

ISRAELI ELECTIONS 2026

They Are Looking for You.

Research report on election-related cyber threats against Israel. Data as of 22 October 2026, five days before election day

UPDATED
22 October 2026

ELECTION DAY
27 October 2026

AUTHORS
Haim Bukra · Naomi Atias



TABLE OF CONTENTS

What is inside.

Research question

What cyber activity is tied to the Israeli election period, and how strong is the evidence?

01	Key findings for citation Six numbers, three quotable lines and one bottom line	03
02	Scope, data and method Sources, evidence grades and limits	04
03	The threat landscape in numbers Incident volumes, types and actors, 12 months	05
04	Who is behind the activity Incidents by camp: Iran-aligned, hacktivist, criminal and others	06
05	Election-linked activity, 4 to 22 October Timeline of observed events and why each is related	07
06	The Handala campaign Countdown, cadence and amplification	08
07	Evidence plates Primary item content from Check Point monitoring	09
08	Claims versus verification What is proven, what is only claimed	12
09	Telegram and dark web trends Weekly and daily activity charts	13
10	Execution versus preparation indicators Rising and falling indicators, with hypothesis	14
11	National response and forecast check Shield of the Elections and what was seen	15
12	State interests and actor types Who may care about the vote and why	16
13	Forecast and scenarios Likelihood, impact and confidence	17
14	Threat actor landscape Five actor types	18
15	Attack methods and timeline Techniques and the three windows	19
16	Analysis and risk assessment Intent, capability and sector exposure	20
17	Recommendations, methodology and indicators What to do and how the numbers were built	21

KEY FINDINGS FOR CITATION

Six numbers, with what each one means

Every figure is shown with its source and its limits.

BOTTOM LINE

The election threat is mainly psychological and influence-driven. Claims outnumber verified compromises, and several recent "leaks" recycle older data.

87

cyber incidents targeting Israel, 1 to 22 October, 66% of them DDoS

Why it is related: DDoS dominates the baseline, as the forecast expects for election day. The pace is not a spike (see page 5).

SOURCE: CHECK POINT CTI REPOSITORY

3

new breach claims in nine days (15 to 22 October), none independently verified

Why it is related: Handala announced a 13-night leak countdown on 14 October and the claims follow that cadence. One of the three is unattributed in the repository.

SOURCE: CHECK POINT CTI REPOSITORY AND INTELLIGENCE DATABASE

6.5M

voter records from a 2020 leak are being re-promoted and re-sold on a hacking forum (4 and 16 October)

Why it is related: Voter data is a ready-made election narrative. Nothing in the posts shows new data.

SOURCE: CHECK POINT FORUM MONITORING

1

explicit DDoS order, with time, IP address and ports, against the campaign site of the Yashar party (16 October)

Why it is related: It is an attack order aimed at a party website two days after the countdown began. No outage was confirmed.

SOURCE: CHECK POINT TELEGRAM MONITORING

-54%

#OpIsrael activity on Telegram since 21 September (Telegram items only)

Why it is related: Visible hacktivist chatter is falling while preparation indicators rise. This may reflect holding capability for the vote, but it is a hypothesis.

SOURCE: CHECK POINT INTELLIGENCE DATABASE

+79%

customer-credential exposures per day at 8 Israeli organizations, September versus April and May

Why it is related: Stolen credentials are the entry point for account takeover and phishing. The rise is not proven to be election-driven.

SOURCE: AGGREGATED ALERT TELEMETRY

QUOTE-READY

Claims are outpacing proof: three breach claims in nine days, and an earlier "leak" of 38,000 soldiers and police officers was recycled 2025 data.

QUOTE-READY

Two of every three cyber incidents recorded against Israel this month are DDoS attacks.

SCOPE, DATA AND METHOD

What was examined and how far it can be trusted

The report asks which cyber activity relates to the Israeli election period (4 to 22 October 2026), how it is changing, and how strong the evidence is for each item.

SOURCE	CONTENT	VOLUME	GRADE
Check Point election monitor	Election-related mentions on Telegram and the dark web, plus brand alerts for the Central Elections Committee	431 alerts, 4 to 22 October. In a sample of 660 items about 92% came from Israeli news channels	A, B
Check Point CTI repository	Incidents tagged country = Israel (OpenCTI), including claimed attacks	87 incidents 1 to 22 October, monthly series for 13 months	B, C
Check Point intelligence database	Telegram channels, forums and paste sites, searched for specific items	Items cited by ID in the evidence plates	A
Aggregated alert telemetry	Alert counts at 8 Israeli organizations in finance, insurance, the public sector, industry and retail	Normalized per day against 13 April to 14 May	A
Leaked-credentials database	Leak events that include credentials of 12 government domains	19.0 per day baseline, 24.3 in September	A

Evidence grades

- ◆ A. Primary item or direct measurement seen in Check Point systems.
- ◆ B. Item relayed by an intermediary channel. The original post was not available.
- ◆ C. Reported claim without primary evidence.
- ◆ D. Historical context.

Status labels used in the report

- VERIFIED confirmed by an official source
- OBSERVED item seen, claim not tested
- CLAIM claim relayed, access not shown
- RECYCLED older data presented as new

Limits and exclusions

- ◆ Counts reflect reported and claimed attacks, not verified impact.
- ◆ Handala's own channel is not ingested, so its posts are known through relays in other channels.
- ◆ About nine in ten election-monitor items are news coverage, so that count measures public attention, not threat activity.
- ◆ Material from other security vendors and election events abroad was not used.

BOTTOM LINE

Direct evidence is limited to a handful of items. Most of the picture rests on claims, which is why every item carries a status label.

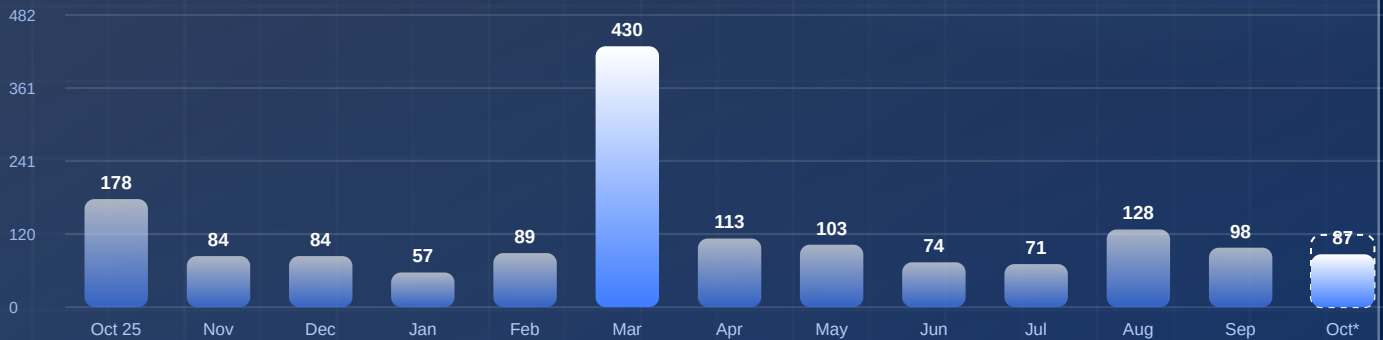
THE THREAT LANDSCAPE IN NUMBERS

Incident volumes, types and actors

Incidents tagged to Israel in the Check Point CTI repository. They are reported and claimed attacks.

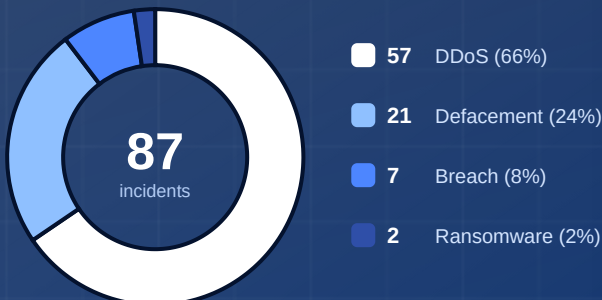
Cyber incidents targeting Israel, by month

OCT PACE 3.95 PER DAY



*October covers 1 to 22 October, with the dashed outline showing the full-month pace (about 119). March 2026 (430) was the Iran-US conflict peak. Per day, October (3.95) is 21% above September (3.27) and in line with August (4.13).

By type, 1 to 22 October



Most active actors, 1 to 22 October



WHY THIS IS RELATED TO THE ELECTIONS

The volumes are not election-specific. They show the environment in which election activity happens: two-thirds of incidents are DDoS and one-quarter are defacements, the two techniques the forecast expects against party, government and results sites. Over 12 months the most active groups were Conquerors Electronic Army (187 DDoS incidents), DieNet (97), Black Ember (90), RipperSec (75), Yemen Cyber Group (68) and NoName057(16) (62).

BOTTOM LINE

October is busy but not abnormal. The risk is a coordinated DDoS wave on a symbolic date, not a new level of baseline activity.

WHO IS BEHIND THE ACTIVITY

Incidents by camp: Iran-aligned, hacktivist, criminal and others

Check Point CTI repository, 1 to 22 October 2026. Camp assignment is an analyst assessment based on actor profiles.

Incidents against Israel by camp, 1 to 22 October (87 incidents)



- Pro-Palestinian and resistance-axis hacktivists: 46 (53%)
- Indonesian hacktivists: 16 (18%)
- Criminal actors: 9 (10%)
- Other DDoS crews: 8 (9%)
- Opportunistic defacers: 8 (9%)

Camp assignment is an analyst assessment based on actor profiles in the Check Point CTI repository. No incidents were tagged to state-linked personas or pro-Russian groups in this window.

CAMP	GROUPS SEEN IN OCTOBER	INCIDENTS	TYPICAL ACTIVITY	WHY IT RELATES TO THE ELECTIONS
Pro-Palestinian and resistance-axis hacktivists	Yemen Cyber Group (34), Cyber Squad 313, which presents itself as Islamic Cyber Resistance in Iraq (11), Qaher (1)	46 (53%)	DDoS against public sites	Symbolic dates draw coordinated DDoS. One group accounts for 39% of all incidents. The Iraq-based group is Iran-aligned (assessment).
Indonesian hacktivists	Trenggalek Cyber Army (13), Cyber Team Indonesia (2), Z-BL4CX-H4T.ID (1)	16 (18%)	Defacement and DDoS	Opportunistic. They join the themes of the day, with low impact.
Criminal actors	Qilin and The Gentlemen (ransomware), Blacknet00, bibimarket, Mr_Raccoonn, jundalnabi, Sumud Cyber Command (2), plus one unattributed breach	9 (10%)	Ransomware, data theft and sale	They use the news cycle to sell data or extort. Not election-specific.
Other DDoS crews	Team1914_official (6), QX-CYBER (1), CyberTroll Team Main (1)	8 (9%)	DDoS	Ideology not established in the repository. Targets include government and media sites.
Opportunistic defacers	coupdegrace (3), chinafans (2), Nolep7, ZhacNocha, mr.anderson (1 each)	8 (9%)	Defacement of small Israeli sites	Low impact, may carry political messages.
Iran state-linked personas (Handala family)	Handala. Copycats Cyber_Handala and handalah_fans were seen in August and September	0 tagged	Hack-and-leak, doxxing, intimidation	The only camp with explicit election messaging. The repository logs incidents, not claims, so Handala's claims are not counted here.
Pro-Russian hacktivists	NoName057(16)	0 (62 in 12 months)	DDoS	No Russian-attributed election activity is confirmed in the sources reviewed.

BOTTOM LINE

Hacktivists are the volume: about eight in ten incidents come from them. The actor with explicit election intent, Handala, appears in the claims, not in the incident counts.

ELECTION-LINKED ACTIVITY

4 to 22 October, with the reason each item is related

4 Oct	Voter-registry database thread bumped on a hacking forum A 2020 voter leak is back in circulation as election day nears.	RECYCLED
5 Oct	TikTok account using the Central Elections Committee's name and logo Impersonating the body that runs the vote.	OBSERVED
9 Oct	List of ten government sites, including the Knesset, posted on Telegram The kind of list that precedes DDoS waves.	OBSERVED
9 Oct	Contact details of senior officials of a national legislature listed on a doxxing site Exposure of officials ahead of the vote.	OBSERVED
14 Oct	Handala announces a 13-night countdown to the elections Explicit election intent from an Iran-linked actor.	OBSERVED
15 Oct	Handala claims a former foreign minister's phone; contacts published First leak claim under the countdown.	CLAIM
15 Oct	Channel posts contact details and credentials of public figures May be compiled from older leaks.	CLAIM
16 Oct	DDoS order against the campaign site of the Yashar party Attack order against a party website.	OBSERVED
16 Oct	Forum user says they paid for the voter database link Recycled data being sold again.	RECYCLED
18 Oct	Claim on an IDF media-monitoring unit device; mostly old or public data Cadence of claims, little new content.	RECYCLED
18 Oct	National Cyber Directorate and Elections Committee announce "Shield of the Elections" Official defensive response.	OFFICIAL
21 Oct	Criminal channel claims "Mossad maps" and thanks Handala for collaboration Criminal and state-linked ecosystems converge.	CLAIM
22 Oct	Claim of breach of an Israeli payment-systems supplier, relayed as Handala's Same campaign window, supply-chain angle.	CLAIM

BOTTOM LINE

Nothing yet shows an election-linked outage. What is visible is intent, target lists and claims, most of them unverified.

THE HANDALA CAMPAIGN

A countdown, a cadence and an echo

Handala announced on 14 October a 13-night leak campaign. Nine nights later the pattern is visible.

Night 9 of 13



Claims since the countdown

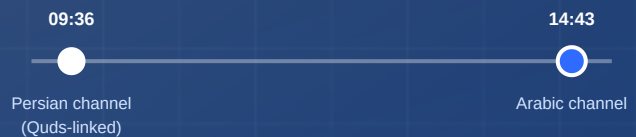


Dark circles are claims relayed without proof. The white circle is the announced intent. The 18 October claim is unattributed in the repository. Handala's own channel is not ingested, so these are known through relays.

What the announcement says

- 1 Intent with a deadline.** The post says the real election begins with Handala in the shadows and that no Israeli official will sleep soundly from that moment.
- 2 "Networks" widens the target set.** Officials, networks and secrets are named as the subject of coming leaks, which signals a claim of access to organizational infrastructure, whether or not real.
- 3 External outlets add reach.** The post says material will be released only through two third-party disclosure outlets, consistent with the loss of some of the group's own sites in 2026.

The echo, 14 October



The same announcement appeared in two languages within five hours.

WHO IS HANDALA

A persona that surfaced in late 2023 and has claimed leaks and destructive attacks against organizations in Israel, Albania and the United States. It is operated by Void Manticore, an actor that Check Point Research links to Iran's Ministry of Intelligence and Security. Karma and Homeland Justice are sister personas.

BOTTOM LINE

Three claims in nine days, none verified. The cadence is the signal: the group intends to keep the election in the headlines until 27 October.

EVIDENCE PLATES I

Attack orders and target lists

Plates reproduce the content of Check Point monitoring items, with the original text and its context.

TELEGRAM · CHANNEL OF H4C

16 OCT 2026 · 13:56 UTC · ITEM 53DCAD44

DDoS order against a political party site

ORDER TIME: 15:30 UTC DATE: 16.OCTOBER.2026

Eliminate: yasharwitheisenkot.com

IP: 138.68.74.28 Port: 80 | 443 | 8080 | 54 | 22 | 9443 | 17

ISP: DigitalOcean, LLC ASN: 14061

"Enough Is Enough, Open Your Eyes! This Is Genocide Not Self Defence."

#FreePalestine #ForJustice

Translation / note: The attached image is an election-themed propaganda poster titled "Israel's Election" (a masked figure, a ballot box, the Knesset and the Palestinian flag).

Why related: the target is the campaign site of a leading party, the order names a time, an address and ports, and the attached poster is election-themed. No outage was confirmed.



IMAGE ATTACHED TO THE ORDER

TELEGRAM · HACKTIVIST CHANNEL

9 OCT 2026 · 05:00 UTC · ITEM 0A627BEE

List of ten government websites

1. Prime Minister's Office 2. Knesset 3. Ministry of Foreign Affairs
4. Ministry of Defense 5. IDF 6. Ministry of Finance
7. Bank of Israel 8. Ministry of Justice (and two more)

Translation / note: Ten official sites, one per line, with no message and no deadline.

Why related: DDoS waves are usually announced in advance on Telegram. This list names the institutions that run and report the election. It is a precursor, not an attack.

From list to outage: what has been seen

STEP 1 · 9 OCT

Target list of ten government sites

OBSERVED



STEP 2 · 16 OCT

Attack order against a party site

OBSERVED



STEP 3

Confirmed outage of an election-related site

NOT OBSERVED

BOTTOM LINE

Two items show preparation to disrupt public election-related websites. Neither shows a successful attack.

EVIDENCE PLATES II

Voter data and an electoral-body imitation

HACKING FORUM · THREAD "ISRAELI ELECTION VOTERS 2020 DATABASE LEAKED"

14 JUN, 4 OCT, 16 OCT 2026 · ITEMS 366D871B, 70B6F37C, F06DA05A

Voter database thread resurfaces

14 Jun 2026 (cold_runner71): "Thx, will mirror"**4 Oct 2026** (DFGHJ): quotes the original post of 28 Jun 2024 and the description of the February 2020 leak: personal data of every voter in Israel, about 6.5 million records**16 Oct 2026** (malhojjg6): "where is the link i paid"**Translation / note:** The thread dates from June 2024 and the data from February 2020. The October replies bump it back to the top.**Why related:** voter data is the classic election leak. Three replies in four months, the latest after payment, show the material is circulating again. Nothing shows new data.

Life of a voter database

Feb 2020

Original leak
6.5M records

Jun 2024

Forum thread
posted

14 Jun 2026

Reply:
"will mirror"

4 Oct 2026

Bumped with
the 2020 summary

16 Oct 2026

Reply: "I paid"
for the link

TIKTOK · ACCOUNT @ELECTIONKNESSET

5 OCT 2026 · ALERT SEVERITY HIGH · STATUS OPEN

Account imitating the Central Elections Committee

Display name: Central Elections Committee for the Knesset (in Hebrew)

Followers: 3,084 Following: 0

Logo match with the Committee's profile image: 0.996

Translation / note: Detected by Check Point brand monitoring for the Committee. The account has not been confirmed as unofficial. The profile image is not reproduced.**Why related:** an account using the electoral body's name and logo can publish false results or instructions. It is the impersonation scenario in the forecast, observed in practice.

BOTTOM LINE

Two direct election items: recycled voter data being resold, and a high-severity account imitating the body that runs the vote.

EVIDENCE PLATES III

Relays and convergence around the Handala campaign



Countdown Begins: Israel's Election under Handala's Shadow—13 Nights of Zionist Nightmare!

Only 13 days remain until the so-called "Great Day of Democracy" in the Zionist regime, a day that is nothing but a celebration of lies.

From now on, the real election begins with Handala in the shadows!

Rest assured, from this moment, not a single Zionist official will sleep soundly.

Due to certain restrictions, all leaks, disclosures, and exposures of officials, networks, and Zionist secrets will be released exclusively through:

Distributed Denial of Secrets
Drop Site News Agency

THE ANNOUNCEMENT ITSELF: HANDALA
POSTER, 14 OCT 2026

TELEGRAM · ARABIC CHANNEL

14 OCT 2026 · 14:43 UTC · ITEM 8C35070B

Handala countdown relayed in Arabic

أعلنت مجموعة «حنظلة» الهكرية عن تكثيف نشاطها مع اقتراب موعد الانتخابات الإسرائيلية

Translation / note: The Handala hacking group announced it is intensifying its activity as the Israeli election date approaches.

Why related: explicit election framing, repeated in Persian (09:36) the same day.

TELEGRAM · ARABIC CHANNEL

22 OCT 2026 · 09:51 UTC · ITEM 30CA9DBB

Claimed breach of an Israeli payment-systems supplier (name withheld)

حنظلة تكشف معلومات مالية تخص مليوني إسرائيلي — عبر اختراقها شركة [name withheld]

Translation / note: Handala reveals financial information on two million Israelis by breaching a supplier of point-of-sale systems. The company name is withheld.

Why related: same campaign window and the same channels that relayed the countdown. Indirect link, claim only.

TELEGRAM · "INTERNATIONAL GLOBAL NETWORK (SLSH)"

21 OCT 2026 · 23:07 UTC · ITEMS 6240376D, 6832B0A0

Criminal channel claims "Mossad maps" and thanks Handala

we send yu maps that you will not find anywhere else in the world. These maps were leaked from the Mossad Israel ... The secret places of the Iron Dome ... total database: 4.2 TB ... We thank Handala for collaborating with us
Attached: a 23 MB PDF named as an environmental impact assessment for a power-station expansion, and sample.json (238 KB)

Why related: shows a financially motivated channel aligning itself with the state-linked campaign in election week. The only sample looks like a planning file, so the claim looks inflated.

BOTTOM LINE

The campaign is reaching beyond Handala's own channel, but the proof offered so far is thin.

CLAIMS VERSUS VERIFICATION

What is proven and what is only claimed

Each item is graded by what the evidence shows and by how it relates to the elections.

ITEM	WHAT WAS SEEN	STATUS	LINK	WHY IT MATTERS
Handala countdown and nightly leaks	Relays in 2 languages	OBSERVED	Direct	Explicit election framing.
Former foreign minister's phone	Claim; archive circulates 3 days later	CLAIM	Direct	Leak under the countdown. Content not verified.
Politicians' contacts and credentials	Channel post	CLAIM	Direct	May be compiled from older leaks.
IDF media-monitoring unit data	Claim; mostly old or public data	RECYCLED	Indirect	Shows cadence, little new content.
38,000 soldiers and police officers	Shown to be 2025 data	RECYCLED	Indirect	Recycling on a symbolic date.
Payment-systems supplier breach	Claim; company silent	CLAIM	Indirect	Same campaign window; supply-chain risk.
"Mossad maps", 4.2 TB	Claim; sample looks like a planning file	CLAIM	Indirect	Criminal and state-linked convergence.
2020 voter database for sale	Thread from 2024, bumped; payment reply	RECYCLED	Direct	Old data, new attention.
DDoS order against a party site	Order text; no outage seen	OBSERVED	Direct	Attack preparation.
Account imitating the Elections Committee	Name and logo match; open	OBSERVED	Direct	Impersonation of the electoral body.

0 of 10

items independently verified as a compromise of an election-related or parliamentary system.

3 of 10

items shown to be recycled or mostly old data.

BOTTOM LINE

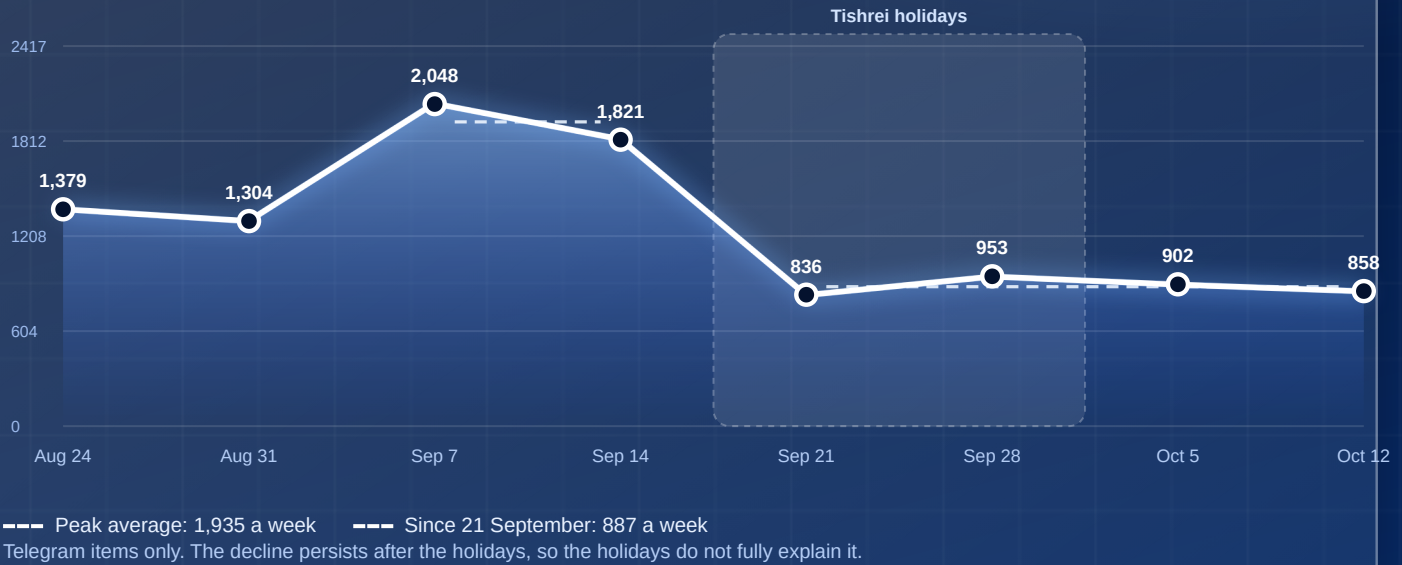
Intent is clear and public. Capability is not demonstrated. The responsible reading is to prepare for the effect of publication, not to treat each claim as a confirmed breach.

TELEGRAM AND DARK WEB TRENDS

Hacktivist chatter is falling; election talk is rising

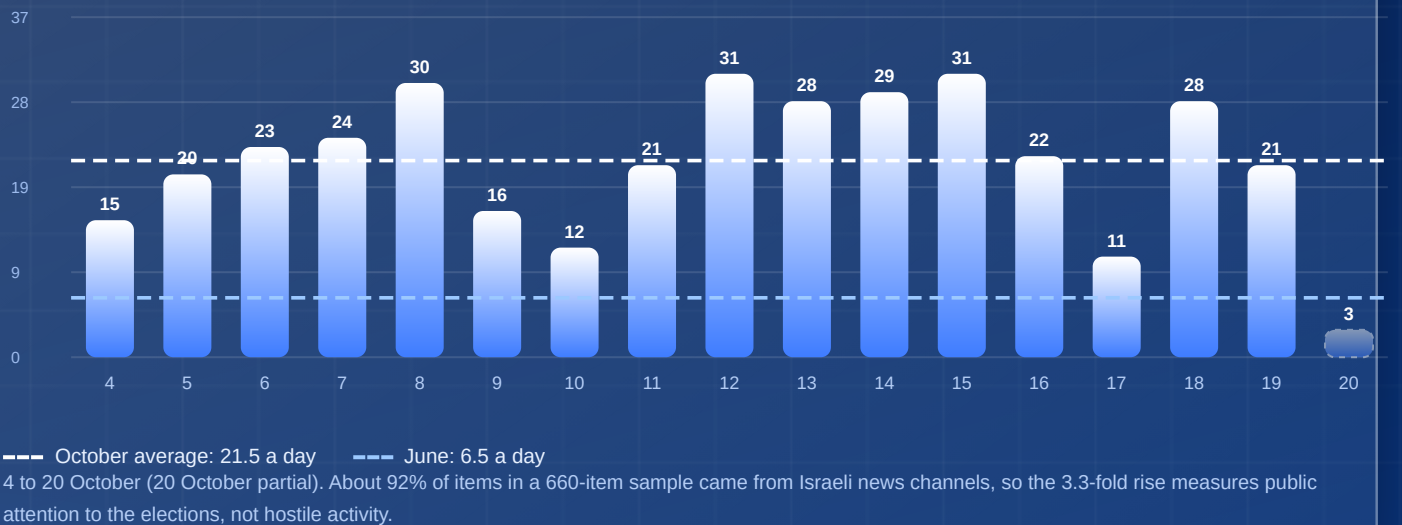
#OpIsrael mentions on Telegram, by week

DOWN 54% SINCE 21 SEPTEMBER



Election-related mentions by day, election monitor

365 IN 17 DAYS



BOTTOM LINE

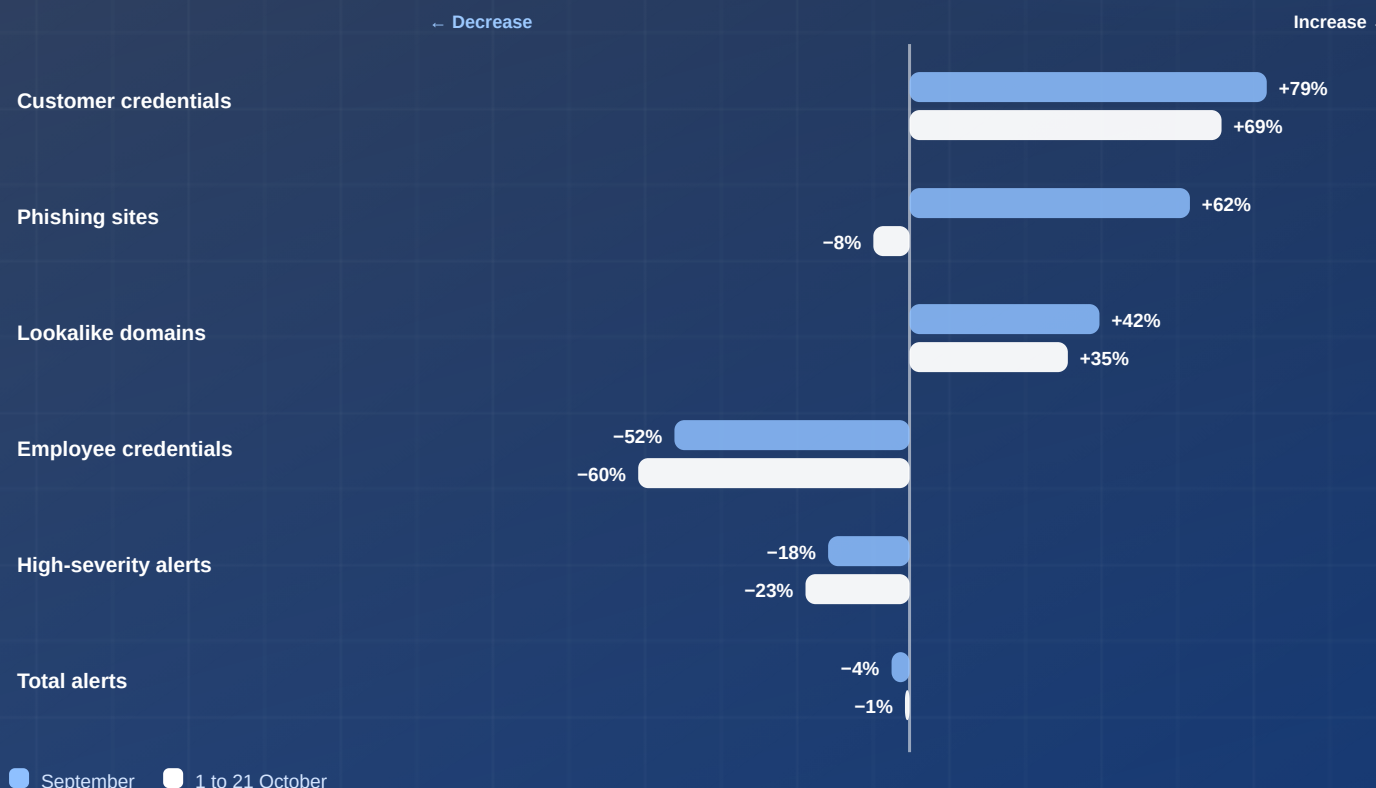
Public attention to the elections is up 3.3 times. Visible hacktivist activity on Telegram is down 54%. The first is the news cycle, the second is the signal to watch.

EXECUTION VERSUS PREPARATION INDICATORS

What is rising, what is falling, and why it is related

Change per day across 8 Israeli organizations, versus 13 April to 14 May.

Change per day, by indicator



Why each indicator is related

Customer credentials: Stolen logins feed account takeover and phishing, the techniques used against officials and official accounts.

Phishing and lookalike domains: Election-themed lures and brand imitation cluster around votes.

Employee credentials and high-severity alerts: Fewer detected intrusions at the organizations measured.

#OpIsrael on Telegram: The visible hacktivist layer.

Hypothesis: the calm before the storm?

When preparation indicators rise and execution indicators fall, one possibility is that attackers are building access and waiting for the moment of greatest impact.

This is an analyst hypothesis. Alternatives include the Tishrei holidays, the size of the sample and detection settings.

BOTTOM LINE

Credential exposure and phishing are up, detected intrusions are down. The data does not prove a link to the elections.

NATIONAL RESPONSE AND FORECAST CHECK

The official answer, and the forecast against what was seen

SHIELD OF THE ELECTIONS

On 18 October the National Cyber Directorate and the Central Elections Committee announced a joint operation against disruption, impersonation, phishing and takeover attempts on election systems. Voting in Israel is on paper, so the operation protects the digital layer around it. The public is asked to close any defaced site and to report it to the national cyber line, 119.

Forecast against what was seen

FORECAST	LIKELIHOOD	WHAT WE HAVE SEEN SO FAR
Leaks about officials	High	A claim against a former foreign minister (15 Oct) and a politician-credentials post (15 Oct). None verified.
DDoS on public websites	High	A target list (9 Oct) and a DDoS order against a party site (16 Oct). No election-linked DDoS wave confirmed in the sources reviewed.
Account impersonation	Medium	A TikTok account using the Elections Committee's name and logo (5 Oct), open for validation.
False or manipulated content	Medium	No confirmed case in the sources reviewed.
Destructive attack	Low	No related claim. The March 2026 Handala record remains the reference.

Left out, and why

- ◆ Foreign election events and reports by other vendors.
- ◆ Incident counts without an election link, except where they explain the baseline.
- ◆ Client-specific alert details.

Read with care

Groups recycle older data around symbolic dates. The material is public. The proof is not.

BOTTOM LINE

The first forecast signals have appeared: leak claims and attack preparation. A confirmed election-day outage has not.

STATE INTERESTS AND ACTOR TYPES

Who may care about the vote, and what has been seen

Interest is not capability. Attribution reflects public reporting and Check Point Research, and is an assessment.

COUNTRY	INTEREST	ASSOCIATED GROUPS	SEEN IN THIS PERIOD	LIKELIHOOD
Iran	Political and psychological pressure, and a chance to show reach on a symbolic date.	Void Manticore, which runs the Handala, Karma and Homeland Justice personas (hack-and-leak, wipers), and Scarred Manticore (espionage and access). Both are tracked by Check Point Research and linked to Iran's Ministry of Intelligence and Security.	Handala countdown and three leak claims, 14 to 22 October.	High
Russia	Shaping public opinion, deepening divisions and weakening trust in institutions. An election period is a natural moment.	State-linked influence networks and pro-Russian hacktivist collectives, mainly DDoS.	No Russian-attributed election activity confirmed in the sources reviewed.	Medium
Hacktivist collectives	Visibility and ideology. Election day is a symbolic target, and some personas front for state operators.	Pro-Iran and pro-Palestinian collectives, pro-Russian collectives and opportunistic DDoS crews.	A government-site target list (9 Oct), a DDoS order against a party site (16 Oct), and 34 DDoS incidents by one group in October.	High

How to read this page

- ◆ Interest is not capability.
- ◆ A hacktivist brand does not rule out a state operator.
- ◆ Treat any persona's claim as intent to verify, not proof of access.

Reading the landscape

Many actors, different motives, one date. The most active actor in the October window (34 incidents) is a DDoS group, while the most election-specific actor is a state-linked leak persona.

BOTTOM LINE

Iran is the actor with an explicit election campaign. Russia is a risk with no confirmed election activity yet. Hacktivists are the volume.

FORECAST AND SCENARIOS

Likelihood against impact, until election day



FORECAST	LIKELIHOOD	CONFIDENCE	WHAT IT LOOKS LIKE
DDoS attacks on public websites	High	80	Short, high-volume waves, usually announced on Telegram.
Leaks about Members of Knesset and public officials	High	80	Contact details, internal documents and personal data. First leaks observed.
Disruption or takedown of government and municipal websites	Medium	60	Outages or defacement, with the highest risk on election day.
Takeover of official social media accounts	Medium	60	Session theft or phishing, used to spread false messages.
False or manipulated content	Medium	60	Fake accounts, fabricated leaks, false results and AI-generated media.
Sale of access and extortion	Medium	60	Use of the noise to sell access or extort.
Destructive attack	Low	60	Wiper malware against higher-value targets.

BOTTOM LINE

Most scenarios need no advanced capability. They depend on exposed services, weak authentication and public attention.

THREAT ACTORS

Five kinds of actor, one shared deadline.

Five types of actor are expected to be active around the elections, and Handala is only one of them. They differ in motivation, capability and in how far their public claims can be trusted.

ACTOR TYPE	MOTIVATION	TYPICAL ACTIVITY	EXPECTED ELECTION-PERIOD OUTPUT	RELIABILITY OF CLAIMS
State-linked influence persona (Handala)	Political and psychological impact on Israel, in line with Iranian state interests	Phishing, account takeover, hack-and-leak, doxxing, wiper malware	Leaks about officials and organizations, claims of penetration, possible disruptive attack	Medium
Pro-Iran and pro-Palestinian hacktivists	Ideology and visibility	DDoS, defacement, unverified leak claims	DDoS waves against government, health, finance and media sites around the vote	Low to Medium
Pro-Russian and other opportunistic hacktivists	Visibility and alignment against shared adversaries	Mainly DDoS	Participation in coordinated campaigns timed to symbolic dates	Low to Medium
Cybercriminals and access brokers	Financial gain	Sale of access and data, ransomware, extortion	Use of the surrounding noise to sell access or extort	Medium
Foreign influence networks	Shaping narratives and eroding trust	Fake accounts posing as Israelis, AI-generated content	Deepfakes, false results and manufactured leaks, peaking close to election day	Medium

Handala as an example

The actor most likely to act on the election announcement. The group appeared in late 2023 and is operated by Void Manticore, which Check Point Research links to Iran's Ministry of Intelligence and Security. Its activity includes phishing and impersonation, theft and leaking of data, doxxing of government and security personnel, and wiper malware aimed at Windows and Linux systems.

In March 2026 it claimed a destructive attack on a US medical technology company carried out through a cloud device-management platform, which showed a willingness and capability to move from leaking to destroying. The group is known to describe its access in the strongest possible terms, which is why claims are graded in this report.

Claims versus capability

Read the intent literally. Verify the capability.

ATTACK METHODS AND TIMELINE

Simple methods, aimed at a symbolic date.

METHOD	HOW IT APPEARS	TYPICAL TARGETS	MITRE ATT&CK
Denial of service (DDoS)	Short, high-volume floods against public websites and portals, usually announced on Telegram	Government, municipal, healthcare, finance, media	T1498, T1499
Website defacement or takedown	Replacement of page content with political messaging, or taking public sites offline	Weakly protected public sites, local authorities	T1491
Account takeover	Session theft, phishing and reuse of leaked credentials against social media and messaging accounts	Official channels, senior staff	T1539, T1566, T1078
Hack-and-leak and doxing	Publication of internal documents, contact lists and personal data, including on Members of Knesset and public officials	Officials, employees, vendors	T1567
Exposed services	Use of internet-facing RDP, SMB and unpatched web services to gain access	Any organization with exposed remote access	T1133, T1021.001, T1190
Destructive attacks	Wiper malware and abuse of device-management tools	Higher-value organizations	T1485, T1561
Impersonation and deepfakes	Fake accounts, spoofed executives, false results, manipulated audio or video	Public-facing brands and executives	T1656

Three windows

NOW TO OCTOBER 26

Before election day

Reconnaissance and phishing, preparation of fake accounts and lookalike domains, and a steady flow of announced leaks designed to build anticipation.

OCTOBER 27

Election day

Highest risk of visible disruption: DDoS against public services, defacement, and false or manipulated content about turnout or results, including AI-generated audio and video.

OCTOBER 28 ONWARD

After election day

Material taken earlier is often published weeks after the operation. Expect leaks, claims of earlier access and follow-up campaigns.

3.5 days

The average gap between new breach claims since the countdown began (15, 18 and 22 October). The cadence shows how a campaign can keep an election in the headlines without a single verified compromise.

ANALYSIS & RISK ASSESSMENT

Read the intent literally. Verify the capability.

- Q1 Why does this concern organizations that are not political?** Previous hacktivist waves hit government portals, healthcare providers, manufacturers and online commerce sites alike, because the aim is visibility rather than a specific victim. Organizations are also routes to others, through shared vendors, shared infrastructure and employees whose data can be leaked.
- Q2 How should the claims be read?** Intent should be taken seriously and capability should be verified. A publication achieves its purpose when it draws public attention, so organizations should prepare for the reputational effect as well as the technical one.
- Q3 What is realistic on election day?** DDoS is highly likely, together with defacement or takedown of public websites, account takeover and fabricated content. A destructive attack is less likely but cannot be excluded, given Handala's March 2026 record.
- Q4 What is being monitored?** Check Point's Exposure Management department monitors Telegram channels, underground forums and social media for election-related statements, calls to action and target lists. The Handala statement is the most prominent election-specific declaration identified so far, and leaks about Members of Knesset have begun to appear.

Risk by sector

The overall risk to Israeli organizations during the election period is assessed as High, with a confidence of 80.

SECTOR	MOST LIKELY SCENARIO	LIKELIHOOD	IMPACT	CONFIDENCE
Government and municipalities	DDoS, takedown or defacement of websites, and leaks about officials including Members of Knesset	High	High	80
Healthcare	Leak of employee or patient data and DDoS against public portals	Medium	Very high	60
Financial services	DDoS and phishing or impersonation of the brand and executives	High	Medium	70
Telecom and critical infrastructure	DDoS, service disruption and claims of network access	Medium	High	60
Technology and service providers	Compromise used as a route to customers, and leaks of customer data	Medium	High	60

This assessment reflects the information available to Check Point's Exposure Management department at the time of this review. It does not constitute a guarantee that any specific organization will or will not be targeted, or confirmation of any organization's exposure, which only the organization can verify directly. Final determination, and any decisions taken as a result, remain the responsibility of each organization.

Bottom line

High risk, confidence 80. The preparation has already begun.

RECOMMENDATIONS

What to do, and when.

IMMEDIATELY, IN THE COMING DAYS

- ☐ **Remove remote access and file-sharing services from direct internet exposure.** Services such as RDP (3389), SMB (445) and RPC (135) should be reachable only through a VPN, zero-trust gateway or bastion host with multi-factor authentication, and network-level authentication should be enabled.
- ☐ **Enforce phishing-resistant multi-factor authentication on administrative accounts and official social media accounts.** Hardware security keys or passkeys should replace SMS and app-based codes where possible, and active sessions on messaging and social media accounts should be reviewed and ended if unrecognized.
- ☐ **Confirm that DDoS protection is active and tested.** Always-on protection, rate limiting and a web application firewall should cover public websites, origin servers should sit behind the protection layer, and a direct contact at the provider should be confirmed.
- ☐ **Publish a list of official communication channels and verify that official accounts are secured.** A single page listing official domains and social media accounts helps the public and the media tell real from fake, and speeds up takedown requests.
- ☐ **Agree an escalation channel that works independently of normal infrastructure.** Out-of-band contact details and a named decision-maker for election day should be agreed in advance.

BEFORE ELECTION DAY

- ☐ **Enforce DMARC at a reject policy together with SPF and DKIM.** This reduces the use of spoofed sender addresses in election-themed phishing and in executive impersonation.
- ☐ **Act quickly on lookalike domains, fake social media profiles and spoofed executive accounts.** Check Point's Exposure Management department monitors for these on behalf of customers, and organizations are recommended to pre-approve takedown actions so that response is not delayed.
- ☐ **Add CAA records and DNSSEC, and lock the domain at the registrar.** These steps reduce the risk of fraudulent certificate issuance and DNS hijacking, which are used to redirect users to fake sites.
- ☐ **Review the exposure of employee and executive data.** Credentials found in recent leaks should be reset, unnecessary personal information should be removed from public pages, and senior staff should be briefed on doxxing and impersonation risk.
- ☐ **Harden public websites against defacement and disruption.** Public information should be served from static or read-only content where possible, file integrity monitoring should be deployed, and an offline copy of key pages should be ready for fast restoration.
- ☐ **Review third-party and supply chain access.** Vendors with remote access or hosting responsibilities should be asked to confirm DDoS readiness, contact details and incident procedures for the election period.
- ☐ **Prepare a procedure for suspicious executive requests and false media content.** Requests that arrive by voice or video should be verified through a second channel, and a short pre-approved statement should be ready in case false content about the organization appears.

One week left

The first five actions close most of the exposure.

APPENDIX AND METHODOLOGY

Recommendations continued, indicators, and how the statistics were calculated

DURING THE ELECTION PERIOD

- ☐ **Increase security monitoring and freeze non-essential changes.** Extended SOC coverage, a change freeze on production systems and a tested incident response plan reduce both the likelihood and the duration of disruption.
- ☐ **Maintain isolated backups and a tested recovery plan.** Destructive attacks target backups as well, so recovery copies should be kept apart from the production network and restoration should be rehearsed.

AFTER ELECTION DAY

- ☐ **Continue to watch for leaks and refresh exposed credentials for several weeks.** Check Point's Exposure Management department will continue to monitor for mentions of customer assets and will report findings through the platform.

Methodology and notes on the statistics

- ◆ **Sources:** the Check Point election monitor (dark web and Telegram), the Check Point intelligence database, the Check Point CTI repository (incidents tagged to Israel), aggregated alert telemetry from 8 Israeli organizations in finance, insurance, the public sector, industry and retail, and the Check Point leaked-credentials database (12 government domains).
- ◆ **Periods:** 13 April to 14 May (baseline, 32 days), September (30 or 31 days, depending on the indicator), and 1 to 21 October (21 days). All values are normalized per day.
- ◆ **The election monitor** ran from 10 to 30 June and from 4 October. Its comparison is to June.
- ◆ **Mention counts** for Handala include several kinds of source. For #OplIsrael the sampled items were Telegram only.
- ◆ **No causal link to the elections is proven.** The Tishrei holidays (September to early October) affect activity. "Calm before the storm" is an analyst hypothesis.

Appendix: indicators of compromise, for detection and hunting

The indicators were drawn from Check Point Research's March 2026 analysis of Handala activity. Infrastructure indicators should be reviewed before blocking, and the absence of a match does not mean the absence of activity.

TYPE	INDICATOR	CONTEXT
IP address	107.189.19.52	Infrastructure linked to Handala activity
IP address	146.185.219.235	Infrastructure linked to Handala activity
IP address	31.57.35.223	Infrastructure linked to Handala activity
IP address	82.25.35.25	Infrastructure linked to Handala activity
SHA-256	08b80ab6a6c4eca08e18096c9468fe0bd2e33fc23142730e59177e6fcd7c902d	File linked to Handala activity
SHA-256	1ab1586975779b7d1ce09315b1312b939a194de6df7c5e92aea4f963835f7b08	File linked to Handala activity
SHA-256	d969ff9fe6099db8f6ef3977a849b1757aa221669387eb29a2c6c0ce4b4abe70	File linked to Handala activity

27.10.2026

They announced it. Close the gaps before they arrive.

Check Point's Exposure Management department continues to monitor the election-related threat landscape and will notify customers through the platform if specific targeting of their assets is identified.

Confidential · Check Point copyright © all rights reserved 2026

