Cyber-Intelligence Report

#ESET

This cyber-intelligence product is a snapshot of selected cyber events. Collection of information is in accordance with clients' guidelines. It contains 'observations', meaning headlines and links to online information. It *MAY* contain comments and analysis. It is copyright David Swan 2026. This report is **TLP:CLEAR**[1] and MAY be shared freely.

If this report does not meet your requirements, is in error or if you need additional information, contact David Swan at DSC.Ops.Vulcan@gmail.com

Cyber Intelligence Report: Iran's IGRC Using Destructive Hacks

This report contains selected cyber-security information from 30th October to 12th November 2026.

Synopsis

1. France identified Iran's IRGC hackers as the refrigeration systems hackers. U.S. agencies are warning: More ICS attacks may be coming. Japan remains under cyber attack; the impact includes individuals. Japanese Government response to their cyber emergency. North Korea was behind the Biance attack. South Korea responded to limit further attacks, but attacks continue. PRC's ARTEX AI campaign continues against Japan. PRC has other cyber campaigns. Some Russian hackers have shifted to destructive attacks. Who is The Cyber Army Of Russia Reborn? Is Belarus joining Russia cyber forces?

2. We report hacker activity based on the threat posed. It is our *assessment* that cyber conflicts such as Russia vs Ukraine, Iran vs Israel, etc. are the most likely sources for the creation of next generation malware and/or a primary source of cyber attacks.

Iranian IRGC Hackers Target Global Refrigeration Systems

3. **France Identifies Hackers Who Hacked Refrigeration Systems As Iranian**. In mid-October a few grocery stores in France reported that their freezers had their controls hacked and turned up as high as 50 degrees C, spoiling the food. "*In early November, similar cyberattacks on commercial refrigerators and freezers were reported across Europe, with grocery stores in Belgium, Ireland, Luxembourg, and Sweden reporting widespread food losses after miscreants spiked temperatures to as high as 122°F (50°C). ... The supermarket attacks, which affected Casino, Leclerc, Coopérative U, Metro, Carrefour, and Intermarché groups, started at least 15 fires and caused food losses in the tens of millions of euros.*"[2] An estimated 700 retail sites were hit.[3] The attacks included French 'blood banks'.[4] "*The affected businesses,*

1 Definition **TLP:CLEAR.** From U.S. Govt Cyber Defense Agency. Traffic Light Protocol (TLP) Definitions and Usage, Recipients may share this information without restriction. Information is subject to standard copyright rules.
2 Source: The Register. France blames Iran for supermarket hack meltdowns
3 Source: The Hacker News. France Blames Iran for Sabotage Attack on Refrigeration Controllers at About 700 Retail Sites
4 Source: ITPro. French blood service hit by cyber attack threatening to turn stocks into "black pudding"

© David Swan Consulting 2026

ranged from major chains to small butcher shops, are in Belgium, Estonia, Ireland, Luxembourg, the Netherlands and Sweden. ... Problems have also been reported in Finland, Italy and Portugal."[5]

4. The next attacks "*targeted freezers at military bases around the* [U.S.]." The hacks were similar to previous Iranian attacks on American water systems.[6] On 9 November the French government "*attributed the refrigeration controller hacks to the Iranian Islamic Revolutionary Guard Corps' (IRGC) Shahid Kaveh cyber unit. ... France's Ministry for Europe and Foreign Affairs said ... 'This is an unprecedented campaign in terms of its scale and level of aggressiveness, thus constituting the first cyber offensive campaign carried out purely for the purpose of sabotage on national territory'."*[7]

5. **It May NOT Be Over**. "*CISA, the FBI, HHS, USDA and the Department of Transportation published a joint advisory on attacks against industrial refrigeration controllers and cold chain monitoring systems. The activity is global. Healthcare, chemical, food and transport companies use these systems to watch temperatures, keep logs, run defrost cycles and save energy, including in refrigerated trucks. ... The targets are electronic temperature controllers and commercial refrigeration controllers used in grocery stores and cold-storage sites. Attackers may exploit flaws in unpatched or internet-accessible controllers to change settings remotely and force units into continuous heating and defrost cycles. In plain terms, someone could cook your freezer from the other side of the world."*[8]

Japan Struggles Under Aggressive Cyber Attacks

6. **Ongoing Cyberattacks Targeting Japan**. The cyber assault on Japan continues. There are unverified reports that the Japanese government is asking citizens to 'disconnect from the Internet'[9] due to the number and the scope of of the attacks.[10]

- 29 Oct: Good Smile Company [Japanese video game developer and toy manufacturer] reports potential leak of full credit card information of 2,800 customers in major data breach
- 29 Oct: Hackers Steal 2.6 Million Records From Sony's Japanese ISP So-net
- 4 Nov: Securitize Japan Breach Exposes Sony Bank and NTT Customer Data
- 4 Nov: Japan's VIP Liner Highway Bus Booking Site Hacked
- 4 Nov: Japanese [crypto] Exchange Zaif Reports Email Leak Affecting 380,000 Users
- 5 Nov: NIKKE publisher confirms PC launcher breach exposed players to security risks
- 5 Nov: NTT Docomo [major Japanese mobile phone carrier] Faces Massive Data Breach due to Cyberattack

5 Source: Security Week. Over 100 European Stores Hit as Supermarket Fridge Attacks Return
6 Source: Next Gov. Officials suspect Iran in series of cyberattacks on military base freezers
7 Source: The Register. France blames Iran for supermarket hack meltdowns
8 Source: Security Affairs. CISA and the FBI Warn Of Attacks against Industrial Refrigeration Controllers
9 Source: Cybersecurity Insiders. Cyber Attack Emergency forces Japan to ask citizens to disconnect devices from internet
10 NOTE: These are in addition to the attacks reported in CIR Volume 6, Edition 22, dated 28 Oct 2026

© David Swan Consulting 2026

Cyber-Intelligence Report

- 6 Nov: Japan banking crisis hits 128 banks. Could Europe be next? *"On Friday, Nov 6, 128 Shinkin Central Banks ... west of the Tokai region suspended all customer services, including ATM withdrawals, deposits, and online transactions, ... Customers and local businesses face indefinite service suspensions with no confirmed restoration timeline."*
- 8 Nov: Iris Ohyama data cloud breach exposes info of 7.7 million customers *"No reopening date as orders face delays and some customers are told to refuse deliveries to cancel purchases."*[11]
- 10 Nov: SEGA confirms 2.2 million email addresses exposed in newsletter data breach

7. **What Is the Impact?** The effect of the cyber attacks range from suspended banking, Internet services unavailable, to having individual bank accounts drained. A camera operator for Korean news, living in Japan, reported: *"When checking his mobile phone on the morning of November 1, he found credit card transaction records from an online shopping mall that he could not recognize. Nine payments had been made over about an hour the previous night, eight of which were for the exact same amount. The total payment amounted to 79,908 yen, equivalent to approximately 680,000 won in Korean currency."*[12] This example is becoming common.

8. **Japan's Emergency Cyber Response**. Prime Minister Sanae Takaichi announced a package of emergency measures. The package outlines four pillars:

- strengthening basic security measures through AI,
- improving information gathering and analysis,
- adopting a strategic approach to respond to attacks and
- enhancing steps to support victims and prevent further damage.

"As part of further measures, Takaichi instructed cybersecurity minister Toshiharu Furukawa to consider revisions to a law strengthening the government's ability to respond to the attacks. ... The government will establish a "top gun" team of cybersecurity specialists to counter hackers and use AI to detect weaknesses in computer systems, and work with overseas IT firms and advanced AI developers to keep information about vulnerabilities up to date." This includes proactively accessing hackers servers in an "*active cyber defense*". "*... the government is considering allowing telecommunications carriers to forcibly block access to specific websites or servers linked to such attacks. ... A "rescue team" consisting of experts from the public and private sectors will be established to be dispatched to cyberattack-hit businesses to assist with initial responses, along with a separate team to give advice to companies at risk before being targeted."* The Japanese government has committed *"10 billion yen ($63 million) from its fiscal 2026 budget reserve funds to beef up cybersecurity measures."*[13]

11 Source: The Register. Japanese homeware giant pulls online store after cloud breach puts 7.7M records at risk
12 Source: SBS News. Watching TV When Unauthorized Payments Flooded In
13 Source: The Mainichi. Japan unveils emergency cybersecurity package amid data breach concerns

© David Swan Consulting 2026

Cyber-Intelligence Report

Cyber Attacks on South Korea

9. **$6.3 Billion Biance Hack Blamed on North Korea**. The FBI has blamed TraderTraitor, a hacking group affiliated with the Lazarus Group, the North Korean hacking organization specializing in hacking crypto exchanges. Before the FBI identified the hackers, "*Blockchain intelligence firms TRM Labs and Elliptic had linked the theft to North Korea, with TRM reporting that most of the $6.36 billion haul disappeared in about 20 minutes. Elliptic, which puts the total closer to $6.43 billion, says it has verified that $2.85 billion of the stolen assets have been frozen or seized.*"[14] Analyst Comments: This is a separate attack from the PRC operated 'ARTEX' AI based attacks.

10. **South Korea's 'AI Labs' Strikes Back**. *"AI Labs said that using its own threat intelligence, it secured about 50 attacker IP addresses and command-and-control (C2) server domains related to the financial sector attack incident."* Previously AI Labs found "*a Chinese administrator string reading 'ARTEX-AI autonomous penetration testing console' was found on an attacker infrastructure server. In response, the security field took steps to block the string, specific user-agent information, and ARTEX-specific attack patterns at firewalls.*"[15] AI Labs warned that these efforts only slow attacks as AI gives the attacking hackers the ability to rapidly change.

11. **Cyber Attacks Continue Against South Korea**.

- Personal info of 39,000 persons leaked from Mirae Asset Securities
- HYBE Data Breach: BTS Agency Reveals Employee and Business Partners' Personal Information, Including Medical Records, Exposed in Cyberattack
- Hack at Financial Security Institute leaks data from firms under assessment. Information related to the security status of some financial firms was leaked.

People's Republic of China

12. '**ARTEX' AI Campaign Expands**. Cyber security firm 'CrowdStrike' is tracking the ARTEX AI campaign. CrowdStrike says the hackers running the campaign were identified in February 2021 and named 'Vapor Panda' (previously VexatiousTemper). "*Starting October 17, 2026, Vapor Panda is said to have used the AI tool against more than 200 distinct organizations across the world, including foreign ministries in Latin America, Europe, Asia, and the Middle East; semiconductor, defense, and think tank organizations in the U.S.; and telecommunications providers in multiple regions. Some of the notable targets listed by CrowdStrike are listed below:*

- *Foreign ministries of two Latin America-based countries, Central America, and Asia*
- *A Middle East-based interior ministry*
- *A European country's foreign ministry, presidency, and prime minister's office, along with defense, justice, finance, and intelligence entities*
- *19 U.S.-based organizations in the pharmaceutical, semiconductor, defense, nuclear, and financial sectors*

14 Source: The Register. FBI pins $6.3B Binance crypto heist on North Korean hackers
15 Source: Chosun Biz. AI-driven hacks test Korea's banks as old defenses hit limits

© David Swan Consulting 2026

- *Telecommunications providers in the U.S., Belgium, and the Philippines."*

Analyst Comments: CrowdStrike's timeline of ARTEX attacks in the Philippines correlates with other reports, specifically 5-7 Nov "*massive wave of data breach and exposure incidents affecting 23 local institutions, including major national government agencies, law enforcement bodies, military systems and educational entities.*"[16]

13. "*Post-exploitation activity has been confirmed at nine organizations, allowing the attacker to deploy BLOODALCHEMY, a derivative of ShadowPad, followed by credential spraying, network scanning, and reconnaissance. 'Vapor Panda' is also said to have conducted password-spraying and credential-scanning activity against at least 12 additional organizations, including U.S. based think tanks and government entities in Europe.*" ARTEX is working well enough that its developer has taken it to 'closed source'. Another cyber security firm 'Zscaler ThreatLabz' said: "*It orchestrates multiple LLM backends to autonomously perform reconnaissance, vulnerability identification, and exploitation, significantly lowering the technical barrier for conducting complex intrusion campaigns.*"[17]

14. **Other PRC Cyber Attacks**.

- On October 23 "*Suspected Chinese attackers … target*[ed] *organizations across the US, Japan, Taiwan, and South Korea …* [by chaining] *PHP2Shell with a Linux kernel privilege-escalation exploit to root 25 servers, including Palo Alto Networks firewalls linked to US government-affiliated organizations.*"[18] The attack used AI with human supervision, and is ongoing.
- 'Volt Typhoon', known for targeting "*space and satellite services, defense and aerospace technology, and policy research*", used four unknown Cisco faults to seize decryption keys and target "*telecoms firms, government entities, defense contractors, satellite and mission-critical communications providers, MSPs, universities with military ties, and critical infrastructure operators,"*[19] mostly in Hawaii, California and Texas.
- A PRC associated hacking group known as 'SlippyNunchucks' is hijacking the Domain Name System (DNS) "*insecure HTTP communications in Windows versions of Sogou Input Method as part of a surveillance campaign designed to deploy an implant called DarkVigil (aka FDMTP).*" According to cyber security company 'ESET' the campaign started on 1 July 2026 and targets "*organizations and Chinese-speaking individuals in Hong Kong, Thailand, Japan, Vietnam, Oman, and Sri Lanka.*"[20]

16 Sources: philstar Global. Massive cyber attacks hit 23 government, private sites
17 Sources: The Hacker News. Chinese Hackers Use AI-Powered ARTEX to Target Over 200 Organizations Worldwide
18 Source: The Register. Suspected Chinese attackers built a custom PHP2Shell exploit and rooted 25 servers
19 Source: Security Week. Cisco SD-WAN Zero-Day Exploitation Tied to Volt Typhoon's 'Silent Train' Network
20 Source: The Hacker News. China-Aligned Hackers Hijack Sogou Input Method DNS Requests to Deploy DarkVigil Backdoor

© David Swan Consulting 2026

Cyber-Intelligence Report

Russian Cyber Activity

15. **Russian Hackers Execute Destructive Attacks**. "*Bloomberg report documents how two groups directed by Russia's military intelligence agency — the Cyber Army of Russia Reborn (CARR) and its industrial-sabotage offshoot Z-Pentest — have deliberately moved beyond website defacements and distributed denial-of-service (DDoS) disruptions into a more dangerous mode of operations*" destructive attacks. The attacks target Industrial Control Systems (ICS) to cripple "*Western water utilities, food processing plants, factories, and waste treatment infrastructure.*" One of the first destructive attacks was in the small Danish village of Tureby. Hacked "*remotely through an internet-facing industrial control interface,* [the hackers] *silently zeroed out the pressure settings, waited for workers to manually restart the pumps, and then surged the pressure until underground pipes burst. … The same basic vulnerability enabled every documented attack: industrial control devices left connected to the public internet with VNC — Virtual Network Computing software — running on its default port, 5900, protected by nothing more than a weak or default password. That is the entire attack surface. And it is everywhere.*"[21]

16. **Who is The Cyber Army Of Russia Reborn?** *"According to a December 2025 DOJ indictment confirmed by the U.S. Department of Justice, CARR* [The Cyber Army of Russia Reborn] *was founded, funded, and directed by the Main Directorate of the General Staff of the Armed Forces of the Russian Federation — the GRU, Russia's military intelligence agency. … The GRU directed the group's targeting choices and financed access to commercial DDoS-for-hire services through a figure using the handle "Cyber_1ce_Killer," paying for service subscriptions in Russian rubles."*[22]

17. **ESET Warns Belarus Joining Russia's Cyber Forces**. In the APT Activity Report for Q2 and Q3 2026 by cyber security company 'ESET', they identified "*the first destructive cyberattack by a Belarus-aligned threat actor against a critical target in Ukraine, suggesting Belarus may be upping its support for Russian national objectives.*" Belarus's hacking team " '*FrostyNeighbor' deployed Chisel, UltraVNC, Cobalt Strike, and a VBScript wiper via Group Policy against a manufacturing company in Ukraine.*" RUSI(NS) Security Advisory Committee suggests that Belarus may be doing the minimum possible in order to appease Russia.[23]

This cyber-intelligence product is produced by David Swan. It is copyright David Swan 2026. This report is **TLP:CLEAR**[24] and MAY be shared freely.

To unsubscribe from this service send an email to DSC.Ops.Vulcan@gmail.com

21 Source: Tech Times. GRU-Backed Hackers Burst Water Mains and Sparked Factory Fires From Denmark to California

22 Ibid.

23 Source: Dark Reading. As Russia's Cyberwar Evolves, Belarus Steps Forward

24 Definition **TLP: CLEAR.** From U.S. Govt Cyber Defense Agency. Traffic Light Protocol (TLP) Definitions and Usage, Recipients may share this information without restriction. Information is subject to standard copyright rules.

© David Swan Consulting 2026