Office of Cybersecurity and Critical Infrastructure Protection
Information Sharing
Flash Alert

TLP:GREEN

FA-10014

March 3, 2026

OCCIP Flash Alert – Increased Claims and Rhetoric Related to Iranian-Aligned Cyber Threat Groups and Activities Targeting U.S. and Partner Critical Infrastructure

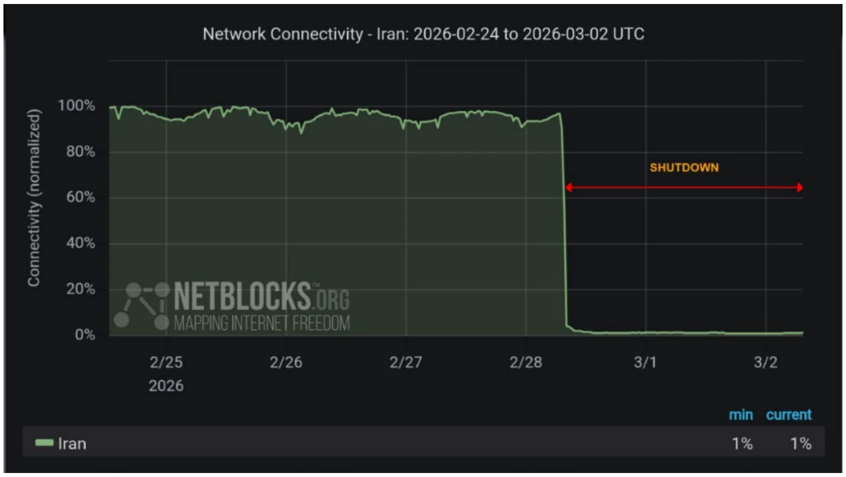
TRAFFIC LIGHT PROTOCOL (TLP): GREEN – RECIPIENTS MAY SHARE **TLP:GREEN** INFORMATION WITH PEERS AND PARTNER ORGANIZATIONS WITHIN THEIR COMMUNITY, BUT NOT VIA PUBLICLY ACCESSIBLE CHANNELS. UNLESS OTHERWISE SPECIFIED, **TLP:GREEN** INFORMATION MAY NOT BE SHARED OUTSIDE OF THE CYBERSECURITY OR CYBER DEFENSE COMMUNITY.

OCCIP Flash Alerts are intended to provide summary information on critical cyber incidents, threats, and actors of interest and relevance to the financial sector.

Details

Ongoing claims and calls for cyber-attacks targeting U.S. entities by Iranian aligned groups could lead to an increase in malicious activity against the financial services sector. Since 28 February 2026, there has been an increase in public messaging by Iranian-aligned cyber actors about targeting U.S. critical infrastructure, to include the financial sector, in retaliation for recent U.S.-Israeli military action against Iran. As of 2 March 2026, no significant cyberattacks against U.S. critical infrastructure organizations have been observed.

Since 28 February 2026, there has been a sharp drop in internet activity in Iran due to a near-total internet blackout, with connectivity at 1 percent of ordinary levels. As of 2 March 2026, metrics from internet monitor NetBlocks show that the internet blackout remains in effect.



Reporting remains inconclusive as to whether the disruption is an Iranian government-imposed blackout or the result of cyberoperations, however, reporting notes that limited activity is ongoing. If this is a self-imposed blackout, this limited activity may be whitelisted traffic enabling Iranian cyber actors to conduct operations against targets of opportunity. Historically, the U.S. financial sector has been viewed as a priority target and a target of opportunity by Iranian-aligned cyber actors.[1]

Since 28 February 2026, activity on Telegram and other social media platforms indicates an increase in messaging from self-identified hacktivist collectives and state-aligned advanced persistent threat (APT) groups claiming responsibility for cyber operations targeting U.S. and Israeli institutions. While some posts assert direct involvement in cyber-attacks, others consist primarily of warnings, threats, or declarations of intent directed at U.S., Israeli, and other Middle Eastern government and private-sector entities. To date, no evidence exists to validate these claims. This behavior aligns with broader information warfare and psychological operations tactics, in which public claims, exaggerated impact statements, and threat narratives are used to create uncertainty, erode public confidence, and amplify geopolitical tensions irrespective of the underlying technical impact.

Some notable claims and public messaging from various APT and Hacktivist groups/collectives in relation to recent events include:[2]

- 2MAR26 – Handala Group claims attack against Israeli energy company.
- 2MAR26 – Cyber Islamic Resistance starts posting messages on channel at 0851 UTC warning of cyber activity at 1800 UTC, subsequently posted at 1800 UTC claiming to have breached an Israeli health insurance company as well as webpage for the National Geographic TV channel in Israel.
- 2MAR26 – DieNet-affiliated channels claim ongoing DDoS activity against government services in Oman, as well as multiple Middle East based banking organizations.
- 2MAR26 – NoName057(16) claims DDoS attacks against Israeli internet infrastructure.
- 2MAR26 – APTIran claims to infiltrate sectors of Jordanian critical infrastructure.
- 1MAR26 – AnonGhost calls for coordinated cyber operations against U.S. and Israeli digital infrastructure, naming financial systems as a target.
- 1MAR26 – RipperSec claims DDoS attack against Israeli website.
- 1MAR26 – Team Dark Storm claims DDoS attack against Israeli financial institutions.

Recommended Actions

Although these claims are unverified, organizations are advised to continue to be vigilant and monitor for any potential incoming threat actor targeting. While Iranian-aligned cyber actors have historically

[1] https://www.cisa.gov/resources-tools/resources/iranian-cyber-actors-may-target-vulnerable-us-networks-and-entities-interest
[2] Screenshots of some claims made by the mentioned threat actors can be found in the Appendix at the conclusion of this report.

overstated claims of success, they are still capable actors who have carried out successful DDoS, wiper malware, ransomware, and credential-based attacks. OCCIP recommends financial institutions reinforce fundamental cyber hygiene practices and leverage available intelligence and information-sharing resources to proactively identify, monitor, and mitigate emerging cyber threats.

Please see the following resources for more information:

- CISA's Iran Threat Overview and Advisories
- OCCIP Flash Alert 10013 – Potential Increased Activity by Iranian Cyber Actors During Escalating Tensions

As a matter of general practice, network defenders are recommended to utilize resources provided by CISA, such as the Known Exploited Vulnerabilities Catalog and CISA Cyber Hygiene Vulnerability Scanning services. These services are designed to assess external network presence by conducting continuous scans of public, static IPs for accessible services and vulnerabilities. In addition, ensure that software vendors adhere to stringent security and transparency standards. This can reduce the risk of compromise due to insecurities in vendor products or potential vulnerabilities within a vendor's systems that could be exploited by attackers.

Reporting Suspicious Activity

Organizations should report incidents and anomalous activity to CISA's 24/7 Operations Center at Contact@mail.cisa.dhs.gov, or FBI through a local field office or FBI's Cyber Division at CyWatch@fbi.gov or 855-292-3937, or any of the U.S. Secret Service's local field offices to report a crime.

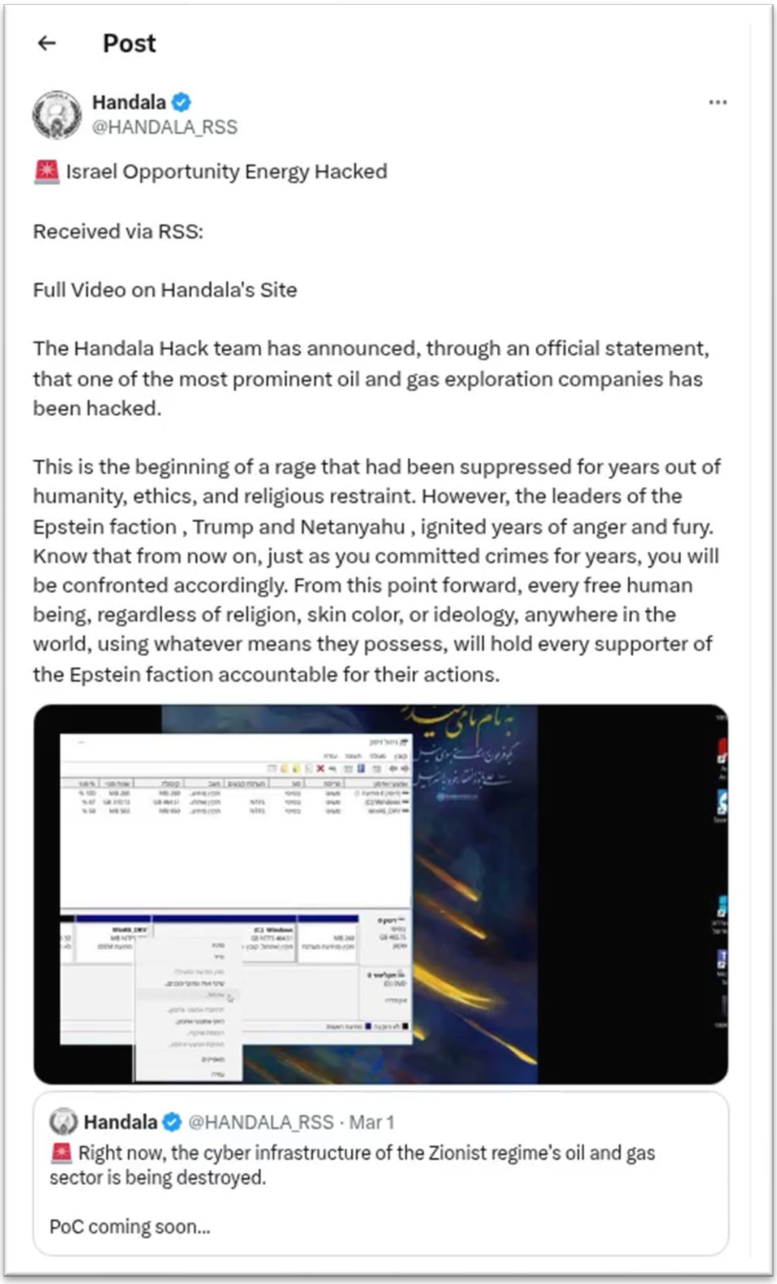
We would like to hear from you on the usefulness of these reports to continuously improve them. Please take a moment to let us know what works and how we can better meet your needs. We invite all input but are particularly interested in input on the following:

- The usefulness of the reports
- The appropriate level of detail
- Ideas for improving the relevance of the reports
- Steps to make information more salient
- Ways to provide more appropriate context
- Topics for future reports

Please direct comments or questions to OCCIP-Coord@treasury.gov.

Flash Alerts are being provided "as-is" for informational purposes only. The Treasury Department does not provide warranties of any kind regarding information contained within.

Appendix: Screenshots of Threat Actor Claims



Handala
@HANDALA_RSS

🚨 Israel Opportunity Energy Hacked

Received via RSS:

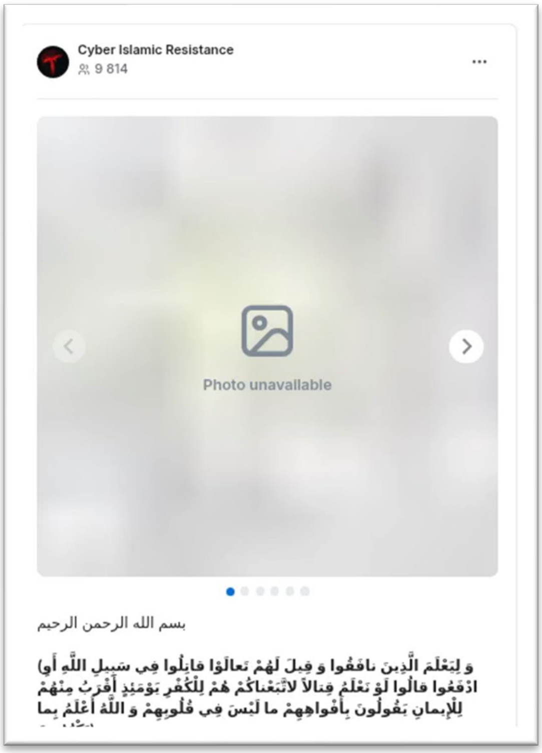
Full Video on Handala's Site

The Handala Hack team has announced, through an official statement, that one of the most prominent oil and gas exploration companies has been hacked.

This is the beginning of a rage that had been suppressed for years out of humanity, ethics, and religious restraint. However, the leaders of the Epstein faction , Trump and Netanyahu , ignited years of anger and fury. Know that from now on, just as you committed crimes for years, you will be confronted accordingly. From this point forward, every free human being, regardless of religion, skin color, or ideology, anywhere in the world, using whatever means they possess, will hold every supporter of the Epstein faction accountable for their actions.

Handala @HANDALA_RSS · Mar 1
🚨 Right now, the cyber infrastructure of the Zionist regime's oil and gas sector is being destroyed.

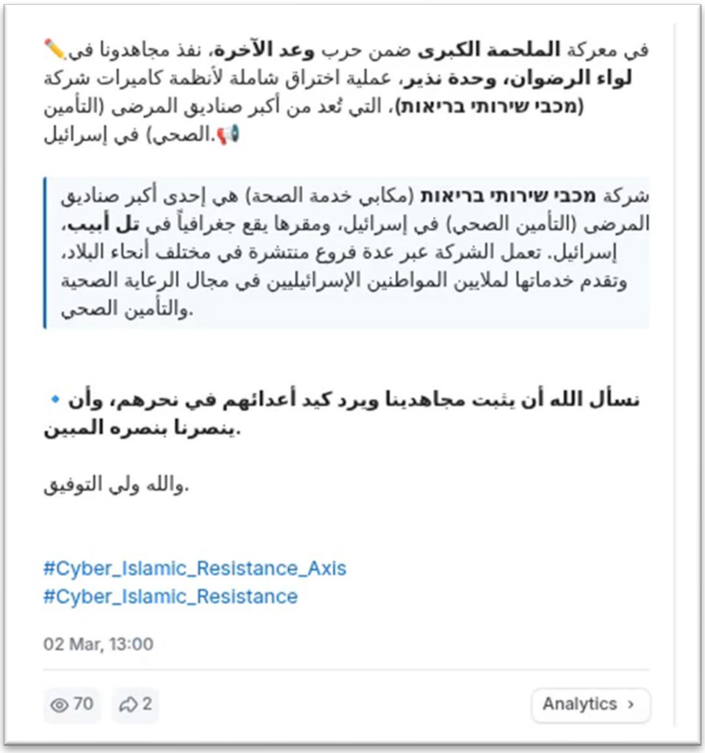
PoC coming soon...



Cyber Islamic Resistance
9 814

بسم الله الرحمن الرحيم

وَ لِيَعْلَمَ الَّذِينَ نافَقُوا وَ قِيلَ لَهُمْ تَعالَوْا قاتِلُوا فِي سَبِيلِ اللَّهِ أَوِ)
ادْفَعُوا قالُوا لَوْ نَعْلَمُ قِتالاً لاتَّبَعْناكُمْ هُمْ لِلْكُفْرِ يَوْمَئِذٍ أَقْرَبُ مِنْهُمْ
لِلْإِيمانِ يَقُولُونَ بِأَفْواهِهِمْ ما لَيْسَ فِي قُلُوبِهِمْ وَ اللَّهُ أَعْلَمُ بِما



في معركة **الملحمة الكبرى** ضمن حرب **وعد الآخرة**، نفذ مجاهدونا في✏️
لواء الرضوان، وحدة نذير، عملية اختراق شاملة لأنظمة كاميرات شركة
(מכבי שירותי בריאות)، التي تُعد من أكبر صناديق المرضى (التأمين
الصحي).📢 في إسرائيل

> شركة **מכבי שירותי בריאות** (مكابي خدمة الصحة) هي إحدى أكبر صناديق
> المرضى (التأمين الصحي) في إسرائيل، ومقرها يقع جغرافياً في **تل أبيب**،
> إسرائيل. تعمل الشركة عبر عدة فروع منتشرة في مختلف أنحاء البلاد،
> وتقدم خدماتها لملايين المواطنين الإسرائيليين في مجال الرعاية الصحية
> والتأمين الصحي.

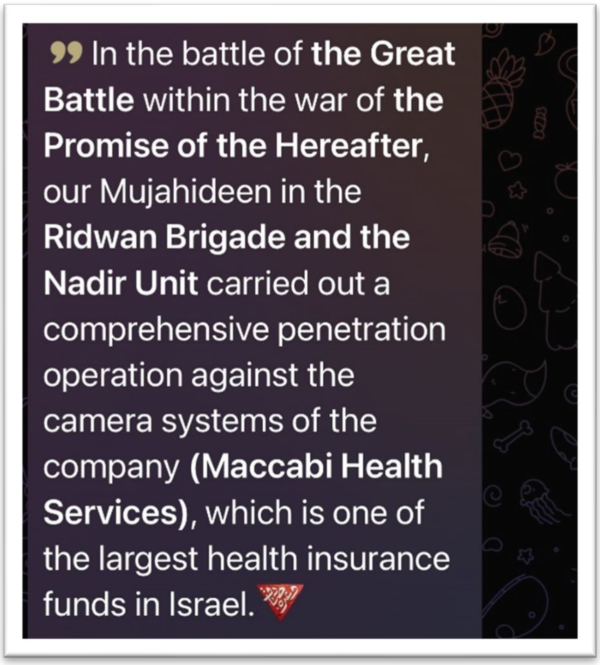
🔹 **نسأل الله أن يثبت مجاهدينا ويرد كيد أعدائهم في نحرهم، وأن
ينصرنا بنصره المبين.**

والله ولي التوفيق.

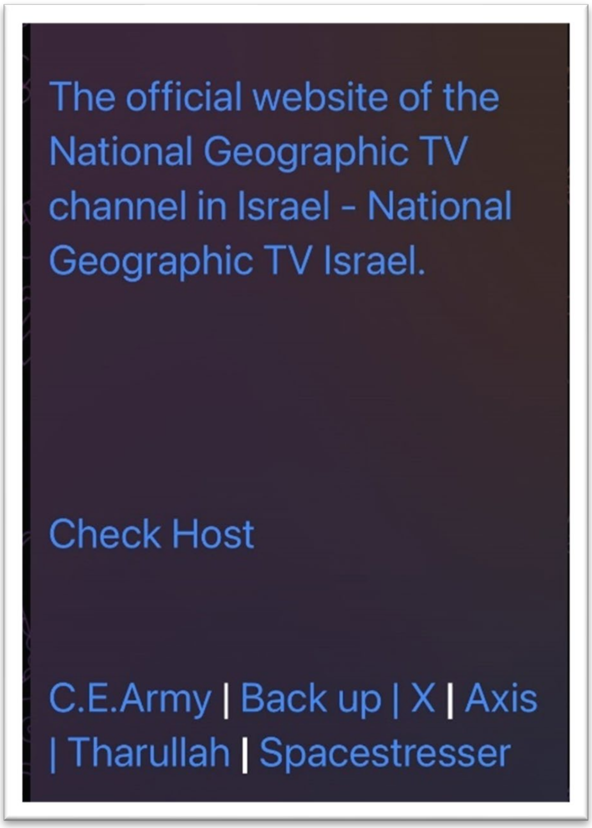
#Cyber_Islamic_Resistance_Axis
#Cyber_Islamic_Resistance

02 Mar, 13:00

👁 70 ↪ 2 Analytics ›



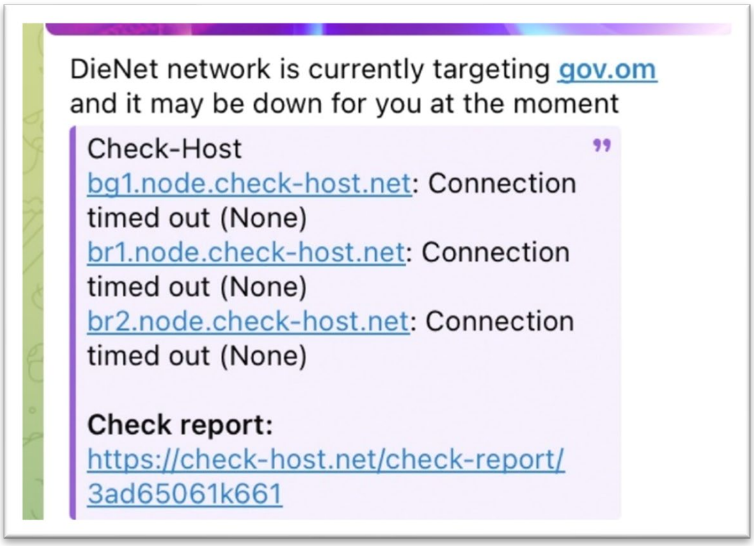
❞ In the battle of **the Great Battle** within the war of **the Promise of the Hereafter**, our Mujahideen in the **Ridwan Brigade and the Nadir Unit** carried out a comprehensive penetration operation against the camera systems of the company **(Maccabi Health Services)**, which is one of the largest health insurance funds in Israel. 🔻



The official website of the National Geographic TV channel in Israel - National Geographic TV Israel.

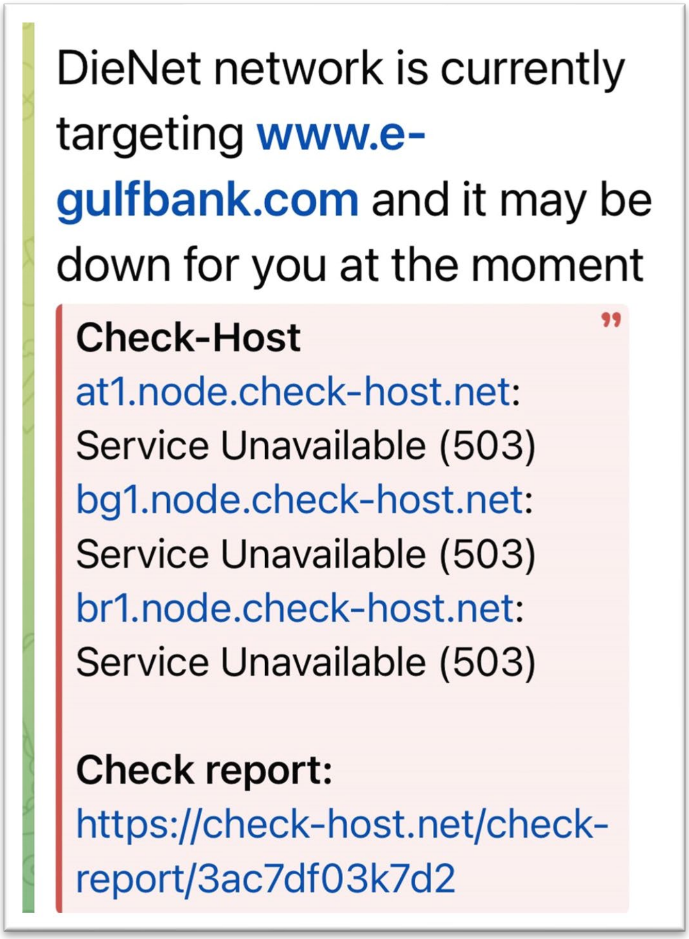
Check Host

C.E.Army | Back up | X | Axis | Tharullah | Spacestresser



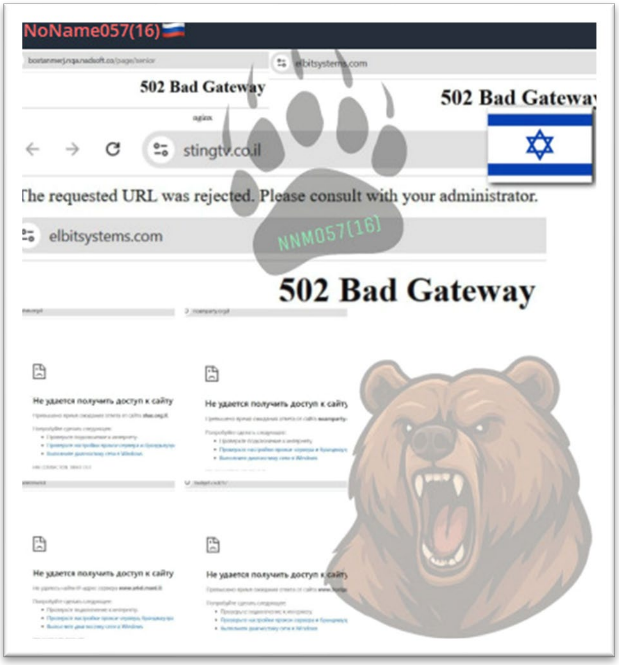
DieNet network is currently targeting gov.om and it may be down for you at the moment

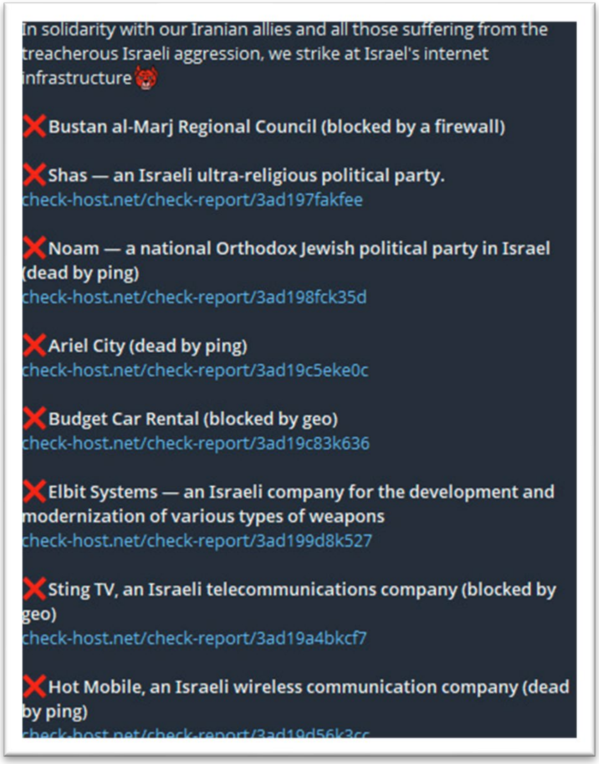
> Check-Host
> bg1.node.check-host.net: Connection timed out (None)
> br1.node.check-host.net: Connection timed out (None)
> br2.node.check-host.net: Connection timed out (None)
>
> **Check report:**
> https://check-host.net/check-report/3ad65061k661



DieNet network is currently targeting www.e-gulfbank.com and it may be down for you at the moment

> **Check-Host**
> at1.node.check-host.net: Service Unavailable (503)
> bg1.node.check-host.net: Service Unavailable (503)
> br1.node.check-host.net: Service Unavailable (503)
>
> **Check report:**
> https://check-host.net/check-report/3ac7df03k7d2


NoName057(16)🇷🇺
elbitsystems.com
502 Bad Gateway
502 Bad Gateway
nginx
stingtv.co.il
The requested URL was rejected. Please consult with your administrator.
elbitsystems.com
NNM057(16)
502 Bad Gateway
Не удается получить доступ к сайту
Не удается получить доступ к сайту
Не удается получить доступ к сайту
Не удается получить доступ к сайту



In solidarity with our Iranian allies and all those suffering from the treacherous Israeli aggression, we strike at Israel's internet infrastructure🐻

❌Bustan al-Marj Regional Council (blocked by a firewall)

❌Shas — an Israeli ultra-religious political party.
check-host.net/check-report/3ad197fakfee

❌Noam — a national Orthodox Jewish political party in Israel (dead by ping)
check-host.net/check-report/3ad198fck35d

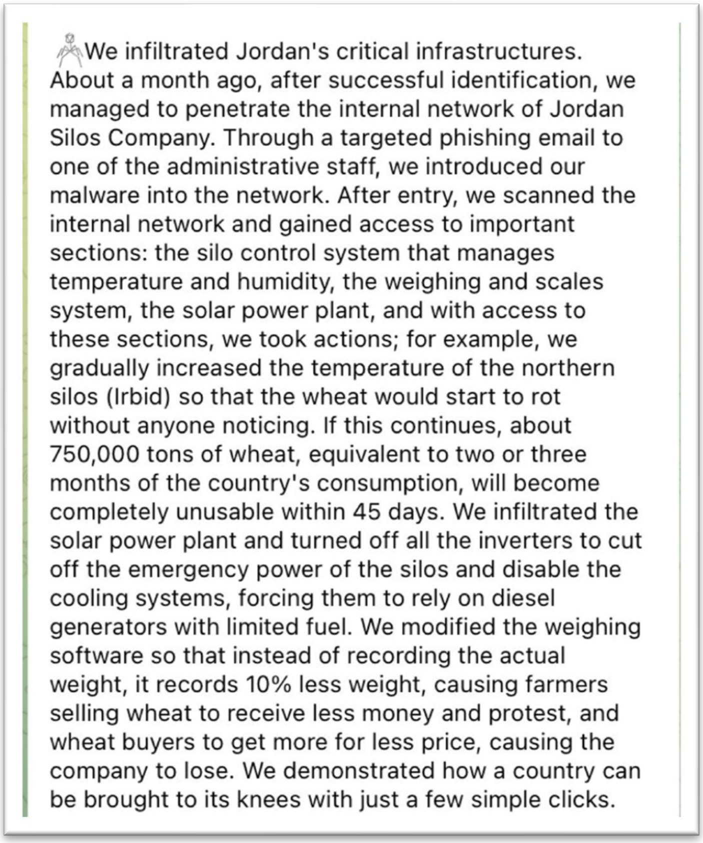
❌Ariel City (dead by ping)
check-host.net/check-report/3ad19c5eke0c

❌Budget Car Rental (blocked by geo)
check-host.net/check-report/3ad19c83k636

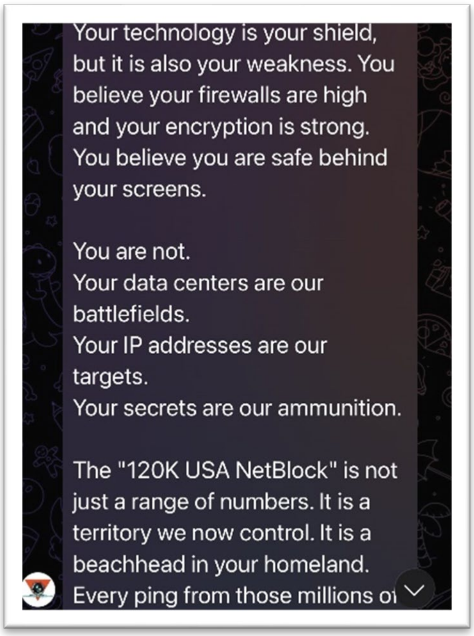
❌Elbit Systems — an Israeli company for the development and modernization of various types of weapons
check-host.net/check-report/3ad199d8k527

❌Sting TV, an Israeli telecommunications company (blocked by geo)
check-host.net/check-report/3ad19a4bkcf7

❌Hot Mobile, an Israeli wireless communication company (dead by ping)
check-host.net/check-report/3ad19d56k3cc



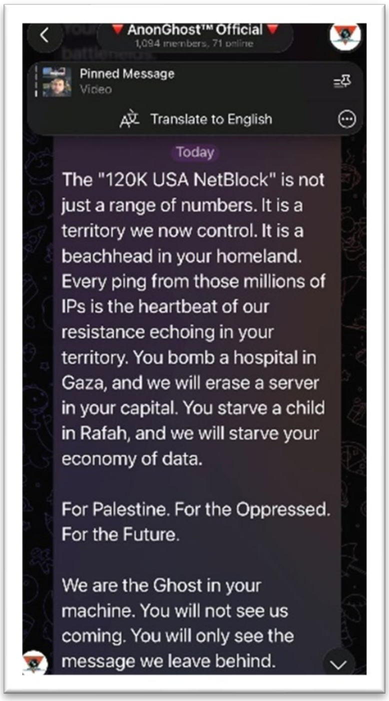
We infiltrated Jordan's critical infrastructures. About a month ago, after successful identification, we managed to penetrate the internal network of Jordan Silos Company. Through a targeted phishing email to one of the administrative staff, we introduced our malware into the network. After entry, we scanned the internal network and gained access to important sections: the silo control system that manages temperature and humidity, the weighing and scales system, the solar power plant, and with access to these sections, we took actions; for example, we gradually increased the temperature of the northern silos (Irbid) so that the wheat would start to rot without anyone noticing. If this continues, about 750,000 tons of wheat, equivalent to two or three months of the country's consumption, will become completely unusable within 45 days. We infiltrated the solar power plant and turned off all the inverters to cut off the emergency power of the silos and disable the cooling systems, forcing them to rely on diesel generators with limited fuel. We modified the weighing software so that instead of recording the actual weight, it records 10% less weight, causing farmers selling wheat to receive less money and protest, and wheat buyers to get more for less price, causing the company to lose. We demonstrated how a country can be brought to its knees with just a few simple clicks.



Your technology is your shield, but it is also your weakness. You believe your firewalls are high and your encryption is strong. You believe you are safe behind your screens.

You are not.
Your data centers are our battlefields.
Your IP addresses are our targets.
Your secrets are our ammunition.

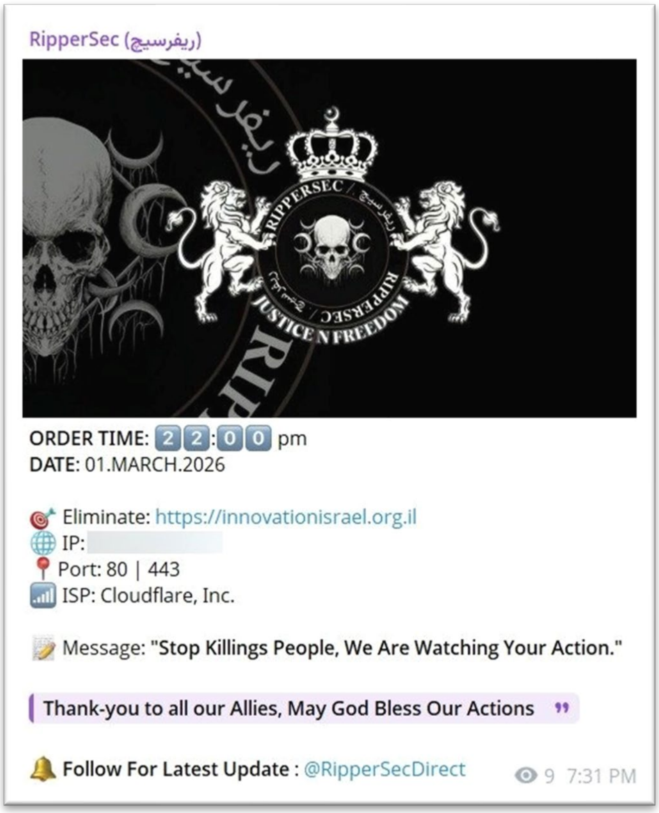
The "120K USA NetBlock" is not just a range of numbers. It is a territory we now control. It is a beachhead in your homeland. Every ping from those millions o



The "120K USA NetBlock" is not just a range of numbers. It is a territory we now control. It is a beachhead in your homeland. Every ping from those millions of IPs is the heartbeat of our resistance echoing in your territory. You bomb a hospital in Gaza, and we will erase a server in your capital. You starve a child in Rafah, and we will starve your economy of data.

For Palestine. For the Oppressed. For the Future.

We are the Ghost in your machine. You will not see us coming. You will only see the message we leave behind.



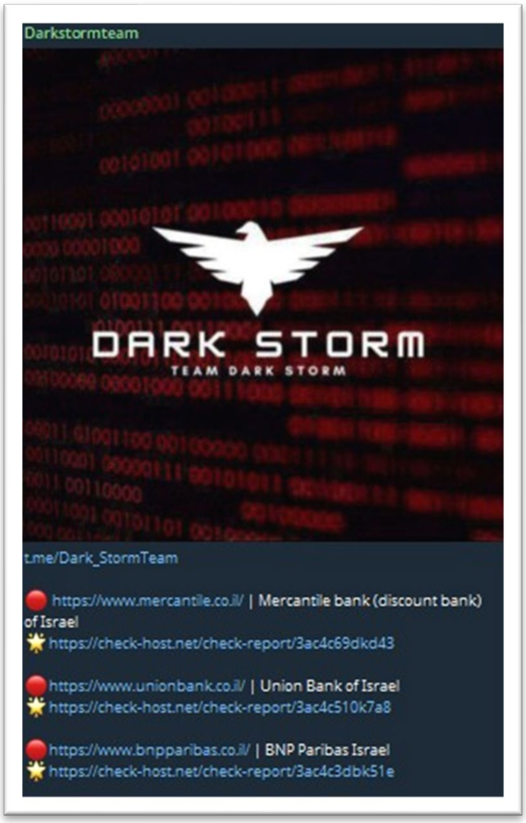
ORDER TIME: 22:00 pm
DATE: 01.MARCH.2026

🎯 Eliminate: https://innovationisrael.org.il
🌐 IP: [redacted]
📍 Port: 80 | 443
📶 ISP: Cloudflare, Inc.

📝 Message: "Stop Killings People, We Are Watching Your Action."

> Thank-you to all our Allies, May God Bless Our Actions

🔔 Follow For Latest Update : @RipperSecDirect



Darkstormteam

t.me/Dark_StormTeam

🔴 https://www.mercantile.co.il/ | Mercantile bank (discount bank) of Israel
🌟 https://check-host.net/check-report/3ac4c69dkd43

🔴https://www.unionbank.co.il/ | Union Bank of Israel
🌟 https://check-host.net/check-report/3ac4c510k7a8

🔴https://www.bnpparibas.co.il/ | BNP Paribas Israel
🌟 https://check-host.net/check-report/3ac4c3dbk51e