

Evolving Cyber Warfare in the US-Israel and Iran Conflict

By: StrikeReady Research

Published: April 28, 2026

Executive Summary

Following the February 28, 2026 launch of Operation Epic Fury/Roaring Lion, the cyber battlespace has transitioned from state-led disruption into a high-velocity, decentralized cyber war. Recent monitoring of cyber activity linked to the US-Israel and Iran conflict indicates continued escalation in both volume and sophistication, with a notable shift toward hybrid operations combining proxy hacktivist activity, state-sponsored intrusion, and pseudo-ransomware tactics targeting Israeli, Western, and Gulf-region organizations.

As the conflict progresses, cyber operations are no longer episodic but are continuously evolving, driven by a combination of state direction, proxy execution, and opportunistic cyber activity. Defense has shifted from isolated actors to an increasingly coordinated Electronic Operations Room that operationalizes intelligence across the Middle East, Turkey, and Africa (META) region with unprecedented speed. StrikeReady continues to provide real-time visibility into emerging threat actors, malware activity, and evolving campaigns, enabling organizations to proactively align their defensive posture with the latest developments in this dynamic threat environment.

Threat Landscape Overview

As cyber operations remain the primary theatre of active conflict in the Iran-Israel geopolitical landscape, let's 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	Observed Activity (April 2026)
Handala Hack	Aliases: Void Manticore, Banished Kitten, Red Sandstorm, Storm-0842, Dune, Karma. Focus: Healthcare, Medical Equipment, and Services across Middle East (Israel) and North America (US). Recent TTPs: T1485: Data Destruction, T1072: Software Deployment Tools, T1491.002: External Defacement, T1078.002: Valid Accounts. StrikeReady IOC Count: 398	Expanded its operations to the UAE, claiming to destroy 6PB of data across key government sectors. This technical sabotage was paired with psychological warfare, including the doxxing of IDF personnel and U.S. officials to undermine institutional trust.
MuddyWater	Aliases: Boggy Serpens, Mango Sandstorm, Static Kitten, Seedworm, Mercury, Earth Vetala, Yellow Nix. Focus: Governments, Financials, Transportation and Logistics in Middle East (Israel, UAE, Jordan), North America (US), and Europe (UK, France). Recent TTPs: T1059.001: PowerShell Command & Scripting, T1027: Obfuscated Information, T1102.003: Web Service, T1557: Adversary-in-the-Middle. StrikeReady IOC Count: 1403	Shifted towards a "Malware-as-a-Service" (MaaS) model, utilizing commercial or criminal tools like ChainShell and CastlerAT to gain stealth and scale. Recent operations include deploying ZionSiphon malware to target Israeli water utilities and using LampoRAT for long-term surveillance while masquerading as legitimate antivirus processes

Storm-1811	Aliases: UNC4393, Russian Legion, The White Pulse, Cardinal Cybercrime Group, Russian Partizan. Focus: Government, Military, and Technology in Middle East (Israel) and Europe (Ukraine). Recent TTPs: TA0001: Initial Access , T1036: Masquerading, T1486: Data Encrypted for Impact, T1562.001: Disable or Modify Tools. StrikeReady IOC Count: 94	Pivoted from financially motivated ransomware to supporting the Russian Legion alliance. Currently executing Vishing-to-Wiper pipelines to disrupt emergency response coordination during regional kinetic strikes.
DieNet	Aliases: DieNet. Focus: Energy, Telecommunications, and Transportation in Middle East (Qatar, Egypt, Israel) and North America (US). Recent TTPs: TA0040: Impact, T1491: Defacement, T1498: Network Denial of Service. StrikeReady IOC Count: 07	Specializes in high-volume network disruption. Recently observed manipulating regional ISP routing tables to redirect local traffic through surveillance-ready gateways during ceasefire negotiations.
L4663R666H05T	Aliases: l4663r666h05t. Focus: E-commerce (Magento/Adobe Commerce), Government, and Legal services worldwide. Recent TTPs: TA0040: Impact, T1491.001: Internal Defacement. StrikeReady IOC Count: 05	Recently executed a mass-automation campaign impacting over 7,500 domains. While primarily notoriety-driven, recent activity shows targeted defacements of Israeli (ISR) government and commercial sites with anti-Israel and anti-GCC messaging.
Hider Nex	Aliases: Tunisian Maskers Cyber Force, hider_nex. Focus: Government, Financial, Telecommunications, and Energy in Middle East (Kuwait, Israel, Morocco), Europe (France), North America (US). Recent TTPs: TA0040: Impact, TA0042: Resource Development, T1498: Network Denial of Service.	A high-volume hacktivist collective specializing in a Hack-and-Leak combined with massive DDoS operations. Recently launched #OpKuwait successfully disrupting critical government portals, including the Ministry of Defense and the Public Authority for Electricity and Water.

Emerging Malware Activity

Malware	Details	Operational Role (Ongoing Conflict)
ZionSiphon	Aliases: zionsiphon. Threat Actor: MuddyWater. Focus: Water Utilities in Middle East (Israel). Recent TTPs: T1083: File and Directory Discovery, T1095: Non-Application Layer Protocol, T1497: Virtualization/Sandbox Evasion, T1071: Application Layer Protocol. StrikeReady IOC Count: 01	Performs strict geographic checks and verifies utility-related software before attempting to manipulate chlorine dosing and hydraulic pressure.

ChainShell	Aliases: chainshell. Threat Actor: MuddyWater. Focus: Government, Defense, and Technology in Middle East (Israel) and North America (US). Recent TTPs: T1071.001: Web Protocols, T1059.001: PowerShell, T1562.001: Disable or Modify Tools StrikeReady IOC Count: 10	A sophisticated command execution shell marking a strategic pivot toward Malware-as-a-Service (MaaS). It utilizes blockchain smart contracts to dynamically retrieve C2 endpoints, providing high resilience against takedowns.
LampoRAT	Aliases: Olalampo, lampo rat. Threat Actor: MuddyWater. Focus: Government, Aviation, Telecommunications, Energy, and Transportation in Asia (Azerbaijan, Israel) Recent TTPs: T1071.001: Web Protocols, T1106: Native API, T1059.003: Windows Command Shell. StrikeReady IOC Count: 59	Designed for long-term surveillance and covert access, frequently masquerading as legitimate antivirus processes (e.g., avp.exe) and abusing encrypted messaging APIs for C2 communication.

Operationalization with StrikeReady

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.

STRIKE READY

Recon / Threat actors

Jane Doe

BasicQuery

threat_actor IN ("Handala Hack", "Storm-1811", "DieNet", "Hider Nex", "Akatsuki Cyber Team", "Cyber Jihad Movement", "Nasir Security", "L4663R666H05T", "Ababil of Minab", "LulzSec Black", "INDOHAXSEC")

ClearSaveSubscriptionsExported artifacts reportsSubscribe

Pin

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

Vulnerabilities

Malware

Ransomware

Rules

Threat actors

News

Tools

Name & Description	Industry	Origin	Strikes
L4663R666H05T L4663R666H05T is a mass web defacement threat actor that became prominent in late February 2026 during a large-scale automated campaign targeting Magento and Adobe Commerce websites worldwide. The actor is primarily associated with mass-stored content defacement activity and used automated techniques to upload plaintext TXT marker files into publicly accessible web directories rather than deploying malware or stealing data. Open source intelligence and defacement archives indicate that...		IDN	0
LulzSec Black LulzSec Black is a hacktivist threat actor that emerged around late 2023 and adopted the historic LulzSec name without any verified connection to the original 2011 group. The actor operates primarily through Telegram and public leak channels, using the LulzSec branding to gain attention and perceived credibility. LulzSec Black is mainly associated with distributed Denial-of-Service (DoS) attacks, website defacements, and exaggerated breach claims rather than advanced intrusions. Its campaigns have...	banking, higher education	+1	0
INDOHAXSEC INDOHAXSEC is an emerging Indonesian hacktivist collective identified by Arctic Wolf researchers as part of a broader rise in Southeast Asian hacktivism. The group became more visible in late 2023 and 2024 through coordinated DDoS attacks and website defacements promoted on Telegram and defacement archives. INDOHAXSEC primarily targets government portals, public sector organizations, and commercial entities, with a strong focus on Israeli and Western-aligned websites in response to...		IDN	0
Ababil of Minab Ababil of Minab is a pro-Iranian hacktivist threat actor believed to originate from Minab, Iran, and is primarily active in ideologically motivated cyber operations. The group is best known for conducting distributed denial of service attacks and website defacements against targets perceived as hostile to Iranian political or religious interests. Ababil of Minab has mainly targeted Israeli, Western, and Gulf region government and commercial websites, often during periods of heightened geopolitical tension. Its...		IRN	0
Handala Hack Handala Hack is a Palestinian group that potentially targets Israel's government and financial sectors.	education, social welfare	+5PSE	2
Storm-1811 Storm-1811 is a financially motivated cybercriminal group known for its involvement in various malicious activities, including deploying Black Basta ransomware. They have been observed exploiting tools like Quick Assist in social engineering attacks, utilizing techniques such as voice phishing (vishing) to target users and organizations. Additionally, Storm-1811 has been known to deploy remote monitoring and management (RMM) tools like ScreenConnect and NetSupport Manager, as well as other...	information technology, business	+3	1
DieNet	software, Online Retail	+5	0

Rows per page

25

1 - 11 of 11

<>

STRIKE READY

Users can navigate to Threat actor page for a detailed overview including its threat association, basic information, associated threat campaigns, artifacts, and more. StrikeReady has a total of **398** IOCs associated with Handala Hack demonstrated ahead. Navigate to StrikeReady Product for more info on threat actors active in Iran-Israel conflict.

The screenshot displays the StrikeReady interface. On the left, a sidebar lists threat actors: L4663R666H05T, LufzSec Black, INDOHAXSEC, Ababil of Minab, Handala Hack, Storm-1811, and DietNet. The main area shows the 'Artifacts' page for the 'Iran-Israel-Conflict' tag. It includes a search bar, filters for 'Artifact Type', 'StrikeReady Ver.', and buttons for 'Export all artifacts (398)', 'Deploy all (398)', 'Retire all (398)', and 'Create case for IOCs (398)'. A table lists artifacts with columns: Artifact Type, Alerts, Strikes, Tags, TLP, and Score. The table contains entries for SHA256 hashes, domains, and IP addresses, each with associated tags like 'malicious', 'iran-israel-conflict', and 'malicious web sites'.

StrikeReady continues to actively enrich **“Iran-Israel-Conflict”** tag 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.

The screenshot displays the StrikeReady interface. The top bar shows the query 'created_at >= 9w AND tag IN ('Iran-Israel-Conflict')'. The main area shows the 'Recon / Artifacts' page. It includes a search bar, filters for 'Artifact Type', 'StrikeReady Ver.', and buttons for 'Export all artifacts (1060)', 'Clear', 'Save', 'Subscriptions', 'Exported artifacts reports', and 'Subscribe'. A table lists artifacts with columns: Artifact Type, Alerts, Strikes, Tags, TLP, Score, and Analyst. The table contains entries for SHA256 hashes, domains, and IP addresses, each with associated tags like 'malicious', 'iran-israel-conflict', and 'malicious web sites'.

STRIKE READY

StrikeReady Analysis Engine Tool provides analysis for suspicious files, domains, IPs, or URLs. Users can view details of all extracted artifacts and may Analyze, Simulate, Export, Deploy, Retire, or View associated artifacts of any selected artifact:

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://outpost24.com/blog/hackivist-cyber-operations-iran-israel/

Tags (Optional)

Add User Tags...

☒ Extract domains

Close

Analyze

Domain: TLP White

israelnews.co.il

+ Add

Status: N/A

Registrar: N/A

First seen: 17 days ago

Domain Rank: N/A

Last seen: 5 hours ago

Are you targeted? 0

Are you at risk? 0

Simulate

Add to NPL

Export artifact

Deploy

Retire

Create case

Associated artifacts

CARA Analysis

Threat association

WHOIS

SSL certificate

Targeted geography and sectors

Associated threat campaigns

Infrastructure

Mitigation rules

Reference

Comments

CARA analysis

Re-analyze

The current security analysis of the Domain: israelnews.co.il reveals a highly concerning profile, primarily driven by a significant Analyst Score: 10, which unequivocally indicates a high probability of malicious intent or compromise, even though a Verdict: Not Found was returned by automated threat intelligence systems. This discrepancy highlights the importance of human analysis in identifying sophisticated threats. The domain was first seen: 2026-04-07 and last seen: 2026-04-24, indicating recent and active use, which warrants immediate and thorough attention. Its underlying infrastructure resolves to IP Address: 185.56.73.55, an endpoint that requires further investigation for any historical or current malicious associations or suspicious network traffic patterns. While the SSL Certificate Authority: Let's Encrypt is a common and legitimate issuer, the certificate's Not after: 2026-07-06 date points to a relatively short validity period, a characteristic frequently observed in rapidly provisioned or ephemeral command-and-control (C2) infrastructure often used by threat actors. Although no explicit Malware or Ransomware associations were directly identified within the provided data, the elevated analyst score strongly suggests a severe underlying threat that could bypass conventional defenses. Consequently, the Overall Risk: High, with a potential impact: Severe on organizational security posture, data integrity, and operational continuity if this domain is accessed or interacted with. Proactive measures, including immediate blocking of this domain and its associated IP, are critically advised to prevent potential exposure and mitigate any adverse effects effectively.

Threat association

WHOIS

SSL certificate

Targeted geography and sectors

Associated threat campaigns

Infrastructure

Mitigation rules

Reference

Analysis engine reports

Search analysis engine...

Total: 13

OPSWAT

Detected By: Religion, News and Media

04/24/2026 7:04 PM

VirusTotal

Detection Ratio: 0 / 94

04/24/2026 7:04 PM

DisposableDomains

Disposable: False

04/24/2026 7:04 PM

DNSResolver

Resolving IPs: 185.56.73.55 | Host Name: israelnews.co.il

04/24/2026 7:04 PM

StrikeReady Assessment enables organizations to continuously 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.

STRIKE READY

Assessments / Strikes

Jane Doe

Basic Query

Strike.CreationDate >= 9w

Clear

Save

Pinned: StrikeReady

Newly added

Not executed

Saved queries

StrikeReady

Custom

Drafts

SMW4626 - BRUSHWORM and BRUSHLOGGER Target Financial Institutions...

Network strike

45

Medium severity

Attack type: Financial Gain

Malware family: BRUSHLOGGER

Category: Trojan

Created at: 04/14/2026

Add to list

Strike now

STA4628 - North Korean UAT10027 Deploys Dohdoor Backdoor Targeting United States

Network strike

80

High severity

Attack type: State-Sponsored

Malware family: Dohdoor

Category: Trojan

Threat actor: UAT-10027

Created at: 04/14/2026

Add to list

Strike now

STA4627 - Transparent Tribe Deploys LuminousCookies Against Government...

Network strike

71

High severity

Attack type: State-Sponsored

Malware family: LuminousCookies

Category: Trojan

Threat actor: Transparent Tribe

Created at: 04/14/2026

Add to list

Strike now

STA4356 - Russian Actor Noname057 Launches Bobik DDoS Surge

Network strike

45

High severity

Attack type: State-Sponsored

Malware family: Bobik

Category: Botnet

Threat actor: Noname057

Created at: 04/14/2026

Add to list

Strike now

STA4619 - Chinese threat actor CL UNK 1068 Expands Operations Against Globa...

Network strike

80

High severity

Attack type: State-Sponsored

Malware family: Xnote

Category: Trojan

Threat actor: CL-UNK-1068

Created at: 04/07/2026

Add to list

Strike now

STA4623 - DangerousPassword Compromised NPM Axios Delivering...

Network strike

54

High severity

Attack type: Financial Gain

Malware family: SILKBELL

Category: Trojan

Threat actor: DangerousPassword

Created at: 04/07/2026

Add to list

Strike now

STA4618 - Mustang Panda Deploys PlugX Amid Middle East Conflict

Network strike

69

High severity

Attack type: State-Sponsored

Malware family: PlugX

Category: Trojan

Threat actor: Mustang Panda

Created at: 04/07/2026

Add to list

Strike now

STA4616 - Chinese Silver Dragon Targets Windows With GearDoor Backdoor

Network strike

80

High severity

Attack type: State-Sponsored

Malware family: SilverScreen

Category: Trojan

Threat actor: Silver Dragon

Created at: 04/03/2026

Add to list

Strike now

STA4617 - Indian SloppyLemming Leveraging BurrowShell Against...

Network strike

80

High severity

Attack type: State-Sponsored

Malware family: BurrowShell

Category: Trojan

Threat actor: SloppyLemming

Created at: 03/30/2026

Add to list

Strike now

STA4622 - Iranian MuddyWater APT Targets Multiple Industries Globally

Network strike

80

High severity

Attack type: State-Sponsored

Malware family: Dindoor

Category: Trojan

Threat actor: MuddyWater

Created at: 03/17/2026

Add to list

Strike now

Rows per page: 20

1 - 20 of 35

STRIKE READY

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 screenshot displays the StrikeReady CARA interface. The main chat area shows a conversation with a user asking about DieNet and Handala Hack. The AI assistant provides detailed information about both groups. The sidebar on the right shows the 'Information' panel for Handala Hack, including properties like Origin Country (the State of Palestine), Aliases (DUNE, Handala Hack), Target Countries (State of Israel, Hashemite Kingdom of Jordan, Republic of Albania, United States of America, United Arab Emirates), and Industries (Healthcare, Government, Public, Telecommunications, Private, Energy, Education, Media, Military).

Information

- Handala Hack**
- PROPERTIES**
 - Origin Country: the State of Palestine
 - Last Updated: 2026-03-14T07:39Z
- Aliases**
 - DUNE
 - Handala Hack
- Target Countries**
 - State of Israel
 - Hashemite Kingdom of Jordan
 - Republic of Albania
 - United States of America
 - United Arab Emirates
- Industries**
 - Healthcare
 - Government
 - Public
 - Telecommunications
 - Private
 - Energy
 - Education
 - Media
 - Military

CARA's Blog Analysis automatically extracts from a given blog or URL, enabling users to quickly perform actions such as Check reputation, Risk Identification, Deployment, and more on the extracted artifacts.

The screenshot displays the StrikeReady CARA interface. The main chat area shows a user asking about extracting artifacts from a URL. The AI assistant provides a list of extracted artifacts and a risk score. The sidebar on the right shows a '20 Green' risk score and a list of artifacts with their associated URLs and confidence levels.

Extract artifacts from https://gghackers.com/zionsiphon-malware/

I have successfully extracted artifacts from https://gghackers.com/zionsiphon-malware/. Here are the details:

File Path: IPv4 (1) registrykeypath

Search iocs

- ☐ Artifacts
- ☒ 2.52.0.0
- ☐ 2.55.255.255
- ☐ 212.150.0.0
- ☐ 212.150.255.255
- ☐ 79.176.0.0
- ☐ 79.191.255.255

Proceed →

Check Reputation

Risk Identification

View SSL Certificates

Resolved Domains

Deploy

Unblock

View Timeline

View Deployments

View Sources

Check reputation 2.52.0.0

Processing your request to check reputation. Navigate to Operations tab on the workbench for results.

20 Green

Status: Offline

Malware Family: 3

Associated URLs: 0

Linked Files: 0

AbuseIPDB: No Verdict

Artifact 2.52.0.0 is reported 0 times, has Abused confidence: 0 and 0 distinct users

AlienVault OTX: No Verdict

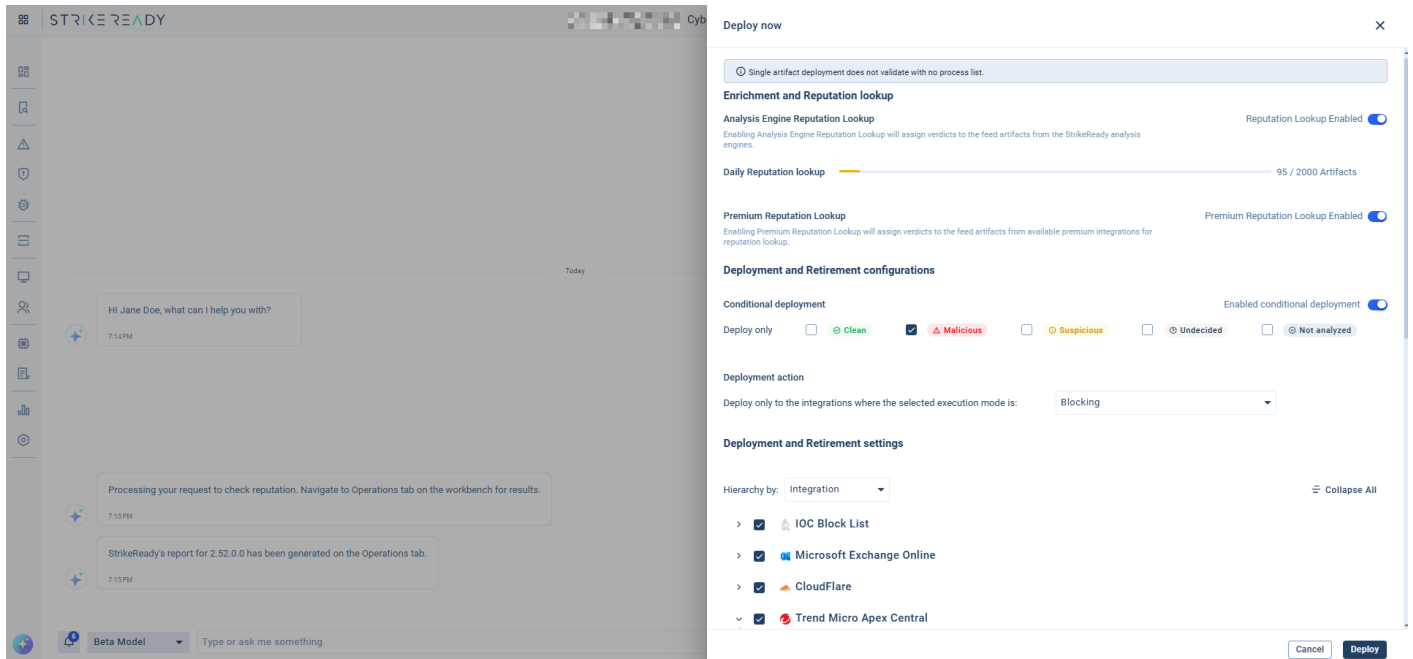
No Verdict Provided for ioc2.52.0.0, this ioc has following open portsNone

HoneyDB: No Verdict

The ANS number for this Artifact is 12400 and its organization is partner-as, il

Intel 471: No Verdict

Users can also operationalize the extracted artifacts via Enrichment and Reputation Lookup & Deployment and Retirement Configurations demonstrated ahead:



Mitigation & Remediation

- Enforce phishing-resistant MFA (FIDO2 where possible) across email, VPN, and cloud services.
- Establish strict verification protocols for internal IT support requests and restrict the use of remote assistance tools like Quick Assist and AnyDesk to counter vishing-to-wiper pipelines
- Prioritize the detection and blocking of C2 infrastructure and DNS-based backdoors associated with the latest hybrid state-sponsored and MaaS campaigns.
- Regularly alert employees to high-precision lures involving Regional Air Defense or Military Strategy themes.
- Isolate and restrict direct internet exposure for all PLC and SCADA management interfaces, with a specific focus on securing Modbus and DNP3 protocols against industrial sabotage.
- Prioritize immediate remediation of CVE-2024-30088, CVE-2024-24919, CVE-2024-4577, CVE-2026-1731, currently being weaponized for initial access and to monitor diplomatic communications.

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