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:

This report contains selected cyber-security information from 17th to 30th April 2026.

Synopsis

1. In this report: a detailed look at Russian hackers and cyberespionage. Leaked database provides an inside look at Russian criminal hackers. ATP28 gets busy: hacking Ukraine as well as a global hack of routers and DNS. Russia's Internet regulator takes it's banks offline? Bitcoin exchange hacked for 1 billion rubles. Unknown (Russian?) hackers target Ukrainian hospitals and healthcare. Russia targets German lawmakers and surges cyberattacks against the UK.

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.

Are Ransomware Attacks Going to Increase or Decrease?

3. **'Outage' Hits Russian Banking Apps:** A major outage on Friday, 3 April disrupted banking apps and payment systems from some of the Russia's largest banks, including Sberbank, VTB, Alfa-Bank, T-Bank and Gazprombank. "*Local media reported the outage also caused problems for ATMs and public transport systems. Turnstiles in the Moscow metro and suburban trains reportedly stopped accepting bank cards, forcing metro staff to allow passengers through for free to prevent crowding. ... The exact cause of the outage remains unclear, but several Russian media outlets, including Forbes Russia, initially suggested it could be linked to government attempts to block internet resources, specifically the blocking of IP addresses used in banking infrastructure. ...This is not an enemy raid or an attack by external actors or malicious foreign hackers," she wrote. "This is our very own Roskomnadzor [*Russia's Internet regulator*] finally getting serious about fighting traffic tunneling and protection services, also known as VPNs."*[2]

4. **Russia Hit By Surge In Cyberattacks.** "*Russia's communications regulator, Roskomnadzor (RKN), has reported an unprecedented spike in cyberattacks targeting*

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 Record. Major outage hits Russian banking apps, metro payments across regions

the country's information resources in February and March, ... RKN data shows that the bulk of malicious traffic originated from the United States, Germany, and the United Kingdom. ... While RKN typically records around 350 attacks per week, the period from February 26 to March 4 saw the total number of attacks rise sharply to 949. Monitoring between March 16 and 22 indicated that the US accounted for 37.6% of cyberattack traffic, followed by Germany with 15.2% and the UK with 11.1%."[3]

5. **Russia's ATP28 Hacked Routers and Hijacked DNS.** "*The US Justice Department and the FBI ... disrupted a network of hacked SOHO routers that Russia used in an espionage operation ...* [operated] *by Russia's General Staff Main Intelligence Directorate (GRU). ... The hackers targeted vulnerable TP-Link and MikroTik routers, changing their DHCP and DNS settings so that traffic from devices connected to these routers would go through the attackers' infrastructure. ... if users ignored invalid TLS certificate warnings triggered by the use of the attacker-controlled infrastructure ... the cyberspies captured traffic the victim would assume was encrypted, harvesting passwords, authentication tokens, emails, and web browsing data."*[4] One of the espionage targets was to mass harvest Microsoft Office authentication tokens. "*The spying campaign allowed state-backed Russian hackers to quietly siphon authentication tokens from users on more than 18,000 networks without deploying any malicious software or code."*[5] When ATP28 had a campaign detected in August 2025, they immediately switched tactics. Cybersecurity analysts say they are 'interested' in seeing APT28's response this time.

6. **APT28 Also Running PRISMEX Spear-Phishing Campaign.** In addition to hacking routers, ATP28 is running another campaign against Ukraine and its allies. The targets are "*government, military, and critical infrastructure in Central and Eastern Europe.*" The campaign is using "*the PRISMEX malware suite, combining a dropper, loader, and implant based on the Covenant framework to enable stealthy, fileless attacks and encrypted command-and-control. ... The campaign shows a clear strategy: disrupt Ukraine's supply chain and operational planning, while extending access to NATO-linked logistics. ... The operation reflects a shift toward tactical disruption rather than pure espionage."*[6] 'Trend Micro's' blog report says "*The campaign's infrastructure preparation was observed to have begun two weeks prior, hinting of the group's advanced knowledge of the* [Microsoft Windows] *vulnerability."*[7]

7. **Ukrainian Healthcare and Hospitals Targeted.** Ukraine's Computer Emergency Response Team (CERT-UA) has identified a campaign "*targeting Ukrainian government entities and municipal healthcare facilities, including clinics and emergency hospitals.*" The identity of the attacker is threat actor UAC-0247, whose affiliation is unclear, however they appear to be conducting cyber espionage. "*Targets include Ukrainian Defense personnel. ... CERT-UA experts analyzed multiple incidents,*

3 Source: caliber.az . Russia experiences record surge in cyberattacks, majority traced to US, Europe
4 Source: Security Week. US Disrupts Russian Espionage Operation Involving Hacked Routers and DNS Hijacking
5 Source: Krebs on Security. Russia Hacked Routers to Steal Microsoft Office Tokens
6 Source: Security Affairs. Russia-linked APT28 uses PRISMEX to infiltrate Ukraine and allied infrastructure with advanced tactics
7 Source: Trend Micro. Pawn Storm Campaign Deploys PRISMEX, Targets Government and Critical Infrastrure

discovering that attackers stole credentials from browsers using CHROMELEVATOR and from WhatsApp via ZAPIXDESK, while also conducting reconnaissance and lateral movement within networks."[8] Preventative measures to inhibit the malware have been published. Analysts Comments: Based on the targeting of Ukrainian defence personnel, the most likely attacker is Russia or a Russian affiliated hacking group.

8. **Sanctioned 'Grinex' Bitcoin Exchange Hacked, Shutting Down.** Grinex, a Kyrgyzstan-incorporated cryptocurrency exchange, associated with Russian cyber activity, "*said it's suspending operations after it blamed Western intelligence agencies for a $13.74 million* [USD] *hack.*" The company said "*Digital forensic evidence and the nature of the attack point to an unprecedented level of resources and technological sophistication ... Preliminary findings suggest the attack was coordinated with the specific objective of inflicting direct damage upon Russia's financial sovereignty. ... Grinex is believed to be a rebrand of Garantex, a cryptocurrency exchange that was sanctioned by the U.S. Treasury Department in April 2022 for laundering funds linked to ransomware and darknet markets like Conti and Hydra. The Treasury renewed sanctions against Garantex in August 2025 for processing more than $100 million in illicit transactions and enabling money laundering.*"[9]

9. **German Lawmakers Targeted In 'Signal' Cyberattacks.** "*Germany, Kyiv's biggest provider of miliary aid, has been battling a surge of cyberattacks, as well as espionage and sabotage plots since Russia's full-scale invasion of Ukraine in 2022.*" On Friday, 24 April, German prosecutors "*launched a spying investigation into phishing attacks targeting lawmakers on the Signal messaging app ... based on an initial suspicion of espionage. ... The wave of attacks has allegedly been directed at lawmakers ... from several parties including the speaker of Parliament, a senior member of Chancellor Friedrich Merz's CDU party, as well as civil servants, diplomats and journalists. ... When the scam is successful, the hackers gain access to photos and files shared on Signal and can also impersonate the person whose account was compromised.*"[10] The attack and investigation are ongoing.

10. **Russia Maintaining Surge In Cyberattacks On UK**. A think tank focused on national security issues in Britain has found "*cyberattacks targeting the United Kingdom's infrastructure surged dramatically—by as much as 1,586%—following the outbreak of the Russia–Ukraine War in 2022.*" The report says this is not a 'one time spike' but a a trend that intensified "*as the UK increased its political, military, and cyber support to Kyiv.*" Britain's active support for Ukraine "*through defense assistance, intelligence sharing, and cyber capabilities ... has made the UK a focal point for retaliatory cyber operations. ... Nearly two-thirds of all observed cyberattacks were directed at NATO member states. Among the eight countries analyzed, the United Kingdom emerged as the most frequently targeted.*"[11]

11. **Russia's Criminal Hackers Marketplace 'RAMP' Exposed.** It is well documented that Russia is a 'sanctuary' country for criminal hackers. In addition to

8 Source: Security Affairs. From clinics to government: UAC-0247 expands cyber campaign across Ukraine
9 Source: The Hacker News. $13.74M Hack Shuts Down Sanctioned Grinex Exchange After Intelligence Claims
10 Source: Courthousenews. Germany launches spying probe into Signal attacks targeting lawmakers
11 Source: Cybersecurity Insiders. Russia Cyber Attacks increased by 1500 percent on UK in a Year

being a home for criminal hackers, Russia hosts infrastructure essential to the hacker environment. One piece of that infrastructure is 'RAMP' a virtual marketplace that "*functioned like a business platform where criminals could sell access, recruit affiliates, advertise ransomware, and negotiate deals in private.*" A cybersecurity company 'Comparitech' "*gained exclusive access to a leaked database from RAMP. The full MySQL dump contains user records, forum threads, private messages, IP logs, and admin activity spanning November 2021 through January 2024. ... The scale is significant. Comparitech's analysis found 7,707 registered users, 1,732 forum threads, 340,333 IP log records, 1,899 private conversations, and 3,875 private messages. In other words, this was not a small corner of the internet. It was a large criminal marketplace with a lot of movement and a lot of participants.*" The forums are also used to recruit new hackers.

12. "*The leak also shows what kinds of organizations were being targeted. RAMP listings included defense contractors, banks, hospitals, energy companies, technology firms, and government agencies across more than 20 countries. ... The United States was the top target. It appeared in 40% of listings where a country could be identified. Government agencies were the most targeted sector, with 21 listings, followed by finance and banking, and technology and telecom, each with 11 listings.*" Ransomware actors in RAMP "*are targeting organizations that are likely to be pressured into paying because they cannot afford downtime, data loss, or public exposure.*"[12] NoName057(16) are users of RAMP.

13. Analysts Comments: **Government Hacking Teams:** We *assess* that there has been a consolidation of personnel into the most 'productive' teams such as ATP28. We *assess* Russia has refined its cyber targeting, attempting to increase the tactical impact(s) of its hacking. We *assess* that the sophistication and number of pro-Russia cyberattacks will continue to increase in the near to medium term.

14. **Pro-Russian Criminal Hackers.** The hack of the 'RAMP' forum exposes a highly organized and complex collective, visibly operating under the direction of the Russian government. We *assess* it will continue to grow in numbers and capability as long as it remains protected and supported by the Russian government. Pro-Russia criminal hackers will be an increasingly potent threat.

15. **Weak On Defence.** The Russian government remains weak on cyber defence, trying to control its Internet, while facing an increasing number of sophisticated attacks. We *expect* to see more cyber incursions resulting in Russian business failures.

---

12 Source: Security Affairs. RAMP Uncovered: Anatomy of Russia's Ransomware Marketplace

13 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.