Latest Cyber Threat Intelligence & Security Insights

Archived: 2026-04-29 02:11:53 UTC

MuddyWater (XTA-GTP2UWKVBL5CFID4), one of Iran's most persistently active and operationally significant state-linked cyber threat actors. This blog integrates live FalconFeeds IOC telemetry with campaign-level analysis, TTP profiling, and full MITRE ATT&CK v14 mapping to provide defenders with the most actionable intelligence picture available on this threat actor as of March 2026.

MuddyWater has undergone a substantial capability evolution over the past 24 months. What was once a noisy, script-heavy intrusion set known for commodity phishing and blunt PowerShell tooling has matured into a sophisticated multi-stage operation deploying memory-resident implants written in Rust (**RustyWater**), advanced custom backdoors (**MuddyViper**), and a hardened operational infrastructure designed to survive blue team tuning and infrastructure takedowns. FalconFeeds telemetry confirms MuddyWater activity indicators clustering tightly around key Iran–Israel and Iran–GCC escalation windows throughout 2024–2026.

Critical Assessment: MuddyWater is not merely a persistent nuisance actor. It functions as **Iran's initial-access broker of choice**, systematically harvesting credentials and network footholds across Israeli, GCC, and Western targets before handing off to higher-tier IRGC operators — including OilRig/APT34 clusters — for espionage and potentially destructive follow-on operations.

Actor Profile & Attribution

Identity & Affiliation

MuddyWater is tracked under multiple aliases across the industry:

Alias	Source Organisation
MuddyWater	FalconFeeds, Symantec, Microsoft
Mango Sandstorm	Microsoft Threat Intelligence
TEMP.Zagros	FireEye / Mandiant
Static Kitten	CrowdStrike
Seedworm	Symantec
TA450	Proofpoint
COBALT ULSTER	SecureWorks
MERCURY	Microsoft (legacy designation)

State Affiliation: MuddyWater is formally assessed by CISA, NCSC (UK), and multiple Western intelligence agencies as operating **under the direction of Iran's Ministry of Intelligence and Security (MOIS)**. This distinguishes MuddyWater from IRGC-aligned actors (APT33, APT34) which operate under separate command authority, though coordination and target sharing between these groups is extensively documented.

Active Since: 2017

Last Confirmed Activity: March 2026

FalconFeeds Profile: https://dash.falconfeeds.io/threat-actor/TA-DDA9B80C3E54FE14

Active Infrastructure Channels: Open Web

Targeting Profile

MuddyWater has established a broad and persistent targeting footprint spanning **40+ countries**. Primary affected nations include:

Tier 1 (Highest Targeting Intensity): Israel, Saudi Arabia, Turkey, Pakistan, Iran (domestic dissidents)

Tier 2 (Sustained Targeting): Albania, Azerbaijan, Bangladesh, Brazil, Bulgaria, Canada, China, Estonia, Finland, France, Germany, Ireland, Italy, Japan, Latvia, Lithuania, Moldova, Netherlands, Norway, Philippines, Poland, Portugal, Romania, Russia, Singapore, Slovakia, South Africa, Sweden, Taiwan, UK, USA, Uzbekistan

Primary Sectors Targeted:

- Government ministries and defence-adjacent entities
- Telecommunications providers (STC, Turkcell, Bezeq)
- Critical infrastructure (energy, aviation, maritime)
- Financial institutions
- Technology and engineering firms
- Education and research institutions

Geopolitical & Strategic Context

MuddyWater as an Iranian Cyber Weapon in the Iran–Israel Conflict

The Iran–Israel conflict has evolved significantly beyond kinetic exchanges of missiles and drones. MuddyWater has become **one of Tehran's most important and flexible cyber assets** in this confrontation, operating across the full spectrum of pre-conflict reconnaissance through active intrusion and potential pre-positioning for destructive operations.

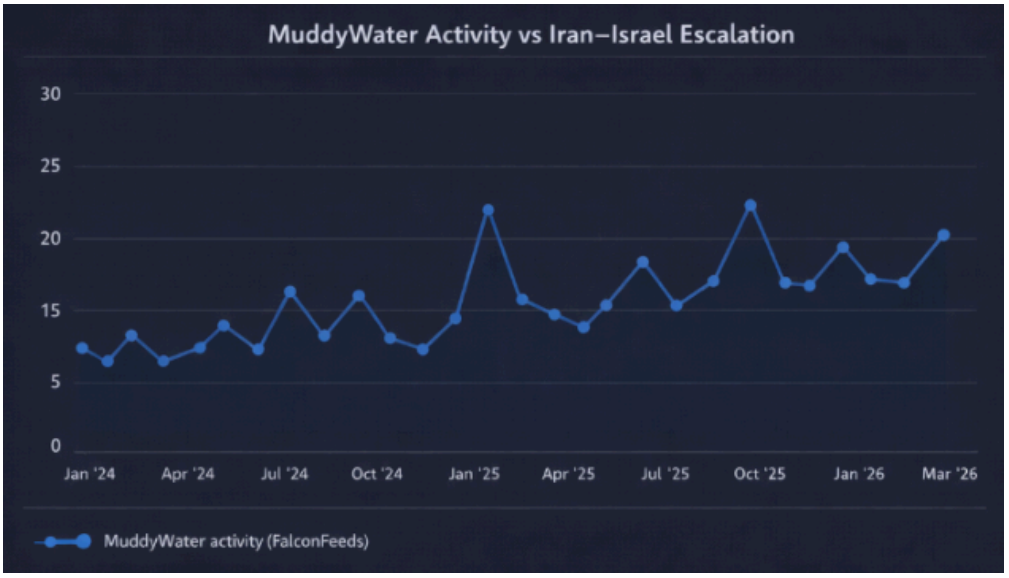
FalconFeeds telemetry spanning January 2024 through March 2026 demonstrates a consistent and statistically significant correlation: **MuddyWater IOC detection rates spike during periods of documented Iran–Israel kinetic or diplomatic escalation.**

Activity peaks were recorded in alignment with:

- The October 2023–April 2024 escalation following the Gaza conflict outbreak
- The April 2024 direct Iranian ballistic missile and drone strikes on Israeli territory
- The October 2024 Israeli strike on Iranian air defence systems
- The November 2024–January 2025 Houthi-Israel shipping conflict intensification

- The March 2026 Iran-Gulf escalation cycle (concurrent with Saudi Arabia IOC clusters)

This pattern is consistent with a **threat actor operating under strategic direction** — campaign tempo adjusts to geopolitical conditions, indicating MuddyWater's operations are coordinated with, or in direct support of, broader Iranian strategic objectives rather than being conducted opportunistically.



The Iran Cyber Ecosystem: MuddyWater's Position

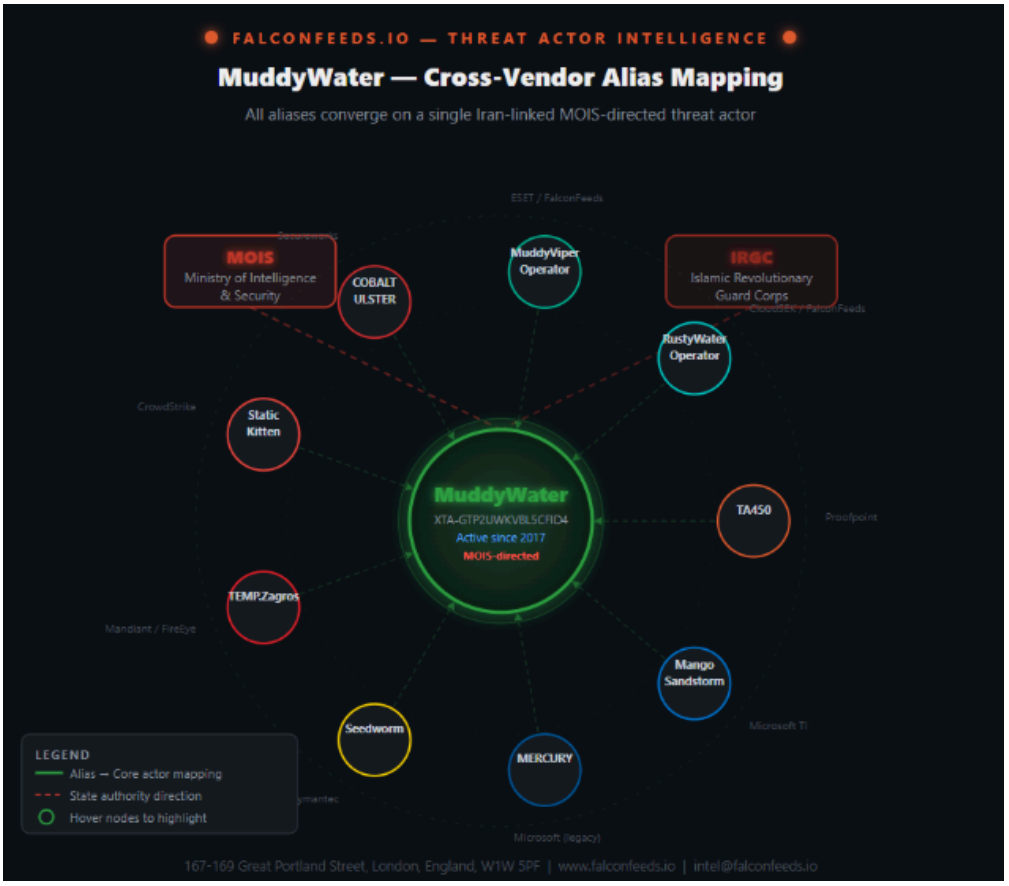
MuddyWater occupies a specific and critical node in Iran's layered cyber ecosystem:

MOIS Direction: MuddyWater receives tasking from Iran's Ministry of Intelligence and Security, the civilian intelligence agency. This contrasts with IRGC-directed actors (APT33 Elfin, APT34 OilRig) who operate under military-intelligence authority.

Initial Access Broker Function: MuddyWater systematically maps target networks, harvests credentials, and establishes persistent footholds. Access is then shared with or sold to other Iran-aligned operators.

Intelligence Sharing: Analysis confirms **target and intelligence sharing** between MuddyWater and the following groups:

- **OilRig / APT34** — receives high-quality network access from MuddyWater for espionage operations
- **Lyceum / HEXANE** — documented recipient of credentials and footholds from MuddyWater intrusions, particularly in Saudi and Israeli manufacturing targets
- **Agrius** — destructive actor that has operated within Israeli networks first accessed by MuddyWater
- **Charming Kitten / APT35** — shares targeting intelligence on Israeli academic and government targets
- **Tortoiseshell / Imperial Kitten** — coordinates on technology-sector targeting



Capability Evolution: From PowerShell to Rust

Historical TTP Baseline (2017–2023)

In its initial operational years, MuddyWater was characterised by **high operational tempo and low technical sophistication**. The hallmarks of this period included:

- Malicious Microsoft Office documents with embedded VBA macros delivered via spear-phishing
- Heavy reliance on PowerShell for initial execution, lateral movement, and persistence
- Use of legitimate Remote Monitoring and Management (RMM) tools (SimpleHelp, AnyDesk, Atera, Syncro) to blend with normal IT operations and avoid EDR detection
- POWERSTATS — a multi-stage PowerShell backdoor — as the primary implant, delivered via document macros
- Noisy brute-force credential access against VPN portals and Outlook Web Access (OWA) endpoints
- Short infrastructure rotation cycles using commodity VPS providers

The group's early-phase operations were characterised by their investigators as "blunt instrument" intrusions — effective due to volume and persistence rather than technical elegance.

Intermediate Phase: Hardened PowerShell & RMM Abuse (2022–2024)

Between 2022 and early 2024, MuddyWater upgraded its PowerShell-based tooling significantly:

- **Dynamic string encryption** implemented in PowerShell backdoors, replacing static strings that were trivially detected by AV signatures
- **Runtime code generation** — PowerShell payloads that generate and execute subsequent stage code at runtime, defeating static sandbox analysis
- **Cloud-hosted multi-stage payloads** — initial lure documents contact cloud storage (OneDrive, Dropbox, legitimate business file shares) to retrieve second-stage payloads, exploiting implicit trust in major cloud provider domains
- **Expanded RMM toolkit abuse** — documented use of SimpleHelp, ScreenConnect (ConnectWise), and Egnyte file-sharing platforms for C2 communication, blending into legitimate enterprise traffic
- **WMI Event Subscription persistence** — MuddyWater adopted WMI-based persistence mechanisms, creating event subscriptions that survive reboots without writing traditional autorun registry keys

FalconFeeds IOC telemetry from this period includes confirmed C2 endpoints using Egnyte-hosted relay infrastructure:

- kinneretacil.egnyte.com (IOC-TRQOWANS8RARX98Z) — Botnet C2
- fbcsoft.egnyte.com (IOC-C7T69ZSR5Z3ZRWKN) — Botnet C2
- cnsmportal.egnyte.com (IOC-8WU7DZ4GVCHUXF2Q) — Botnet C2
- instance-n3e3x9-relay.screenconnect.com (IOC-SXWUCGFTXPE5X3MO) — Botnet C2

The use of legitimate, enterprise-trusted cloud relay infrastructure represents a **significant defensive evasion advancement** — proxy-aware firewalls and web gateways that permit traffic to Egnyte or ConnectWise domains are effectively blind to this C2 channel.

Current Generation: Memory-Resident Implants (2024–2026)

MuddyWater's most recent capability generation represents a **step change in technical maturity** that brings the group's tradecraft closer to the standards of Tier-1 advanced persistent threat actors.

MuddyViper & Fooder (September 2024 – March 2025)

Between September 30, 2024 and March 18, 2025, ESET and FalconFeeds documented a major campaign wave targeting **Israeli critical infrastructure** across technology, engineering, manufacturing, local government, and education sectors, with confirmed victim impact in Egypt.

Fooder — The Loader: Fooder is a custom loader delivered as an innocuous-looking executable, frequently disguised as entertainment applications (e.g., Snake_Game.exe). Its primary function is to **reflectively load MuddyViper directly into process memory** without writing the payload to disk, defeating file-based detection and most EDR solutions that rely on on-disk signature scanning.

Key technical characteristics of Fooder:

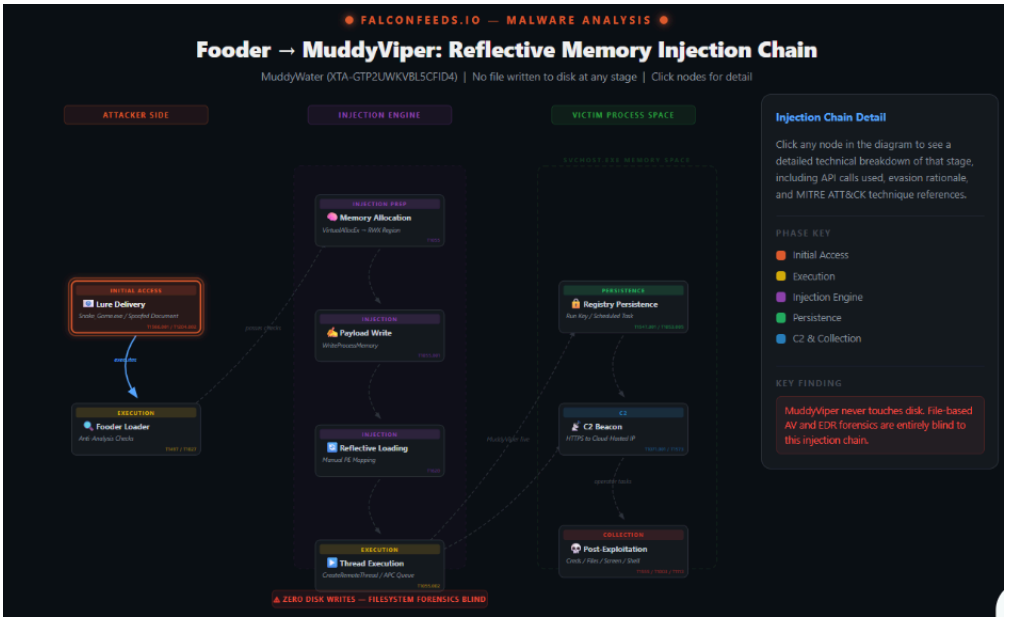
- Icon and metadata spoofing to impersonate legitimate Windows applications
- In-memory payload injection via reflective DLL loading techniques
- No disk-resident payload stage — the final implant never touches the filesystem in a detectable form

- Anti-analysis: checks for debugging environments and terminates if detected

MuddyViper — The Backdoor: MuddyViper is MuddyWater's most sophisticated implant to date as of the 2024–2025 campaign wave. Its capabilities include:

- Full system reconnaissance: hardware enumeration, OS version, running processes, network configuration
- Credential harvesting: browser-stored passwords, Windows Credential Manager, cached domain credentials
- Browser data exfiltration: cookies, browsing history, saved form data
- Arbitrary command execution via interactive shell
- File operations: upload, download, move, delete, compress
- Persistence maintenance via registry-based autostart mechanisms
- C2 communication over encrypted channels (HTTPS)

In at least one confirmed manufacturing-sector intrusion, MuddyWater deployed Fooder/MuddyViper alongside **a custom Mimikatz credential-harvesting loader**, with the harvested credentials subsequently used by **Lyceum** for deeper lateral movement into the victim network — directly confirming the initial-access broker dynamic.



RustyWater — Rust-Based RAT (2026)

In early 2026, CloudSEK, CSO Online, and FalconFeeds independently documented a new MuddyWater capability: **RustyWater**, a Remote Access Trojan written entirely in the **Rust programming language**.

The adoption of Rust represents a deliberate and significant capability investment by MuddyWater:

- **Rust's memory safety model** eliminates entire classes of memory corruption vulnerabilities that could expose operator infrastructure or destabilise the implant during operation
- **Rust binaries are significantly harder to reverse engineer** than equivalent C or C++ code — Rust's compilation model produces complex binary layouts that confound standard reverse engineering workflows
- **Rust's ecosystem produces smaller, self-contained binaries** with fewer detectable library dependencies

- **Rust is not commonly associated with malware** in AV/EDR training datasets, resulting in lower signature detection rates compared to equivalent C-based implants

Delivery Mechanism: RustyWater is delivered via targeted spear-phishing emails themed around:

- Cybersecurity advisories and threat alerts (luring security teams)
- Official government or regulatory notices
- Diplomatic correspondence and maritime/shipping operations
- Financial sector compliance requirements

Lure documents are either malicious Word files with embedded macros or icon-spoofed executables designed to appear as legitimate documents.

RustyWater Technical Profile:

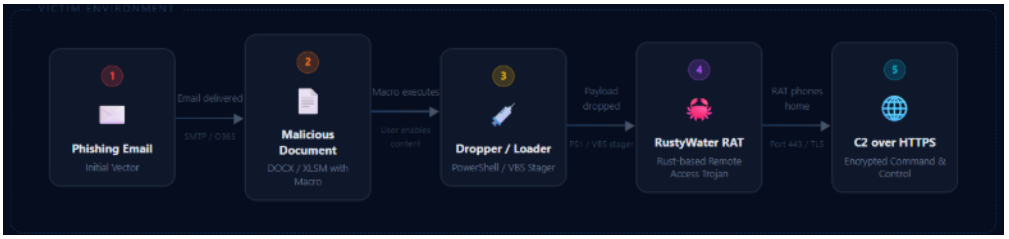
C2: Encrypted HTTPS-based communication with custom URI paths and headers to mimic legitimate web traffic

Persistence: Registry-based autostart entries (Run/RunOnce keys with system-mimicking names)

Anti-Analysis:

- Anti-debugging routines (checks for debugger presence via API timing and exception handling)
- Anti-VM checks (CPUID enumeration, registry key checks, hardware fingerprinting)
- Position-independent XOR string encryption (strings are decrypted at runtime, not stored in plaintext)
- Randomised sleep intervals between C2 callbacks (defeating sandbox timeout-based detection)

Post-Compromise Capabilities: Modular architecture allowing dynamic capability extension based on target environment



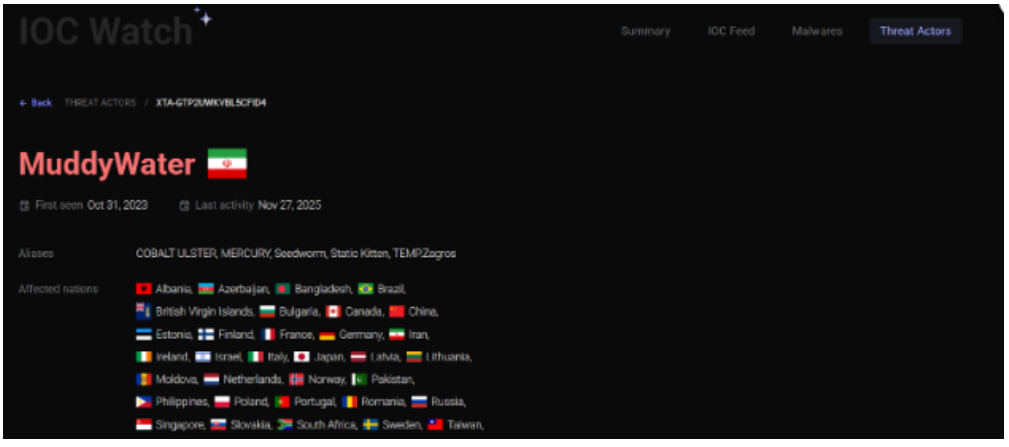
Live IOC Intelligence — FalconFeeds Telemetry

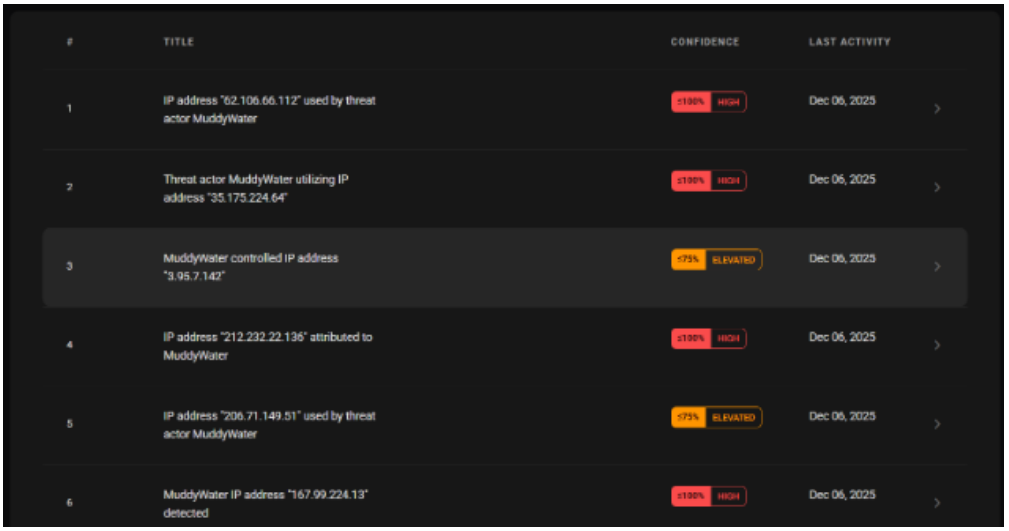
All indicators below are sourced from the FalconFeeds platform and attributed to MuddyWater (XTA-GTP2UWKVBL5CFID4).

High-Confidence IP Indicators (100% Confidence)

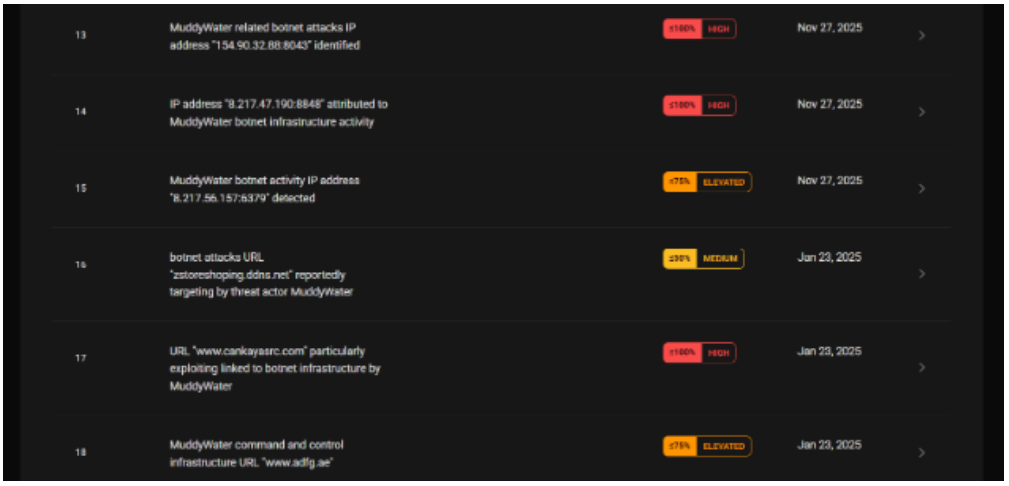
IP Address	IOC ID	Threat Type	Confidence	Notes
62.106.66.112	IOC-R4YKPY797H1ZXKHS	—	HIGH	Recent MuddyWater attributed IP
35.175.224.64	IOC-WRD2XBEH3OAHEMMY	—	HIGH	AWS-hosted; recent attribution
212.232.22.136	IOC-DNKXNSI2DBWU8HG4	—	HIGH	Attributed to MuddyWater
167.99.224.13	IOC-OIIPZNOXN3XENPCE	—	HIGH	DigitalOcean VPS
89.163.252.232	IOC-A0YY1UNL3IRN2CSY	Botnet C2	HIGH	Confirmed C2 node
87.236.212.22	IOC-28DNTB6UIFI01ZAK	Botnet C2	HIGH	Active C2 infrastructure
83.171.238.62	IOC-KYUIUZTMD6WZ49SG	Botnet C2	HIGH	Confirmed botnet relay
46.4.105.116	IOC-GUKP8CNXAYDY37B4	Botnet C2	HIGH	Hetzner-hosted node
46.166.176.242	IOC-10SYUNJ2HYEI2PQT	Botnet C2	HIGH	Confirmed relay
45.67.230.91	IOC-N36POOS342UO2H8E	Botnet C2	HIGH	Active MuddyWater node
45.150.64.39	IOC-UEKGC2M01H5G7ZL8	Botnet C2	HIGH	Confirmed infrastructure
45.150.64.23	IOC-PW63KKH9ZRPM9VSC	Botnet C2	HIGH	Same /24 cluster as above
45.150.108.198	IOC-PTIZ97R9V44VEMYG	—	HIGH	Associated infrastructure
45.142.212.61	IOC-1FDG5OZ53I7H3ILR	Botnet C2	HIGH	Confirmed C2
38.132.99.167	IOC-YRRQB2FPEQPNKAHT	Botnet C2	HIGH	US-hosted relay
23.95.220.166	IOC-2HXCANALC10ICHY8	Botnet C2	HIGH	Confirmed C2 node
194.4.50.133	IOC-91Z46DMXBFWVZ4Q3	—	HIGH	European-hosted
194.11.246.78	IOC-NBB82GUXLWYQJ0T5	—	HIGH	Confirmed attribution
185.198.57.75	IOC-AJ3IRZCRW4MM5W5G	Botnet C2	HIGH	Active relay node
185.183.98.242	IOC-6VCVNSP9WXIQDY69	Botnet C2	HIGH	Confirmed
185.183.96.7	IOC-WGWZ52CM7M0QHB89	Botnet C2	HIGH	Same subnet cluster
185.162.235.182	IOC-LJP2UQU9PPZ04X3M	Botnet C2	HIGH	Active infrastructure
185.141.27.143	IOC-5WG9KK2ALUIKPI02	Botnet C2	HIGH	Confirmed C2
185.141.27.14	IOC-BFWUHIASSSHTRFRK	Botnet C2	HIGH	Same /24 as above
185.117.75.101	IOC-Q9A4CAA1MDREXD9N	Botnet C2	HIGH	Active relay
185.117.73.74	IOC-G3NSJLT3040F65HM	Botnet C2	HIGH	Confirmed
185.25.51.108	IOC-IM5L93W4ABD8PKNW	Botnet C2	HIGH	Active C2 node
185.82.202.240	IOC-DKNVNOXQ2Q41MAZL	Botnet C2	HIGH	Confirmed
169.150.227.230	IOC-6FYBE5JISHTA836A	—	HIGH	Attributed node
162.223.89.11	IOC-DFFYCIHDQNTGJZA5	Botnet C2	HIGH	Confirmed C2 relay
146.70.172.227	IOC-0V13B0T2OUV3N2Q1	—	HIGH	Confirmed attribution
95.181.161.50	IOC-6FEWMMRIP1XKKC8E	Botnet C2	HIGH	Confirmed C2
51.16.209.105	IOC-SUU2KIIEG3VY2043	—	HIGH	**Dual attribution: MuddyWater + TA450**
5.252.23.52	IOC-MGR21RLQDD8ZKPKB	—	HIGH	Confirmed attribution

Infrastructure Note: The 45.150.64.x/24 subnet cluster (nodes .23, .39, .239) represents a dedicated MuddyWater infrastructure block. Defenders should apply enhanced monitoring across the full /24 rather than blocking individual IPs only, as MuddyWater rotates within known subnets.





#	TITLE	CONFIDENCE	LAST ACTIVITY
1	IP address "62.106.66.112" used by threat actor MuddyWater	≤100% HIGH	Dec 06, 2025
2	Threat actor MuddyWater utilizing IP address "35.175.224.64"	≤100% HIGH	Dec 06, 2025
3	MuddyWater controlled IP address "3.95.7.142"	≤75% ELEVATED	Dec 06, 2025
4	IP address "212.232.22.136" attributed to MuddyWater	≤100% HIGH	Dec 06, 2025
5	IP address "206.71.149.51" used by threat actor MuddyWater	≤75% ELEVATED	Dec 06, 2025
6	MuddyWater IP address "167.99.224.13" detected	≤100% HIGH	Dec 06, 2025



13	MuddyWater related botnet attacks IP address "154.90.32.88:8043" identified	≤100% HIGH	Nov 27, 2025
14	IP address "8.217.47.190:8848" attributed to MuddyWater botnet infrastructure activity	≤100% HIGH	Nov 27, 2025
15	MuddyWater botnet activity IP address "8.217.56.157:6379" detected	≤75% ELEVATED	Nov 27, 2025
16	botnet attacks URL "zstoreshoping.ddns.net" reportedly targeting by threat actor MuddyWater	≤90% MEDIUM	Jan 23, 2025
17	URL "www.cankayasrc.com" particularly exploiting linked to botnet infrastructure by MuddyWater	≤100% HIGH	Jan 23, 2025
18	MuddyWater command and control infrastructure URL "www.adfg.ae"	≤75% ELEVATED	Jan 23, 2025

Active Botnet C2 IP:Port Indicators

Indicator	IOC Link	Threat Type	Confidence
154.90.32.88:8043	IOC-ND9SK86VK4G6P7U5	Botnet C2	HIGH
8.217.47.190:8848	IOC-9L3G0INWCGVJ2ROJ	Botnet C2	HIGH

Analyst Note: Port 8043 and 8848 are non-standard ports used to evade port-based firewall rules blocking common C2 ports. Outbound connections to these port/IP combinations from any internal host should be treated as confirmed compromise indicators.

Botnet C2 Domain Indicators

The following domains have been confirmed as MuddyWater C2 infrastructure:

Domain	IOC Link	ThreatType
www.cankayasrc.com	IOC-HXOX5DB0WGSRH9WK	Botnet C2
wmcpk.org	IOC-HA7QB2AI6E00LR93	Botnet C2
webftpcloud.com	IOC-3P33CE6SW9P9LIAH	Botnet C2
web3secureapp.com	IOC-GM1XQXZW1BRGYOAZ	Botnet C2
vatacloud.com	IOC-LDXPXTT2O1OKD5SA	Botnet C2
softwaree-cloud.com	IOC-FF5BNIS4C8LG21U5	Botnet C2
smtpcloudapp.com	IOC-XRKOAWF55UVN7B0Y	Botnet C2
protocol-security.in	IOC-GXOGCH6ASH7LWUQ6	Botnet C2
oauth-services.live	IOC-9HR44JAPMFTMKIH1	Botnet C2
myhealthmedical.ae	IOC-QZHZEN4DDQGTYUVT	Botnet C2
mirosoftcloud.ddns.net	IOC-B8CLY7XNGHQO23CG	Botnet C2
microsoftofice.zyns.com	IOC-O8WTOEYO12TWWFD3	Botnet C2
offlce.dnset.com	IOC-GLTWBSDY7HEEPPG3	Botnet C2
logincheck.in	IOC-OFFJTKEGRWR0FQ8Y	Botnet C2
logind2-secure.tk	IOC-5I57M14KF17BVSFZ	Botnet C2
login-secure-account.cf	IOC-8PP1VFXMK7ROBKPF	Botnet C2
kinneretacil.egnyte.com	IOC-TRQOWANS8RARX98Z	Botnet C2
fbcsoft.egnyte.com	IOC-C7T69ZSR5Z3ZRWKN	Botnet C2
cnsmportal.egnyte.com	IOC-8WU7DZ4GVCHUXF2Q	Botnet C2
instance-n3e3x9-relay.screenconnect.com	IOC-SXWUCGFTXPE5X3MO	Botnet C2

Pattern Note: MuddyWater consistently registers domains that impersonate Microsoft services (microsoftofice, mirosoftcloud), security protocols (protocol-security.in, logincheck.in), and cloud services (vatacloud.com, webftpcloud.com). Defenders should build regex-based detection rules for this naming convention pattern in addition to blocking known indicators.

Full MITRE ATT&CK v14 Mapping

Tactic	Technique ID	Technique Name	MuddyWater Implementation
Initial Access	T1566.001	Phishing: Spearphishing Attachment	Malicious DOCX/XLSM with macros; RustyWater via icon-spoofed EXE
Initial Access	T1566.002	Phishing: Spearphishing Link	Links to cloud-hosted payloads (OneDrive, Dropbox, Egnyte)
Initial Access	T1133	External Remote Services	SSH/OWA/VPN brute-force for credential-based access
Initial Access	T1190	Exploit Public-Facing Applications	VPN appliance exploitation for initial network foothold
Execution	T1059.001	PowerShell	POWERSTATS delivery; encoded PowerShell download cradles
Execution	T1059.005	Visual Basic	VBA macros in lure documents triggering PowerShell
Execution	T1204.002	User Execution: Malicious File	Victim enabling macros or running icon-spoofed Fooder executable
Execution	T1047	Windows Management Instrumentation	WMI for lateral movement and command execution
Persistence	T1547.001	Registry Run Keys / Startup Folder	RustyWater and MuddyViper registry-based autostart
Persistence	T1053.005	Scheduled Task/Job	Scheduled tasks named with system-like strings post-compromise
Persistence	T1546.003	WMI Event Subscription	WMI subscriptions for persistent execution across reboots
Persistence	T1078	Valid Accounts	Use of harvested VPN/OWA credentials for persistent access
Privilege Escalation	T1055	Process Injection	Fooder reflective DLL injection to load MuddyViper in memory
Privilege Escalation	T1134	Access Token Manipulation	Post-exploitation token impersonation for elevated access
Defense Evasion	T1027	Obfuscated Files or Information	PowerShell Base64 encoding; Rust XOR string encryption
Defense Evasion	T1036.005	Masquerading: Match Legitimate Name	Scheduled tasks named 'WindowsUpdate', 'AdobeFlash' etc.
Defense Evasion	T1218	System Binary Proxy Execution	Living-off-the-land via WScript/CScript/PowerShell
Defense Evasion	T1497	Virtualization/Sandbox Evasion	RustyWater anti-VM and anti-debug checks
Defense Evasion	T1562.001	Impair Defenses: Disable or Modify Tools	AV/EDR evasion via memory-resident execution

Defense Evasion	T1090.002	Proxy: External Proxy	Egnyte, ConnectWise, legitimate cloud services as C2 relays
Credential Access	T1110.001	Brute Force: Password Guessing	SSH/OWA/VPN credential stuffing from external nodes
Credential Access	T1003	OS Credential Dumping	Custom Mimikatz loader for LSASS credential harvesting
Credential Access	T1555	Credentials from Password Stores	Browser credential theft via MuddyViper
Discovery	T1082	System Information Discovery	Full hardware/OS enumeration by MuddyViper on deployment
Discovery	T1057	Process Discovery	Running process enumeration for AV/EDR identification
Discovery	T1016	System Network Configuration Discovery	Network interface and routing table enumeration
Discovery	T1087	Account Discovery	Active Directory user/group enumeration post-access
Lateral Movement	T1021.002	Remote Services: SMB/Windows Admin Shares	Lateral movement via harvested credentials
Lateral Movement	T1021.001	Remote Desktop Protocol	RDP lateral movement using stolen credentials
Collection	T1213	Data from Information Repositories	SharePoint/Exchange intelligence collection
Collection	T1560	Archive Collected Data	Compression of exfiltrated data before C2 upload
Collection	T1113	Screen Capture	MuddyViper screen capture capability
Command & Control	T1071.001	Application Layer Protocol: HTTP	HTTPS C2 with custom URIs mimicking CDN traffic
Command & Control	T1102	Web Service	Egnyte/Dropbox/OneDrive as C2 relay platforms
Command & Control	T1132.001	Data Encoding: Standard Encoding	Base64-encoded payload transmission in HTTP bodies
Command & Control	T1573	Encrypted Channel	TLS-encrypted C2 for RustyWater; HTTPS for all implants
Exfiltration	T1041	Exfiltration Over C2 Channel	Data exfiltration via established C2 connection
Exfiltration	T1048	Exfiltration Over Alternative Protocol	DNS-based exfiltration documented in select campaigns

Campaign Intelligence: Recent Waves

MuddyViper / Fooder Campaign (Sept 2024 – March 2025)

- **Targets:** Israeli technology, engineering, manufacturing, local government, education organisations; one confirmed Egyptian critical-infrastructure victim
- **Delivery:** Fooder loader disguised as Snake_Game.exe and similar executables
- **Implant:** MuddyViper reflectively loaded into memory
- **Objective:** Credential harvesting, network mapping, initial-access brokering for Lyceum
- **Notable TTP:** Mimikatz loader variant deployed for LSASS credential harvesting

RustyWater Campaign (2026 — Ongoing)

- **Targets:** Diplomatic, maritime, financial, and telecom entities across the Middle East; Israel primary focus; Saudi Arabia and GCC secondary
- **Delivery:** Spear-phishing attachments themed around diplomacy, maritime, financial compliance, and cybersecurity alerts
- **Implant:** RustyWater Rust-based RAT with encrypted HTTP C2
- **Evasion:** Anti-debugging, anti-VM, position-independent XOR encryption, randomised sleep intervals
- **Concurrent Activity:** Overlaps with CAMPAIGN-2026-GULF-01 IOC cluster activity targeting Saudi Arabia (see FF-IW-20260304-SA)

Botnet Infrastructure Campaign (Jan 2025 — Ongoing)

- **Infrastructure:** Large-scale botnet C2 network confirmed across multiple ASNs
- **Notable Nodes:** 154.90.32.88:8043 and 8.217.47.190:8848 (confirmed botnet C2 at non-standard ports)
- **Scale:** 100+ confirmed IOCs across IP, domain, and URL indicator types in FalconFeeds telemetry
- **Pattern:** MuddyWater maintains a persistent, redundant C2 infrastructure pool, rotating IPs within known /24 subnets

Sector Impact Assessment

Israel — Primary Target Landscape

Israeli organisations face the highest MuddyWater threat concentration. The combination of RustyWater delivery via diplomatic and cybersecurity-themed lures, the Fooder/MuddyViper campaign against critical infrastructure, and MuddyWater's documented role as an initial-access broker for Agrius (a destructive wiper operator targeting Israel) creates a multi-stage escalation risk. Any Israeli organisation in technology, engineering, defence-adjacent sectors, local government, or telecommunications should treat this threat profile as directly relevant to their environment.

Saudi Arabia & GCC

Saudi Arabia, and broader GCC organisations face MuddyWater activity in coordination with larger Iranian APT campaigns. The concurrent CAMPAIGN-2026-GULF-01 cluster (FF-IW-20260304-SA) demonstrates that MuddyWater-style credential-access and initial-access-brokering activity supports larger OilRig/APT34 operations targeting Saudi energy, financial, and government infrastructure.

Telecommunications

Telecom providers across the Middle East, Europe, and Asia face sustained targeting. MuddyWater's interest in telecommunications spans both intelligence collection (call records, subscriber data) and infrastructure disruption potential. The group's use of RMM tools that telecom IT teams routinely whitelist (SimpleHelp, ScreenConnect) creates elevated risk that intrusion activity will not trigger standard detection rules.

Government & Defence

Government ministries across all affected regions face spear-phishing risk from MuddyWater's "cybersecurity guidelines" and "official notice" lure themes — themes specifically calibrated to be convincing to security-aware government employees. The group's WMI-based persistence and memory-resident implant execution are specifically designed to evade the host-based detection tools most commonly deployed in government environments.

Recommended Immediate Actions

Priority Actions — Complete Within 2 Hours:

1. Ingest all IOC tables into SIEM, EDR, and firewall block lists
2. Query 72-hour log window for outbound connections to all listed IPs and domains
3. Immediate hunt for connections to 154.90.32.88:8043 and 8.217.47.190:8848 — treat any match as confirmed compromise
4. Alert on outbound connections to Egnyte and ScreenConnect relay domains if not in approved software inventory

Network-Layer Controls (24 Hours):

5. Block all IP indicators in both inbound and outbound directions at edge firewalls, WAF, and EDR network policies

6. Implement enhanced scrutiny on traffic to/from AS ranges heavily represented in IOC list (Hetzner AS24940, OVH AS16276, DigitalOcean AS14061)

7. Review DNS logs for queries to any MuddyWater-attributed domains

8. Enable SSL/TLS inspection on outbound HTTPS to cloud-hosted IPs with no associated domain name — this covers RustyWater and POWERSTATS C2 traffic

Endpoint & Identity Controls (24 Hours):

9. Hunt for PowerShell Event ID 4104 entries with Base64-encoded strings longer than 500 characters spawned from WINWORD.EXE, EXCEL.EXE, or OUTLOOK.EXE

10. Hunt for WMI Event Subscription creation (Event IDs 19, 20, 21) by non-administrative processes

11. Review scheduled tasks for system-mimicking names ('WindowsUpdate', 'AdobeFlash', 'SystemCertificate') created within the last 30 days

12. Enforce MFA on all internet-facing remote access (VPN, OWA, RDP gateways) — MuddyWater credential-stuffing activity is significantly degraded against MFA-protected endpoints

13. Hunt for processes executing from %APPDATA%\Microsoft\Windows\Themes\ or %APPDATA%\Roaming\Microsoft\ with non-Microsoft digital signatures

Threat Hunting Queries (Ongoing):

14. Endpoint hunt: Rust-compiled binaries (identifiable by Rust-specific panicking strings in binary metadata) executing from user-writable directories

15. Network hunt: HTTP POST requests to cloud-hosted IPs (no associated domain) with fixed Content-Length values of 256, 512, or 1024 bytes at regular intervals

16. Email gateway: Filter attachments with .docx/.xlsm/.exe extensions from external senders with diplomatic, maritime, or cybersecurity-themed subjects

17. DNS hunt: High-entropy subdomain queries (>20 random characters) suggesting DNS exfiltration activity consistent with documented MuddyWater/APT34 tooling

FalconFeeds Ongoing Monitoring

FalconFeeds maintains active 24/7 tracking of MuddyWater (XTA-GTP2UWKVBL5CFID4) under elevated priority status. Clients subscribed to **FalconFeeds** IOC watch will receive automated push notifications within minutes of new IOC detections, infrastructure changes, new malware family identifications, and campaign-level escalation events.

Karthika Santhosh Kumar

Share Article
