.exe.
- Establishing persistence via Windows Registry modification.
- Communicating with its Command-and-Control (C2) server over WinHTTP, receiving and executing attacker commands.

## What is the significance of the C2 domain “screenai[.]online”?

arrow\_drop\_down

The domain screenai[.]online served as the core command-and-control hub for the operation, registered on 17 August 2025 via NameCheap and hosted on 159[.]198[.]36[.]115 behind Cloudflare infrastructure. It remained active for approximately five days, indicating a short and tightly controlled attack window.

## How did Group-IB attribute the campaign to MuddyWater?

arrow\_drop\_down

Attribution was made with high confidence based on shared malware code and macros previously observed in MuddyWater campaigns, consistent targeting patterns focused on governmental entities, and the presence of MuddyWater’s known tools, including FakeUpdate, Phoenix, and PDQ RMM.

## What is MuddyWater’s background and motivation?

arrow\_drop\_down

MuddyWater (also known by aliases such as Seedworm, TA450, Boggly Serpens, and Earth Vetala) has operated since 2017 and is reportedly linked to Iran’s Ministry of Intelligence and Security (MOIS); its primary objectives include long-term espionage and intelligence gathering, tactical disruption of geopolitical adversaries, and maintaining sustained access to strategic sectors such as government, energy, and telecommunications.

## Indicators of Compromise (IOCs)

Backdoor mononoke.exe	668dd5b6fb06fe30a98dd59dd802258b45394ccd7cd610f0aaab43d801bf1a1e
Backdoor mononoke.exe	5ec5a2adaa82a983fcc42ed9f720f4e894652bd7bd1f366826a16ac98bb91839
Backdoor sysProcUpdate	1883db6de22d98ed00f8719b11de5bf1d02fc206b89fedd6dd0df0e8d40c4c56
Backdoor sysProcUpdate	3ac8283916547c50501eed8e7c3a77f0ae8b009c7b72275be8726a5b6ae255e3
Backdoor sysProcUpdate	76fa8dca768b64aefedd85f7d0a33c2693b94bdb55f40ced7830561e48e39c75

Backdoor	sysProcUpdate	3d6f69cc0330b302ddf4701bbc956b8fca683d1c1b3146768dcbce4a1a3932ca
C2	Creation date	screenai[.]online
Domain	2025-08-17	
C2 IP	real IP address behind CloudFlare	159[.]198[.]36[.]115