

DREAM

CTI Analysis Report

Turbid Currents: MuddyWater Attribution

Table of Contents

Executive Summary 2

Attack #1: NetivTech Targeting..... 7

 Attacker Attribution 7

Attack #2: ProcessPlanet..... 9

 Attacker Attribution 9

Attack #3: Photosjournalism 11

 Attacker Attribution 11

Attack #4: Hungary Gov Targeting..... 13

 Attacker Attribution 13

Attack #5: Diplomatic and Embassies Targeting 15

 Attacker Attribution 15

Attack #6: UAE Marine Sector Targeting 16

 Attacker Attribution 16

Attack #7: Azerbaijan Diplomatic Targeting..... 18

 Attacker Attribution 18

Attack #8: The Microsoft Lure 20

 Attacker Attribution 21

Attack #9: Seminar Lure..... 22

 Attacker Attribution 22

Conclusion..... 24

Indicators of Compromise (IoCs)..... 25

Executive Summary

This report provides a detailed overview of phishing campaigns associated with the Iranian APT group **MuddyWater** (also known as **Static Kitten** or **Mercury**). These campaigns, active between **February 2025 and October 2025**, demonstrate the group's persistence, technical consistency, and evolving tactics, techniques, and procedures (TTPs). The operations targeted **Israel, Hungary, the United Arab Emirates (UAE), Azerbaijan, Turkmenistan, and diplomatic missions worldwide**, reflecting MuddyWater's broad geopolitical interests and regional intelligence priorities.

In our **previous publication**, the campaign was tentatively attributed to an Iranian-linked cluster sharing overlapping TTP's tactics, techniques, and procedures (TTPs) with several known groups. However, subsequent discoveries prompted a **re-evaluation** of the entire infrastructure, tooling, and operational workflow. This report presents a comprehensive **re-analysis of nine interconnected attacks**, including the recent intrusion against several entities, with the objective of achieving a **conclusive and evidence-based attribution**.

Through detailed examination of **command-and-control infrastructure, malware families, and email delivery mechanisms**, Dream identified a unified operational fingerprint that aligns with **MuddyWater**. The consistent use of identical **C2 response patterns**, VBS loaders, and encoded staging logic across multiple regions including the Middle East, Europe, and South Asia points to a single orchestrating entity.

This report therefore not only **revisits earlier assumptions** but establishes a **definitive link** between previously isolated incidents and MuddyWater's long-standing espionage apparatus. By dissecting the actor's **infrastructure reuse, malware development lifecycle, and cross-operation TTPs**, Dream presents a **clear and technically substantiated attribution narrative**.

Overall, the **ten attacks** described in this report demonstrate that **MuddyWater** consistently employs the same **infrastructure patterns, reuses malware tools, and replicates phishing templates** across its operations. Together, these findings expose a **well-coordinated campaign** that underscores the group's persistence and strategic focus on **defense, government, education, and diplomatic sectors**.

Attribution across these campaigns was established through multiple technical pivots:

Identifier	Registration Timestamp, Registrar, and App.msi Template.	Phishing Document Templates	Raw Hex to Bytes Decoding	Recurring "#success!" HTTP Fingerprint and Shared Hosting Providers	Code Similarity
#1	Yes	Yes	Yes	-	-
#2	Yes	-	-	-	-
#3	-	Yes	-	Yes	-
#4	-	-	Yes	-	-
#5	-	-	-	Yes	Yes
#6	-	-	-	Yes	Yes
#7	-	-	-	-	Yes
#8	-	-	-	-	Yes
#9	-	-	-	-	Yes

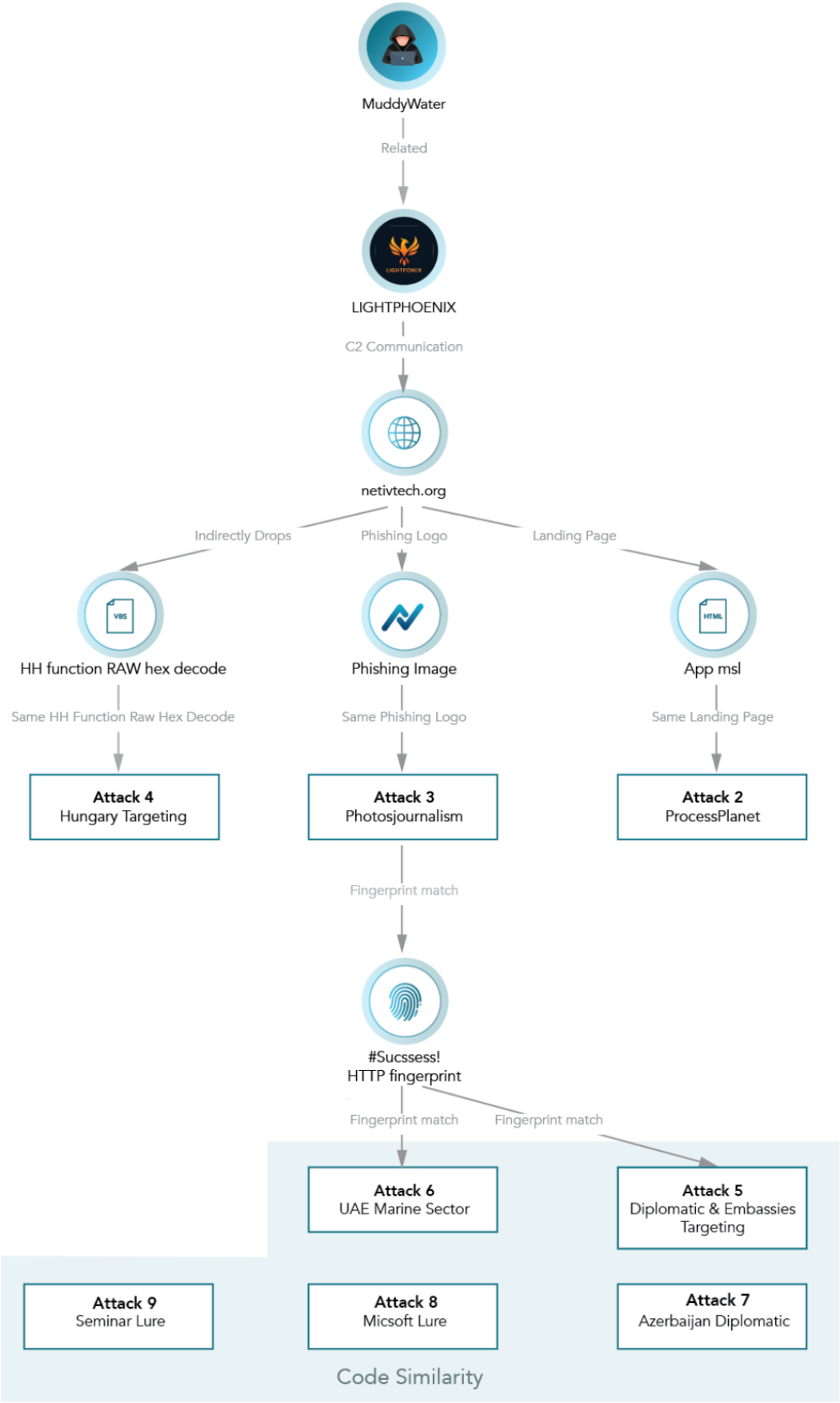


Figure 1: The Pivoting and Attribution Logic of the Turbid Currents attacks.

The following table summarizes each attack and its general description:

Attack Alias	Description	Date
Attack #1: NetivTech	Targeted an Israeli defense supplier using a spoofed IIOSH document by delivering the LIGHTPHOENIX malware, attributed to the MuddyWater APT, through a Word-to-VBS dropper chain. Using three distinct TTPs supporting attribution: • The App.MSI landing page template. • A phishing document spoofing IIOSH. • The HH decoding function.	Jun 2025
Attack #2: ProcessPlanet	Infrastructure-only setup with no confirmed victims. Domain registered simultaneously with Attack #1 and reused the App.MSI template.	Feb 2025
Attack #3: Photosjournalism	Two dropper chains using shifted-hex decoding and distinctive #success! Server responses. Phishing docs visually matched Attack #1.	Jun 2025
Attack #4: Hungary Gov	Likely targeted the Hungarian government with government-themed phishing documents. Reused HH decoding function and raw hex-to-bytes logic from Attack #1.	Apr 2025
Attack #5: Diplomatic Missions	Global phishing attacks against embassies and consulates were delivered using a compromised Oman MFA mailbox. The operation deployed the sysProcUpdate malware, and the C2 server returned the distinctive "#success!" server response linked to MuddyWater.	Aug 2025
Attack #6: UAE Marine Sector	Marine infrastructure-themed phishing. Delivered sysProcUpdate malware by decoding three-digit numbers to ASCII, and returned the distinctive "#success!" server response.	Aug 2025
Attack #7: Azerbaijan Diplomatic	MuddyWater impersonated the Azerbaijan Investment Company (AIC) using a convincing Azerbaijani-language Word document.	Sep 2025

Attack Alias	Description	Date
Attack #8: The Microsoft Lure	MuddyWater used a Spanish-language CV phishing lure impersonating UAE-based company to trick victims into enabling macros that deployed the Miaza V2.	Sep 2025
Attack #9: Seminar Lure	MuddyWater conducted regionally tailored seminar-themed phishing attacks targeting at list Oman and Egypt	Oct 2025

Attack #1: NetivTech Targeting

In June 2025, MuddyWater launched a phishing campaign against **NetivTech**, an Israeli company specializing in advanced mechanical and electro-mechanical systems. NetivTech is a trusted supplier to the **Israeli Ministry of Defense** and healthcare, printing, and high-tech industries, making it an attractive espionage target. The lure was a malicious Word document titled “*New Protocols and Rules.doc*”, designed to impersonate the **Israel Institute for Occupational Safety and Hygiene (IIOSH)**, lending authenticity to the attack.

The attack technical details are as follows:

Target	Israeli company NetivTech is a supplier to the Ministry of Defense, healthcare, and high-tech companies.
C2	netivtech[.]org (mimicking netivtech[.]com)
Lure	Phishing document spoofing IIOSH (Israel Institute for Occupational Safety and Hygiene).
Dropper Chain	Word document → VBS script → LIGHTPHOENIX malware

Attacker Attribution

When the document was opened, it triggered a known MuddyWater drop chain, using a VBS script with the **HH function** and raw hex-to-bytes decoding to rebuild the payload, which delivered the **LIGHTPHOENIX** malware.

Analysis of the infrastructure showed the use of the spoofed domain netivtech[.]org, which mimicked the legitimate netivtech.com, and a unique **App.msi HTML file** acting as a fake “Coming Soon” landing page with a 28-day countdown timer and a “**Notify Me**” button with correlate with other MuddyWater attack describe in this report.

Security vendors like ESET, Fortinet, and Palo Alto Networks attributed this campaign to MuddyWater, further solidifying the connection.

The LIGHTPHOENIX malware has already been publicly linked to MuddyWater operations, supporting the attribution of this campaign. In addition to LIGHTPHOENIX, another malware sample was delivered through URLs associated with netivtech[.]org (MD5: a9effec03c1945f791e72c39acf51f8f).

This sample has been identified by multiple security vendors as a MuddyWater-related threat, further confirming the connection between the observed infrastructure and the group’s known activities.

The attack's unique features are as follows:

- **Decoding Method:** HH function + raw hex → bytes decoding.
- **Unique Landing Page:** App.MSI HTML file is disguised as a “Coming Soon” page with a countdown timer and “Notify Me” button.
- **Phishing Document:** Crafted to appear as if sent by IIOSH (Israel Institute for Occupational Safety and Hygiene).

Popular threat label 🔗 trojan.muddywater		Threat categories	trojan		Family labels	muddywater	
Arctic Wolf	🚩	Unsafe		Bkav Pro	🚩	W64.AIDetectMalware	
CrowdStrike Falcon	🚩	Win/malicious_confidence_100% (W)		Cynet	🚩	Malicious (score: 100)	
DeepInstinct	🚩	MALICIOUS		Elastic	🚩	Malicious (high Confidence)	
ESET-NOD32	🚩	A Variant Of Win64/MuddyWater.J		Fortinet	🚩	W64/MuddyWater.J!tr	
Ikarus	🚩	Win32.Outbreak		Kaspersky	🚩	UDS:Trojan.Win32.GenericML.xnet	
McAfee Scanner	🚩	Ti!4CEE79E24AA3		Microsoft	🚩	Trojan:Win32/Wacatac.B!ml	
Palo Alto Networks	🚩	Generic.ml		Rising	🚩	Trojan.MuddyWater!8.F548 (CLOUD)	

Figure 2: A sample classified by ESET, Fortinet, and Palo Alto Networks as a MuddyWater variant.

Attack #2: ProcessPlanet

In February 2025, threat activity was observed using the command-and-control domain **processplanet[.]org**. No confirmed victims or phishing lures were recovered, leaving the specific targeting unknown.

The attack technical details are as follows:

Target	N/A
C2	processplanet[.]org → 194[.]111[.]246[.]101
Lure	N/A
Dropper Chain	N/A

Attacker Attribution

Attribution analysis reveals strong overlaps with the previously observed **NetivTech** campaign. Both **processplanet[.]org** and **netivtech[.]org** were registered via **NameCheap** at the exact same timestamp (2024-11-27T16:32:31Z), indicating coordinated domain preparation and infrastructure control. In addition, both domains hosted the distinctive **App.MSI** HTML landing page, a fake “Coming Soon” site featuring a 28-day countdown timer and a “Notify Me” button, highlighting a shared operational template and consistent threat actor tooling.

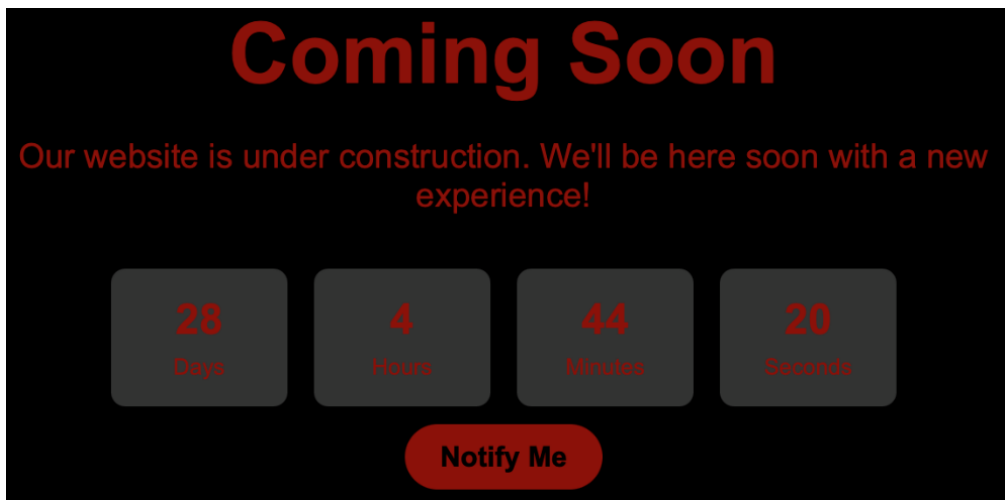


Figure 3: An example of App.msi and the Coming Soon landing page display.

The attack's unique features are as follows:

- **Domain Registration:** The domain processplanet[.]org was registered through NameCheap on 2024-11-27T16:32:31Z.
- **Landing Page Artifact:** Used the same App.MSI HTML file observed in the wild. This file mimics a "Coming Soon" landing page, displaying a 28-day countdown timer ending at 12:00 PM, along with generic text and a "Notify Me" button.

Attack #3: Photosjournalism

In June 2025, a major telecom provider in Central Asia was targeted in a highly coordinated phishing campaign attributed to **MuddyWater**. The attackers used the domain **photosjournalism[.]com** as part of their command-and-control infrastructure, distributing macro-enabled Word documents crafted to impersonate the **Israel Institute for Occupational Safety and Hygiene (IIOSH)**. The lures were nearly identical to earlier MuddyWater campaigns, reusing the same template, iconography, and decoy formatting to maintain visual consistency and credibility. The messages were not sent through legitimate user accounts but were injected directly into the organization’s mail transport system, bypassing authentication and internal sender validation mechanisms.

The attack technical details are as follows:

Target	major telecom provider in Central Asia
C2	photosjournalism[.]com → 45[.]150[.]108[.]151
Lure	Phishing document spoofing IIOSH (Israel Institute for Occupational Safety and Hygiene).
Dropper Chain	Word document → VBS script → EXE file (two distinct chains were observed)

Attacker Attribution

The reuse of the same phishing template seen in Attack #1 was evident again in this campaign, with documents closely matching the earlier design and showing MuddyWater’s dependence on recurring lures.

Infrastructure analysis also revealed the recurring fingerprint of an HTTP body response containing **“#success!”**, along with the use of BlueVPS hosting, one of the group’s preferred infrastructure providers.

This strong alignment across phishing document design, decoding techniques, and infrastructure markers directly attributes the activity to MuddyWater, with Attack #3 representing a cluster of two closely connected chains that demonstrate the group’s repeated use of document templates and specialized decoding methods across multiple campaigns.

כדי להציג את המסמך, הפעל את Active content



Figure 4: An example of the phishing document spoofing the Israel Institute for Occupational Safety and Hygiene (IIOSH)

The attack's unique features are as follows:

- **Decoding Method:** Shifted-Hex decoding.
- **Infrastructure Response:** The fingerprint of an HTTP body response containing "#success!".

Attack #4: Hungary Gov Targeting

On April 2025, MuddyWater activity was detected using a direct IP address hosted by BitLaunch, rather than a domain-based command-and-control server. The phishing lure posed as the Hungarian police, presenting itself as an urgent government message. The document told recipients to “Enable Content” and enter their password to access supposedly important information. This social engineering tactic strongly suggests the campaign aimed to compromise Hungarian law enforcement and government institutions. The linked dropper chain used the HH function and raw hex → bytes decoding to rebuild the malware payload, demonstrating both the reuse of established MuddyWater techniques and the group’s flexibility in using bare IP infrastructure.

The attack technical details are as follows:

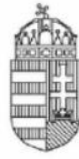
Target	Likely Hungarian government / police , based on phishing lure content.
C2	46[.]101[.]36[.]39 (BitLaunch hosting, direct IP with no domain).
Lure	The phishing document is consistent with government-themed targeting.
Dropper Chain	Word document → VBS script → EXE file.

Attacker Attribution

The reuse of the HH function and raw hex Reusing the HH function and decoding raw hex to bytes are similar to those in Attack #1. These methods show consistency across MuddyWater campaigns and establish a strong technical link between them. When combined with the group’s typical techniques, this highlights MuddyWater’s expansion beyond Israeli targets into Central Europe, using customized phishing lures that exploit trust in national police.

Bytes decoding identical to those seen in Attack #1 demonstrate continuity and establish a strong technical link between campaigns. Overall, this suggests MuddyWater’s expansion beyond Israeli targets, using tailored phishing lures to exploit trust in national police authorities.

Figyelem!
A tartalom fontos.
Kattintson az **Enable content** gombra, és adja meg a jelszavát.



BARANYA MEGYEI RENDŐR-FŐKAPITÁNYSÁG
GAZDASÁGI IGAZGATÓSÁG

Figure 5: An example of the phishing document spoofed the Hungarian police, instructing the recipient to "Enable Content" and enter their password.

The attack's unique features are as follows:

- **Decoding method:** Raw hex to bytes.
- **Function name:** HH.
- **Infrastructure pattern:** Direct IP (46[.]101[.]36[.]39) hosted at BitLaunch.

Attack #5: Diplomatic and Embassies Targeting

In August 2025, MuddyWater actors used the domain `screenai[.]online` in a large-scale phishing campaign targeting embassies, consulates, and diplomatic missions across Europe, the Middle East, Africa, and Asia.

The phishing lures impersonated official communications from the Ministry of Foreign Affairs (MFA) and were sent through a compromised Oman MFA email account. When opened, the phishing files deployed VBS scripts that reconstructed the `sysProcUpdate` malware using the three-digit numeric to ASCII decoding method through the `dddd` function. This same decoding approach had been seen in other MuddyWater operations, highlighting the group's consistent use of certain tools.

The attack technical details are as follows:

Target	Embassies, consulates, and diplomatic missions across Europe, Middle East, Africa, and Asia.
C2	<code>screenai[.]online</code> → <code>159[.]198[.]36[.]115</code>
Lure	Phishing Word documents impersonating MFA communications, distributed via a compromised Oman MFA mailbox.
Dropper Chain	Word document → VBS script → <code>sysProcUpdate</code> malware (three chains were observed).

Attacker Attribution

The campaign showed the characteristic MuddyWater fingerprint of an HTTP body response containing `"#success!"`. This connection strongly ties the activity to MuddyWater and aligns it with the group's broader operational patterns. Attack #5 is one of MuddyWater's most ambitious and wide-reaching efforts, targeting diplomatic entities worldwide through a mix of compromised infrastructure and consistent tradecraft.

The attack's unique features are as follows:

- **Dropped Malware:** `sysProcUpdate`
- **Decoding Method:** Three-Digit Numeric → ASCII.
- **Decoding Function:** `dddd`.
- **Infrastructure Response:** The fingerprint of an HTTP body response containing `"#success!"`.

Attack #6: UAE Marine Sector Targeting

In August 2025, MuddyWater conducted a phishing campaign targeting the UAE marine and energy sector, using the C2 domain `screenai[.]online`. The bait was a malicious Word document titled “DPR for dredging in FreeSpan_16082025.2.doc,” designed to look like an official daily progress report for a marine infrastructure project. To enhance credibility, the document featured branding from the NPCC-Saipem Joint Venture and NMDC Dredging & Marine, two key companies in the UAE’s offshore energy and marine engineering sectors. When opened, the file deployed the `sysProcUpdate` malware, reconstructed through the Three-Digit Numeric → ASCII decoding method implemented via the `dddd` function. The campaign also displayed the recurring MuddyWater server marker “#success!”, further embedding it into the group’s operations.

The attack technical details are as follows:

Target	UAE marine sector
C2	<code>screenai[.]online</code> → <code>159[.]198[.]36[.]115</code>
Lure	Malicious Word document (DPR for dredging in FreeSpan.doc) masquerading as a marine infrastructure project file.
Dropper Chain	Word document → VBS script → sysProcUpdate malware (two chains were observed)

Attacker Attribution

The distinctive server response “# success!”, combined with the reuse of the **dddd decoding function** and the **three-digit numeric → ASCII decoding method**, strongly attributes this activity to **MuddyWater**. The campaign also delivered the **sysProcUpdate malware**, aligning it with the group’s previously observed toolset. These technical overlaps – malware family, decoding logic, and recurring infrastructure marker – reinforce attribution and illustrate MuddyWater’s consistent tradecraft across operations.

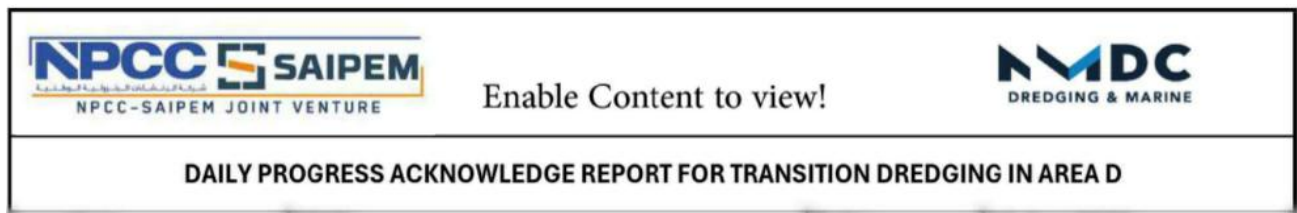


Figure 6: An example of the phishing document spoofing NPCC-Saipem Joint Venture and NMDC Dredging & Marine to target the UAE marine sector.

The attack's unique features are as follows:

- **Dropped malware:** sysProcUpdate
- **Decoding method:** Three-Digit Numeric → ASCII.
- **Decoding function:** dddd.
- **Server response marker:** #success!.

Attack #7: Azerbaijan Diplomatic Targeting

In September 2025, MuddyWater launched a targeted campaign against Azerbaijan, impersonating the Azerbaijan Investment Company (AIC).

The lure was a fraudulent Word document designed to look like an official AIC announcement inviting employees to an upcoming Zoom call.

The document replicated AIC’s legitimate logo, address, and contact information, and was written entirely in Azerbaijani to increase authenticity.

While the embedded Zoom link served only to enhance credibility, the malicious payload was executed immediately upon opening the Word file, beginning the infection chain without additional user interaction.

The Azerbaijan Investment Company (AIC), founded in 2006, is a state-owned entity under the Ministry of Economy. It invests directly in projects that diversify the non-oil sector of Azerbaijan’s economy, focusing on agriculture, industry, logistics, infrastructure, and technology.

By leveraging AIC’s well-known identity, the attackers effectively crafted a believable social-engineering vector targeting Azerbaijani public-sector employees.

The attack technical details are as follows:

Target	Azerbaijani government and state-affiliated organizations
C2	64[.]7[.]198[.]12 (BitLaunch hosting, direct IP with no domain).
Lure	Fake AIC Zoom training invitation (Word document in Azerbaijani)
Dropper Chain	Word document → VBS script → EXE file

Attacker Attribution

The tool’s use of **UDP-based communication over ports 1269 and 1259**, coupled with the **reuse of distinctive code elements**, provides strong indicators linking this activity to **MuddyWater**. These patterns align closely with previously analyzed samples associated with the group’s udp communication-based malware family. The combination of **network behavior** and **consistent implementation style** demonstrates clear **code lineage and operational continuity**, reinforcing the attribution to MuddyWater and underscoring the group’s characteristic tradecraft across multiple campaigns.



Figure 7: An example of the phishing document spoofing AIC to target Azerbaijani government and state-affiliated organizations

The attack's unique features are as follows:

- **Communication Similarity:** The malware communicated over UDP ports 1269 and 1259, mirroring MuddyWater's known network patterns and message structure.
- **Malware Variant:** A newly identified sample named **MiazaV2** was deployed, sharing core code similarities with the group's previous toolset.

Attack #8: The Microsoft Lure

On **September 15, 2025**, MuddyWater carried out a phishing campaign using a Spanish-language lure that impersonated CNS Middle East (CNS ME), a legitimate IT systems integrator based in the United Arab Emirates.

The malicious **Word document**, formatted as a professional CV, displayed a **blurred applicant's headshot and the red CNS corporate logo, making it appear genuine.**

The **blurred formatting** was intentionally designed to **trick recipients into clicking "Enable Content"**, a common social-engineering technique used to activate embedded macros. Once macros were enabled, the document triggered the **download and execution of the malware "Miaza V2"**, a recently updated variant of MuddyWater's loader family. The file then revealed the fake résumé content to complete the deception.

Although the document's text was entirely **in Spanish**, the use of a **UAE company logo** indicates a clear **mismatch between the language and the spoofed brand**, suggesting the material was **repurposed** from previous lure templates. The inconsistency of the Spanish language, combined with a Middle Eastern company identity, suggests that the campaign was likely targeted at **European or Spanish-speaking organizations**, particularly **HR or recruitment departments**, where such content would appear credible.

The lure communicated with its command-and-control (C2) infrastructure via the domain **microsoft[.]store**, a deliberate misspelling of *Microsoft*, designed to disguise malicious traffic as legitimate.

A **heavily obfuscated VBS macro** within the document executed the infection chain, reflecting **MuddyWater's recurring TTPs** observed across multiple regional spear-phishing campaigns.

Target	Likely Spanish organizations or recruiters (based on language and design)
C2	microsoft[.]store → 62[.]60[.]148[.]85
Lure	Fake Spanish (Word document in Spanish)
Dropper Chain	Word document → VBS script → EXE file

Attacker Attribution

The tool's use of **UDP-based communication over ports 1269 and 1259**, coupled with the **reuse of distinctive code elements**, provides strong indicators linking this activity to **MuddyWater**. These patterns align closely with previously analyzed samples associated with the group's udp communication-based malware family. The combination of **network behavior** and **consistent implementation style** demonstrates clear **code lineage and operational continuity**, reinforcing the attribution to MuddyWater and underscoring the group's characteristic tradecraft across multiple campaigns.

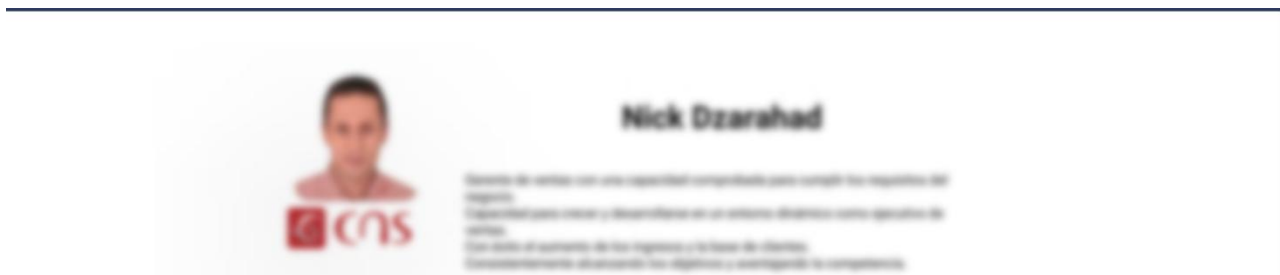


Figure 8: An example of the phishing document looks like a fake CV, displayed a blurred applicant headshot and the red CNS corporate logo

The attack's unique features are as follows:

- **Communication Similarity:** The malware communicated over **UDP ports 1269 and 1259**, mirroring MuddyWater's known network patterns and message structure.
- **Malware Variant:** A newly identified sample named **MiazaV2** was deployed, sharing core code similarities with the group's previous toolset.

Attack #9: Seminar Lure

On **October 7th, 2025**, MuddyWater launched a new phishing campaign targeting the Middle East, and likely Oman. The operation used a malicious Word document titled “Middle East and Maritime Economy.doc,” designed to look like a legitimate International Seminar Registration Form. The lure instructed recipients to “Enable Content to view this document,” a common tactic used to activate malicious macros. Once enabled, the document ran an obfuscated VBS payload, which downloaded a new malware variant and established communication with the command-and-control (C2) domain bootcamptg[.]org.

Two weeks later, on **October 21st, 2025**, MuddyWater reused the same infrastructure and document template in a new phishing wave likely targeting **Egypt**. This variant used a lure titled “**sondouq.doc**,” which translates to the word “*sondouq*” (صندوق), meaning “box” or “fund” in Arabic, thus suggesting a possible attempt to localize the bait for Arabic-speaking recipients. While the file maintained the same “International Seminar Registration” theme, it delivered a **modified VBS loader and distinct payload**. Despite these updates, the **infection vector** and **C2 chain** (bootcamptg[.]org → 161.35.228.250) remained unchanged, highlighting MuddyWater’s **iterative and regionally adaptive attack framework** targeting organizations across the **Middle East**.

Target	Likely Middle-Eastern entities (Oman and Egypt)
C2	bootcamptg[.]org → 161[.]35[.]228[.]250
Lure	Fake international seminar registration form
Dropper Chain	Word document → VBS script → EXE file (two different chains)

Attacker Attribution

Multiple technical indicators strongly support attributing both the October 7 and October 21 attacks to MuddyWater. The VBS loaders deployed in each operation show clear similarities. In addition at the code level. Additionally, the malware delivery chain remained consistent across the attacks described in this report: each attack used a macro-enabled Word document to run an obfuscated VBS stage, which then downloaded the subsequent payload. This recurring delivery pattern aligns with MuddyWater’s established TTPs.

The attack’s unique features are as follows:

- **Two lure documents:** “Middle East and Maritime Economy.doc” and “sondouq.doc”

- **Infrastructure Reuse:** Internal reuse of the same C2 domain (bootcamptg.org) and IP (161.35.228.250) across both waves.
- **Loader Evolution:** Iterative changes to the VBS loader and final payload while preserving the same dropper chain and seminar registration theme.

Conclusion

The campaign exposes MuddyWater's ongoing operations against Israel and regional governments, targeting defence, government, and educational institutions. These findings highlight MuddyWater's continued activity and its use of multi-vector phishing chains.

All attacks documented in this report are linked to MuddyWater based on the supporting technical evidence shared and detailed in this report.

Dream recommends the following actions to prevent a similar attack success:

- **Patch Management:** Prioritize patching Microsoft Office to reduce macro-enabled exploitation and Windows Script Host components.
- **Email Security Controls:** Strengthen mail filters to block or quarantine attachments containing macros, especially .DOC and .VBS files.
- **Configuration Hardening:**
 - Disable or restrict Microsoft Office macros by default.
 - Enforce firewall rules to block outbound connections to known MuddyWater C2 domains ([see IoC table](#)).

Indicators of Compromise (IoCs)

The CTI analysis includes the following IoCs:

#	Attack #	IoC Type	Identifier	Type
1.	1	File Hash	b445a9e92bc9609884c4ed6304a5dbdb	VBS
2.	1	File Hash	07824f0ee982774b25a3beeadc727734	DOC
3.	1	File Hash	32f51a376a8277649088047dd61efdf5	EXE
4.	1	File Hash	a9effec03c1945f791e72c39acf51f8f	EXE
5.	1	File Hash	61c45a0f9422406f27dc7342fb713cef	MSI
6.	1	Domain	Netivtech[.]org	C2
7.	2	Domain	Processplanet[.]org	C2
8.	2	IP	194[.]11[.]246[.]101	C2
9.	3	File Hash	e905d26ff243c54576ac78496189af7d	VBS
10.	3	File Hash	6636407299e0b1a74961ae998cec20e0	DOC
11.	3	File Hash	4dee09dcd5ab407ee9086445303e7cdf	EXE
12.	3	File Hash	d067c3fff70c1d61b60f2409090caade	VBS
13.	3	File Hash	adf7606b900fa1d4630f7fd63a585e60	DOC
14.	3	File Hash	844d714c0bdab06d4d85e26202e654dc	EXE
15.	3	Domain	Photosjournalism[.]com	C2
16.	3	IP	45[.]150[.]108[.]151	C2
17.	4	File Hash	759f5fea34a502edc8b0f4cf830cc6f4	VBS
18.	4	File Hash	2c19001d5b81037ac70ef17f887cbec0	DOC
19.	4	File Hash	c0fad3bdb4d0bd55ac8966687cf7c8fa	EXE
20.	4	IP	46[.]101[.]36[.]39	C2
21.	5	File Hash	8b01d3ba8a5df19a37d9bd212875c4aa	VBS
22.	5	File Hash	3ab16bd1c339fd0727be650104b74dd1	DOC

#	Attack #	IoC Type	Identifier	Type
23.	5	File Hash	7e73ca410dc6480c77a9236c0733c0a1	EXE
24.	5	File Hash	e71743da2965b2b85cc00dba5d9f6515	VBS
25.	5	File Hash	e2a5019f85a8aed140b13c87cf9a791a	DOC
26.	5	File Hash	69fed0fafc29065ff081793b4647bfc0	VBS
27.	5	File Hash	1de19958e7c2ef14addfb35b43a594ec	DOC
28.	5 and 6	Domain	Screenai[.]online	C2
29.	5 and 6	IP	159[.]198[.]36[.]115	C2
30.	6	File Hash	7e3c10bb262865a0daaf5c88a2fe7a79	VBS
31.	6	File Hash	e73ba93d008affdc4cce0cb4e18ae5c6	DOC
32.	6	File Hash	a408e056425307096dbf3e8b50a0b673	EXE
33.	6	File Hash	7e3c10bb262865a0daaf5c88a2fe7a79	VBS
34.	6	File Hash	d6ad04612f9a6060f3955c43ad5cf236	DOC
35.	6	File Hash	a408e056425307096dbf3e8b50a0b673	EXE
36.	7	File Hash	03a9dec54484756c7c1e2dc75df7efe4	VBS
37.	7	File Hash	07502104c6884e6151f6e0a53966e199	DOC
38.	7	File Hash	aa75a0baebc93d4ca7498453ef64128a	EXE
39.	7	File Hash	2963aaff56043ebae6d48589aa47a70	DOC
40.	7	IP	64[.]7[.]198[.]112	C2
41.	8	Domain	microsoft[.]store	C2
42.	8	Domain	fourdjecem[.]shop	Related Domain
43.	8	IP	62[.]60[.]148[.]85	C2
44.	8	File Hash	26e5ff398ec6b30c51d6b6552bb932f8	EXE
45.	8	File Hash	d1af72a943f3b1eb45934e07f205c5ed	DOC
46.	8	File Hash	b4b673c0a60e57c9c8f7560d609902b6	EXE
47.	9	Domain	bootcamptg[.]org	C2

#	Attack #	IoC Type	Identifier	Type
48.	9	IP	161[.]35[.]228[.]250	C2
49.	9	File Hash	cb9c3b49e8ceea7a058f8b09936cd338	VBS
50.	9	File Hash	b15c11faf60a41f855e117d9c1886b92	EXE
51.	9	File Hash	d9619d23098231bec2f17787d1d1b182	DOC
52.	9	File Hash	80f9e456c55af2a2fda224b58adfd72f	VBS
53.	9	File Hash	e67c4eee0f424064d811794fc8f80130	EXE
54.	9	File Hash	14fb6a186166577fab71d56cbe1c74d9	DOC
55.	9	Domain	portal-transafe[.]com	Related Domain
56.	9	Domain	Phoenixplus[.]co[.]za	Related Domain