

Cyber Escalation amid US-Israel & Iran Conflict

By: StrikeReady Research

Published: March 17, 2026

Executive Summary

On February 28, 2026, the US and Israel launched a joint military campaign, Operation Epic Fury/Roaring Lion, against Iran. As the conflict escalated into direct kinetic warfare, cyber operations have increasingly shifted toward a full-scale cyber war. The initial coordinated US and Israeli strikes disrupted IRGC command-and-control infrastructure and significantly reduced domestic connectivity to a critical 4% in Iran. Since then, the digital battlespace has evolved beyond traditional state-led espionage into a decentralized threat landscape targeting governments, critical infrastructure, and private sector organizations.

With the recently established Electronic Operations Room, state-sponsored actors, affiliated hacktivists, and cybercriminal groups are operating with overlapping objectives to target Israeli, Western, and Gulf-region infrastructure. Concurrently, the Middle East, Turkey, and Africa (META) region has experienced a drastic surge in conflict-themed social engineering campaigns, enabling threat actors to conduct intelligence collection while capitalizing on escalated geopolitical urgency. StrikeReady brings actionable visibility into this volatile cyber activity, enabling organizations to operationalize threat intelligence into defensive and strategic readiness.

Threat Landscape Overview

As cyber operations emerge as the primary theatre of active conflict in the Iran-Israel geopolitical landscape, let us take a deep dive into StrikeReady's latest intelligence and operational capabilities aimed at strengthening organizational security posture.

Iran-aligned threat actors

Threat Actor	Details	Recent Activity (March 2026)
Handala Hack	Aliases: Void Manticore, Banished Kitten, Red Sandstorm, Storm-0842, Dune, Karma Focus: Healthcare, Medical Equipment, and Services across Asia (Israel), North America (US), and Europe (Albania) Observed TTPs: T1485: Data Destruction, T1072: Software Deployment Tools, T1491.002: External Defacement, T1078.002: Valid Accounts	Responsible for a massive wiper attack on Stryker Corp (US). Claimed a breach of Verifone, allegedly leaking transaction data. Abused Microsoft Intune to push malware and broadcast threats.
MuddyWater	Aliases: Mango Sandstorm, Static Kitten, Seedworm, Mercury, TEMP.Zagros, Earth Vetala, Yellow Nix Focus: Governments, Financials, Transportation and Logistics in Asia (Israel, UAE, Jordan, Turkmenistan), North America (US), and Europe (UK, France) Observed TTPs: T1059.001: PowerShell Command & Scripting, T1027: Obfuscated Files or Information, T1102.003: Web Service, T1557: Adversary-in-the-Middle	Deployed a previously unknown backdoor named Dindoor against US banks and airports. Currently deploying BugSleep and MuddyViper backdoors against Israeli maritime logistics. Observed using AI-assisted malware iteration to bypass EDR signatures during the blackout.

Charming Kitten (APT42)

Aliases: Mint Sandstorm, Newsbeef, Phosphorus, TA453, Rocket Kitten, Charming Cypress

Focus: Government, Technology, Research & Development, and diplomatic entities in Asia (Saudi Arabia, Kuwait, Qatar), and North America (US)

Observed TTPs: T1566: Phishing, T1137.006: Office Application Startup Add-ins, T1102: Web Service, T1114.002: Remote Email Collection, T1555.003: Credentials from Web Browsers

Conducted credential phishing campaign targeting prominent US/Israel think tanks using fake roundtable invites focused on Middle East air defense to harvest military strategy data.

APT33 (Peach Sandstorm)

Aliases: Elfin, Magnallium, Refined Kitten, Holmium

Focus: Government, Financials, Telecommunication, and Energy in Middle East (Saudi Arabia, Kuwait, Qatar), and North America (US)

Observed TTPs: T1485: Data Destruction, T1567.002: Exfiltration to Cloud Storage, T1098: Account Manipulation, T1528: Steal Application Access Token

Iran's primary kill-switch threat to Gulf Energy and Aviation networks if the conflict widens. Pivoted to identity-centric targeting and cloud-native persistence (ALMA backdoor) to prepare destructive wiper operations against Western-aligned maritime and energy infrastructure.

APT34 (OilRig)

Aliases: Hazel Sandstorm, Helix Kitten, Crambus, IRN2, Cobalt Gypsy, Pumpkin Sandstorm, ATK40

Focus: Governments, Telecommunications, and Media across Middle East (UAE, Saudi Arabia), North America (US), and Europe.

Observed TTPs: T1566: Phishing, T1071.001: Web Protocols, T1568.002: Domain Generation Algorithms, T1078.002: Domain Accounts

Specializes in deep persistence in Middle Eastern government and diplomatic networks. Utilizing CVE-2024-30088 to monitor diplomatic ceasefire negotiations and coalition internal communications

Operationalization with StrikeReady

StrikeReady Recon StrikeReady Recon provides relevant activity linked to all the active threat actors. It also provides insights into emerging threat intelligence to help security teams monitor how detection and response technologies are being utilized.

Basic Query		threat_actor IN ("charming kitten", "apt33", "Handala Hack", "Tortoiseshell", "Infy", "parisite", "muddy water", "cyberav3ngers", "OilRig")		Clear	Save	Subscriptions	Exported artifacts reports	Subscribe
Pinned :		Exploit In the WILD within last 1 Month		Zero Day CVE within last 1 Month		Patchable CVEs within last 1 Month		CVE with Critical Severity within last 1 Month
Artifacts		Rules		Vulnerabilities		Malware		Ransomware
Threat actors		News		Tools				
Name & Description		Industry		Origin		Strikes		
Handala Hack		education, social welfare		PSE		2		
Cyber Avengers		petrochemical, energy		IRN		0		
Infy		private organizations, diplomats		IRN		1		
APT33		pharmaceutical, education		IRN		17		
OilRig		oil and gas, manufacturing		IRN		15		
Tortoiseshell		satellite communication, information technology		IRN		2		
Parisite		defense, petrochemical		IRN		0		
Charming Kitten		defense, higher education		IRN		8		

Users can navigate to Threat actor page for a detailed overview including its basic information, threat association, and more.

STRIKE READY

Basic Query threat_actor IN ("apt33", "charming kitten")

Artifacts

Rules

Vulnerabilities

Malware

Name & Description

Handala Hack

Cyber Avengers

Infy

Parasite

Charming Kitten

APT33

OilRig

Pioneer Kitten

Threat actor

OilRig

Threat association

Basic information

Associated threat campaigns

Mitigation rules

Reference

Threat association

Malware

Ransomware

Threat type

Tools

Threat campaigns

Vulnerabilities

MITRE ATT&CK Tactics and Techniques

Tactics

Techniques

Basic information

Aliases

Targeted Sectors

Targeted Countries

Targeted Regions

StrikeReady enables organizations to operationalize external intelligence feeds through an automated **Threat Advisory Deployment** via Email Ingestion to streamline their workflow. If configured, extracted artifacts can be automatically enriched, deployed or retired across integrated security controls. Each ingestion creates a case and notifies users in real-time.

STRIKE READY

Subscriptions

Subscriptions

Ingestion emails

Archived

Subscribed by

Subscription action

State

Integration

Title

Subscription action

Tags

Iran-Israel Update

Deployment

Creating email ingestion box

Select ingestion action for email ingestion box

Add to threat model

Deployment operationalization

Retirement operationalization

Retro-lookup operationalization

Cancel

StrikeReady has introduced a new tag **"Iran-Israel-Conflict"** that help analysts quickly filter all the threat intelligence associated with the ongoing geopolitical escalation. This query can be subscribed to in Recon to stay protected from new threats.

Basic

Query

created_at ~> 5w AND tag IN ("iran-israel-conflict")

🔍

Find

🗑️

Clear

🔖

Save

📄

Subscriptions

📦

Exported artifacts reports

📄

Subscribe

Pinned :

Exploit in the WILD within last 1 Month

Zero Day CVE within last 1 Month

Patchable CVEs within last 1 Month

CVE with Critical Severity within last 1 Month

📄

Saved queries

Artifacts

Export all artifacts (683)

Artifacts	Alerts	Strikes	Tags	TLP	Score	
☐ IPv4 31.57.35.223 Source: Check Point	⚠️ 0	📄 1	All 17 netbird medical	○ White	75 StrikeReady ⚠️ Malicious	57 Analyst By 🏆 CARA
☐ IPv4 82.25.35.25 Source: Check Point	⚠️ 0	📄 1	All 17 netbird medical	○ White	75 StrikeReady ⚠️ Malicious	64 Analyst By 🏆 CARA
☐ IPv4 107.189.19.52 Source: GBHackers	⚠️ 0	📄 1	All 17 netbird medical	○ White	75 StrikeReady ⚠️ Malicious	57 Analyst By 🏆 CARA
☐ SHA256 0b80ab6a6c4eca08e18096c9468fe0bd2e33fc23142730e591776fcd... File type: peexe Source: Check Point	⚠️ 0	📄 1	All 17 netbird medical	○ White	65 StrikeReady ⚠️ Suspicious	45 Analyst By 🏆 CARA
☐ SHA256 1ab1586975779b7d1ce09315b1312b939a194de6df7c5e92aea4f96383... File type: peexe Source: https://research.checkpoint.com/2026/handala-hack-unveiling-groups-modus-operandi/	⚠️ 0	📄 1	All 16 netbird medical	○ White	75 StrikeReady ⚠️ Malicious	57 Analyst By 🏆 CARA
☐ SHA256 d969ff9fe099db8f6ef3977a849b175aa221669387eb29a2c6c0ce4b4... File type: peexe Source: https://research.checkpoint.com/2026/handala-hack-unveiling-groups-modus-operandi/	⚠️ 0	📄 1	All 16 netbird medical	○ White	65 StrikeReady ⚠️ Suspicious	45 Analyst By 🏆 CARA
☐ MD5 5986ab04dd6b3d259935249741d3eff2 Source: https://research.checkpoint.com/2026/handala-hack-unveiling-groups-modus-operandi/	⚠️ 0	📄 1	All 16 netbird medical	○ White	75 StrikeReady ⚠️ Malicious	74 Analyst By 🏆 CARA
☐ MD5 3cb9dea916432ffb8784ac36d1f2d3cd Source: GBHackers	⚠️ 0	📄 1	All 16 netbird medical	○ White	75 StrikeReady ⚠️ Malicious	74 Analyst By 🏆 CARA
☐ SHA256 8aafccf65c128aa57cc7206adeeb845b2b7f1100a3e987d8486d5919b...	-	-	-	-	75 StrikeReady	Add Score

Rows per page 25

1 ~ 25 of 683

StrikeReady Analysis Engine Tool provides analysis (single or multiple artifacts) for suspicious files, domains, IPs, or URLs from external sources that could pose security risks. Users can view details of all extracted artifacts and may Analyze, Simulate, Export, Deploy, Retire, or View associated artifacts of any selected artifact as shown:

Initiating analysis

☐ Single artifact

☐ Multi-artifacts from text

☒ Multi-artifacts from URL

☐ Multi-artifacts from File

Multi-artifacts from URL

Add url source to extract artifacts to analyze.

 <https://research.checkpoint.com/2026/handala-hack-unveiling-groups-modus-operandi/>

Tags (Optional)

Add User Tags...

☒ Extract domains ⓘ

Close

Analyze

The screenshot displays the STRIKE READY web application interface. On the left sidebar, there's a navigation menu with icons for home, search, alerts, and other functions. The main panel shows details for a specific IP address, 31.57.35.223, which is identified as belonging to Zenlayer Inc. It lists various threat indicators like malware, ransomware, and threat actors, along with their associated MITRE ATT&CK tactics and techniques. A right-hand pane provides additional context, including analysis engine reports from Augur Security and StrikeReady Intelligence, both flagging the IP as malicious.

STRIKE READY

URL Extraction & Enrichment

<https://research.checkpoint.com/2026/handala-hack-unveils-new-zero-days/>

Updated by Jane Doe | Updated at: 03/17/2026, 08:10 AM

Artifacts

- Total selected: 1 [Deploy (1)] [Retire (1)] [Create case (1)]
- [] Artifacts
- [x] IPv4 31.57.35.223
Source: Check Point
- [] IPv4 82.25.35.25
Source: Check Point
- [] IPv4 146.185.219.235
Source: Check Point
- [] IPv4 107.189.19.52
Source: GBHackers
- [] SHA256 08b80ab6ac4cca08e18096c9468fe0bd2e33fcd
File type: peexe Source: Check Point
- [] SHA256 d969f9fe09db86ef3977a849b1757aa22169
File type: peexe
Source: https://research.checkpoint.com/2026/handala-hack-unveils-new-zero-days/
- [] MD5 5986ab04d6b3d259935249741d3eff2

IPv4 TLP White

31.57.35.223 Open in new tab OK To Deploy

All 17 netbird medical albania asia Iran + Add

Status: online ASN: 21859
ISP name: Zenlayer Inc Location: United Kingdom
First seen: 16 days ago Last seen: 5 hours ago

Are you targeted? 0
Are you at risk? 1

75 StrikeReady Malicious

57 Analyst

By CARA Alerts Cases Sources

Threat association Basic information IP Whois Location Targeted geography and sectors Associated threat campaigns Mitigation rules Reference Comments

Threat association

- Malware Wiper s0041 (secityics_threat_intelligence)
- Ransomware -
- Threat actors Handala Hack DUNE homeland_justice (secityics_threat_intelligence)
- Threat type void_manticores (secityics_threat_intelligence)
- Tools Wiper Malware Malicious Site
- Threat campaigns -
- Vulnerabilities CVE-2020-0796

MITRE ATT&CK Tactics and Techniques Open in MITRE view

Tactics	Techniques
-	Establish & Maintain Infrastructure (T1329)
-	-

Basic information

Network	31.57.35.0/24
Ports	445 3389
Country	United Kingdom
ASN Name	ZEN-ECN - Zenlayer Inc, US
ASN	21859

Analysis engine reports

Search analysis engine...

Total: 23

Augur Security

ASN Number 21859 | IP Address 31.57.35.223

03/17/2026 8:10 AM

StrikeReady Intelligence

MALICIOUS

03/17/2026 8:10 AM

VirusTotal

Detection Ratio: 5 / 94 | Country GB | ASN 21859
AS OWNER Zenlayer Inc | last Analysis Date 1773643027

03/17/2026 8:10 AM

OPSWAT

STRIKE READY

StrikeReady Assessment allows users to monitor their security posture with its Stats Dashboard, Strikes, and Plan Execution workflows. It helps understand the effectiveness of your organization's security measures and identify areas that may need attention.

The interface shows a grid of 10 threat intelligence cards. Each card contains the following information:

- Title:** e.g., "STA4614 - APT37 Deploys Multiple Backdoors Through LNK Based Attack Chain"
- Attack type:** e.g., "State-Sponsored"
- Malware family:** e.g., "THUMBSBD"
- Category:** e.g., "Trojan"
- Threat actor:** e.g., "APT37"
- Severity:** e.g., "71 High severity"
- Created at:** e.g., "03/16/2026"
- Actions:** "+ Add to list", "Strike now"

StrikeReady's CARA, Cyber AI Response Analyst, can inform you about the relevant threat actors, recent strikes, exploited vulnerabilities, or IOCs and advise the best course of action with real-time actionable insights to improve your response time.

The interface displays a detailed view of strikes related to APT33. It includes a list of 17 strikes and a grid of 8 detailed strike cards. Each card contains the following information:

- Title:** e.g., "STA1383 - APT33 Targets Saudi Organizations With StoneDrill"
- Attack type:** e.g., "State-Sponsored"
- Malware family:** e.g., "StoneDrill"
- Category:** e.g., "Trojan"
- Threat actor:** e.g., "APT33"
- Severity:** e.g., "67 High severity"
- Created at:** e.g., "02/01/2025 05:25 PM"
- Actions:** "+ Add to list", "Strike now"

The sidebar on the right provides additional information about APT33:

- PROPERTIES:** Origin Country: Islamic Republic of Iran, Last Updated: 2026-02-16T12:58Z
- Aliases:** APT 33, APT33, Elfin, MAGNALLIUM, Refined Kitten
- Target Countries:** United States of America, Islamic Republic of Iran, State of Israel, Korea, Republic of, Kingdom of Saudi Arabia

CARA's Blog Analysis automatically extracts from a given blog or URL, enabling users to quickly operationalize it through deployment and retirement configurations as demonstrated:

Extract artifacts from <https://research.checkpoint.com/2026/handala-hack-unveiling-groups-modus-operandi/>.

8:38 AM

J

The following artifacts have been extracted from <https://research.checkpoint.com/2026/handala-hack-unveiling-groups-modus-operandi/> as per your request:

8:38 AM

IPv4 (2) MDS

Search locs

☐ Artifacts

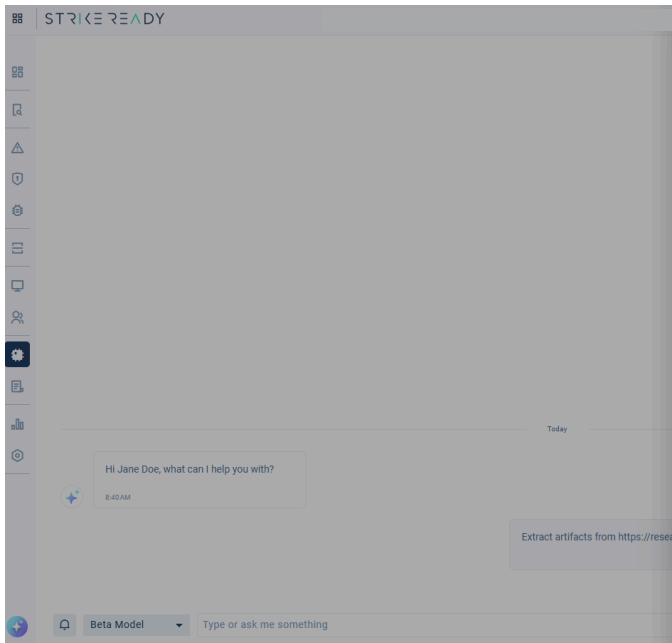
☒ 107.189.19.52

☒ 146.185.219.235

☐ 31.57.35.223

☐ 82.25.35.25

Proceed →



Deploy now

Deployment and Retirement configurations

Deployment action

Deploy only to the integrations where the selected execution mode is:

Blocking

Hierarchy by: Integration

☒ IOC Block List

☒ 879

☒ IPv4

☒ Trend Micro Vision One (XDR)

☒ Ameer_zone

☒ IPv4

☒ zohaib_sim

☒ IPv4

☒ PAN EDL

☒ Local=Zone

☒ IPv4

Cancel

Deploy

Mitigation & Remediation

- Enforce phishing-resistant MFA (FIDO2 where possible) across email, VPN, and cloud services.
- Enforce least privilege access and continuous monitoring of administrative actions.
- Implement advanced email filtering for spearphishing links and attachments.
- Monitor outbound traffic for anomalous connections to cloud services, Telegram APIs, or DNS tunneling activity.
- Restrict direct internet exposure of ICS/SCADA management interfaces wherever operationally feasible. Implement network segmentation, VPN-based access controls, and strict authentication for remote industrial system management.
- Alert employees to lures specifically themed around regional air defense, roundtable invites, and military strategy, which are currently used by Charming Kitten to harvest intelligence.
- Prioritize immediate patching of CVE-2024-30088, CVE-2024-24919, CVE-2024-4577, CVE-2026-1731, currently being weaponized for initial access and lateral movement.

Indicators of Compromise (IOCs):

Indicator	IOC Type	Threat Actor
1ab1586975779b7d1ce09315b1312b939a194de6df7c5e92aea4f963835f7b08aa124a4b4df12b34e74ee7f6c683b2ebecAce9a8edcf9be345823b4fdcf5d868a2001892410e9f34ff0d02c8bc9e7c53b0bd10da58461e1e9eab26bdbf410c79c23bac59d70661bb9a99573cf098d668e9395a636dc6f6c20f92c41013c30be8	SHA-256	Handala Hack APT41 MuddyWater MuddyWater
fileportalshare.netlify.app fortigate.forticloud.online airconnectionapi.azurewebsites.net 1stemployer.com bootcamptg.org	Domain	Charming Kitten APT34 (OilRig) Tortoiseshell Tortoiseshell MuddyWater
https://1drv.ms/b/c/cbec61ab8028f986/IQDa9igU3D3BRqiyNtth76AzAbOM6jUpa8apnuRI-zKXKow?e=E8blfd	URL	Charming Kitten
46.246.3.223 46.246.3.245 146.185.219.235 107.189.19.52 159.198.68.25	IPv4	APT34 (OilRig) APT34 (OilRig) Handala Hack Handala Hack MuddyWater

StrikeReady Research is working day and night to find further information and will keep its customers updated as events regarding this conflict unfold.