STRIKEREADY

# 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.<br>**Focus:** Healthcare, Medical Equipment, and Services across Middle East (Israel) and North America (US).<br>**Recent TTPs:** T1485: Data Destruction, T1072: Software Deployment Tools, T1491.002: External Defacement, T1078.002: Valid Accounts.<br>**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.<br>**Focus:** Governments, Financials, Transportation and Logistics in Middle East (Israel, UAE, Jordan), North America (US), and Europe (UK, France).<br>**Recent TTPs:** T1059.001: PowerShell Command & Scripting, T1027: Obfuscated Information, T1102.003: Web Service, T1557: Adversary-in-the-Middle.<br>**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.<br>**Focus:** Government, Military, and Technology in Middle East (Israel) and Europe (Ukraine).<br>**Recent TTPs:** TA0001: Initial Access , T1036: Masquerading, T1486: Data Encrypted for Impact, T1562.001: Disable or Modify Tools.<br>**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.<br>**Focus:** Energy, Telecommunications, and Transportation in Middle East (Qatar, Egypt, Israel) and North America (US).<br>**Recent TTPs:** TA0040: Impact, T1491: Defacement, T1498: Network Denial of Service.<br>**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.<br>**Focus:** E-commerce (Magento/Adobe Commerce), Government, and Legal services worldwide.<br>**Recent TTPs:** TA0040: Impact, T1491.001: Internal Defacement.<br>**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.<br>**Focus:** Government, Financial, Telecommunications, and Energy in Middle East (Kuwait, Israel, Morocco), Europe (France), North America (US).<br>**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. |

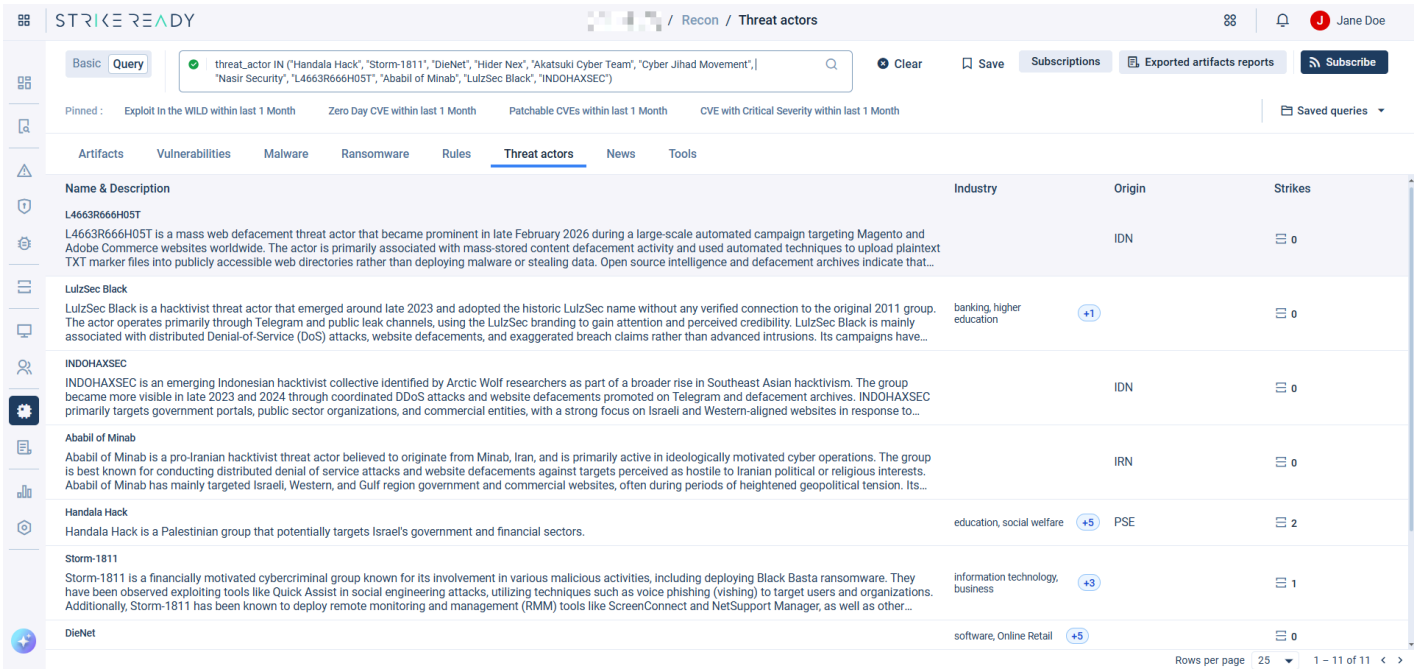
## Emerging Malware Activity

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

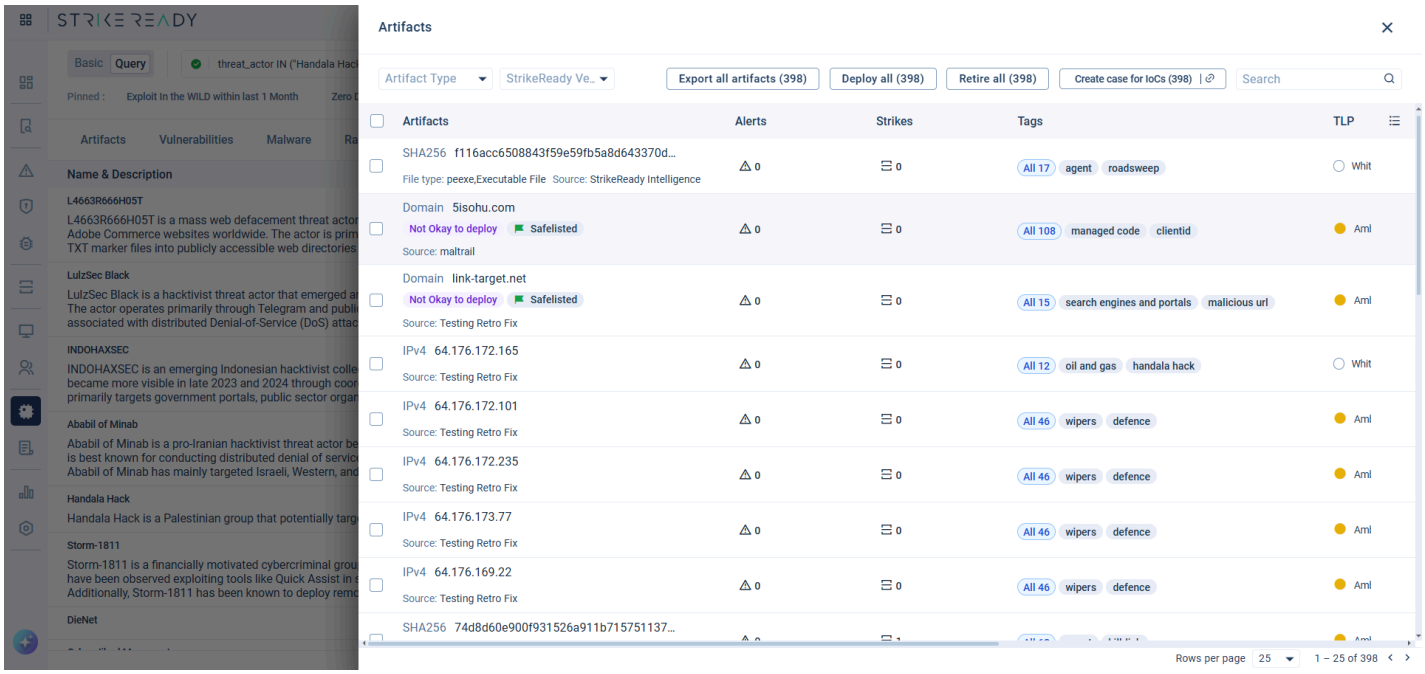
| | | |
|---|---|---|
| ChainShell | **Aliases:** chainshell.<br>**Threat Actor:** MuddyWater.<br>**Focus:** Government, Defense, and Technology in Middle East (Israel) and North America (US).<br>**Recent TTPs:** T1071.001: Web Protocols, T1059.001: PowerShell, T1562.001: Disable or Modify Tools<br>**StrikeReady 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.<br>**Threat Actor:** MuddyWater.<br>**Focus:** Government, Aviation**,** Telecommunications, Energy, and Transportation in Asia (Azerbaijan, Israel)<br>**Recent TTPs:** T1071.001: Web Protocols, T1106: Native API, T1059.003: Windows Command Shell.<br>**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

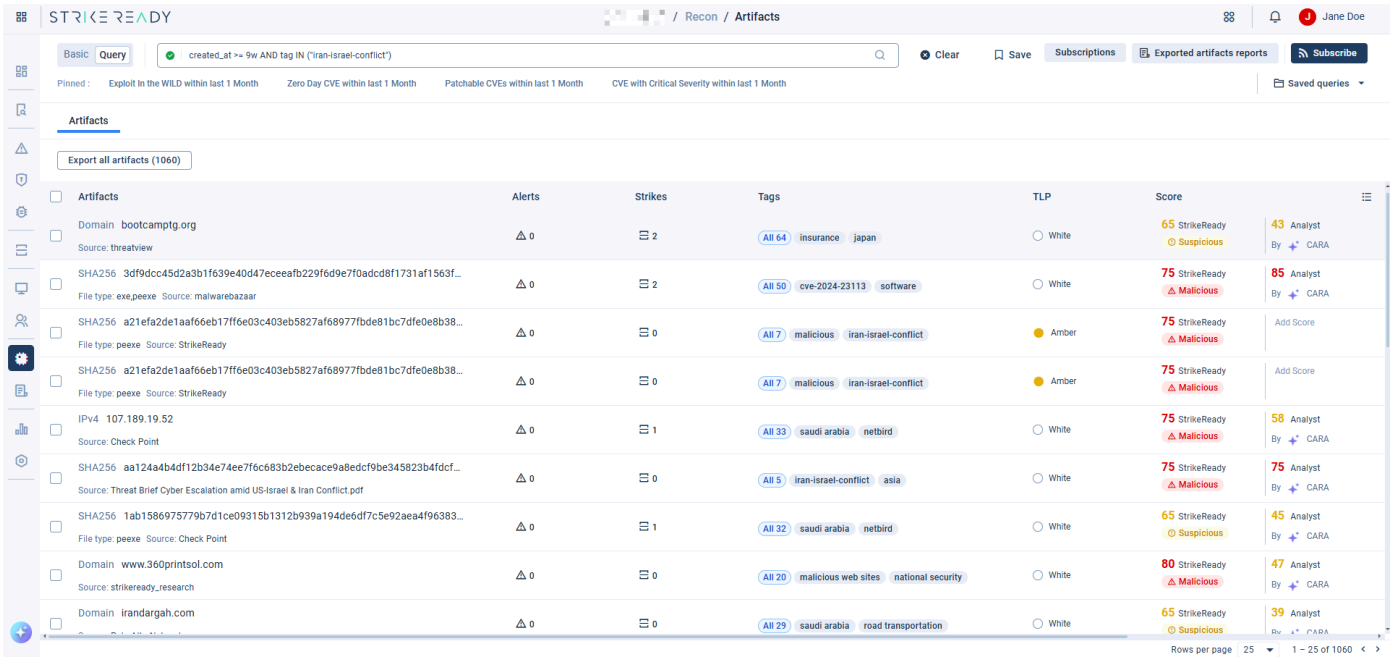
**StrikeReady Recon** provides relevant activity linked to all the active threat actors. It also provides insights into emerging threat intelligence to help security teams monitor how detection and response technologies are being utilized.



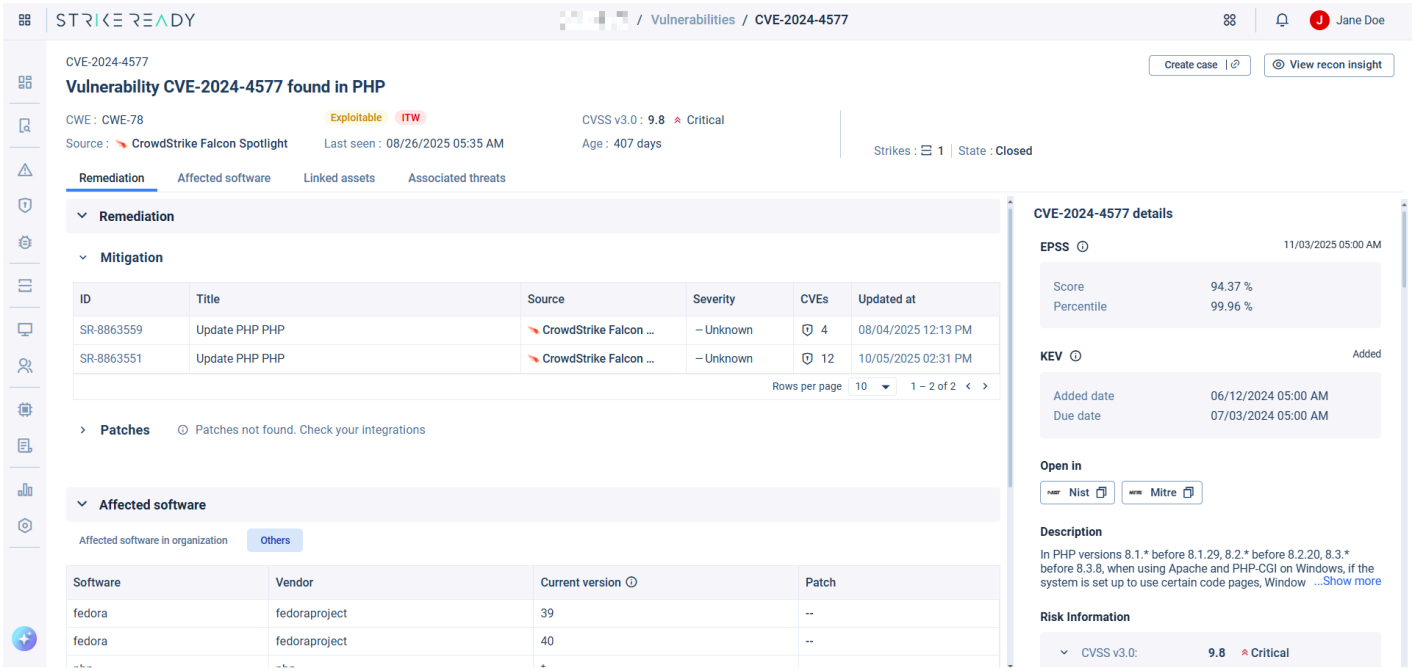
Users can navigate to Threat actor page for a detailed overview including its threat association, basic information, associated threat campaigns, artifacts, and more. StrikeReady has a total of **398** IOCs associated with Handala Hack demonstrated ahead. Navigate to StrikeReady Product for more info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



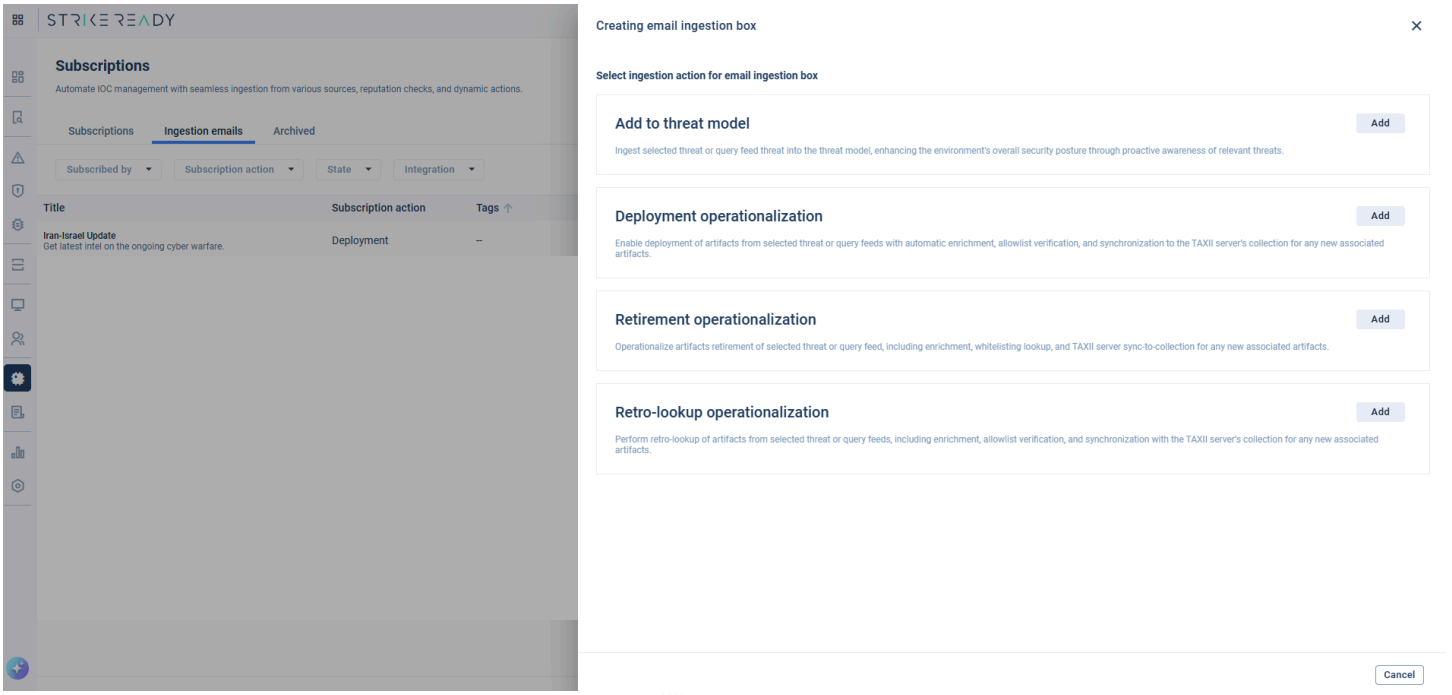

StrikeReady continues to actively enrich "**Iran-Israel-Conflict**" tag that help analysts quickly filter all the threat intelligence associated with the ongoing geopolitical escalation. This query can be subscribed to in Recon to stay protected from new threats.



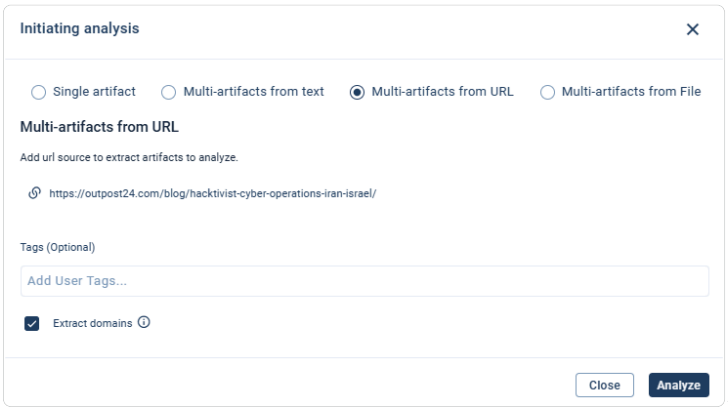
Users can also view details about the relevant vulnerabilities via StrikeReady Recon or Vulnerabilities. The primary objectives of this section are to provide risk exposure, security hygiene, and risk management.

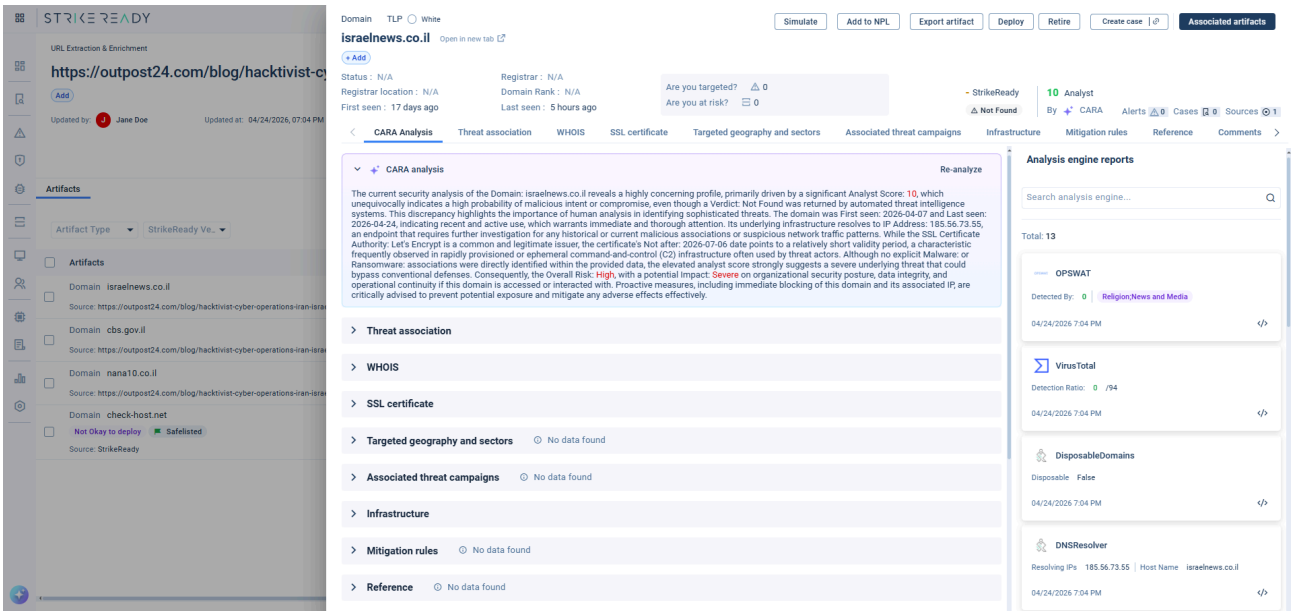



StrikeReady enables organizations to operationalize external intelligence feeds through an automated **Threat Advisory Deployment** via Email Ingestion to streamline their workflow. If configured, extracted artifacts can be automatically enriched, deployed or retired across integrated security controls.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

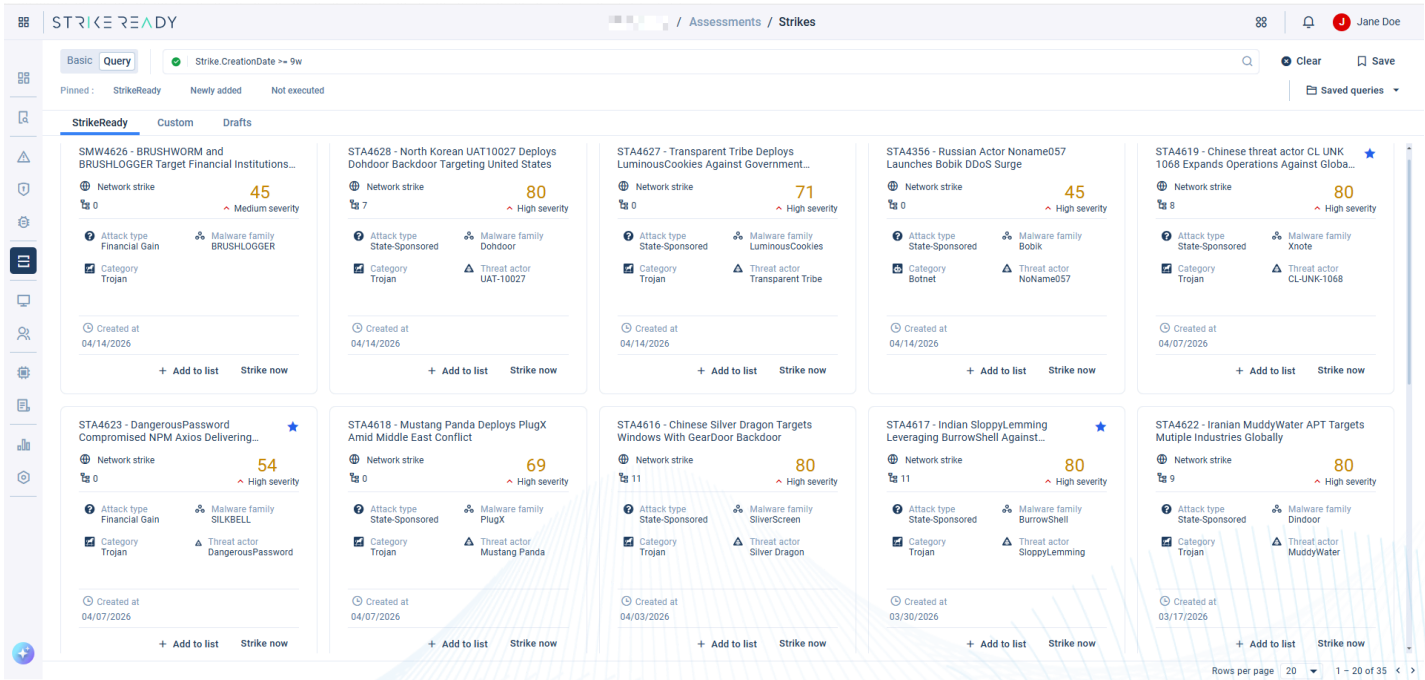


**StrikeReady Analysis Engine Tool** provides analysis for suspicious files, domains, IPs, or URLs. Users can view details of all extracted artifacts and may Analyze, Simulate, Export, Deploy, Retire, or View associated artifacts of any selected artifact:

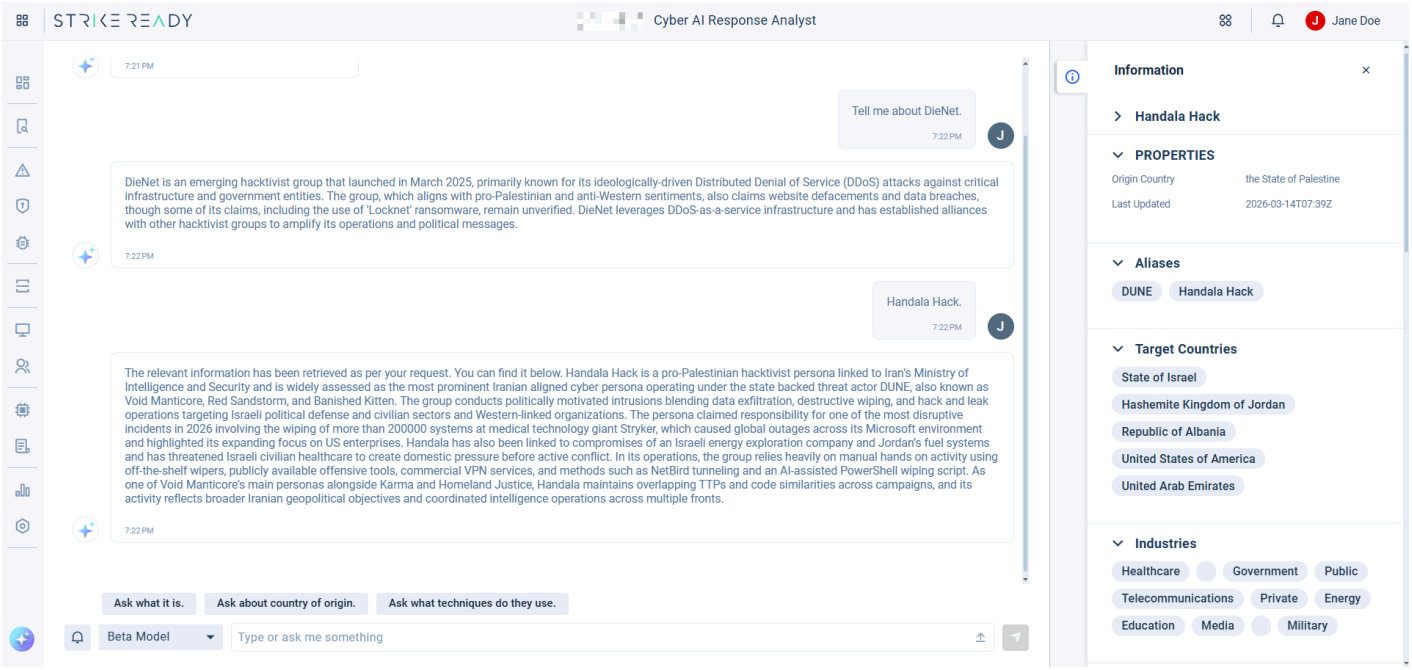


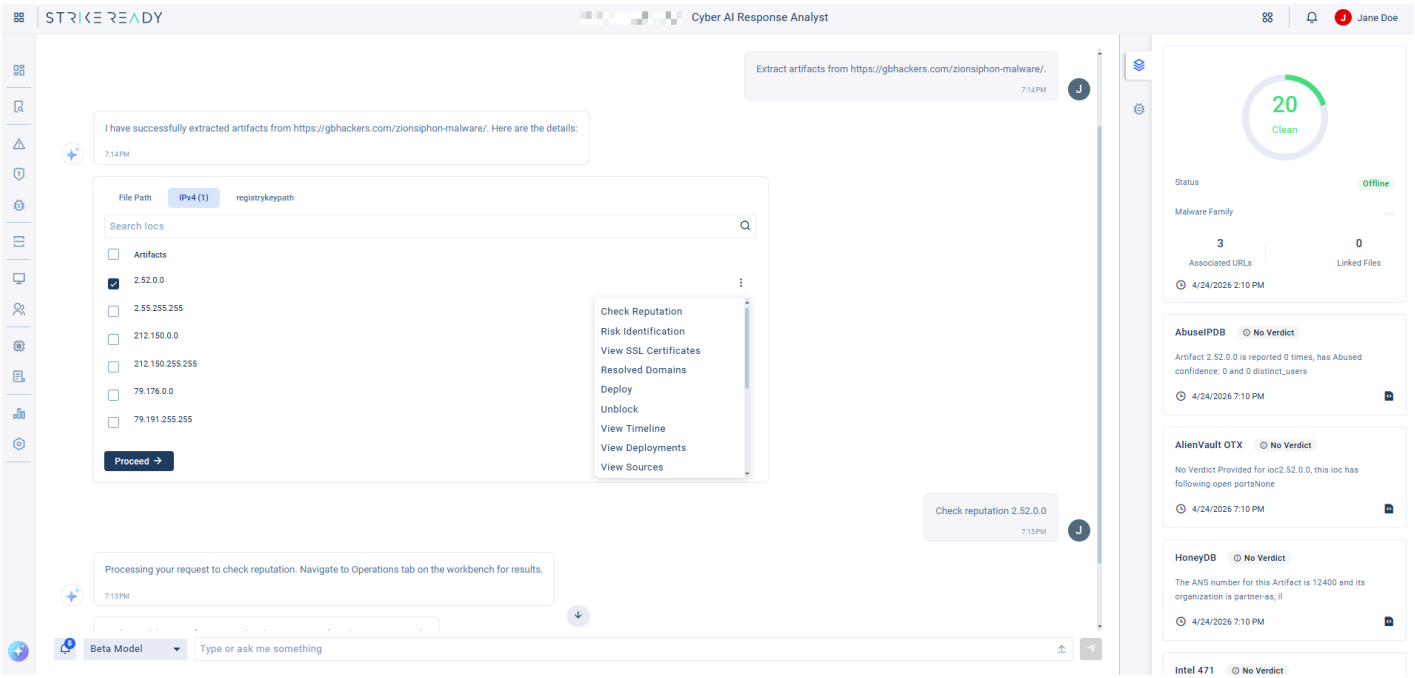

**StrikeReady Assessment** enables organizations to continuously monitor their security posture with its Stats Dashboard, Strikes, and Plan Execution workflows. It helps understand the effectiveness of your organization's security measures and identify areas that may need attention.



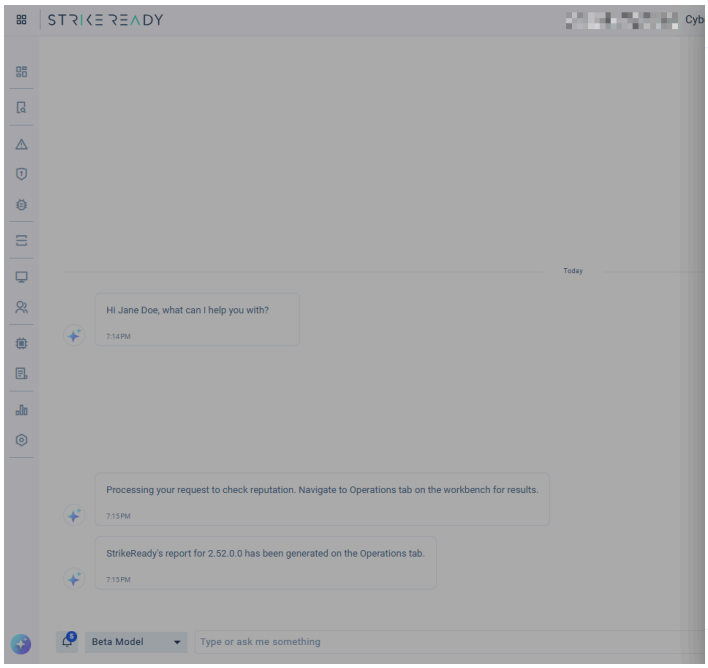
**StrikeReady's CARA**, Cyber AI Response Analyst, can inform you about the relevant threat actors, recent strikes, exploited vulnerabilities, or IOCs and advise the best course of action with real-time actionable insights to improve your response time.

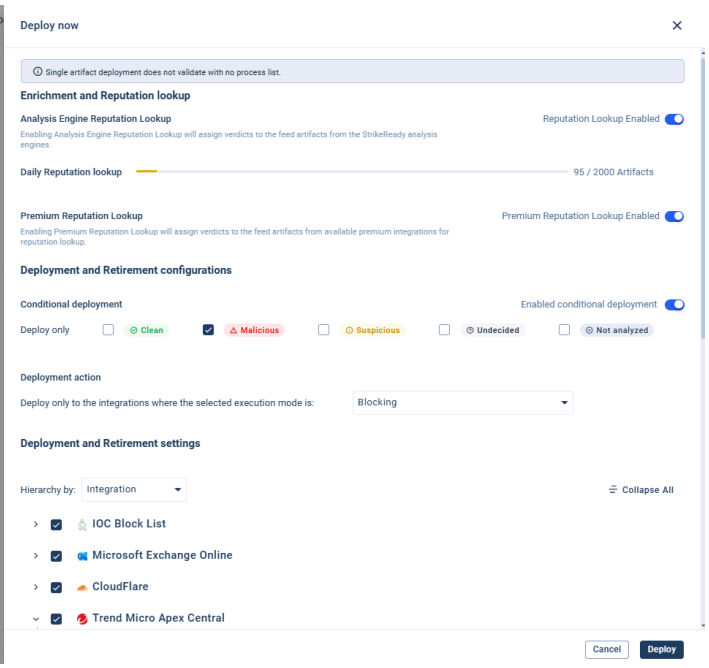



**CARA's Blog Analysis** automatically extracts from a given blog or URL, enabling users to quickly perform actions such as Check reputation, Risk Identification, Deployment, and more on the extracted artifacts.



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.