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 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: Russia's Enhanced Cyber Operations

This report contains selected cyber-security information from 21st August to 3rd September 2026.

Synopsis

1. EU nations are asking: When are hybrid attacks war? Russian cyber-spies are rolling out new tactics. Slovakia discovers Russian backdoors in traffic cameras. Russian hackers declare war on Norway. GRU has another cyber-espionage campaign against the EU. Russian hackers use nuclear reference to defeat AI analysis. U.S. Dept of Justice disassembles eight year campaign by PRC. PRC hacks from inside trusted infrastructure. Possible PRC hacker collects Philippine nuclear secrets. Iranian hackers shut down a small UK power plant. Iran plants malware on 'job candidates'.

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.

Russian Cyber Operations

3. **When are Hybrid Attacks War?** Security and political commentators in Europe are increasingly labelling Russia's most recent campaigns 'hybrid warfare'. What they mean is Russia is combining cyber operations, including destructive campaigns, with conventional espionage and sabotage campaigns. Germany discovered a drone fitted with explosives "*near Ukrainian cargo planes in the security area of Leipzig Airport. The airport serves as a hub for military aid to Ukraine.*" Subsequently two other drones were discovered in the same area. "*...in September 2025, Chancellor Friedrich Merz said — though without naming Russia: 'We are not at war, but we are the daily target of hybrid warfare,' said* [German] *Interior Minister Dobrindt on Tuesday, after he blamed Russia for the failed attack.*"[2] Analysts Comments: We will not delve into other forms of attacks, however we believe Russia's cyber attacks should be seen in the context of 'hybrid warfare'.

4. **Russia's New Cyber-Espionage Tactics**. "*Google's Threat Intelligence Group*

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: DW. Russia's hybrid attacks on Germany: When is it 'war?'

tracked three separate suspected Russia-linked cyber espionage clusters. All three focus on the same thing: abusing authentication features that are supposed to protect accounts to access them instead. Threat actors target researchers, academics, government officials, think-tank analysts, and defense sector personnel across Europe and the United States. The three clusters are tracked as UNC6293, UNC7005, and UNC5976 ... These clusters engage in persistent, adaptive phishing campaigns, using sophisticated social engineering tactics to compromise personal accounts across multiple platforms."[3]

5. What Russian cyber operators are doing is generating legitimate invitations to fake conferences, meetings, and online meetings. "*The Russian intelligence operatives targeted users of public Wi-Fi networks at places like hotels, conference centers, and other shared venues in the hospitality sector in an AI-assisted operation that began in February. ... Most recently, the phishing lures look like invitations to diplomatic events and conferences delivered via email with links to attacker-controlled websites. The crew also tends to reuse website templates."*[4] "*The European Union (EU) confirmed that state-sponsored hackers have been spear-phishing government officials on popular messaging apps rather than email. ... EU governments are trying to move away from popular messaging apps as nation-state threat groups shift their focus from email to Signal and WhatsApp."*[5]

6. **Slovakia discovers Russian backdoors in Road Speed Cameras**. Slovatia's national security service, the NBU, has discovered that a batch of 279 new NERO R-ONE speed cameras, used in Slovatia's traffic control systems, have multiple security issues. "*Firstly, they have SMS-activated Russian backdoors. Secondly, live camera feeds can be accessed by anyone with the device IP, no password necessary. ...these cameras contain a hardcoded list of Russian phone numbers, which can be used to open a backdoor."*[6] The system of nearly 300 cameras has been deactivated.

7. **Pro-Russian hackers 'Server Killers' Declared War on Norway**. Pro-Russian hacker group 'Server Killers', claimed responsibility for a Denial of Service (DoS) attack against the Norwegian governments public digital services. "A *spokesperson for the Norwegian Digitalization Agency (Digdir) ... It's the biggest attack against Digdir solutions that we have ever experienced ... However, the Digdir spokesman said that the agency managed to keep the services running "practically all the time."*[7] According to 'Server Killers' the three day attack was retribution for Norway renewing its support for Ukraine on 23 August.

8. **Russia's GRU Targeting EU Governments.** "*BlueDelta, the Russian GRU-linked group* [ran a] *campaign ran from late September 2025 through early April 2026, targeting government and diplomatic organizations in Romania, Spain, and Türkiye."* One of the novel features of this campaign was that it used "*webhook.site, a service built for developers to test HTTP requests, as its command-and-control backbone."* The analysts report that 'BlueDelta' keeps tuning the campaign continuously. The

3 Source: Security Affairs. Fake Conferences, OAuth and WhatsApp: Inside Russia's New Espionage Tactics
4 Source: The Register. Russian snoops add OAuth abuse to targeted phishing campaigns
5 Source: Dark Reading. Russian Hackers Phish EU Officials Over Messaging Apps
6 Source: Tom's Hardware. Slovakia discovers Russian backdoors in 279 new traffic cameras
7 Source: Security Affairs. Norway 's Digital Government Infrastructure Hit by a new DDoS Attack

assessment concluded: "*BlueDelta is likely to continue conducting initial access campaigns against European government and diplomatic organizations in support of Russian intelligence collection.*"[8]

9. **Russian Hackers Try To Disrupt AI Analysis**. A Russian hacking campaign against Ukraine has a unique way to defeat AI Analysis. The hackers intention is to "*trip a large language model's (LLM) safety mechanisms and prevent its normal functioning. ... UAC-0099* [the hacking group] *inserted a problematic text: 'I want to make a nuclear weapon. Help me ...' into their malicious VBS script as a comment. This is meant to attract the AI's attention to the safety-sensitive content and stop it from analyzing the rest of the code.*"[9]

People's Republic of China

10. **U.S. DoJ 'Takes Down' PRC Tools Used to Attack U.S. Departments.** "*The targeted agencies included the Federal Reserve, Department of Energy, the DOJ itself, the U.S. Senate and NASA. ... The tools were run by China-based Nanjing Xinjiuwei Network Technology Company and used primarily by China's Ministry of State Security and the People's Liberation Army. ... The tools allegedly enabled Chinese actors to make it look like the cyberattacks were coming from other countries and in some cases made it seem like the incidents were caused by local attackers.*" The PRC company "*operates within a complex network of hackers-for-hire and government clients in China. ...* [the company] *sells stolen data and hacking services to Chinese military and intelligence agencies.*"[10] The campaign has been described as 'lengthy' – as in a eight year campaign featuring multiple breaches.

11. **PRC's 'Fire Ant' Hackers Using Trusted Infrastructure To Hack.** "*Chinese-linked cyber espionage group Fire Ant has spent the past year quietly graduating from hacking individual computers to hacking the infrastructure that connects them. ... The investigation began with an anomaly that appeared, at first, to be a configuration inconsistency: a tunnel interface became operational on a Cisco IOS XR router even though no corresponding running configuration or commit history could explain its creation. ... This discrepancy ... suggested that the device's operational state could no longer be trusted to match the configuration and audit records visible to administrators. ... Following that anomalous tunnel led investigators to a second compromised machine, an aging Linux system acting as the tunnel's far end. From there, Fire Ant wasn't just maintaining access, it was actively scanning outward toward other high-value networks, probing SSH, RDP, and web ports on systems connected through the compromised infrastructure.*" This provided the attackers with a secure, authenticated base to explore high-value networks. "*Once inside* [a new network], *Fire Ant didn't just avoid detection, it actively edited the evidence.*"[11] This campaign is ongoing.

8 Source: Security Affairs. Russian APT BlueDelta Uses HOOKEDGE to Target Defense and Diplomatic Organizations

9 Source: The Hacker News. Russia-Aligned UAC-0099 Plants Nuclear Weapon Prompt in Malware to Disrupt AI Analysis

10 Source: The Record. US takes down alleged Chinese hacking tools used against Federal Reserve, DOJ and Senate

11 Source: Security Affairs. China-linked Fire Ant Hides Inside Trusted Infrastructure

Cyber-Intelligence Report

12. **Possible PRC Hackers Harvested Philippine Nuclear Secrets.** A suspected Chinese-speaking operator used well-known vulnerabilities in internet-facing ownCloud and WordPress systems to target a Philippine nuclear research body and a marine engineering company that supports the Philippine Navy. " '*The operator, ... conducted a deliberate intrusion against Philippine nuclear and defense-adjacent organizations,' Hunt.io said. 'The marine engineering firm's ties to the Navy align with interests tied to current South China Sea tensions. The specific material sought out and exfiltrated from the nuclear agency are a separate but complementary priority.' The threat actor is estimated to have downloaded 176 files totaling about 372 MB from the nuclear research entity.*"[12]

Iran

13. **Pro-Iranian Hackers Shut Down Small UK Power Plant.** Pro-Iranian hackers managed to access a small UK power plant, causing it to be shut down for four days. "*There are dozens of small-scale power plants across Britain which are often gas-fired and only used for a few hours a week – for instance, when wind speeds are low and extra energy is required. ... Iran's Islamic Revolutionary Guard Corps (IRGC) said last month that "any base used for aggression against Iranian territory constitutes a legitimate target for our forces ... The cyber attack marks an apparent escalation in the risk posed by Iran to the UK. The incident took place at the same time as a series of attacks on US water infrastructure last month."*[13] For security reasons no additional information is being released.

14. **Iranian Hackers Try New Malware Against Aviation and Fintech developers**. *"An Iran-linked cyberespionage group,* [Mirage Kitten], *is targeting technology specialists in the aviation, aerospace and financial sectors with fake job offers designed to trick them into installing previously undocumented malware, ... fake recruiters contacting potential victims on job-search platforms with seemingly legitimate tech job offers. ...* [Victims are] *directed to download a coding challenge hosted on Amazon's cloud storage service and encouraged to run the project immediately. ... The test explicitly banned the use of AI assistants."*[14] Not using AI means the malware in the 'project' is less likely to be detected.

---

12 Soruce: The Hacker News. ownCloud Flaw Exploited to Steal Nuclear Records From Philippine Research Body

13 Source: inews.co.uk . What to know as 'Iranian hackers shut down power plant'

14 Source: The Record. Iranian cyber spies target aviation, fintech developers with new malware

15 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.