The Tripartite Cyber War

Cyber Warfare Analysis of Iran - Israel and U.S. Conflict

(June 2025 – April 2026)

Table of Contents

Overview

The digital conflict between Iran, Israel, and the United States has significantly escalated since June 2025, soon after the *12-day war* and all parties involved leveraging cyberattacks as key tools of their hybrid warfare strategies.

Beyond these nation-states, hacktivists, cybercriminals, and allied state actors have exploited periods of geopolitical tension, targeting critical infrastructure, industrial control systems (ICS), operational technology (OT), and public safety mechanisms.

The cyber conflict transitioned from a "gray zone" shadow war to full-spectrum digital combat in February 2026. While a provisional ceasefire was reached between the U.S. and Iran on April 7, the digital front remains highly volatile.

Major incidents include the near-total blackout of Iran's internet by Israeli-led operations and retaliatory Iranian strikes against U.S. and Israeli critical infrastructure. Pro-Iranian hacktivist collectives, coordinated via the "Electronic Operations Room," continue to target energy, water, and healthcare sectors globally.

Chronology of Recent Escalation (June – April 2026)

June 13–24, 2025: The Twelve-Day War

- **Initiation:** Operation Rising Lion, launched by Israel on June 13, 2025, involved massive air strikes aimed at crippling Iran's nuclear infrastructure at Natanz, Fordow, and Isfahan, alongside targeting senior military leadership.
- **Iranian Response:** Iran launched over 550 ballistic missiles and over 1,000 suicide drones (Operation True Promise) during the conflict, targeting Israeli cities and US military bases in the region, causing limited casualties and damage.
- **US Intervention:** On June 22, the US launched Operation Midnight Hammer, using B-2 bombers to destroy key underground Iranian nuclear sites, causing "major damage".
- **Conflict Impact:** The war led to thousands of casualties. Reports indicate over 1,255 people were killed in Iran, while Israeli sources reported 28+ civilian deaths.
- **Outcome:** A US-brokered ceasefire was implemented on June 24, 2025. Israel claimed to have set back Iran's nuclear and missile capabilities by several years.

February 27–28, 2026: The "Digital Fog"

- **Operation Epic Fury / Roaring Lion:** Coordinated kinetic strikes by the U.S. and Israel on Iranian leadership compounds were preceded by the largest cyberattack in history.

- **National Blackout:** Iran's connectivity dropped to **4%** of normal levels within hours. This "digital fog" crippled internal military communications and state media (IRNA, Tasnim). Network data show Iran's internet blackout is now in its 44th day, continuing in its seventh week past the 1032 hour mark.

March 2026: The Retaliatory Wave

- **Electronic Operations Room:** Established on Feb 28, this Telegram-based umbrella group coordinated 50+ hacktivist cells.
- **Stryker Medical Breach:** The group Handala Hack claimed responsibility for disrupting U.S. medical manufacturer Stryker, citing retaliation for civilian casualties. The company confirmed the attack but said it was contained only to its Microsoft environment.
- **Infrastructure Targeting:** CISA and the FBI issued "FLASH" advisories regarding Iranian-affiliated actors (CyberAv3ngers) infiltrating Rockwell Automation PLCs in the U.S. water and energy sectors. Another advisory said the telecom and communications sector was also a prime target and commonly used Wi-Fi routers were the gateway for the Iranian hackers.

April 2026: The Ceasefire & Pivot

- **April 7, 2026:** A two-week ceasefire is announced.
- **Threat Intelligence Forecast:** Experts warn that a kinetic lull allows Iranian APTs to shift from regional tactical targets to long-term strategic infiltration of U.S. defense contractors and data centers.

Key Statistics

1. Increased Attack Rates Post-February 2026

- **3.5x increase** in cyberattacks against **Israel**, making it the most targeted nation globally (21% of all incidents in the 24 hours post-strike on February 28).
- **18%** of global cyberattacks (4,239 incidents) between June 2025 and April 2026 targeted the **United States**, making it the top targeted nation over the 10-month timeline.

2. Distribution of Attack Types

- **37%** DDoS attacks: Primary disruption technique targeting financial institutions, government bodies, and military systems.
- **20%** Threat claims: Focus on psychological warfare via announcements and threats. Prominent groups: *AnonGhost* and *Cyber Isnaad Front*.
- **14%** Data breaches and leaks: Primarily targeting defense, government institutions, and private corporations in Israel and the U.S.
- **11%** Website defacements: Propaganda tool targeting public-facing websites in Israel and the Middle East.
- **10%** Ransomware attacks: With permanent destruction intent, several attacks were directed at U.S. and Israeli critical infrastructure.
- **5%** Initial access sales: Exploits targeting hard-to-reach industrial control systems (ICS) and SCADA environments.

3. Critical Sectors Targeted

The top industries targeted by Iranian-linked state-sponsored or hacktivist attacks were:
- Government/Public Sector: **27%**
- Manufacturing: **20%**
- Telecommunications: **12%**
- Media/Internet: **9%**
- Banking/Financial Services: **5.3%**

4. Critical Threat Sources

- **33% reported incidents** were attributed to **state-sponsored Iranian APT groups**, including APT34, APT39, and APT35 (Charming Kitten).
- **Hacktivist groups** were linked to **47% of incidents**, acting as proxies or independent actors:
    - **RipperSec**: Most active, targeting Israeli government agencies.
    - **313 Team/UniT 313**: Launched multi-country operations targeting Israel, the U.S., and Gulf states.

5. Specific Malware

- **20% of ransomware attacks** involved **Sicarii ransomware**, a destructive strain used by Iranian-linked actors to encrypt and permanently damage data.

6. Hacktivist and APT Group Activity

- Leading hacktivist group: **RipperSec**, responsible for **41% of DDoS activity** globally when acting independently or as proxies.
- Repeated targets include:
    - **Israel Defense Forces (IDF)**: DDoS and data breaches.
    - **U.S. cities**: 10 ransomware campaigns targeting local government systems and regional hospitals.
    - **Saudi and UAE financial sectors**: 28 defacement and DDoS attacks over 10 months.

7. Operational Outcomes of Cyberattacks

- **Iranian infrastructure disruptions**:
    - Israeli Operation "Rising Lion" caused **4 major industrial outages** in Iran, targeting steel mills and refineries directly responsible for economic output.
    - Iranian financial systems saw **a 45% reduction** in processing capacity due to malware deployed by Israeli-linked actors.

- **U.S. and Israeli critical infrastructure under attack**:
    - **140% increase** in DDoS attacks targeting Israeli entities after September 2025. At the height of the conflict, there were **40 DDoS attacks per day** targeting Israeli entities, with some extremist hacktivist affiliates threatening the U.S. for its support of Israel.
    - **$2.1 billion in ransomware damages** inflicted as U.S.-focused Iranian attacks intensified.

Iran

Motivations Behind Iranian Cyber Operations

Retaliation Against Military Strikes

- The U.S.-Israel military strikes on Iranian nuclear facilities and other strategic sites (February 2026) played a key role in sparking retaliatory cyberattacks.
- Iran leveraged its cyber capabilities as an asymmetric warfare tool to disrupt, sabotage, and impose costs on its adversaries, especially when conventional military responses were limited.
- For example, attacks on Stryker, critical medical suppliers, and NHS systems in the UK epitomize Iran's use of cyberattacks as a retaliatory tool while simultaneously showcasing its global reach and operational capabilities.

Undermining Critical Infrastructure

- Iranian actors sought to degrade and disrupt critical infrastructure, aiming to strain the functional capacity and public confidence in adversarial states like the U.S. and Israel.
    - Target sectors included energy, utilities, and transportation, with multiple Distributed Denial-of-Service (DDoS), ransomware, and wiper malware attacks reported globally.
    - Disruptions to the Jordanian wheat reserves in 2025 reflect how Iran leveraged cyber capabilities to sow chaos in neighboring countries that aligned with its adversaries.

Influence Operations to Bolster Iran's Regional Standing

- Iran has long used cyber operations to secure political and ideological objectives domestically and abroad.
    - The Twelve-Day War of 2025 between Israel and Iran emphasized the significance of the information domain, wherein both nations sought to control the narrative and garner domestic and international support. Iran's efforts focused on propaganda, discrediting rivals, and driving security fatigue among its adversaries' populations [1].
    - Example: Iranian actors incited dissent via large-scale disinformation campaigns leveraging AI-generated content and targeted U.S. and Israeli audiences to undermine public confidence in leadership decisions.

Socio-Political Goal of Regime Stability

- Domestically, Iran sought to suppress dissent and control its population, especially during political unrest. Censorship included scaling internet activity down to as low as 1% of regular levels during national protests or periods of heightened internal dissent.

- Iranian operations surveilled and pursued dissidents abroad through spear-phishing attacks, digital harassment, and disinformation efforts to suppress their voices and influence.

Strategic Espionage

- Iranian hackers focused on espionage to gain access to sensitive military, political, and industry-related data across the U.S., Israel, and global targets.
    - This included penetrating supply chain networks tied to defense contractors and conducting surveillance of critical national infrastructure, such as energy grids and water supply systems.
    - Exfiltrating sensitive information allowed Iran to execute hack-and-leak operations and collect intelligence about adversaries' military readiness and potential vulnerabilities.

Ransomware and Wiper Malware

- Iranian state-sponsored actors launched ransomware and wiper malware attacks against Israeli critical services, including government entities, utilities, and healthcare systems.

- For instance, Iranian-aligned hackers leveraged malware capable of exfiltrating and wiping sensitive data in several waves between June 2025 and early 2026.

- High-profile ransomware attacks have been observed, including deployments targeting prominent Israeli and U.S. organizations.

Hacktivism and Influence Operations

- Hacktivism surged in favor of Iran as an instrument to amplify geopolitical propaganda and disrupt adversaries like Israel, the U.S., and allied nations. Iran has mobilized hacktivist groups such as Cyber Av3ngers, Mysterious Team Bangladesh, and others aligned with pro-Iranian causes.

- Example: Groups like DieNet threatened to target U.S. assets if it intervened in the Israel-Iran war and later claimed attacks on Israeli governmental organizations, including disinformation campaigns.

Targeting Critical Infrastructure and ICS/OT Environments

- Iranian actors escalated efforts to exploit vulnerabilities in ICS and OT systems, focusing attacks on the energy, transport, and water sectors.

- Iranian actors likely initiated denial-of-service (DoS) attacks and manipulated ICS (like the 2024 incident where water storage tanks in Texas were compromised).

- Disruptions in Middle Eastern energy supply chains were noted, including targeting Jordan and Saudi Arabia when they supported U.S.

Attacks on Neighboring Middle Eastern Countries

- Iran's cyber operations extended to neighboring countries that supported Israel and U.S.

For example:

- The Mysterious Team Bangladesh issued warnings and targeted Jordan and Saudi Arabia critical infrastructure.

- Previous attacks like hacking a wheat storage facility in Jordan exemplified efforts to destabilize the region's food security.

Key Threat Actor Profiles

- **Handala Hack (MOIS-linked):** The most prominent persona in the 2026 conflict. Known for "hack-and-leak" operations and wiper attacks. Recently threatened "Quds Day" waves against Israeli and U.S. influencers. Claimed hack on U.S. medtech giant Stryker. The company took more than 10 days for recovery post the confirmed cyberattack.
- **CyberAv3ngers (IRGC CEC):** Specializes in OT (Operational Technology) attacks. Focuses on internet-facing industrial control systems (ICS).
- **Peach Sandstorm / Gray Sandstorm:** Iranian APTs observed conducting massive password-spraying campaigns against Microsoft 365 environments, impacting over 300 organizations in Israel and the UAE in March 2026

Tools, Tactics, and Techniques Used by Iranian State-Sponsored Actors

Malware and Exploits

Ransomware Deployment: Iranian threat actors, such as APT34 (OilRig) and APT39 (Remix Kitten), deployed custom ransomware and wiper malware in their campaigns against Israeli and U.S. targets.

- The ransomware often featured obfuscation techniques to evade detection and was designed to destroy systems rather than solely demand ransoms.
- For example, Sicarii, a ransomware with a critical flaw that permanently discards encryption keys, was used to encrypt data but rendered recovery impossible—even if a ransom payment was made.

Wiper Malware: Iranian actors utilized destructive malware to paralyze critical infrastructure.

- Examples include Shamoon, which has evolved into more sophisticated iterations, capable of wiping systems within operational technology (OT) domains.

Malware Evolution

- **Wipers:** Use of BibiWiper, Hatef, and Rewire variants.

- **Telegram C2:** The FBI documented Iranian MOIS actors using Telegram bots as command-and-control infrastructure for malware like Pictory and KeePass lookalikes to target dissidents and researchers.

Command Injection Exploits:

- Iranian hackers exploited vulnerabilities similar to **CVE-2023-20198** (used by the PRC group Salt Typhoon) to access critical infrastructure, modify configurations, and exfiltrate data.

Tools

Social Engineering Toolkits: Iranian threat actors used spear-phishing emails, often with themes such as Hamas-Israel conflicts or the U.S.-Iran conflict, to lure high-value targets, especially in government, defense, and energy sectors.

These tools often employed convincing email spoofing frameworks and custom malspam equipped with tracking pixels.

Tactics

Distributed Denial-of-Service (DDoS) Attacks:

- Hacktivist groups like Cyber Av3ngers and pro-Iranian sympathizers conducted DDoS attacks on Israeli and U.S. government systems, airports, transportation hubs, and financial institutions.
- DDoS campaigns typically relied on botnets built using compromised IoT devices.

Hack-and-Leak Operations:

- Iranian-linked groups engaged in hack-and-leak operations, such as leaking sensitive U.S. military data acquired through cyber espionage. They often used platforms like Telegram to distribute leaked information

Israel

Motivations Behind Israeli Cyber Operations

Protecting National Security

- Israel's primary motivation was to combat perceived existential threats posed by Iran's nuclear development program and its proxy networks across the Middle East.
- Through Operation Rising Lion (June 2025) and subsequent cyber offensives, Israel targeted Iran's nuclear facilities, missile systems, and military infrastructure, aiming to delay or neutralize Iran's ability to develop nuclear weapons.

Gaining Strategic and Tactical Advantage

- Israel frequently engaged in cyber espionage operations against Iranian military and political structures to track Iran's weapon development or plan future countermeasures.
- Israeli cyber threat actors were reportedly embedded in Iranian networks, utilizing their intrusion to conduct both real-time reconnaissance operations and coordinated military strikes.

Countering Regional Influence

- Following the Twelve-Day War (2025), Israel's cyber operations shifted to combat Iranian public influence campaigns.
    - Operations included discrediting Iran's propaganda narratives through its own hack-and-leak and disinformation campaigns.
    - For instance, actions targeting the BadeSaba app were designed to sow distrust between Iranian citizens and their government while making Israel's cyber reach and capabilities visibly intimidating.

Disrupting Iranian Proxies

- Besides directly targeting Iran, Israeli operations aimed to undermine Iranian proxies operating in the region, including those in Lebanon, Syria, and Iraq.
- For example, campaigns targeted communication channels used by groups like Hezbollah, shutting down support infrastructures for Iranian-aligned militias.

Offensive Cyber Operations

- Israel launched Operation Rising Lion in June 2025, a campaign targeting Iranian critical infrastructure, including missile bases, nuclear development facilities, and key military assets through both kinetic and cyber means. This included Mossad-led sabotage operations.

- Israeli actors, likely Predatory Sparrow, targeted Iran's financial infrastructure and military systems, causing:

- Service outages in Iran's Bank Sepah, disconnecting customers from accounts and halting withdrawals and card transactions.

- Sabotage of steel plants, railroads, and gas stations in Iran.

Espionage and Pre-emptive Cyber Measures

- Israel worked closely with U.S. agencies to degrade Iranian cyber capabilities.

- A reported Israeli bombing destroyed a section of Iran's cyber warfare headquarters near Tehran, limiting its ability to respond.

- Espionage, including real-time surveillance of Iranian military and nuclear development, featured prominently in Israel's cyber operations.

Key Actor Profiles

Unit 8200: Orchestrated the hack of surveillance/CCTV cameras. Operations focused on degrading C2 (Command & Control) structures and intercepting IRGC communications.

Tools, Tactics, and Techniques Used by Israel

Malware and Exploits

Predatory Sparrow's Custom Malware:

- The Israeli-aligned group Predatory Sparrow used tailored malware tools to disrupt Iran's financial and ICS systems. Custom malware was deployed to sabotage key industrial systems, including steel plants and energy pipelines.

Covert Network Exploits:

- Leveraging intelligence gathered by cyber reconnaissance, Israeli actors likely used covert exploits targeting Siemens PLCs and ICS devices, similar to those used in past operations like Stuxnet.

Tactics

Precision Espionage:

- Israeli cyber teams employed targeted spear-phishing campaigns and strategic compromises of Iranian military, academic, and governmental systems.

Cyber Sabotage:

- Israeli intelligence used sophisticated virus models, possibly evolved iterations of Stuxnet, during Operation Rising Lion to damage Iranian nuclear enrichment facilities systematically. A covert USB infection strategy, likely leveraging local agents, facilitated direct delivery of malicious strains to restricted networks.

United States

- The U.S. joined forces with Israel in joint strikes on Iranian nuclear and military infrastructure in February 2026, provoking a strong cyber retaliation from Iran.

- U.S. cybersecurity operations focused on:

 - Collaborating with Israel to launch offensive cyberattacks, which allegedly degraded Iranian military and digital networks.

 - Enhancing security across its own and allied critical infrastructures by sharing intelligence and issuing warnings about Iran's cyber retaliation capabilities.

Motivations Behind U.S. Cyber Operations

Protecting Regional Allies

- The U.S. joined Israel in its strikes on Iranian nuclear infrastructure during operations launched in February 2026, reinforcing its commitment to defending regional allies and preserving geopolitical stability in the Middle East 2.
- The use of offensive cyber tactics, paired with targeted airstrikes, indicates a coordinated strategy to weaken Iran's military assets while minimizing casualties or collateral damage from conventional methods.

Thwarting Iranian Retaliation

- As Iran ramped up its cyber retaliation post-strike, the U.S. aggressively pursued Iranian cyber infrastructure to neutralize its ability to counterattack.
- Real-time disruptions of Iranian command-and-control (C2) servers and dismantling of key ransomware infrastructure were paramount in mitigating potential harm to U.S. critical infrastructure.

Safeguarding U.S. Cyber Interests

- The U.S. proactively worked to defend against Iranian cyberattacks on sectors like energy, water systems, and banking. Iranian hackers exploited known vulnerabilities in ICS systems and attempted to target recognition-rich institutions .
- U.S. response involved issuing security advisories to critical infrastructure operators worldwide and implementing mitigation strategies to contain the spread of Iranian malware.

Key Actor Profile

US Cyber Command: In January 2026, during the capture and extraction of the Venezuelan President Nicolas Maduro, the agency used offensive cyber capabilities to likely blackout the entire country during the period of the operation. A claim that was

confirmed by the POTUS in one his public address. It is likely possible that U.S. is or plans to use such capabilities against Iran.

Tools, Tactics, and Techniques Used by the United States

Tools

Advanced Cyber Surgeries:

- During critical joint cyber-offensive campaigns with Israel (e.g., February 2026 military operations), the U.S. likely employed tools similar to TAILHOOK, a highly classified and modular offensive tool designed by U.S. intelligence agencies.

Exploitation Frameworks:

- Frameworks such as Metasploit (heavily modified) and bespoke offensive tools enabled the U.S. actors to penetrate Iranian infrastructure and execute remotely triggered destructive attacks.

Tactics

Zero-Day Exploits:

- U.S.-based cyber teams leveraged undisclosed zero-day vulnerabilities in industrial equipment, communication networks, and OT systems within Iranian nuclear and infrastructure facilities.

Specialized Cyber Operations Teams:

- Cyber teams worked with Unit 8200 (Israel's cyber warfare team) to deliver tailor-made payloads that disrupted processes and spread laterally across networks.

Malware

- **Evolution of Stuxnet**:

  Building on the legacy of the "Olympic Games" operation, it is suspected that the U.S. deployed enhanced malware to sabotage Iranian nuclear centrifuges and military systems, effectively causing hardware failures or rendering key installations inoperable.

Vulnerabilities Exploited During the Conflict Period

The threat landscape from June 2025 to April 2026 has been dominated by the exploitation of critical- and high-severity vulnerabilities, a trend that is both industry- and region-agnostic. The provided data, reveals a significant number of flaws with CVSS scores of 9.0 or higher, indicating a persistent focus by threat actors on impactful vulnerabilities.

Notably, vendors such as Cisco, Fortinet, and Microsoft appear multiple times, highlighting recurring challenges in securing widely deployed enterprise products. The affected technologies span a broad range of network infrastructure, including security appliances, VPN gateways, and enterprise management platforms, which are attractive targets due to their privileged position in corporate networks.

The persistence of older vulnerabilities on this list alongside newer ones also suggests that many organizations struggle with timely patch management.

CVE ID	Product	Vendor	CVSS(V3)
CVE-2021-32030	Gt Ac2900 Firmware	Asus	9.8
CVE-2024-56145	Cms	Craft	9.8
CVE-2025-32433	Otp	Erlang	10.0
CVE-2024-42009	Webmail	Roundcube	9.3
CVE-2025-24016	Wazuh	Wazuh	9.9
CVE-2024-0769	Dir 859	D Link	9.8
CVE-2024-54085	Megarac Spx	Ami	9.8
CVE-2025-6543	Netscaler Application Delivery Controller	Citrix	9.8
CVE-2014-3931	Multi Router Looking Glass	Multi Router Looking Glass Project	9.8
CVE-2016-10033	Phpmailer	Phpmailer Project	9.8
CVE-2025-47812	Wing Ftp Server	Wftpserver	10.0
CVE-2025-25257	Fortiweb	Fortinet	9.8
CVE-2025-53770	Sharepoint Enterprise Server	Microsoft	9.8
CVE-2025-2776	On Prem	Sysaid	9.8
CVE-2025-54309	Crushftp	Crushftp	9.8
CVE-2025-20281	Identity Services Engine	Cisco	10.0
CVE-2025-20337	Identity Services Engine	Cisco	10.0
CVE-2025-54948	Apex One	Trendmicro	9.8

CVE-2025-43300	Macos	Apple	10.0
CVE-2025-7775	Netscaler Application Delivery Controller	Citrix	9.8
CVE-2025-57819	Freepbx	Freepbx	9.8
CVE-2025-53690	Experience Manager	Sitecore	9.0
CVE-2025-5086	Delmia Apriso	Dassault Syst Mes	9.0
CVE-2025-10585	Chrome	Google	9.8
CVE-2025-20333	Adaptive Security Appliance	Cisco	9.9
CVE-2025-10035	Goanywhere Mft	Fortra	9.8
CVE-2015-7755	Screenos	Juniper	9.8
CVE-2017-1000353	Jenkins	Jenkins	9.8
CVE-2025-21043	Devices	Samsung	9.8
CVE-2010-3765	Firefox	Mozilla	9.8
CVE-2025-61882	Concurrent Processing	Oracle	9.8
CVE-2016-7836	Skysea Client View	Skygroup	9.8
CVE-2025-54253	Experience Manager	Adobe	10.0
CVE-2025-2746	Xperience	Kentico	9.8
CVE-2025-2747	Xperience	Kentico	9.8
CVE-2025-61932	Lanscope Endpoint Manager And Detection Agent	Motex	9.8
CVE-2025-54236	Commerce	Adobe	9.1
CVE-2025-59287	Windows Server 2012	Microsoft	9.8
CVE-2025-6205	Delmia Apriso	Dassault Syst Mes	9.1
CVE-2025-24893	Xwiki Platform	Xwiki Platform	9.8
CVE-2025-48703	Centos Web Panel	Centos Webpanel	9.0
CVE-2025-21042	Devices	Samsung	9.8
CVE-2025-9242	Fireware Os	Watchguard	9.8
CVE-2025-12480	Triofox	Triofox	9.1
CVE-2025-64446	Fortiweb	Fortinet	9.8
CVE-2025-61757	Identity Manager	Oracle	9.8
CVE-2025-55182	React Server Dom Parcel	Meta	10.0
CVE-2022-37055	Go Rt Ac750 Firmware	Dlink	9.8
CVE-2025-66644	Arrayos Ag	Array	9.8
CVE-2025-58360	Geoserver	Geoserver	9.8

CVE-2025-14611	Centrestack	Gladinet	9.8
CVE-2025-59718	Fortios	Fortinet	9.8
CVE-2025-59374	Live Update Client	Asus	9.8
CVE-2025-20393	Secure Email	Cisco	10.0
CVE-2025-14733	Fireware Os	Watchguard	9.8
CVE-2025-37164	Oneview	Hpe	9.8
CVE-2026-20045	Unified Communications Manager	Cisco	9.8
CVE-2024-37079	Cloud Foundation	Vmware	9.8
CVE-2025-52691	Smartermail	Smartertools	10.0
CVE-2026-24061	Inetutils	Gnu	9.8
CVE-2026-23760	Smartermail	Smartertools	9.8
CVE-2026-24858	Fortianalyzer	Fortinet	9.8
CVE-2026-1281	Endpoint Manager Mobile	Ivanti	9.8
CVE-2019-19006	Freepbx	Sangoma	9.8
CVE-2025-40551	Web Help Desk	Solarwinds	9.8
CVE-2025-11953	Metro Development Server	Metro Development Server	9.8
CVE-2026-24423	Smartermail	Smartertools	9.8
CVE-2025-40536	Web Help Desk	Solarwinds	9.8
CVE-2024-43468	System Center Configuration Manager	Microsoft	9.8
CVE-2026-1731	Remote Support Privileged Remote Access	Beyondtrust	9.8
CVE-2020-7796	Zimbra Collaboration Suite	Synacor	9.8
CVE-2021-22175	Gitlab	Gitlab	9.8
CVE-2026-22769	Recoverpoint For Virtual Machines	Dell	10.0
CVE-2026-20127	Catalyst Sd Wan Manager	Cisco	10.0
CVE-2017-7921	Ds 2Cd2032 I Firmware	Hikvision	9.8
CVE-2021-22681	Factorytalk Services Platform	Rockwellautomation	9.8
CVE-2025-26399	Web Help Desk	Solarwinds	9.8
CVE-2026-20963	Sharepoint Server	Microsoft	9.8

CVE-2026-20131	Secure Firewall Management Center	Cisco	10.0
CVE-2025-32432	Cms	Craft	10.0
CVE-2025-54068	Livewire	Livewire	9.8
CVE-2026-33017	Langflow	Langflow Ai	9.8
CVE-2025-53521	Big Ip Apm	F5	9.8
CVE-2026-3055	Netscaler Application Delivery Controller	Citrix	9.8
CVE-2026-35616	Forticlientems	Fortinet	9.8
CVE-2026-1340	Endpoint Manager Mobile	Ivanti	9.8

Zero-Day Vulnerabilities

From June 2025 to April 2026, analysis of the 52 total observed zero-day vulnerabilities reveals that over 86% were rated as critical (30) or high (15), indicating a strong trend towards severe, exploitable flaws.

Notably, vendors such as Citrix, Fortinet, and Samsung experienced multiple critical zero-day events, underscoring a recurring pattern of vulnerabilities in widely-used network devices, security appliances, and mobile technologies. The active exploitation of these zero-days in products like Netscaler Application Delivery Controller and Fortinet's Fortisiem suggests a focused interest from threat actors in targeting enterprise-grade infrastructure for initial access and lateral movement. The diversity of affected products, from enterprise servers like Microsoft Sharepoint to endpoint security solutions like Trendmicro Apex One, highlights the broad attack surface presented by these critical vulnerabilities.

CVE ID	Product	Vendor	CVSS(V3)
CVE-2025-6543	Netscaler Application Delivery Controller	Citrix	9.8
CVE-2025-53770	Sharepoint Enterprise Server	Microsoft	9.8
CVE-2025-54948	Apex One	Trendmicro	9.8
CVE-2025-25256	Fortisiem	Fortinet	9.8
CVE-2025-43300	Macos	Apple	10.0
CVE-2025-7775	Netscaler Application Delivery Controller	Citrix	9.8
CVE-2025-57819	Freepbx	Freepbx	9.8
CVE-2025-53690	Experience Manager	Sitecore	9.0
CVE-2025-21042	Devices	Samsung	9.8

CVE-2025-21043	Devices	Samsung	9.8
CVE-2025-10585	Chrome	Google	9.8
CVE-2025-61932	Lanscope Endpoint Manager And Detection Agent	Motex	9.8
CVE-2025-64446	Fortiweb	Fortinet	9.8
CVE-2025-14611	Centrestack	Gladinet	9.8
CVE-2025-20393	Secure Email	Cisco	10.0
CVE-2025-14733	Fireware Os	Watchguard	9.8

Iranian Cyber Operations' Global Reach

Threats to the West

Iranian state-sponsored actors extended their offensive campaigns globally:

- Cyberattacks on North American water, energy, and telecommunications networks were reported.
- Cyberattack on US-based healthcare company Stryker, disrupted operations worldwide.
- Use of spear phishing and social engineering attacks to infiltrate networks, with a focus on government, military, critical infrastructure, and private-sector organizations.

Influence Operations by AI and Hack-and-Leak Tactics

- Leveraging **AI-generated bots**, Iran conducted coordinated disinformation and influence campaigns, both regionally and globally:

- Proliferation of fake content to sway public opinion and undermine trust in Israeli and U.S. institutions.

- Hack-and-leak operations targeting sensitive government and military data were used to destabilize adversaries and exploit their lack of trust among citizens.

Hacktivism and Malware Deployment in the Conflict

- Over 100 hacktivist groups participated in the Iran-Israel cyber conflict, with the majority supporting Iran's agenda.

- Threat actor activity levels peaked during key conflict milestones, such as Combat Operation Rising Lion in June 2025 or the U.S.-Israel strikes in February 2026.

- Examples:

- Arabian Ghosts and Mysterious Team Bangladesh staged several large-scale distributed denial-of-service (DDoS) attacks on Israeli telecom and public health sectors.

- Iran's APT34 (OilRig) and APT39 (Remix Kitten) operated joint ransomware and espionage campaigns against U.S. military contractors.

Geopolitical Response

- Post the Israeli bombing of Iran's cyber unit in Tehran, an observed decline in Iranian cyber activity was linked to resource constraints, Internet blackouts, and losses of senior leadership in cyber warfare operations.

- Russia-affiliated actors, such as NoName057(16), also became involved in the conflict, conducting their own campaigns against Israeli critical infrastructure.

Conclusion

The period from June 2025 to April 2026 was an unprecedented era of hybrid cyber warfare between Iran, Israel, and the United States. Intensifying geopolitical tensions have resulted in waves of destructive ransomware, DDoS attacks, and hacktivism, targeting critical infrastructures such as energy, healthcare, and financial systems. Both sides employed cyber capabilities for offensive and defensive strategies, while disinformation and influence campaigns flooded the digital battlefield.

Global organizations, particularly those in critical sectors, remain at risk of collateral damage as cyberattacks continue to ripple across networks worldwide. This conflict has highlighted the need for international cooperation, robust cybersecurity defenses, and a proactive approach to mitigate the spread and impact of cyber hostilities.

Industry Recognition

Cyble's capabilities are highly praised by global analysts, industry critics, and cybersecurity leaders

Gartner

Cyble Recognized in **Three Gartner® Hype Cycle™ Reports** for the **Second Consecutive Year 2025, TechScape 2025 & More**

FROST & SULLIVAN

Cyble Named Leader in Frost Radar™ Cyber Threat Intelligence 2024

Y Combinator

Cyble featured among AI startups backed by Y Combinator (YC) 2025

FORRESTER®

Cyble Recognized in Forrester's **External Threat Intelligence** Service Providers Landscape, **Q1 2026 report**

QKS Group

SPARK Matrix™ 2025

LEADER

Cyble Named as a Leader in Digital Threat Intelligence Management

AMERICA'S BEST STARTUP EMPLOYERS Forbes 2026

Recognized as one of America's Best Startup Employers by Forbes

Cyble Secures Four Prestigious Honors at the 2026 Global Infosec Awards

Gartner Peer Insights.

Ranked No. 1 among the top Security Threat Intelligence Providers.

4.8/5

Cyble Named in America's Greatest Startup Workplaces 2025, By Newsweek

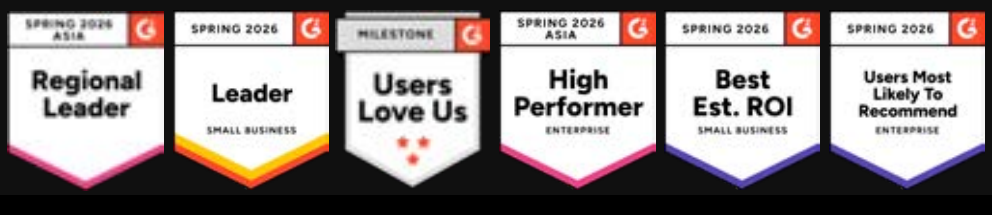
Cyble Wins Three Top InfoSec Innovator 2025 Awards

Named a leader in the G2 Grid for Dark Web Monitoring and Threat Intelligence

2026 WINNER CYBER SECURITY EXCELLENCE AWARDS

BEST SOFTWARE 2026 Top 50

Cyble Sets a New Benchmark With **40 Badges in G2 Spring 2026 Report** — Its Highest Ever



OUR INVESTORS

BLACKBIRD · KING RIVER · SUMMIT PEAK · Singtel innov8 · BizLabs · Y Combinator · SPIDER CAPITAL · svb Silicon Valley Bank

10080 North Wolfe Road, Suite SW3-200, Cupertino, CA 95014 | contact@cyble.com | +1 888 673 2067


Stay Ahead of the Next Threat
REQUEST YOUR DEMO NOW!
Experience the power of predictive security with Cyble.