CHECK POINT

EXPOSURE MANAGEMENT

THE USE OF DDOS ATTACKS IN THE ISRAEL-IRAN WAR

April 2026



TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

BACKGROUND 4

ATTACKS OBSERVED 5

DDOS ATTACKS 5

COLLABORATIONS OBSERVED BETWEEN GROUPS 15

COMPARATIVE ANALYSIS: JUNE 2025 ISRAEL-IRAN CONFLICT VS. THE FEB-APRIL ISRAEL-IRAN WAR 16

CONCLUSIONS 17

RECOMMENDATIONS 19

CONTACT US 22

EXECUTIVE SUMMARY

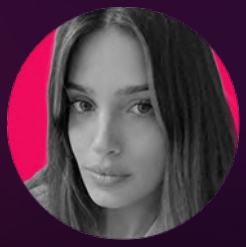
Between February 28 and April 7, 2026, the Israel-Iran war unfolded as a 38-day period of simultaneous physical and digital hostilities between Israel and Iran - more than three times the duration of the June 2025 Israel-Iran conflict. Check Point Exposure Management analyzed the operation using intelligence collected across open, deep, and dark web sources, identifying key threat actors, attack techniques, sectors targeted, and strategic implications.

This analysis is underpinned by Check Point's large-scale intelligence collection and processing capabilities, enabling continuous monitoring of a vast ecosystem of threat actor communications, infrastructure, and data flows across open and clandestine environments. This provides visibility into adversarial activity at a scale and depth not typically accessible to individual organizations, allowing for early identification of emerging patterns, coordinated campaigns, and evolving threat methodologies.

Distributed Denial-of-Service attacks were a dominant tactic across the operation's first five weeks, sustained at elevated levels by a rotating ecosystem of hacktivist groups operating under shared ideological frameworks and coordinating primarily through Telegram. Government and Defense were the most heavily targeted sectors, though Education, Telecommunications, Insurance, and Finance also absorbed significant pressure. The Finance and Banking sector demonstrated the strongest defensive posture, maintaining consistent availability throughout the operation - a pattern attributed to proactive geo-IP blocking measures that Israeli financial institutions had implemented and maintained across the full 38-day period. As the operation progressed, DDoS activity gradually gave way to data-leak narratives, defacement campaigns, and recycled dataset distribution, particularly in the final weeks when actors shifted toward perception-driven operations under the OpIsrael 2026 framework.

Amit Navon & Naomi Atias





**This is part of a larger body of research we published to our customers, aimed at analyzing and contextualizing cyber activity throughout the conflict.*



BACKGROUND

On February 28, 2026, the Israel-Iran war commenced, encompassing both physical and cyber hostilities between Israel and Iran. The operation spanned 38 days and concluded on April 7, 2026. Prior to the escalation, intelligence assessments confirmed that Iran had been expanding its cyber operational capacity since August 2025, developing a structured "shadow cyber force" composed of dozens of groups across complementary capability tiers - establishing command-and-control servers, acquiring domains, and building recruitment infrastructure ahead of a planned regional escalation.

The eight-month inter-operation period between the June 2025 conflict and the Feb-April Israel-Iran war was therefore not a period of cyber inactivity but of deliberate preparation. The speed and breadth of actor mobilization on Day 1 of the operation - with at least five distinct groups claiming operations across eight sectors within the first 48 hours - is consistent with pre-planned hacktivist mobilization rather than spontaneous response to kinetic events.

Check Point Exposure Management tracked and recorded over 450 incidents across the operation period. Official statements from Israeli authorities indicated that Iranian cyber operations continued to target high-impact assets including critical infrastructure, but that these attempts were largely being mitigated - a factor that contributed to a visible shift in adversary targeting toward more accessible private sector organizations in the operation's later phases.

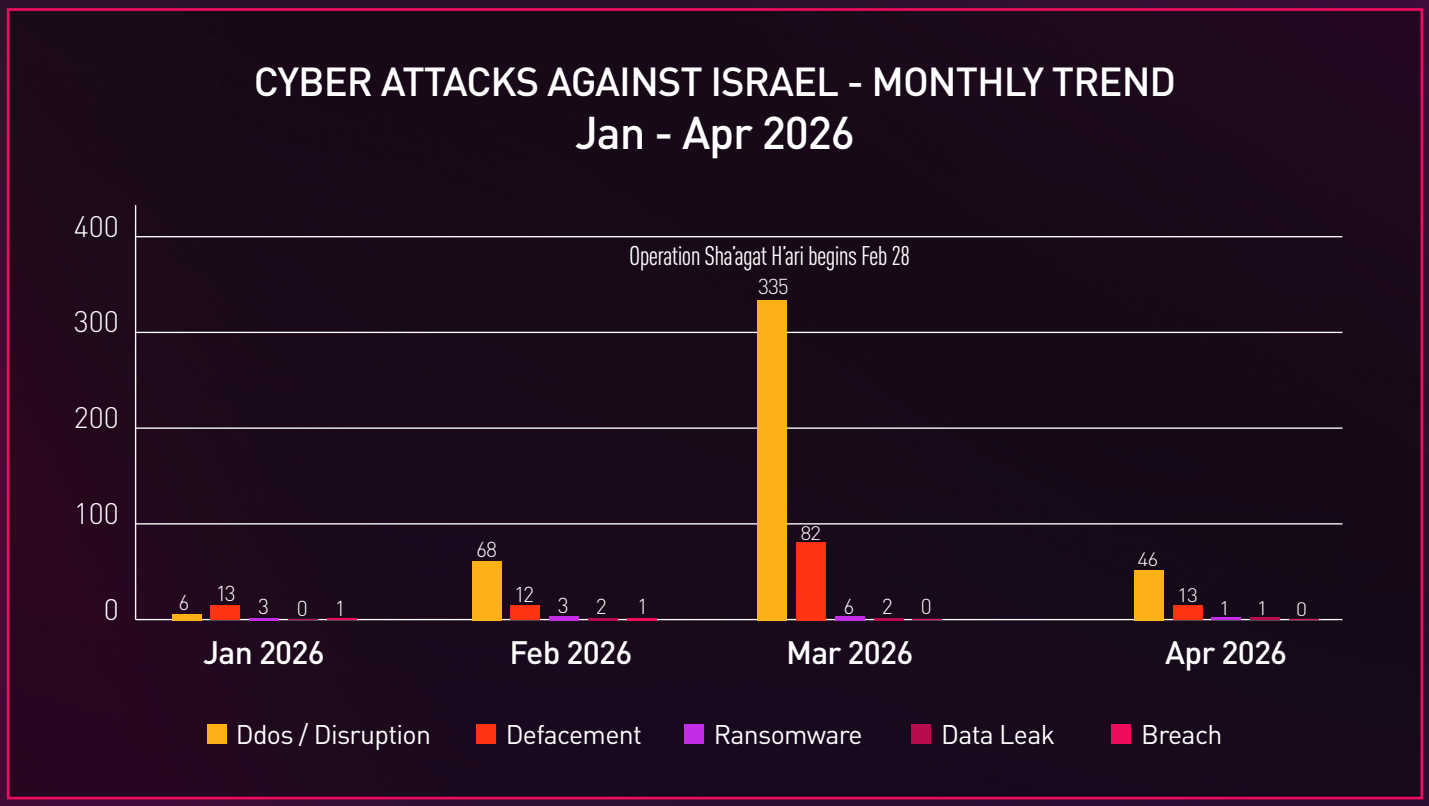


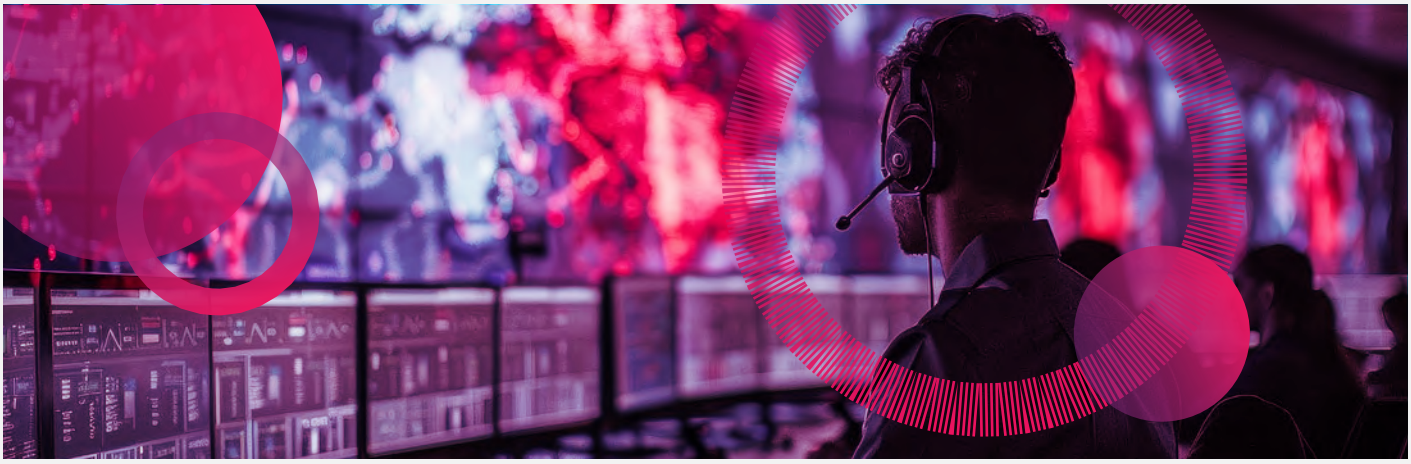
Figure 1: Attacks against Israel - Monthly trend

ATTACKS OBSERVED

DDoS Attacks

DDoS Attacks Per Day - Campaign Timeline

The DDoS campaign across the Feb-April Israel-Iran war's 38-day window exhibited a structured three-phase pattern. This phase structure reflects a more sophisticated and sustained operational framework than has been observed in prior Israel-Iran conflict cyber cycles.



Phase I - Escalation (February 28 - March 7)

DDoS activity surged immediately on Day 1, February 28, with at least four distinct threat actor groups - RipperSec, Keymous+, Nation of Saviors, and Hider_Nex - claiming coordinated operations across at least eight targets spanning finance, telecommunications, energy, government, media, defense, and civilian infrastructure. This constituted the densest period of DDoS activity in the operation.

Telecommunications emerged as the most heavily targeted sector in Phase I, with at least five separate providers affected. The primary Israeli telecommunications provider was subjected to a compound operation by Hider_Nex combining a volumetric DDoS attack with a claimed large-scale subscriber data exfiltration. A regional community provider also reported a cyberattack causing disruptions to telephony, internet, and television services with no attribution established at the time.

By March 3-5, the actor ecosystem had expanded significantly. At least six distinct groups - Mad Ghost, BD Anonymous, HackHax, Z-Net, RipperSec, and CEArmy - were active simultaneously, extending targeting across defense, energy, telecommunications, logistics, healthcare, academia, media, municipal councils, and government services. RipperSec was the most prolific actor of Phase I, claiming at least five simultaneous targets on Day 1 alone. By March 5, Dark Storm Team claimed its most strategically significant DDoS cluster of the entire operation: simultaneous attacks against the Prime Minister's Office, three government ministries, and the national security agencies. This concentration on Israel's apex governmental architecture represented the most symbolically significant DDoS cluster observed.

Phase I Assessment:

Maximum DDoS intensity; pre-planned multi-actor mobilization from Day 1; telecommunications and government bore the heaviest load; at least 10+ distinct actor groups active; both single-vector and multi-vector operations observed; fabricated DDoS claims also detected, with at least one claim identified as containing manipulated timestamp data.



Phase II - Sustained Campaign (March 8 - March 28)

Phase II represents the longest and analytically most rich period of the operation. DDoS activity continued at elevated but rotational levels, with distinct actor groups cycling in and out rather than operating simultaneously at full capacity. This rotation pattern - not visible in the June 2025 conflict's 12-day window - indicates greater operational coordination and resource management across the hacktivist ecosystem.

March 9-12 saw DDoS campaigns led by Team Fearless and NoName057(16) targeting the Israeli Central Bank, State Comptroller, media broadcasting companies, municipal governments, and defense contractors. NoName057(16) and the affiliated Cyber Islamic Resistance appeared to coordinate attacks targeting defense infrastructure and municipal platforms simultaneously. March 10 saw a renewed wave led by NoName057(16), Mad Ghost, and Team Fearless, including the temporary takedown of a prominent national news website - one of the few DDoS operations in the entire operation with partially confirmed service impact.

March 12 brought DDoS claims against digital payment services, telecommunications, and media-adjacent organizations from Keymous+ and Moroccan Black Cyber Army. Influence operations also emerged alongside DDoS: public transport information displays were manipulated to show a false missile alert message - assessed as a psychological influence operation exploiting high-visibility public information systems.

March 15-17 saw continued multi-actor DDoS campaigns. The March 16 window introduced new actors: Fynix (Iraqi linked Islamic Cyber Resistance), claiming attacks against a defense technology firm specializing in sonar systems and a FinTech platform. Check-Host results for the FinTech target showed a "Resource Limit Is Reached" error, indicating some degree of actual service degradation - one of the more credible DDoS impact indicators of the operation. RipperSec's targeting of a major Christian Zionist advocacy organization also represented an extension of targeting beyond Israeli domestic entities.

March 22-24 featured the highest volume of simultaneous DDoS actors. NoName057(16) demonstrated the most structured and consistent DDoS campaign of the period, targeting defense-related organizations, telecommunications providers, municipal authorities, transportation infrastructure, and political bodies with greater target prioritization than other groups. C.E. Army conducted extensive, template-based DDoS campaigns against financial services, education, defense-adjacent industries, technology, logistics, and civilian platforms - characterized by high posting volume, duplicated targets, and semi-automated behavior. DieNet Network produced the highest raw volume of DDoS claims, targeting commercial platforms, media, education, non-profit organizations, and low-profile civilian services - largely indiscriminate with branded "attack notification" pages designed to enhance perceived credibility. CoupTeam/BotnetKingdom produced limited technical indicators including Cloudflare error responses and time-bound disruptions, providing partial validation of service degradation.

March 26-29 saw C.E. Army sustain its DDoS campaign with a deliberate sectoral focus on the Israeli insurance sector, targeting a digital insurance platform, an insurance agency, and a fuel and energy company across three consecutive days - the latter representing a notable expansion into energy infrastructure targeting. NoName057(16) shifted to targeting municipalities, transportation infrastructure, political organizations, and financial institutions. BD Anonymous claimed a government-affiliated public initiative website with monitoring links indicating temporary connectivity issues.

Phase II Assessment:

Rotational actor ecosystem with groups cycling in and out over 21 days; NoName057(16) demonstrated most structured targeting; C.E. Army and DieNet Network dominated by volume; new actors added (Fynix, CoupTeam/BotnetKingdom); insurance sector emerged as C.E. Army's sustained focus; energy sector added to target set; fabricated evidence and "proof amplification" tactics proliferating.





Phase III - De-escalation and Narrative Pivot (March 29 - April 7)

Phase III is defined by a measurable decline in DDoS publication volume alongside a sharp increase in data leak claims, defacement activity, and recycled dataset distribution. This pivot was analytically consistent with two dynamics: defensive adaptation making sustained DDoS increasingly less effective, and the OpIsrael 2026 annual period providing a narrative framework for visibility-focused activity that does not require operational disruption to generate psychological impact.

By March 31, the DDoS landscape showed a clear slowdown in both volume and quality. RuskiNet conducted one DDoS operation with observable real-world impact - an Israeli media outlet was temporarily unavailable while core broadcasting services continued operating - making it one of the few confirmed-impact DDoS incidents of the entire operation. C.E. Army continued publishing DDoS claims within short timeframes, but without substantiated evidence of sustained disruption.

April 1 saw the rise of OTP flooding - large-scale abuse of legitimate SMS and email authentication mechanisms to generate confusion - and RuskiNet's continued low-impact DDoS claims against minor Israeli entities. No coordination between actors was observed.

By April 7-12, DDoS had been effectively supplanted by data-driven narrative operations as the primary visible activity. April 7 report explicitly noted: "While DDoS operations previously played a central role, current activity shows a decline in verified service disruption, alongside a continued presence of unsubstantiated DDoS claims with limited or no observable impact." DDoS publications were now primarily associated with C.E. Army and DieNet, functioning as low-barrier visibility tools rather than mechanisms for operational disruption. The April 12 report confirmed "a decline in the volume of DDoS-related publications" as the dominant trend.

Phase III Assessment:

Measurable DDoS volume decline; pivot to data leak narratives and recycled datasets under OpIsrael 2026 framework; RuskiNet confirmed media-sector disruption (Mar 31) one of few confirmed-impact DDoS events of the operation; DDoS continued as background noise but no longer primary tactic; de-escalation consistent with post-ceasefire patterns.

DDoS Attacks by Threat Actor

The following table summarizes all identified DDoS threat actors observed across the 38-day operation, organized by estimated activity level and phase presence:

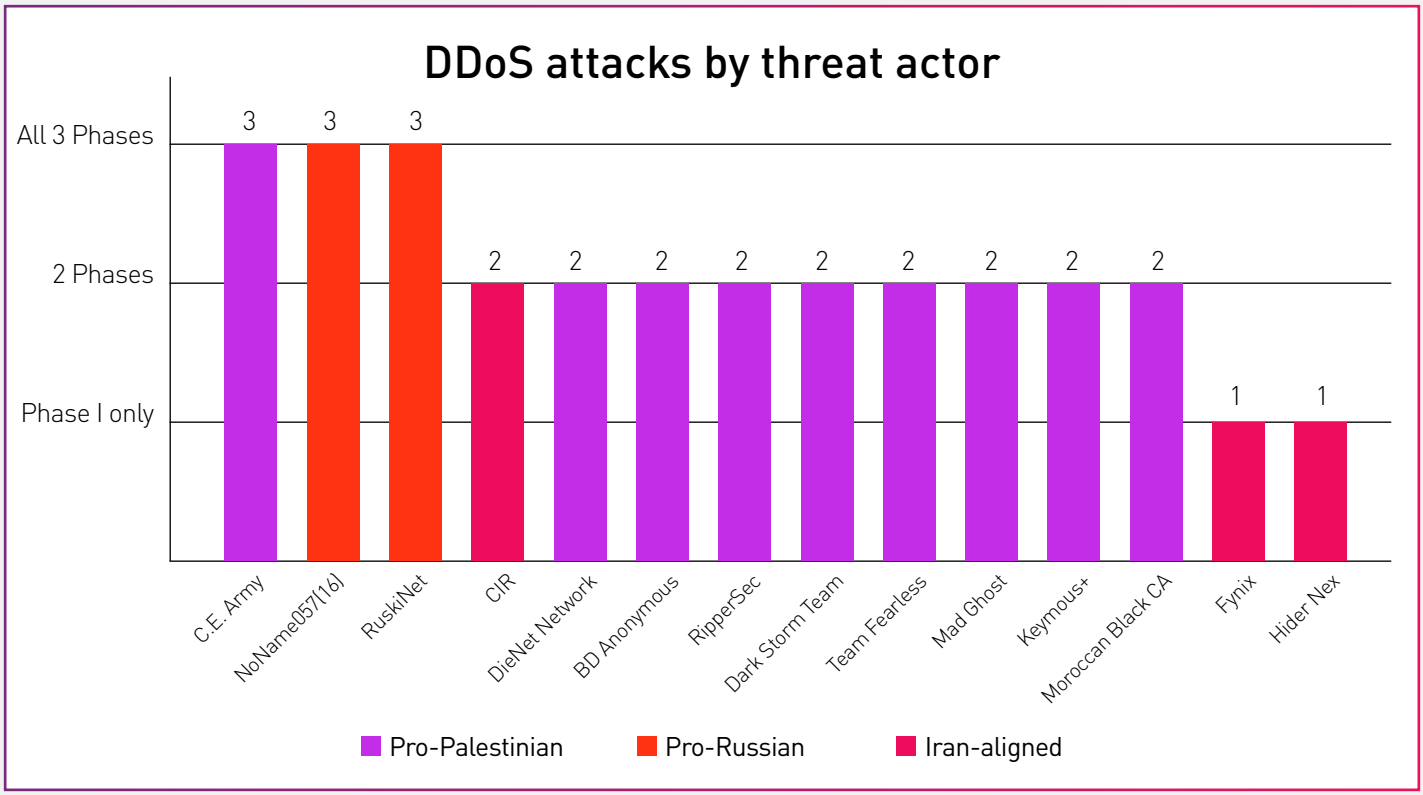


Figure 2: DDoS attacks by threat actor

DDoS Attacks by Sector

The following analysis is based on the cumulative DDoS targeting observed across the operation. Sector distribution percentages below are derived from this verified dataset. Sector attribution reflects the primary intended target category for each claimed operation, not confirmed impact.

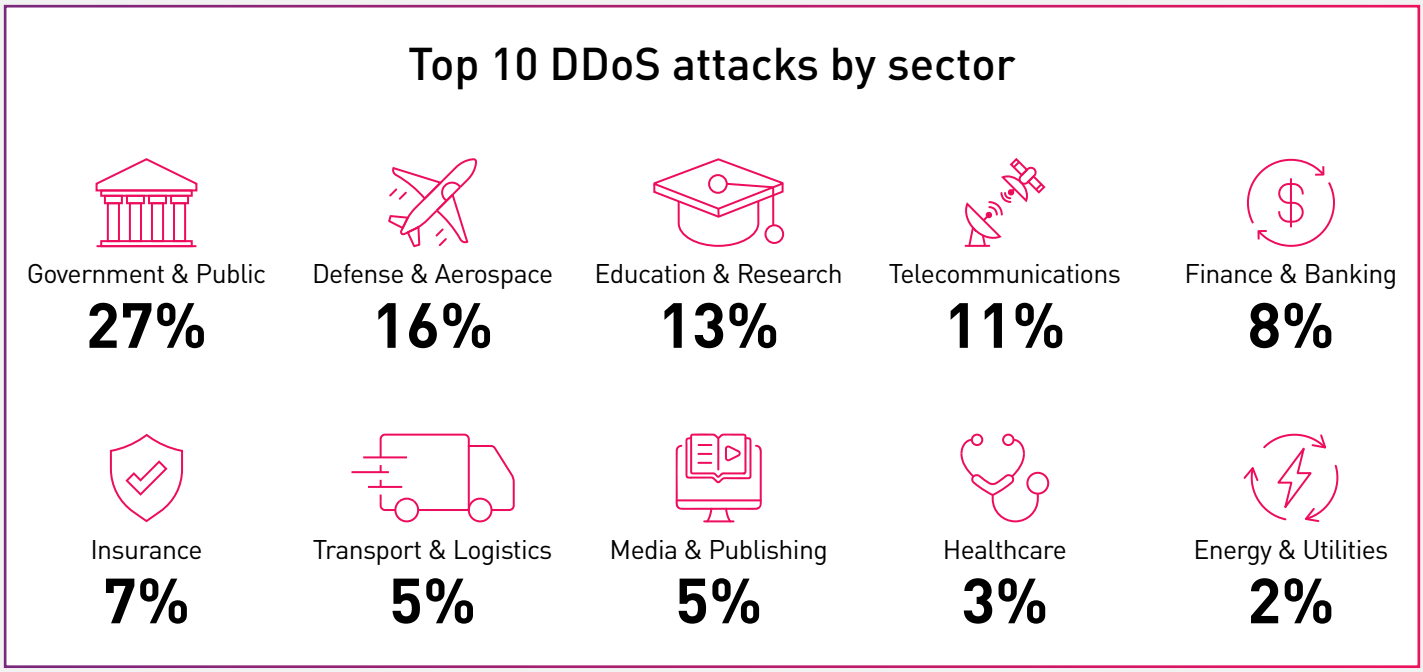
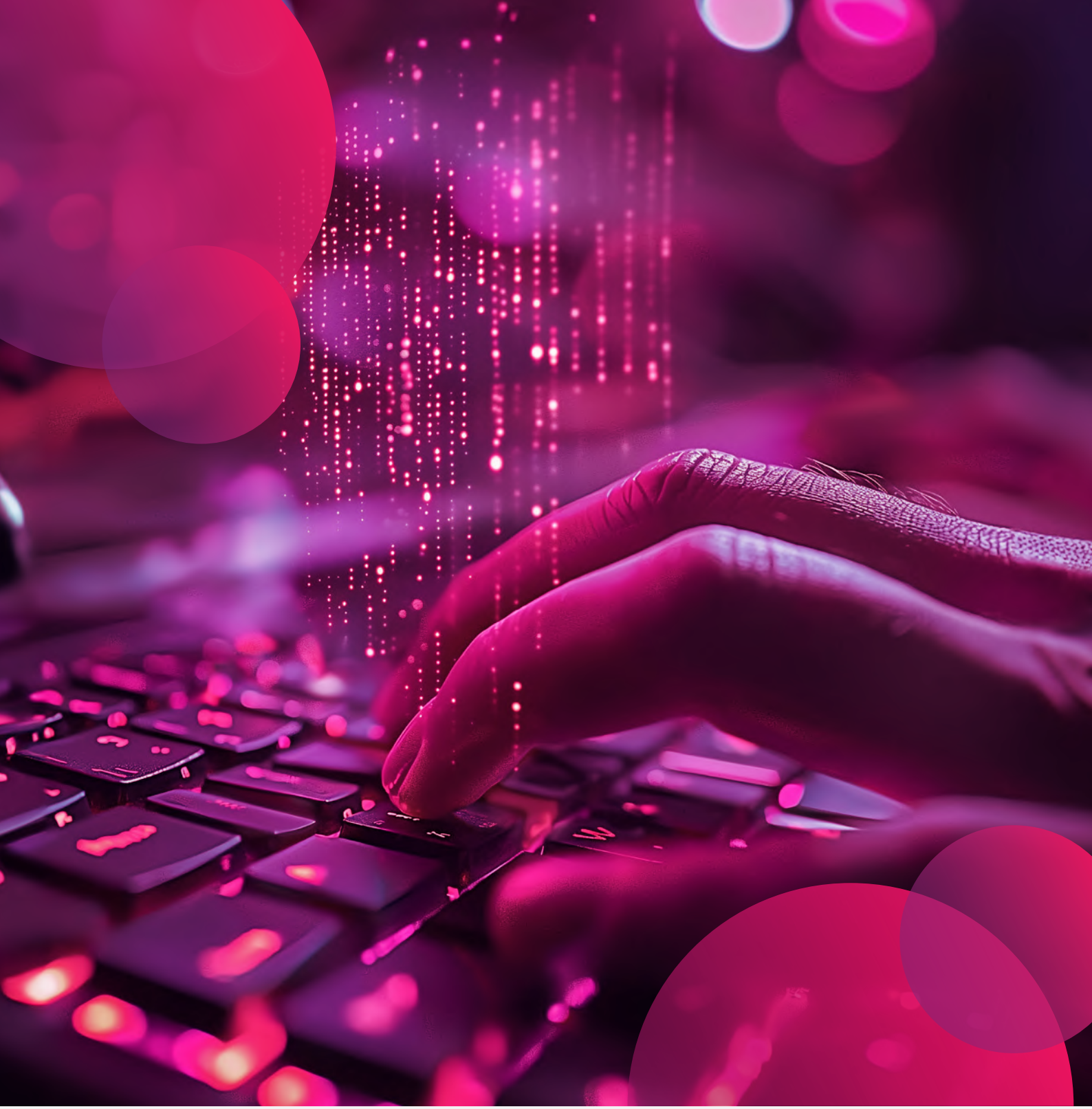


Figure 3: DDoS attacks by sector



Finance and Banking - Strategic Absence or Successful Defense?

For the second consecutive major operation, the Finance and Banking sector experienced a disproportionately low volume of confirmed DDoS impact relative to threat actor intent. This pattern - now observed across both the June 2025 and the Feb-April Israel-Iran war - warrants specific analytical treatment.

The primary defensive measure contributing to this outcome is geo-IP blocking, which Israeli banks reportedly implemented at the peak of DDoS activity, blocking all incoming IP traffic originating from outside the country. Sustaining this measure across 38 days - more than three times the duration of the June 2025 conflict - implies that the policy was formalized or maintained at a higher threat threshold than in the prior operation.

The data does show attempted targeting. Dark Storm Team, NoName057(16), RipperSec, and DabiAl Leaks all claimed operations against financial institutions during the operation. The national banking authority was specifically targeted during the March 10 wave by Team Fearless, with some service degradation indicators reported. A financial regulatory entity was targeted in mid-March by BD Anonymous under the "Operation Electronic Holocaust" framing. However, none of these incidents resulted in confirmed sustained disruption consistent with a successful DDoS campaign.

It is also critical to note that the low DDoS impact on the Finance and Banking sector does not indicate the sector was untargeted by cyber operations more broadly. Phishing campaigns impersonating the National Insurance Institute, Israeli banks, and payment services were active throughout the operation. The social engineering attack surface against financial sector customers was under sustained pressure even as institutional DDoS defenses held.

Assessment:

The Finance and Banking sector's resistance to DDoS impact across two consecutive operations is the most clearly positive defensive outcome observable from the data. However, the sector remains a high-value target. The absence of confirmed impact is not equivalent to reduced adversary intent - it reflects a successful defensive posture that must be actively maintained. Should geo-IP restrictions be relaxed, financial institutions should anticipate immediate re-targeting.





DDoS Tactics, Techniques, and Procedures (TTPs)

The following TTP observations are drawn from across all 29 daily reporting documents and reflect patterns that were consistent across Phase I through III:

Evidence and Proof Methods Used by Threat Actors

- Check-Host availability tool links: The primary "proof" mechanism across all actors and phases. Widely noted to reflect defensive mechanisms (WAF/CDN filtering, geo-blocking) rather than confirmed outages, and are frequently non-conclusive.
- Browser error screenshots: HTTP 503, 502 Bad Gateway, 500 Internal Server Error, 403 Forbidden, and Cloudflare 524 timeout errors widely shared as attack evidence. These are not independently confirmatory of DDoS causation.
- Commercial IP stresser services: C.E. Army, CIR, and several affiliated actors consistently used commercial IP stresser infrastructure rather than custom tooling, consistent with low-sophistication DDoS operators.
- Branded attack notification pages: DieNet Network used custom "attack notification" web pages asserting ongoing attacks against target domains - a perception tool rather than technical evidence.
- Fabricated claims with manipulated evidence: At least one DDoS claim during Phase I was identified as fabricated, with the accompanying screenshot showing manipulated timestamp data reflecting a future date.
- Conflicting indicators: In multiple cases, DDoS claims showed partial availability alongside reported errors - suggesting either partial targeting success, defensive rate-limiting, or geo-based access restrictions mistaken for outages.

Coordination and Amplification Patterns

- Telegram as primary coordination and publication platform: All major DDoS actors published claims, recruited participants, and amplified results via Telegram channels throughout the operation.
- Cross-channel amplification: Claims published by one actor were routinely reshared across affiliated channels, multiplying perceived reach without additional operational activity.
- OpIsrael as shared operational framework: The OpIsrael annual campaign provided a narrative umbrella that enabled actors from diverse geographies - Bangladesh, Morocco, Turkey, Indonesia, Iraq - to coordinate under shared ideology without direct operational collaboration.
- Target list sharing: Multiple reports noted that target lists were shared across Telegram channels, enabling lower-capability actors to simply claim operations against pre-identified targets without independent targeting intelligence.



DDoS Claim Credibility Framework

The DDoS campaign across the Feb-April Israel-Iran war's 38-day window exhibited a structured three-phase pattern. This phase structure reflects a more sophisticated and sustained operational framework than has been observed in prior Israel-Iran conflict cyber cycles.

Credibility Level	Indicators Present
Confirmed Impact	Independent monitoring confirmation; real-world service reports; sustained outage duration > 1 hour
Medium Credibility	Check-Host with consistent timeout results; multiple nodes showing errors; Cloudflare resource-limit errors
Low Credibility	Single Check-Host link; mixed availability results; HTTP error messages only; no independent validation
Fabricated / Unverified	Check-Host shows normal availability; manipulated screenshots; future timestamps; conflicting evidence

Breach, Data Leakage, and Ransomware Threat Actors

Threat Actor	Alignment / Motivation	Primary Method	Activity Level	Credibility
Handala	Iran-aligned / Pro-Palestinian	Phishing, credential compromise, mobile access, defacement	Very High	Mixed - partial evidence; psychological amplification throughout
Anonymous For Justice	Pro-Palestinian	Destructive data deletion with video evidence	High (daily cadence)	Medium - video evidence adds credibility; volumes unverified forensically
Cyber Isnaad Front	Pro-Iranian	Document drip-release campaign (energy/water)	Medium (10+ installments)	Low-Medium - historical docs; not confirmed current access
ShinyHunters	Financially motivated criminal	Supply-chain, token harvesting, ransom demands	High (single high-impact op)	High - partial Snowflake external corroboration
KillSec	Financially motivated criminal	Ransomware claims, extortion	Medium (2 Israeli claims)	Low - consistent non-delivery pattern; 24-year deadline anomaly

Recommendation:

Full threat actor cards, including associated IOCs, are available via he Check Point Platform.





COLLABORATIONS OBSERVED BETWEEN GROUPS

Overview

Inter-group collaboration during the Feb-April Israel-Iran war was more visible than in the June 2025 conflict, enabled by the longer operational window and Telegram's role as a coordination and recruitment hub. Collaboration manifested in three forms: ideological alignment under the shared #OpIsrael and "Great Epic Battle" frameworks; explicit alliance announcements; and operational amplification where one actor's claims were republished across affiliated channels.

Documented Collaborations

- Cyber Islamic Resistance and Cyb3r Drag0nz (Kurdish hacktivist): Explicit alliance referenced in defacement content on March 2, signaling cohesion under a wider anti-Israel cyber front and growing cooperation between Cyb3r Drag0nz and pro-Iranian ecosystems.

- NoName057(16) and Cyber Islamic Resistance: Coordinated targeting of defense sector infrastructure and municipal platforms observed across multiple reporting windows - parallel operations against the same targets suggesting implicit if not explicit coordination.

- C.E. Army ecosystem and affiliated clusters: C.E. Army functioned as a hub actor with affiliated groups amplifying campaigns and sharing targeting lists across Telegram channels under the "Great Epic Battle" campaign branding.

- Pro-Russian and pro-Palestinian convergence: NoName057(16), RuskiNet, and Cardinal operated in parallel with pro-Palestinian groups, explicitly declaring solidarity with Iran and framing operations as part of a coordinated anti-Israel campaign.

- Hacktivist recruitment drives: Cyber Islamic Resistance published explicit low-barrier Telegram recruitment calls requiring no technical expertise; RuskiNet published parallel recruitment calls seeking data extraction and DDoS capabilities - both timed to the OpIsrael period.

- Moroccan Black Cyber Army: Announced engagement in OpIsrael campaign framework on March 31, reflecting geographic expansion of the coalition to North Africa.

COMPARATIVE ANALYSIS:
June 2025 Israel-Iran Conflict vs. the Feb-April Israel-Iran war

The Feb-April Israel-Iran war was more than three times the duration of the June 2025 conflict (38 days versus 12), and this difference produced a fundamentally different type of cyber campaign. Whereas the June 2025 conflict was characterized by a single sharp DDoS burst followed by rapid decline, the Feb-April Israel-Iran war exhibited a sustained, rotational structure in which actor groups cycled in and out over multiple weeks. The actor ecosystem more than tripled - from approximately six to eight distinct DDoS groups to more than twenty - reflecting both broader hacktivist mobilization and successful recruitment drives conducted during the inter-operation period.

The threat category mix also expanded significantly. The June 2025 conflict was dominated almost entirely by DDoS; the Feb-April Israel-Iran war added ransomware extortion by criminal actors, a sustained destructive data deletion campaign against civilian companies, and a supply-chain breach with externally corroborated downstream impact. The longer window also revealed a deliberate late-operation pivot toward data-leak narratives and recycled datasets under the OpIsrael 2026 framework - a shift reflecting both the maturation of information warfare as a standalone tactic and the effect of Israeli defensive adaptation reducing the practical impact of sustained DDoS.



Two defensive patterns from the June 2025 conflict were confirmed and reinforced. The Finance and Banking sector's resistance to DDoS impact held across all 38 days, a stronger demonstration of institutionalized geo-IP blocking policy than the shorter prior operation could provide. Conversely, Education and Insurance saw meaningful escalation - sectors that were lightly targeted before. The introduction of FBI infrastructure takedowns against an Iran-aligned actor represents a new law enforcement dimension absent from the June 2025 conflict, though their limited operational effect underscores the resilience of multi-channel hacktivist groups.

Taken together, the two operations trace a clear trajectory: the Israel-Iran cyber conflict is becoming longer, more organizationally sophisticated, and more diverse in both tactics and threat actor composition. Future escalations should be expected to exhibit at minimum comparable complexity.



CONCLUSIONS

The Feb-April Israel-Iran war demonstrated a significant evolution in the Israel-Iran cyber conflict across multiple dimensions. The 38-day duration introduced a three-phase campaign structure that the June 2025 conflict's 12 days could not produce, revealing how sustained geopolitical conflicts generate increasingly sophisticated and diverse cyber threat ecosystems.

The DDoS landscape was the most analytically rich component of the operation. More than 20 distinct actor groups were identified across the 38 days - triple the June 2025 ecosystem - with a clear rotation pattern in Phase II suggesting greater operational coordination than has been previously observed. The confirmed pivot from DDoS to data-driven narratives in Phase III, documented explicitly in daily reports from April 7 and April 12, represents a tactical evolution reflecting both defensive adaptation and the maturation of information warfare as a standalone capability.

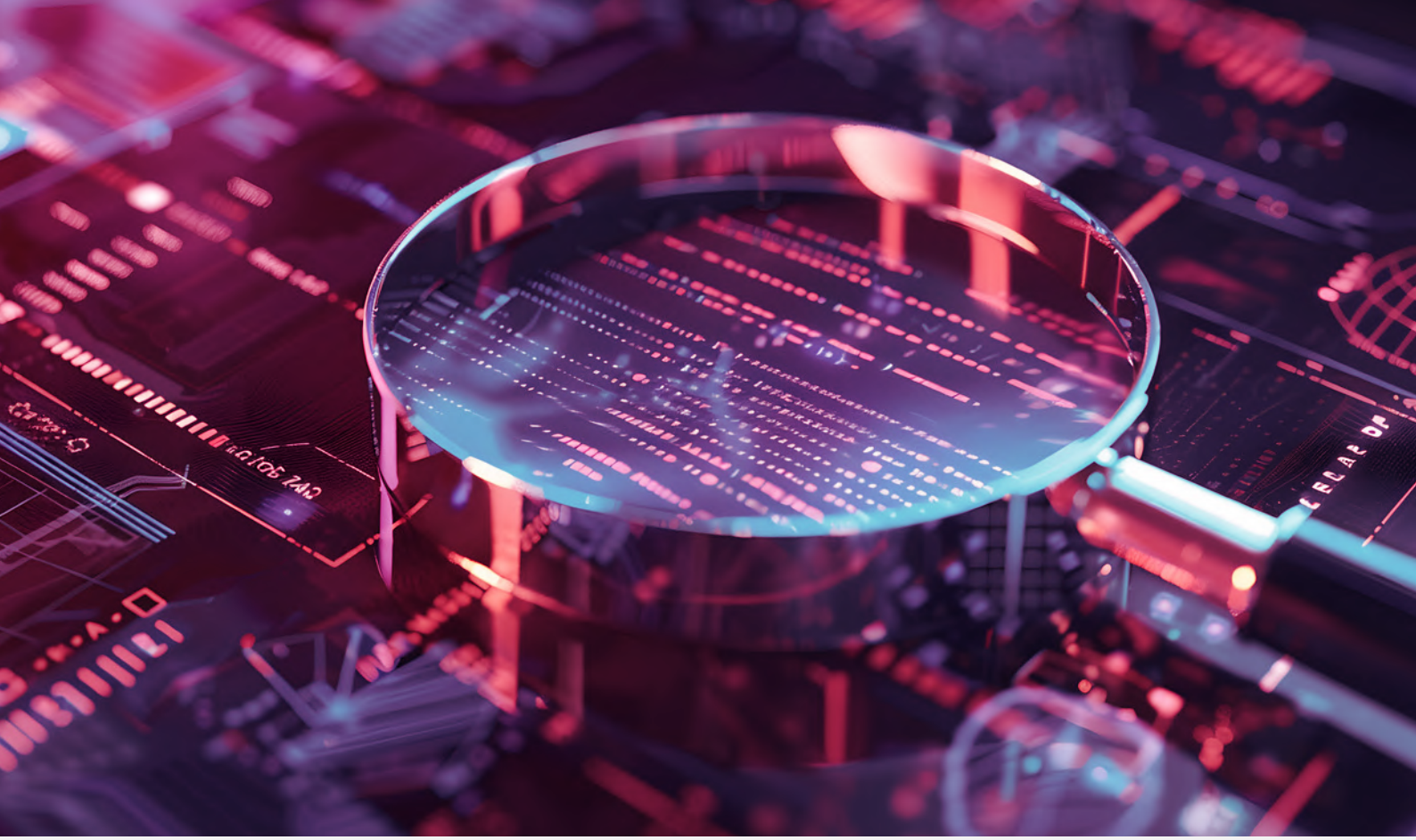
The Finance and Banking sector's second consecutive confirmed resistance to DDoS impact across an even longer operational window is the most clearly positive defensive finding. Geo-IP blocking sustained over 38 days is evidence of effective institutionalized policy, though sustained alertness is required - the absence of confirmed DDoS impact does not indicate reduced adversary intent.

Toward the later stages of the operation, a measurable degradation in threat actor output quality was observed. Multiple groups exhibited signs of operational fatigue, reflected in reduced posting frequency, lower-effort targeting, and an increased reliance on recycled datasets and previously circulated breach material. This shift was accompanied by a rise in fabricated or exaggerated claims lacking technical validation, indicating a temporary decline in capability or prioritization rather than intent.

Looking forward, if hostilities between Israel and Iran resume, threat actor activity is expected to rapidly re-escalate. Unlike the later stages of the current operation, actors will likely return with renewed intensity, leveraging pre-prepared infrastructure, refined targeting lists, and accumulated operational experience. The next phase is assessed to place greater emphasis on psychological and perception-driven operations — including large-scale leak claims, impersonation campaigns, and narrative amplification — rather than consistently achieving verifiable real-world impact. This suggests a continued shift toward influence-oriented cyber activity designed to generate public pressure, erode trust, and create a perception of systemic vulnerability, even in the absence of technically significant breaches.

The Feb-April Israel-Iran war reaffirms that cyberspace is a persistent domain of the Israel-Iran conflict, not a supplementary tactic activated only during kinetic escalations. Future escalations should be expected to exhibit similar or greater complexity, combining overt disruption attempts, covert access operations, and increasingly sophisticated information warfare layers.





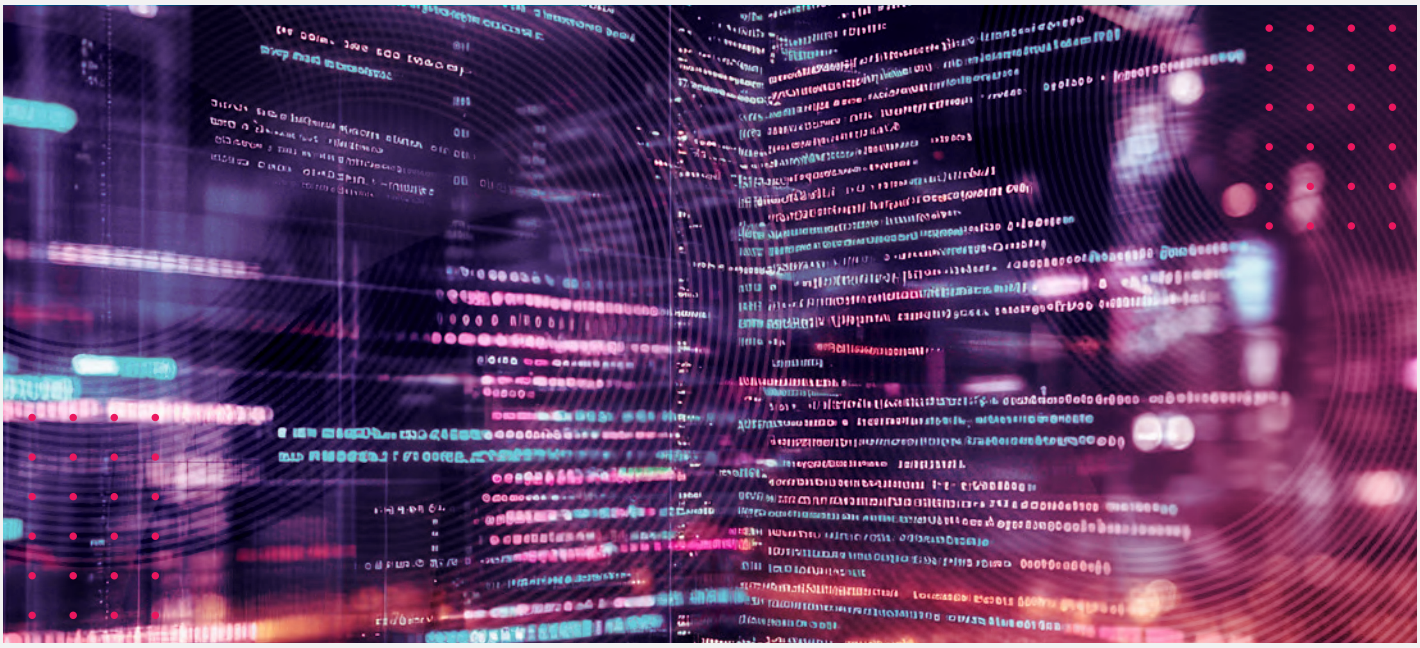
RECOMMENDATIONS

DDoS Protection Recommendations

- Deploy scalable DDoS mitigation solutions capable of sustained 30+ day resilience - not just peak-day spike absorption. She'agat H'ari demonstrated that organizations must plan for weeks of elevated attack volume across three distinct phases, not a single surge.
- Formalize geo-IP blocking as policy with clearly defined criteria for activation, maintenance, and deactivation. The Finance and Banking sector's sustained 38-day geo-IP blocking provides the strongest evidence to date of this measure's effectiveness in the Israel-Iran conflict context.
- Establish network redundancy and automatic DNS failover for all public-facing services. The actor rotation model means disruption windows may open when specific groups re-engage - redundancy ensures continued availability during these windows.
- Implement DDoS claim credibility validation processes. The proliferation of fabricated claims (manipulated screenshots, conflicting Check-Host results, proof amplification) creates analytical noise. Organizations should build rapid triage processes to distinguish genuine DDoS impact from narrative artifacts.
- Develop sustained conflict DDoS incident response plans covering multi-week operational periods, including staff rotation, escalation thresholds for prolonged degradation, and communication protocols for extended disruptions - not just single-event playbooks.
- Anticipate DDoS activity around Jewish calendar milestones, OpIsrael annual period (April), and geopolitical escalation dates - threat actors consistently align operations with these markers.

Breach and Data Leakage Mitigation Recommendations

- Implement Zero Trust Architecture with strict identity verification and lateral movement restrictions. The Iran-linked password spraying campaign targeting cloud identity platforms across hundreds of organizations underscores that identity is the primary attack surface - not perimeter.
- Strengthen MFA enforcement on all internet-facing systems and cloud platforms. The password spraying campaign specifically targeted cloud-based enterprise identity and communication platforms accessible over the internet.
- Establish data leak validation processes to distinguish genuine breaches from recycled datasets and narrative amplification. The OpIsrael 2026 data leak ecosystem showed the majority of claims based on recycled or historical data - invest in the analytical capacity to differentiate quickly.
- Secure internet-facing IoT assets including CCTV systems, which were repeatedly targeted or claimed as compromised across multiple reporting windows throughout the operation.



Ransomware-Specific Recommendations

- Maintain offline and immutable backups for all critical systems, tested regularly. KillSec and Anonymous For Justice both targeted organizations whose data recovery capability may have been limited.
- Segment networks to limit lateral movement and contain ransomware spread. The INC Ransom incident involving a major construction enterprise demonstrates that strategically significant companies remain viable ransomware targets.
- Treat ransomware claims from conflict-opportunistic groups like KillSec with analytical skepticism - validate independently before assuming confirmed breach, given this group's consistent pattern of non-delivery even after ransom deadlines.
- Develop pre-incident ransomware response playbooks including legal, communications, and payment decision frameworks, and establish relationships with national CERTs and law enforcement before an incident occurs.

Supply-Chain and Third-Party Risk Recommendations

- Conduct supply-chain risk assessments for all technology vendors with privileged access to internal systems, cloud environments, or customer data. The ShinyHunters incident demonstrates that one compromised vendor can cascade to multiple downstream organizations.
- Review and restrict third-party integration permissions in cloud platforms - particularly Snowflake and equivalent services - applying least-privilege principles and enforcing token expiration and rotation policies.
- Audit authentication token management practices for all cloud platforms with third-party integrations. Review access logs for unusual activity patterns consistent with harvested token use.

New Recommendations - 2026 Specific

- Invest in data claim validation capabilities enabling accurate rapid assessment during high-volume attack periods. The ability to distinguish genuine exposures from recycled narratives reduces both over-reaction and under-reaction risk in a noisy environment.
- Develop sustained conflict cyber resilience frameworks - moving beyond point-in-time hardening to operational security postures capable of maintaining effectiveness across 30+ day conflict periods, including staff rotation plans and fatigue management.
- Systematically collect and correlate IOCs (domains, IPs, hashes, communication channels) to identify recurring infrastructure and enhance detection, blocking, and threat hunting capabilities.



CONTACT US

ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

PHILIPPINES

Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F,
1-2-8, Toranomon Minato-ku, Tokyo 105-0001

ABOUT CHECK POINT EXPOSURE MANAGEMENT

Check Point's exposure management changes the game.

We combine billions of internal telemetry points with billions of external signals from the open, deep, and dark web to deliver a unified intelligence fabric. This provides clear visibility across the full attack surface, including brand risk.

The industry is moving from fragmented feeds to real context and real priorities. We support that shift through active threat validation, confirmation of compensating controls, and deduplication across tools, so teams can focus on what actually matters.
With safe-by-design remediation, fixes aren't just assigned, they're implemented. Every fix is validated before enforcement, enabling measurable risk reduction without downtime.

Gartner predicts organizations adopting continuous threat exposure management with mobilization will see 50% fewer successful attacks by 2028. We're leading that shift with action, not just tickets, and Fortune 500 organizations across major industries already rely on Check Point Exposure Management.

For more information visit: checkpoint.com/exposure-management

© Check Point, 2026. All Rights Reserved.