CloudSEK
REPORTS

Event Report

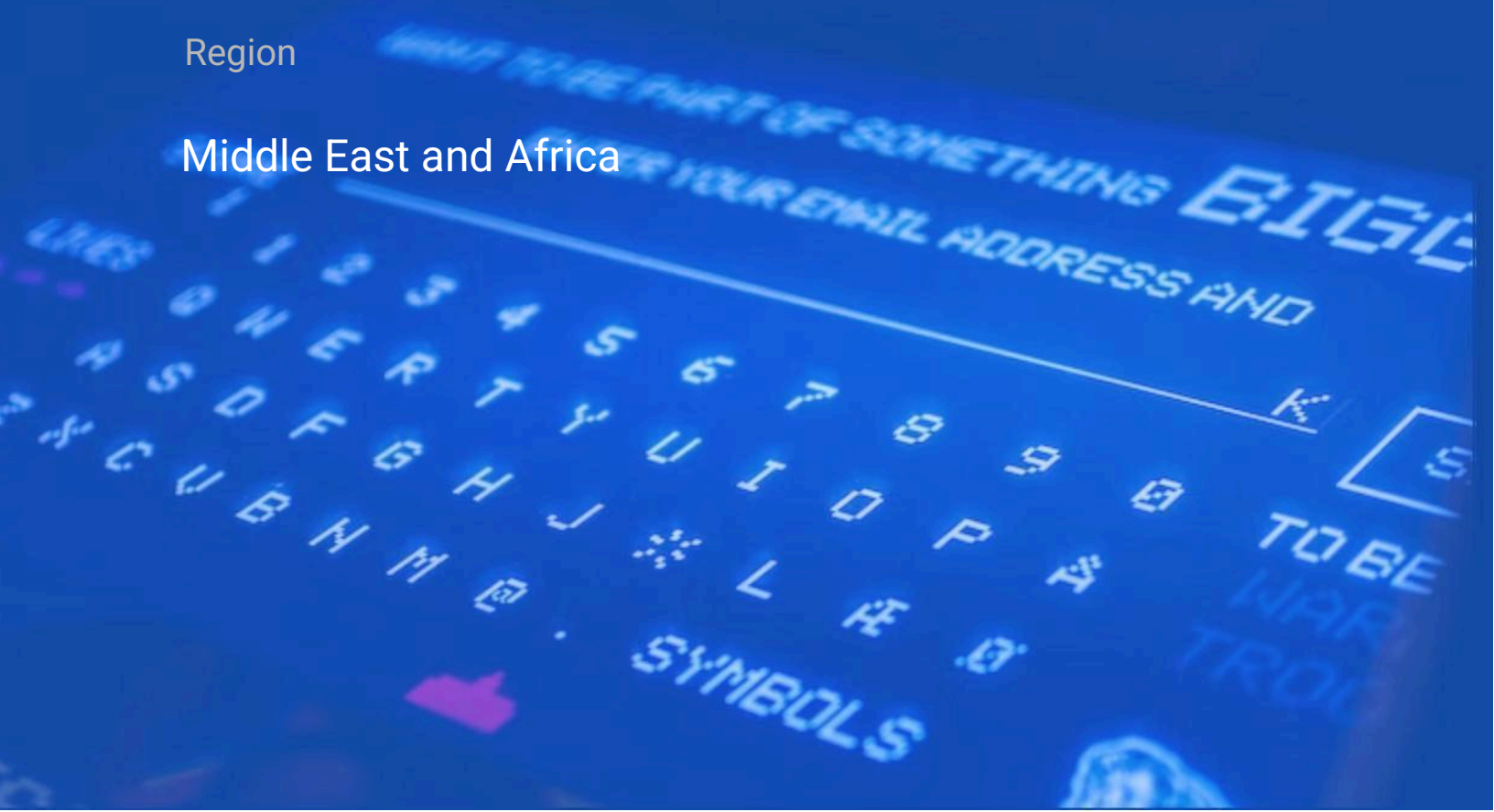
Kitten Had the Map all Along : RAISING GCC TENSIONS & THE PRE-POSITIONING MAP

Category

Adversary Intelligence

Region

Middle East and Africa



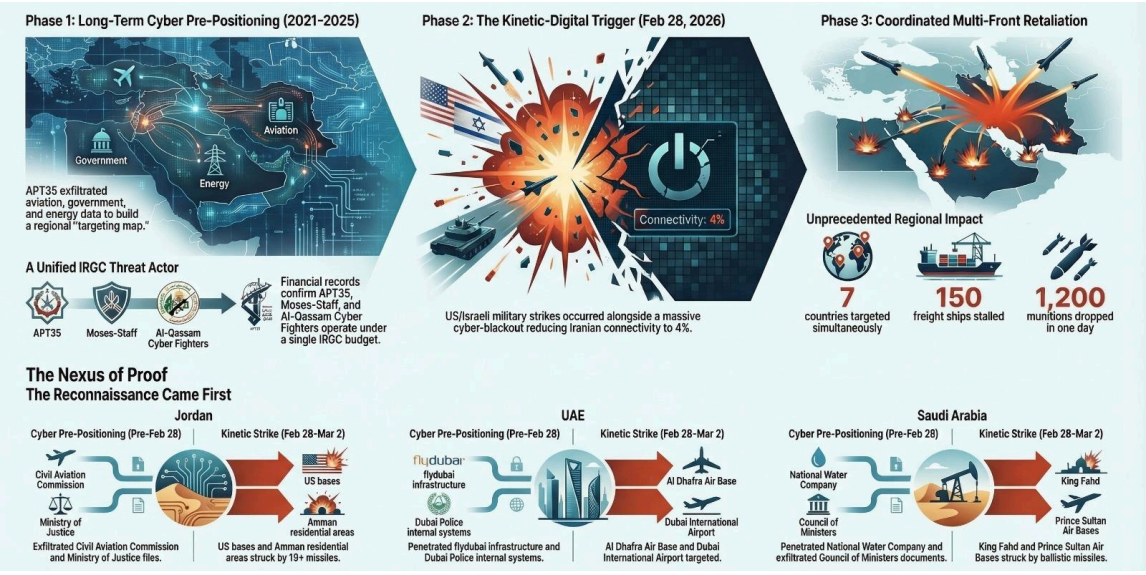
Executive Summary

On February 28, 2026, the United States and Israel launched Operation Epic Fury — a coordinated strike campaign targeting Iran's nuclear infrastructure, ballistic missile production, IRGC command compounds, and senior leadership across 24 of Iran's 31 provinces. Supreme Leader Ali Khamenei is assessed to have been killed during the strikes, though at time of publication that assessment relies on a limited number of corroborating sources. Iran responded with a multi-day ballistic missile and Shahed drone campaign striking seven countries simultaneously: Saudi Arabia, the UAE, Kuwait, Bahrain, Qatar, Jordan, and Israel. That campaign was still active as of our analysis cutoff.

This report looks at the conflict, the cyber operations running in parallel, and the pre-positioned access APT35 appears to have maintained across the region.

The Central Finding: The Reconnaissance Came First

The overlap between APT35's documented cyber operations and Iran's subsequent kinetic targets is, frankly, too consistent to be coincidental — though we stop short of claiming the leak proves a formal operational handoff between cyber collection and kinetic targeting. What we can say with confidence is this: every country Iran struck with missiles had been systematically profiled and in several cases penetrated by APT35 prior to the strikes. Jordan's Ministry of Justice and Civil Aviation Commission. The UAE's Government, Ministry of Education, and flydubai infrastructure. Saudi Arabia's Council of Ministers documents and National Water Company. Kuwait's civil aviation. Qatar's Al Udeid Air Base support infrastructure. Israel's ICS networks, modems (580+ compromised devices), and civilian digital infrastructure.



The specific sequencing matters: APT35 exfiltrated Jordan's Civil Aviation files before Iran struck Jordanian airspace. Dubai Government materials were obtained before strikes targeted Al Dhafra and Dubai airports. Saudi Council of Ministers decision documents were compromised before the first missile hit Riyadh. We think the most parsimonious explanation is that cyber operations served as intelligence preparation for the battlefield — but we acknowledge an alternative interpretation: that both the cyber targeting and kinetic targeting simply reflected the same standing Iranian strategic priorities, without a formal handoff.

The Actor: A Unified IRGC Threat Now Confirmed

APT35 (also tracked as Charming Kitten, Phosphorus, Mint Sandstorm, Magic Hound) is attributed to the IRGC Intelligence Organization, Unit 1500, Department 40, commanded by Abbas Rahrovi (a.k.a. Abbas Hosseini, NID: 4270844116) through front company Zharf Andishaan Tafakkor Sefid. The KittenBusters leak is assessed with high confidence based on a combination of Farsi/Jalali calendar timestamps, blockchain-verified Bitcoin transactions, BellaCiao source code matching Bitdefender's 2023 analysis, granular operator daily reports, and independently confirmed active server credentials. That said, some elements of the dataset remain unverified and we note those caveats where they arise.

One finding from the leak that we did not initially anticipate: Episode 4 Bitcoin records appear to confirm the financial unification of APT35 with two previously distinct personas — Moses-Staff (destructive operations against Israel) and Al-Qassam Cyber Fighters (DDoS against US/Israeli finance). Both appear funded from the same operational budget. This significantly changes the attribution picture for a range of historical operations.

Section 2: Operation Epic Fury - The Conflict in Full

2.1 What Happened: Feb 28, 2026

On the morning of February 28, 2026, the United States and Israel launched what Israeli sources designated Operation Epic Fury (Israeli designation: Roar of the Lion) — a coordinated military campaign striking Iran's nuclear infrastructure, ballistic missile production facilities, IRGC command compounds, naval assets, and senior leadership across 24 of Iran's 31 provinces. The Israeli air force reportedly dropped over 1,200 munitions in a single day, though independent verification of that figure has not been possible at time of writing.

Simultaneously, Israel launched a significant cyber operation against Iran. Iranian internet connectivity dropped to approximately 4% of normal levels (per NetBlocks monitoring). IRGC communications infrastructure, state media, government digital services, and mobile applications went offline. Western intelligence sources cited in open reporting indicated the digital component was intended to disrupt IRGC

command-and-control and limit coordination of retaliatory strikes. Iran also conducted its own partial internet shutdown in some regions — a pattern consistent with past crisis responses.

2.2 Iranian Kinetic Retaliation: The Full Strike Log

Iran responded immediately with an unprecedented multi-day, multi-country ballistic missile and drone campaign under the hashtag #HARD_REVENGE. The IRGC declared all US military assets throughout the region 'legitimate targets' and stated this operation will continue relentlessly until the enemy is decisively defeated.' Below is the confirmed strike log across all targeted countries:

COUNTRY	CONFIRMED MILITARY TARGETS	CONFIRMED CIVILIAN TARGETS STRUCK	SCALE
Saudi Arabia	King Fahd Air Base (Riyadh); Prince Sultan Airbase; King Salman HQ; Eastern Province military sites; King Khalid International Airport (intercepted)	Riyadh residential areas; Eastern Province civilian zones	Multiple ballistic missiles Saudi Arabia declared it 'reserved the right to respond including military options.' Tadawul exchange down 1.5%.
UAE	Al Dhafra Air Base (Abu Dhabi) - penetrated defenses, 1 killed; Jebel Ali Port (fire from debris)	Dubai Palm / Fairmont hotel (fire); Burj Al Arab (debris damage); Dubai International Airport (injuries); Zayed International Airport (1 killed, 7 injured); Etihad Towers area (Israeli embassy vicinity)	167 missiles + 541 UAVs engaged by air defenses per UAE MoD. Multiple penetrations. 3 killed (Pakistani, Nepalese, Bangladeshi nationals); 58 wounded.
Kuwait	Ali Al Salem Air Base (US & Italian troops) intercepted; 97 ballistic missiles & 283 drones total engaged	Kuwait International Airport , terminal damaged by drone (injuries); residential areas struck (1 killed, 32 injured)	Kuwait suspended the stock exchange. The Kuwait Foreign Ministry summoned Iran's ambassador. Kuwait intercepted 97 BMs + 283 drones per government statement.
Bahrain	US Fifth Fleet HQ (Manama/Juffair), parts of HQ struck; Bahrain International Airport targeted	Crowne Plaza Hotel (drone fire); residential tower struck; Era Views Towers apartment building hit by drone; several residential buildings in Manama	45 missiles & 9 drones (incl. Shahed-136) intercepted per government. Bahrain confirmed airport material damage. Air raid sirens activated. Day 2 follow-on strikes.
Qatar	Al Udeid Air Base (largest US air base in Middle East); US radar systems; Doha airport	Residential areas Doha outskirts; RAF Typhoon downed an Iranian drone bound for Qatari airspace (UK involvement confirmed)	44 missiles + 8 UAVs Day 1. Qatar claims to have intercepted all. Qatar Airways suspended flights. Qatar exchange down 2%. Qatar 'reserved right to respond.'
Jordan	US bases; Amman capital; northern regions;	Amman residential areas; north Jordan struck	13 ballistic missiles + 49 drones intercepted per

	Bundeswehr field camp in eastern Jordan (1 German soldier injured)		Jordan statement. 2 missiles breached defenses. Jordan 'dealt with' 49 reports of falling debris.
Israel	Military installations nationwide; Iron Dome repeatedly engaged	Beit Shemesh synagogue (9 killed, 11 missing, 51 injured); Tel Aviv residential (1 woman killed); West Jerusalem ballistic missile (6 wounded); Residential areas throughout country	Dozens of missiles & drones per day. Iron Dome breached multiple times. 3 US soldiers KIA from Iranian attacks across the theater.

HISTORIAN'S NOTE

'For the first time in history, all the GCC states were targeted by the same actor within 24 hours. a scenario long discussed in regional security planning appears to be unfolding.' commented by Sinem Cengiz, Qatar University Gulf Studies Center, speaking to Breaking Defense, March 2, 2026. Iran also struck a UK RAF base on Cyprus (2 missiles, UK disputed this), a US-led coalition position near Erbil (Iraq), and a Palau-flagged oil tanker in the Strait of Hormuz. The Strait remains closed. 150 freight ships stalled.

Section 3: The Cyber Warfare – Active Operation as of Mar 2, 2026

The cyber dimension of this conflict is not hypothetical. Multiple threat actors are confirmed active.

3.1 Confirmed Active Cyber Operations

Actor / Group	Affiliation	Confirmed Actions (Live)	Next Likely Targets
Handala Hack	MOIS (Iran Ministry of Intelligence)	Feb 28: Claimed attacks on Jordan infrastructure. Confirmed Clalit healthcare breach (Israel's largest network). Threatened UAE. Claimed ICS disruption of Israeli manufacturing and energy distribution . Jordanian fuel station infrastructure attack confirmed by other Intel sources.	Israeli hospitals, water systems, ICS. UAE government and financial networks. Jordan fuel infrastructure.
Cyber Islamic Resistance	IRGC-aligned multi-group coalition	DDoS and data-wiping attacks against US and Israeli military logistics providers	US defense industrial base, Israeli logistics, GCC defense contractors.
APT35 / Dept. 40 (Moses-Staff)	IRGC-IO Unit 1500	Pre-positioned access across Jordan, UAE, Saudi Arabia, Kuwait confirmed. Webshell activation assessed as likely underway, though not yet confirmed independently. Moses-Staff persona assessed ready for ransomware/wiper ops.	Israel (via Moses-Staff), Jordan MoJ, UAE aviation, Saudi energy sector.
APT33 / Elfin	IRGC	Shamoon 4.0 wiper deployed Jan 24, 2026 against the Saudi energy	Saudi Aramco, GCC petrochemical sector, UAE energy.

		sector (15,000 workstations). Confirmed prior to kinetic strikes.	
CyberAv3ngers	IRGC-CEC	Historically targeted Unitronics PLCs at US water plants (2023). Currently on elevated alert. 6 officials sanctioned by the US Treasury.	US water/wastewater ICS, Israeli industrial systems, GCC Unitronics-based infrastructure.

3.2 The Cyber-Kinetic Integration Doctrine

Operation Epic Fury may represent one of the clearest recent examples of coordinated kinetic and cyber operations occurring in parallel at a regional scale:

PHASE	ACTOR	ACTION	TIMING
Pre-Strike Cyber Prep	APT35 (IRGC-IO)	Years of cyber pre-positioning across GCC targets, that is, aviation intelligence, government databases, energy sector access, legal system files. All now documented in KittenBusters leak.	2021–2025 (documented in leak)
Phase 1: Digital Pre-Strike	Israel / US (attributed)	The Iranian internet has been reduced to 4% capacity. IRGC C2 disrupted. State media offline. Prayer apps hacked to broadcast regime-change messages to Iranian citizens.	Feb 28, first hours
Phase 2: Kinetic Strikes	Israel / US	1,200+ munitions across 24 Iranian provinces. Nuclear, missile, naval, leadership, IRGC compound targets. Khamenei was killed.	Feb 28
Phase 3: Iranian Kinetic Retaliation	IRGC (kinetic)	Hundreds of ballistic missiles + Shahed drones across 7+ countries. Targeting US bases, airports, ports, hotels. The Strait of Hormuz is closed.	Feb 28 – ongoing
Phase 4: Iranian Cyber Retaliation	MOIS/IRGC-IO (cyber)	Handala: Jordan infrastructure, Israeli ICS confirmed. Cyber Islamic Resistance: wiper attacks on logistics. APT35 webshell activation likely. Fatimiyoun: wiper attempts vs Western finance.	Feb 28 – ongoing
Phase 5: Escalation (Projected)	APT35 / Moses-Staff	Destructive wiper/ransomware under Moses-Staff persona vs Israeli firms. BellaCiao redeployment. Shamoon 4.0 escalation vs Saudi/UAE energy. SCADA targeting per Episode 3 documented objectives.	Next 1–4 weeks

CISA WARNING

The US Cybersecurity and Infrastructure Security Agency (CISA) is operating with sharply reduced staffing due to a funding lapse at its parent agency, the Department of Homeland Security. As Nextgov/FCW reported: 'This is a bad time for Washington's cyber agency to be operating with limited staff.' Iran knows this. The timing of the conflict with CISA's depleted capacity is operationally significant.

Section 4: The Kinetic-Cyber Nexus – Country by Country

This is the central analytical section of this report. For each country Iran has bombed, we document three things in parallel: (1) the kinetic strikes that occurred, (2) what APT35/Charming Kitten already knew and had access to from the KittenBusters leak, and (3) the expected follow-on cyber operations. The alignment is systematic and deliberate.

COUNTRY	KINETIC STRIKES (Feb 28–Mar 2)	APT35 CYBER PRE-POSITIONING (from Leak)	EXPECTED CYBER FOLLOW-ON OPS
Saudi Arabia(CRITICAL THREAT)	King Fahd Air Base & Prince Sultan Airbase struck. Riyadh and Eastern Province targeted. Shamoon 4.0 ALREADY deployed Jan 24, 2026 — 15,000 Saudi energy workstations wiped. Tadawul down 1.5%. Saudi Arabia threatened military response.	CONFIRMED in Leak: National Water Company penetrated (Ep.1). Saudi Council of Ministers decision documents exfiltrated — Iran knew Saudi government policy positions in real time (Ep.1). Energy sector access via legal firm clients — Qistas supply chain yielded 74GB of legal sector data including Saudi clients (Ep.1). APT35 explicitly targeted Saudi energy intelligence.	Shamoon 4.0 escalation against Saudi Aramco and downstream petrochemical sector. SCADA/ICS attacks on water and power infrastructure (documented as APT35 objective in Ep.3). Saudi Central Bank and financial institutions targeted per historical Shamoon 2016 pattern. Influence ops amplifying anti-MBS messaging.
UAE(CRITICAL THREAT)	Al Dhafra Air Base struck. Dubai Palm hotel fire. Burj Al Arab debris damage. Dubai International Airport hit. Zayed International Airport. Jebel Ali Port fire. 167 missiles + 541 UAVs engaged. The Etihad Towers near the Israeli embassy were targeted. Day 2 follow-on strikes confirmed.	CONFIRMED in Leak: Analysis of files contained within the Episode 3 dataset of the KittenBusters disclosure references BellaCiao malware activity associated with aviation-related infrastructure, including references to the domain uniforms.flydubai.com. While the dataset suggests targeting activity against this infrastructure, independent confirmation of successful compromise has not been established at the time of publication. Files within the Episode 4 dataset reference internal materials associated with Dubai infrastructure. These files suggest data access by APT35 operators; however, the precise method of acquisition and scope of access cannot be independently confirmed from the dataset alone. AMEEN ALKHALIJ server — entire fake UAE government recruitment honeypot operated by APT35 to identify and track UAE ex-government and security employees (Ep.2). UAE-targeted phishing Telegram channels operational. Credentials of UAE government employees in APT35 database. | SHELL HISTORY (additional): UAE Ministry of Education Exchange server (mail.moe.gov.ae)	IMMINENT: Pre-positioned flydubai access mirrors kinetic airport strikes — aviation management system disruption. Dubai Government data used for targeting of UAE security personnel. AMEEN ALKHALIJ honeypot re-activated to identify UAE crisis responders. UAE financial sector (DIFC) targeted. Handala has already threatened UAE ('will be left riding camels'). Port of Jebel Ali logistics systems targeted.

		targeted via ProxyLogon (CVE-2021-26855) — webshell planted at ecp\auth\favico.aspx, target email Aimie.Hamer harvested pre-exploit. UAE Government internal system itrendwall.dubaipolice.ae probed with web.config exfiltration attempt on port 9091. Systematic subdomain enumeration and port scanning across: Dubai Municipality (dm.gov.ae), Dubai Land Department (dubailand.gov.ae), Dubai Naturalisation & Residency Dept (dnrd.ae / gdrfad.gov.ae), Roads & Transport Authority (rta.ae), Emaratech (UAE govt IT supplier — supply chain target), Central Bank UAE (centralbank.ae). Purpose-built dubai-ranges.txt and dubai-smb.txt target lists confirm UAE was a pre-planned, deliberate campaign, not opportunistic scanning.	
Kuwait(HIGH THREAT)	Ali Al Salem Air Base targeted (US/Italian troops). Kuwait International Airport struck by drone — terminal building damaged. 97 ballistic missiles + 283 drones intercepted per government.. Kuwait suspended the stock exchange.	CONFIRMED in Leak: Kuwait documented in Ep.2 attack reports as target for government and civilian sector campaigns. Aviation reconnaissance documented (Kuwait Airport was a confirmed target in pre-conflict reports). Government network infrastructure scanned and mapped in preparation for the attack phase. Kuwait's proximity to Saudi energy infrastructure makes it a critical access node.	HIGH: Airport drone strike mirrors documented civil aviation targeting in pre-conflict reconnaissance. Kuwait stock exchange suspension creates conditions for APT35 financial disruption ops. Kuwait government communications interference. Supply chain attacks via Kuwaiti IT service providers serving GCC-wide clients.
Bahrain(HIGH THREAT)	US Fifth Fleet HQ (Manama) struck — parts of HQ confirmed hit. Crowne Plaza Hotel drone strike (fire). Residential tower hit. Era Views Towers apartment building struck. Bahrain International Airport targeted. 45 missiles + 9 Shahed-136 drones intercepted.	CONFIRMED in Leak: Bahrain documented as target in Ep.2 operational reports. US Fifth Fleet facilities represent one of the highest-value intelligence targets in the region — APT35 collection against US naval deployment schedules, coordination plans, and operational capabilities directly supported Iranian targeting intelligence for the kinetic strike on the Fifth Fleet HQ.	HIGH: US Fifth Fleet operational communications are now an active cyber target — attempts to access naval C2 and logistics networks expected. Handala confirmed threats against GCC states. Bahrain Banking and financial sector disruption. Influence operations amplifying civilian casualty imagery from Crowne Plaza and residential building strikes.
Qatar(HIGH THREAT)	Al Udeid Air Base (largest US air base in Middle East) attacked. US radar systems targeted. Doha airport struck. 16 injured. Qatar Airways suspended. 44 missiles + 8 UAVs on Day 1. Qatar's exchange down 2%.	CONFIRMED in Leak: Qatar documented in Ep.2 as target. Al Udeid hosts the air component for US Central Command — mapping US air operations from this base was a critical intelligence priority. Qatar hosts Al Jazeera (global media) and serves as US-Iran diplomatic intermediary — both roles make Qatar a target for communications compromise. APT35 specifically targets media organizations.	HIGH: Al Udeid air operations disruption via cyber. Al Jazeera and Qatari state media targets for disinformation injection (APT35 influence operations template). Diplomatic communications compromise — Qatar was negotiating between US and Iran hours before strikes began; those communications are a counterintelligence priority. Qatar financial sector (QIA sovereign wealth fund) targeted.

Jordan(CRITICAL — ALREADY ATTACKED)	Amman capital struck. Northern Jordan. 13 ballistic missiles + 49 drones intercepted. 2 missiles penetrated defenses. US bases targeted. Bundeswehr camp struck. Jordan handled 54 debris reports.	MOST DOCUMENTED TARGET in Leak: Jordan Ministry of Justice penetrated via Telerik CVE (Ep.1) — court case data, legal proceedings, judge and lawyer databases. Operational notes within the Episode 2 attack report reference activity targeting Jordan's Civil Aviation Commission. The dataset indicates potential access to aviation-related documents. 'Jordan Campaign' is documented as a massive multi-sector operation (Ep.4 Gemini analysis). APT35 had deeper pre-positioned access in Jordan than any other GCC country.	ALREADY ACTIVE: Handala confirmed attack on Jordanian fuel station infrastructure (Flashpoint, Mar 1). Handala posted 'Hello Jordan… The destruction of cyber infrastructures is currently underway' on Feb 28. Jordan Ministry of Justice webshells likely activated for destructive wiper operations. Civil Aviation Commission access enables real-time Jordan airspace intelligence. Jordan's role in downing Iranian missiles makes it a high-priority cyber retaliation target.
Israel(CRITICAL — PRIMARY TARGET)	Synagogue, Beit Shemesh (9 killed, 11 missing, 51 injured). Tel Aviv residential (1 killed, 20+ injured). West Jerusalem (6 wounded). Iron Dome breached multiple times. Nationwide missile and drone barrages continuing.	PRIMARY TARGET in Leak: 580+ Israeli modems exploited for DNS manipulation. Multiple Israeli .co.il domains compromised. Mass social engineering against Israeli civilians. ICS and SCADA targeting explicitly documented in Ep.3 strategic objectives. Moses-Staff persona specifically built for destructive operations against Israeli firms. BellaCiao deployed against Israeli targets (confirmed Bitdefender). 120+ pre-staged social media influence posts ready. | SHELL HISTORY (additional): Rafael Advanced Defense Systems (rafael.co.il) — Israel's primary weapons manufacturer — specifically targeted: full subdomain enumeration, port scanning, .git repository harvesting from all-in.rafael.co.il intranet portal, web fuzzing against career portal. This directly corroborates the IRGC directive (Ep.3 doc 682089f4…) citing Israeli defense infrastructure as explicit objective. SQL injection campaigns against Israeli civilian sites: lametayel.co.il (travel), carsforum.co.il (car forum), motorhome.co.il (retailer), israelweather.co.il (weather), hotels.co.il — confirming civilian economic targeting beyond SCADA/government focus. Emaratech-style supply-chain approach also attempted against Israeli commercial web infrastructure.	CRITICAL — ONGOING: Moses-Staff ransomware/wiper deployment against Israeli firms imminent. Sagheb RAT targeting Israeli security researchers and defense sector personnel. SCADA attacks on Israeli power grid and water (documented objective). Mass modem DNS manipulation already proven at scale. CyberAv3ngers confirmed active against Israeli ICS. Influence operations amplifying civilian casualty imagery from Beit Shemesh synagogue strike.
🇮🇶 Iraq / Kurdistan (SHELL HISTORY)+	Iraq: IRGC-backed PMF forces active in theatre. Kurdish region: strategic IRGC interest (PKK, Peshmerga intelligence).	CONFIRMED EXFILTRATION (Shell History): SQLmap run against Sulaymaniyah Governorate website (slemani.gov.krd) — successfully dumped database tables: employees, users, role_permissions. Also: KRG residency portal (api.residency.digital.gov.krd),	HIGH: KRG employee and citizen data exfiltrated. Supports targeting of Kurdish political/security personnel of IRGC interest. Iraq MoFA intelligence access.

		myaccount.gov.krd, kfms.digital.gov.krd, Asiacell telecom (Iraq's largest carrier, asiacell.com). Iraqi Ministry of Foreign Affairs (mofa.gov.iq), Iraqi DMA (webmail.dma.gov.iq). This is a completed data exfiltration, not reconnaissance. [Source: zsh_history.txt lines 1779–1824, 1636–1642, 1904]	

ANALYST VERDICT — THE PRE-POSITIONING PROOF

The overlap between kinetic targets and documented cyber reconnaissance suggests a deliberate alignment between cyber intelligence collection and subsequent targeting. APT35 exfiltrated Jordan's Civil Aviation Commission files before Iran targeted Jordanian airspace. APT35 penetrated the Dubai government before Iran targeted Dubai airports and the area near the Israeli embassy. APT35 obtained Dubai Government materials and deployed BellaCiao against UAE aviation before Iran struck flydubai's operational domain. The leaked files are not just a historical intelligence product, they are the reconnaissance map for the kinetic campaign now underway.

Section 5: APT35 Attribution Dossier — The Unified Actor

The dataset contains claims of attacks attempting to impair essential services.

5.1 Leadership & Organizational Structure

Commander	Abbas Rahrovi (a.k.a. Abbas Hosseini) — National ID: 4270844116 — IRGC official managing APT35 through front companies
IRGC Unit	IRGC Intelligence Organization (IRGC-IO) — Counterintelligence Division — Unit 1500 — Department 40
Physical Base	Shuhada Base, Tehran — BellaCiao malware development confirmed here
Primary Front Company	Zharf Andishaan Tafakkor Sefid (Deep White Thinking Institute) — signed by official IRGC-IO authority Manouchehr Vosoughi Niri
Also Known As	APT35 / Charming Kitten / Phosphorus / Magic Hound / MINT SANDSTORM (Microsoft)
Confirmed Unified Personas	Moses-Staff (destructive ransomware/wiper ops, Israel focus) + Al-Qassam Cyber Fighters (DDoS, US/Israeli finance) — BOTH CONFIRMED SAME ACTOR via Ep.4 infrastructure files

5.2 Key Personnel Exposed

NAME / ID	ROLE
Abbas Rahrovi / Abbas HosseiniID: 4270844116	Commanding officer — runs Dept. 40 through front companies; 'shadow man' now publicly exposed
Vahid MolawiID: 0323217087	Technical operator — named in hours report; Badge 9235-4; exposed in Episode 2
Mohammad NajaflooID: 4270878835	Former senior employee who maintained server infrastructure Excel sheets for couple of years
Mohammad Erfan Hamidi ArefID: 0023199709 (b. Jun 12, 2000)	Current operational staff at Zharf Andishaan front company; took over infrastructure management from Najafloo
Mohsen ForoughiID: 1467932698	Equipment procurement officer — credentials throughout financial CSV files; hardware and service sourcing for IRGC
Manouchehr Vosoughi Niri	IRGC-IO official authority — signed front company documents; provides organizational legitimacy and legal cover
Mehdi Sharifi — Badge 9235-1	Office Manager / Administrative Head
Esmaeil Heydari — Badge 9235-2	Senior Technical Operator (202+ hours/month documented)
Amir Hossein Aminejad — Badge 9235-7	Technical Operator (164+ hours/month documented)

MOSES-STAFF = APT35: WHY THIS MATTERS NOW

Since 2021, the Moses-Staff persona has conducted destructive ransomware and wiper attacks targeting Israeli government, financial, and transportation sectors. Evidence from the KittenBusters disclosure indicates that Moses-Staff operates within the broader IRGC-IO Department 40 operational structure, suggesting that multiple past campaigns were coordinated through the same unit. In the current escalation environment, the persona may be leveraged for destructive cyber activity. While the public release of malware source code and infrastructure details has exposed parts of the group’s tooling, any previously established access within Israeli networks could still be used to support follow-on operations.

Section 6: Malware Arsenal — Episode 3 Source Code Disclosure

Episode 3 of the KittenBusters leak released the complete source code for APT35's custom malware suite. This is unprecedented and a hostile nation-state's active malware toolkit, completely exposed. The disclosure enables precise YARA rules and behavioral detection. The same malware is now being deployed against the countries in the nexus table above.

MALWARE	LANGUAGE	KEY CAPABILITIES	EVASION TECHNIQUES	C2 METHOD
BellaCiao Var. 1	C#/.NET dropper	Webshell: remote cmd exec, file upload/download; Windows Service persistence	Obfuscated payload; AV-tested vs Defender, Kaspersky, Avira, ESET; anti-debugging	HTTP/S with pre-shared header auth; prevents sandbox analysis
BellaCiao Var. 2	PowerShell	Plink (PuTTY) reverse proxy; custom PS webserver; Windows Service persistence; used vs Turkish Foreign Ministry (confirmed case study in leak)	Legitimate binary abuse (Plink); PowerShell obfuscation	Plink reverse proxy tunnel to attacker C2
Sagheb RAT	Native code FUD designed	Keylogger; screenshot; Firefox + Telegram Desktop credential theft; full filesystem access; shell; scheduled task auto-run; anti-debugging	FUD native code avoids .NET signatures; XOR-encrypted C2; anti-debugging; customized for each target	TOR routing + custom relay servers + DNS forwarder layering
RAT-2Ac2	C#/.NET	Keylogger; full system enumeration (OS/CPU/RAM/AV/.NET/FS); file ops	Pre-shared HTTP header secret prevents sandbox; custom substitution cipher for webshell commands	HTTP/S — header-authenticated; non-standard encoding
Python/Webshell FW	Python + ASP/ASPX	Manages multiple compromised hosts; webshells execute commands and relay output; SSH/web tunneling for lateral movement	Non-standard HTTP header encoding; web-native appearance blends into traffic	Custom HTTP encoding in headers
TAGHEB System	Unknown	Windows OS infection and initial access acquisition	Documented in training materials; AV evasion tested	Unknown — documented in training materials only

Section 7: Financial Operations and Infrastructure – Episode 4

Episode 4 exposed the complete financial backbone and infrastructure procurement system of APT35. Three CSV files representing the group's operational ledger from 2021 through late 2024. This is exceptionally rare in APT analysis: a complete, blockchain-verified financial record of state-sponsored cyber operations.

7.1 Bitcoin Financial Trail

- 19-month continuous ledger: April 10, 2023 – November 12, 2024. 50–60+ transactions.
- Transaction amounts: $10–$197 per transaction. Covers domain registrations, SSL certs, hosting, SMS verification, identity creation.
- Operational security: Every wallet used exactly 2 transactions (receive + immediate forward). Zero remaining balances. Deliberate single-use wallet policy.
- Blockchain verification confirmed by independent analysis: 10 sample wallet addresses verified against mempool.space API, amounts matched leaked CSV exactly.
- Payments reference Moses-Staff explicitly: 'SSl moses' — confirms Moses-Staff is funded by the same operational budget as APT35.
- Payments reference Qassam domain: 'gassam.su' — confirms Al-Qassam is the same financial entity.
- Regular, evenly distributed payment cadence — sustained operational tempo, not campaign-specific funding.

7.2 Server Infrastructure Registry

INFRASTRUCTURE CATEGORY	PROVIDER / DETAIL	SIGNIFICANCE
Domain Registrars	Namecheap (primary), Namesilo, Shinjiru (non-Western scrutiny ops)	Registration patterns reveal persona management strategy; Shinjiru used when Namecheap scrutiny risk is elevated
DNS Management	Cloudns.net (primary), Modern Izmir (backup)	Cloudns.net appears across hundreds of malicious infrastructure setups globally; confirms operational playbook
Legitimate Hosting	EDIS Global, EDIS AT, DediStart — IP ranges: 95.169.196.0/24, 185.141.63.0/24	European datacenter ranges used for operations requiring legitimate-appearing infrastructure
Anonymization Hosting	TheOnionHost, Impreza Host (Tor-friendly, $50–85/service), ISHOSTING, Ultrahost	Sensitive operations and C2 hosted here; Tor-friendly providers offer no-log guarantees
Email Infrastructure	Dozens of ProtonMail accounts: may.arnold@protonmail.com, ronald.iverson@protonmail.com (VERIFIED ACTIVE Oct 2025) — Western-name persona pattern	Each email is a complete phishing identity. Account credentials were confirmed active.
SMS Verification	SMSpva.com, OnlineSim.io, PVAPins.com — API keys exposed	Used to create verified social media, email, and SaaS accounts for personas at scale
Domestic Iranian Networks	AsiaTech (Rohi): 185.142.95.244; Pishgaman: 185.212.193.240/29; TD-LTE 5.202.186.76/30, 5.202.45.174–175	Confirms operational presence inside Iran. Multiple 50Mbps dedicated connections — safe house infrastructure

Operational VoIP	1543.ir - Iranian-hosted VoIP system	Internal communications; .ir TLD confirms domestic hosting for security
Counterintelligence Honeypot	dreamy-jobs.com (VIP Human Solutions cluster, 35+ fake recruitment sites since 2017)	Confirmed by Google/Mandiant March 2024: targeted Iranian, Syrian, and Hezbollah security personnel for profiling and double-agent recruitment. Directly linked to APT35 via Ep.4 CSV.
C2 / Jump Servers (Shell History)	88.80.145.107 — C2 listener (LHOST in msfvenom payloads); 88.80.145.122 — file staging server + SSH jump node; 88.80.145.126 — secondary SSH relay. SSH user: aftelecom (port 443 — firewall evasion). All three within 88.80.145.0/24.	Operator's active C2 and jump infrastructure identified directly from shell history. 88.80.145.107 used as LHOST in msfvenom reverse-shell payload generation (Windows backdoor user-creation payloads). 88.80.145.122 served credential files (pass.txt, u.txt, p.txt) to the operator machine and accepted SSH tunnels for ProxyShell exploitation relay. SSH account "aftelecom" on port 443 is a deliberate firewall-bypass technique. Operator username on attack workstation confirmed as "luki" (/home/luki/ throughout history). Second account "soozan" created (adduser soozan) suggesting shared workstation or second operator. [Source: zsh_history.txt lines 88, 914–925, 937–943, 2072, 2109–2111]
Anonymisation Proxy (Shell History)	SOCKS5 proxy: 103.57.251.31:3512 — used to route nmap scans via proxied connection to avoid attribution	External SOCKS5 proxy used to anonymise active reconnaissance scans (nmap via --proxies socks5://103.57.251.31:3512). Confirms multi-layer anonymisation: traffic routed through proxy before reaching targets. Add 103.57.251.31 to IOC IP list. [Source: zsh_history.txt lines 877–882]

Section 8: Consolidated IOCs

Network Domains

- dreamy-jobs.com — APT35 counterintelligence honeypot (Google/Mandiant confirmed) — BLOCK IMMEDIATELY
- gassam.su — Al-Qassam/Qassam persona domain (Bitcoin ledger confirmed)
- aecars.store — Phishing/social engineering lure infrastructure
- 1543.ir — APT35 internal VoIP
- sunrapid.com, lydston.com and variants — Domain spoofing infrastructure

IP Ranges

- 95.169.196.0/24 — EDIS Global primary operations hosting
- 185.141.63.0/24 — Secondary legitimate-appearance hosting
- 185.212.193.240/29, 185.212.195.32/29 — Pishgaman domestic Iranian network
- 109.230.93.128/29, 109.230.93.168/29 — Basebox safe house operational nodes
- 5.202.186.76/30, 5.202.45.174–175 — Iranian domestic LTE allocation
- 88.80.145.0/24 — C2 listener (.107), file staging (.122), SSH relay (.126) — confirmed operator attack infrastructure [Shell History]
- 103.57.251.31 — SOCKS5 anonymisation proxy used to route active scanning [Shell History]

Email / Identity

- may.arnold@protonmail.com — VERIFIED ACTIVE APT35 phishing account
- ronald.iverson@protonmail.com — VERIFIED ACTIVE APT35 phishing account
- Pattern: [firstname].[lastname]@protonmail.com — Western-name ProtonMail personas at scale
- Facebook/Instagram: kaelajnz — social engineering persona for target cultivation

Active CVEs — Patch Immediately If Unpatched

CVE	PRODUCT	APT35 EXPLOITATION
CVE-2024-1709/1708	ConnectWise ScreenConnect	Day-1 exploitation — within 24 hours of public disclosure. Mass multi-country campaigns confirmed.
CVE-2021-34473/34523/31207	Microsoft Exchange (ProxyShell)	Active. Used for institutional compromise and database credential extraction.
CVE-2024-21887/21893/22024	Ivanti Connect Secure (VPN)	Active. VPN appliances as initial access vector into government/enterprise networks.
CVE-2021-44228	Apache Log4j (Log4Shell)	Active. Broad Java application targeting.
CVE-2019-18935 / CVE-2017-11317	Telerik .NET	Used in Jordan Ministry of Justice penetration — active and documented.
CVE-2012-1823	PHP CGI RCE	Legacy unpatched systems. WISE University vector.
GoAhead / TP-LINK / ASUS / D-Link / Cisco RV	Consumer/SMB routers	Mass exploitation campaign — 580+ devices compromised. DNS manipulation.

Section 9: Defensive Recommendations

IMMEDIATE — Next 24 Hours (Do Now)

- Block IOC domains and IPs: dreamy-jobs.com, gassam.su, aecars.store, 1543.ir and all listed IP ranges.
- Emergency patch sprint: ConnectWise ScreenConnect (CVE-2024-1709), ProxyShell (Exchange), Ivanti Connect Secure, Telerik. If cannot patch — ISOLATE.
- Hunt for Plink.exe (PuTTY suite component) execution in server environments — BellaCiao Variant 2 primary indicator.
- Hunt for Adminer.php and custom ASP/ASPX webshells on all internet-facing servers.
- Rotate all Domain Administrator credentials. Audit new admin accounts created since January 1, 2024.

- Enable enhanced logging on: Active Directory events, Exchange transport, Acronis backup portal access, Cisco device logins.
- If your org operates in Jordan, UAE, Saudi Arabia: initiate immediate compromise assessment — you are in the highest-risk zone.

HIGH PRIORITY — Within 72 Hours

- Build YARA rules from the public BellaCiao source code (Episode 3 leak). This is a unique opportunity to build precision detection for an active threat.
- Configure behavioral detection for Sagheb RAT: TOR circuit establishment from non-user processes; XOR-encrypted HTTP traffic to non-standard endpoints.
- Audit SOHO/consumer router fleet (TP-LINK, ASUS, D-Link, Cisco RV) — APT35 mass-exploited 580+ devices. Identify any showing DNS redirect behavior.
- Validate DDoS mitigation posture — Al-Qassam DDoS persona pattern (Operation Ababil-style attacks on financial sector) expected to activate within days.
- Implement MFA everywhere if not already done — Sagheb RAT specifically steals Telegram Desktop and Firefox credentials to bypass MFA.
- If you use Sophos, Trend Micro, or SentinelOne: APT35 has documented bypass research and AV evasion testing against all three. Verify behavioral coverage is enabled, not just signature-based.

STRATEGIC CONTEXT	'They don't need to win a naval battle in the Gulf to hurt the US. They can simply hold our power grids, water systems, and hospitals hostage from halfway around the world to force our hand at the negotiating table.' said Tatyana Bolton, Monument Advocacy cybersecurity practice, speaking to Nextgov/FCW, February 28, 2026. This is the operational doctrine APT35 is executing.

Conclusion: The Map was in the Leak

The KittenBusters disclosure initially appeared to provide rare visibility into the internal operations of APT35, a forensic inside view of Iran's most capable cyber unit. We now understand it as something more specific: the pre-conflict reconnaissance map for the kinetic campaign that began on February 28, 2026.

Every country Iran struck with ballistic missiles and drones in the past days was systematically profiled and penetrated by APT35 before the first missile was launched. Jordan's air and judicial infrastructure. UAE's aviation and other systems. Saudi Arabia's government decision-making and energy sector intelligence. Kuwait's civil aviation. Qatar's strategic military posture at Al Udeid. Bahrain's US Fifth Fleet operations. Israel's ICS, modems, and civilian digital infrastructure. These were not random targets of

opportunity. They were documented, named, and exploited by Department 40 under Abbas Rahrovi's direction, years before the strikes began.

With Khamenei assassinated, Iran's conventional deterrence degraded, and the IRGC operating under unprecedented pressure, cyber operations have transitioned from a supplementary intelligence tool to the primary instrument of Iranian strategic power. The intelligence assessment is correct: Iran-linked cyber units were activated and retooling before the kinetic trigger. Available indicators suggest Iranian-linked cyber units have already begun operational activity consistent with a broader retaliatory campaign. The question is the severity, duration, and whether the cybersecurity community can move fast enough to operationalize the extraordinary intelligence advantage the KittenBusters disclosure has provided.

FINAL THREAT RATING	APT35/Charming Kitten/Moses-Staff/Al-Qassam is a unified IRGC-IO actor with confirmed pre-positioned access across every bombed GCC country, active operations underway via Handala and Cyber Islamic Resistance personas, complete malware source code now public, a blockchain-verified financial infrastructure, and a commanding officer still operational. The period immediately following Operation Epic Fury is likely to represent a period of elevated risk for Iranian cyber retaliation.

References

- *Intelligence source and information reliability - Wikipedia
- #Traffic Light Protocol - Wikipedia
- https://github.com/KittenBusters/CharmingKitten

CloudSEK

We Predict Cyber Threats

Monitor. Analyse. Predict.

Secure your Tomorrow,Today!

Request for a Free Demo of our platform:

SCAN ME

OR

Mail us at **info@cloudsek.com**
or visit **https://cloudsek.com**

Gain access to a free trial and Detailed POC on CloudSEK Platform

Registered Office:

CloudSEK Research Pte Ltd.
51 Chin Swee Rd. #07-12 Manhattan House,
Singapore 169876

Regional Office: United States

CloudSEK Inc.
8 The Green, Ste A, Dover, DE - 19901
United States

Regional Office: India

CloudSEK Information Security Pvt Ltd
16/1, WINGS, Cambridge Rd, Halasuru,
Cambridge Layout, Jogupalya,
Bengaluru, Karnataka, India - 560008

Regional Office: United Kingdom

CloudSEK, 4th floor, Rex House,
4, 12 Regent Street, London,
SW1Y 4PE - United Kingdom