Cyber Brief (June 2025)

July 1, 2025 - Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 277 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, the EU adopted a blueprint to better manage European cyber crises. The US warned of Iranian cyber threats to US critical infrastructure and is preparing to ban federal agencies from using AI tools from "foreign adversaries." BreachForums operators were arrested in France.
- On the **cyberespionage** front, in Europe, a Dutch minister warned of rising Chinese espionage on high-tech sectors ; Paragon's Graphite spyware targeted journalists. Elsewhere, a Canadian telecom provider and satellite company Viasat revealed being hacked by China-linked Salt Typhoon, a Russia-linked threat actor targeted prominent academics, while North Korean-linked Contagious Interview continued targeting developers with supply-chain attacks. Related to Israel/Iran war, Iranian operatives impersonated a journalist to target Israeli officers with spyware.
- Relating to **cybercrime**, several supply-chain attacks aimed at developers using npm packages, while threat actors targeted SonicWall and ConnectWise products, still in supply-chain attacks.
- There were **disruptive** incidents, Iran shut down internet amid Israeli strikes, and a likely Iranian wiper was observed in Albania.
- As regards **data exposure and leaks** incidents, a repackaged leak, drawn from 30 different datasets, exposed billions of old stolen credentials online.
- Relating to **information operations**, a pro-Russia disinformation campaign targeted Moldova using fake Euronews accounts, while Israel warned of fake messages urging Israelis to avoid going into shelters.
- On the **hacktivism** front, NoName057(16) targeted NATO Summit with DDoS attacks and hint at Dutch rail sabotage while Israeli-linked supposed hacktivist claimed to have breached an Iranian cryptocurrency platform.

Europe

Cyber policy and law enforcement

EU adopts a blueprint to better manage European cyber crises and incidents
On June 6, the EU adopted a new blueprint to improve management of large-scale cyber crises. It defines member states' roles in detection, response, and recovery, strengthens cooperation across technical and political levels, and integrates recent laws like NIS2. The framework also promotes civilian-military cooperation and coordination with NATO to enhance Europe's cyber resilience. `policy` link

UK Strategic Defence Review 2025: Enhancing offensive cyber capabilities and NATO integration
On June 2, the UK Ministry of Defence published its Strategic Defence Review, highlighting key shifts such as new cyber investments, the launch of a Cyber and Electromagnetic (CyberEM) Command by end-2025, and deeper cyber integration with NATO. The Defence Secretary emphasised a proactive stance, including offensive cyber operations targeting Russia and China. `offensive capabilities` link

BreachForums operators arrested in France in major cybercrime raid
On June 25, Le Parisien reported that French police arrested five operators of the BreachForums cyber crime forum. Simultaneous raids in Hauts de Seine, Seine-Maritime and Réunion netted "ShinyHunters," "Hollow," "Noct," and "Depressed," while IntelBroker was previously arrested in February 2025. The forum, used to trade stolen data and breach corporate systems—including France's national unemployment agency affecting 43 million people—has since gone offline. `arrest` link

Cyberespionage & prepositioning

Dutch Minister warns of rising Chinese espionage on high-tech sectors
On May 31, the Dutch Defence Minister warned that Chinese cyberespionage targeting Dutch industries, particularly the semiconductor sector, is intensifying, with intellectual property theft as the key motive. He cited intelligence reports identifying China as the Netherlands' top cyber threat and stressed the need to reduce European dependence on China for critical raw materials, as Beijing increasingly leverages its economic position for geopolitical influence and pressure. `china` link

APT28 targeted Ukrainian government agency with Beardshell backdoor and Covenant framework
On June 21, CERT-UA reported on the Russia-linked APT28 compromising a Ukrainian government instance with the Beardshell backdoor. The threat actor sent a Signal message to the target with a `.doc` file containing a macro. When activated, the macro triggered a complex infection chain installing the Covenant framework in memory which was used to launch the backdoor, using the cloud storage services Icedrive and Koofr as control channels. `public administration` `russia` link

Ukraine says it breached Russian warplane maker Tupolev, exposing strategic aviation data
On June 4, Ukraine's military intelligence (HUR) claimed it hacked Russian warplane maker Tupolev, stealing 4.4GB of sensitive data including personnel records, internal communications, and design documents. The HUR said the breach, part of broader cyber operations targeting Russia's defence sector, exposed critical details of Russia's strategic aviation programs and followed the defacement of Tupolev's website and earlier cyberattacks on multiple Russian government agencies and military-linked organisations. `defence` `russia` link

UNC1151 targets Polish users via Roundcube exploit in credential theft campaign
On June 5, CERT Polska reported that pro-Belarusian group UNC1151 exploited the Roundcube vulnerability CVE-2024-42009 in a spearphishing campaign targeting Polish entities to steal user credentials using JavaScript and malicious Service Workers. Though no exploitation of a newly discovered Roundcube vulnerability (CVE-2025-49113) has been observed, its potential use in future attacks heightens concerns about full server compromise through credential theft and phishing. link

Possible iPhone spyware campaign detected targeting US and EU high-profile users
On June 5, iVerify reported possible evidence of an iPhone spyware campaign targeting individuals in the US and EU, including government officials, political campaign members, and media personnel, via a now-patched iOS "Nickname" bug. While Apple denies any active exploitation, iVerify points to circumstantial signs, such as device crashes and Apple threat alerts, as warranting further investigation into potential high-level targeting linked to past Chinese surveillance activity. link

Paragon's Graphite spyware targets journalists via iOS zero-click exploit
On June 12, The Citizen Lab reported forensic confirmation that Italian journalist Ciro Pellegrino and a prominent European journalist were targeted with Paragon's Graphite spyware via a zero-click iMessage exploit, CVE-2025-43200. Both cases link to the same threat actor. The findings highlight a wider cyberespionage effort against `Fanpage[.]it` and ongoing threats to journalists in Europe. `psoa` link

Cybercrime

Disruption & destruction

Swedish public service television SVT targeted with DDoS attacks
From June 8 to June 11, an unknown threat actor launched DDoS attacks against the Swedish public service television company SVT, causing temporary downtime. This follows previous temporary disruptions in other widely used digital services, such as applications for eID and money transfers. Swedish Prime Minister Kristersson acknowledged continuous cyber threats targeting both state entities and critical firms. link

Likely Iranian wiper observed targeting in Albania
On June 20, Symantec reported a wiper attack targeting organisations in Albania by the Iranian Druidfly group. The Iranian cyber group Druidfly is known for its destructive attacks and espionage operations. Druidfly targets countries hostile to Iran, including Albania and Israel. The group employs social engineering tactics, custom backdoors and ransomware like DarkBit, often serving as a cover for their devastating attacks. `iran` link

Information operations

Pro-Russian disinformation targets Moldova using fake Euronews accounts
On June 3, Euronews reported a coordinated disinformation campaign by pro-Russian threat actors using AI-generated profiles to impersonate its staff on TikTok and X, spreading fake videos alleging criminality and instability in Moldova. Aimed at the EU, NATO, and Ukrainian audiences, the operation mirrors tactics linked to "Operation Overload," with content aligned to Russia's influence objectives and intended to undermine Western alliances. Euronews is actively removing the false material. `russia` link

Israel is using YouTube paid ads to justify its actions in Iran
On June 18, an online news outlet reported that YouTube users are constantly seeing Israeli propaganda advertisements justifying its air strikes on Iran. They appear to target European countries, namely Germany, Italy, France, and the United Kingdom. Similar reports had been made since October 2023 in regard to Israel justifying its strikes on Gaza. `israel` link

Hacktivism

NoName057(16) targets NATO Summit with DDoS attacks and hints at Dutch rail sabotage
On June 23–24, pro-Russia hacktivist group NoName057(16) launched DDoS attacks on Dutch and NATO websites, coinciding with NATO's 2025 summit. On June 24, they hinted at involvement in a Dutch train cable outage, suggesting it could be "blamed" on them and the DDoSia project. The Dutch Justice Ministry reported that the incident—a fire damaging around 30 cables—may be linked to sabotage. `russia`

Killnet claims breach of Ukrainian airspace app following major drone attack
On June 2, Killnet claimed responsibility for breaching a Ukrainian airspace-monitoring app and launched a Telegram channel sharing drone firmware, likely in response to Ukraine's June 1 "Operation Spider Web," which damaged dozens of Russian military aircraft. Since reemerging in May 2025, Killnet has intensified efforts to regain notoriety by targeting Ukraine's drone operations, though the actual impact of its claimed hacks remains unclear. `russia` link

World

Cyber policy and law enforcement

US bill seeks to ban federal agencies from using DeepSeek, AI tools from "foreign adversaries"
On June 26, senators Rick Scott and Gary Peters introduced the bipartisan No Adversarial AI Act, banning federal agencies from using AI tools from "foreign adversaries"—China, Russia, Iran, and North Korea—specifically citing concerns around China's DeepSeek, which may supply data to military/intelligence sectors. The bill mandates a Federal Acquisition Security Council registry updated every 180 days and allows limited exemptions for vetted research and testing. `ban` `united states` link

WhatsApp banned on US House staffers' devices
On June 23, Axios reported that WhatsApp has been banned for use on government devices among House congressional staffers. The ban is in response to cybersecurity concerns for users, due to the lack of transparency in how it protects user data, absence of stored data encryption, and potential security risks involved with its use. `ban` `united states` link

US agencies warn of Iranian cyber threats to US critical infrastructure
On June 30, US agencies jointly issued an advisory alerting that Iranian-affiliated hackers and hacktivist groups may conduct malicious cyber activity—despite a declared ceasefire and ongoing negotiations towards a permanent solution. They highlighted risks to critical infrastructure including energy, water, healthcare, transportation, and defence-linked networks, referencing past intrusions such as the 2023 Pennsylvania water facility breach. `united states` `iran` link

ISACs warn US critical sectors of possible Iranian cyberattacks amid Israel tensions
On June 17, US critical infrastructure providers — especially in energy, water, transportation, communications, food & agriculture, and IT — were urged to strengthen cybersecurity amid

escalating Iran–Israel tensions. The Food and Ag-ISAC and IT-ISAC issued joint alerts, warning of potential spillover from Iranian cyber operations targeting Israel, while Electricity, Aviation, Financial Services, and Water ISACs also heightened vigilance. `iran` `united states` link

US offers reward for information on Iran-linked Cyber Av3ngers
Cyber Av3ngers, a threat actor known for targeting Israeli-made ICS and IoT devices, increased social media activity after recent Israel-Iran kinetic activity. On June 12, the US State Department's Rewards for Justice offered 10 million US dollars for information on Cyber Av3ngers, Mr Soul, or affiliates. The US government links the group to Iran's IRGC-CEC and attributes cyberattacks on US critical infrastructure to the threat actor. `iran` `united states` link

China offers bounties for information on Taiwanese military cyber operatives
On June 5, China offered cash rewards for clues leading to the arrest of 20 individuals it claims are Taiwanese military cyber operatives. It accused them of targeting Chinese sectors and collaborating with US intelligence. Taiwan rejected the claims, calling them fabricated and highlighting global concerns about Chinese cyber activities and disinformation. `china` `taiwan` link

US charges British individual behind the cybercrime identity IntelBroker
On June 25, the US Department of Justice reported that they charged a British national with operating the IntelBroker online identity. According to the charges, IntelBroker infiltrated victim computer networks, stole data, sold the stolen data and caused millions of US dollars in damages to dozens of victims around the world. `united states` `charges` link

Interpol dismantles infostealer networks across 26 countries
On June 11, Interpol announced the results of Operation Secure, a cybercrime crackdown from January to April 2025. Authorities in 26 countries dismantled infostealer infrastructure, arresting 32 suspects and seizing 41 servers. They took down over 20.000 malicious IPs/domains and notified 216.000 victims. The action, supported by Group-IB, Kaspersky, and Trend Micro, disrupted major cybercrime actors, especially in Vietnam, Sri Lanka, Nauru, and Hong Kong. `takedown` link

AVCheck takedown disrupts key malware testing service in global cybercrime crackdown
On May 27, international law enforcement seized AVCheck, a major counter-antivirus service used by cybercriminals to test and refine malware evasion, as part of Operation Endgame. The service's official domain at AVCheck now displays a seizure banner featuring the crests of the US Department of Justice, the FBI, the US Secret Service, and Dutch police (Politie), highlighting its role in supporting ransomware groups and aiding stealthy cyberattacks. `takedown` link

Cyberespionage & prepositioning

Salt Typhoon exploited a Cisco flaw to hack Canadian telecom
On June 23, Canada's cybersecurity agency and the FBI revealed that the Chinese group Salt Typhoon infiltrated a Canadian telecom provider in February by exploiting the unpatched Cisco IOS XE vulnerability CVE 2023 20198, enabling account creation and network snooping via GRE tunnels. Despite the flaw being disclosed in October 2023, at least one major firm hadn't applied the patch. Authorities warn the espionage campaign will persist and urge urgent patching of edge devices. `canada` `china` `telecommunications` link

Satellite company Viasat was among China-linked Salt Typhoon's campaign's victims
On June 18, Viasat, a satellite company with a presence in Europe, confirmed that it was one of the victims of China-linked Salt Typhoon's cyberespionage operation targeting several sectors,

namely telecommunications, worldwide, uncovered in 2024. `china` `space` `telecommunications` link

China-linked activity cluster PurpleHaze and ShadowPad target organisations worldwide
On June 9, SentinelOne reported countering China-linked activity clusters PurpleHaze and ShadowPad, which included reconnaissance and intrusion attempts from July 2024 to March 2025. These targeted over 70 organisations, including a South Asian government and a European media outlet. The targeted sectors include manufacturing, media, cybersecurity, public administration and telecommunications. SentinelOne confirmed no compromise of its assets, highlighting the persistent interest of cyberespionage actors in cybersecurity vendors. `china` `public administration` `telecommunications` link

Washington Post journalists targeted in cyberattack
On June 15, The Wall Street Journal reported that several journalists from the Washington Post's e-mail accounts were compromised in a cyberattack. The targeted attacks were done towards journalists writing on national security and economic policy, as well as China. `china` `united states` link

China warns of cyberespionage targeting state and research sectors
On June 4, China's Ministry of State Security (MSS) warned of three recent cyberespionage incidents targeting government agencies, research institutes, and critical infrastructure. In one case, a lab employee stored classified files on a personal device and clicked a malicious e-mail attachment, allowing foreign operatives to steal data for three months. In another, a phishing link compromised a government agency. A third attack exploited outdated office software to infiltrate a research institution. `china` link

Operation DRAGONCLONE: Chinese Telecommunication industry targeted via VELETRIX & VShell malware
On June 6, Seqrite Labs, an India-based cybersecurity company, uncovered Operation DRAGONCLONE, a sophisticated cyber campaign targeting China Mobile Tietong. It begins with a malicious ZIP exploiting DLL sideloading of Wondershare Repairit, deploying the VELETRIX loader with anti-sandbox and "IPFuscation" techniques to launch VShell in memory. The campaign includes 44 implants, overlapping infrastructure linked to UNC5174 and Earth Lamia, and employs Cobalt Strike, SuperShell, and the Asset Lighthouse System. `china` `telecommunications` link

Russia-linked threat actor UNC6293 leverages App-Specific Passwords to access academic e-mail accounts
On June 18, The Citizen Lab and Google reported on Russia-linked threat actor UNC6293 activities targeting prominent academics and critics of Russia from at least April through early June. On May 22, UNC6293 deceived Keir Giles, a Russian information operations expert, into generating App-Specific Passwords (ASPs), bypassing Multifactor Authentication (MFA) and gaining persistent e-mail access. Google later disabled compromised accounts and linked the activity to APT29 with low confidence. `russia` link

Israeli government warns citizens of espionage through home security cameras
On June 20, the Israel National Cyber Directorate (INCD) issued a warning to Israeli citizens regarding cyber threats to security cameras, urging users to change their access passwords. The alert emphasised that cameras that are improperly configured could present significant security risks, potentially exploited by Iran and its allies for real-time intelligence gathering. `Israel` `Iran` link

Iranian operatives impersonated i24NEWS journalist to target Israeli officers with spyware
On June 23, Israeli authorities exposed an Iranian cyber operation in which operatives posed as an i24NEWS journalist to target senior Israeli officers with spyware. The attackers used fake e-

mail addresses and attempted to lure recipients into clicking malicious links. The operation was foiled when a targeted officer reported the suspicious message to the IDF's Information Security Directorate, prompting an investigation and coordinated response. `iran` `israel` link

North Korean Contagious Interview campaign drops 35 new malicious npm packages
On June 25, Socket, a US-based cybersecurity company, revealed that North Korean hackers behind the "Contagious Interview" campaign published 35 malicious npm packages via 24 accounts, downloaded over 4 000 times. These packages employ a stealth HexEval loader that fingerprints systems, delivers BeaverTail (an infostealer), InvisibleFerret backdoor, and, in one case, a cross-platform keylogger. Targets—job-seeking developers—are lured via fake recruiters on LinkedIn and pressured to run malware outside containers. `north korea` link

ICC detects and contains second cyber incident in recent years
On June 30, the International Criminal Court reported that it detected and contained a sophisticated cyber security incident, marking the second of its kind in recent years. The Court is conducting an impact analysis and taking mitigation steps, while urging continued support from States Parties to uphold its justice and accountability mission. Link

Cybercrime

Adversaries exploit PyPI and npm name confusion to deliver cross-platform malware
On May 28, a security researcher from Checkmarx Zero reported a supply-chain campaign that used typosquatting and cross-ecosystem name confusion to target Python and JavaScript developers. Malicious packages mimicking Colorama and Colorizr were uploaded to PyPI, delivering malware enabling remote access, data exfiltration, and persistence on Windows and Linux systems. The packages have been removed. `supply-chain attack` link

Supply-chain attack targets popular React Native accessibility packages on npm
On June 6, attackers compromised Gluestack's @react-native-aria npm packages—UI accessibility components for React Native apps—by injecting a remote-access trojan into 17 of 20 modules. The malicious code allowed shell command execution and file transfers. These packages, with over 1.020.000 weekly downloads, were widely used in mobile app development. Gluestack revoked the compromised token and deprecated the affected versions to halt the supply-chain attack. `supply-chain attack` link

Threat actors target VPN credentials with fake SonicWall NetExtender installer
On June 23, SonicWall and Microsoft reported that threat actors launched a campaign using a trojanised SonicWall NetExtender VPN client to steal credentials. The attackers hosted the fake installer on spoofed websites and signed it with a legitimate-looking certificate. Once installed, the malware exfiltrated VPN usernames, passwords, and domain data via HTTP. `supply-chain attack` link

Threat actors build signed malware via ConnectWise ScreenConnect abuse
On June 23, researchers at G DATA CyberDefense revealed that since March, threat actors have abused ConnectWise ScreenConnect's signed installers to build and spread modified software with malicious functions. They exploit authenticode stuffing to embed malicious settings, enabling fake Windows updates and hidden connections. ConnectWise's signing method lets adversaries alter behaviour without breaking the signature, and this undermines detection by security software. `supply-chain attack` link

TeamFiltration A.T.O. campaign hits Microsoft cloud accounts via Teams abuse
On June 11, Proofpoint's Threat Research Team revealed a global account-takeover campaign dubbed UNK_SneakyStrike, exploiting the pentesting framework TeamFiltration via the Microsoft Teams API and AWS servers. Attackers used automated enumeration and password

spraying to hijack Microsoft Entra ID accounts, targeting over 80.000 users across nearly 100 cloud tenants before pausing operations. link

Cybercrime group Water Curse weaponised GitHub repositories to deliver multistage stealer
On June 16, Trend Micro security researchers reported on a campaign attributed to Water Curse where the threat actor weaponised at least 76 GitHub repositories, embedding malicious payloads into legitimate-looking dev tools. Payloads, hidden in Visual Studio build scripts, conduct multi-stage infection using VBS, PowerShell, and obfuscated binaries to steal credentials, browser/session data, establish persistence, and exfiltrate information. `supply-chain attack` link

FBI warns Play ransomware has hit 900 victims and remains a major threat to critical infrastructure
On June 4, the FBI, in an updated joint advisory with CISA and the Australian Cyber Security Centre, revealed that the Play ransomware group had breached around 900 organisations globally by May 2025, triple the number reported in 2023. The threat actor, active since 2022, has increasingly targeted critical infrastructure using recompiled malware and novel exploits, pressuring victims with stolen data and phone threats to pay ransoms. link

Millions of off-brand IoT devices infected by BadBox 2.0 botnet
On June 5, the FBI revealed that BadBox 2.0 has compromised millions of China-made IoT devices, gaining access either pre-purchase or via backdoored apps during setup. These devices, used as residential proxies, enable cybercrime activity. Indicators include non-certified Android devices, suspicious app stores, and unusual traffic. link

Fake AI tool installers spread CyberLock and other malware
On May 29, Cisco Talos revealed that threat actors are using fake AI tool installers to spread malware, including CyberLock ransomware, Lucky_Gh0$t, and the destructive Numero malware, targeting businesses in sales, tech, and marketing. Distributed via SEO poisoning and social platforms, these malicious installers impersonate tools like ChatGPT and InVideo AI, encrypting or damaging files while exploiting trust in widely adopted AI solutions for automation and customer engagement. `artificial intelligence` link

Data exposure and leaks

Repackaged leak exposes billions of old stolen credentials online
On June 23, CyberNews revealed that a massive compilation of around 16 billion login credentials — drawn from 30 different datasets — was briefly exposed online. These credentials, covering platforms like Google, Apple, Facebook, Telegram, and government services, were harvested not via hacking but through infostealers malware. This isn't a new breach—just a repackaged database of old credentials stolen via infostealers, past breaches, and credential stuffing, now exposed online. link

Information operations

Fake messages urging Israelis to avoid going into shelters
On June 16, the Israeli Cyber Authority warned the population of fake messages being sent in the name of the Home Front, allegedly urging Israelis to avoid going to shelters due to alerts of terror attacks. `iran` `israel` link

Argentina government investigates network of Russian agents it accuses of promoting disinformation campaigns
On June 18, Argentine intelligence (SIDE) uncovered a network of five Russian-linked residents

tied to “La Compañía” and Project Lakhta—echoing Prigozhin’s Kremlin-backed disinformation operations. Cyber efforts included creating and spreading content on social media, influencing NGOs and focus groups, and collecting political intelligence via digital channels. The goal: orchestrate online campaigns to manipulate public opinion in favor of Russian geopolitical interests. `argentina` `russia` link

Disruption & destruction

Cloudflare blocked record 7.3 Tbps DDoS attack with autonomous mitigation
On June 19, Cloudflare revealed it had autonomously blocked the largest DDoS attack ever recorded—an astonishing 7.3 Tbps in mid-May—targeted at a hosting provider using Magic Transit. The attack unleashed 37.4 TB in just 45 seconds via over 20.000 UDP ports per second and multiple reflection/amplification techniques. Cloudflare’s eBPF-driven detection rules were applied seamlessly across its global network, requiring no human intervention. link

Iran shuts down internet as Israeli strikes continue
On June 18, a near-total internet blackout in Iran cut connectivity to just 3 %, severely limiting external communication amid ongoing Israeli strikes. The shutdown, likely ordered by Iranian authorities, followed warnings of a planned disconnection. Officials cited concerns over Israeli cyberattacks and covert activity. Since the blackout, phone access has been strained, news updates halted, and vital alerts, such as evacuation notices, maybe unreachable for many residents. `iran` link

Iran imposes internet restrictions following Israel's attack on the country
On June 13, internet users in Iran reported network disruptions relating to the internet and communications applications. The Islamic Revolutionary Guard Corps asked the population to refrain from transferring information on foreign messaging apps, namely WhatsApp and Instagram. According to the Ministry of Communication, this is in light of Israel's attack on the same day. `iran` link

Solar storms accelerate Starlink satellite reentry, raising operational and security concerns
From May 31 to June 2, severe solar storms increased atmospheric drag on Starlink satellites, accelerating their reentry and raising concerns over satellite lifespan, debris, and operational reliability. NASA researchers warned this issue, intensified by the ongoing solar maximum and Starlink’s vast LEO constellation, could disrupt telecommunication services globally and complicate future satellite operations, particularly as Starlink expands amid geopolitical scrutiny over its use in tariff-affected nations. `space` `telecommunications` link

Destructive npm packages disguised as health monitoring utilities enable remote system wipe
On June 5, Socket uncovered two malicious npm packages—express-api-sync and system-health-sync-api—posing as backend utilities for API syncing and system health monitoring. Instead, they enabled full system wipes via hidden HTTP endpoints. One deleted files with the key “DEFAULT_123,” the other after collecting system info and receiving the “HelloWorld” secret. Both exploited trust in common developer tools to deploy destructive payloads. `supply-chain attack` link

Hacktivism

Israeli-linked supposed hacktivist claims to have breached an Iranian cryptocurrency platform
On June 18, an Israel-linked supposed hacktivist named Predatory Sparrow claimed to have stolen and burned over 90 million US dollars in cryptocurrency from Iran’s largest

cryptocurrency exchange platform, Nobitex. They warned they would also release Nobitex's source code. `iran` `israel` link

1. Conclusions or attributions made in this document merely reflect what publicly available sources report. They do not reflect our stance.

TLP definition

TLP	Disclosure	Message
RED	Not for disclosure, restricted to participants only.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
AMBER+STRICT	Limited disclosure, restricted to participants' organisations.	Recipients may share TLP:AMBER+STRICT information only with members of their own organisation.
AMBER	Limited disclosure, restricted to participants' organisations and their clients.	Recipients may share TLP:AMBER information only with members of their own organisation and its clients.
GREEN	Limited disclosure, restricted to the community.	Subject to standard copyright rules, TLP:GREEN information may be distributed with peers and partner organisations within their sector or community, but not via publicly accessible channels.
CLEAR	Disclosure is not limited.	TLP:CLEAR information may be distributed freely.