INTRUVENT

THREAT ACTOR INTELLIGENCE PROFILE

Cotton Sandstorm

IRGC Influence Operations and Destructive Capability Group / Emennet Pasargad / Neptunium

Version 1.0
Last Updated March 18, 2026
Classification TLP:CLEAR
Attribution Confidence HIGH

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

IO + D

Influence Operations Combined with Destructive Capability

IRGC-linked group specializing in hack-and-leak, election interference, and psychological warfare since 2020

1 Attribution & Identity

ATTRIBUTION CONFIDENCE: HIGH

Cotton Sandstorm is assessed with high confidence to be an Iranian state-sponsored cyber operations group operating under direction of the Islamic Revolutionary Guard Corps (IRGC). The U.S. Department of Justice unsealed indictments against two Emennet Pasargad employees (Seyyed Mohammad Hosein Musa Kazemi and Sajjad Kashian) in November 2021, directly linking the company to the 2020 U.S. election interference campaign. The U.S. Department of Treasury sanctioned Emennet Pasargad as an IRGC front company. Microsoft Threat Intelligence tracks this group as Cotton Sandstorm (formerly Neptunium). In 2024, a superseding indictment added additional charges related to continued operations under the rebranded company name Aria Sepehr Ayandehsazan (ASA).

Background

Cotton Sandstorm is an Iranian threat actor distinguished from other Iranian groups by its primary focus on influence operations, hack-and-leak campaigns, and psychological warfare rather than traditional espionage or purely destructive operations. The group operates through the front company Emennet Pasargad (rebranded to Aria Sepehr Ayandehsazan in 2024), which provides commercial cover for IRGC-directed cyber operations.

The group first gained international attention through its voter intimidation campaign during the 2020 U.S. presidential election. It obtained voter registration data from at least one U.S. state, sent threatening emails to Democratic voters while impersonating the Proud Boys, and attempted to distribute a fabricated video alleging election fraud. This operation demonstrated the group's willingness and capability to conduct influence operations against Western democracies.

Cotton Sandstorm has evolved beyond pure influence operations. Microsoft Threat Intelligence reported in 2023 that the group had expanded its capabilities to include destructive attacks. This convergence of influence operations and destructive capability makes Cotton Sandstorm a uniquely versatile threat actor within the Iranian cyber ecosystem. While groups like APT33 and Agrius focus on espionage or destruction, Cotton Sandstorm combines network intrusion, data theft, and amplified public messaging into coordinated campaigns designed to maximize psychological impact.

Known Aliases

`Cotton Sandstorm (Microsoft)` `Neptunium (Microsoft, legacy)`
`Emennet Pasargad (Company name)`
`Aria Sepehr Ayandehsazan / ASA (Rebranded company)`
`Haywire Kitten (CrowdStrike)` `DEV-0198 (Microsoft, legacy)`

Operational Personas

Cover identities and false-flag operations used for specific campaigns.

`Proud Boys (spoofed, 2020)` `Atlas Group (hack-and-leak persona)`
`Hackers of Savior (hacktivist persona)` `Al-Toufan (hacktivist persona)`

QUICK FACTS

- **Origin:** Iran (IRGC)
- **Active Since:** 2020 (earliest confirmed)
- **Motivation:** Influence operations, psychological warfare, destructive capability
- **Sophistication:** Moderate to High
- **Last Observed:** March 2026 (Operation Epic Fury posture)
- **Sponsor:** IRGC
- **Signature TTP:** Hack-and-leak combined with amplification campaigns
- **Front Company:** Emennet Pasargad / Aria Sepehr Ayandehsazan

> *"Cotton Sandstorm, an Iranian threat actor linked to Iran's Islamic Revolutionary Guard Corps (IRGC), has matured its influence operations by deploying a wider range of online personas and expanding its network of cyber-enabled influence operations."*
>
> Microsoft Threat Intelligence, Iran Turning to Cyber-Enabled Influence Operations (February 2023)

2 Targeting Profile

Industries

- **Elections / Democracy** (2020 U.S. election, 2024 election cycle)
- **Government** (U.S. state voter databases, Israeli government)
- **Media / Broadcasting** (website defacement, disinformation)
- **Sports / Events** (2022 FIFA World Cup, 2024 Paris Olympics targeting)
- **Technology** (network scanning, infrastructure abuse)
- **Critical Infrastructure** (assessed, post-Epic Fury)

Regions

- **United States** (primary influence target, 2020-present)
- **Israel** (hack-and-leak, destructive operations)
- **Europe** (France, 2024 Olympics targeting)
- **Gulf States** (influence operations)
- **Global** (broad social media manipulation)

Technologies Targeted

- **Voter Registration Systems** (state election infrastructure)
- **Web Applications** (website defacement)
- **Email Infrastructure** (mass spoofed email campaigns)
- **Social Media Platforms** (fake persona networks)
- **Streaming / IPTV** (broadcast interception attempts)
- **Cloud Services** (data hosting for leak operations)

Influence-Destruction Convergence

Microsoft reported in 2023 that Cotton Sandstorm had expanded beyond pure influence operations to include destructive attacks. This convergence means the group can steal data, amplify it through fake personas and social media manipulation, and then destroy the victim's infrastructure to compound the psychological and operational impact. This "hack, leak, destroy, amplify" pattern is the group's operational signature.

3 Tactics, Techniques & Procedures

The following techniques are attributed to Cotton Sandstorm based on the DOJ indictment (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. Technique IDs below reference the ATT&CK Enterprise matrix.

RECONNAISSANCE

- `T1589.002` Gather Victim Identity: Email Addresses
- `T1593` Search Open Websites/Domains
- `T1595` Active Scanning

INITIAL ACCESS

- `T1190` Exploit Public-Facing Application
- `T1078` Valid Accounts
- `T1566` Phishing (credential harvesting)

PERSISTENCE

- `T1505.003` Web Shell
- `T1078` Valid Accounts

COLLECTION

- `T1530` Data from Cloud Storage
- `T1213` Data from Information Repositories
- `T1114` Email Collection

EXFILTRATION

- `T1567` Exfiltration Over Web Service

IMPACT

- `T1491.002` CORE External Defacement (website defacement)
- `T1498` Network Denial of Service
- `T1485` Data Destruction
- `T1561` Disk Wipe [REQUIRES VERIFICATION]

RESOURCE DEVELOPMENT

- `T1583.001` Acquire Infrastructure: Domains
- `T1585.001` Establish Accounts: Social Media
- `T1585.002` Establish Accounts: Email
- `T1608` Stage Capabilities

INFLUENCE OPERATIONS (NON-ATT&CK)

- CORE Hack-and-leak via fabricated personas
- CORE Mass threatening email campaigns
- CORE Fabricated video/media creation
- CORE Social media amplification networks
- CORE Election interference / voter intimidation

MITRE ATT&CK Coverage Gap

Cotton Sandstorm is not currently tracked as a standalone group in the MITRE ATT&CK framework (as of March 2026). The techniques listed above are derived from DOJ indictment details, CISA advisories, Microsoft Threat Intelligence reporting, and FBI Flash alerts. Some technique mappings are analytical assessments based on described behaviors. Techniques marked [REQUIRES VERIFICATION] lack direct vendor confirmation of specific ATT&CK ID mapping.

Kill Chain Pattern: Hack, Leak, Amplify, Destroy

Cotton Sandstorm follows a distinctive operational pattern: (1) gain access to target systems through exploitation or credential theft, (2) exfiltrate sensitive data, (3) stage the data on leak sites or distribute through fabricated personas, (4) amplify the leak through social media manipulation and mass communications, and (5) in later operations, destroy victim infrastructure. This multi-phase approach maximizes psychological and reputational damage while supporting Iranian strategic objectives.

4 Tooling & Infrastructure

Known Tools and Capabilities

Capability	Type	Description	Source
Open-source reconnaissance tools	Reconnaissance	Scanning of voter registration databases and election infrastructure using publicly available tools. The indictment described use of commercial scanning products to identify vulnerable websites.	DOJ Indictment (Nov 2021)
Mass email infrastructure	Influence Operations	Capability to send tens of thousands of spoofed emails. In the 2020 election operation, threatening emails were sent to registered voters across multiple U.S. states while impersonating the Proud Boys.	DOJ Indictment (Nov 2021); FBI
Fabricated video production	Influence Operations	Created and attempted to distribute a fabricated video purporting to show election fraud. The video was designed to undermine confidence in the election process.	DOJ Indictment (Nov 2021)
Social media persona networks	Influence Operations	Created and managed networks of fake social media accounts across multiple platforms for amplification and disinformation. Microsoft reported expanded persona networks in 2023.	Microsoft Threat Intelligence (Feb 2023)
Website defacement tools	Destructive / Psychological	Capability to deface websites with propaganda messaging. Used against multiple Israeli targets. [REQUIRES VERIFICATION] for specific tooling details.	Microsoft Threat Intelligence (2023)
Custom malware / destructive tools	Destructive	Microsoft reported in 2023 that Cotton Sandstorm expanded capabilities to include destructive attacks. Specific malware families have not been publicly named in detail. CISA AA24-241A (2024) described use of default credentials and open-source tools for initial access, with custom scripts for data exfiltration and infrastructure manipulation.	Microsoft (2023); CISA AA24-241A (2024)
AI-generated content	Influence Operations	Microsoft reported in 2024 that Cotton Sandstorm had begun using AI-generated content to support influence operations targeting the 2024 U.S. election cycle. [REQUIRES VERIFICATION] for specific AI tooling used.	Microsoft Threat Intelligence (Aug 2024)

Infrastructure

Category	Details	Source
Front Company	Emennet Pasargad, an Iranian cybersecurity company that served as a front for IRGC operations. Rebranded to Aria Sepehr Ayandehsazan (ASA) after public exposure. Sanctioned by U.S. Treasury Department.	DOJ (2021); Treasury OFAC (2021); DOJ Superseding Indictment (2024)
Email Infrastructure	Used compromised and fabricated email accounts to send mass threatening messages. Spoofed the identity of the Proud Boys organization for voter intimidation emails.	DOJ Indictment (Nov 2021)
Leak Sites / Data Hosting	Registered domains and used cloud services to host stolen data for hack-and-leak operations. Distributed data through Telegram channels and purpose-built websites.	Microsoft (2023); FBI (2021)
Social Media	Maintained persistent networks of fake accounts across Facebook, Twitter/X, Instagram, and Telegram for amplification. Microsoft reported expanded persona networks in 2023.	Microsoft (Feb 2023)
VPN / Anonymization	Used commercial VPN services for operational anonymization. The DOJ indictment described use of VPN services to mask Iranian origin of operations. [REQUIRES VERIFICATION] for specific VPN providers used.	DOJ Indictment (Nov 2021)

Limited Technical IOC Availability

Cotton Sandstorm has significantly thinner public technical documentation compared to other Iranian groups (APT33, APT34, Agrius). The DOJ indictment and CISA advisories describe operational behaviors but provide limited specific technical indicators (file hashes, C2 domains, malware samples). Microsoft has not published detailed IOC lists for Cotton Sandstorm operations. The IOC section of this report reflects these gaps.

5 Notable Campaigns

2020 U.S. Presidential Election Voter Intimidation

Oct 2020

United States
Elections
Influence Operations
Voter Intimidation

Cotton Sandstorm's most publicly documented campaign. The group obtained voter registration data from at least one U.S. state election website. Using this data, operatives sent threatening emails to tens of thousands of registered Democratic voters, impersonating the Proud Boys, a U.S. far-right group. The emails threatened recipients with consequences if they did not vote for the incumbent president. Simultaneously, the group created and attempted to distribute a fabricated video purporting to show fraudulent mail-in ballot manipulation. The DOJ indicted Seyyed Mohammad Hosein Musa Kazemi and Sajjad Kashian for this operation in November 2021.

HBO Intrusion and Data Theft

2017

United States
Media / Entertainment
Hack-and-Leak

Prior to the 2020 election campaign, Emennet Pasargad personnel were linked to the 2017 intrusion of HBO (Home Box Office) networks. The operation resulted in the theft and public leak of unaired television episodes and internal documents. The DOJ indictment referenced this operation as demonstrating the group's pre-existing hack-and-leak capability. The HBO intrusion established the operational pattern of data theft followed by public disclosure for maximum impact.

Attribution Note

The HBO hack attribution to Emennet Pasargad personnel is based on the DOJ indictment. The operation predates the "Cotton Sandstorm" designation. Some sources attribute this operation to the individual actors rather than the organizational group.

Israeli Infrastructure Hack-and-Leak Operations

2021-2023

Israel
Government
Hack-and-Leak
Website Defacement

Microsoft Threat Intelligence reported that Cotton Sandstorm conducted multiple hack-and-leak operations and website defacements against Israeli targets between 2021 and 2023. These operations used fabricated hacktivist personas to distribute stolen data and amplified messaging through social media networks. The group targeted Israeli government websites and private sector organizations, combining data theft with public messaging designed to undermine confidence in Israeli cybersecurity defenses.

Source Limitation

Microsoft described these operations in aggregate reporting. Individual campaign details (specific victims, dates, volumes of data stolen) are not available from reviewed public sources.

2022 FIFA World Cup Influence Operation

Nov 2022

Qatar
Global
Sports Events
Influence Operations

Microsoft reported that Cotton Sandstorm conducted influence operations surrounding the 2022 FIFA World Cup in Qatar. The operation used social media personas to amplify messaging around the event. Specific objectives included undermining the host country's reputation and promoting Iranian strategic narratives. [REQUIRES VERIFICATION] for specific operational details and impact metrics.

2024 U.S. Election Cycle Targeting

2024

United States
Elections
Influence Operations
AI-Generated Content

Microsoft Threat Intelligence reported in August 2024 that Cotton Sandstorm had begun laying groundwork for influence operations targeting the 2024 U.S. presidential election. The group reportedly expanded its use of AI-generated content for social media manipulation and fake persona creation. A DOJ superseding indictment (2024) added charges related to continued operations under the rebranded company name Aria Sepehr Ayandehsazan (ASA), confirming that the group remained operationally active despite the 2021 indictment and sanctions.

2024 Paris Olympics Targeting

Jul-Aug 2024

France
Global
Sports Events
Influence Operations

Microsoft reported Cotton Sandstorm conducted influence operations targeting the 2024 Paris Olympics, continuing the group's pattern of targeting high-profile international sporting events. The operation used fabricated personas and social media amplification to spread anti-Israel messaging tied to the conflict in Gaza. [REQUIRES VERIFICATION] for specific operational methods and infrastructure used.

Operation Epic Fury Posture

Feb-Mar 2026

United States
Israel
Influence Operations
Destructive Capability

Following the commencement of U.S. and Israeli military strikes on Iran (Operation Epic Fury, February 28, 2026), Cotton Sandstorm was listed among 15+ Iranian APT groups assessed to be activated by the IRGC and MOIS. The Intruvent Iran Conflict SITREP (INT-GSR-2026-IRANCONFLICT) identifies Cotton Sandstorm as part of the activated threat landscape. The group's combined influence operations and destructive capability make it a significant concern for organizations in government, media, elections, and critical infrastructure sectors during the current conflict.

Assessed current posture: Cotton Sandstorm is likely conducting or preparing influence operations targeting Western audiences to shape narrative around the Iran conflict. The group's demonstrated willingness to target U.S. election infrastructure and its expanded destructive capability (reported by Microsoft, 2023) suggest it may attempt combined hack-and-leak plus destructive operations against Western targets. Confidence: MODERATE.

6 Detection & Response Recommendations

Detection Opportunities

Influence Operation Infrastructure

- > Anomalous bulk email originating from your domain (spoofing detection)
- > Newly registered domains mimicking your organization or executives
- > Fabricated social media accounts referencing your organization or data
- > Unexpected data appearing on paste sites or Telegram channels
- > Inbound credential phishing campaigns targeting employee accounts

Hack-and-Leak Indicators

- > Large-volume data exfiltration to cloud storage services
- > Unauthorized access to databases containing PII or sensitive records
- > Creation of archive files (ZIP, 7z, RAR) on servers by unexpected processes
- > Web shell deployment on public-facing servers
- > Unusual VPN or proxy connections to administrative interfaces

Website Defacement

- > Unauthorized modifications to web server content files
- > Changes to index.html or landing pages outside deployment windows
- > Web server processes writing HTML/JS files to document roots
- > CMS admin panel access from unusual locations or IP ranges

Destructive Activity

- > Mass file deletion or modification patterns
- > Shadow copy deletion combined with file system changes
- > Unexpected service termination or system shutdown commands
- > Database drop or truncation commands from unexpected sources

Sample Detection Queries

Mass Spoofed Email Detection (KQL)

DETECTION ONLY

```
// Detect mass outbound email that may indicate spoofed campaigns
// Cotton Sandstorm sent tens of thousands of spoofed emails (DOJ, 2021)
EmailEvents
| where EmailDirection == "Outbound"
| where SenderFromDomain != SenderMailFromDomain  // SPF domain mismatch
| summarize EmailCount = count(), Recipients = dcount(RecipientEmailAddress)
    by SenderFromAddress, SenderMailFromDomain, bin(Timestamp, 1h)
| where EmailCount > 100
| sort by EmailCount desc
```

Website Content Modification Detection (KQL)

DETECTION ONLY

```
// Detect unauthorized modifications to web server content
// Cotton Sandstorm conducts website defacement (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 ".js"
| where InitiatingProcessFileName !in~ ("w3wp.exe", "httpd.exe", "nginx.exe")
| project Timestamp, DeviceName, FileName, FolderPath,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

Bulk Data Staging for Exfiltration (KQL)

DETECTION ONLY

```
// Detect large archive creation that may precede hack-and-leak operations
DeviceProcessEvents
| where FileName in~ ("7z.exe", "7za.exe", "rar.exe", "zip.exe")
| where ProcessCommandLine has "a"  // Archive creation mode
| project Timestamp, DeviceName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

Voter Database / PII Access Monitoring (KQL)

INVESTIGATION AID

```
// For organizations managing voter registration or PII databases
// Monitor for bulk data extraction attempts
DeviceNetworkEvents
| where RemotePort in (1433, 3306, 5432, 27017)  // SQL Server, MySQL, PostgreSQL, MongoDB
| where InitiatingProcessFileName !in~ ("sqlservr.exe", "mysqld.exe",
    "postgres.exe", "mongod.exe")
| summarize ConnectionCount = count() by DeviceName,
    InitiatingProcessFileName, RemoteIP, bin(Timestamp, 1h)
| where ConnectionCount > 50
| sort by ConnectionCount desc
```

Election Infrastructure Context

Cotton Sandstorm obtained voter registration data from at least one U.S. state in 2020 (DOJ indictment). Organizations managing voter databases or election infrastructure should implement enhanced monitoring for bulk data access, especially during election cycles.

Web Shell Detection on Public-Facing Servers (KQL)

DETECTION ONLY

```
// Detect web shell file creation on public-facing web servers
DeviceFileEvents
| where ActionType == "FileCreated"
| where FileName endswith ".aspx" or FileName endswith ".php"
    or FileName endswith ".jsp"
| where FolderPath has_any ("inetpub", "wwwroot", "htdocs", "public_html")
| project Timestamp, DeviceName, FileName, FolderPath, SHA256,
    InitiatingProcessFileName
| sort by Timestamp desc
```

A Appendix A: Indicators of Compromise

Blocking Guidance: 3-Tier IOC Classification

Tier 1: Block (High Confidence)

DMARC / SPF enforcement: Enforce strict DMARC (p=reject) and SPF policies to prevent email domain spoofing. This is the most effective defense against Cotton Sandstorm's mass spoofed email campaigns. Not an IOC, but a blocking mechanism.

Tier 2: Alert / Monitor (Shared Infrastructure)

VPN / proxy IPs: Cotton Sandstorm uses commercial VPN services for anonymization. Blocking VPN provider IP ranges will affect legitimate employees and partners. Recommend contextual monitoring: alert on VPN connections to administrative interfaces and require analyst review.

Social media persona indicators: Monitor for fake accounts referencing your organization rather than attempting to block at the platform level. Report identified fake accounts to platform trust and safety teams.

Tier 3: Investigate (Unconfirmed)

Cotton Sandstorm technical IOCs: Specific file hashes, C2 domains, and malware samples for Cotton Sandstorm operations are not available from public sources reviewed during this research session. Microsoft, CISA, and the FBI have described operational behaviors but have not published detailed technical IOC lists for this actor. If IOCs become publicly available, classify per the verification workflow before deploying.

Critical IOC Gap

Unlike well-documented Iranian groups (APT33, APT34, Agrius), Cotton Sandstorm lacks publicly available technical IOCs (file hashes, C2 infrastructure, specific malware samples). The DOJ indictment describes operational behaviors, and CISA AA24-241A (2024) provides defensive guidance, but neither publication includes the detailed technical indicators that would enable hash-based or network-based detection. Detection for this actor relies primarily on behavioral indicators and influence operation monitoring.

Organizations that believe they may be targeted by Cotton Sandstorm should contact CISA (central@cisa.dhs.gov) or the FBI Internet Crime Complaint Center (IC3) for access to classified or restricted indicator sets that are not available in public reporting.

Named Individuals (DOJ Indictment)

Name	Role	Source	Status
Seyyed Mohammad Hosein Musa Kazemi	Emennet Pasargad employee; conducted reconnaissance of U.S. election infrastructure and created the voter intimidation emails	DOJ Indictment (Nov 2021)	Indicted; $10M reward offered
Sajjad Kashian	Emennet Pasargad employee; managed infrastructure and contributed to the 2020 election operation	DOJ Indictment (Nov 2021)	Indicted; $10M reward offered

Rewards for Justice

The U.S. State Department's Rewards for Justice program offered up to $10 million for information on foreign government-directed election interference, specifically referencing the Cotton Sandstorm / Emennet Pasargad 2020 election operation. A 2024 superseding indictment named additional individuals associated with the rebranded Aria Sepehr Ayandehsazan (ASA) company.

Sanctioned Entity

Entity	Type	Sanction Details	Source
Emennet Pasargad	IRGC front company	Designated by U.S. Treasury OFAC. Sanctioned under Executive Order 13848 for foreign interference in U.S. elections.	Treasury Department (2021)
Aria Sepehr Ayandehsazan (ASA)	Rebranded front company	Referenced in DOJ 2024 superseding indictment as the successor entity to Emennet Pasargad.	DOJ (2024)

B Appendix B: 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] **U.S. Department of Treasury / OFAC** - Designation of Emennet Pasargad under E.O. 13848 (November 2021)
treasury.gov

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

[4] **FBI** - FBI Flash: Indicators Associated with Emennet Pasargad (2021-2022)
fbi.gov / ic3.gov

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

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

Vendor Threat Intelligence (Primary)

[7] **Microsoft Threat Intelligence** - "Iran Turning to Cyber-Enabled Influence Operations for Greater Effect" (February 2023)
Describes Cotton Sandstorm's expanded persona networks and influence operation maturation.

[8] **Microsoft Threat Intelligence** - "Iran Steps Up Influence Operations Aimed at U.S. Election" (August 2024)
Reports AI-generated content usage and 2024 election cycle targeting.

[9] **Microsoft Threat Intelligence** - Digital Threats from East Asia and Iran: Influence Operations Reporting (2023-2024)
Aggregate reporting on Cotton Sandstorm campaign evolution.

Intruvent Intelligence

[10] **Intruvent Technologies** - INT-GSR-2026-IRANCONFLICT-v1.3: Iran Conflict Geopolitical Situation Report (March 2026)
Lists Cotton Sandstorm among 15+ activated Iranian APT groups following Operation Epic Fury.

TRACK THIS THREAT ACTOR CONTINUOUSLY

BRACE monitors Cotton Sandstorm and 275+ threat actors with sector-specific intelligence, detection rules, and automated alerting.

- ✓ Real-time threat actor tracking
- ✓ Sector-specific risk scoring (ITR)
- ✓ Detection rules updated with each reporting cycle

See BRACE Plans →

or

Need incident response or forensics support? Contact us at contact@intruvent.com