INTRUVENT

COMPREHENSIVE THREAT HUNTING GUIDE

Cotton Sandstorm: Influence Operations and Destructive Capability Detection

Hunting hack-and-leak infrastructure, election interference indicators, mass email campaigns, website defacement, and destructive payloads

Version 1.0
Classification TLP:CLEAR
Published March 18, 2026
Total Hunt Time 5 Hours
Threat Actor Cotton Sandstorm / Emennet Pasargad (IRGC)
Target Sectors Elections, Government, Media, Technology, Critical Infrastructure

Intruvent Technologies
INT-THG-2026-COTTONSANDSTORM-v1.0

Table of Contents

Overview

Executive Summary 3
MITRE ATT&CK Mapping 4

Hunt Modules

Module 1: Mass Email / Voter Intimidation Campaign Detection 5
Module 2: Website Defacement Detection 6
Module 3: Credential Harvesting and Phishing Infrastructure 7
Module 4: Hack-and-Leak Data Staging and Exfiltration 8
Module 5: Voter / Public Database Access Detection 9
Module 6: Social Media Influence Infrastructure 10
Module 7: Web Shell and Initial Access Detection 11
Module 8: Destructive Payload Detection 12
Module 9: VPN / Proxy Infrastructure Detection 13
Module 10: Cloud Account Abuse for Data Hosting 14

Appendices

Appendix A: Indicators of Compromise 15
Appendix B: Detection Rules 16
Appendix C: References 18

1 Executive Summary

AT A GLANCE

THREAT ACTOR Cotton Sandstorm / Emennet Pasargad (IRGC, Iran)	PRIMARY OBJECTIVE Influence operations, hack-and-leak, election interference, destructive capability
ACTIVE SINCE 2020 (confirmed); 2017 (alleged HBO intrusion)	TARGET SECTORS Elections, Government, Media, Technology, Sports Events
KEY DIFFERENTIATOR Combined influence operations and destructive capability	IOC AVAILABILITY Limited; behavioral detection emphasized over hash-based

Cotton Sandstorm (also tracked as Neptunium by Microsoft, Haywire Kitten by CrowdStrike) is an Iranian state-sponsored threat actor operating through the front company Emennet Pasargad (later rebranded to Aria Sepehr Ayandehsazan). The group operates under direction of the Islamic Revolutionary Guard Corps (IRGC) and specializes in influence operations that combine network intrusion, data theft, and amplified public messaging for maximum psychological impact.

The group gained international attention through its 2020 U.S. presidential election voter intimidation campaign, where it obtained voter registration data, sent tens of thousands of threatening emails impersonating the Proud Boys, and attempted to distribute fabricated election fraud videos. Two Emennet Pasargad employees were indicted by the DOJ in November 2021. Microsoft reported in 2023 that Cotton Sandstorm had expanded its capabilities to include destructive attacks, making it a hybrid influence-destruction threat.

This guide provides **10 hunt modules** designed to help defenders detect: (1) influence operation infrastructure such as mass email campaigns and website defacement, (2) hack-and-leak data staging and exfiltration, (3) credential harvesting targeting public-facing applications, (4) destructive payload deployment, and (5) operational infrastructure including VPN anonymization and cloud abuse. Total estimated hunt time is **5 hours**.

Limited Technical IOC Availability

Cotton Sandstorm has significantly thinner public technical documentation than other Iranian groups (APT33, APT34, Agrius). The DOJ indictment and CISA advisories describe operational behaviors but provide limited specific technical indicators. Detection for this actor relies primarily on behavioral patterns and influence operation monitoring rather than hash-based or network IOC lookups.

Threat Overview

Cotton Sandstorm occupies a unique niche in the Iranian cyber ecosystem. While APT33 focuses on espionage and Agrius on destruction, Cotton Sandstorm combines intrusion with information warfare. The group's operational cycle follows a "hack, leak, amplify, destroy" pattern: gain access to target systems, steal sensitive data, stage it for public release through fabricated personas, amplify the leak through social media manipulation and mass communications, and (in later operations) destroy victim infrastructure.

The group's evolution from pure influence operations (2020) to combined influence-destruction capability (2023+) represents a significant escalation. Microsoft reported this capability expansion in February 2023, noting that Cotton Sandstorm had deployed "a wider range of online personas" and expanded "its network of cyber-enabled influence operations." The 2024 superseding DOJ indictment confirmed the group remained active under the rebranded company name Aria Sepehr Ayandehsazan (ASA).

During the current Iran conflict (Operation Epic Fury, February 2026), Cotton Sandstorm is assessed as activated alongside 15+ other Iranian APT groups (Intruvent SITREP v1.3). The group's combined capabilities make it particularly dangerous: it can simultaneously conduct influence operations to shape public narrative about the conflict while performing destructive operations against targeted infrastructure.

KEY CHARACTERISTICS

- IRGC state-sponsored (Iran)
- Hack-and-leak operations
- Mass email voter intimidation
- Website defacement
- Fabricated video/media
- Social media persona networks
- Expanded destructive capability (2023+)
- AI-generated content (2024+)
- Sports event targeting (Olympics, World Cup)
- Sanctioned by U.S. Treasury

2 MITRE ATT&CK Mapping

The following techniques are attributed to Cotton Sandstorm based on DOJ indictment details (2021), CISA Advisory AA24-241A (2024), Microsoft Threat Intelligence reporting (2023-2024), and FBI Flash alerts. Cotton Sandstorm is not currently listed as a standalone group in MITRE ATT&CK.

`T1190`
Exploit Public-Facing Application
Exploitation of web applications including state election websites to obtain voter registration data (DOJ, 2021)

`T1566`
Phishing
Credential harvesting campaigns targeting government and media organizations (CISA AA24-241A, 2024)

`T1078`
Valid Accounts
Use of compromised credentials for initial access; CISA reported brute force and credential access activity (AA24-241A)

`T1505.003`
Web Shell
Web shell deployment on compromised servers for persistent access [REQUIRES VERIFICATION for specific shell variants]

`T1491.002` CORE
External Defacement
Website defacement with propaganda messaging; core influence operation tactic against Israeli and Western targets (Microsoft, 2023)

`T1585.001` CORE
Establish Accounts: Social Media
Creation of fake social media persona networks for amplification and disinformation (Microsoft, 2023)

`T1585.002`
Establish Accounts: Email
Fabricated email accounts for spoofed mass email campaigns, including Proud Boys impersonation (DOJ, 2021)

`T1583.001`
Acquire Infrastructure: Domains
Registration of domains for leak sites, phishing, and influence operation infrastructure (DOJ, 2021; FBI)

`T1567`
Exfiltration Over Web Service
Use of cloud services and web platforms to host and distribute stolen data for hack-and-leak operations

`T1530`
Data from Cloud Storage
Targeting cloud-hosted data repositories for exfiltration in hack-and-leak operations

`T1485`
Data Destruction
Destructive capability added to operational toolkit (Microsoft, 2023); specific tooling details not publicly available

`T1498`
Network Denial of Service
DDoS capability as part of broader influence operation toolkit [REQUIRES VERIFICATION for specific tools]

3 Hunt Modules

1 Mass Email / Voter Intimidation Campaign Detection

Duration: 30 min Priority: CRITICAL

Objective: Detect mass spoofed email campaigns, voter intimidation infrastructure, and domain spoofing consistent with Cotton Sandstorm's 2020 election operation.

Background

Cotton Sandstorm's most documented operation involved sending tens of thousands of threatening emails to registered U.S. voters while impersonating the Proud Boys (DOJ indictment, November 2021). The emails used spoofed sender addresses and were designed to intimidate voters. The group also attempted to disseminate a fabricated video alleging election fraud. This module focuses on detecting the email infrastructure and domain spoofing patterns used in such campaigns.

Hunt Procedure: Spoofed Outbound Email Detection

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR OFFICE 365)

```
// Detect outbound emails where the From domain does not match the MailFrom domain
// This indicates potential email spoofing (Cotton Sandstorm TTP per DOJ, 2021)
EmailEvents
| where EmailDirection == "Outbound"
| where SenderFromDomain != SenderMailFromDomain
| summarize EmailCount = count(),
    UniqueRecipients = dcount(RecipientEmailAddress)
    by SenderFromAddress, SenderMailFromDomain, bin(Timestamp, 1h)
| where EmailCount > 50
| sort by EmailCount desc
```

Hunt Procedure: Inbound Threatening / Intimidation Email Detection

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR OFFICE 365)

```
// Detect inbound emails containing threatening language patterns
// Cotton Sandstorm sent threatening voter intimidation emails (DOJ, 2021)
EmailEvents
| where EmailDirection == "Inbound"
| where Subject has_any ("we will come after you", "we know where you live",
    "vote for", "you have been identified", "we are watching")
| project Timestamp, SenderFromAddress, SenderMailFromDomain,
    RecipientEmailAddress, Subject, AuthenticationDetails
| sort by Timestamp desc
```

Hunt Procedure: DMARC / SPF Authentication Failure Spike

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR OFFICE 365)

```
// Monitor for spikes in DMARC/SPF failures that may indicate spoofing of your domain
EmailEvents
| where EmailDirection == "Inbound"
| where AuthenticationDetails has "spf=fail" or AuthenticationDetails has "dmarc=fail"
| summarize FailCount = count() by SenderMailFromDomain, bin(Timestamp, 1h)
| where FailCount > 100
| sort by FailCount desc
```

- ☐ Review all outbound email for domain mismatch between From and MailFrom headers (spoofing indicator)
- ☐ Search inbound email for threatening language patterns consistent with voter intimidation
- ☐ Monitor DMARC/SPF failure rates for your domain; a sudden spike may indicate your domain is being spoofed
- ☐ Verify DMARC policy is set to p=reject for all organizational domains
- ☐ Check for recently registered domains that closely mimic your organization's domain (typosquatting)

Election Infrastructure Priority

Organizations managing voter databases, election systems, or government communications infrastructure should prioritize this module. Cotton Sandstorm specifically targeted U.S. state voter registration systems in 2020 and has demonstrated continued interest in election interference (2024 election cycle targeting per Microsoft).

2 Website Defacement Detection

Duration: 30 min Priority: CRITICAL

Objective: Detect unauthorized modifications to public-facing web content consistent with Cotton Sandstorm website defacement operations.

Background

Microsoft Threat Intelligence reported that Cotton Sandstorm conducts website defacement as a core influence operation tactic (T1491.002). The group defaces websites with propaganda messaging to amplify Iranian strategic narratives and demoralize adversaries. Defacement targets have included Israeli government and private sector websites. During the current conflict (Operation Epic Fury), website defacement activity by Iranian groups has increased. Detecting unauthorized web content changes provides an early indicator of Cotton Sandstorm activity.

Hunt Procedure: Unauthorized Web Content Modification

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect modifications to web server content files outside normal deployment
// Cotton Sandstorm defaces websites for influence operations (Microsoft, 2023)
DeviceFileEvents
| where ActionType == "FileModified"
| where FolderPath has_any ("wwwroot", "inetpub", "htdocs", "html", "public_html")
| where FileName endswith ".html" or FileName endswith ".htm"
    or FileName endswith ".php" or FileName endswith ".aspx"
    or FileName endswith ".jsp" or FileName endswith ".js"
| where InitiatingProcessFileName !in~ ("msdeploy.exe", "w3wp.exe",
    "dotnet.exe", "node.exe", "php-cgi.exe")
| project Timestamp, DeviceName, FileName, FolderPath,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

Hunt Procedure: CMS Admin Panel Access from Unusual Sources

DETECTION ONLY

KQL (MICROSOFT SENTINEL / WEB LOGS)

```
// Monitor admin panel access on CMS platforms (WordPress, Drupal, etc.)
// Unauthorized CMS access precedes defacement
CommonSecurityLog
| where RequestURL has_any ("/wp-admin", "/wp-login.php",
    "/administrator", "/admin/login", "/user/login")
| where HttpStatusCode in (200, 302)
| summarize AccessCount = count() by SourceIP, RequestURL,
    bin(TimeGenerated, 1h)
| where AccessCount > 10
| sort by AccessCount desc
```

Hunt Procedure: Index File Replacement Detection

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect replacement of index/default pages (primary defacement vector)
DeviceFileEvents
| where ActionType in ("FileCreated", "FileModified")
| where FileName in~ ("index.html", "index.htm", "index.php",
    "default.aspx", "default.html", "index.asp")
| where FolderPath has_any ("wwwroot", "inetpub", "htdocs")
| project Timestamp, DeviceName, FileName, FolderPath, SHA256,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

- ☐ Audit all modifications to web root directories within the past 30 days; compare against authorized deployment logs
- ☐ Verify CMS admin panel access logs for unauthorized sessions, especially from VPN exit nodes or foreign IPs
- ☐ Check file integrity monitoring (FIM) alerts for index.html and default page replacements
- ☐ Review web server access logs for POST requests to file upload endpoints

Defacement as Precursor

Website defacement may be the visible component of a broader intrusion. If defacement is detected, assume the attacker has deeper access to the web server and potentially the internal network. Conduct full forensic analysis of the compromised server, including web shell hunting (see Module 7).

3 Credential Harvesting and Phishing Infrastructure

Duration: 30 min Priority: HIGH

Objective: Detect credential harvesting campaigns, phishing infrastructure, and brute force access patterns consistent with Cotton Sandstorm and CISA AA24-241A advisory indicators.

Background

CISA Advisory AA24-241A (August 2024) described Iranian cyber actors (including entities linked to Cotton Sandstorm's operational ecosystem) using brute force and credential access techniques to compromise critical infrastructure organizations. The advisory documented use of password spraying, MFA push notification fatigue attacks, and credential stuffing. Cotton Sandstorm's initial access to U.S. voter databases in 2020 also relied on exploiting weak authentication on public-facing election infrastructure (DOJ, 2021).

Hunt Procedure: Brute Force / Password Spraying Detection

DETECTION ONLY

KQL (MICROSOFT SENTINEL / AZURE AD)

```
// Detect password spraying patterns (CISA AA24-241A indicator)
// Multiple accounts targeted from a single source in a short window
SigninLogs
| where ResultType != 0  // Failed sign-ins
| summarize FailedAttempts = count(),
    TargetAccounts = dcount(UserPrincipalName),
    Accounts = make_set(UserPrincipalName, 20)
    by IPAddress, bin(TimeGenerated, 15m)
| where FailedAttempts > 20 and TargetAccounts > 5
| sort by FailedAttempts desc
```

Hunt Procedure: MFA Push Notification Fatigue

DETECTION ONLY

KQL (MICROSOFT SENTINEL / AZURE AD)

```
// Detect MFA push fatigue attacks (CISA AA24-241A indicator)
// Repeated MFA prompts followed by eventual approval
SigninLogs
| where ResultType == 50074  // MFA required
| summarize MFAPrompts = count() by UserPrincipalName,
    IPAddress, bin(TimeGenerated, 10m)
| where MFAPrompts > 5
| sort by MFAPrompts desc
```

Hunt Procedure: Credential Stuffing via Public-Facing Applications

DETECTION ONLY

KQL (MICROSOFT SENTINEL / WEB LOGS)

```
// Detect credential stuffing against web login endpoints
CommonSecurityLog
| where RequestURL has_any ("/login", "/signin", "/auth",
    "/api/login", "/Account/Login")
| where HttpStatusCode in (401, 403)
| summarize FailedLogins = count() by SourceIP, RequestURL,
    bin(TimeGenerated, 15m)
| where FailedLogins > 50
| sort by FailedLogins desc
```

- ☐ Review Azure AD / Entra ID sign-in logs for password spraying patterns (many accounts, single IP, rapid failures)
- ☐ Check for MFA push notification fatigue attacks (repeated MFA prompts to same user from same IP)
- ☐ Audit public-facing application login endpoints for credential stuffing activity
- ☐ Verify that all administrative accounts have phishing-resistant MFA (FIDO2 / certificate-based)
- ☐ Search for newly registered domains that mimic your organization's login pages

CISA AA24-241A Reference

CISA Advisory AA24-241A (August 2024) provides detailed guidance on defending against Iranian brute force and credential access techniques. Organizations should review this advisory for additional detection strategies and hardening recommendations specific to Iranian threat actor tradecraft.

4 Hack-and-Leak Data Staging and Exfiltration

Duration: 35 min Priority: CRITICAL

Objective: Detect data staging, archiving, and exfiltration patterns consistent with Cotton Sandstorm hack-and-leak operations.

Background

Hack-and-leak is Cotton Sandstorm's signature operational pattern. The group gains access to target systems, exfiltrates sensitive data, then distributes it through fabricated personas, Telegram channels, and purpose-built leak sites to maximize reputational damage. The 2017 HBO operation (attributed to Emennet Pasargad personnel per the DOJ indictment) and 2020-2023 Israeli operations demonstrate this pattern. Detecting data staging and exfiltration provides a critical early warning before the public leak phase.

Hunt Procedure: Large Archive File Creation

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect creation of large archive files that may precede exfiltration
// Cotton Sandstorm stages data before public leak (Microsoft, 2023)
DeviceFileEvents
| where ActionType == "FileCreated"
| where FileName endswith ".zip" or FileName endswith ".7z"
    or FileName endswith ".rar" or FileName endswith ".tar.gz"
| where FileSize > 104857600  // Files larger than 100MB
| project Timestamp, DeviceName, FileName, FolderPath, FileSize,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by FileSize desc
```

Hunt Procedure: Data Archiving Tool Execution

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect archiving tool usage for potential exfiltration preparation
DeviceProcessEvents
| where FileName in~ ("7z.exe", "7za.exe", "rar.exe", "zip.exe", "tar.exe")
| where ProcessCommandLine has_any (".zip", ".7z", ".rar", ".tar", ".gz")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

Hunt Procedure: Large Outbound Data Transfers

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect large outbound data transfers to cloud storage services
// Cotton Sandstorm uses cloud services for data hosting (FBI, 2021)
DeviceNetworkEvents
| where RemotePort in (443, 80)
| where RemoteUrl has_any ("drive.google.com", "dropbox.com",
    "mega.nz", "onedrive.live.com", "transfer.sh", "file.io",
    "anonfiles.com", "gofile.io", "wetransfer.com")
| summarize TotalConnections = count(),
    DataSent = sum(SentBytes)
    by DeviceName, RemoteUrl, bin(Timestamp, 1h)
| where TotalConnections > 20 or DataSent > 52428800  // 50MB
| sort by DataSent desc
```

- ☐ Search for large archive files (>100MB) created on servers in the past 30 days
- ☐ Review all archiving tool executions, especially on database servers or file servers
- ☐ Monitor outbound transfers to cloud storage services for unusual volume or timing
- ☐ Check DLP alerts for sensitive data patterns (PII, financial records, intellectual property) being transferred externally
- ☐ Review Telegram bot API connections from corporate network (potential leak channel)

Hack-and-Leak Window

Once data is exfiltrated, Cotton Sandstorm may hold it for days or weeks before public release. Detecting the exfiltration phase provides a critical opportunity to prepare a response plan, notify affected parties, and coordinate with law enforcement before the leak becomes public. If large-scale data exfiltration is confirmed, engage legal counsel and incident response teams immediately.

5 Voter / Public Database Access Detection

Duration: 25 min Priority: HIGH

Objective: Detect unauthorized access to voter registration databases, PII repositories, and public-facing data systems that Cotton Sandstorm has targeted for influence operations.

Background

The DOJ indictment (November 2021) confirmed that Cotton Sandstorm obtained voter registration data from at least one U.S. state election website. This data was used to target specific voters with threatening emails. The group scanned approximately 11 U.S. state election websites for vulnerabilities and successfully accessed voter data from at least one. Organizations managing any form of public-facing database containing PII should assess their exposure to this type of targeted access.

Hunt Procedure: Database Server Bulk Data Access

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect unusual database connection patterns from non-standard processes
// Cotton Sandstorm accessed voter databases via web application exploitation (DOJ, 2021)
DeviceNetworkEvents
| where RemotePort in (1433, 3306, 5432, 27017)  // SQL, MySQL, PostgreSQL, MongoDB
| where InitiatingProcessFileName !in~ ("sqlservr.exe", "mysqld.exe",
    "postgres.exe", "mongod.exe", "sqlcmd.exe", "mysql.exe",
    "psql.exe", "w3wp.exe")
| summarize ConnectionCount = count()
    by DeviceName, InitiatingProcessFileName, RemoteIP, bin(Timestamp, 1h)
| where ConnectionCount > 20
| sort by ConnectionCount desc
```

Hunt Procedure: SQL Injection Attempt Detection

DETECTION ONLY

KQL (MICROSOFT SENTINEL / WAF LOGS)

```
// Detect SQL injection attempts against public-facing web applications
CommonSecurityLog
| where RequestURL has_any ("' OR ", "1=1", "UNION SELECT",
    "DROP TABLE", "exec(", "xp_cmdshell", "information_schema")
| summarize AttemptCount = count() by SourceIP, RequestURL,
    bin(TimeGenerated, 1h)
| where AttemptCount > 5
| sort by AttemptCount desc
```

- ☐ Audit database access logs for bulk SELECT queries against PII tables from unexpected sources
- ☐ Review WAF logs for SQL injection attempts against public-facing applications
- ☐ Verify that all public-facing databases require authentication and input validation
- ☐ Check for API endpoints that expose voter or customer data without proper rate limiting

Election Infrastructure Scope

This module is particularly relevant for state and local government organizations managing voter registration databases, election management systems, or any public-facing data portals. The 2020 DOJ indictment confirmed that Cotton Sandstorm systematically scanned U.S. state election websites before targeting specific systems for exploitation.

6 Social Media Influence Infrastructure

Duration: 25 min Priority: MEDIUM

Objective: Detect indicators that your organization is being targeted by Cotton Sandstorm's social media influence operations, including fake persona networks and amplified leak campaigns.

Background

Microsoft reported in February 2023 that Cotton Sandstorm had deployed "a wider range of online personas" and expanded its "network of cyber-enabled influence operations." The group creates fake social media accounts across multiple platforms (Facebook, Twitter/X, Instagram, Telegram) to amplify stolen data, spread disinformation, and manipulate public discourse. In 2024, Microsoft reported the group began using AI-generated content to support these operations. This module focuses on detecting indicators that your organization is being targeted by such campaigns.

Hunt Procedure: Monitoring for Brand/Organization Mentions in Leak Channels

INVESTIGATION AID

MANUAL INVESTIGATION CHECKLIST

```
// This module requires manual OSINT investigation rather than automated queries
// Conduct the following searches across platforms:

1. Search Telegram for channels mentioning your organization name
   - Focus on channels with Persian-language operators
   - Check channels associated with known personas: "Atlas Group",
     "Hackers of Savior", "Al-Toufan"

2. Search Twitter/X for accounts:
   - Created recently (within 30 days)
   - Posting about your organization with negative framing
   - Sharing links to unknown paste/file hosting sites
   - Cross-posting identical content (coordinated amplification)

3. Search paste sites (Pastebin, Ghostbin, Rentry):
   - Your organization name + "leak" or "breach" or "data"
   - Employee email addresses or internal document titles

4. Check Have I Been Pwned and breach notification services:
   - For any reported breaches of your domain that you did not disclose
```

- ☐ Conduct regular OSINT monitoring for your organization's name on Telegram and paste sites
- ☐ Monitor for newly registered domains that reference your organization (brand monitoring)
- ☐ Check social media for coordinated campaigns of recently created accounts posting about your organization
- ☐ Report identified fake accounts to platform trust and safety teams for takedown
- ☐ Coordinate with your communications/PR team to prepare holding statements for potential hack-and-leak scenarios

Brand Monitoring Services

Automated brand monitoring and digital risk protection services can supplement manual OSINT for this module. Platforms such as Recorded Future, Digital Shadows (now ReliaQuest), and ZeroFox provide automated monitoring of dark web, paste sites, and social media for organizational exposure.

7 Web Shell and Initial Access Detection

Duration: 30 min Priority: HIGH

Objective: Detect web shell deployment and initial access indicators on public-facing web servers consistent with Cotton Sandstorm intrusion patterns.

Background

Cotton Sandstorm gains initial access through exploitation of public-facing web applications (T1190) and uses web shells for persistent access (T1505.003). The DOJ indictment described exploitation of at least one U.S. state election website to obtain voter data. CISA AA24-241A documented Iranian actors using similar techniques against critical infrastructure. Web shell detection provides a high-value early indicator of intrusion activity that precedes data theft and defacement operations.

Hunt Procedure: Web Shell File Creation

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect web shell files created in web server directories
DeviceFileEvents
| where ActionType == "FileCreated"
| where FileName endswith ".aspx" or FileName endswith ".php"
    or FileName endswith ".jsp" or FileName endswith ".jspx"
| where FolderPath has_any ("inetpub", "wwwroot", "htdocs",
    "public_html", "webapps")
| project Timestamp, DeviceName, FileName, FolderPath, SHA256,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

Hunt Procedure: Web Server Process Spawning Reconnaissance Commands

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect suspicious child processes from IIS or Apache workers
// Web shell command execution triggers these process chains
DeviceProcessEvents
| where InitiatingProcessFileName in~ ("w3wp.exe", "httpd.exe",
    "apache2", "nginx", "php-cgi.exe", "java.exe", "tomcat")
| where FileName in~ ("cmd.exe", "powershell.exe", "certutil.exe",
    "bitsadmin.exe", "net.exe", "whoami.exe", "systeminfo.exe",
    "ipconfig.exe", "tasklist.exe", "reg.exe")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

Hunt Procedure: Public-Facing Application Vulnerability Scanning

DETECTION ONLY

KQL (MICROSOFT SENTINEL / WAF LOGS)

```
// Detect vulnerability scanning against public-facing web applications
// Cotton Sandstorm scanned 11 U.S. state election websites (DOJ, 2021)
CommonSecurityLog
| where HttpStatusCode in (404, 403, 500)
| summarize ErrorCount = count(),
    UniqueURLs = dcount(RequestURL)
    by SourceIP, bin(TimeGenerated, 15m)
| where ErrorCount > 100 and UniqueURLs > 20
| sort by ErrorCount desc
```

- ☐ Review all web-accessible directories for unexpected script files (.aspx, .php, .jsp) created in the past 90 days
- ☐ Check for web server processes spawning command-line tools (cmd.exe, powershell.exe, whoami.exe)
- ☐ Audit WAF and web server logs for vulnerability scanning patterns (high error rates from single IPs)
- ☐ Verify that all public-facing web applications are patched and hardened per vendor recommendations

8 Destructive Payload Detection

Duration: 30 min Priority: CRITICAL

Objective: Detect destructive payloads and data destruction patterns consistent with Cotton Sandstorm's expanded destructive capability reported by Microsoft in 2023.

Background

Microsoft Threat Intelligence reported in February 2023 that Cotton Sandstorm had expanded beyond influence operations to include destructive attacks (T1485). Specific malware families and tools used for destructive operations have not been publicly detailed by Microsoft or other vendors. This module uses behavioral detection for destructive activity patterns rather than hash-based lookups, reflecting the limited public IOC availability for Cotton Sandstorm's destructive toolkit.

Hunt Procedure: Mass File Deletion / Overwrite Pattern

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect rapid file deletion or modification (wiper behavior)
// Cotton Sandstorm expanded to include destructive capability (Microsoft, 2023)
DeviceFileEvents
| where ActionType in ("FileDeleted", "FileModified")
| summarize FileCount = count(),
    DistinctExtensions = dcount(tostring(split(FileName, ".")[-1])),
    DistinctFolders = dcount(FolderPath)
    by DeviceName, InitiatingProcessFileName, bin(Timestamp, 5m)
| where FileCount > 500 and DistinctFolders > 10
| sort by FileCount desc
```

Hunt Procedure: Shadow Copy and Recovery Destruction

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect shadow copy and backup destruction (pre-wiper activity)
DeviceProcessEvents
| where ProcessCommandLine has_any (
    "vssadmin delete shadows",
    "wmic shadowcopy delete",
    "bcdedit /set {default} recoveryenabled no",
    "wbadmin delete catalog",
    "wbadmin delete systemstatebackup")
| project Timestamp, DeviceName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

Hunt Procedure: Raw Disk Access (MBR/Partition Destruction)

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect processes accessing raw physical disk handles
DeviceProcessEvents
| where ProcessCommandLine has_any (
    "\\\\.\\PhysicalDrive",
    "PhysicalDrive0",
    "IOCTL_DISK_DELETE_DRIVE_LAYOUT")
| where FileName !in~ ("diskpart.exe", "diskmgmt.msc", "chkdsk.exe")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

- ☐ Monitor for mass file deletion or modification patterns (>500 files in 5 minutes)
- ☐ Search for shadow copy deletion commands (vssadmin, wmic, bcdedit) executed outside normal patching windows
- ☐ Check for processes accessing raw physical disk handles (MBR/partition destruction)
- ☐ Review for unexpected service stop commands targeting backup, database, or security services

Destructive Capability Confirmation Gap

Microsoft reported Cotton Sandstorm's expansion to destructive operations in 2023, but specific malware families, file hashes, and technical details have not been publicly documented. The behavioral detections in this module are broadly applicable to Iranian destructive operations and are not Cotton Sandstorm-specific. If destructive activity is detected, cross-reference with other Iranian wiper families (Agrius wipers, Void Manticore/BiBi wiper) and engage incident response.

9 VPN / Proxy Infrastructure Detection

Duration: 25 min Priority: MEDIUM

Objective: Detect anomalous VPN and proxy usage patterns consistent with Cotton Sandstorm's operational anonymization techniques.

Background

The DOJ indictment (November 2021) described Cotton Sandstorm's use of VPN services to mask the Iranian origin of operations. CISA AA24-241A similarly documented Iranian actors using VPN infrastructure for anonymized access to compromised networks. This module focuses on detecting anomalous VPN connections to administrative interfaces and sensitive systems. Note that blocking VPN providers broadly is not recommended, as legitimate employees and partners may use VPN services.

Hunt Procedure: Admin Portal Access from VPN / Anonymizer IPs

DETECTION ONLY

KQL (MICROSOFT SENTINEL / AZURE AD)

```
// Detect sign-ins to admin portals from known VPN provider ASNs
// Cotton Sandstorm uses VPN services for anonymization (DOJ, 2021)
// NOTE: This query generates alerts, NOT blocking actions
SigninLogs
| where TimeGenerated > ago(7d)
| where ResultType == 0
| mv-expand NetworkLocationDetails
| where NetworkLocationDetails.networkType in ("vpn", "proxy", "tor", "anonymizer", "hosting")
    or tostring(NetworkLocationDetails) has_any ("VPN", "Proxy", "Tor", "Anonymizer", "Hosting")
| where AppDisplayName has_any ("admin", "portal", "exchange", "sharepoint")
    or ResourceDisplayName has_any ("admin", "portal", "exchange", "sharepoint")
| project TimeGenerated, UserPrincipalName, IPAddress, Location,
    NetworkType = tostring(NetworkLocationDetails.networkType),
    AppDisplayName, ConditionalAccessStatus, RiskState
| sort by TimeGenerated desc
```

Hunt Procedure: Impossible Travel Detection

DETECTION ONLY

KQL (MICROSOFT SENTINEL / AZURE AD)

```
// Detect impossible travel patterns that may indicate VPN-based access
SigninLogs
| where ResultType == 0
| summarize Locations = make_set(Location),
    IPs = make_set(IPAddress),
    LocationCount = dcount(Location)
    by UserPrincipalName, bin(TimeGenerated, 1h)
| where LocationCount > 2
| sort by LocationCount desc
```

- ☐ Review admin portal sign-ins for connections from VPN, proxy, or hosting provider IPs
- ☐ Check for impossible travel alerts in Azure AD Identity Protection
- ☐ Verify that Conditional Access policies require compliant devices for admin access
- ☐ Audit VPN access logs for connections from unexpected geographic regions

Shared Infrastructure Caveat

VPN services are used by millions of legitimate users, including employees working remotely. Do NOT implement blanket blocks on VPN provider IP ranges. Treat VPN-sourced connections to sensitive systems as contextual signals requiring analyst review, not as standalone blocking indicators.

10 Cloud Account Abuse for Data Hosting

Duration: 20 min Priority: MEDIUM

Objective: Detect abuse of cloud storage accounts and services for hosting stolen data in hack-and-leak operations.

Background

Cotton Sandstorm uses cloud services and web platforms to host and distribute stolen data for hack-and-leak operations (FBI, 2021; Microsoft, 2023). The group registers accounts on file hosting services, creates purpose-built leak websites, and uses Telegram channels for data distribution. Detecting unauthorized cloud account creation, unusual data uploads from corporate systems, and cloud storage API abuse provides indicators of ongoing leak preparation.

Hunt Procedure: Unauthorized Cloud Storage Uploads

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR CLOUD APPS)

```
// Detect large uploads to cloud storage services from corporate endpoints
// Cotton Sandstorm stages data on cloud services for leak operations
CloudAppEvents
| where Timestamp > ago(24h)
| where ActionType has_any ("Upload", "FileUploaded")
| where Application has_any ("Dropbox", "Google Drive", "Box", "WeTransfer", "Mega")
| extend FileName = tostring(RawEventData.FileName)
| where FileName has_any (".zip", ".7z", ".rar", ".tar", ".gz")
    or FileName has_any (".csv", ".xlsx", ".pdf", ".docx", ".pst")
| summarize UploadCount = count(),
    Files = make_set(FileName, 50),
    Apps = make_set(Application)
    by AccountDisplayName, AccountObjectId, bin(Timestamp, 1h)
| where UploadCount > 10
| sort by UploadCount desc
```

Hunt Procedure: Telegram Bot API Communication

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect connections to Telegram Bot API (potential leak channel)
// Cotton Sandstorm distributes leaked data through Telegram (Microsoft, 2023)
DeviceNetworkEvents
| where RemoteUrl has "api.telegram.org"
    or RemoteUrl has "t.me"
| where InitiatingProcessFileName !in~ ("Telegram.exe", "telegram-desktop")
| project Timestamp, DeviceName, RemoteUrl,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

- ☐ Review cloud storage upload activity for large or unusual file uploads, especially archives
- ☐ Monitor for Telegram Bot API connections from non-Telegram applications (data exfiltration indicator)
- ☐ Check for new cloud storage accounts created using corporate email addresses
- ☐ Audit file sharing links created in corporate cloud storage for external sharing with unknown parties

A Appendix A: Indicators of Compromise

Blocking Guidance: 3-Tier IOC Classification

Tier 1: Block (High Confidence)

DMARC/SPF policy enforcement (p=reject): The most effective defense against Cotton Sandstorm's mass email spoofing campaigns. Enforce strict DMARC policies for all organizational domains.

Phishing-resistant MFA (FIDO2, certificate-based): Blocks credential access techniques documented in CISA AA24-241A.

Tier 2: Alert / Monitor (Shared Infrastructure)

VPN / proxy / hosting provider IPs: Cotton Sandstorm uses commercial VPN services (DOJ, 2021). Blocking VPN ranges will affect legitimate users. Implement contextual alerting: flag VPN-sourced connections to admin portals and sensitive systems for analyst review. Do NOT block at network level.

Cloud storage and file hosting services: The group uses legitimate cloud platforms for data hosting. Monitor for unusual upload patterns rather than blocking cloud services.

Tier 3: Investigate (Unconfirmed)

Technical IOCs (hashes, C2 domains, malware samples): Specific technical IOCs for Cotton Sandstorm are not available from public sources reviewed during this research session. The DOJ indictment, CISA advisories, and Microsoft reporting describe behavioral patterns but do not publish detailed indicator sets. Organizations that believe they may be targeted should contact CISA or the FBI for access to restricted indicators.

IOC Availability Gap

Cotton Sandstorm has significantly thinner public IOC documentation than other Iranian groups. No specific file hashes, C2 domains, or malware sample identifiers are available from the public sources reviewed for this guide. All detection in this guide relies on behavioral patterns rather than signature-based matching. This is a known limitation. Security teams should supplement this guide with:

- CISA AIS (Automated Indicator Sharing) feeds for real-time Iranian threat indicators
- FBI InfraGard membership for access to restricted threat intelligence
- Microsoft Threat Intelligence APIs for Cotton Sandstorm tracking data
- Sector-specific ISACs (EI-ISAC for election infrastructure, IT-ISAC for technology)

Sanctioned Entities

Entity	Type	Status	Source
Emennet Pasargad	IRGC front company	Sanctioned (OFAC, E.O. 13848)	U.S. Treasury (2021)
Aria Sepehr Ayandehsazan (ASA)	Rebranded front company	Indicted (DOJ, 2024)	DOJ Superseding Indictment (2024)
Seyyed Mohammad Hosein Musa Kazemi	Individual operator	Indicted; $10M reward	DOJ (2021); Rewards for Justice
Sajjad Kashian	Individual operator	Indicted; $10M reward	DOJ (2021); Rewards for Justice

Known Personas

Persona	Type	Context	Source
Proud Boys (spoofed)	False-flag impersonation	2020 U.S. election voter intimidation emails	DOJ Indictment (Nov 2021)
Atlas Group	Hack-and-leak persona	Data leak operations against Israeli targets	Microsoft (2023)
Hackers of Savior	Hacktivist persona	Website defacement and influence operations	Microsoft (2023)
Al-Toufan	Hacktivist persona	Influence operations	Microsoft (2023) [REQUIRES VERIFICATION for specific attribution]

B Appendix B: Detection Rules

KQL Detection Rules

Email Domain Spoofing Detection KQL

DETECTION ONLY

MICROSOFT DEFENDER FOR OFFICE 365

```
// RULE: Detect spoofed outbound email (Cotton Sandstorm mass email TTP)
EmailEvents
| where EmailDirection == "Outbound"
| where SenderFromDomain != SenderMailFromDomain
| summarize EmailCount = count(),
    Recipients = dcount(RecipientEmailAddress)
    by SenderFromAddress, SenderMailFromDomain, bin(Timestamp, 1h)
| where EmailCount > 50
| extend AlertSeverity = "High"
| project Timestamp, SenderFromAddress, SenderMailFromDomain,
    EmailCount, Recipients, AlertSeverity
```

Website Defacement Detection KQL

DETECTION ONLY

MICROSOFT DEFENDER FOR ENDPOINT

```
// RULE: Detect unauthorized modification of web content files
DeviceFileEvents
| where ActionType == "FileModified"
| where FolderPath has_any ("wwwroot", "inetpub", "htdocs", "public_html")
| where FileName in~ ("index.html", "index.htm", "index.php",
    "default.aspx", "default.html")
| where InitiatingProcessFileName !in~ ("msdeploy.exe", "w3wp.exe",
    "dotnet.exe")
| extend AlertSeverity = "Critical"
| project Timestamp, DeviceName, FileName, FolderPath,
    InitiatingProcessFileName, AlertSeverity
```

Mass File Destruction Detection KQL

DETECTION ONLY

MICROSOFT DEFENDER FOR ENDPOINT

```
// RULE: Detect mass file deletion/modification (destructive activity)
DeviceFileEvents
| where ActionType in ("FileDeleted", "FileModified")
| summarize FileCount = count(),
    DistinctExtensions = dcount(tostring(split(FileName, ".")[-1]))
    by DeviceName, InitiatingProcessFileName, bin(Timestamp, 5m)
| where FileCount > 500
| extend AlertSeverity = "Critical"
| project Timestamp, DeviceName, InitiatingProcessFileName,
    FileCount, DistinctExtensions, AlertSeverity
```

Password Spraying Detection KQL

DETECTION ONLY

MICROSOFT SENTINEL / AZURE AD

```
// RULE: Detect password spraying (CISA AA24-241A indicator)
SigninLogs
| where ResultType != 0
| summarize FailedAttempts = count(),
    TargetAccounts = dcount(UserPrincipalName)
    by IPAddress, bin(TimeGenerated, 15m)
| where FailedAttempts > 20 and TargetAccounts > 5
| extend AlertSeverity = "High"
| project TimeGenerated, IPAddress, FailedAttempts,
    TargetAccounts, AlertSeverity
```

C Appendix C: References

Government Advisories & Legal Documents

[1] **U.S. Department of Justice** - "Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election" (November 2021)
justice.gov

[2] **CISA** - Advisory AA24-241A: "Iranian Cyber Actors' Brute Force and Credential Access Activity Compromises Critical Infrastructure" (August 2024)
cisa.gov

[3] **U.S. Department of Treasury / OFAC** - Designation of Emennet Pasargad under E.O. 13848 (November 2021)

[4] **FBI** - FBI Flash: Indicators Associated with Emennet Pasargad (2021-2022)

[5] **U.S. Department of Justice** - Superseding Indictment: Aria Sepehr Ayandehsazan (ASA) (2024)

[6] **U.S. State Department / Rewards for Justice** - Reward offer for Iranian election interference information (2021)

Vendor Threat Intelligence

[7] **Microsoft Threat Intelligence** - "Iran Turning to Cyber-Enabled Influence Operations for Greater Effect" (February 2023)

[8] **Microsoft Threat Intelligence** - "Iran Steps Up Influence Operations Aimed at U.S. Election" (August 2024)

[9] **Microsoft Threat Intelligence** - Digital Threats from East Asia and Iran: Influence Operations Reporting (2023-2024)

Intruvent Intelligence

[10] **Intruvent Technologies** - INT-GSR-2026-IRANCONFLICT-v1.3: Iran Conflict Geopolitical Situation Report (March 2026)

[11] **Intruvent Technologies** - INT-TAP-2026-COTTONSANDSTORM-v1.0: Cotton Sandstorm Threat Actor Profile (March 2026)

NEED HELP IMPLEMENTING THESE DETECTIONS?

Our threat hunting team can deploy, tune, and operationalize these detection rules in your environment.

✓ Detection rule deployment and tuning
✓ Managed threat hunting operations
✓ Incident response retainer

Contact Our Team

or

Automate continuous detection with BRACE, our sector-specific threat intelligence platform. See BRACE plans →