ZEROFOX INTELLIGENCE

| Flash |

U.S. Military Strikes on Iran – Cyber SITREP #2: March 6, 2026

F-2026-03-06c

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Geopolitics, Hacktivism, Cyberattacks

March 6, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 11:00 AM (EST) on March 6, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | U.S. Military Strikes on Iran – Cyber SITREP #2: March 6, 2026

| Key Findings

- U.S. and EU federal agencies have issued additional warnings that Iran-aligned cyber threat actors are very likely to target Western critical and digital infrastructure in retaliation for the ongoing U.S.-led attacks in Iran.

- Pro-Palestinian threat collective and extortionist group “Handala Hack Team” and pro-Russian threat actor “NoName057(16)” have thus far been among the most prominent threat collectives active during the Iran conflict.

- ZeroFox has observed an abundance of likely illegitimate cyberattack and leak claims this week. Less-established threat actors are likely to use geopolitical events to gain inflated prominence by exaggerating or misrepresenting the severity and scale of their cyber-based operations or to propagate political messaging and/or fearmongering.

- Between February 26 and March 5, ZeroFox observed at least 287 separate regional and industry-wide cyber incidents that included ransomware attacks, Initial Access Broker (IAB) sales, and vulnerabilities/exploits—a likely steadying volume in cyber incidents day-to-day as the conflict continues.

Latest Details

Further Warnings of Potential Cyberattacks

ZeroFox has observed continued, coordinated cyber operations targeting government infrastructure and private-sector entities across the Middle East, predominantly targeting Israel. Several government institutions have issued warnings regarding the increased threat of cyberattacks in response to the Iran conflict.

- Europol warned that the Middle East conflict will have immediate security repercussions for the European Union, with heightened risks of terrorism, organized crime, violent extremism, cyberattacks, and AI-enabled fraud.[1] Iran-linked groups are likely to pursue destabilizing activities that include intimidation campaigns, terrorist financing, and cybercrime.

- On March 5, Kuwait's National Cybersecurity Center said that it had detected and immediately addressed several cyber activities and threats targeting digital systems in the country, without impacting the continuity of services or critical digital infrastructure.[2]

- U.S. federal agencies, including the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS), remain on heightened alert while monitoring potential lone-actor threats and cyber activity.[3] If the Iran conflict persists for the next few weeks, there is a roughly even chance that U.S. entities—especially those directly involved in U.S. military efforts—will be targets in politically motivated lone-wolf cyberattacks, social engineering campaigns to obtain credentials and sensitive information, access for espionage, and data breaches.

[1] hXXps://www.reuters[.]com/world/europol-warns-iran-crisis-raises-threat-terror-extremism-cyberattacks-2026-03-05/

[2] hXXps://x[.]com/ncsckw/status/2029598743142556109?s=20

[3] hXXps://www.theguardian[.]com/world/2026/mar/06/security-increase-iran-attack-us-israel-bombing

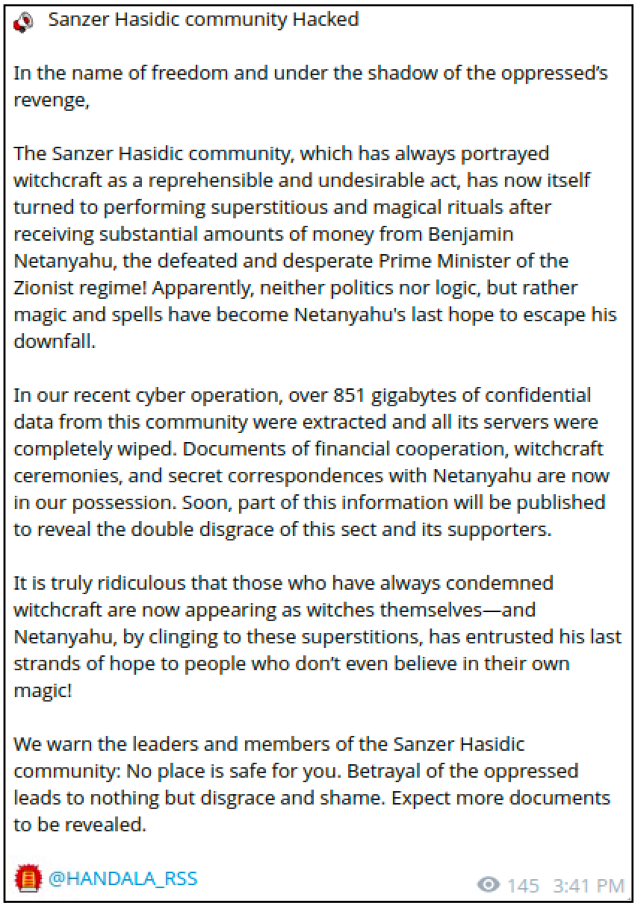
Prominent Collectives

Pro-Palestinian (and pro-Iran-aligned) threat collective and extortionist group Handala Hack Team and pro-Russian threat actor NoName057(16) have thus far been among the most prominent threat collectives active during the Iran conflict. Both collectives have a well-established history of politically and ideologically motivated cyberattacks—largely against Western institutions and perceived political allies.

These collectives have made an abundance of claims, announcements, and alleged leaks/breaches directly related to Israeli-American military actions in Iran, almost certainly driven by political/ideological stances regarding the region. This activity is very likely aimed at spreading ideological messaging, advancing Iranian-backed military efforts, and degrading U.S. and Israeli capabilities or otherwise harming military service members, critical infrastructure, and sensitive national security defenses.

Handala Hack Team

Handala Hack Team claimed to have exfiltrated 851 GB of data from the orthodox Jewish Sanzer Hasidic community, wiping its servers and obtaining documents allegedly detailing financial ties and correspondence with Israeli Prime Minister Benjamin Netanyahu. The collective has stated that portions of the data will be publicly released and released a video of one of its alleged operators seemingly accessing the files Handala Hack Team claims to have exfiltrated. These claims are likely exaggerated; however, if they are legitimate, the leaked files are likely to reveal sensitive information that can be used in further politically motivated cyberattacks, such as extortion or blackmail.



Sanzer Hasidic community Hacked

In the name of freedom and under the shadow of the oppressed's revenge,

The Sanzer Hasidic community, which has always portrayed witchcraft as a reprehensible and undesirable act, has now itself turned to performing superstitious and magical rituals after receiving substantial amounts of money from Benjamin Netanyahu, the defeated and desperate Prime Minister of the Zionist regime! Apparently, neither politics nor logic, but rather magic and spells have become Netanyahu's last hope to escape his downfall.

In our recent cyber operation, over 851 gigabytes of confidential data from this community were extracted and all its servers were completely wiped. Documents of financial cooperation, witchcraft ceremonies, and secret correspondences with Netanyahu are now in our possession. Soon, part of this information will be published to reveal the double disgrace of this sect and its supporters.

It is truly ridiculous that those who have always condemned witchcraft are now appearing as witches themselves—and Netanyahu, by clinging to these superstitions, has entrusted his last strands of hope to people who don't even believe in their own magic!

We warn the leaders and members of the Sanzer Hasidic community: No place is safe for you. Betrayal of the oppressed leads to nothing but disgrace and shame. Expect more documents to be revealed.

@HANDALA_RSS

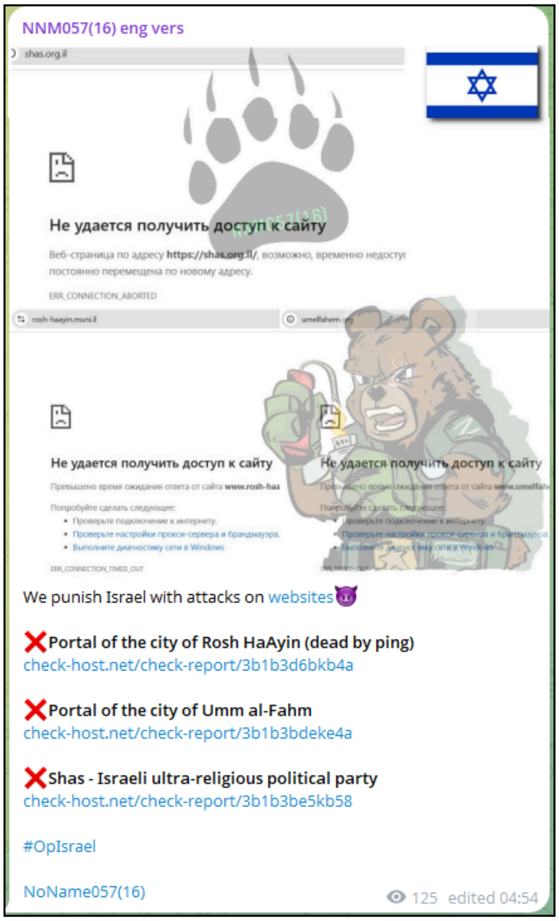
145 3:41 PM

Handala Hack Team's Telegram post

Source: ZeroFox Intelligence

NoName057(16)

Pro-Russian threat actor NoName057(16) announced on its English-language Telegram channel that it has conducted distributed denial-of-service (DDoS) attacks against the websites of the Israeli cities of Rosh HaAyin and Umm al-Fahm, as well as the Israeli political party Shas, an ultra-Orthodox conservative constituency in Israel. The activity is a part of the group's cyber campaign against Israel and the United States in retaliation for the current Iran conflict.



NNM057(16) eng vers

Не удается получить доступ к сайту

Веб-страница по адресу **https://shas.org.il/**, возможно, временно недоступ
постоянно перемещена по новому адресу.

ERR_CONNECTION_ABORTED

Не удается получить доступ к сайту

Превышено время ожидания ответа от сайта **www.rosh-haa**

Попробуйте сделать следующее:

- Проверьте подключение к интернету.
- Проверьте настройки прокси-сервера и брандмауэра.
- Выполните диагностику сети в Windows

ERR_CONNECTION_TIMED_OUT

Не удается получить доступ к сайту

Превышено время ожидания ответа от сайта **www.umelfah**

Попробуйте сделать следующее:

- Проверьте подключение к интернету.
- Проверьте настройки прокси-сервера и брандмауэра.
- Выполните диагностику сети в Windows

ERR_TIMED_OUT

We punish Israel with attacks on websites😈

❌Portal of the city of Rosh HaAyin (dead by ping)
check-host.net/check-report/3b1b3d6bkb4a

❌Portal of the city of Umm al-Fahm
check-host.net/check-report/3b1b3bdeke4a

❌Shas - Israeli ultra-religious political party
check-host.net/check-report/3b1b3be5kb58

#OpIsrael

NoName057(16) 125 edited 04:54

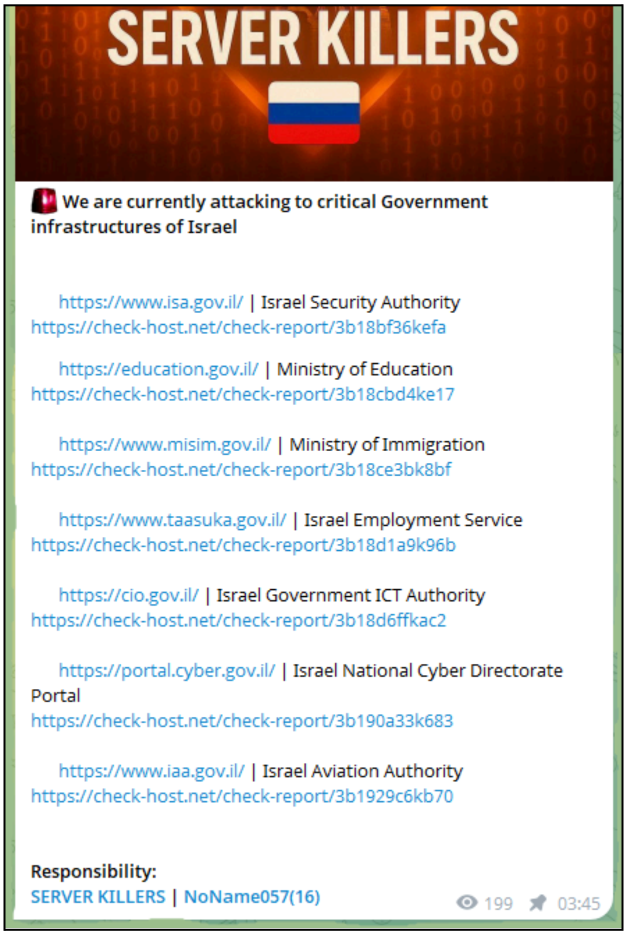
NoName057(16)'s Telegram post

Source: ZeroFox Intelligence

Server Killers

On March 6, 2026, pro-Russian group "Server Killers", seemingly in conjunction with NoName057(16), claimed on its Telegram channel to have compromised the web services of several Israeli government entities, including the Ministry of Education, the Ministry of Immigration, the Israel Employment Service, the Government ICT Authority, the National Cyber Directorate portal, and the Israel Aviation Authority.

- Server Killers announced it had "attacked critical government infrastructures of Israel" but did not specify the nature of the allegedly compromised websites. Based on the government organizations listed on the Telegram post, it is unlikely that Server Killers' compromise will expose significant sensitive data.



We are currently attacking to critical Government infrastructures of Israel

https://www.isa.gov.il/ | Israel Security Authority
https://check-host.net/check-report/3b18bf36kefa

https://education.gov.il/ | Ministry of Education
https://check-host.net/check-report/3b18cbd4ke17

https://www.misim.gov.il/ | Ministry of Immigration
https://check-host.net/check-report/3b18ce3bk8bf

https://www.taasuka.gov.il/ | Israel Employment Service
https://check-host.net/check-report/3b18d1a9k96b

https://cio.gov.il/ | Israel Government ICT Authority
https://check-host.net/check-report/3b18d6ffkac2

https://portal.cyber.gov.il/ | Israel National Cyber Directorate Portal
https://check-host.net/check-report/3b190a33k683

https://www.iaa.gov.il/ | Israel Aviation Authority
https://check-host.net/check-report/3b1929c6kb70

Responsibility:
SERVER KILLERS | NoName057(16)

199 03:45

Server Killers' Telegram post

Source: ZeroFox Intelligence

Claimed Attacks

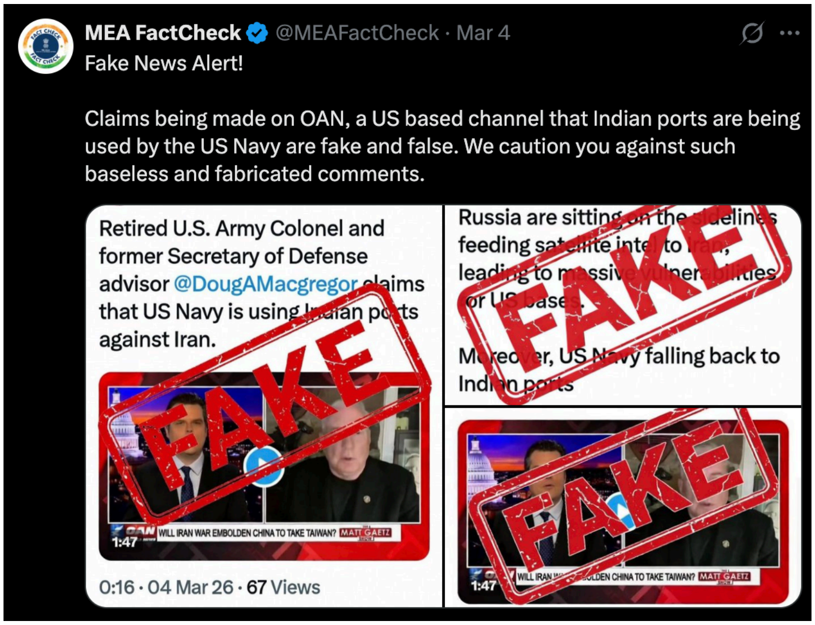
On March 6, ZeroFox continued to observe an abundance of threat actors and hacktivist collectives—primarily those who self-describe as pro-Iranian, pro-Islamic, pro-Palestinian, or pro-Russian—claiming to have conducted DDoS attacks, website defacements, data exfiltration, and intrusions into industrial control systems (ICS).

[Analyst Note: During periods of geopolitical tension, politically driven actors are likely to increase their efforts towards targeting oppositional entities; however, these actors are equally likely to exaggerate or misrepresent the severity and nature of their operations in order to propagate political messaging and/or fearmonger to gain inflated prominence.]

Disinformation

ZeroFox observed a notable wave of disinformation spreading through social media platforms such as X and Reddit, in which users are claiming that the U.S. military has been bombing nothing more than “drawings” of Iranian F-14s.[4][5] Most of these posts use similar language and expressions, likely indicating that this is a part of coordinated effort to spread disinformation and discredit the U.S. and Israeli militaries’ statements. These views are being amplified on Reddit by accounts that have previously posted pro-Iranian content.

A former U.S. military service member made claims on a U.S. news channel that the United States is using Indian ports or naval bases to launch attacks against Iran during the ongoing conflict. India’s Ministry of External Affairs’ (MEA) official FactCheck X account dismissed these statements, calling the allegations false and fabricated.[6]



MEA FactCheck @MEAFactCheck · Mar 4

Fake News Alert!

Claims being made on OAN, a US based channel that Indian ports are being used by the US Navy are fake and false. We caution you against such baseless and fabricated comments.

Retired U.S. Army Colonel and former Secretary of Defense advisor @DougAMacgregor claims that US Navy is using Indian ports against Iran.

0:16 · 04 Mar 26 · 67 Views

Russia are sitting on the sidelines feeding satellite intel to Iran, leading to massive vulnerabilities for US bases.

Moreover, US Navy falling back to Indian ports

FAKE
FAKE
FAKE
1:47
OAN WILL IRAN WAR EMBOLDEN CHINA TO TAKE TAIWAN? MATT GAETZ SHOW
1:47
WILL IRAN WAR EMBOLDEN CHINA TO TAKE TAIWAN? MATT GAETZ SHOW

MEA FactCheck’s X post

Source: ZeroFox Intelligence

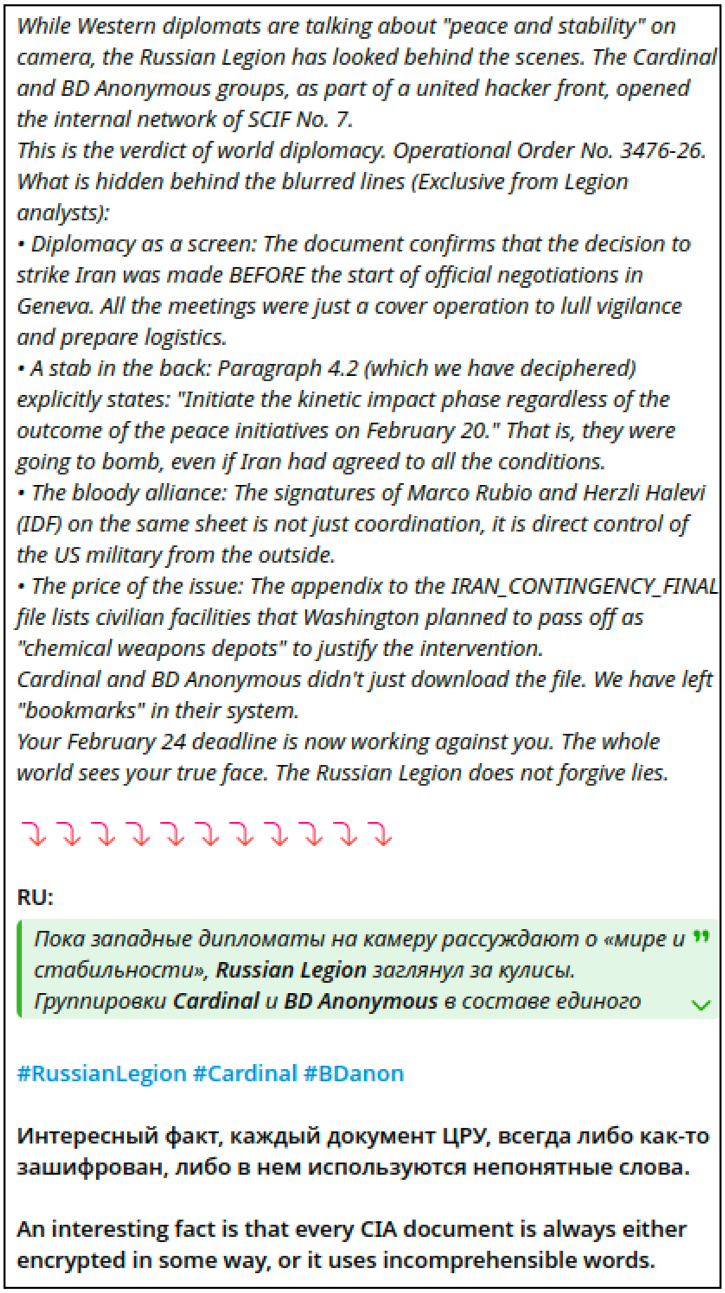
[4] hXXps://x[.]com/Newsweek/status/2029544155060314414?s=20
[5] hXXps://x[.]com/nCo6YCbWqCm3vPE/status/2029724926110781482?s=20
[6] hXXps://x[.]com/MEAFactCheck/status/2029233689570492805?s=20

Disinformation campaigns are often rampant during geopolitical conflicts and are very likely orchestrated by adversarial states to discredit official claims and influence public opinion. Such campaigns are likely to lead to the general public unknowingly spreading misinformation, subsequently causing confusion, division, and skepticism on media platforms.

Additional Findings:

Notable cyber activity over the last 24 hours (this is not an exhaustive list):

- Threat collective “**Russia Legion**”, seemingly in conjunction with threat collective “Cardinal Group”, claimed on Telegram that it had accessed an internal sensitive compartmented information facility (SCIF) network and obtained a document titled “Joint Contingency Operational Order No. 3476-26” allegedly signed by senior U.S. officials such as Marco Rubio and John Ratcliffe. Russia Legion alleges the document references pre-planned strikes against Iran. Further, Cardinal Group claimed it disabled Israeli air-defense systems in Tel Aviv and the central region, including Iron Dome and RADA radar infrastructure, while leaving Jerusalem untouched. Additionally, the collectives advertised two alleged intelligence documents referencing regional military activity and geopolitical tensions. These claims are very likely exaggerated. The documents shown in the images shared are likely forged attempts to resemble official documents by leveraging the names of high-ranking U.S. officials.



While Western diplomats are talking about "peace and stability" on camera, the Russian Legion has looked behind the scenes. The Cardinal and BD Anonymous groups, as part of a united hacker front, opened the internal network of SCIF No. 7.
This is the verdict of world diplomacy. Operational Order No. 3476-26.
What is hidden behind the blurred lines (Exclusive from Legion analysts):
• Diplomacy as a screen: The document confirms that the decision to strike Iran was made BEFORE the start of official negotiations in Geneva. All the meetings were just a cover operation to lull vigilance and prepare logistics.
• A stab in the back: Paragraph 4.2 (which we have deciphered) explicitly states: "Initiate the kinetic impact phase regardless of the outcome of the peace initiatives on February 20." That is, they were going to bomb, even if Iran had agreed to all the conditions.
• The bloody alliance: The signatures of Marco Rubio and Herzli Halevi (IDF) on the same sheet is not just coordination, it is direct control of the US military from the outside.
• The price of the issue: The appendix to the IRAN_CONTINGENCY_FINAL file lists civilian facilities that Washington planned to pass off as "chemical weapons depots" to justify the intervention.
Cardinal and BD Anonymous didn't just download the file. We have left "bookmarks" in their system.
Your February 24 deadline is now working against you. The whole world sees your true face. The Russian Legion does not forgive lies.

⤵⤵⤵⤵⤵⤵⤵⤵⤵⤵⤵

RU:

> *Пока западные дипломаты на камеру рассуждают о «мире и стабильности», **Russian Legion** заглянул за кулисы.*
> *Группировки **Cardinal** и **BD Anonymous** в составе единого*

#RussianLegion #Cardinal #BDanon

Интересный факт, каждый документ ЦРУ, всегда либо как-то зашифрован, либо в нем используются непонятные слова.

An interesting fact is that every CIA document is always either encrypted in some way, or it uses incomprehensible words.

Russian Legion's Telegram post

Source: ZeroFox Intelligence

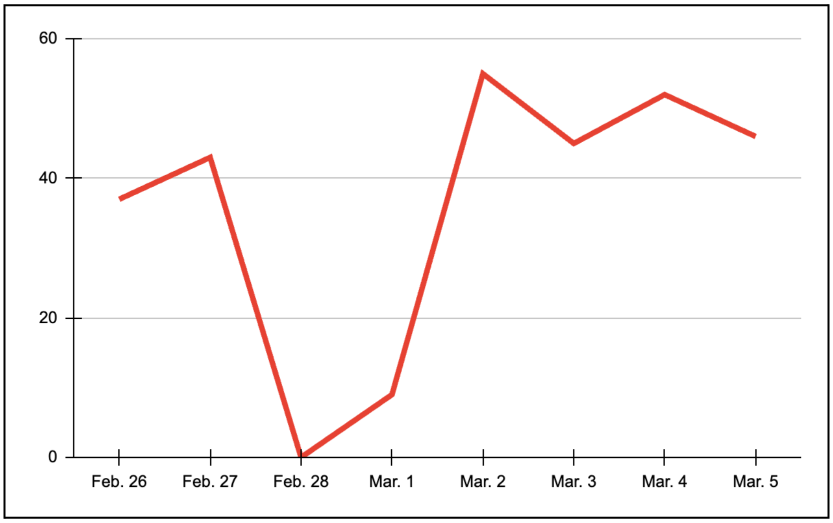
- Threat collective "**DieNet**" claimed responsibility for DDoS attacks targeting several Qatari government websites, including the Ministries of Interior, Labor, Education, and Transportation, as well as the Hukoomi eGovernment portal, Customs Authority, and the Central Municipal Council.

- Threat collective “**Islamic Cyber Resistance in Iraq – 313 Team**” claimed responsibility for targeting 26 Kuwaiti government IP domains, reportedly disrupting multiple state websites in DDoS attacks. Affected entities allegedly include the Ministry of Defense, National Guard, Ministry of Health, and the national e-government portal. The collective provided check-host links as evidence to support its claims on its Telegram channel. Most of these DDoS attacks are very likely temporary disruptions, if they have any effect at all, and are not significantly impactful to raise an alarm. These attacks are very likely to draw attention to 313 Team’s political agenda and, to a certain extent, influence public opinion.

Cyber Activity on the Rise

Over the last week (February 26–March 5), ZeroFox has observed at least 287 separate regional and industry-wide cyber incidents, including ransomware attacks, IAB sales, and vulnerabilities/exploits—a significant uptick in cyber incidents day-to-day as the Iran conflict has continued to escalate.

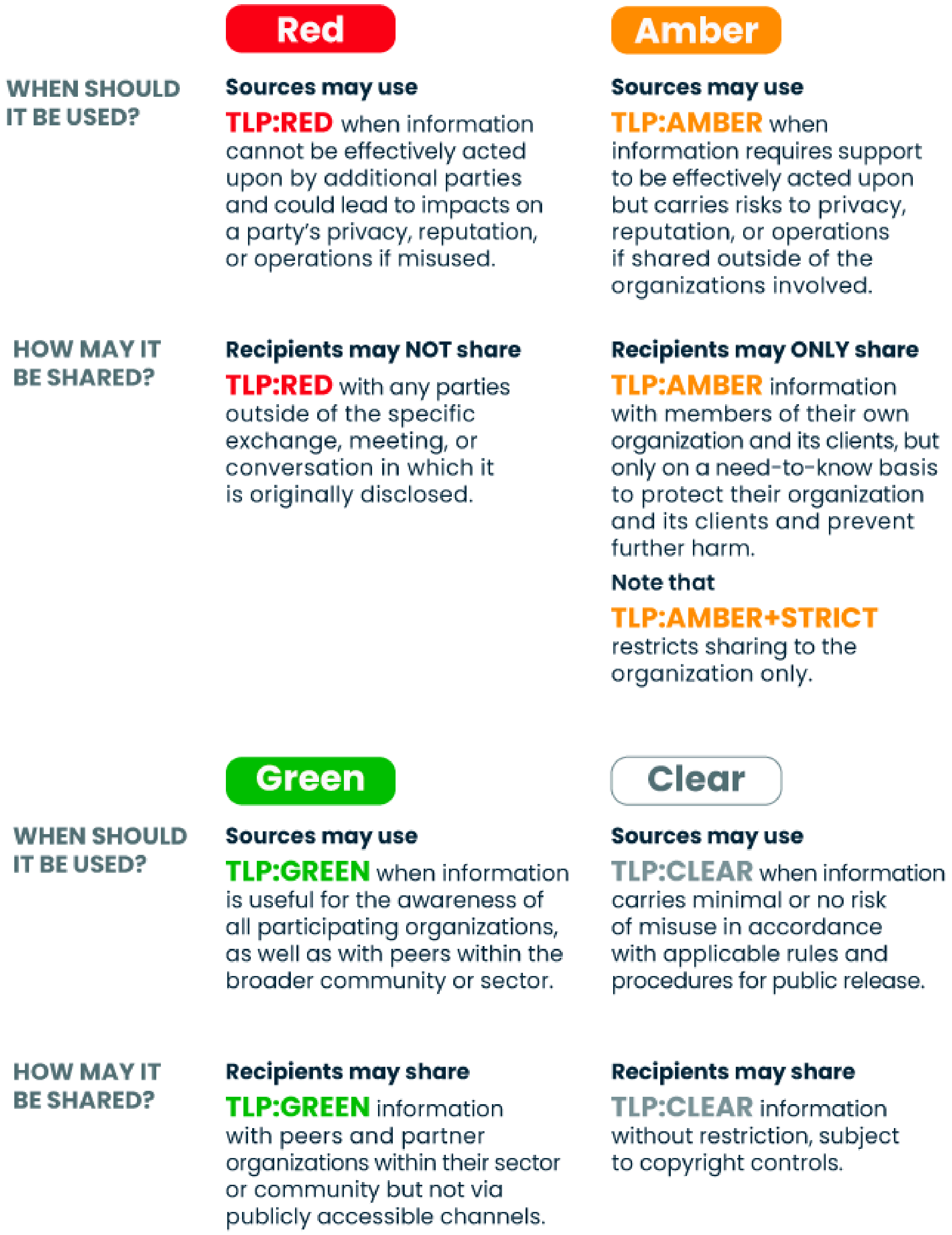
- There were at least 46 separate incidents on March 5. While remaining notably high, there is a roughly even chance that cyber incidents will continue steadily within the 40–50 incidents-per-day range. A spike in activity is likely if there is a significant escalation in U.S.-Israeli military actions against Iran.



Cyber incidents region-wide and industry-wide (February 26–March 5, 2026)

Source: ZeroFox Intelligence

Appendix A: Traffic Light Protocol for Information Dissemination

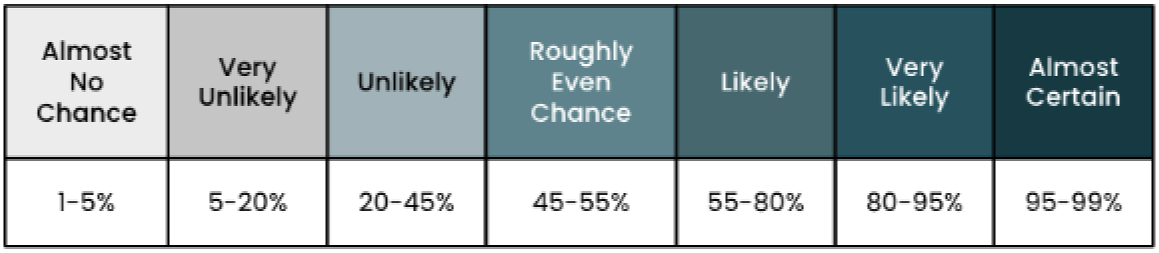


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.



Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%