INTRUVENT

COMPREHENSIVE THREAT HUNTING GUIDE

# MuddyWater RMM Tool Abuse

## Hunting for MOIS-Linked Remote Monitoring Tool Abuse and C2 Framework Activity

**Version** 1.0
**Published** March 11, 2026
**Trigger Event** Dindoor/FakeSet US Infrastructure Campaign
**Classification** TLP:CLEAR
**Total Hunt Time** 4.5–5.5 Hours
**Target Sectors** Financial, Aviation, Defense, Government, Telecom

Intruvent Technologies
INT-THG-2026-MUDDYWATER-RMM-v1.0

## Table of Contents

### Overview

Executive Summary 3
MITRE ATT&CK Mapping 4

### Hunt Modules

Module 1: Unauthorized RMM Tool Installation Detection 5
Module 2: Atera Agent Abuse Analysis 6
Module 3: ScreenConnect/SimpleHelp Anomaly Detection 7
Module 4: PowerShell POWERSTATS/Encoded Command Detection 8
Module 5: DarkBeatC2 Communication Pattern Detection 9
Module 6: PDF-to-RMM Phishing Delivery Chain 10
Module 7: BugSleep Backdoor Detection 11
Module 8: Cloud Service Exfiltration (OneDrive/Egnyte/SharePoint) 12
Module 9: Dindoor and FakeSet Backdoor Hunt 13
Module 10: Lateral Movement via RMM Tools 14

### Appendices

Appendix A: Indicators of Compromise 15
Appendix B: Detection Rules 18
Appendix C: References 21

## 1 Executive Summary

### AT A GLANCE

**THREAT ACTOR**
MuddyWater / Mango Sandstorm (MOIS, Iran)

**PRIMARY TECHNIQUE**
RMM Tool Abuse and Custom C2 Frameworks

**TRIGGER EVENT**
Dindoor/FakeSet US Campaign, March 2026

**TARGET SECTORS**
Financial, Aviation, Defense, Government, Telecom

**KEY TTPS**
T1219 Remote Access Tools, T1059.001 PowerShell

**BUSINESS IMPACT**
Persistent access, data exfiltration, destructive handoff

MuddyWater (also tracked as Mango Sandstorm by Microsoft, Seedworm by Symantec, Static Kitten by CrowdStrike, and TA450 by Proofpoint) is a subordinate element within Iran's Ministry of Intelligence and Security (MOIS). Officially attributed by USCYBERCOM and a joint CISA/FBI/CNMF/NCSC-UK advisory in early 2022, MuddyWater has conducted cyber espionage operations since at least 2017, targeting government, telecommunications, energy, education, and technology sectors across the Middle East, Europe, Asia, and North America.

On March 5, 2026, Broadcom's Symantec Threat Hunter Team publicly disclosed that MuddyWater had pre-positioned two new backdoors, **Dindoor** (Deno runtime) and **FakeSet** (Python-based), inside US financial, aviation, NGO, and defense software company networks since early February 2026 (source: Broadcom/Symantec). This disclosure, combined with the group's sustained abuse of legitimate Remote Monitoring and Management (RMM) tools such as Atera, ScreenConnect, SimpleHelp, and AnyDesk, establishes the urgent need for proactive threat hunting across enterprise environments.

This guide provides **10 hunt modules** designed to detect MuddyWater's distinctive tactics: unauthorized RMM tool installations, Atera Agent abuse, ScreenConnect and SimpleHelp anomalies, POWERSTATS PowerShell backdoor activity, DarkBeatC2 communications, PDF-based phishing delivery chains, BugSleep backdoor indicators, cloud service exfiltration, Dindoor/FakeSet backdoor artifacts, and lateral movement via RMM tools. Total estimated hunt time is **4.5 to 5.5 hours**.

### Threat Overview

MuddyWater has systematically evolved its tooling over nine years of operations. The group pioneered the abuse of legitimate RMM software as an initial access and persistence mechanism, rotating through ScreenConnect, Syncro, SimpleHelp, RemoteUtilities, Atera Agent, Level, PDQ, and AnyDesk to avoid detection (source: HarfangLab, ESET, Group-IB). This living-off-the-land approach allows MuddyWater to maintain persistent access without deploying custom malware that might trigger endpoint detection.

In parallel, MuddyWater has developed and discarded five custom C2 frameworks: SimpleHarm, MuddyC3 (Python2), PhonyC2 (Python3), MuddyC2Go (Golang), and DarkBeatC2. Each transition was typically forced by public exposure or source code leaks of the previous framework (source: Deep Instinct). The group's most recent campaigns in 2026 demonstrate a shift toward compiled-language implants, including RustyWater (Rust-based), CHAR (Rust-based with Telegram C2), and Dindoor (Deno runtime), indicating continued investment in defense evasion through novel runtime environments (source: CloudSEK, Group-IB, Broadcom/Symantec).

MuddyWater operates within a broader MOIS ecosystem that includes Scarred Manticore (espionage and initial access), Void Manticore/Handala (destructive operations), Lemon Sandstorm (infrastructure pre-positioning), and Cotton Sandstorm (influence operations). This coordination means that MuddyWater intrusions can serve as precursors to destructive attacks by sibling units (source: Check Point Research, Microsoft).

**KEY CHARACTERISTICS**

- MOIS state-sponsored (Iran)
- 8+ RMM tools abused since 2021
- 5 custom C2 frameworks developed
- PDF-to-RMM phishing delivery chain
- Egnyte/Backblaze/Wasabi cloud abuse
- Deno and Rust runtime adoption (2026)
- Telegram bot C2 (CHAR, GRAMDOOR)
- Rclone-based data exfiltration
- Active inside US critical infrastructure
- MOIS handoff to destructive units

## 2 MITRE ATT&CK Mapping

The following techniques have been observed in MuddyWater campaigns, with sources from CISA, Microsoft, Deep Instinct, Check Point, ESET, Group-IB, and Broadcom/Symantec. MuddyWater is tracked as **G0069** in the MITRE ATT&CK framework with 58 documented techniques.

**T1219** KEY TTP
**Remote Access Tools**
Systematic abuse of Atera, ScreenConnect, SimpleHelp, AnyDesk, Syncro, Level, PDQ, and RemoteUtilities for persistence

**T1059.001**
**PowerShell**
POWERSTATS backdoor, encoded commands, PhonyC2/MuddyC2Go/DarkBeatC2 PowerShell payloads for post-exploitation

**T1566.001**
**Spearphishing Attachment**
PDF attachments with embedded URLs linking to Egnyte-hosted RMM installers; VBA macro-enabled Word documents

**T1566.002**

**Spearphishing Link**

Direct links to file-sharing platforms (Egnyte, OneHub, Mega) hosting malicious RMM agent installers

**T1059.007** 2026

**JavaScript**

Dindoor backdoor uses Deno JavaScript/TypeScript runtime for command execution and C2 over HTTPS

**T1071.001**

**Web Protocols**

BugSleep C2 over raw TCP port 443; RustyWater HTTP JSON C2 with Base64 and XOR obfuscation

**T1102.002**

**Bidirectional Communication**

CHAR and GRAMDOOR backdoors use Telegram Bot API for C2; Small Sieve uses Telegram over HTTPS

**T1190**

**Exploit Public-Facing Application**

CVE-2021-44228 (Log4Shell in SysAid), CVE-2023-27350 (PaperCut RCE), CVE-2020-1472 (Zerologon)

**T1547.001**

**Registry Run Keys / Startup Folder**

UDPGangster persists via HKCU Startup; RustyWater persists via Registry Run key pointing to CertificationKit.ini

**T1583.006**

**Web Services**

Egnyte, Backblaze, Wasabi, OneHub, and Mega cloud services abused for payload hosting and data exfiltration

**T1027.010**

**Command Obfuscation**

BugSleep byte-subtraction obfuscation (subtract 3 mod 256); RustyWater XOR-encrypted strings; Base64 encoding

**T1105**

**Ingress Tool Transfer**

Downloads additional tools post-compromise including Rclone, LIGOLO tunneling, CrackMapExec, and go-socks5

## 3 Hunt Modules

### 1 Unauthorized RMM Tool Installation Detection

Duration: 30 min Priority: CRITICAL

*Objective: Identify installations of Remote Monitoring and Management (RMM) tools that MuddyWater has used across campaigns since 2021, including Atera, ScreenConnect, SimpleHelp, AnyDesk, Syncro, Level, PDQ, and RemoteUtilities.*

---

#### Background

MuddyWater pioneered the systematic abuse of legitimate RMM tools for initial access and persistence. Rather than deploying custom malware that might trigger endpoint detection, the group installs commercially available RMM agents that blend with normal IT operations. HarfangLab documented the Atera Agent campaign spanning late October 2023 through April 2024 across Israel, India, Algeria, Turkey, Italy, and Egypt. ESET reported the group also uses Level and PDQ in 2024-2025 campaigns. Group-IB's Operation Olalampo report (February 2026) identified AnyDesk deployment via the HTTP_VIP downloader. Organizations that do not maintain a whitelist of approved RMM software are particularly vulnerable.

#### Prerequisites

- Microsoft Defender for Endpoint (DeviceProcessEvents, DeviceFileEvents tables)
- Software inventory or approved RMM tool list from IT management

#### Hunt Procedure: Detect Known MuddyWater RMM Tools

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect installation or execution of RMM tools used by MuddyWater
// Source: HarfangLab, ESET, Group-IB, CISA AA22-055A
let MuddyWaterRMM = dynamic([
    "AteraAgent.exe", "ScreenConnect.ClientService.exe",
    "SimpleHelp.exe", "AnyDesk.exe", "Syncro.Overmind.Service.exe",
    "RemoteUtilities.exe", "rutserv.exe", "rfusclient.exe",
    "level-windows-amd64.exe", "PDQConnect.Agent.exe"
]);
DeviceProcessEvents
| where FileName in~ (MuddyWaterRMM)
| project Timestamp, DeviceName, FileName, FolderPath,
    ProcessCommandLine, InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

#### Hunt Procedure: RMM Installer File Creation Detection

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect RMM installer files being dropped on disk
DeviceFileEvents
| where ActionType == "FileCreated"
| where FileName matches regex @"(?i)(atera|screenconnect|simplehelp|anydesk|syncro|remoteutil|level-windows|pdqconnect)"
| where FileName endswith ".exe" or FileName endswith ".msi"
| project Timestamp, DeviceName, FileName, FolderPath,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

### Expected Results and Escalation Criteria

☐ Cross-reference all detected RMM tools against the IT-approved software list

☐ Any RMM tool not on the approved list warrants immediate investigation

☐ Multiple different RMM tools on a single endpoint is a strong indicator of compromise

☐ RMM tools installed via PowerShell, cmd.exe, or browser downloads outside IT workflows require escalation

**Critical: Legitimate Tool, Malicious Use**

All RMM tools listed above are legitimate commercial software. Detection does not confirm compromise. However, any installation not traceable to an authorized IT deployment process should be treated as suspicious, especially when the installing user account is not in the IT department.

## 2 Atera Agent Abuse Analysis

Duration: 30 min Priority: **CRITICAL**

*Objective: Detect unauthorized Atera Agent installations and identify abuse patterns consistent with MuddyWater's preferred RMM tool for persistent access.*

### Background

Atera Agent became MuddyWater's primary RMM tool from late October 2023 through at least mid-2024 (source: HarfangLab). Atera provides a significant operational advantage: the C2 infrastructure is entirely managed by Atera's legitimate cloud platform, meaning the attacker does not need to maintain any attacker-controlled servers. The agent installation typically arrives via spear-phishing links pointing to file-sharing platforms (Egnyte, OneHub, Mega) where the Atera installer is hosted. Deep Instinct's DarkBeatC2 research confirmed Atera delivery via Egnyte in 2024 campaigns.

### Prerequisites

- Microsoft Defender for Endpoint (DeviceProcessEvents, DeviceNetworkEvents, DeviceRegistryEvents tables)
- Atera license records from IT procurement (to identify authorized tenant IDs)

### Hunt Procedure: Atera Agent Process and Service Detection

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect Atera Agent processes and service installations
// Source: HarfangLab RMM campaign analysis
DeviceProcessEvents
| where FileName in~ ("AteraAgent.exe", "AteraSetup.msi",
    "AteraAgentSetup.exe")
    or ProcessCommandLine has "AteraAgent"
| project Timestamp, DeviceName, FileName, FolderPath,
    ProcessCommandLine, InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

### Hunt Procedure: Atera Agent Network Connections

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Monitor Atera Agent network connections for C2 activity
DeviceNetworkEvents
| where InitiatingProcessFileName =~ "AteraAgent.exe"
| summarize ConnectionCount=count(),
    RemoteIPs=make_set(RemoteIP),
    RemoteDomains=make_set(RemoteUrl)
    by DeviceName, bin(Timestamp, 1h)
| sort by ConnectionCount desc
```

### Hunt Procedure: Atera Agent Registry Persistence

**INVESTIGATION AID**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect Atera Agent service registration in the registry
DeviceRegistryEvents
| where RegistryKey has "AteraAgent"
    or RegistryValueData has "AteraAgent"
| project Timestamp, DeviceName, ActionType, RegistryKey,
    RegistryValueName, RegistryValueData, InitiatingProcessFileName
| sort by Timestamp desc
```

- ☐ Verify whether the organization has an authorized Atera license; if not, any Atera installation is unauthorized
- ☐ If Atera is authorized, compare the tenant ID in the agent configuration against the known corporate tenant ID
- ☐ Check the initiating process for Atera installations; delivery via browser downloads from Egnyte or OneHub is consistent with MuddyWater
- ☐ Review the timeline of installation relative to any phishing emails received by the user

**Atera Cloud C2: No Attacker Infrastructure to Block**

Because Atera Agent communicates through Atera's legitimate cloud infrastructure, network-level IOC blocking is not effective. Detection must focus on identifying unauthorized agent installations at the endpoint level. Blocking Atera's cloud domains would disrupt legitimate MSP operations.

## 3 ScreenConnect/SimpleHelp Anomaly Detection

Duration: 25 min Priority: **HIGH**

*Objective: Detect unauthorized ScreenConnect and SimpleHelp installations and identify anomalous remote access sessions that may indicate MuddyWater activity.*

### Background

ScreenConnect (ConnectWise) and SimpleHelp were among the earlier RMM tools in MuddyWater's rotation, documented by CISA in advisory AA22-055A and by multiple vendor reports. Unlike Atera, ScreenConnect can be self-hosted, meaning MuddyWater can run its own ScreenConnect relay server on attacker-controlled infrastructure. SimpleHelp has also been used for persistence on victim devices (source: CSO Online). Both tools leave distinct process artifacts and network connection patterns that differ from legitimate IT deployments.

### Prerequisites

- Microsoft Defender for Endpoint (DeviceProcessEvents, DeviceNetworkEvents tables)
- List of authorized ScreenConnect relay servers (if ScreenConnect is used by IT)

### Hunt Procedure: ScreenConnect Client Detection

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect ScreenConnect client processes and services
// Source: CISA AA22-055A; multiple vendor reports
DeviceProcessEvents
| where FileName in~ ("ScreenConnect.ClientService.exe",
    "ScreenConnect.WindowsClient.exe")
    or ProcessCommandLine has "ScreenConnect"
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

### Hunt Procedure: ScreenConnect Connections to Non-Approved Relays

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Identify ScreenConnect connections to relay servers not on the approved list
let ApprovedRelays = dynamic(["relay.yourcompany.com"]); // Replace with your approved ScreenConnect relays
DeviceNetworkEvents
| where InitiatingProcessFileName =~ "ScreenConnect.ClientService.exe"
| where RemoteUrl !in (ApprovedRelays)
| project Timestamp, DeviceName, RemoteIP, RemoteUrl, RemotePort,
    InitiatingProcessFileName
| sort by Timestamp desc
```

### Hunt Procedure: SimpleHelp Process Detection

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect SimpleHelp remote access tool processes
DeviceProcessEvents
| where FileName in~ ("SimpleHelp.exe", "SimpleService.exe",
    "Remote Access.exe")
    or ProcessCommandLine has "SimpleHelp"
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

☐ If ScreenConnect is authorized, verify all relay server connections match the approved relay list

☐ Any ScreenConnect instance connecting to an unknown relay server warrants immediate investigation

☐ SimpleHelp installations not traceable to IT deployment should be treated as unauthorized

☐ Check whether ScreenConnect/SimpleHelp sessions occurred outside business hours or from unexpected user accounts

**What to Look For**

MuddyWater frequently uses self-hosted ScreenConnect relays on cloud infrastructure. Connections to Vultr, OVH, or Stark Industries hosted relay servers are consistent with MuddyWater's known infrastructure preferences. Legitimate ScreenConnect deployments connect to the organization's own relay or to ConnectWise's cloud relay (screenconnect.com).

## 4 PowerShell POWERSTATS/Encoded Command Detection

Duration: 30 min Priority: **HIGH**

*Objective: Detect POWERSTATS backdoor activity and encoded PowerShell commands generated by MuddyWater's C2 frameworks (PhonyC2, MuddyC2Go, DarkBeatC2).*

### Background

POWERSTATS (also called Powermud) has been MuddyWater's signature PowerShell backdoor since the group's first documented campaigns in 2017 (source: Unit 42). All of MuddyWater's custom C2 frameworks generate PowerShell payloads for post-exploitation: PhonyC2 (Python3, source code leaked 2023), MuddyC2Go (Golang), and DarkBeatC2 all produce encoded PowerShell commands that communicate back to C2 infrastructure (source: Deep Instinct). Detection of heavily encoded or obfuscated PowerShell execution, particularly involving Base64, compressed streams, or IEX (Invoke-Expression), is a strong indicator of MuddyWater activity.

### Prerequisites

- Microsoft Defender for Endpoint (DeviceProcessEvents table)
- PowerShell Script Block Logging enabled (Event ID 4104)

### Hunt Procedure: Encoded PowerShell Command Detection

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect PowerShell executions with encoding, compression, or download cradles
// Source: CISA AA22-055A; Deep Instinct PhonyC2/MuddyC2Go/DarkBeatC2 research
DeviceProcessEvents
| where FileName in~ ("powershell.exe", "pwsh.exe")
| where ProcessCommandLine has_any (
    "-EncodedCommand", "-enc ", "-e ",
    "FromBase64String", "IEX", "Invoke-Expression",
    "IO.Compression", "IO.MemoryStream",
    "Net.WebClient", "DownloadString",
    "Invoke-WebRequest", "iwr ", "wget ",
    "Start-BitsTransfer", "bitsadmin"
)
| project Timestamp, DeviceName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

### Hunt Procedure: PowerShell Connecting to Known C2 Domains

**BLOCKING SAFE**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect PowerShell connections to known MuddyWater C2 domains
// Source: Deep Instinct DarkBeatC2 (Apr 2024)
let MuddyC2Domains = dynamic([
    "googlelinks.net", "googlevalues.com", "websiteapicloud.com"
]);
DeviceNetworkEvents
| where InitiatingProcessFileName in~ ("powershell.exe", "pwsh.exe")
| where RemoteUrl has_any (MuddyC2Domains)
| project Timestamp, DeviceName, RemoteUrl, RemoteIP,
    InitiatingProcessCommandLine
| sort by Timestamp desc
```

### Hunt Procedure: PowerShell Script Block Logging Analysis

**INVESTIGATION AID**

KQL (MICROSOFT SENTINEL)

```
// Review decoded PowerShell script blocks for MuddyWater patterns
Event
| where EventID == 4104
| where EventData has_any (
    "POWERSTATS", "Invoke-Expression",
    "System.Net.WebClient", "DownloadString",
    "FromBase64String", "IO.Compression"
)
| project TimeGenerated, Computer, EventData
| sort by TimeGenerated desc
```

☐ Examine decoded Base64 commands for C2 URLs, system enumeration, or credential harvesting

☐ Look for PowerShell processes spawned by unexpected parent processes (mshta.exe, rundll32.exe, wscript.exe)

☐ Correlate encoded PowerShell executions with network connections to external IPs

☐ Check for PowerShell download cradles that fetch additional payloads from cloud storage (Egnyte, Backblaze)

**False Positive Guidance**

Encoded PowerShell is used by legitimate IT automation tools (SCCM, Intune, DSC). Focus triage on executions where the parent process is unusual (browser, Office application, or scripting engine) and the encoded command contains network communication or credential access functions.

## 5 DarkBeatC2 Communication Pattern Detection

Duration: 20 min Priority: **HIGH**

*Objective: Detect network communications to DarkBeatC2 infrastructure, MuddyWater's most recently documented C2 framework, including known IPs, domains, and hosting providers.*

---

### Background

DarkBeatC2 is the fifth known C2 framework developed by MuddyWater, identified by Deep Instinct in April 2024. The framework reuses IP subnets previously associated with SimpleHarm and PhonyC2 campaigns, primarily on OVH hosting. One IP (185.236.234.161) was hosted on Stark Industries, a hosting provider with a documented history of abuse. DarkBeatC2 manages PowerShell-based communications with compromised endpoints and coordinates Atera Agent delivery via Egnyte file-sharing links (source: Deep Instinct).

### Prerequisites

- Microsoft Defender for Endpoint (DeviceNetworkEvents table) or firewall/proxy logs
- DNS query logs (if available)

### Hunt Procedure: DarkBeatC2 IP Detection

**BLOCKING SAFE**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect connections to confirmed DarkBeatC2 infrastructure
// Source: Deep Instinct DarkBeatC2 (Apr 2024)
let DarkBeatC2IPs = dynamic([
    "91.121.240.104",  // PhonyC2 C2 (confirmed by Microsoft)
    "91.121.240.102",  // DarkBeatC2 (googlelinks.net)
    "137.74.131.19",   // DarkBeatC2 (googlevalues.com)
    "164.132.237.68",  // DarkBeatC2
    "185.236.234.161"  // DarkBeatC2 (Stark Industries hosting)
]);
DeviceNetworkEvents
| where RemoteIP in (DarkBeatC2IPs)
| project Timestamp, DeviceName, RemoteIP, RemotePort,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

### Hunt Procedure: DarkBeatC2 Domain Resolution Detection

**BLOCKING SAFE**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect DNS lookups for known DarkBeatC2 domains
// Source: Deep Instinct DarkBeatC2 (Apr 2024)
let DarkBeatDomains = dynamic([
    "googlelinks.net", "googlevalues.com", "websiteapicloud.com"
]);
DeviceNetworkEvents
| where RemoteUrl has_any (DarkBeatDomains)
| project Timestamp, DeviceName, RemoteUrl, RemoteIP,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

**High-Confidence Indicators**

All IPs and domains in this module are confirmed MuddyWater infrastructure from published Deep Instinct and Microsoft research. Any match warrants immediate escalation to incident response. These IPs are hosted on OVH and Stark Industries; they are dedicated C2 infrastructure with no legitimate use case.

## 6 PDF-to-RMM Phishing Delivery Chain

Duration: 25 min Priority: HIGH

*Objective: Detect the MuddyWater phishing delivery chain where PDF attachments contain embedded URLs linking to cloud-hosted RMM tool installers.*

---

### Background

In March 2024, Proofpoint documented MuddyWater's tactical evolution: the group began embedding malicious URLs inside PDF attachments rather than placing them directly in email bodies. This approach bypasses email link scanning because the URL exists within the PDF document, not in the email metadata. The PDFs use pay-related or webinar/course invitation social engineering lures targeting employees at multinational organizations. The embedded URL directs victims to Egnyte, OneHub, or Mega file-sharing platforms where a ZIP archive containing an RMM agent installer (typically Atera) is hosted (source: Proofpoint, Check Point, ESET).

### Prerequisites

- Microsoft Defender for Endpoint (DeviceFileEvents, DeviceProcessEvents tables)
- Email gateway logs with attachment metadata

### Hunt Procedure: PDF-Triggered Download Chain

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect the PDF > Browser > ZIP > RMM installer chain
// Source: Proofpoint TA450 (Mar 2024); ESET MuddyViper (Dec 2025)
DeviceFileEvents
| where ActionType == "FileCreated"
| where FileName endswith ".zip" or FileName endswith ".msi" or FileName endswith ".exe"
| where InitiatingProcessFileName in~ ("chrome.exe", "msedge.exe",
    "firefox.exe", "iexplore.exe")
| where InitiatingProcessCommandLine has_any (
    "egnyte.com", "onehub.com", "mega.nz", "mega.co.nz",
    "backblazeb2.com", "sharepoint.com"
)
| project Timestamp, DeviceName, FileName, FolderPath,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

### Hunt Procedure: Egnyte File-Sharing Link Detection

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect browser connections to Egnyte hosting MuddyWater payloads
// Egnyte is a legitimate cloud platform; focus on unexpected downloads
DeviceNetworkEvents
| where RemoteUrl has "egnyte.com"
| where InitiatingProcessFileName in~ ("chrome.exe", "msedge.exe",
    "firefox.exe")
| summarize DownloadCount=count(),
    URLs=make_set(RemoteUrl)
    by DeviceName, bin(Timestamp, 1h)
| sort by DownloadCount desc
```

### Hunt Procedure: Email Attachment PDF with Embedded Links

**INVESTIGATION AID**

KQL (MICROSOFT DEFENDER FOR OFFICE 365)

```
// Identify emails with PDF attachments that were followed by downloads
EmailAttachmentInfo
| where FileType == "pdf"
| where Timestamp > ago(30d)
| join kind=inner (
    DeviceFileEvents
    | where ActionType == "FileCreated"
    | where FileName endswith ".zip" or FileName endswith ".msi"
    | where Timestamp > ago(30d)
) on $left.RecipientEmailAddress == $right.AccountName
| where datetime_diff('minute', Timestamp1, Timestamp) between (0 .. 60)
| project EmailTimestamp=Timestamp, FileName, Subject=SenderDisplayName,
    DownloadedFile=FileName1, DeviceName
| sort by EmailTimestamp desc
```

☐ Search email logs for PDFs received from external senders with pay-related, webinar, or course invitation subject lines

☐ Correlate PDF receipt time with subsequent Egnyte/OneHub/Mega downloads within 60 minutes

☐ Check downloaded ZIP archives for RMM installer content (Atera, ScreenConnect, SimpleHelp)

☐ Review the sending domain for recently registered or typosquatting characteristics

**Social Engineering Lures**

MuddyWater phishing emails typically impersonate HR departments (salary/bonus themes), IT departments (software update themes), or training providers (webinar/course invitations). The PDF content appears legitimate but contains an embedded link to a file-sharing platform. Proofpoint identified Israeli employees at multinational organizations as primary targets in the March 2024 campaign.

## 7 BugSleep Backdoor Detection

Duration: 30 min Priority: HIGH

*Objective: Detect BugSleep (also called MuddyRot) backdoor artifacts, including known file hashes, network behavior on TCP port 443, and byte-subtraction obfuscation patterns.*

---

### Background

BugSleep is a custom x64 C-language implant first observed in May 2024, representing MuddyWater's partial shift from legitimate RMM tools to purpose-built malware (source: Check Point Research, July 2024). Sekoia independently analyzed the same malware under the name MuddyRot. The backdoor communicates over raw TCP port 443 (not TLS/HTTPS), uses byte-subtraction obfuscation (subtracting each byte by 3, modulo 256), and provides reverse shell, file upload/download, and persistence capabilities. Check Point identified 50+ spear-phishing emails deploying BugSleep across 10+ sectors targeting Turkey, Azerbaijan, Jordan, Saudi Arabia, Israel, and Portugal. Payloads were hosted on Egnyte.

### Prerequisites

- Microsoft Defender for Endpoint (DeviceFileEvents, DeviceNetworkEvents, DeviceProcessEvents tables)

### Hunt Procedure: BugSleep Hash-Based Detection

BLOCKING SAFE

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect known BugSleep/MuddyRot backdoor samples
// Source: PolySwarm, Check Point Research (Jul 2024), Sekoia
let BugSleepHashes = dynamic([
    "94278fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7130c472",
    "b8703744744555ad841f922995cef5dbca11da22565195d05529f5f9095fbfca"
]);
DeviceFileEvents
| where SHA256 in (BugSleepHashes)
| project Timestamp, DeviceName, FileName, SHA256, FolderPath,
    InitiatingProcessFileName, ActionType
```

### Hunt Procedure: Raw TCP Port 443 Communications (Non-TLS)

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect processes using raw TCP on port 443 without TLS
// BugSleep uses raw TCP on port 443, not HTTPS
DeviceNetworkEvents
| where RemotePort == 443
| where InitiatingProcessFileName !in~ (
    "chrome.exe", "msedge.exe", "firefox.exe", "iexplore.exe",
    "Teams.exe", "outlook.exe", "OneDrive.exe", "svchost.exe",
    "MsMpEng.exe", "MsSense.exe"
)
| where InitiatingProcessFileName !endswith ".dll"
| summarize ConnectionCount=count(),
    RemoteIPs=make_set(RemoteIP)
    by DeviceName, InitiatingProcessFileName, bin(Timestamp, 1h)
| where ConnectionCount > 5
| sort by ConnectionCount desc
```

### Hunt Procedure: Mutex and Persistence Indicators

**INVESTIGATION AID**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Hunt for suspicious executables in common MuddyWater staging paths
DeviceFileEvents
| where ActionType == "FileCreated"
| where FolderPath has_any ("\\ProgramData\\", "\\Users\\Public\\",
    "\\AppData\\Roaming\\")
| where FileName endswith ".exe"
| where InitiatingProcessFileName in~ ("powershell.exe", "cmd.exe",
    "wscript.exe", "mshta.exe")
| project Timestamp, DeviceName, FileName, FolderPath,
    InitiatingProcessFileName, InitiatingProcessCommandLine, SHA256
| sort by Timestamp desc
```

**Hash Match Requires Immediate Response**

Both BugSleep hashes listed above are confirmed malicious from Check Point Research and Sekoia analysis. Any match warrants immediate endpoint isolation and forensic investigation. BugSleep provides the operator with reverse shell access and file exfiltration capabilities.

## 8 Cloud Service Exfiltration (OneDrive/Egnyte/SharePoint)

Duration: 20 min Priority: **MEDIUM**

*Objective: Detect data exfiltration via cloud storage services, particularly Rclone to Wasabi, and file uploads to Egnyte, Backblaze, or other platforms abused by MuddyWater.*

### Background

MuddyWater systematically abuses legitimate cloud services throughout the attack lifecycle. Egnyte serves as a payload hosting platform for RMM installers and BugSleep (source: HarfangLab, Check Point, Deep Instinct). Backblaze was used to distribute the FakeSet backdoor in the February 2026 US campaign (source: Broadcom/Symantec). For exfiltration, the group uses Rclone to transfer stolen data to Wasabi cloud storage buckets; this technique was observed at a compromised US defense software company (source: Broadcom/Symantec, March 2026). OneHub and Mega have also been used for payload staging (source: ESET).

### Prerequisites

- Microsoft Defender for Endpoint (DeviceProcessEvents, DeviceNetworkEvents, DeviceFileEvents tables)
- Cloud Access Security Broker (CASB) logs, if available

### Hunt Procedure: Rclone Execution Detection

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect Rclone usage for data exfiltration
// Source: Broadcom/Symantec Dindoor/FakeSet campaign (Mar 2026)
DeviceProcessEvents
| where FileName =~ "rclone.exe"
    or ProcessCommandLine has "rclone"
| project Timestamp, DeviceName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

### Hunt Procedure: Connections to MuddyWater Cloud Infrastructure

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Monitor connections to cloud services used by MuddyWater for staging/exfil
// These are legitimate services; focus on unexpected process names
DeviceNetworkEvents
| where RemoteUrl has_any (
    "wasabi", "backblazeb2.com", "egnyte.com",
    "onehub.com", "mega.nz", "mega.co.nz"
)
| where InitiatingProcessFileName !in~ (
    "chrome.exe", "msedge.exe", "firefox.exe",
    "OneDrive.exe", "Teams.exe", "outlook.exe"
)
| project Timestamp, DeviceName, RemoteUrl,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

- ☐ Rclone is rarely used in enterprise environments; any execution should be investigated unless explicitly authorized by IT
- ☐ Rclone command lines containing "sync", "copy", or "move" with external cloud targets are strong exfiltration indicators
- ☐ Non-browser processes connecting to Egnyte, Backblaze, or Wasabi warrant investigation
- ☐ Large data transfers to cloud storage outside business hours are high-priority findings

**Shared Infrastructure Caveat**

Egnyte, Backblaze, Wasabi, OneDrive, and SharePoint are all legitimate cloud services used by millions of organizations. Do NOT block these services at the network level. Detection must focus on identifying unexpected processes (not browsers or approved applications) communicating with these platforms, combined with suspicious command-line parameters indicating bulk data transfer.

## 9 Dindoor and FakeSet Backdoor Hunt

Duration: 30 min Priority: **MEDIUM**

*Objective: Detect artifacts of MuddyWater's newest backdoors, Dindoor (Deno runtime) and FakeSet (Python-based), deployed against US critical infrastructure in February 2026.*

### Background

Broadcom's Symantec Threat Hunter Team disclosed on March 5, 2026 that MuddyWater had pre-positioned Dindoor and FakeSet backdoors inside US bank, airport, NGO, and defense software company networks since early February 2026. Dindoor uses the Deno JavaScript/TypeScript runtime for command execution and HTTPS C2. FakeSet is Python-based and was downloaded from Backblaze cloud storage. Both were signed with code signing certificates issued to "Amy Cherne"; FakeSet also used a certificate issued to "Donald Gay", a certificate previously used to sign Stagecomp and Darkcomp malware attributed to MuddyWater by Google, Microsoft, and Kaspersky. Specific SHA256 hashes for these samples were not published in open-source secondary reporting. [REQUIRES VERIFICATION: full hashes available in the Broadcom threat intelligence portal]

### Prerequisites

- Microsoft Defender for Endpoint (DeviceProcessEvents, DeviceFileEvents tables)
- Code signing certificate verification tools

### Hunt Procedure: Deno Runtime Detection

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect Deno runtime execution (Dindoor uses Deno for C2)
// Deno is rarely used in enterprise environments
// Source: Broadcom/Symantec (Mar 5, 2026)
DeviceProcessEvents
| where FileName =~ "deno.exe"
    or ProcessCommandLine has "deno"
    or ProcessCommandLine has "Deno"
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName, FolderPath
| sort by Timestamp desc
```

### Hunt Procedure: Executables Downloaded from Backblaze/Wasabi Cloud Storage

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect executables downloaded from cloud storage used by MuddyWater for payload delivery
// For certificate-based detection, use the DeviceFileCertificateInfo table
// to search for signers "Amy Cherne" or "Donald Gay" (Broadcom/Symantec, Mar 2026)
DeviceFileEvents
| where ActionType == "FileCreated"
| where FileName endswith ".exe" or FileName endswith ".dll"
| where FileOriginUrl has_any ("backblaze", "wasabi")
    or InitiatingProcessCommandLine has_any ("backblaze", "wasabi")
| project Timestamp, DeviceName, FileName, FolderPath, SHA256,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

### Hunt Procedure: Python-Based Backdoor Indicators

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect Python execution patterns consistent with FakeSet backdoor
// FakeSet is Python-based; look for unexpected Python execution
DeviceProcessEvents
| where FileName in~ ("python.exe", "python3.exe", "pythonw.exe")
| where InitiatingProcessFileName !in~ (
    "cmd.exe", "powershell.exe", "explorer.exe",
    "code.exe", "pycharm64.exe"  // Exclude known dev tools
)
| where ProcessCommandLine !has "pip"
| project Timestamp, DeviceName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName, FolderPath
| sort by Timestamp desc
```

☐ Deno runtime is extremely uncommon in enterprise environments; any instance requires investigation

☐ Check code signing certificates on suspicious executables for "Amy Cherne" or "Donald Gay" issuance

☐ Files downloaded from Backblaze by non-browser processes are consistent with FakeSet delivery

☐ Python processes communicating with external C2 servers, especially running outside developer workstations, warrant escalation

**Pre-Positioned US Access**

According to Broadcom/Symantec reporting, MuddyWater maintained access to US financial, aviation, and defense supply chain networks via these backdoors since early February 2026. If any indicators are found, treat as a confirmed nation-state intrusion and engage incident response immediately.

## 10 Lateral Movement via RMM Tools

Duration: 20 min Priority: **MEDIUM**

*Objective: Detect lateral movement patterns where MuddyWater uses RMM tools, tunneling utilities, and post-exploitation frameworks to spread across the network after initial access.*

### Background

After establishing initial access through RMM tools or phishing, MuddyWater leverages several techniques for lateral movement. Mandiant documented the group's use of LIGOLO tunneling and CrackMapExec for network enumeration in the UNC3313 campaign (source: Mandiant, February 2022). ESET identified go-socks5 reverse tunneling in the MuddyViper campaign (source: ESET, December 2025). The group also deploys additional RMM tools on secondary targets within the network, effectively propagating legitimate remote access software as a lateral movement mechanism.

### Prerequisites

- Microsoft Defender for Endpoint (DeviceProcessEvents, DeviceNetworkEvents tables)
- Network flow data (optional, for tunnel detection)

### Hunt Procedure: Tunneling Tool Detection

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect LIGOLO, go-socks5, and other tunneling tools
// Source: Mandiant UNC3313 (Feb 2022); ESET MuddyViper (Dec 2025)
DeviceProcessEvents
| where FileName in~ ("ligolo.exe", "ligolo-ng.exe",
    "chisel.exe", "plink.exe", "gost.exe")
    or ProcessCommandLine has_any (
        "ligolo", "go-socks5", "chisel",
        "plink.exe -ssh", "-D 1080"
    )
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

### Hunt Procedure: CrackMapExec and Credential Harvesting

**DETECTION ONLY**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect CrackMapExec and related lateral movement tools
// Source: Mandiant UNC3313 (Feb 2022)
DeviceProcessEvents
| where FileName in~ ("crackmapexec.exe", "cme.exe",
    "nxc.exe", "netexec.exe")
    or ProcessCommandLine has_any (
        "crackmapexec", "cme smb", "nxc smb",
        "sekurlsa::logonpasswords", "lsadump"
    )
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

### Hunt Procedure: RMM Tool Spread Across Multiple Endpoints

**INVESTIGATION AID**

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Identify RMM tools appearing on multiple endpoints in a short timeframe
// Rapid spread suggests lateral movement, not IT deployment
let RMMTools = dynamic([
    "AteraAgent.exe", "ScreenConnect.ClientService.exe",
    "AnyDesk.exe", "SimpleHelp.exe"
]);
DeviceProcessEvents
| where FileName in~ (RMMTools)
| where Timestamp > ago(7d)
| summarize FirstSeen=min(Timestamp), LastSeen=max(Timestamp),
    EndpointCount=dcount(DeviceName),
    Endpoints=make_set(DeviceName)
    by FileName
| where EndpointCount > 3
| extend SpreadTimeHours = datetime_diff('hour', LastSeen, FirstSeen)
| sort by EndpointCount desc
```

☐ LIGOLO, chisel, and go-socks5 are penetration testing tools rarely found in production environments

☐ CrackMapExec or NetExec on any endpoint outside authorized penetration testing requires immediate investigation

☐ RMM tools appearing on 3+ endpoints within a 24-hour window, absent a documented IT rollout, suggest adversary propagation

☐ Check for WMI or PsExec-based deployment of RMM tools across the network

**MOIS Handoff Risk**

MuddyWater operates within the MOIS ecosystem alongside destructive units such as Void Manticore (Storm-0842). Check Point Research documented a structured handoff model where MuddyWater or Scarred Manticore conducts espionage, then transfers access to Void Manticore for destructive operations. Detecting lateral movement may indicate the espionage phase is advanced and destruction could follow.

## A Appendix A: Indicators of Compromise

### Blocking Guidance: 3-Tier IOC Classification

**Tier 1: Block (High Confidence)**

**DarkBeatC2 IPs** (91.121.240.104, 91.121.240.102, 137.74.131.19, 164.132.237.68, 185.236.234.161): Confirmed MuddyWater C2 infrastructure by Deep Instinct and Microsoft. Hosted on OVH and Stark Industries dedicated servers. Safe to add to firewall deny rules. *Caveat: Reassess if OVH/Stark Industries reassigns these IPs to new customers.*

**DarkBeatC2 domains** (googlelinks.net, googlevalues.com, websiteapicloud.com): Confirmed C2 domains. Safe for DNS blocklists.

**All malware SHA256 hashes** listed below (BugSleep, UDPGangster, RustyWater, PowGoop, POWERSTATS): Confirmed malicious with no legitimate use case. Safe for hash-based blocking and EDR prevention policies.

**UDPGangster C2 IP** (157.20.182.75): Confirmed C2 server for UDPGangster backdoor (source: FortiGuard Labs).

**RustyWater C2 IPs** (159.198.66.153, 159.198.68.25, 161.35.228.250) and domain (nomercys.it[.]com): Confirmed C2 infrastructure (source: CloudSEK).

**Tier 2: Alert / Monitor (Shared Infrastructure)**

**Egnyte (egnyte.com):** Legitimate enterprise file-sharing platform used by MuddyWater for payload hosting. Blocking Egnyte will disrupt legitimate business operations. Monitor for non-browser processes downloading from Egnyte. Recommend alerting only.

**Backblaze (backblazeb2.com):** Legitimate cloud storage used by MuddyWater to distribute FakeSet. Blocking will disrupt backup and storage operations. Monitor for executable downloads from Backblaze. Recommend alerting only.

**Wasabi cloud storage:** Legitimate cloud storage used by MuddyWater for Rclone-based data exfiltration. Blocking may disrupt cloud storage operations. Monitor Rclone processes connecting to Wasabi endpoints.

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

**OVH IP ranges (91.121.x.x, 137.74.x.x, 164.132.x.x):** OVH is a major cloud hosting provider. Only the specific DarkBeatC2 IPs above are Tier 1. Broader OVH ranges are Tier 2 (alerting only).

**Tier 3: Investigate (Unconfirmed)**

**Dindoor and FakeSet hashes:** Specific SHA256 hashes for these February 2026 backdoors were not published in open-source secondary reporting. They are reportedly available through the Broadcom/Symantec threat intelligence portal. [REQUIRES VERIFICATION]

**Code signing certificates ("Amy Cherne", "Donald Gay"):** These certificate names are confirmed MuddyWater indicators, but blocking by certificate signer name requires careful implementation to avoid false positives on legitimate signers with similar names. Verify certificate thumbprints before creating blocking rules.

### 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 |
| `b8703744744555ad841f922995cef5dbca11da22565195d05529f5f909` | BugSleep/MuddyRot backdoor | PolySwarm / Sekoia (2024) | High |

| | | | |
|---|---|---|---|
| `5fbfca` | | | |
| `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) | CloudSEK (Jan 2026) | High |
| `f38a56b8dc0e8a581999621eef65ef497f0ac0d35e953bd94335926f00e9464f` | RustyWater/Archer RAT (Rust) | 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 (OVH) | Microsoft; Deep Instinct (Jun 2023) | High |
| `91.121.240.102` | IPv4 | DarkBeatC2 (OVH) | Deep Instinct (Apr 2024) | High |
| `137.74.131.19` | IPv4 | DarkBeatC2 (OVH) | Deep Instinct (Apr 2024) | High |
| `164.132.237.68` | IPv4 | DarkBeatC2 (OVH) | Deep Instinct (Apr 2024) | High |
| `185.236.234.161` | IPv4 | DarkBeatC2 (Stark Industries) | Deep Instinct (Apr 2024) | High |
| `157.20.182.75` | IPv4 | UDPGangster C2 (UDP port 1269) | FortiGuard Labs (Dec 2025) | High |
| `159.198.66.153` | IPv4 | RustyWater C2 | CloudSEK (Jan 2026) | High |
| `159.198.68.25` | IPv4 | RustyWater C2 | CloudSEK (Jan 2026) | High |
| `161.35.228.250` | IPv4 | RustyWater C2 | CloudSEK (Jan 2026) | High |

### C2 Domains

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

### C2 Infrastructure (Telegram Bot)

| Indicator | Type | Context | Source | Confidence |
|---|---|---|---|---|
| `stager_51_bot` | Telegram Bot Username | CHAR backdoor C2 (Operation Olalampo) | Group-IB (Feb 2026) | High |

### File Paths and Artifacts

| Indicator | Type | Context | Source | Confidence |
|---|---|---|---|---|
| `C:\Users\Public\ui.txt` | File Path | UDPGangster decoded payload location | 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 persistence (Rust PE as reddit.exe) | CloudSEK (Jan 2026) | High |

|  |  |  |  |  |
|---|---|---|---|---|
| `xhxhxhxhxhxpp` | Mutex | UDPGangster mutex | FortiGuard Labs (Dec 2025) | High |

## B Appendix B: Detection Rules

### KQL Detection Rules

**Unauthorized RMM Tool Installation** KQL

DETECTION ONLY

MICROSOFT DEFENDER FOR ENDPOINT

```
// RULE: Alert on execution of RMM tools used by MuddyWater
// Source: HarfangLab, ESET, Group-IB, CISA AA22-055A
let MuddyWaterRMM = dynamic([
    "AteraAgent.exe", "ScreenConnect.ClientService.exe",
    "SimpleHelp.exe", "AnyDesk.exe", "Syncro.Overmind.Service.exe",
    "RemoteUtilities.exe", "rutserv.exe", "rfusclient.exe",
    "level-windows-amd64.exe", "PDQConnect.Agent.exe"
]);
DeviceProcessEvents
| where FileName in~ (MuddyWaterRMM)
| summarize ExecutionCount=count(),
    Devices=make_set(DeviceName),
    FirstSeen=min(Timestamp), LastSeen=max(Timestamp)
    by FileName
| sort by ExecutionCount desc
```

**DarkBeatC2 Network Communication** KQL

BLOCKING SAFE

MICROSOFT DEFENDER FOR ENDPOINT

```
// RULE: Detect connections to confirmed MuddyWater C2 infrastructure
// Source: Deep Instinct (Apr 2024); Microsoft Threat Intelligence
// Confirmed dedicated C2 IPs (Deep Instinct, Microsoft, FortiGuard)
let DarkBeatC2_IPs = dynamic([
    "91.121.240.104", "91.121.240.102", "137.74.131.19",
    "164.132.237.68", "185.236.234.161", "157.20.182.75"
]);
let MuddyDomains = dynamic([
    "googlelinks.net", "googlevalues.com",
    "websiteapicloud.com", "nomercys.it.com"
]);
DeviceNetworkEvents
| where RemoteIP in (DarkBeatC2_IPs) or RemoteUrl has_any (MuddyDomains)
| project Timestamp, DeviceName, RemoteIP, RemoteUrl, RemotePort,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

**RustyWater C2 IP Detection (Shared Infrastructure)** KQL

DETECTION ONLY

MICROSOFT DEFENDER FOR ENDPOINT

```
// RULE: Detect connections to RustyWater C2 IPs (Tier 2: shared infrastructure)
// These IPs may be on shared hosting; require analyst review before action
// Source: CloudSEK (Jan 2026)
let RustyWaterC2 = dynamic([
    "159.198.66.153", "159.198.68.25", "161.35.228.250"
]);
DeviceNetworkEvents
| where RemoteIP in (RustyWaterC2)
| project Timestamp, DeviceName, RemoteIP, RemoteUrl, RemotePort,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

### MuddyWater Malware Hash Detection

KQL

**BLOCKING SAFE**

MICROSOFT DEFENDER FOR ENDPOINT

```
// RULE: Detect known MuddyWater malware file hashes on endpoints
let MuddyHashes = dynamic([
    "12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa",
    "dd7ee54b12a55bcc67da4ceaed6e636b7bd30d4db6f6c594e9510e1e605ade92",
    "94278fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7130c472",
    "b8703744744555ad841f922995cef5dbca11da22565195d05529f5f9095fbfca",
    "7ea4b307e84c8b32c0220eca13155a4cf66617241f96b8af26ce2db8115e3d53",
    "b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c",
    "42ca7d3fcd6d220cd380f34f9aa728b3bb68908b49f04d04f685631ee1f78986",
    "76aad2a7fa265778520398411324522c57bfd7d2ff30a5cfe6460960491bc552",
    "f38a56b8dc0e8a581999621eef65ef497f0ac0d35e953bd94335926f00e9464f",
    "9b5e36bb7518a9e333c31d09b589102f89e3425571dd434820ab3c437dc4e0d9"
]);
DeviceFileEvents
| where SHA256 in (MuddyHashes)
| project Timestamp, DeviceName, FileName, SHA256, FolderPath,
    InitiatingProcessFileName, ActionType
```

### Rclone Data Exfiltration

KQL

**DETECTION ONLY**

MICROSOFT DEFENDER FOR ENDPOINT

```
// RULE: Detect Rclone execution (used by MuddyWater for Wasabi exfiltration)
// Source: Broadcom/Symantec (Mar 2026)
DeviceProcessEvents
| where FileName =~ "rclone.exe" or ProcessCommandLine has "rclone"
| project Timestamp, DeviceName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

### Telegram Bot C2 Communication

KQL

**DETECTION ONLY**

MICROSOFT DEFENDER FOR ENDPOINT

```
// RULE: Detect non-browser processes connecting to Telegram API
// Source: Group-IB Operation Olalampo (Feb 2026); Mandiant UNC3313 (Feb 2022)
DeviceNetworkEvents
| where RemoteUrl has "api.telegram.org"
| where InitiatingProcessFileName !in~ (
    "Telegram.exe", "Teams.exe", "slack.exe",
    "chrome.exe", "msedge.exe", "firefox.exe", "safari"
)
| project Timestamp, DeviceName, InitiatingProcessFileName,
    InitiatingProcessCommandLine, RemoteUrl, RemoteIP
| sort by Timestamp desc
```

## Sigma Rule: Unauthorized RMM Tool Execution

**Sigma Rule Disclaimer**

This Sigma rule requires conversion to your SIEM's native query language using sigmac or pySigma. Test thoroughly in a non-production environment before deployment. Adjust the exclusion list for RMM tools authorized in your environment.

**DETECTION ONLY**

SIGMA (YAML)

```
title: MuddyWater RMM Tool Execution
id: b2c3d4e5-f6a7-8901-bcde-muddywater001
status: experimental
description: |
    Detects execution of Remote Monitoring and Management tools
    associated with MuddyWater campaigns. These are legitimate tools;
    detection indicates unauthorized installation, not confirmed compromise.
references:
    - https://harfanglab.io/insidethelab/muddywater-rmm-campaign/
    - https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-055a
    - https://www.group-ib.com/blog/muddywater-operation-olalampo/
author: Intruvent Technologies
date: 2026-03-11
tags:
    - attack.persistence
    - attack.t1219
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image|endswith:
            - '\AteraAgent.exe'
            - '\ScreenConnect.ClientService.exe'
            - '\SimpleHelp.exe'
            - '\AnyDesk.exe'
            - '\Syncro.Overmind.Service.exe'
            - '\rutserv.exe'
            - '\rfusclient.exe'
    filter_authorized:
        Image|contains:
            - 'C:\Program Files\YourApprovedRMM'
    condition: selection and not filter_authorized
falsepositives:
    - Legitimate IT-deployed RMM tools (update filter_authorized)
    - MSP-managed environments with authorized RMM agents
level: medium
```

## YARA Rule: UDPGangster Backdoor

**BLOCKING SAFE**

YARA

```
rule MuddyWater_UDPGangster {
    meta:
        description = "Detects UDPGangster backdoor used by MuddyWater"
        author = "Intruvent Technologies"
        date = "2026-03-11"
        reference = "FortiGuard Labs (Dec 2025)"
        tlp = "TLP:CLEAR"
        hash = "7ea4b307e84c8b32c0220eca13155a4cf66617241f96b8af26ce2db8115e3d53"

    strings:
        $mutex = "xhxhxhxhxhxpp" ascii wide
        $pdb = "gangster" ascii
        $path1 = "\\RoamingLow\\SystemProc.exe" ascii wide
        $path2 = "\\Users\\Public\\ui.txt" ascii wide
        $udp_port = { F5 04 }  // Port 1269, little-endian (x86 byte order)

    condition:
        uint16(0) == 0x5A4D and
        ($mutex or $pdb) and
        (1 of ($path*))
}
```

### YARA Rule: RustyWater RAT Artifacts

**BLOCKING SAFE**

YARA

```
rule MuddyWater_RustyWater {
    meta:
        description = "Detects RustyWater/Archer RAT Rust-based implant artifacts"
        author = "Intruvent Technologies"
        date = "2026-03-11"
        reference = "CloudSEK (Jan 2026)"
        tlp = "TLP:CLEAR"
        hash = "76aad2a7fa265778520398411324522c57bfd7d2ff30a5cfe6460960491bc552"

    strings:
        $path1 = "CertificationKit.ini" ascii wide
        $path2 = "reddit.exe" ascii wide
        $domain = "nomercys" ascii
        $rust1 = "reqwest" ascii
        $rust2 = "tokio" ascii

    condition:
        uint16(0) == 0x5A4D and
        ((2 of ($path*, $domain)) or
        ($domain and 1 of ($rust*)))
}
```

## C Appendix C: 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] **MITRE ATT&CK** - Group G0069: MuddyWater
attack.mitre.org

## Vendor Threat Intelligence (Primary)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Investigative Journalism

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

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

## OSINT and Analyst Research

[22] **PolySwarm** - "MuddyWater's UDPGangster Backdoor"

blog.polyswarm.io

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

[24] **Deep Instinct GitHub** - PhonyC2 MuddyWater Research
github.com/deepinstinct

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

## Secondary Sources

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

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

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

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

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

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

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