INTRUVENT

COMPREHENSIVE THREAT HUNTING GUIDE

MDM/Intune Weaponization

Hunting for Handala (Void Manticore) MDM Abuse in Microsoft Intune Environments

Version 1.0
Published March 11, 2026
Trigger Event Stryker Corporation Attack
Classification TLP:CLEAR
Total Hunt Time 4.5–5.5 Hours
Target Sectors Healthcare, MedTech, Critical Infrastructure

Intruvent Technologies
INT-THG-2026-HANDALA-MDM-v1.0

Table of Contents

Overview

Executive Summary 3
MITRE ATT&CK Mapping 4

Hunt Modules

Module 1: Intune Admin Account Audit 5
Module 2: Intune Wipe/Retire Event Analysis 6
Module 3: Graph API Endpoint Monitoring 7
Module 4: Conditional Access and PIM Review 8
Module 5: Starlink and Anomalous ISP Detection 9
Module 6: Endpoint Wiper Artifact Hunt 10
Module 7: Intune Script and Config Profile Review 11
Module 8: Telegram Exfiltration Channel Detection 12
Module 9: Scarred Manticore Precursor Hunt 13
Module 10: BYOD and Mobile Device Exposure Assessment 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
Void Manticore / Storm-0842 (MOIS, Iran)

PRIMARY TARGETS
Microsoft Intune / MDM Environments

TRIGGER EVENT
Stryker Corporation, March 11, 2026

TARGET SECTORS
Healthcare, MedTech, Critical Infrastructure

NOVEL TTP
T1072 Software Deployment Tools via MDM

BUSINESS IMPACT
Mass device wipe across all enrolled platforms

On March 11, 2026, the Handala hacktivist persona (assessed with high confidence as Iran's MOIS-linked **Void Manticore / Storm-0842**) claimed responsibility for a destructive wiper attack against **Stryker Corporation** (NYSE: SYK), a $100B+ medical technology company with 56,000+ employees across 60+ countries. According to multiple investigative reports (Krebs on Security, Zetter Zero Day, CNN), the attackers compromised Microsoft Intune MDM administration and pushed remote wipe commands across all enrolled devices, including Windows, macOS, iOS, and Android endpoints. Confirmed impacts include SYK shares falling approximately 4.5%, the Cork, Ireland HQ shutting down (affecting 4,000–5,500 employees), manufacturing systems going offline, and the Handala logo being displayed on all login screens. Employees resorted to WhatsApp for communication, and personal BYOD devices enrolled in Intune were also wiped.

Handala claimed 200,000+ systems wiped and 50TB of data exfiltrated; these figures remain **unverified**. The initial access vector has not been publicly disclosed. **[REQUIRES VERIFICATION]**

This guide provides **10 hunt modules** specifically designed to help defenders detect MDM abuse, audit Intune configurations, and hunt for precursor Void Manticore activity. The modules cover Intune admin account auditing, bulk wipe detection, Graph API monitoring, Conditional Access review, Starlink ISP detection, endpoint wiper artifacts, Intune script review, Telegram C2 detection, Scarred Manticore precursor hunting, and BYOD exposure assessment. Total estimated hunt time is **4.5–5.5 hours**.

Threat Overview

Void Manticore (also tracked as **Storm-0842** by Microsoft, **Banished Kitten** by CrowdStrike) is the destructive operations unit of Iran's Ministry of Intelligence and Security (MOIS). The group operates under the public-facing persona "Handala Hack Team" and has escalated from web shell deployments in Albania (2022) to custom wiper malware families against Israel (2023–2024) to MDM weaponization against a multinational corporation (2026).

The Stryker attack represents a significant escalation in capability. Rather than deploying traditional wiper malware to individual endpoints, the attackers weaponized a legitimate enterprise management tool to execute destruction at scale. A single compromised Intune administrator account can push wipe, retire, or reset commands to every enrolled device in the organization, across all platforms and geographies simultaneously.

Check Point Research has documented a "one-two punch" operational model: **Scarred Manticore** (Storm-0861) conducts the initial espionage intrusion, then hands off access to Void Manticore for destructive operations. Defenders should hunt for both espionage precursors and destructive indicators.

KEY CHARACTERISTICS

- MOIS state-sponsored (Iran)
- MDM/Intune weaponization (novel)
- 6+ custom wiper families
- BYOVD privilege escalation
- Process hollowing (RegAsm.exe)
- Telegram bot C2
- Starlink connectivity (Jan 2026+)
- Scarred Manticore handoff model
- ASPX web shell deployment
- Psychological warfare operations

2 MITRE ATT&CK Mapping

The following techniques have been observed in Void Manticore / Handala campaigns, with sources from CISA, Check Point, Splunk, and Trellix:

`T1078.004`
Valid Accounts: Cloud Accounts
Compromised Intune/Entra ID administrator credentials to access MDM console

`T1072` NOVEL
Software Deployment Tools
Weaponized Microsoft Intune MDM to push remote wipe commands across enrolled devices globally

`T1566`
Phishing
CrowdStrike-themed phishing emails (Jul 2024) from crowdstrike.com.vc with PDF lures

`T1190`
Exploit Public-Facing Application
CVE-2019-0604 (SharePoint) in Albania; probing external apps for misconfigurations (Jan 2026+)

`T1059.010`
AutoIT/AutoHotKey
AutoIt script (.a3x) used as intermediate loader in CrowdStrike-themed wiper chain

`T1068`
Exploitation for Privilege Escalation
BYOVD using ListOpenedFileDrv_32.sys and rwdsk.sys (ElRawDisk) for raw disk access

`T1055.012`
Process Hollowing
Wiper payload injected into RegAsm.exe via process hollowing; ntdll.dll unhooking for EDR bypass

`T1485`
Data Destruction
BiBi wiper corrupts files with random data; partition wipers destroy MBR/GPT

`T1561`
Disk Wipe
LowEraser, Pinky, JustMBR partition wipers using IOCTL_DISK_DELETE_DRIVE_LAYOUT

`T1491`
Defacement
Handala logo displayed on Stryker login screens; "Karma" and "Homeland Justice" defacement pages

`T1102`
Web Service
Telegram bots used for wiper C2 communications and data exfiltration

3 Hunt Modules

1 Intune Admin Account Audit

Duration: 30 min Priority: CRITICAL

Objective: Identify unauthorized or compromised Intune administrator accounts that could be used to push destructive MDM commands.

Background

In the Stryker attack, administrative access to Microsoft Intune enabled the attacker to push remote wipe commands across all enrolled devices globally. The first step in any MDM hunt is to audit who holds administrative privileges and whether those accounts show signs of compromise. Focus on Intune Administrator, Global Administrator, and any custom roles with device management permissions.

Hunt Procedure: List All Intune/Global Admin Role Assignments

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// List all users with Intune Administrator or Global Administrator roles
AuditLogs
| where OperationName == "Add member to role"
| where TargetResources has_any ("Intune Administrator", "Global Administrator")
| project TimeGenerated, InitiatedBy.user.userPrincipalName,
    TargetResources[0].userPrincipalName, TargetResources[0].modifiedProperties
| sort by TimeGenerated desc
```

Hunt Procedure: Recently Added Admin Accounts (Last 90 Days)

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect admin role assignments in the past 90 days
AuditLogs
| where TimeGenerated > ago(90d)
| where OperationName has_any ("Add member to role", "Add eligible member to role")
| where TargetResources has_any ("Intune Administrator", "Global Administrator",
    "Cloud Device Administrator")
| project TimeGenerated, AddedBy=InitiatedBy.user.userPrincipalName,
    NewAdmin=TargetResources[0].userPrincipalName, RoleName=OperationName
| sort by TimeGenerated desc
```

Hunt Procedure: Admin Sign-in Anomaly Detection

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Review admin account sign-in patterns for anomalies
let IntuneAdmins = AuditLogs
    | where OperationName has "Add member to role"
    | where TargetResources has "Intune Administrator"
    | distinct tostring(TargetResources[0].userPrincipalName);
SigninLogs
| where UserPrincipalName in (IntuneAdmins)
| where TimeGenerated > ago(30d)
| project TimeGenerated, UserPrincipalName, IPAddress, Location,
    AppDisplayName, DeviceDetail, RiskState, ConditionalAccessStatus
| sort by TimeGenerated desc
```

- ☐ Cross-reference all Intune admins against authorized personnel list from IT management
- ☐ Verify no service accounts have been granted admin roles outside of change control
- ☐ Check for admin accounts signing in from unusual locations, new devices, or new IP ranges
- ☐ Confirm all admin accounts have phishing-resistant MFA enforced (FIDO2, Windows Hello)

Critical Finding Indicator

Any admin role assignment that cannot be traced to an authorized change request warrants immediate investigation. Unauthorized Intune admin access is the prerequisite for MDM-based wipe attacks.

2 Intune Wipe/Retire Event Analysis

Duration: 30 min Priority: CRITICAL

Objective: Detect anomalous or bulk wipe, retire, and factory reset commands in Intune audit logs that may indicate MDM weaponization.

Background

The core destructive action in the Stryker attack was pushing wipe commands through Microsoft Intune to enrolled devices across all platforms. In normal operations, wipe and retire actions are infrequent, targeted, and tied to specific IT tickets (employee offboarding, lost/stolen devices). A burst of wipe commands, especially outside business hours or originating from a single account, is a high-fidelity indicator of MDM abuse.

Hunt Procedure: Intune Wipe/Retire/Reset Operations

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect all wipe, retire, and reset operations from Intune audit logs
// NOTE: LoggedByService == "Intune" requires Intune diagnostic settings
// routed to your workspace. If no results, try filtering on OperationName only.
AuditLogs
| where LoggedByService == "Intune"
| where OperationName has_any ("Wipe", "Retire", "Reset", "remoteLock",
    "cleanWindowsDevice", "windowsDefenderScan")
| project TimeGenerated, OperationName, InitiatedBy.user.userPrincipalName,
    TargetResources[0].displayName, Result
| sort by TimeGenerated desc
```

Hunt Procedure: Threshold Alert for Bulk Wipe Activity

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Alert if more than 10 wipe/retire commands issued per hour by any single user
AuditLogs
| where LoggedByService == "Intune"
| where OperationName has_any ("Wipe", "Retire", "Reset")
| summarize WipeCount=count() by bin(TimeGenerated, 1h),
    Initiator=tostring(InitiatedBy.user.userPrincipalName)
| where WipeCount > 10
| sort by WipeCount desc
```

Hunt Procedure: Correlate Wipe Initiator with Known Admins

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Identify wipe commands issued by accounts not in the authorized admin list
let AuthorizedAdmins = dynamic(["admin1@company.com", "admin2@company.com"]); // Update with your authorized list
AuditLogs
| where LoggedByService == "Intune"
| where OperationName has_any ("Wipe", "Retire", "Reset")
| extend Initiator = tostring(InitiatedBy.user.userPrincipalName)
| where Initiator !in (AuthorizedAdmins)
| project TimeGenerated, OperationName, Initiator,
    TargetDevice=TargetResources[0].displayName
| sort by TimeGenerated desc
```

Critical: Bulk Wipe Threshold

In normal operations, an organization rarely exceeds 5–10 wipe commands per day. Any single account issuing more than 10 wipe commands per hour should trigger an immediate investigation. In the Stryker attack, wipe commands were reportedly pushed to devices across 60+ countries simultaneously.

3 Graph API Endpoint Monitoring

Duration: 20 min Priority: HIGH

Objective: Detect unauthorized or scripted Microsoft Graph API calls to Intune device management endpoints that could automate mass device wipe operations.

Background

Microsoft Intune management can be fully automated via the Microsoft Graph API. The `deviceManagement/managedDevices` endpoint supports POST actions including `/wipe`, `/retire`, `/resetPasscode`, and `/cleanWindowsDevice`. An attacker with a compromised admin token or service principal could script mass wipe operations without ever touching the Intune portal UI. This makes Graph API monitoring essential for detecting automated MDM abuse.

Prerequisite: MicrosoftGraphActivityLogs Table

The queries in this module use the `MicrosoftGraphActivityLogs` table, which requires Microsoft Graph activity logs to be routed to your Log Analytics workspace via diagnostic settings. If this table is empty or missing, configure it in the Azure portal under Microsoft Entra ID > Diagnostic settings > MicrosoftGraphActivityLogs. Without this configuration, these queries will return no results.

Hunt Procedure: Monitor Destructive Graph API Calls

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect POST requests to Intune device management destructive endpoints
MicrosoftGraphActivityLogs
| where RequestMethod == "POST"
| where RequestUri has_any ("/managedDevices/", "/deviceManagement/")
| where RequestUri has_any ("/wipe", "/retire", "/resetPasscode",
    "/cleanWindowsDevice", "/remoteLock", "/deleteUserFromSharedAppleDevice")
| project TimeGenerated, RequestMethod, RequestUri, UserAgent,
    ServicePrincipalId, UserId, ResponseStatusCode
| sort by TimeGenerated desc
```

Hunt Procedure: Unusual Service Principal Access to Intune APIs

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect service principals accessing Intune device management endpoints
MicrosoftGraphActivityLogs
| where RequestUri has "/deviceManagement/"
| where isnotempty(ServicePrincipalId)
| summarize RequestCount=count(), Endpoints=make_set(RequestUri)
    by ServicePrincipalId, bin(TimeGenerated, 1h)
| where RequestCount > 50
| sort by RequestCount desc
```

Hunt Procedure: Unusual Graph API Caller Patterns

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Identify unusual user agents or rapid-fire Graph API calls (scripted behavior)
MicrosoftGraphActivityLogs
| where RequestUri has "/deviceManagement/"
| summarize RequestCount=count(), DistinctEndpoints=dcount(RequestUri),
    UserAgents=make_set(UserAgent) by UserId, bin(TimeGenerated, 15m)
| where RequestCount > 100 or DistinctEndpoints > 20
| sort by RequestCount desc
```

What to Look For

Legitimate Intune automation (e.g., compliance scripts) will use known service principals with predictable patterns. Suspicious indicators include: new service principals accessing device management APIs, high-volume POST requests to wipe endpoints, unusual user agents (e.g., Python, PowerShell, curl), and activity outside business hours.

4 Conditional Access and PIM Review

Duration: 25 min Priority: HIGH

Objective: Verify that Conditional Access policies protect MDM administrator accounts and that Privileged Identity Management (PIM) is properly configured for just-in-time admin access.

Background

Conditional Access policies and Privileged Identity Management (PIM) are the primary controls preventing unauthorized admin access to Intune. If an attacker compromises admin credentials but Conditional Access requires phishing-resistant MFA from a compliant device, the credentials alone are insufficient. Similarly, PIM ensures admin roles are not permanently assigned, reducing the window of opportunity. This module audits these controls for gaps.

Hunt Procedure: Conditional Access Gap Analysis

INVESTIGATION AID

KQL (MICROSOFT SENTINEL)

```
// Identify admin sign-ins that bypassed Conditional Access
SigninLogs
| where TimeGenerated > ago(30d)
| where UserPrincipalName in ("admin1@company.com", "admin2@company.com") // Replace with your admin list
| where ConditionalAccessStatus != "success"
| project TimeGenerated, UserPrincipalName, IPAddress, AppDisplayName,
    ConditionalAccessStatus, ConditionalAccessPolicies
| sort by TimeGenerated desc
```

Hunt Procedure: Check for Excluded Users/Groups in CA Policies

INVESTIGATION AID

KQL (MICROSOFT SENTINEL)

```
// Identify sign-ins where CA policies were not applied (excluded users)
SigninLogs
| where TimeGenerated > ago(30d)
| where ConditionalAccessStatus == "notApplied"
| where AppDisplayName has_any ("Microsoft Intune", "Microsoft Graph",
    "Azure Portal", "Microsoft Endpoint Manager")
| project TimeGenerated, UserPrincipalName, IPAddress,
    AppDisplayName, ConditionalAccessStatus
| summarize Count=count() by UserPrincipalName, AppDisplayName
| sort by Count desc
```

Hunt Procedure: PIM Role Activation Review

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Review PIM role activations for Intune admin roles
AuditLogs
| where OperationName has_any ("Add member to role in PIM completed",
    "Add eligible member to role in PIM requested")
| where TargetResources has_any ("Intune Administrator", "Global Administrator")
| project TimeGenerated, OperationName,
    ActivatedBy=InitiatedBy.user.userPrincipalName,
    Role=TargetResources[0].displayName, Result
| sort by TimeGenerated desc
```

Manual Review Checklist

- ☐ Verify phishing-resistant MFA (FIDO2, Windows Hello, certificate-based) is required for all Intune admin accounts
- ☐ Confirm no users or groups are excluded from Conditional Access policies targeting admin roles
- ☐ Verify PIM is enabled and all Intune admin roles require just-in-time activation (not persistent assignment)
- ☐ Check that PIM activations require approval and have maximum activation durations (e.g., 8 hours)
- ☐ Confirm that break-glass accounts are monitored and their usage triggers alerts
- ☐ Verify that Conditional Access policies require compliant/hybrid-joined devices for admin portal access

Common Gaps

The most dangerous configuration gap is a permanently assigned Global Administrator account without phishing-resistant MFA. Organizations that rely on SMS or push-notification MFA remain vulnerable to real-time phishing and MFA fatigue attacks. Also verify that legacy authentication protocols are blocked for admin accounts.

5 Starlink and Anomalous ISP Detection

Duration: 20 min Priority: MEDIUM

Objective: Detect sign-ins from Starlink (AS14593) and other anomalous ISPs associated with Handala operational infrastructure.

Background

Since January 2026, Check Point Research observed Handala campaigns originating from Starlink IP ranges (AS14593). Iran's internet connectivity is severely restricted, but Starlink terminals are widely smuggled into the country. This provides Handala operatives with connectivity that bypasses Iranian internet infrastructure. Additionally, Void Manticore has historically used Vultr cloud hosting (64.176.0.0/12) for C2 infrastructure.

Shared Infrastructure Warning

AS14593 (Starlink) serves millions of legitimate subscribers worldwide. This is a **DETECTION query for analyst review**. Do NOT deploy as an automated blocking rule. Blocking Starlink would disrupt legitimate remote workers, travelers, and rural employees who rely on satellite internet.

Hunt Procedure: Starlink ASN Sign-in Detection

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect sign-ins from Starlink (AS14593)
// WARNING: Shared infrastructure. For alerting only, NOT blocking.
SigninLogs
| where AutonomousSystemNumber == 14593
| project TimeGenerated, UserPrincipalName, IPAddress,
    Location, AppDisplayName, DeviceDetail,
    RiskState, ConditionalAccessStatus
| sort by TimeGenerated desc
```

Hunt Procedure: Vultr IP Range Sign-in Detection

BLOCKING SAFE

KQL (MICROSOFT SENTINEL)

```
// Detect sign-ins from known Void Manticore C2 IPs on Vultr
// These specific IPs were confirmed as C2 by Check Point Research
let VultrC2IPs = dynamic(["64.176.169.22", "64.176.172.235",
    "64.176.172.165", "64.176.173.77", "64.176.172.101"]);
SigninLogs
| where IPAddress in (VultrC2IPs)
| project TimeGenerated, UserPrincipalName, IPAddress,
    Location, AppDisplayName, RiskState, ResultType
| sort by TimeGenerated desc
```

Hunt Procedure: Broader Vultr Range Monitoring

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Monitor sign-ins from the broader Vultr range (64.176.0.0/16)
// Vultr is a cloud provider; this is for alerting only
SigninLogs
| where IPAddress startswith "64.176."
| where IPAddress !in (dynamic(["64.176.169.22", "64.176.172.235",
    "64.176.172.165", "64.176.173.77", "64.176.172.101"]))
| summarize SignInCount=count(), Users=make_set(UserPrincipalName),
    Apps=make_set(AppDisplayName)
    by IPAddress, bin(TimeGenerated, 1d)
| where SignInCount > 3
| sort by SignInCount desc
```

Triage Guidance

For Starlink sign-ins: cross-reference the user with HR/IT records to determine if the employee legitimately uses Starlink (remote workers, rural locations). For Vultr C2 IP matches: escalate immediately; these are confirmed Void Manticore infrastructure. For broader Vultr range matches: investigate the account and verify the sign-in is expected.

6 Endpoint Wiper Artifact Hunt

Duration: 45 min Priority: HIGH

Objective: Hunt for Handala wiper malware artifacts on endpoints, including file hashes, behavioral indicators, BYOVD drivers, and process hollowing patterns.

Background

Handala has deployed six or more wiper families since 2022: CL Wiper, BiBi (Linux and Windows), Hatef, Hamsa, LowEraser, Pinky, and JustMBR. Even if MDM was the primary destruction vector in the Stryker attack, traditional wiper deployment remains in their playbook. The CrowdStrike-themed campaign (July 2024) demonstrated a sophisticated attack chain: NSIS installer, Carroll batch script with garbage code obfuscation, AutoIt script, process hollowing into RegAsm.exe, and wiper execution with BYOVD for privilege escalation.

Hunt Procedure: Hash-Based Detection

BLOCKING SAFE

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect known Handala wiper hashes on endpoints
let HandalaHashes = dynamic([
    "d0c03d40772cd468325bbc522402f7b737f18b8f37a89bacc5c8a00c2b87bfc6",
    "deeaf85b2725289d5fc262b4f60dda0c68ae42d8d46d0dc19b9253b451aea25a",
    "87f0a902d6b2e2ae3647f10ea214d19db9bd117837264ee15d622b5314ff03d5",
    "85fa58cc8c4560adb955ba0ae9b9d6cab2c381d10dbd42a0bceb8b62a92b7636",
    "74d8d60e900f931526a911b7157511377c0a298af986d42d373f51aac4f362f6",
    "cc77e8ab73b577de1924e2f7a93bcfd852b3c96c6546229bc8b80bf3fd7bf24e",
    "40417e937cd244b2f928150cae6fa0eff5551fdb401ea072f6ecdda67a747e17",
    "96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8",
    "19001dd441e50233d7f0addb4fcd405a70ac3d5e310ff20b331d6f1a29c634f0",
    "8316065c4536384611cbe7b6ba6a5f12f10db09949e66cb608c92ae8b69e4d67",
    "9e519211947c63d9bf6f4a51bc161f5b9ace596c2935a8eedfce4057f747b961",
    "fe07dca68f288a4f6d7cbd34d79bb70bc309635876298d4fde33c25277e30bd2",
    "ca9bf13897af109cb354f2629c10803966eb757ee4b2e468abc04e7681d0d74a",
    "f116acc6508843f59e59fb5a8d643370dce82f492a217764521f46a856cc4cb5",
    "e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05acc948b8b965480ca0",
    "3c9dc8ada56adf9cebfc501a2d3946680dcb0534a137e2e27a7fcb5994cd9de6",
    "7ad64b64e0a4e510be42ba631868bbda8779139dc0daad9395ab048306cc83c5",
    "45bf0057b3121c6e444b316afafdd802d16083282d1cbfde3cdbf2a9d0915ace",
    "cad2bc224108142b5aa19d787c19df236b0d12c779273d05f9b0298a63dc1fe5"
]);
DeviceFileEvents
| where SHA256 in (HandalaHashes)
| project Timestamp, DeviceName, FileName, SHA256, FolderPath, ActionType
```

Hunt Procedure: BiBi Wiper File Extension Pattern

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect files being renamed with ".BiBi" extension (BiBi wiper indicator)
DeviceFileEvents
| where ActionType == "FileRenamed"
| where FileName endswith ".BiBi"
| project Timestamp, DeviceName, FileName, FolderPath,
    InitiatingProcessFileName, InitiatingProcessCommandLine
```

Hunt Procedure: RegAsm.exe Process Hollowing Detection

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect RegAsm.exe launched with no arguments or with network connections
// Handala hollows wiper payload into RegAsm.exe
DeviceProcessEvents
| where FileName =~ "RegAsm.exe"
| where ProcessCommandLine == FileName
    or ProcessCommandLine endswith "RegAsm.exe"
    or ProcessCommandLine == ""
| project Timestamp, DeviceName, ProcessCommandLine,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| join kind=inner (
    DeviceNetworkEvents
    | where InitiatingProcessFileName =~ "RegAsm.exe"
    | project NetworkTimestamp=Timestamp, DeviceName, RemoteIP, RemoteUrl
) on DeviceName
| where abs(datetime_diff('second', Timestamp, NetworkTimestamp)) < 300
| project Timestamp, DeviceName, ProcessCommandLine,
    InitiatingProcessFileName, RemoteIP, RemoteUrl
| sort by Timestamp desc
```

Hunt Procedure: BYOVD Driver Detection

BLOCKING SAFE

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect known Handala BYOVD drivers
DeviceFileEvents
| where FileName in~ ("ListOpenedFileDrv_32.sys", "rwdsk.sys")
| project Timestamp, DeviceName, FileName, FolderPath, SHA256,
    InitiatingProcessFileName
```

Hunt Procedure: Shadow Copy Deletion

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect shadow copy deletion (common wiper pre-step)
DeviceProcessEvents
| where ProcessCommandLine has_any ("vssadmin delete shadows",
    "wmic shadowcopy delete", "bcdedit /set {default} recoveryenabled no")
| project Timestamp, DeviceName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
```

Critical: Any Hash Match Is High Confidence

All hashes in the detection query above are confirmed malicious from published vendor research (Check Point, Splunk, Trellix, CISA, Intezer). A match on any hash warrants immediate endpoint isolation and forensic investigation.

7 Intune Script and Config Profile Review

Duration: 30 min Priority: HIGH

Objective: Identify malicious or unauthorized scripts and configuration profiles deployed via Intune that could serve as backdoors or deliver destructive payloads.

Background

Beyond wipe commands, attackers with Intune admin access can deploy malicious PowerShell scripts, shell scripts, or configuration profiles to managed devices. Intune supports script deployment to Windows, macOS, and Linux endpoints. An attacker could use this capability to deploy wiper malware, establish persistence, exfiltrate data, or disable security controls across the entire fleet. Remediation scripts (Proactive Remediations) execute on a recurring schedule and could serve as persistent backdoors.

Hunt Procedure: List Recently Added/Modified Scripts

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect new or modified Intune script deployments
AuditLogs
| where LoggedByService == "Intune"
| where OperationName has_any ("DeviceManagementScript", "Script",
    "deviceShellScript", "deviceCustomAttributeShellScript")
| where OperationName has_any ("Create", "Update", "Patch")
| project TimeGenerated, OperationName,
    ModifiedBy=InitiatedBy.user.userPrincipalName,
    TargetResources, Result
| sort by TimeGenerated desc
```

Hunt Procedure: Detect LOLBin Execution via Intune Scripts

INVESTIGATION AID

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect LOLBin execution spawned by Intune Management Extension
// NOTE: powershell.exe and cmd.exe are legitimately spawned by Intune for
// every script deployment. Focus triage on unexpected LOLBins (mshta, certutil,
// bitsadmin, regsvr32, rundll32) and review command lines for encoded payloads.
DeviceProcessEvents
| where InitiatingProcessFileName =~ "IntuneManagementExtension.exe"
    or InitiatingProcessFileName =~ "AgentExecutor.exe"
| where FileName in~ ("powershell.exe", "cmd.exe", "wscript.exe",
    "cscript.exe", "mshta.exe", "certutil.exe", "bitsadmin.exe",
    "regsvr32.exe", "rundll32.exe")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName
| sort by Timestamp desc
```

Hunt Procedure: Configuration Profile Changes

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Monitor configuration profile creation and modification
AuditLogs
| where LoggedByService == "Intune"
| where OperationName has_any ("deviceConfiguration", "DeviceConfiguration",
    "compliancePolicy", "deviceEnrollmentConfiguration")
| where OperationName has_any ("Create", "Update", "Patch", "Delete")
| project TimeGenerated, OperationName,
    ModifiedBy=InitiatedBy.user.userPrincipalName,
    Details=TargetResources[0].modifiedProperties
| sort by TimeGenerated desc
```

Manual Review Checklist

- ☐ In the Intune portal, review all PowerShell scripts under Devices > Scripts. Verify each script's purpose and author.
- ☐ Review all Proactive Remediation scripts; check for any that download files, execute encoded commands, or modify security settings
- ☐ Audit all configuration profiles for unexpected changes to firewall rules, Defender exclusions, or credential settings
- ☐ Check for recently created Win32 app deployments that could deliver malicious payloads
- ☐ Review app protection policies for unexpected modifications that could weaken data protection

Proactive Remediations as Backdoors

Proactive Remediation scripts run on a recurring schedule (hourly, daily, or custom). An attacker could create a detection script that always returns "non-compliant" paired with a remediation script that executes their payload. Review all remediation scripts for encoded commands, download cradles, or reverse shells.

8 Telegram Exfiltration Channel Detection

Duration: 20 min Priority: MEDIUM

Objective: Detect processes communicating with the Telegram API for command-and-control or data exfiltration purposes.

Background

Handala uses Telegram bots for wiper C2 communications, confirmed across multiple campaigns. The CrowdStrike-themed wiper (July 2024) used Bot Key `7277950797:AAF99Nw5rAT1BHnMmwY_tQNYJFU3dYJ5RHc` with Chat ID `7436061126` (source: Trellix). The HamsaUpdate/Hatef wiper used Bot ID `6428401585` with Channel ID `6932028002` (source: Intezer, Splunk). Telegram's legitimate use in many organizations makes blocking impractical; instead, focus on identifying non-Telegram-client processes connecting to the Telegram API.

Hunt Procedure: Non-Client Telegram API Connections

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect processes connecting to Telegram API that are NOT the Telegram client
// Legitimate Telegram usage will appear; focus on unexpected process names
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
```

Hunt Procedure: Telegram Bot Key Detection in Process Command Lines

BLOCKING SAFE

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Hunt for known Handala Telegram bot keys in command lines or file content
let HandalaBotKeys = dynamic([
    "7277950797:AAF99Nw5rAT1BHnMmwY_tQNYJFU3dYJ5RHc",  // CrowdStrike-themed campaign (source: Trellix)
    "6428401585"  // Hatef/Hamsa campaign bot ID (source: Intezer); full token not publicly available
]);
DeviceProcessEvents
| where ProcessCommandLine has_any (HandalaBotKeys)
| project Timestamp, DeviceName, FileName, ProcessCommandLine, AccountName
```

Triage Guidance

Focus on unexpected processes making Telegram API calls: PowerShell, cmd.exe, Python, RegAsm.exe, or any unknown executable. Browser-based Telegram Web access will appear through browser process names and can be filtered. A bot key match from the second query is a high-confidence Handala indicator.

9 Scarred Manticore Precursor Hunt

Duration: 30 min Priority: MEDIUM

Objective: Hunt for Scarred Manticore (Storm-0861) espionage indicators that often precede Void Manticore destructive operations.

Background

Check Point Research documented a structured collaboration model between two MOIS units: **Scarred Manticore** (Storm-0861) conducts initial espionage intrusions, establishes persistent access, and exfiltrates intelligence. When the decision is made to shift to destruction, access is handed off to **Void Manticore** (Storm-0842). This "one-two punch" was observed in the Albania campaign and multiple Israel operations. Detecting Scarred Manticore indicators provides an early warning that destructive operations may follow.

Hunt Procedure: ASPX Web Shell Detection

BLOCKING SAFE

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Hunt for known Scarred Manticore / Void Manticore web shell filenames
let KnownWebShells = dynamic([
    "error4.aspx", "pickers.aspx", "ClientBin.aspx",
    "evaluatesiteupgrade.cs.aspx"
]);
DeviceFileEvents
| where FileName in~ (KnownWebShells)
| project Timestamp, DeviceName, FileName, FolderPath, SHA256,
    InitiatingProcessFileName
| sort by Timestamp desc
```

Hunt Procedure: Karma Shell Behavioral Detection

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect ASPX files with characteristics of Karma Shell
// Karma Shell uses base64 + XOR (key: 23) obfuscation
DeviceFileEvents
| where FileName endswith ".aspx"
| where ActionType == "FileCreated"
| where FolderPath has_any ("inetpub", "wwwroot", "OWA", "Exchange")
| project Timestamp, DeviceName, FileName, FolderPath, SHA256,
    InitiatingProcessFileName
| sort by Timestamp desc
```

Hunt Procedure: Unusual IIS Worker Process Activity

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect suspicious child processes spawned by IIS (w3wp.exe)
DeviceProcessEvents
| where InitiatingProcessFileName =~ "w3wp.exe"
| where FileName in~ ("cmd.exe", "powershell.exe", "certutil.exe",
    "bitsadmin.exe", "net.exe", "net1.exe", "whoami.exe",
    "systeminfo.exe", "ipconfig.exe")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessCommandLine
| sort by Timestamp desc
```

Hunt Procedure: Connections to Vultr C2 IPs

BLOCKING SAFE

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect endpoint connections to confirmed Void Manticore C2 infrastructure
DeviceNetworkEvents
| where RemoteIP in ("64.176.169.22", "64.176.172.235",
    "64.176.172.165", "64.176.173.77", "64.176.172.101")
| project Timestamp, DeviceName, InitiatingProcessFileName,
    RemoteIP, RemotePort, RemoteUrl
| sort by Timestamp desc
```

Espionage Precedes Destruction

If Scarred Manticore indicators are found, the organization may already be in the espionage phase. Void Manticore destructive operations could follow at any time. Prioritize incident response and consider proactive Intune admin account lockdown while investigating.

10 BYOD and Mobile Device Exposure Assessment

Duration: 20 min Priority: MEDIUM

Objective: Assess exposure of personal BYOD devices to Intune wipe actions and verify that enrollment policies limit destructive capabilities on personal devices.

Background

In the Stryker attack, personal devices enrolled in Intune were also wiped, according to reporting by Zetter Zero Day. Employees were instructed to remove Intune, Company Portal, Microsoft Teams, and VPN applications from personal devices. This highlights a critical risk: when personal devices are enrolled in MDM with full wipe capabilities, an attacker who compromises Intune administration can destroy employees' personal data, photos, and applications. Organizations must distinguish between corporate and personal device enrollment and enforce selective wipe (corporate data only) for BYOD.

Hunt Procedure: Inventory Devices by Ownership Type

INVESTIGATION AID

KQL (MICROSOFT SENTINEL)

```
// Inventory enrolled devices by ownership type (Corporate vs Personal)
IntuneDevices
| where isnotempty(DeviceName)
| summarize DeviceCount=count() by OwnerType, OS, ComplianceState
| sort by DeviceCount desc
```

Hunt Procedure: Identify Personal Devices with Full Wipe Capability

INVESTIGATION AID

KQL (MICROSOFT SENTINEL)

```
// List personal (BYOD) devices that are fully enrolled (not just MAM)
IntuneDevices
| where OwnerType == "Personal"
| where ManagementAgent has "mdm"  // Full MDM enrollment, not just MAM
| summarize BYODCount=count() by OS, ComplianceState
| sort by BYODCount desc
```

Manual Review Checklist

- ☐ In Intune portal, verify enrollment restrictions limit personal device enrollment to MAM-only (App Protection) where possible
- ☐ Confirm that full device wipe is restricted to corporate-owned devices; personal devices should only allow selective wipe (corporate data removal)
- ☐ Review compliance policies to verify they do not inadvertently grant full wipe capability on BYOD
- ☐ Check that device enrollment type for BYOD uses "User Enrollment" (iOS) or "Work Profile" (Android) rather than full device management
- ☐ Verify that corporate apps on personal devices use app protection policies with selective wipe capability
- ☐ Assess the total count of personal devices under full MDM enrollment and plan migration to MAM-only where appropriate

Employee Impact Warning

A full wipe of a personal device destroys all personal data, including photos, messages, and personal applications. In the Stryker incident, employees lost personal data on BYOD devices. Migrating personal devices from full MDM enrollment to MAM-only (App Protection Policies) removes the risk of personal data destruction while maintaining corporate data protection.

A Appendix A: Indicators of Compromise

Blocking Guidance: 3-Tier IOC Classification

Tier 1: Block (High Confidence)

Vultr C2 IPs (64.176.169.22, 64.176.172.235, 64.176.172.165, 64.176.173.77, 64.176.172.101): Check Point confirmed these as dedicated C2 infrastructure. Safe to add to Conditional Access block lists or firewall deny rules. *Caveat: Reassess if Vultr reassigns these IPs to new customers.*

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

BYOVD drivers (ListOpenedFileDrv_32.sys, rwdsk.sys): Known vulnerable drivers exploited for privilege escalation. Safe for driver blocklist policies.

Tier 2: Alert / Monitor (Shared Infrastructure)

Starlink IPs (AS14593): Shared satellite internet infrastructure used by millions of legitimate subscribers worldwide. Deploy as detection/alerting queries only. Require analyst review before action. Do NOT block at network level.

Storjshare URLs: Storjshare is a legitimate decentralized cloud storage platform. Block specific known-malicious URLs only; do not block the entire domain.

Telegram API (api.telegram.org): Blocking Telegram API will disrupt legitimate Telegram usage. Monitor for non-Telegram-client processes connecting to this endpoint.

Broader Vultr range (64.176.0.0/12): Vultr is a cloud hosting provider used by thousands of legitimate customers. Only the five specific C2 IPs above are confirmed Tier 1. The broader range is Tier 2 (alerting only).

Tier 3: Investigate (Unconfirmed)

Residential ISP IPs: Any residential ISP IPs observed in connection with Handala 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.

Stryker attack initial access vector: The specific initial access mechanism for the Stryker Intune compromise has not been publicly disclosed. [REQUIRES VERIFICATION]

File Indicators (SHA256)

Indicator	Context	Source	Confidence
`D0C03D40772CD468325BBC522402F7B737F18B8F37A89BACC5C8A00C2B87BFC6`	Void Manticore wiper (Israel)	Check Point Research (May 2024)	High
`DEEAF85B2725289D5FC262B4F60DDA0C68AE42D8D46D0DC19B9253B451AEA25A`	Void Manticore wiper (Israel)	Check Point Research (May 2024)	High
`87F0A902D6B2E2AE3647F10EA214D19DB9BD117837264EE15D622B5314FF03D5`	Void Manticore wiper (Israel)	Check Point Research (May 2024)	High
`85FA58CC8C4560ADB955BA0AE9B9D6CAB2C381D10DBD42A0BCEB8B62A92B7636`	Void Manticore wiper (Israel)	Check Point Research (May 2024)	High
`74D8D60E900F931526A911B7157511377C0A298AF986D42D373F51AAC4F362F6`	Void Manticore wiper (Israel)	Check Point Research (May 2024)	High
`CC77E8AB73B577DE1924E2F7A93BCFD852B3C96C6546229BC8B80BF3FD7BF24E`	Void Manticore wiper (Israel)	Check Point Research (May 2024)	High
`40417e937cd244b2f928150cae6fa0eff5551fdb401ea072f6ecdda67a747e17`	BiBi-Windows Wiper	BlackBerry Research (Nov 2023)	High
`f116acc6508843f59e59fb5a8d643370dce82f492a217764521f46a856cc4cb5`	GoXML ransomware (Albania)	CISA AA22-264A (Sep 2022)	High
`e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05acc948b8b965480ca0`	CL Wiper (Albania)	CISA AA22-264A (Sep 2022)	High
`3c9dc8ada56adf9cebfc501a2d3946680dcb0534a137e2e27a7fcb5994cd9de6`	rwdsk.sys raw disk driver (Albania)	CISA AA22-264A (Sep 2022)	High
`7ad64b64e0a4e510be42ba631868bbda8779139dc0daad9395ab048306cc83c5`	ClientBin.aspx web shell (Albania)	CISA AA22-264A (Sep 2022)	High
`45bf0057b3121c6e444b316afafdd802d16083282d1cbfde3cdbf2a9d0915ace`	disable_defender.exe (Albania)	CISA AA22-264A (Sep 2022)	High
`96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8`	CrowdStrike-themed wiper payload	Splunk (Jul 2024)	High
`19001dd441e50233d7f0addb4fcd405a70ac3d5e310ff20b331d6f1a29c634f0`	Phishing PDF (CrowdStrike lure)	Splunk (Jul 2024)	High
`8316065c4536384611cbe7b6ba6a5f12f10db09949e66cb608c92ae8b69e4d67`	OpenFileFinder.dll (BYOVD loader)	Splunk (Jul 2024)	High
`9e519211947c63d9bf6f4a51bc161f5b9ace596c2935a8eedfce4057f747b961`	Related wiper sample (Jul 2024)	Splunk (Jul 2024)	High
`fe07dca68f288a4f6d7cbd34d79bb70bc309635876298d4fde33c25277e30bd2`	HamsaUpdate loader (Hatef wiper)	Intezer	High
`ca9bf13897af109cb354f2629c10803966eb757ee4b2e468abc04e7681d0d74a`	HamsaUpdate loader variant	Intezer	High

Network Indicators (C2 IPs)

Indicator	Type	Context	Source	Confidence
`64.176.169.22`	IPv4	C2 infrastructure (Vultr)	Check Point Research (May 2024)	High
`64.176.172.235`	IPv4	C2 infrastructure (Vultr)	Check Point Research (May 2024)	High
`64.176.172.165`	IPv4	C2 infrastructure (Vultr)	Check Point Research (May 2024)	High
`64.176.173.77`	IPv4	C2 infrastructure (Vultr)	Check Point Research (May 2024)	High
`64.176.172.101`	IPv4	C2 infrastructure (Vultr)	Check Point Research (May 2024)	High

These IPs belong to Vultr, a cloud hosting provider. Check Point Research confirmed them as dedicated C2 infrastructure for Void Manticore. However, Vultr may reassign these IPs to new customers. Reassess periodically and verify current assignment before maintaining in block lists.

C2 Infrastructure (Telegram Bots)

Indicator	Type	Context	Source	Confidence
`7277950797:AAF99Nw5rAT1BHnMmwY_tQNYJFU3dYJ5RHc`	Telegram Bot Key	CrowdStrike-themed wiper C2 (Jul 2024)	Trellix	High
`7436061126`	Telegram Chat ID	CrowdStrike-themed wiper C2 (Jul 2024)	Trellix	High
`6428401585` (bot ID only; full token not publicly available)	Telegram Bot ID	HamsaUpdate/Hatef wiper C2	Intezer, Splunk	High
`6932028002`	Telegram Channel ID	HamsaUpdate/Hatef wiper C2	Intezer, Splunk	High

Download URLs & Phishing Domains

Indicator	Type	Context	Source	Confidence
`hxxps://link[.]storjshare[.]io/s/jwyite7mez2ilyom2esxw2jq3apq/crowdstrikeisrael/update.zip`	URL	Wiper payload (CrowdStrike lure)	Trellix	High
`hxxps://link[.]storjshare[.]io/s/jvktcsf5ypoak5aucs6fn6noggga/crowdstrikesupport/update.zip`	URL	Wiper payload variant (CrowdStrike lure)	Trellix, Splunk	High
`hxxps[:]//www[.]shirideitch[.]com/wp-content/uploads/2022/06/RedAlert.apk`	URL	Malicious RedAlert APK distribution	Unit 42 (Mar 2026)	High
`hxxps[:]//api[.]ra-backup[.]com/analytics/submit.php`	URL	RedAlert APK C2 endpoint	Unit 42 (Mar 2026)	High
`crowdstrike.com.vc`	Domain	Phishing domain impersonating CrowdStrike	Splunk, Trellix, CyberScoop	High

B Appendix B: Detection Rules

KQL Detection Rules

Intune Mass Wipe Detection

KQL

DETECTION ONLY

MICROSOFT SENTINEL

```
// RULE: Alert on bulk Intune wipe/retire/reset operations
// Threshold: >10 wipe commands per hour from a single account
AuditLogs
| where LoggedByService == "Intune"
| where OperationName has_any ("Wipe", "Retire", "Reset",
    "cleanWindowsDevice")
| summarize WipeCount=count(),
    Devices=make_set(TargetResources[0].displayName)
    by bin(TimeGenerated, 1h),
    Initiator=tostring(InitiatedBy.user.userPrincipalName)
| where WipeCount > 10
| extend AlertSeverity = case(
    WipeCount > 100, "Critical",
    WipeCount > 50, "High",
    WipeCount > 10, "Medium",
    "Low")
| sort by WipeCount desc
```

Starlink Sign-in Detection

KQL

DETECTION ONLY

This query detects sign-ins from AS14593 (Starlink). This ASN serves millions of legitimate Starlink subscribers. **This is a detection query for analyst review. Do NOT deploy as an automated blocking rule.**

MICROSOFT SENTINEL

```
// RULE: Detect sign-ins from Starlink (AS14593)
// WARNING: Shared infrastructure. Alert only, NOT for blocking.
SigninLogs
| where AutonomousSystemNumber == 14593
| project TimeGenerated, UserPrincipalName, IPAddress,
    Location, AppDisplayName, DeviceDetail,
    RiskState, ConditionalAccessStatus
| extend AlertContext = "Starlink ISP - verify with HR/IT if user legitimately uses satellite internet"
| sort by TimeGenerated desc
```

Graph API Device Management Abuse

KQL

DETECTION ONLY

MICROSOFT SENTINEL

```
// RULE: Detect scripted or bulk Graph API calls to destructive endpoints
MicrosoftGraphActivityLogs
| where RequestMethod == "POST"
| where RequestUri has "/managedDevices/"
| where RequestUri has_any ("/wipe", "/retire", "/resetPasscode",
    "/cleanWindowsDevice")
| summarize CallCount=count(),
    Endpoints=make_set(RequestUri)
    by UserId, ServicePrincipalId, bin(TimeGenerated, 15m)
| where CallCount > 5
| sort by CallCount desc
```

RegAsm.exe Process Hollowing

KQL

DETECTION ONLY

MICROSOFT DEFENDER FOR ENDPOINT

```
// RULE: Detect RegAsm.exe with no arguments or with network activity
// Handala hollows wiper payloads into RegAsm.exe
DeviceProcessEvents
| where FileName =~ "RegAsm.exe"
| where ProcessCommandLine == "" or ProcessCommandLine endswith "RegAsm.exe"
| join kind=leftouter (
    DeviceNetworkEvents
    | where InitiatingProcessFileName =~ "RegAsm.exe"
    | where Timestamp > ago(30d)
    | summarize NetworkConnections=count(),
        RemoteIPs=make_set(RemoteIP)
        by DeviceName, NetBin=bin(Timestamp, 5m)
) on DeviceName
| where isnull(NetBin) or abs(datetime_diff('minute', Timestamp, NetBin)) < 10
| project Timestamp, DeviceName, ProcessCommandLine,
    InitiatingProcessFileName, NetworkConnections, RemoteIPs
```

Telegram Exfiltration Detection

KQL

DETECTION ONLY

MICROSOFT DEFENDER FOR ENDPOINT

```
// RULE: Detect non-browser/non-Telegram processes calling Telegram API
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: RegAsm Process Hollowing

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 for environment-specific false positives.

DETECTION ONLY

SIGMA (YAML)

```
title: Suspicious RegAsm.exe Execution - Possible Process Hollowing (Handala)
id: a1b2c3d4-e5f6-7890-abcd-handala001
status: experimental
description: |
    Detects RegAsm.exe launched with no arguments or spawning
    network connections, consistent with Handala wiper process
    hollowing technique (T1055.012).
references:
    - https://www.trellix.com/blogs/research/handalas-wiper-targets-israel/
    - https://www.splunk.com/en_us/blog/security/handalas-wiper-threat-analysis-and-detections.html
author: Intruvent Technologies
date: 2026-03-11
tags:
    - attack.defense-evasion
    - attack.t1055.012
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image|endswith: '\RegAsm.exe'
    filter_normal:
        CommandLine|contains:
            - '.dll'
            - '.exe'
            - '/codebase'
            - '/registered'
    condition: selection and not filter_normal
falsepositives:
    - Legitimate .NET assembly registration without file arguments (rare)
level: high
```

YARA Rule: BiBi Wiper Pattern

BLOCKING SAFE

YARA

```
rule Handala_BiBi_Wiper {
    meta:
        description = "Detects BiBi wiper variants (Windows only; Linux variant is ELF and requires a separate rule)"
        author = "Intruvent Technologies"
        date = "2026-03-11"
        reference = "BlackBerry Research (Nov 2023); SecurityJoes (Oct 2023)"
        tlp = "TLP:CLEAR"
        hash_win = "40417e937cd244b2f928150cae6fa0eff5551fdb401ea072f6ecdda67a747e17"

    strings:
        $ext = ".BiBi" ascii wide
        $cmd_shadow1 = "vssadmin delete shadows" ascii wide nocase
        $cmd_shadow2 = "wmic shadowcopy delete" ascii wide nocase
        $cmd_recovery = "bcdedit" ascii wide nocase
        $mutex = "BiBi" ascii wide

    condition:
        uint16(0) == 0x5A4D and
        $ext and
        (1 of ($cmd_*)) and
        $mutex
}
```

C Appendix C: References

Government Advisories

[1] **CISA** - "Iranian State Actors Conduct Cyber Operations Against the Government of Albania" (Advisory AA22-264A, September 2022)
cisa.gov

[2] **MITRE ATT&CK** - Campaign C0038: HomeLand Justice
attack.mitre.org

Vendor Threat Intelligence (Primary)

[3] **Check Point Research** - "Bad Karma, No Justice: Void Manticore Destructive Activities in Israel" (May 2024)
research.checkpoint.com

[4] **Check Point Research** - "Iranian MOIS Actors & the Cyber Crime Connection" (March 10, 2026)
research.checkpoint.com

[5] **Check Point Blog** - "What Defenders Need to Know about Iran's Cyber Capabilities"
blog.checkpoint.com

[6] **Check Point Blog** - "Unveiling Void Manticore: Structured Collaboration Between Espionage and Destruction in MOIS"
blog.checkpoint.com

[7] **Palo Alto Unit 42** - "Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran"
unit42.paloaltonetworks.com

[8] **Splunk** - "Handala's Wiper: Threat Analysis and Detections"
splunk.com

[9] **Trellix** - "Handala's Wiper Targets Israel"
trellix.com

[10] **Intezer** - "Operation HamsaUpdate: A Sophisticated Campaign Delivering Wipers Puts Israeli Infrastructure at Risk"
intezer.com

[11] **SecurityJoes** - "BiBi-Linux: A New Wiper Dropped By Pro-Hamas Hacktivist Group" (October 30, 2023)
securityjoes.com

[12] **BlackBerry** - "BiBi Wiper Used in the Israel-Hamas War Now Runs on Windows" (November 2023)
blogs.blackberry.com

Investigative Journalism

[13] **Krebs on Security** - "Iran-Backed Hackers Claim Wiper Attack on Medtech Firm Stryker" (March 11, 2026)
krebsonsecurity.com

[14] **Zetter Zero Day** - "Iranian Hacktivists Strike Medical Device Maker Stryker in Severe Attack that Wiped Systems" (March 11, 2026)
zetter-zeroday.com

[15] **TechCrunch** - "Pro-Iran hacktivist group says it is behind attack on medical tech giant Stryker" (March 11, 2026)
techcrunch.com

[16] **Newsweek** - "Stryker cyber attack: Alleged Iran-linked group Handala causes outage"
newsweek.com

OSINT & Analyst Research

[17] **Nariman Gharib** - "Handala's Thailand Blunder: MOIS Accidentally Exposes Access to Bangkok Airport" (December 2025)
blog.narimangharib.com

[18] **ICT (International Institute for Counter-Terrorism)** - "Bibi Gate: Handala Hack Team, A Mask for Iranian Psychological Warfare" (December 2025)
ict.org.il

[19] **KELA** - "Handala Hack: Telegram Breach of Israeli Officials"
kelacyber.com

[20] **OP Innovate** - "Disrupting Handala: Did OP Innovate Help Silence a Major Cyber Threat?"
op-c.net

Secondary Sources

[21] **SOCRadar** - "Dark Web Profile: Storm-842 (Void Manticore)"
socradar.io

[22] **Malpedia** - "BANISHED KITTEN / Void Manticore"
malpedia.caad.fkie.fraunhofer.de

[23] **CFR Cyber Operations Tracker** - "Storm-842"
cfr.org

[24] **Iran International** - "Iran-linked 'Handala Hack' now routing attacks via Starlink" (January 20, 2026)
iranintl.com

[25] **Times of Israel** - "Iranian hackers broadcast rocket sirens, odes to terrorism in 20 Israeli kindergartens" (January 2025)
timesofisrael.com

[26] **The Record (Recorded Future News)** - "Hackers hijack emergency sirens in kindergartens across Israel"
therecord.media

[27] **GovInfoSecurity** - "Medtech Firm Stryker Disrupted by Pro-Iran Hackers"
govinfosecurity.com

[28] **The Register** - "Cybercrime isn't just a cover for Iran's government goons" (March 10, 2026)
theregister.com

[29] **Brandefense** - "Inside Void Manticore"
brandefense.io

[30] **Medium / Andrey Pautov** - "CTI Research: Handala Hack Group (aka Handala Hack Team)" (March 2026)
medium.com