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 2025. 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: Russia vs Ukraine, PRC Update and AI is Evil

This report contains selected cyber-security information from 24th March to 3rd April 2025.

Synopsis

1. We start by updating the relatively low-level cyber exchanges between Russia and Ukraine. NoName057(16) attacked major Belgian government websites. Russia hacked Ukraine's Railroad operator. Someone's targeting Defense Contractors who support Ukraine. Ukraine targets a Russian ISP, Russia's second largest oil company, and Russian railroads. The U.S. is investigating if banned PRC companies are still operating in the U.S. An old PRC hacking group has re-emerged. And from the headlines, two AI is Evil stories and a trusted Elon Musk staffer in DOGE has supported cyber-criminals.

2. It is our *assessment* that the three major cyber conflicts, (Russia vs Ukraine, Iran vs Israel, and the People's Republic of China) are the most likely sources for the creation of next generation malware and/or a primary source of cyber attacks. This includes government funded hackers (military, intelligence and civilian employees), affiliated hackers (criminals and mercenaries), and volunteer 'supporters'.

Russia vs Ukraine

3. **NoName057(16) Attacks Belgian Government.** On 24th March, NoName057(16) DDoS attacked "*several major Belgian websites including MyGov.be … as well as the platform of the Walloon Parliament.*" One source said that some sites were 'taken down', "*however, most of those sites appear to be functioning again.*" The attack was described as "*a relatively harmless DDoS attack.*" The justification for the attack was "*a new aid package of 1 billion euros from Belgium for Ukraine.*"[2]

4. **Ukraine's Railway Operator Hacked.** On 25th March, there were multiple reports of a cyber-attack against Ukraine's national railway operator, Ukrzaliznytsia hitting both passanger and freight services. Online ticket sales were disrupted, forcing the use of physical tickets. According to the operator: "*The key objective of the enemy was not achieved: train movement is stable, running on time without delays, and*

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: belga News Agency. Pro-Russian hackers attack Belgian government websites

all operational processes are running in backup mode. The railway continues to operate despite physical attacks on infrastructure, and it cannot be stopped even by the most insidious cyberattacks."[3] The attack was described as: "*highly systematic, non-trivial, and multi-layered."* The company also said: "*Some railway sections lost power, but trains keep running,"*[4]

5. Analysts Comment: The restoration of data from backups, along with the fact some 'sections lost power', suggests this was more than a Distributed Denial of Service Attack (DDoS). Regardless, the railway was NOT shutdown. Restoration of services appears to have commenced within hours. Reuters reported that online services were 'partially restored' by 27th March.[5]

6. **Defense Contractors Supporting Ukraine Being Phished.** A large-scale phishing campaign targeting Defence Contractors supporting Ukraine has been identified. Analysis from DomainTools Investigations reports "*nearly 880 spoofed domains of worldwide IT, defense and aerospace firms between December and March."* DomainTools spokesperson declined to provide details, but stated "*There is insufficient evidence to attribute this activity to a known actor; however, the activity likely has a cyber espionage motivation."*[6]

7. **Russian ISP 'Lovit' Hacked.** Also on the 25th, the Ukrainian IT Army, a volunteer hacker group, announced that it had taken down Russian Internet provider 'Lovit'. Apparently services were interrupted in Moscow and St Petersburg for three days, starting Friday. "*The attack targeted the company's critical infrastructure and online systems, affecting Lovit's mobile app, website and user accounts. ... also prevented residents of apartment buildings using Lovit's services from accessing their homes, as it disabled intercom systems. Businesses in affected buildings reported failures in payment terminals and loyalty programs, ... Roskomnadzor said Lovit was unprepared for such a large-scale incident. As of Monday, the attack was still ongoing. ... "*[Lovit] *is the sole provider to most newly built residential complexes by PIK, making it possible to inflict maximum damage, the company told local media."*[7]

8. **Russia's Number Two Oil Company Hacked.** Microsoft reports that on the 26th March, the Russian oil company 'Lukoil' was hacked. "*Lukoil employees were unable to access their work computers, with the screen displaying a strange message about a malfunction, eerily resembling a hack. ... Lukoil is one of the largest Russian oil companies, the second in Russia in terms of oil production. ... After a similar attack last year, it took about three days to restore the system."*[8]

9. **Russia's Railroads Hacked.** On March 31, the Moscow Metro website displayed a message from Ukrzaliznytsia (UZ), Ukraine's state railway company reading: "*The application and ticket sales website have been restored, but disruptions in their work are still possible. We are currently stabilizing the systems."* On 1st April "*Russia's*

3 Source: Security Affairs. A Cyberattack hits Ukraine's National Railway Operator Ukrzaliznytsia
4 Source: Info Security. Ukraine Railway Systems Hit by Targeted Cyber-Attack
5 Source: Reuters. Ukraine state railway says online services partially restored after cyber attack
6 Source: NextGov. Phishing campaign seeks to siphon Ukraine war intelligence from defense contractors
7 Source: The Record. Lengthy disruption of Russian internet provider claimed by Ukrainian hacker group
8 Source: Microsoft. Russian oil giant blocked by a cyber-attack

state-owned railway company, Russian Railways (RZD), reported a massive DDoS attack that took down its official website and mobile application."[9] Service was restored that afternoon. Analysts Comment: Both attacks appear to be 'nuisance attacks' designed to embarrass the Kremlin. Taken together with the DDoS attack on the Russian Lovit ISP – and previous attacks, there appears to be an ongoing effort to disrupt 'Russia's normal way of life'.

PRC

10. **Banned PRC Telecom Companies *MAY* Still be Operating In U.S.** For several years the government has been removing PRC companies such as Huawei, ZTE, Hikvision, Hytera, Pacifica Networks, Dahua, China Mobile, China Telecom, and China Unicom from U.S. Telecommunications, based off concerns that they were/could spy for the PRC.[10] "*Government funding for their products and services has been cut off, they have been banned from operating in the country, and the FCC has invested billions of dollars in a 'rip-and-replace' program whose goal is to help small telecom firms replace equipment made by Chinese companies.*" FCC Chairman Brendan Carr said "*We have reason to believe that, despite those actions, some or all of these Covered List entities are trying to make an end run around those FCC prohibitions by continuing to do business in America on a private or 'unregulated' basis,*"[11]

11. **PRC Hackers 'FamousSparrow' Back In Action.** Active since at least 2019, the 'FamousSparrow' hacking group became infamous for its hacking of hotel networks, particularly in Asia. They also targeted "*governments, international organizations, engineering companies, and law firms.*" After the group was exposed, it *appeared* to go 'inactive'. While investigating compromises in a US financial-sector trade group and a Mexican research institute, 'ESET', a cybersecurity company, discovered signature 'FamousSparrow' tools. "*The deployed payloads are new versions of SparrowDoor, a backdoor that appears to be exclusive to this group. While these new versions exhibit significant upgrades in code quality and architecture, they can still be traced back directly to earlier, publicly documented versions.*"[12]

12. Ongoing investigations now suggest that 'FamousSparrow' was busy conducting cyber-espionage between 2022 and 2024. Victims included 'a governmental institution in Honduras' as well as a research organization in Mexico. Microsoft has linked 'FamousSparrow' to the 'Salt Typhoon' hacking group, but has not explained why they have linked them.[13] Cybersecurity company 'Trend Micro' has also linked the groups. Analysts Comment: (1) Hackers are sometimes linked because of common computer code in malware and/or shared command and control systems. (2) The ability of FamousSparrow to: 'go dark', resume cyber-espionage operations, develop new tools and resume dynamic operations says a lot about how much funding the PRC is pouring

9 Source: Kyiv Post. Russian Railways Hit by Cyberattack – Website, App Knocked Offline
10 Employees of some of these companies such as 'Huawei' have been indicted for spying.
11 Source: Despite Rip-and-Replace Efforts, FCC Suspects Banned Chinese Telecom Providers Still Active in US
12 Source: welivesecurity. You will always remember this as the day you finally caught FamousSparrow
13 Source: The Register. China's FamousSparrow flies back into action, breaches US org after years off the radar

into its cyber operations. The complexity of the work, skill sets required and scope of operations suggest there are at least dozens of highly skilled hackers involved, who have deep technical resources supporting them.

From Headlines

13. **AI used for Evil.** The Register is reporting "*Criminal networks have evolved into global, technology-driven criminal enterprises, exploiting digital platforms, illicit financial flows and geopolitical instability to expand their influence,*" Europol executive director Catherine De Bolle said. "*The same qualities that make AI revolutionary – accessibility, adaptability and sophistication – also make it a powerful tool for criminal networks, … Organized criminals are rapidly adopting AI to automate tasks, expand operations at scale, and stay a step ahead of law enforcement by making their activities harder to detect.*"[14]

14. **AI Supports the Zero-Knowledge Threat Actor.** "*Research from Cato CTRL demonstrated how almost anyone, with no experience in malware coding, can manipulate LLMs like OpenAI's ChatGPT, Microsoft Copilot and DeepSeek, to override these guardrails, and conduct malicious activities like developing an infostealer malware.*"[15] Stated another way, a person who has passable skills using AI, can leverage AI to become a wizard hacker and cyber-criminal.

15. **Elon Musk DOGE Staff Provided Tech Support To CyberCriminals**. Edward Coristine is among the most visible members of Elon Musk's DOGE staff. Musk has 'championed' the nineteen year old on 'X', saying "*Big Balls* [his Internet alias] *is awesome.*" Reuters saw corporate and digital records showing "Coristine ran a company called DiamondCDN that provided network services," … including "*a website run by a ring of cybercriminals operating under the name "EGodly,*"[16] On Feb. 15, 2023, "*EGodly thanked Coristine's company for its assistance in a post on the Telegram messaging app. … We extend our gratitude to our valued partners DiamondCDN for generously providing us with their amazing DDoS protection and caching systems, which allow us to securely host and safeguard our website,*"[17]

---

14 Source: The Register. Mobsters now overlap with cybercrime gangs and use AI for evil, Europol warns

15 Source: Security Week. AI Giving Rise of the 'Zero-Knowledge' Threat Actor

16 Source: USA Today. Exclusive: DOGE staffer, 'Big Balls', provided tech support to cybercrime ring, records show

17 Source: Reuters. Exclusive: DOGE staffer, 'Big Balls', provided tech support to cybercrime ring, records show

18 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.