INTRUVENT

THREAT ACTOR INTELLIGENCE PROFILE

MuddyWater

MOIS Cyber Espionage Unit / Mango Sandstorm / Static Kitten

Version 1.0
Last Updated March 11, 2026
Classification TLP:CLEAR
Attribution Confidence HIGH

Intruvent Technologies
INT-TAP-2026-MUDDYWATER-v1.0

9 Years

Active Espionage Operations (2017 – Present)

20+ malware families | 58 MITRE ATT&CK techniques | US critical infrastructure compromised (March 2026)

1 Attribution & Identity

ATTRIBUTION CONFIDENCE: HIGH

MuddyWater is assessed with high confidence to be a subordinate element within Iran's Ministry of Intelligence and Security (MOIS). This attribution was officially established by US Cyber Command on January 12, 2022, and reinforced by a joint advisory from the FBI, CISA, CNMF, and NCSC-UK on February 24, 2022 (AA22-055A). The group has conducted cyber espionage campaigns on behalf of MOIS since at least 2017, with some evidence suggesting operations may date to 2018 or earlier.

Background

MuddyWater is Iran's most prolific MOIS-affiliated cyber espionage group. First publicly identified and named by Palo Alto Unit 42 in November 2017, the group has since been tracked under more than a dozen vendor designations and has grown from deploying basic PowerShell backdoors into operating multiple custom C2 frameworks, Rust-based implants, and Deno-runtime backdoors.

The group's primary mission is intelligence collection in support of Iranian national security objectives. Its targeting of government, defense, telecommunications, and energy sectors across the Middle East, Europe, and North America aligns with Iranian geopolitical interests. Unlike its MOIS counterpart Void Manticore (Handala), which focuses on destructive operations, MuddyWater's core function is persistent espionage access, though it has participated in at least one destructive operation (the 2023 Technion attack, conducted in partnership with Storm-1084/DarkBit).

MuddyWater operates within a broader MOIS cyber ecosystem that includes Scarred Manticore (Storm-0861) for espionage and initial access provision, Void Manticore (Storm-0842/Handala) for destructive operations, Lemon Sandstorm for infrastructure pre-positioning in ICS/SCADA environments, and Cotton Sandstorm for influence operations. Documented overlaps in tooling and infrastructure across these groups suggest coordinated tasking by MOIS leadership.

Known Aliases

`MuddyWater` `Mango Sandstorm` `Static Kitten (CrowdStrike)` `MERCURY (Microsoft, legacy)` `TEMP.Zagros (Mandiant)` `Seedworm (Symantec)` `TA450 (Proofpoint)` `G0069 (MITRE)` `UNC3313 (Mandiant)` `Earth Vetala (Trend Micro)` `COBALT ULSTER (Secureworks)`

QUICK FACTS

- **Origin:** Iran (MOIS)
- **Active Since:** At least 2017
- **Motivation:** State-sponsored espionage
- **Sophistication:** High
- **Last Observed:** March 2026 (US targets)
- **Sponsor:** MOIS
- **MITRE ID:** G0069
- **C2 Frameworks:** 5+ custom
- **Malware Families:** 20+

> *"MuddyWater is a subordinate element within Iran's Ministry of Intelligence and Security (MOIS). This APT group has targeted a range of government and private-sector organizations across sectors including telecommunications, defense, local government, and oil and natural gas, in Asia, Africa, Europe, and North America."*
>
> CISA Advisory AA22-055A, co-authored by FBI, CISA, CNMF, and NCSC-UK (February 2022)

2 Targeting Profile

Industries

- **Government** (primary, since 2017)
- **Telecommunications**
- **Defense / Aerospace**
- **Oil & Gas / Energy**
- **Financial Services** (US bank, 2026)
- **Aviation** (US airport, 2026)
- **Education** (Technion, 2023)
- **Technology / IT**
- **Pharmaceuticals**

Regions

- **Middle East** (primary, since 2017)
- **Israel** (escalated since Oct 2023)
- **Turkey**
- **India / Pakistan**
- **United States** (2026, critical infra)
- **Canada** (NGOs, 2026)
- **Europe** (Italy, Portugal)
- **North Africa** (Algeria, Egypt)
- **Central Asia** (Turkmenistan)

Technologies

- **RMM Tools** (Atera, ScreenConnect, SimpleHelp, AnyDesk)
- **Microsoft Exchange**
- **Cloud Services** (Egnyte, Backblaze, Wasabi)
- **SysAid IT Management**
- **PaperCut Print Management**
- **Windows Endpoints**
- **PowerShell / VBA**

Recent Escalation: US Critical Infrastructure (March 2026)

In early February 2026, Broadcom/Symantec discovered MuddyWater pre-positioned inside a US bank, a US airport, US and Canadian NGOs, and the Israeli operation of a US defense/aerospace software company. The Dindoor and FakeSet backdoors were deployed prior to Operation Epic Fury (February 28, 2026), indicating strategic pre-positioning aligned with anticipated Iran conflict escalation.

3 Tactics, Techniques & Procedures

INITIAL ACCESS

- `T1566.001` Spearphishing Attachment
- `T1566.002` Spearphishing Link
- `T1190` Exploit Public-Facing Application
- `T1204.001` Malicious Link
- `T1204.002` Malicious File

EXECUTION

- `T1059.001` PowerShell
- `T1059.003` Windows Command Shell
- `T1059.005` Visual Basic
- `T1059.006` Python
- `T1059.007` JavaScript NOVEL
- `T1047` WMI
- `T1203` Exploitation for Client Execution

PERSISTENCE

- `T1547.001` Registry Run Keys / Startup Folder
- `T1053.005` Scheduled Task
- `T1137.001` Office Template Macros
- `T1219` Remote Access Tools

DEFENSE EVASION

- `T1027.003` Steganography
- `T1027.004` Compile After Delivery
- `T1027.010` Command Obfuscation
- `T1036.005` Match Legitimate Name/Location
- `T1140` Deobfuscate/Decode Files
- `T1218.005` Mshta
- `T1218.011` Rundll32
- `T1574.001` DLL Search Order Hijacking
- `T1562.001` Disable or Modify Tools

DISCOVERY

- `T1016` System Network Config Discovery
- `T1033` System Owner/User Discovery
- `T1049` System Network Connections
- `T1057` Process Discovery
- `T1082` System Information Discovery
- `T1083` File and Directory Discovery
- `T1518.001` Security Software Discovery

CREDENTIAL ACCESS

- `T1003.001` LSASS Memory
- `T1003.004` LSA Secrets
- `T1552.001` Credentials In Files
- `T1555.003` Credentials from Web Browsers

COMMAND & CONTROL

- `T1071.001` Web Protocols
- `T1102.002` Bidirectional Communication
- `T1104` Multi-Stage Channels
- `T1105` Ingress Tool Transfer
- `T1132.001` Standard Encoding
- `T1573.001` Symmetric Cryptography
- `T1583.006` Web Services

EXFILTRATION

- `T1041` Exfiltration Over C2 Channel
- `T1560.001` Archive via Utility
- `T1074.001` Local Data Staging

C2 Framework Evolution

MuddyWater has developed and deployed at least five custom C2 frameworks, each transition typically forced by public exposure or source code leaks: **MuddyC3** (Python2) → **SimpleHarm** → **PhonyC2** (Python3, 2021+) → **MuddyC2Go** (Golang, 2020+) → **DarkBeatC2** (2024). In 2026, the group also adopted Telegram bot-based C2 (CHAR backdoor, Operation Olalampo).

Tooling Sophistication Trajectory

PowerShell scripts (2017) → Macro-enabled documents (2018+) → Legitimate RMM tool abuse (2021+) → Custom C implants / BugSleep (2024) → Rust-based implants / RustyWater (2026) → Deno runtime / Dindoor (2026). This progression demonstrates a clear pattern of adopting newer, less-detected runtime environments to evade security controls.

4 Tooling & Infrastructure

Custom Malware Arsenal

Tool	Type	Description	First Seen
Dindoor	Backdoor (Deno/JS)	JavaScript/TypeScript backdoor running on the Deno runtime. Executes commands on compromised systems; C2 over HTTPS. Signed with certificate issued to "Amy Cherne."	Feb 2026
FakeSet	Backdoor (Python)	Python-based backdoor downloaded from Backblaze cloud storage. Signed with certificates issued to "Amy Cherne" and "Donald Gay" (latter linked to Stagecomp/Darkcomp).	Feb 2026
RustyWater / Archer RAT	RAT (Rust)	Rust-based implant using async networking (reqwest, tokio). Process injection into explorer.exe; persistence via Registry Run key (CertificationKit.ini). XOR-encrypted strings; JSON/Base64/XOR C2 protocol.	Jan 2026
CHAR	Backdoor (Rust)	Rust backdoor controlled via Telegram bot C2 ("stager_51_bot"). Supports directory navigation and command execution. Shows signs of AI-assisted development (emojis in debug strings).	Jan 2026
GhostFetch	Downloader	First-stage downloader that loads additional malware directly into memory. Part of Operation Olalampo.	Jan 2026
GhostBackDoor	Backdoor	Advanced backdoor deployed via Operation Olalampo. Full capabilities not publicly detailed.	Jan 2026
HTTP_VIP	Downloader	System reconnaissance and native downloader. Authenticates with external server; deploys AnyDesk from C2.	Jan 2026
MuddyViper	Backdoor	Collects system info, executes commands, transfers files, exfiltrates Windows credentials and browser data. Loaded by Fooder (Snake game disguise). CNG cryptographic API adoption.	Sep 2024
UDPGangster	Backdoor (C/C++)	UDP-based C2 on port 1269. Supports heartbeat, cmd.exe execution, file exfiltration, payload deployment, and C2 updates. Extensive anti-analysis (debugger/VM detection).	Nov 2025
BugSleep / MuddyRot	Backdoor (C, x64)	Reverse shell, file upload/download, persistence. C2 over raw TCP port 443. String obfuscation (subtract 3 per byte mod 256). Deployed via phishing with Egnyte-hosted payloads.	May 2024
POWERSTATS / Powermud	Backdoor (PowerShell)	Signature first-stage implant. Credential theft, C2 communication, data collection. Used from 2017 onward.	2017
PowGoop	DLL Loader	Disguises as Google Update (goopdate.dll). Decrypts and runs PowerShell downloader; beacon communicates with C2 for additional payloads.	Pre-2022
Small Sieve	Backdoor (Python)	Persistence and foothold expansion; Telegram Bot API for C2 over HTTPS; custom string and traffic obfuscation.	Pre-2022
Canopy / Starwhale	Spyware (VBA/WSF)	Collects system info (username, computer name, IP). Distributed via spearphishing with Office documents.	Pre-2022
Mori	Backdoor	Uses DNS tunneling for C2 and data exfiltration.	Pre-2022
GRAMDOOR	Backdoor	Telegram Bot API for C2 communication; sends and receives messages via actor-created Telegram chat room.	Late 2021
DarkBit	Ransomware (Go)	AES symmetric encryption with RSA-encrypted key. Used as cover persona for Technion attack. Ransomware was subsequently cracked, allowing free data recovery.	Feb 2023

Legitimate Tools Abused

Tool	Type	Context	Source
Atera Agent	RMM	Primary RMM tool (late 2023 through 2024). No attacker infrastructure required; Atera handles all C2.	HarfangLab; Multiple vendors
ScreenConnect	RMM	Earlier RMM tool in rotation for initial access and persistence.	CISA AA22-055A
SimpleHelp	RMM	Used for persistence on victim devices.	CSO Online
Syncro / RemoteUtilities / Level / PDQ	RMM	Various RMM tools rotated through for LOTL access (2021-2025).	ESET; HarfangLab
AnyDesk	Remote Access	Deployed by HTTP_VIP downloader in Operation Olalampo (Jan 2026).	Group-IB (Feb 2026)
Rclone	File Sync	Used to exfiltrate data to Wasabi cloud storage (Feb 2026 US campaign).	Broadcom/Symantec (Mar 2026)
LIGOLO	Tunneling	Used for lateral movement and tunneling.	Mandiant (Feb 2022)
CrackMapExec	Post-exploitation	Network enumeration and lateral movement.	Mandiant (Feb 2022)

Infrastructure Patterns

Category	Details	Source
C2 Frameworks	Five custom C2 frameworks documented: MuddyC3 (Python2, deprecated), SimpleHarm (deprecated), PhonyC2 (Python3, deprecated after leak), MuddyC2Go (Golang), DarkBeatC2 (2024+).	Deep Instinct (multiple reports)
Payload Hosting	Egnyte file-sharing platform (RMM installers, BugSleep payloads), Backblaze (FakeSet delivery), OneHub, Mega.	HarfangLab; Check Point; Broadcom
Data Exfiltration	Wasabi cloud storage (via Rclone), Telegram Bot API, DNS tunneling (Mori backdoor).	Broadcom; CISA AA22-055A
Code Signing	Certificates issued to "Amy Cherne" (Dindoor, FakeSet) and "Donald Gay" (FakeSet, Stagecomp, Darkcomp). The "Donald Gay" certificate provides the strongest attribution link between the Feb 2026 US campaign and MuddyWater.	Broadcom/Symantec (Mar 2026)
Infrastructure Reuse	IP subnet 91.121.240.x reused across SimpleHarm, PhonyC2, and DarkBeatC2 campaigns (91.121.240.104, 91.121.240.102). Stark Industries hosting (185.236.234.161) used for DarkBeatC2.	Deep Instinct (Apr 2024)

5 Notable Campaigns

First Attributed Campaigns

Feb – Oct 2017

Middle East · Government · POWERSTATS

First publicly attributed MuddyWater campaigns. Spear-phishing with malicious documents deploying the POWERSTATS PowerShell backdoor against government and private sector organizations across the Middle East. Unit 42 published the first public analysis naming the group "MuddyWater" on November 14, 2017.

CISA Advisory / USCYBERCOM Attribution

Jan – Feb 2022

Global · Government · MOIS Attribution

US Cyber Command officially linked MuddyWater to MOIS on January 12, 2022, uploading 12+ malware samples to VirusTotal. On February 24, the FBI, CISA, CNMF, and NCSC-UK published joint advisory AA22-055A, the most comprehensive government assessment to date. Documented malware variants included PowGoop, Small Sieve, Canopy/Starwhale, Mori, and POWERSTATS. Mandiant separately tracked the UNC3313 cluster, linked to MuddyWater with moderate confidence, using GRAMDOOR and STARWHALE backdoors with Telegram bot C2.

Technion / DarkBit Ransomware

Feb 2023

Israel · Education · Destructive

Ransomware attack against the Technion, Israel Institute of Technology, using the DarkBit persona. Demanded 80 BTC ($1.7M). MuddyWater provided initial access using PhonyC2, while Storm-1084 (DEV-1084) executed destructive operations. Microsoft later documented this partnership, revealing destruction of on-premises servers, VMs, storage accounts, and Azure cloud environments. This was the first confirmed MuddyWater destructive operation using a false persona to mask state-sponsored sabotage. Israel's National Cyber Directorate attributed the attack to MuddyWater.

PhonyC2 / MuddyC2Go Campaigns

2022 – 2023

Israel · Log4j · PaperCut

MuddyWater exploited Log4j (CVE-2021-44228) in Israeli SysAid applications and PaperCut vulnerabilities (CVE-2023-27350, CVE-2023-27351) using the PhonyC2 framework. Deep Instinct publicly exposed PhonyC2 in June 2023, leading to a source code leak that forced the group to transition to MuddyC2Go (Golang-based). MuddyC2Go was identified in attacks against Israel in November 2023.

BugSleep / MuddyRot Campaigns

May – Jul 2024

Turkey · Azerbaijan · Israel · Saudi Arabia

Deployment of BugSleep (also called MuddyRot), a custom x64 C-language implant replacing reliance on legitimate RMM tools. Check Point Research identified 50+ spear-phishing emails targeting 10+ sectors in Turkey, Azerbaijan, Jordan, Saudi Arabia, Israel, and Portugal. Payloads were disguised as webinar/course invitations and hosted on Egnyte. The backdoor communicates over raw TCP port 443 with byte-subtraction obfuscation.

DarkBeatC2 Campaigns

Feb – Apr 2024

Israel · Middle East · Atera Agent

Deep Instinct identified DarkBeatC2 as MuddyWater's fifth known C2 framework. Infrastructure included IPs 91.121.240.102, 137.74.131.19, 164.132.237.68, and 185.236.234.161 (Stark Industries hosting), along with domains googlelinks[.]net, googlevalues[.]com, and websiteapicloud[.]com. The framework managed PowerShell-based communication and delivered Atera Agent installers via Egnyte.

MuddyViper Campaign

Sep 2024 – Mar 2025

Israel · Egypt · Technology · Manufacturing

ESET documented a campaign targeting Israeli organizations (technology, engineering, manufacturing, local government, education) and one target in Egypt. The group deployed MuddyViper backdoor via the Fooder loader, which disguised itself as a Snake game and used custom delay functions to evade automated analysis. Additional tools included CE-Notes and LP-Notes credential stealers and go-socks5 reverse tunneling.

Operation Olalampo

Jan 2026

MENA · Telegram C2 · AI-Assisted Dev

Group-IB documented a multi-pronged campaign deploying four new malware families: GhostFetch (first-stage downloader), CHAR (Rust backdoor with Telegram bot C2 "stager_51_bot"), HTTP_VIP (native downloader deploying AnyDesk), and GhostBackDoor. Targeting spanned the MENA region. Notably, the CHAR backdoor contained debug strings with emojis, a trait rarely seen in human-authored code, suggesting AI-assisted development.

RustyWater RAT Campaign

Jan 2026

Middle East · Diplomatic · Maritime · Rust-Based

CloudSEK identified RustyWater (also called Archer RAT / RUSTRIC), MuddyWater's first documented Rust-based implant, targeting diplomatic, maritime, financial, and telecom entities in the Middle East. Spear-phishing emails impersonated TMCell (Turkmenistan mobile operator) with "Cybersecurity Guidelines" subject lines. The RAT featured async networking via Rust crates (reqwest, tokio), process injection into explorer.exe, and persistence through a Registry Run key pointing to CertificationKit.ini.

Dindoor / FakeSet: US Critical Infrastructure

Feb – Mar 2026

United States · Financial · Aviation · Defense Supply Chain

Broadcom/Symantec discovered MuddyWater pre-positioned inside a US bank, a US airport, US and Canadian NGOs, and the Israeli operation of a US defense/aerospace software company. Two new backdoors were deployed: **Dindoor** (Deno runtime, JavaScript/TypeScript) and **FakeSet** (Python, downloaded from Backblaze). Both were signed with certificates issued to "Amy Cherne"; FakeSet was also signed with a "Donald Gay" certificate previously linked to Stagecomp and Darkcomp (confirmed MuddyWater tools by Google, Microsoft, and Kaspersky).

Rclone was used to exfiltrate data from the defense software company to Wasabi cloud storage. The campaign was active from early February 2026, pre-dating Operation Epic Fury (February 28, 2026), indicating strategic pre-positioning aligned with anticipated military operations.

Ongoing Threat

As of March 11, 2026, MuddyWater remains active on compromised US networks. Activity on these networks increased following Operation Epic Fury. Pre-positioned access in financial, aviation, and defense supply chain networks represents an ongoing threat to US critical infrastructure.

6 Detection & Response Recommendations

Detection Opportunities

RMM Tool Abuse

- Monitor for unauthorized installations of Atera Agent, ScreenConnect, SimpleHelp, Syncro, AnyDesk, and Level
- Alert on RMM agent installations outside of approved change windows
- Detect RMM processes launched by Office applications or scripting engines
- Track Egnyte, Backblaze, and OneHub downloads of executable content

PowerShell / Scripting Anomalies

- Heavily obfuscated PowerShell with Base64 encoding and string concatenation (POWERSTATS signature)
- PowerShell scripts downloading from cloud storage services
- WMI-based persistence creation via PowerShell
- Mshta.exe or Rundll32.exe executing scripted payloads

C2 Indicators

- DNS tunneling activity (Mori backdoor)
- Non-Telegram-client processes connecting to api.telegram.org
- Deno runtime (deno.exe) process execution in enterprise environments
- Outbound UDP traffic on port 1269 (UDPGangster)
- Raw TCP connections on port 443 that are not TLS (BugSleep)

File System Artifacts

- `goopdate.dll` in Google Update directories (PowGoop)
- `CertificationKit.ini` in C:\ProgramData (RustyWater)
- `SystemProc.exe` in %AppData%\RoamingLow (UDPGangster)
- Mutex: xhxhxhxhxhxpp (UDPGangster)
- Rclone binary with Wasabi storage configuration

Sample Detection Queries

RMM Tool Abuse Detection (KQL)

DETECTION ONLY

```
// Detect unauthorized RMM tool installations commonly abused by MuddyWater
DeviceProcessEvents
| where FileName in~ (
    "AteraAgent.exe", "ScreenConnect.ClientService.exe",
    "SimpleHelp.exe", "Syncro.Overmind.Service.exe",
    "AnyDesk.exe", "level-windows-amd64.exe",
    "PDQConnect.Agent.exe", "rutserv.exe"
)
| where InitiatingProcessFileName !in~ ("msiexec.exe", "sccm.exe")
| project Timestamp, DeviceName, FileName, FolderPath,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

Tuning Required

This query will generate false positives in environments that legitimately use these RMM tools. Exclude known-approved RMM deployments by adding your organization's sanctioned tools to an exclusion list. Do NOT deploy as an automated blocking rule.

Known MuddyWater C2 Hash Detection (KQL)

BLOCKING SAFE

```
let MuddyWaterHashes = dynamic([
    "12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa",
    "dd7ee54b12a55bcc67da4ceaed6e636b7bd30d4db6f6c594e9510e1e605ade92",
    "94278fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7130c472",
    "b8703744744555ad841f922995cef5dbca11da22565195d05529f5f9095fbfca",
    "7ea4b307e84c8b32c0220eca13155a4cf66617241f96b8af26ce2db8115e3d53",
    "76aad2a7fa265778520398411324522c57bfd7d2ff30a5cfe6460960491bc552",
    "f38a56b8dc0e8a581999621eef65ef497f0ac0d35e953bd94335926f00e9464f",
    "9b5e36bb7518a9e333c31d09b589102f89e3425571dd434820ab3c437dc4e0d9",
    "b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c",
    "42ca7d3fcd6d220cd380f34f9aa728b3bb68908b49f04d04f685631ee1f78986"
]);
DeviceFileEvents
| where SHA256 in (MuddyWaterHashes)
| project Timestamp, DeviceName, FileName, SHA256, FolderPath
```

Suspicious PowerShell Patterns (POWERSTATS-style) (KQL)

INVESTIGATION AID

```
// Detect heavily obfuscated PowerShell execution typical of POWERSTATS
DeviceProcessEvents
| where FileName =~ "powershell.exe"
| where ProcessCommandLine has_any (
    "FromBase64String", "IEX", "Invoke-Expression",
    "downloadstring", "Net.WebClient",
    "[System.Convert]::", "Reflection.Assembly"
)
| where ProcessCommandLine matches regex @"(\-[eE][nN][cC]\s|[A-Za-z0-9+/=]{100,})"
| project Timestamp, DeviceName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

Investigation Aid

This query targets broad PowerShell obfuscation patterns used by MuddyWater's POWERSTATS and related tools. It will match legitimate administrative scripts that use Base64 encoding. Designed for manual threat hunting, not production deployment.

PDF-to-RMM-Installer Phishing Chain (KQL)

DETECTION ONLY

```
// Detect PDF documents leading to RMM installer downloads
// Matches MuddyWater's TA450 phishing delivery chain
DeviceFileEvents
| where Timestamp > ago(30d)
| where FileName endswith ".pdf"
| join kind=inner (
    DeviceNetworkEvents
    | where Timestamp > ago(30d)
    | where RemoteUrl has_any ("egnyte.com", "backblaze", "onehub.com", "mega.nz")
    | project NetworkTimestamp=Timestamp, DeviceId, RemoteUrl
) on DeviceId
| where datetime_diff('minute', NetworkTimestamp, Timestamp) between (0 .. 10)
| project Timestamp, DeviceName, FileName, RemoteUrl, NetworkTimestamp
| sort by Timestamp desc
```

A Appendix A: Indicators of Compromise

Blocking Guidance: 3-Tier IOC Classification

Tier 1: Block (High Confidence)

Dedicated C2 IPs (91.121.240.104, 91.121.240.102, 137.74.131.19, 164.132.237.68, 185.236.234.161, 157.20.182.75): Confirmed as dedicated MuddyWater C2 infrastructure by Microsoft, Deep Instinct, and FortiGuard. Safe to add to Conditional Access block lists or firewall deny rules. *Caveat: Hosting providers may reassign IPs over time. Reassess periodically.*

Known C2 domains (googlelinks[.]net, googlevalues[.]com, websiteapicloud[.]com, nomercys[.]it[.]com): Confirmed MuddyWater infrastructure. Safe for DNS-level blocking.

All malware SHA256 hashes listed below: Confirmed malicious with no legitimate use case. Safe for hash-based blocking and EDR prevention policies.

Tier 2: Alert / Monitor (Shared Infrastructure)

RustyWater C2 IPs (159.198.66.153, 159.198.68.25, 161.35.228.250): These IPs may be hosted on shared cloud infrastructure. Deploy as detection/alerting queries only. Require analyst review before blocking. Verify current hosting assignment before action.

Cloud storage platforms (Egnyte, Backblaze, Wasabi): These are legitimate cloud services used by MuddyWater for payload hosting and data exfiltration. Block specific known-malicious URLs only; do not block entire domains, as this will disrupt legitimate business operations.

Telegram API (api.telegram.org): Used by Small Sieve, GRAMDOOR, and CHAR for C2. Blocking Telegram API will disrupt legitimate Telegram usage. Monitor for non-Telegram-client processes connecting to this endpoint.

Tier 3: Investigate (Unconfirmed)

Residential ISP IPs: Any residential ISP IPs observed in connection with MuddyWater campaigns may represent the threat actor's true origin, a compromised residential device acting as a proxy, or a legitimate user. Do not block without verifying against known employee/partner IP addresses.

Dindoor and FakeSet hashes: Specific SHA256 hashes for these backdoors were not published in open-source secondary reporting. They are available in the Broadcom/Symantec threat intelligence portal. [REQUIRES VERIFICATION: access Broadcom portal directly for full IOC set.]

File Indicators (SHA256)

Indicator	Context	Source	Confidence
`12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa`	PowGoop DLL loader (goopdate.dll)	CISA AA22-055A (Feb 2022)	High
`dd7ee54b12a55bcc67da4ceaed6e636b7bd30d4db6f6c594e9510e1e605ade92`	PowGoop component (vcruntime140.dll)	CISA AA22-055A (Feb 2022)	High
`94278fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7130c472`	BugSleep/MuddyRot backdoor	PolySwarm / Check Point (Jul 2024)	High
`b8703744744555ad841f922995cef5dbca11da22565195d05529f5f9095fbfca`	BugSleep/MuddyRot backdoor	PolySwarm / Sekoia (2024)	High
`7ea4b307e84c8b32c0220eca13155a4cf66617241f96b8af26ce2db8115e3d53`	UDPGangster backdoor	FortiGuard Labs (Dec 2025)	High
`b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c`	UDPGangster backdoor (related)	FortiGuard Labs / PolySwarm (Dec 2025)	High
`42ca7d3fcd6d220cd380f34f9aa728b3bb68908b49f04d04f685631ee1f78986`	UDPGangster backdoor (related)	FortiGuard Labs / PolySwarm (Dec 2025)	High
`76aad2a7fa265778520398411324522c57bfd7d2ff30a5cfe6460960491bc552`	RustyWater/Archer RAT (Rust implant)	CloudSEK (Jan 2026)	High
`f38a56b8dc0e8a581999621eef65ef497f0ac0d35e953bd94335926f00e9464f`	RustyWater/Archer RAT (Rust implant)	CloudSEK (Jan 2026)	High
`9b5e36bb7518a9e333c31d09b589102f89e3425571dd434820ab3c437dc4e0d9`	POWERSTATS backdoor	Unit 42 / multiple vendors	High

Network Indicators (C2 IPs)

Indicator	Type	Context	Source	Confidence
`91.121.240.104`	IPv4	PhonyC2 C2 server; Log4j/SysAid exploitation	Microsoft; Deep Instinct (Jun 2023)	High
`91.121.240.102`	IPv4	DarkBeatC2 infrastructure; googlelinks[.]net	Deep Instinct (Apr 2024)	High
`137.74.131.19`	IPv4	DarkBeatC2 infrastructure; googlevalues[.]com	Deep Instinct (Apr 2024)	High
`164.132.237.68`	IPv4	DarkBeatC2 infrastructure	Deep Instinct (Apr 2024)	High
`185.236.234.161`	IPv4	DarkBeatC2; Stark Industries hosting	Deep Instinct (Apr 2024)	High
`157.20.182.75`	IPv4	UDPGangster C2 server (UDP port 1269)	FortiGuard Labs (Dec 2025)	High
`159.198.66.153`	IPv4	RustyWater C2; nomercys[.]it[.]com	CloudSEK (Jan 2026)	High
`159.198.68.25`	IPv4	RustyWater C2 infrastructure	CloudSEK (Jan 2026)	High
`161.35.228.250`	IPv4	RustyWater C2 infrastructure	CloudSEK (Jan 2026)	High

IPs 91.121.240.x and 137.74.131.x are OVH-hosted dedicated servers confirmed as MuddyWater infrastructure by Deep Instinct and Microsoft. IP 185.236.234.161 is hosted by Stark Industries, a provider with documented associations with malicious hosting. IPs 159.198.x.x and 161.35.228.250 may be on shared hosting infrastructure; verify current assignment before maintaining in block lists.

C2 Domains

Indicator	Type	Context	Source	Confidence
`googlelinks[.]net`	Domain	DarkBeatC2; pointed to 91.121.240.102 (Feb 2024)	Deep Instinct (Apr 2024)	High
`googlevalues[.]com`	Domain	DarkBeatC2; pointed to 137.74.131.19 (Feb 2024)	Deep Instinct (Apr 2024)	High
`websiteapicloud[.]com`	Domain	DarkBeatC2 infrastructure	Deep Instinct (Apr 2024)	High
`nomercys[.]it[.]com`	Domain	RustyWater RAT C2 domain	CloudSEK (Jan 2026)	High

C2 Infrastructure (Telegram Bot)

Indicator	Type	Context	Source	Confidence
`stager_51_bot`	Telegram Bot Username	CHAR backdoor C2 (Operation Olalampo, Jan 2026); bot first name: "Olalampo"	Group-IB (Feb 2026)	High

File System Artifacts

Indicator	Type	Context	Source	Confidence
`C:\Users\Public\ui.txt`	File Path	UDPGangster dropper writes decoded payload here	FortiGuard Labs (Dec 2025)	High
`%AppData%\RoamingLow\SystemProc.exe`	File Path	UDPGangster persistence location	FortiGuard Labs (Dec 2025)	High
`C:\ProgramData\CertificationKit.ini`	File Path	RustyWater implant (Rust PE masquerading as reddit.exe)	CloudSEK (Jan 2026)	High
`xhxhxhxhxhxpp`	Mutex	UDPGangster mutex (shared across Turkey, Israel, Azerbaijan samples)	FortiGuard Labs (Dec 2025)	High
`C:\Users\gangster\source\repos\udp_3.0 - Copy - Copy\x64\release_86\udp_3.0.pdb`	PDB Path	UDPGangster debug path (reveals developer username "gangster")	FortiGuard Labs (Dec 2025)	High

Code Signing Certificates

Issued To	Context	Source	Confidence
`Amy Cherne`	Used to sign Dindoor and FakeSet backdoors (Feb 2026)	Broadcom/Symantec (Mar 2026)	High
`Donald Gay`	Used to sign FakeSet (2026); previously signed Stagecomp and Darkcomp (confirmed MuddyWater tools by Google, Microsoft, and Kaspersky). Strongest attribution link for US campaign.	Broadcom/Symantec; Google; Microsoft; Kaspersky	High

B Appendix B: References

Government Advisories

[1] **CISA** - "Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks" (Advisory AA22-055A, February 2022)
cisa.gov

[2] **CISA** - Malware Analysis Report MAR-10369127-1.v1, "MuddyWater" (February 2022)
cisa.gov

[3] **USCYBERCOM** - Public Attribution: MuddyWater linked to Iran MOIS (January 12, 2022)
x.com/cnmf_cyberalert

[4] **Israel National Cyber Directorate** - "Iranian Government-Sponsored Threat Actor MuddyWater Conducts Cyber Attack Against Israel" (February 2023)
gov.il

[5] **MITRE ATT&CK** - Group G0069: MuddyWater
attack.mitre.org

Vendor Threat Intelligence (Primary)

[6] **Broadcom / Symantec** - "Seedworm: Iranian APT on Networks of U.S. Bank, Airport, Software Company" (March 5, 2026)
security.com

[7] **Deep Instinct** - "PhonyC2: Revealing a New Malicious Command & Control Framework by MuddyWater" (June 2023)
deepinstinct.com

[8] **Deep Instinct** - "MuddyC2Go: Latest C2 Framework Used by Iranian APT MuddyWater Spotted in Israel" (November 2023)
deepinstinct.com

[9] **Deep Instinct** - "DarkBeatC2: The Latest MuddyWater Attack Framework" (April 2024)
deepinstinct.com

[10] **Check Point Research** - "New BugSleep Backdoor Deployed in Recent MuddyWater Campaigns" (July 2024)
research.checkpoint.com

[11] **Sekoia** - "MuddyWater replaces Atera by custom MuddyRot implant in a recent campaign" (2024)
blog.sekoia.io

[12] **ESET** - "MuddyWater: Snakes by the riverbank" (December 2, 2025)
welivesecurity.com

[13] **Group-IB** - "Operation Olalampo: Inside MuddyWater's Latest Campaign" (February 2026)
group-ib.com

[14] **CloudSEK** - "Reborn in Rust: Muddy Water Evolves Tooling with RustyWater Implant" (January 2026)
cloudsek.com

[15] **FortiGuard Labs** - "UDPGangster Campaigns Target Multiple Countries" (December 2025)
fortinet.com

[16] **Microsoft** - "MERCURY and DEV-1084: Destructive attack on hybrid environment" (April 7, 2023)
microsoft.com

[17] **Mandiant / Google Cloud** - "Left On Read: Telegram Malware Spotted in Latest Iranian Cyber Espionage Activity" (February 2022)
cloud.google.com

[18] **HarfangLab** - "MuddyWater campaign abusing Atera Agents" (2024)
harfanglab.io

[19] **Proofpoint** - "TA450 Uses Scam Emails with PDF Attachments to Phish" (March 2024)
proofpoint.com

[20] **Palo Alto Unit 42** - "Muddying the Water: Targeted Attacks in the Middle East" (November 14, 2017)
unit42.paloaltonetworks.com

Investigative Journalism

[21] **The Register** - "Iran intelligence backdoored US bank, airport networks" (March 5, 2026)
theregister.com

[22] **Cybersecurity Dive** - "State-linked actors targeted US networks in lead-up to Iran war" (March 2026)
cybersecuritydive.com

OSINT & Analyst Research

[23] **PolySwarm** - "MuddyWater's UDPGangster Backdoor"
blog.polyswarm.io

[24] **PolySwarm** - "MuddyWater Using New Backdoor to Target Middle East"
blog.polyswarm.io

[25] **Deep Instinct GitHub** - PhonyC2-MuddyWater-Research
github.com

[26] **Huntress** - "Unmasking an Attack Chain of MuddyWater"
huntress.com

Secondary Sources

[27] **The Hacker News** - "Iran-Linked MuddyWater Hackers Target U.S. Networks With New Dindoor Backdoor" (March 2026)
thehackernews.com

[28] **Infosecurity Magazine** - "Iran's MuddyWater Hackers Hit US Firms with New Dindoor Backdoor" (March 2026)
infosecurity-magazine.com

[29] **Help Net Security** - "Iran-linked APT targets US critical sectors with new backdoors" (March 6, 2026)
helpnetsecurity.com

[30] **SOCRadar** - "Iranian APT MuddyWater Uses Dindoor Malware to Target U.S. Networks" (March 2026)
socradar.io

[31] **Dark Reading** - "Iran's 'MuddyWater' Levels Up With MuddyViper Backdoor" (December 2025)
darkreading.com

[32] **BleepingComputer** - "US links MuddyWater hacking group to Iranian intelligence agency" (January 2022)
bleepingcomputer.com

[33] **BleepingComputer** - "New BugSleep malware implant deployed in MuddyWater attacks" (July 2024)
bleepingcomputer.com

[34] **Picus Security** - "TTPs and Malware used by MuddyWater Cyber Espionage Group"
picussecurity.com

[35] **Secureworks** - "COBALT ULSTER" (Threat Profile)
secureworks.com

[36] **Malpedia** - "MuddyWater"
malpedia.caad.fkie.fraunhofer.de

[37] **The Record** - "Israel blames state-sponsored Iranian hackers for ransomware attack on university" (February 2023)
therecord.media

[38] **Flashpoint** - "Escalation in the Middle East: Tracking Operation Epic Fury" (March 2026)
flashpoint.io

[39] **SOCRadar** - "Iran vs. Israel & US Cyber War 2026: Operation Epic Fury Threat Intelligence" (March 2026)
socradar.io

[40] **AttackIQ** - "Defending Against Iranian Cyber Threats in the Wake of Operation Epic Fury" (March 5, 2026)
attackiq.com

[41] **Tenable** - "Cyber Retaliation: Analyzing Iranian Cyber Activity Following Operation Epic Fury" (March 2026)
tenable.com