# Cyber-Intelligence Report

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 2024. 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: Iran's cyber capabilities are improving

This report contains selected cyber-security information from 2nd to 14th November 2024.

### Synopsis

1. Russian attempts to undermine U.S. democracy 'ongoing'. Pro-Russia hackers are now DDoSing South Korea. Iran continues to step up its cyber attacks, targeting IT cameras and more organizations. Iran did manage to block sales at some Israeli gas stations. Israel may have DDoSed Iran's gas stations, again. A pro-Iranian group is using a new version of 'Wiper' malware. China compromises U.S. telecommunications. China rebuilding 'Volt Typhoon' botnet. Exploitation of the MOVEit breach continues.

2. Russia vs Ukraine cyberwar. Russia appears to be committed to the following ongoing 'Course of Action' for its cyber forces:

> Russian cyber forces, including allied and supporting hackers, continue to launch campaigns against Ukrainian targets, **including perceived Ukrainian allies.** Targeting Includes: critical infrastructure, industrial infrastructure, political, and media organizations as well as targets of opportunity.

### Russia vs Ukraine

3. **Russia Ready To Continue Post-Election Tampering.** The U.S. Cybersecurity and Infrastructure Security Agency was concerned that Russia would continue to try and tamper with the U.S. political system following the election. "*The CISA was "very concerned" about the ways foreign adversaries might ramp up their efforts during the election certification period.*" Two videos were attributed to 'Kremlin spin doctors' but were being spread by 'some well-known Republicans'. The threat from Russia appears to be ongoing. "'*The Russians have made clear that they are determined to use disinformation to undermine American democracy. Eight years ago that was through leaked emails and false stories,' said Higgins, a partner at law firm Eversheds Sutherland. 'Now it's through cheap-fake and deep fake videos, including videos falsely alleging election irregularities.'*"[2]

---

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: Defense One. Russia produced fake video of immigrant election fraud in Georgia, officials say

# Cyber-Intelligence Report

4. **Pro-Russian Hackers Attacking South Korea.** Since North Korea's recent deployment of troops to Russia (against Ukraine), the South Korean government has observed more frequent pro-Russian hacktivist attacks. "*The DDoS attacks primarily impact civilian and government sites, ... Some websites experienced temporary outages, but no major damage occurred.*" South Korea's National Intelligence Service's Cyber Crisis Management Division is monitoring and coordinating responses. "*According to The Record Media, pro-Russian hacker groups behind the recent attacks on South Korea includes NoName057(16), Z Pentest, and Alligator Black Hat.*"[3]

**Iran vs Israel**

5. **U.S. Advisory on Iranian Hackers.** On 5th November, the US departments of Justice and Treasury published a joint advisory about an Iranian cyber-operations group, Emennet Pasargad (also known as Cotton Sandstorm). The group is targeting IT assets including IP Cameras. Target areas have expanded to organizations in France and Sweden, a variety of election sites and systems, in addition to targets in Israel and the United States. "*The latest intelligence highlights Iran's increasing use of cyber operations as a way to target its perceived enemies.*" The group's objective appears to be to "*undermine public confidence in Israel and Western nations by using hack-and-leak campaigns and disrupting government services, including elections.*"[4]

6. **Israeli Gas Stations DDoSed.** On 10th November, Israeli company 'Hyp Credit Guard' informed Israeli media "*In the last hour, we experienced a DDoS attack on some of the company's services and the communication providers connected to us. ... At this point, the attack was blocked, and the service returned to normal operation. We are coordinating with all security agencies to ensure continued normal operation.*"[5] The company claims the attack lasted an hour while some customers reported being unable to use their credit cards for several hours. Two media sources "*reported that an Iran-linked hacker group took responsibility for the attack. ... A similar attack last month targeted Israel's credit Automated Bank Services, which said at the time that a DDoS attack caused many bodies connected to the company through the internet to experience disruptions in processing transactions.*"[6] "*In addition to retail outlets, Israeli gas stations have also become frequent targets for cyberattacks [DDoS attacks] on gas stations. Gas stations, which process numerous credit card transactions daily, are critical nodes in the financial ecosystem.*"[7]

7. Analysts Comment: We have seen a number of Iranian claims of cyber attacks on Israel. There have been similar attacks against Israeli gas stations, generally with low or negligible impact. This is one of the few times when claims were supported by reports in Israeli media. This attack was a DDoS attack against the Credit Card company and its Internet Service providers.

3 Source: Security Affairs. A surge in Pro-Russia cyberattacks after decision to monitor North Korean Troops in Ukraine
4 Source: Dark Reading. Iranian APT Group Targets IP Cameras, Extends Attacks Beyond Israel
5 Source: The Jerusalem Post. Credit cards readers across Israeli stores, gas stations crash in cyberattack
6 Source: The Times of Israel. DDoS cyberattack temporarily blocks Israeli credit card payments
7 Source: The CyberExpress. Cyberattack Disrupts Israel's Gas Stations and Payment Systems—Here's What We Know

# Cyber-Intelligence Report

8. **Iranian Gas Stations DDoSed.** On 10th November, Iran's National Oil Products Distribution Company reported a 'technical glitch' disrupted operations at many of Iran's gas stations. "*A statement to Iranian television that the failure was caused by a "technical issue related to the payment system," which led to a significant number of gas stations being unable to operate. ... Bank Mellat, one of Iran's largest banks, later confirmed that the issue with fuel price payments had been resolved, stating that its experts had fixed the technical problem and restored the payment systems to normal operation.*"[8] Analysts Comment: This 'technical glitch' follows the pattern of Israeli cyber attacks against Iranian gas stations. We *assess* that this was most likely another Israeli cyber attack.

9. **Pro-Iranian Hackers Using 'Wiper' Malware.** In October 2024, a Hamas linked hacker group called 'WIRTE' used a 'wiper' malware in cyber attacks against Israel, targeting "*several Israeli organizations, such as hospitals and municipalities*" using a legitimate email address. Known for their espionage attacks, they "*recently engaged in at least two waves of disruptive attacks against Israel. ... The email contained a newly created version of the SameCoin Wiper ... SameCoin is a bespoke wiper that was uncovered in February 2024 as used by a Hamas-affiliated threat actor to sabotage Windows and Android devices. The malware was distributed under the guise of a security update.*"[9]

10. The 'WIRTE' group has been active since at least August 2018. According to 'Check Point Software' they have "*also targeted the Palestinian Authority, Jordan, Iraq, Saudi Arabia, and Egypt. ... The hacking crew is assessed to be part of a politically motivated group called the Gaza Cyber Gang (aka Molerats and TA402). ... This cluster's activity has persisted throughout the war in Gaza.*" According to Check Point, "*Despite ongoing conflict in the Middle East, the group has persisted with multiple campaigns, showcasing a versatile toolkit that includes wipers, backdoors, and phishing pages used for both espionage and sabotage.*"[10]

11. Analysts Comment: These paragraphs illustrate Iran's (and allied organizations) progressive increase in cyber capability. Israel is a skilled cyber defender. Iran's hackers are demonstrating significantly increased capability ranging from the DDoS attacks to the 'SameCoin Wiper' attacks. As pro-Iranian hackers increase their capabilities and target sets, less prepared nations, such as Canada, need to take note.

## China

12. **China Compromises U.S. Telecommunications Networks.** On 13th November, the FBI and US Cybersecurity and Infrastructure Security Agency (CISA) confirmed "*a broad and significant cyber espionage campaign*" conducted by Chinese (PRC) hackers against US telecommunications networks: Verizon, AT&T, and Lumen Technologies. The "*digital assaults resulted in the "theft of customer call records data, the compromise of private communications of a limited number of individuals who are primarily involved in government or political activity, and the copying of certain*

8 Source: Menafn. Technical glitch disrupts operations at several gas stations in Iran
9 Source: The Hacker News. Hamas-Affiliated WIRTE Employs SameCoin Wiper in Disruptive Attacks Against Israel
10 Source: IBID

*information that was subject to US law enforcement requests pursuant to court orders.*" Stated another way, the hackers "*compromised the wiretapping systems used for court-ordered surveillance*" as well as "*targeted phones belonging to people affiliated with US Democratic presidential candidate Kamala Harris, along with Republican president-elect Donald Trump and VP-elect JD Vance.*"[11] The joint statement does not name the attack but analysts are agreed it fits the description of 'Salt Typhoon', a previously identified cyber-attack on U.S. telecommunications.

13. **China Rebuilding Disabled 'Volt Typhoon' Botnet.** 'SecurityScorecard' researchers are reporting that People's Republic of China (PRC) hackers are rebuilding the 'Volt Typhoon botnet' "*using the same infrastructure and techniques.*" In May 2023, Microsoft identified that the 'Volt Typhoon' network had compromised U.S. bases in Guam and had spread globally using U.S. telecommunications networks. Part of the compromise was the creation of a 'botnet' to conceal malicious traffic. "*The threat actor routes [electronic traffic] through compromised small office and home office (SOHO) network devices, including routers, firewalls, and VPN hardware.*"[12] The once neutralized botnet is currently being rebuilt, with CISA warning that the group has been positioning itself within critical infrastructure networks.

**MOVEit Breach ... continued**.

14. A hacker has announced on "*the BreachForums cybercrime forum ... that they had obtained Amazon employee information, including names, phone numbers, email addresses, job titles, and other information related to job role. ... The hacker claimed the data originated from the 2023 MOVEit hack.*" The MOVEit hack exploited "*a zero-day vulnerability in Progress Software's MOVEit file transfer software.*" Launched by the Cl0p ransomware group, nearly 2,800 organizations and nearly 100 million individuals were compromised. Amazon said "*the data came from a third-party property management vendor. ... The hacker claims the Amazon employee database has roughly 2.8 million entries, but it's unclear how many employees are impacted. The same hacker has also leaked data on several other major companies' employees, including BT, McDonald's, Lenovo, Delta Airlines, and HP. The data appears to be the result of the same MOVEit hack impacting the same real estate services company that stored Amazon employee data."*[13]

---



11 Source: The Register. Reminder: China-backed crews compromised 'multiple' US telcos in 'significant cyber espionage campaign'

12 Source: Security Affairs. China's Volt Typhoon botnet has re-emerged

13 Source: Security Week. Amazon Employee Data Leaked by Hacker

14 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.