INTRUVENT

THREAT ACTOR INTELLIGENCE PROFILE

Lemon Sandstorm

Assessed IRGC-Linked Espionage and Pre-Positioning Unit

Version 1.1
Last Updated March 18, 2026
Classification TLP:CLEAR
Attribution Confidence HIGH (Iranian state); MODERATE (IRGC linkage)

Intruvent Technologies
INT-TAP-2026-LEMONSANDSTORM-v1.1

Version History
v1.1 (March 18, 2026): Added Section 6, "Access Brokerage Operations (Fox Kitten / Pioneer Kitten)," covering the MITRE G0117 taxonomy overlap, VPN mass exploitation pipeline, access sales to ransomware affiliates and Iranian state groups, Pay2Key ransomware operations, CISA/FBI Advisory AA24-241A key findings, and access brokerage-specific detection indicators. Renumbered Detection section to Section 7.
v1.0 (March 11, 2026): Initial publication.

2+ Years

Confirmed Pre-Positioning Inside Critical National Infrastructure

Microsoft assessment (2024) | Middle East CNI intrusion documented by Fortinet (May 2023 to Feb 2025) | OT network was a confirmed target

1 Attribution & Identity

STATE ATTRIBUTION CONFIDENCE: HIGH | IRGC LINKAGE: MODERATE (ANALYTICAL ASSESSMENT)

Lemon Sandstorm is assessed with **high confidence** to be an Iranian state-sponsored threat actor. The group has been independently tracked by Microsoft, CrowdStrike, Dragos, Mandiant, Secureworks, ClearSky, and MITRE since at least 2017. CISA and the FBI have issued multiple joint advisories (AA20-259A, AA24-241A) attributing its operations to Iran-based actors.

The specific organizational affiliation within the Iranian government remains analytical. Some sources associate the group with Iran's Islamic Revolutionary Guard Corps (IRGC) based on its critical infrastructure targeting patterns and alignment with Iranian strategic objectives. CrowdStrike assesses Pioneer Kitten as "likely a contract element operating in support of the Iranian government, rather than one operated by the government itself." The FBI identified **Danesh Novin Sahand** (registration ID: 14007585836) as a front company used to support the group's malicious cyber activities. *The IRGC linkage should be treated as an analytical inference, not a confirmed attribution.*

Background

Lemon Sandstorm is a long-running Iranian state-sponsored threat group specializing in VPN and network appliance exploitation, persistent access operations, and pre-positioning within critical national infrastructure. Active since at least 2017, the group has compromised over 200 organizations across the defense, energy, government, healthcare, manufacturing, and technology sectors.

The group operates a dual-purpose model: supporting Iranian government intelligence objectives while simultaneously generating revenue through ransomware affiliate partnerships and access brokering. Under the moniker "Br0k3r," the group advertises access to compromised networks on underground forums and Tor-hosted sites. The FBI identified this ransomware activity as potentially unsanctioned by Tehran, noting that group members have expressed concern about Iranian government monitoring of their money-laundering activities (CISA AA24-241A).

In 2025, Dragos documented a formalized handoff model in which Lemon Sandstorm (tracked by Dragos as "Parisite") provides initial IT access to the **Pyroxene** threat group, which specializes in IT-to-OT traversal within aviation, aerospace, defense, and maritime sectors. This operational pipeline represents a significant escalation in the group's capability to enable industrial control system disruption.

Known Aliases

`Lemon Sandstorm` `Pioneer Kitten` `Fox Kitten` `Parisite` `UNC757` `COBALT FOXGLOVE` `RUBIDIUM (deprecated)` `TunnelMaster (deprecated)` `G0117 (MITRE)` `Br0k3r (self-designated)` `xplfinder (self-designated)`

QUICK FACTS

Origin: Iran (assessed IRGC-linked contractor)
Active Since: At least 2017
Motivation: Espionage, pre-positioning, access brokering, ransomware
Sophistication: High
Last Observed: March 2026 (heightened threat)
Front Company: Danesh Novin Sahand
CVEs Exploited: 14+
Custom Tools: 8+ (Fortinet IR report)
Ransomware Affiliations: ALPHV/BlackCat, NoEscape, Ransomhouse, Pay2Key

> *"Pioneer Kitten is likely a contract element operating in support of the Iranian government, rather than one operated by the government itself."*
>
> CrowdStrike, Pioneer Kitten Adversary Profile (2020)

2 Targeting Profile

Industries

- **Energy / Oil & Gas** (primary, since 2017)
- **Water / Utilities**
- **Transportation**
- **Telecommunications**
- **Defense / Military**
- **Government**
- **Healthcare**
- **Manufacturing / Engineering**
- **Technology**
- **Aviation / Aerospace** (via Pyroxene)
- **Maritime** (via Pyroxene)

Regions

- **Middle East** (Israel, UAE, Bahrain, Kuwait)
- **North America** (United States, primary)
- **Western Europe**
- **Australia**
- **North Africa**

Technologies Targeted

- **Pulse Secure / Ivanti VPN**
- **Fortinet FortiOS**
- **Palo Alto PAN-OS**
- **Citrix ADC / NetScaler**
- **F5 BIG-IP**
- **Check Point Security Gateways**
- **ZKTeco BioTime**
- **IIS Web Servers**
- **ICS/SCADA (reconnaissance)**

Critical Infrastructure Pre-Positioning

Microsoft assessed in 2024 that Lemon Sandstorm has maintained persistent access within Western critical national infrastructure for at least two years. The Fortinet incident response report (May 2025) documented a two-year intrusion into a Middle East CNI entity (May 2023 to February 2025), with forensic traces potentially dating back to May 2021. The restricted OT network was confirmed as a key target, though penetration of the OT environment was not confirmed.

3 Tactics, Techniques & Procedures

RECONNAISSANCE
- **T1596** Search Open Technical Databases

INITIAL ACCESS
- **T1190** Exploit Public-Facing Application PRIMARY
- **T1133** External Remote Services
- **T1078** Valid Accounts

EXECUTION
- **T1059** Command and Scripting Interpreter
- **T1059.001** PowerShell
- **T1059.003** Windows Command Shell

PERSISTENCE
- **T1136.001** Create Local Account
- **T1505.003** Web Shell
- **T1546.008** Accessibility Features (Sticky Keys)
- **T1053.005** Scheduled Task
- **T1098** Account Manipulation

PRIVILEGE ESCALATION
- **T1078.002** Domain Accounts
- **T1078.003** Local Accounts

DEFENSE EVASION
- **T1036.004** Masquerade Task or Service
- **T1036.005** Match Legitimate Name/Location
- **T1027.010** Command Obfuscation
- **T1027.013** Encrypted/Encoded File
- **T1562.001** Disable or Modify Tools
- **T1562.010** Downgrade Attack

CREDENTIAL ACCESS
- **T1110** Brute Force
- **T1555.005** Credentials from Password Managers
- **T1552.001** Credentials in Files
- **T1003.001** LSASS Memory
- **T1003.003** NTDS (Volume Shadow Copy)
- **T1056** Input Capture

DISCOVERY
- **T1087.001** Local Account Discovery
- **T1087.002** Domain Account Discovery
- **T1083** File and Directory Discovery
- **T1046** Network Service Discovery
- **T1018** Remote System Discovery
- **T1482** Domain Trust Discovery
- **T1012** Query Registry
- **T1217** Browser Information Discovery

LATERAL MOVEMENT
- **T1021.001** Remote Desktop Protocol
- **T1021.002** SMB/Windows Admin Shares
- **T1021.004** SSH
- **T1021.005** VNC
- **T1105** Ingress Tool Transfer
- **T1210** Exploitation of Remote Services

COLLECTION
- **T1213.005** Data from Microsoft Teams
- **T1530** Data from Cloud Storage
- **T1005** Data from Local System
- **T1039** Data from Network Shared Drive
- **T1560.001** Archive via Utility (7-Zip)

COMMAND & CONTROL
- **T1572** Protocol Tunneling SIGNATURE
- **T1090** Proxy
- **T1102** Web Service
- **T1219** Remote Access Software

EXFILTRATION
- **T1041** Exfiltration Over C2 Channel

IMPACT
- **T1657** Financial Theft (ransomware / access sales)

Signature Technique: Protocol Tunneling (T1572)

Protocol tunneling is the operational hallmark of this threat actor. The group deploys an extensive toolkit of tunneling utilities (Ngrok, SSHMinion, POWSSHNET, Ligolo-ng, Chisel, FRP, Plink) to maintain persistent outbound access from compromised networks. CrowdStrike originally tracked the group as "TunnelMaster" based on this characteristic behavior.

4 Tooling & Infrastructure

Custom Malware (Fortinet IR Report, May 2025)

Eight custom tools identified during the Middle East CNI intrusion investigation (May 2023 to February 2025).

Tool	Type	Description	First Deployed
Havoc	C2 Framework (C++/Golang)	Post-exploitation C2 framework supporting HTTP/HTTPS/SMB transport. Decrypted from `conhost.dll` and injected into cmd.exe. Supports DLL injection, .NET assembly execution, lateral movement, token manipulation, and reverse port forwarding.	May 2023
HanifNet	Backdoor (.NET)	Unsigned .NET executable (`masf.exe`) that retrieves and executes commands from C2 server. Accepts arguments `ml`, `l`, and `1`. Uses XML config file in same directory.	Aug 2023
HXLibrary	Malicious IIS Module (.NET)	Retrieves three identical text files hosted on Google Docs to fetch the C2 server address; then sends web requests to C2 for tasking.	Oct 2023
CredInterceptor	Credential Harvester (DLL)	DLL-based tool that harvests credentials from Windows LSASS process memory.	Nov 2023
RemoteInjector	Payload Loader	Loader component used to execute next-stage payloads, primarily Havoc.	Apr 2024
NeoExpressRAT	Backdoor	Uses Discord for C2 communication. Retrieves configuration from C2 server for follow-on communications.	Aug 2024
RecShell	Web Shell	Reconnaissance-focused web shell for initial access and environment enumeration.	Apr 2024
DropShell	Web Shell	Web shell with file upload capabilities for payload delivery.	Nov 2024

Tunneling and Remote Access Tools

Tool	Type	Source
Ngrok	Tunneling utility (legitimate, repurposed); creates random subdomains for C2	MITRE ATT&CK G0117; CISA AA24-241A
SSHMinion	Custom SSH tunneling tool; namesake characteristic of Pioneer Kitten	CrowdStrike
POWSSHNET	Custom SSH-based backdoor	Secureworks; CrowdStrike
Ligolo / Ligolo-ng	Open-source tunneling and proxy tool	CISA AA24-241A
Chisel	TCP/UDP tunnel over HTTP, secured via SSH	Secureworks
FRP (Fast Reverse Proxy)	Open-source reverse proxy; TCP, UDP, HTTP, HTTPS support	Secureworks; MITRE ATT&CK G0117
Plink (PuTTY Link)	SSH client for tunneling and lateral movement	Fortinet IR; MITRE ATT&CK G0117
MeshCentral Agent	Legitimate RMM software deployed for persistent remote access	Fortinet IR; CISA AA24-241A
AnyDesk	Legitimate remote access tool deployed as backup mechanism	CISA AA24-241A

Credential and Utility Tools

Tool	Type	Source
Mimikatz	Credential dumping from LSASS	Secureworks
PsExec	Remote execution and lateral movement (MITRE S0029)	MITRE ATT&CK G0117
STSRCheck	Custom network scanning and exploitation tool	Secureworks
Servo	Custom tool; limited public documentation	Secureworks
DarkLoadLibrary	Open-source in-memory DLL loader; used to load SystemBC	Fortinet IR
SystemBC	Proxy backdoor and ransomware precursor; loaded via DarkLoadLibrary	Fortinet IR
China Chopper	Open-source web shell (MITRE S0020)	MITRE ATT&CK G0117
contig.exe	Microsoft SysInternals tool repurposed for DLL side-loading	CISA AA24-241A

Ransomware Operations

Ransomware	Relationship	Period	Source
Pay2Key	Operator (information operation)	Nov-Dec 2020	ClearSky Pay2Kitten (Dec 2020)
ALPHV / BlackCat	Affiliate / access provider	2024	CISA AA24-241A (Aug 2024)
NoEscape	Affiliate / access provider	2024	CISA AA24-241A (Aug 2024)
Ransomhouse	Affiliate / access provider	2024	CISA AA24-241A (Aug 2024)
Pay2Key.I2P	Operator / RaaS platform	Feb 2025 to present	Morphisec (Jul 2025)

CVEs Exploited (14 Confirmed)

CVE	Product	Type	First Observed	Source
`CVE-2019-11510`	Pulse Secure VPN	Arbitrary file read	2019	CISA AA20-259A; ClearSky
`CVE-2019-11539`	Pulse Secure VPN	Remote code execution	2019	CISA AA20-259A
`CVE-2018-13379`	Fortinet FortiOS SSL VPN	Path traversal / credential theft	2019	ClearSky; MITRE
`CVE-2019-1579`	Palo Alto GlobalProtect	Remote code execution	2019	ClearSky; MITRE
`CVE-2019-19781`	Citrix ADC / NetScaler	Directory traversal / RCE	2019-2020	CISA AA20-259A; AA24-241A
`CVE-2020-5902`	F5 BIG-IP	Remote code execution	2020	CISA AA20-259A
`CVE-2022-1388`	F5 BIG-IP	Auth bypass / RCE	2022	CISA AA24-241A
`CVE-2023-3519`	Citrix NetScaler ADC/Gateway	Remote code execution	2023	CISA AA24-241A
`CVE-2024-3400`	Palo Alto PAN-OS	Command injection	Apr 2024	CISA AA24-241A
`CVE-2024-24919`	Check Point Security Gateways	Information disclosure	Jul 2024	CISA AA24-241A
`CVE-2024-21887`	Ivanti Connect Secure VPN	Command injection	2024	CISA AA24-241A
`CVE-2023-38950`	ZKTeco BioTime	Vulnerability exploitation	Dec 2024	Fortinet IR (May 2025)
`CVE-2023-38951`	ZKTeco BioTime	Vulnerability exploitation	Dec 2024	Fortinet IR (May 2025)
`CVE-2023-38952`	ZKTeco BioTime	Vulnerability exploitation	Dec 2024	Fortinet IR (May 2025)

Rapid Exploit Adoption

Secureworks reports that this group has adopted new RCE exploits within hours of public disclosure. Organizations with internet-facing VPN, firewall, or gateway appliances should prioritize patching these product families and treat any delay as an active risk.

5 Notable Campaigns

Fox Kitten VPN Campaign

2017-2019

Global | Defense | Energy | 200+ orgs

The group's foundational campaign involved large-scale exploitation of VPN vulnerabilities across Pulse Secure, Fortinet, Palo Alto, and Citrix appliances. ClearSky estimated over 200 companies were compromised, primarily in the defense and energy sectors. ClearSky assessed with medium probability that APT33 and APT34 collaborated within the Fox Kitten campaign framework. The operational fingerprint of using "kharpedar" (with minor variations) as a password in web shells and compromised accounts dates to this period and persists to this day.

Access Broker Operations

Jul 2020

United States | Israel | Underground Forums

CrowdStrike identified an actor associated with Pioneer Kitten advertising access to compromised networks on underground hacking forums. This was the first confirmed monetization of government-directed access. Under the "Br0k3r" moniker, the group later operated a Tor site selling domain administrator credentials, Active Directory hashes, DNS zone files, and domain trust mappings. The CISA/FBI advisory (AA24-241A) confirmed the group "actively participates in locking down networks and devising extortion strategies" for ransomware affiliates rather than simply selling access.

Pay2Key Ransomware Campaign

Nov-Dec 2020

Israel | Insurance | Logistics | Info Operation

Dozens of Israeli companies were targeted with Pay2Key ransomware in a hack-and-leak campaign. The FBI assessed Pay2Key as an information operation aimed at undermining Israeli cyber infrastructure security perceptions, not primarily a financial operation. ClearSky linked Pay2Key to Fox Kitten with medium-high confidence.

ALPHV/BlackCat Ransomware Affiliation

2024

United States | Multiple Sectors

CISA/FBI/DC3 Joint Advisory AA24-241A (August 2024) disclosed that Lemon Sandstorm had partnered with ALPHV/BlackCat, NoEscape, and Ransomhouse ransomware operations. The advisory identified the Br0k3r and xplfinder monikers, the Danesh Novin Sahand front company, TOX identifiers used for communication, and 14 Bitcoin wallet addresses associated with ransomware payments.

Middle East CNI Intrusion (Fortinet IR)

May 2023 - Feb 2025

Middle East | Critical Infrastructure | OT Targeting

Fortinet's incident response team documented a prolonged four-phase intrusion into a Middle East critical national infrastructure entity. The intrusion began with compromised SSL VPN credentials in May 2023 (with forensic traces potentially dating to May 2021). Eight custom tools were deployed across the phases: Havoc, HanifNet, HXLibrary, CredInterceptor, RemoteInjector, NeoExpressRAT, RecShell, and DropShell. The restricted OT network was confirmed as the primary target. When the victim attempted containment, the group responded with new tools (SystemBC, MeshCentral Agent) and re-entry techniques, including ZKTeco BioTime vulnerability exploitation and spear-phishing campaigns targeting 11 employees for Microsoft 365 credentials.

Middle East CNI Intrusion: Four-Phase Campaign

Source: Fortinet FortiGuard Incident Response (May 2025)

PHASE 1: ESTABLISHMENT (MAY 2023 - APR 2024)
- Initial access via compromised SSL VPN credentials
- Web shell deployment on external-facing servers
- Havoc C2 framework (May), HanifNet backdoor (Aug), HXLibrary IIS module (Oct)
- CredInterceptor credential harvester targeting LSASS (Nov)

↓

PHASE 2: CONSOLIDATION (APR 2024 - NOV 2024)
- RecShell recon web shell and RemoteInjector loader deployed (Apr)
- NeoExpressRAT backdoor using Discord for C2 (Aug)
- DropShell file upload web shell (Nov)
- Lateral movement via Plink and Ngrok; email exfiltration

↓

PHASE 3: RESPONSE TO CONTAINMENT (NOV - DEC 2024)
- Victim initiated containment; actor responded within days
- MeshCentral Agent deployed for persistent remote management (Dec)
- SystemBC proxy backdoor loaded via DarkLoadLibrary (Dec)
- SystemBC is a known ransomware precursor, raising concerns of destructive intent

↓

PHASE 4: RE-ENTRY ATTEMPTS (DEC 2024 - FEB 2025)
- Exploitation of ZKTeco BioTime vulnerabilities (CVE-2023-38950/38951/38952)
- Spear-phishing campaign targeting 11 employees for M365 credentials
- OT network confirmed as the primary objective but not penetrated

Pay2Key.I2P Resurgence

Feb 2025

United States | Israel | RaaS

Pay2Key ransomware reemerged after approximately five years, now operating as "Pay2Key.I2P" on the I2P network. According to Morphisec, the updated ransomware incorporates Mimic/ELENOR-Corp capabilities. A coordinated launch campaign promoted the operation across five to six Russian-language darknet forums. The standard affiliate share is 70%, increasing to 80% for attacks targeting "enemies of Iran" (primarily Israel and the United States). Morphisec reported 51+ ransom payouts in the first four months of operation, calling it "a dangerous convergence of Iranian state-sponsored cyber warfare and global cybercrime."

Parisite-Pyroxene Collaboration

Early 2025

United States | Western Europe | Israel | OT/ICS

Dragos identified a formalized collaboration in which Parisite (Lemon Sandstorm) provides initial IT access to the newly tracked Pyroxene threat group. Pyroxene specializes in internal reconnaissance and movement from IT toward OT environments, targeting aviation, aerospace, defense, and maritime sectors across the United States, Western Europe, Israel, and the UAE. This handoff model demonstrates an industrial-scale pipeline for converting IT access into potential OT impact.

Operation Epic Fury: Heightened Threat

Feb 28, 2026 - Present

Critical Infrastructure | Energy | Water | ICS/SCADA

Following the commencement of US and Israeli military strikes on Iran (Operation Epic Fury / Operation Roaring Lion) on February 28, 2026, Lemon Sandstorm represents one of the most immediate threats to Western critical infrastructure. With confirmed pre-positioning inside CNI for at least two years, active ransomware operations, and the Dragos-documented Parisite-Pyroxene handoff model for OT targeting, the group possesses both the access and capability for disruptive ICS/SCADA operations in energy and water sectors.

As of March 11, 2026, no confirmed post-February 28 activation of pre-positioned access has been reported publicly. Multiple government and vendor advisories (CISA, Unit 42, BeyondTrust, CloudSEK) have warned of Iranian cyber retaliation, with 60+ hacktivist groups mobilized within hours of the strikes.

Current Threat Assessment (March 2026)

Lemon Sandstorm's dormant access within critical infrastructure may be activated for disruptive operations in the current escalated threat environment. Organizations in the energy, water, transportation, and telecommunications sectors should treat this as an active and immediate risk. Prioritize: (1) VPN/gateway appliance patching, (2) web shell detection on network appliances, (3) tunneling tool monitoring, (4) OT network segmentation verification.

6 Access Brokerage Operations (Fox Kitten / Pioneer Kitten)

MITRE G0117 TAXONOMY NOTE

MITRE ATT&CK tracks Fox Kitten as **G0117**, listing Lemon Sandstorm, Pioneer Kitten, Parisite, UNC757, and RUBIDIUM as aliases for the same intrusion set. Some vendors (Microsoft, MITRE) treat these designations as a single group. Others (CrowdStrike, Dragos) differentiate the **access brokerage function** from the espionage and pre-positioning missions. This section covers the access broker operational arm: the systematic exploitation of internet-facing VPN and firewall appliances, the sale or transfer of that access to other Iranian groups and criminal ransomware affiliates, and the group's own ransomware operations under the Pay2Key brand.

VPN and Network Appliance Mass Exploitation

The access brokerage model depends on a high-volume, opportunistic initial access pipeline. Fox Kitten continuously scans for internet-facing VPN concentrators, firewalls, and remote access gateways vulnerable to known CVEs. Secureworks reports that the group has weaponized new RCE exploits within hours of public disclosure. The target appliance families and associated CVEs are documented in Section 4 of this report. The operational pattern follows a consistent cycle:

Access Brokerage Pipeline

Source: CISA AA24-241A; CrowdStrike; Secureworks; ClearSky

PHASE 1: MASS SCANNING AND EXPLOITATION
- Automated scanning of Shodan, Censys, and direct IP ranges for vulnerable appliances (T1596)
- Rapid exploitation of VPN/firewall CVEs within hours of public disclosure (T1190)
- Target appliances: Fortinet FortiOS, Pulse Secure/Ivanti, Citrix NetScaler, Palo Alto PAN-OS, F5 BIG-IP, Check Point Security Gateways
- Credential harvesting from VPN session files and configuration databases

↓

PHASE 2: PERSISTENCE AND NETWORK ENUMERATION
- Web shell deployment on compromised appliances (T1505.003)
- Local account creation with trailing dollar signs to evade detection (T1136.001)
- Protocol tunneling via Ngrok, Ligolo, Chisel, FRP, Plink (T1572)
- Active Directory enumeration: domain trust maps, admin accounts, DNS zone files

↓

PHASE 3: ACCESS PACKAGING
- Domain administrator credentials extracted and packaged for sale
- Active Directory hashes, DNS zone files, and domain trust mappings collected
- Access quality assessed: sector, revenue, network size, OT connectivity
- Buyer selection: Iranian intelligence objectives take priority over criminal sales

↓

PHASE 4: ACCESS TRANSFER OR RANSOMWARE DEPLOYMENT
- **Path A (State):** Access transferred to IRGC-affiliated groups for espionage or pre-positioning (e.g., Pyroxene for OT targeting)
- **Path B (Criminal):** Access sold to ransomware affiliates (ALPHV/BlackCat, NoEscape, Ransomhouse) for a percentage of ransom proceeds
- **Path C (Hybrid):** Group directly participates in locking networks and devising extortion strategies alongside ransomware affiliates

Dual-Purpose Access Model

The FBI assessed that group members operate the access brokerage in part as a personal revenue stream, potentially without full sanctioning from Tehran. FBI analysis of intercepted communications revealed that group members expressed concern about Iranian government monitoring of their money-laundering activities (CISA AA24-241A). This creates a situation where the same compromised network may be exploited for both state espionage and criminal ransomware operations, complicating incident response priorities.

Access Sales and Ransomware Affiliate Partnerships

The group's evolution from a pure espionage operator to an access broker was first identified by CrowdStrike in July 2020, when an actor associated with Pioneer Kitten was observed advertising access to compromised networks on underground hacking forums. The CISA/FBI/DC3 Joint Advisory AA24-241A (August 28, 2024) confirmed the scope and sophistication of these operations.

Attribute	Details	Source
Underground Monikers	`Br0k3r` (primary), `xplfinder` (active as of 2024)	CISA AA24-241A
Sales Platform	Tor-hosted site; underground hacking forums	CrowdStrike (2020); CISA AA24-241A
Products Sold	Domain administrator credentials, Active Directory hashes, DNS zone files, domain trust mappings, full network access	CISA AA24-241A
Communication Channels	TOX messaging (IDs documented in Appendix A)	CISA AA24-241A
Ransomware Partners	ALPHV/BlackCat, NoEscape, Ransomhouse	CISA AA24-241A (Aug 2024)
Revenue Model	Percentage of ransom proceeds; group "actively participates in locking down networks and devising extortion strategies" rather than simply selling access	CISA AA24-241A
Front Company	Danesh Novin Sahand (Registration ID: 14007585836)	CISA AA24-241A
Payment Infrastructure	14 Bitcoin wallet addresses identified (see Appendix A)	CISA AA24-241A

Pay2Key Ransomware Operations

Before the group expanded into affiliate partnerships with established ransomware-as-a-service (RaaS) platforms, it developed and operated its own ransomware brand. Pay2Key represents the intersection of Iranian state-sponsored operations and financially motivated cybercrime.

Campaign	Period	Details	Source
Pay2Key (Original)	Nov-Dec 2020	Targeted dozens of Israeli companies in insurance, logistics, and technology sectors. Ransom demands of 7-9 Bitcoin per victim (approximately $140,000 at the time). The FBI assessed Pay2Key as an **information operation** aimed at undermining Israeli cyber infrastructure security perceptions, not primarily a financial operation. ClearSky linked Pay2Key to Fox Kitten with medium-high confidence. Stolen data was leaked on a dedicated site to amplify psychological impact.	ClearSky Pay2Kitten (Dec 2020); FBI
Pay2Key.I2P (Resurgence)	Feb 2025 to present	Pay2Key reemerged after approximately five years, now operating on the I2P anonymity network. Incorporates Mimic/ELENOR-Corp capabilities. Promoted across five to six Russian-language darknet forums. Standard affiliate share: 70%, increasing to 80% for attacks targeting "enemies of Iran" (Israel, United States). Morphisec reported 51+ ransom payouts in the first four months of operation.	Morphisec (Jul 2025)

> *"A dangerous convergence of Iranian state-sponsored cyber warfare and global cybercrime."*
>
> Morphisec, "Pay2Key's Resurgence: Iranian Cyber Warfare Targets the West" (July 2025)

Access Handoff to Iranian State Groups

The access brokerage function serves Iranian strategic intelligence requirements in addition to generating revenue. Two confirmed handoff relationships have been documented:

Receiving Group	Relationship	Objective	Source
Pyroxene	Formalized handoff; Parisite (Lemon Sandstorm) provides initial IT access	IT-to-OT traversal in aviation, aerospace, defense, and maritime sectors	Dragos (2025/2026)
APT33 / APT34	Shared campaign infrastructure; ClearSky assessed medium-probability collaboration	Espionage operations against defense and energy sectors during the Fox Kitten VPN campaign (2017-2019)	ClearSky Fox Kitten Campaign (Feb 2020)

Implications for Incident Response

When Lemon Sandstorm/Fox Kitten compromises a network, incident responders must consider three potential downstream outcomes: (1) the access may be retained for long-term espionage and pre-positioning, (2) the access may be sold or transferred to ransomware affiliates for near-term monetization, or (3) the access may be handed to a specialized group like Pyroxene for OT targeting. A single initial compromise can result in multiple independent threat actors operating within the same network with different objectives and timelines.

CISA/FBI Advisory AA24-241A: Key Findings

The Joint Cybersecurity Advisory AA24-241A, published August 28, 2024, by the FBI, CISA, and the Department of Defense Cyber Crime Center (DC3), represents the most comprehensive U.S. government disclosure on the access brokerage operations. Key findings include:

- The group has been continuously active since at least 2017, targeting organizations in education, finance, healthcare, defense, and local government in the United States, Israel, Azerbaijan, and the UAE.
- A "significant percentage" of the group's operations against U.S. organizations are intended to obtain network access for subsequent collaboration with ransomware affiliates.
- The group does not merely sell access; it "actively participates in locking down networks and devising extortion strategies" alongside its ransomware partners.
- The advisory identified the Danesh Novin Sahand front company (Registration ID: 14007585836) and two TOX communication identifiers used by the group.
- 14 Bitcoin wallet addresses were identified in connection with ransomware payments and access sales.
- The advisory provided detection signatures for web shells on Citrix NetScaler devices, persistence mechanisms on Windows systems, and tunneling tool indicators.

Detection Indicators Specific to Access Brokerage

VPN Exploitation Indicators
- Unauthenticated access to VPN session files or configuration databases on Pulse Secure, Fortinet, Citrix, or Palo Alto appliances
- Web shell files appearing in VPN appliance web directories (`/var/vpn/themes/imgs/`, `/netscaler/logon/`)
- Mass login attempts from a single source IP across multiple VPN accounts
- VPN configuration changes (new local accounts, modified ACLs) outside change windows

Access Handoff Indicators
- Multiple distinct C2 frameworks or tunneling tools appearing within the same compromised environment (suggests access transfer to a second operator)
- New remote access tools (MeshCentral, AnyDesk) deployed after initial compromise tools are already present
- Credential dumping (LSASS, NTDS.dit) followed by a pause, then new activity with different tooling
- AD reconnaissance artifacts (domain trust maps, DNS zone exports) staged for exfiltration

Pay2Key Indicators
- Ransomware notes referencing "Pay2Key" or "pay2key.i2p"
- I2P network traffic from endpoints that do not normally use anonymity networks
- Reverse proxy tools deployed immediately before encryption (lateral movement preparation)
- Data exfiltration to leak sites preceding or accompanying encryption

Operational Fingerprints
- The password string `kharpedar` (with minor variations) in web shell configs, compromised accounts, or authentication logs
- Local accounts with trailing dollar signs (`sqladmin$`) hidden from `net user` output
- Scheduled tasks named `SpaceAgentTaskMgrSHR` or random 8-character strings
- DLL side-loading at `C:\Windows\ADFS\version.dll`

7 Detection & Response Recommendations

Detection Opportunities

VPN/Gateway Appliance Integrity
- Audit all internet-facing VPN, firewall, and gateway appliances for known CVEs exploited by this actor
- Search for web shells in standard appliance web directories (`/var/vpn/themes/imgs/`, `/netscaler/logon/`, `/xui/common/images/`)
- Verify firmware integrity and check for unauthorized modifications
- Review SSL VPN logs for anomalous authentication patterns

Tunneling Tool Detection
- Alert on execution of Ngrok, Chisel, Ligolo, FRP, or Plink from non-standard directories
- Monitor for outbound SSH connections to unusual destinations
- Detect processes creating reverse tunnels or SOCKS proxies
- Monitor for Ngrok subdomain DNS resolution patterns

Credential Harvesting Indicators
- Monitor for LSASS process access by non-standard processes (CredInterceptor, Mimikatz, procdump)
- Detect Volume Shadow Copy creation followed by NTDS.dit extraction
- Alert on KeePass database file access from unusual processes
- Search for the "kharpedar" password string in logs and configuration files

Persistence Artifacts
- Search for accounts: `sqladmin$`, `adfsservice`, `IIS_Admin`, `iis-admin`, `John McCain`
- Audit scheduled tasks for `SpaceAgentTaskMgrSHR` or random 8-character service names
- Check for `C:\Windows\ADFS\version.dll` (DLL side-loading)
- Audit IIS modules for unauthorized .NET assemblies (HXLibrary pattern)

Sample Detection Queries

Web Shell Detection on Network Appliances (KQL)

DETECTION ONLY

```
// Detect web requests to known Lemon Sandstorm web shell paths
// Requires web server or proxy logs ingested into Sentinel
CommonSecurityLog
| where RequestURL has_any (
    "UpdateChecker.aspx",
    "netscaler.php",
    "ctxHeaderLogon.php",
    "sanpdebug.php",
    "ui_style.php"
)
| project TimeGenerated, SourceIP, RequestURL,
    DeviceAction, DestinationHostName
| sort by TimeGenerated desc
```

Tunneling Tool Execution (KQL)

DETECTION ONLY

```
// Detect execution of tunneling tools associated with Lemon Sandstorm
DeviceProcessEvents
| where FileName in~ ("ngrok.exe", "chisel.exe", "ligolo.exe",
    "ligolo-ng.exe", "frpc.exe", "plink.exe")
    or ProcessCommandLine has_any ("ngrok", "chisel", "ligolo",
    "frpc", "ssh -R", "ssh -D", "ssh -L")
| where FolderPath !startswith "C:\\Program Files" and FolderPath !startswith "C:\\Program Files (x86)"
| project Timestamp, DeviceName, FileName,
    ProcessCommandLine, FolderPath, AccountName
| sort by Timestamp desc
```

Suspicious Local Account Creation (KQL)

DETECTION ONLY

```
// Detect creation of accounts matching Lemon Sandstorm patterns
// Note: Dollar-sign suffix accounts are hidden from net user
SecurityEvent
| where EventID == 4720
| where TargetUserName has_any (
    "sqladmin$", "adfsservice", "IIS_Admin",
    "iis-admin", "John McCain")
    or TargetUserName matches regex @"\$$"
| project TimeGenerated, Computer, TargetUserName,
    SubjectUserName, SubjectDomainName
| sort by TimeGenerated desc
```

LSASS Credential Access Detection (KQL)

DETECTION ONLY

```
// Detect non-standard processes accessing LSASS
// Tuning required: baseline your environment for expected LSASS access
DeviceProcessEvents
| where FileName in~ ("procdump.exe", "procdump64.exe", "masf.exe")
    or (ProcessCommandLine has "lsass"
    and FileName !in~ ("svchost.exe", "csrss.exe", "MsMpEng.exe"))
| project Timestamp, DeviceName, FileName,
    ProcessCommandLine, AccountName
| sort by Timestamp desc
```

C2 Domain IOC Match (KQL)

BLOCKING SAFE

```
// Match known Lemon Sandstorm C2 domains
let LemonSandstormDomains = dynamic([
    "api.gupdate.net",
    "gupdate.net",
    "apps.gist.githubapp.net",
    "githubapp.net",
    "login.forticloud.online",
    "fortigate.forticloud.online",
    "cloud.sophos.one"
]);
DnsEvents
| where Name has_any (LemonSandstormDomains)
| project TimeGenerated, Computer, Name,
    IPAddresses, QueryType
| sort by TimeGenerated desc
```

DLL Side-Loading at Known Path (KQL)

BLOCKING SAFE

```
// Detect DLL writes to ADFS directory used for side-loading
DeviceFileEvents
| where FolderPath has "\\Windows\\ADFS\\"
    and FileName =~ "version.dll"
| project Timestamp, DeviceName, FileName,
    FolderPath, InitiatingProcessFileName,
    InitiatingProcessCommandLine
| sort by Timestamp desc
```

A Appendix A: Indicators of Compromise

Blocking Guidance: 3-Tier IOC Classification

Tier 1: Block (High Confidence)

C2 Domains (`api.gupdate[.]net`, `gupdate[.]net`, `apps.gist.githubapp[.]net`, `githubapp[.]net`, `login.forticloud[.]online`, `fortigate.forticloud[.]online`, `cloud.sophos[.]one`): These domains are confirmed C2 and credential harvesting infrastructure with no legitimate use case. Safe to add to DNS block lists and firewall deny rules.

Malware hashes for custom tools (when available from Fortinet PDF report): Confirmed malicious with no legitimate use. Safe for hash-based blocking and EDR prevention policies.

Web shell filenames at documented paths (`UpdateChecker.aspx`, `netscaler.php`, `ctxHeaderLogon.php`, `sanpdebug.php`, `ui_style.php`): Safe to alert on and investigate at the listed file system paths.

Tier 2: Alert / Monitor (Shared Infrastructure)

Cloud provider IPs (DigitalOcean: 138.68.90.19, 167.99.202.130, 134.209.30.220; AWS: 51.16.51.81, 51.20.138.134, 13.53.124.246, 18.134.0.66; Vultr: 45.76.65.42; other VPS: 78.141.238.182): These IPs belong to major cloud and VPS providers. Blocking cloud provider IP ranges will disrupt legitimate services and integrations. Deploy as detection/alerting queries only. Require analyst review before any blocking action. Do NOT block at the network level.

files.catbox[.]moe: Legitimate file hosting service also used by non-malicious actors. Do NOT block the domain. Monitor for connections in context of other indicators only.

Infrastructure ASNs (AS14061/DigitalOcean, AS16509/Amazon-AWS): These ASNs serve millions of legitimate users and services. ASN-level detection queries are for analyst review only. Do NOT deploy as automated blocking rules.

Tier 3: Investigate (Unconfirmed)

Historical IPs without hosting context (193.149.190.248, 206.71.148.78, 193.149.187.41): These historical indicators may no longer be associated with threat activity. Verify current assignment and usage context before any action. Recommend monitoring only if observed in conjunction with other indicators.

Self-signed certificate names (`futureenergy.us`, `next-finance.mil`): Identified by Censys on Fox Kitten infrastructure. Useful for threat hunting but require contextual analysis. The .mil TLD on non-government infrastructure is anomalous and worth investigating.

Network Indicators (IP Addresses)

Indicator	Context	Source	Tier
`138.68.90.19`	Actor infrastructure (DigitalOcean, active through Aug 2024)	CISA AA24-241A	Tier 2: Monitor
`167.99.202.130`	Actor infrastructure (DigitalOcean, active through Aug 2024)	CISA AA24-241A	Tier 2: Monitor
`78.141.238.182`	Actor infrastructure (VPS, active through Aug 2024)	CISA AA24-241A	Tier 2: Monitor
`51.16.51.81`	Actor infrastructure (AWS, active through Aug 2024)	CISA AA24-241A	Tier 2: Monitor
`51.20.138.134`	Actor infrastructure (AWS, active through Aug 2024)	CISA AA24-241A	Tier 2: Monitor
`134.209.30.220`	Actor infrastructure (DigitalOcean, active through Aug 2024)	CISA AA24-241A	Tier 2: Monitor
`13.53.124.246`	Actor infrastructure (AWS, active through Aug 2024)	CISA AA24-241A	Tier 2: Monitor
`18.134.0.66`	Historical actor infrastructure (AWS)	CISA AA24-241A	Tier 2: Monitor
`193.149.190.248`	Historical actor infrastructure	CISA AA24-241A	Tier 3: Investigate
`45.76.65.42`	Historical actor infrastructure (Vultr)	CISA AA24-241A	Tier 2: Monitor
`206.71.148.78`	Historical actor infrastructure	CISA AA24-241A	Tier 3: Investigate
`193.149.187.41`	Historical actor infrastructure	CISA AA24-241A	Tier 3: Investigate

All IP addresses listed above belong to cloud providers, VPS hosts, or have unconfirmed hosting provenance. Blocking any of these IP ranges will affect legitimate services hosted on shared infrastructure. Recommend contextual monitoring and correlation with other indicators before taking blocking action.

Network Indicators (Domains)

Indicator	Context	Source	Tier
`api.gupdate[.]net`	C2 domain (observed since April 2024)	CISA AA24-241A; Censys; Fortinet IR	Tier 1: Block
`gupdate[.]net`	C2 domain (Middle East CNI intrusion)	Fortinet IR (May 2025)	Tier 1: Block
`apps.gist.githubapp[.]net`	Active C2 endpoint (Middle East CNI intrusion)	Fortinet IR (May 2025)	Tier 1: Block
`githubapp[.]net`	C2 domain	CISA AA24-241A; Censys	Tier 1: Block
`login.forticloud[.]online`	Credential harvesting domain impersonating Fortinet	CISA AA24-241A	Tier 1: Block
`fortigate.forticloud[.]online`	Credential harvesting domain impersonating Fortinet	CISA AA24-241A	Tier 1: Block
`cloud.sophos[.]one`	Credential harvesting domain impersonating Sophos	CISA AA24-241A	Tier 1: Block
`files.catbox[.]moe`	Legitimate file hosting used for payload delivery	CISA AA24-241A	Tier 2: Monitor

Web Shell Indicators

Name	Type	Path / Context	Source
`UpdateChecker.aspx`	ASPX web shell (obfuscated C#)	IIS servers; three modules: Base, CommandShell, FileManager	Fortinet IR (May 2025)
`RecShell`	Recon web shell	External-facing servers	Fortinet IR (May 2025)
`DropShell`	File upload web shell	External-facing servers	Fortinet IR (May 2025)
`netscaler.php`	PHP web shell	Citrix NetScaler devices	CISA AA24-241A
`ctxHeaderLogon.php`	PHP web shell	Citrix NetScaler devices	CISA AA24-241A
`netscaler.1`	Web shell	Citrix NetScaler devices	CISA AA24-241A
`sanpdebug.php`	PHP web shell	`/netscaler/logon/sanpdebug.php`	CISA AA24-241A
`ui_style.php`	PHP web shell	`/netscaler/logon/LogonPoint/uiareas/ui_style.php`	CISA AA24-241A
`China Chopper`	Web shell (MITRE S0020)	Various deployments	MITRE ATT&CK G0117

Persistence Artifacts

Type	Indicator	Context	Source
File Path	`/var/vpn/themes/imgs/`	Web shell directory on Citrix NetScaler	CISA AA24-241A
File Path	`/netscaler/logon/LogonPoint/uiareas/`	Web shell deployment directory	CISA AA24-241A
File Path	`/xui/common/images/`	Web shell deployment directory	CISA AA24-241A
File Path	`C:\Windows\ADFS\version.dll`	Malicious DLL side-loading location	CISA AA24-241A
Scheduled Task	`SpaceAgentTaskMgrSHR`	Persistence task (Windows\Spaceport\)	CISA AA24-241A
Local Account	`sqladmin$`	Trailing dollar sign hides from net user	CISA AA24-241A
Local Account	`adfsservice`	Persistence account	CISA AA24-241A
Local Account	`IIS_Admin`	Persistence account	CISA AA24-241A
Local Account	`iis-admin`	Persistence account	CISA AA24-241A
Local Account	`John McCain`	Unusual naming to appear legitimate	CISA AA24-241A
Password Pattern	`kharpedar`	Unique operational fingerprint used since 2017 in web shells and compromised accounts	Secureworks

Actor Identifiers

Type	Indicator	Context	Source
TOX ID (xplfinder)	`ea2ec0c3859d8d8c36d95a298beef6d7add17856655bfbea2554b8714f7c7c69`	Communication identifier	CISA AA24-241A
TOX ID (Br0k3r)	`B761680E23F2EBB5F6887D315EBD05B2D7C365731E093B49ADB059C3DCCAA30C`	Communication identifier	CISA AA24-241A
Front Company	**Danesh Novin Sahand** (Reg. ID: 14007585836)	Iranian IT company used as cover for operations	CISA AA24-241A
Bitcoin Address	`bc1q8n7jjgdepuym825zwwftr3qpem3tnjx3m50ku0`	Ransomware/access sales payments	CISA AA24-241A
Bitcoin Address	`bc1qlwd94gf5uhdpu4gynk6znc5j3rwk9s53c0dhjs`	Ransomware/access sales payments	CISA AA24-241A

CISA AA24-241A lists 14 total Bitcoin wallet addresses. The remaining 12 require manual extraction from the full advisory document or STIX data files. SHA256 hashes for the eight custom malware tools identified in the Fortinet IR report require manual extraction from the PDF at fortinet.com.

Infrastructure Fingerprinting (Censys Analysis, Sep 2024)

Pattern	Details	Use Case
Geolocations	London, Stockholm, Frankfurt, Tel Aviv, Los Angeles	Infrastructure hunting
ASNs	AS14061 (DigitalOcean), AS16509 (Amazon/AWS)	Infrastructure correlation
Software Signatures	Mirth Connect, Ivanti Connect Secure, Ray Dashboard	Host identification
Certificate Patterns	Self-signed with implausible names (`futureenergy.us`, `next-finance.mil`)	Infrastructure discovery
Scale	38,862 additional potentially malicious hosts identified matching these patterns	Ongoing hunting

B Appendix B: References

Government Advisories

[1] **CISA / FBI / DC3** - "Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations" (Advisory AA24-241A, August 28, 2024)
cisa.gov

[2] **CISA / FBI** - "Iran-Based Threat Actor Exploits VPN Vulnerabilities" (Advisory AA20-259A, September 15, 2020)
cisa.gov

[3] **FBI IC3** - "Iran-based Cyber Actors Enabling Ransomware Attacks on U.S. Organizations" (August 28, 2024)
ic3.gov

Vendor Threat Intelligence (Primary)

[4] **Fortinet FortiGuard IR** - "Investigating Iranian Intrusion into Strategic Middle East Critical National Infrastructure" (May 2025)
fortinet.com

[5] **Microsoft Threat Intelligence** - Lemon Sandstorm Tracking (Microsoft Digital Defense Report 2025)
microsoft.com

[6] **CrowdStrike** - "PIONEER KITTEN: Targets & Methods" (September 2020)
crowdstrike.com

[7] **CrowdStrike** - "Pioneer Kitten Adversary Profile"
crowdstrike.com

[8] **Secureworks** - "COBALT FOXGLOVE Threat Profile"
secureworks.com

[9] **ClearSky** - "Fox Kitten Campaign" v1 (February 2020)
clearskysec.com

[10] **ClearSky** - "Pay2Kitten: Fox Kitten 2" (December 2020)
clearskysec.com

[11] **Dragos** - OT/ICS Threat Intelligence, 2026 Year in Review
dragos.com

[12] **Morphisec** - "Pay2Key's Resurgence: Iranian Cyber Warfare Targets the West" (July 2025)
morphisec.com

[13] **Censys** - "Analysis of Fox Kitten Infrastructure Reveals Unique Host Patterns and Potentially New IOCs" (September 2024)
censys.com

[14] **MITRE ATT&CK** - "Fox Kitten, Group G0117"
attack.mitre.org

Investigative Journalism

[15] **The Hacker News** - "Iranian Hackers Maintain 2-Year Access to Middle East CNI via VPN Flaws and Malware" (May 2025)
thehackernews.com

[16] **Dark Reading** - "Lemon Sandstorm Reveals Risks to Middle East Infrastructure" (May 2025)
darkreading.com

[17] **The Register** - "Iranian ransomware crew reemerges, promises big bucks for attacks on US or Israel" (July 9, 2025)
theregister.com

[18] **Bleeping Computer** - "Iranian hackers act as brokers selling critical infrastructure access" (August 28, 2024)
bleepingcomputer.com

OSINT & Analyst Research

[19] **Picus Security** - "Pioneer Kitten: Iranian Threat Actors Facilitate Ransomware Attacks Against U.S. Organizations"
picussecurity.com

[20] **Huntress** - "Fox Kitten Threat Actor Profile"
huntress.com

[21] **Malpedia** - "Fox Kitten"
malpedia.caad.fkie.fraunhofer.de

[22] **FortiGuard Labs** - "Fox Kitten Threat Actor Profile"
fortiguard.fortinet.com

2026 Iran Conflict Context

[23] **CloudSEK** - "A Threat Actor Landscape Assessment of ICS/OT Targeting in the 2026 Iran-US Conflict" (March 2026)
cloudsek.com

[24] **BeyondTrust** - "Threat Advisory: Iran-Aligned Cyber Actors Respond to Operation Epic Fury" (March 2026)
beyondtrust.com

[25] **Trellix** - "The Iranian Cyber Capability"
trellix.com

[26] **Cybersecurity Dive** - "US entities face heightened cyber risk related to Iran war" (March 2026)
cybersecuritydive.com

[27] **Flashpoint** - "Escalation in the Middle East: Tracking Operation Epic Fury Across Military and Cyber Domains" (March 2026)
flashpoint.io

[28] **SecurityWeek** - "3 Threat Groups Started Targeting ICS/OT in 2025: Dragos" (February 2026)
securityweek.com

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

[30] **Proofpoint** - "Iran conflict drives heightened espionage activity against Middle East targets" (March 2026)
proofpoint.com

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

Secondary Sources

[32] **Risky.Biz** - "Iranian APT moonlights as access broker and ransomware helper" (August 2024)
risky.biz

[33] **Red Hot Cyber** - "Fox Kitten and Br0k3r: The Iranian Cyber Contractor Collaborating with Ransomware Gangs"
redhotcyber.com

[34] **FDD** - "Pioneer Kitten: A New Iranian Cyber Threat Group Emerges" (September 16, 2020)
fdd.org

[35] **HHS Cybersecurity** - "Iranian Threat Actors & Healthcare" (November 3, 2022)
hhs.gov

[36] **Cyble** - "Iranian State-Sponsored Hackers Have Become Access Brokers for Ransomware Gangs" (August 2024)
cyble.com

[37] **Bleeping Computer** - "Iranian hackers work with ransomware gangs to extort breached orgs" (August 2024)
bleepingcomputer.com

[38] **SecurityWeek** - "Iranian Hackers Target Israeli Companies With Pay2Key Ransomware" (December 2020)
securityweek.com

TRACK THIS THREAT ACTOR CONTINUOUSLY

BRACE monitors Lemon 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