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: The Evolution of Cybercrime … Continued

This report contains selected cyber-security information from 14th to 27th November 2025.

Synopsis

1. Continuing with the evolution of cybercrime: "Russia-linked crooks bought a bank for Christmas to launder cyber loot", Trend Micro reports that some cyber scams are now powered by AI, PRC hackers have added AI operated cyber espionage to their inventory, and Businesses don't seem to be learning. Another PRC cyber-campaign uncovered. The PRC is hacking their own organizations. A Russian port operator was hacked and NoName057(16) DDoSes Denmark. Iran learns digital targeting. Iranian hackers are targeting families to increase pressure on victims.

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'.

The Evolution of Cybercrime

3. **Russian Cybercriminals Bought A Bank To Launder Their Loot**. The UK's National Crime Agency (NCA) traced the 'dirty cash' "*from drugs, firearms, and immigration crime*" from at least 28 UK towns and cities to a Russian linked money laundering network. On Christmas day 2024 that Russian criminal network purchased "*a controlling stake in a Kyrgyzstan bank.*" That bank, Keremet, "*was later identified as facilitating cross-border payments for Promsvyazbank, the Russian state-owned lender that bankrolls companies in the military-industrial base.*" NCA analysts say this is "*the heart of a global ecosystem that links street-level offending to sanctions evasion, Russian state activity, and cybercrime.*"[2]

4. "*The NCA says Altair Holding SA – a company linked to TGR boss Rossi – bought a 75 percent stake in Keremet Bank on December 25, 2024. Keremet was then used to route payments for Promsvyazbank and companies supplying Russia's military sector. Also circling the scheme was Ilan Shor, a Russian-Moldovan oligarch involved in a*

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. Russia-linked crooks bought a bank for Christmas to launder cyber loot

© David Swan Consulting 2025

Cyber-Intelligence Report

string of sanctions-busting payment platforms, including A7, which launched a rouble-backed crypto token designed to enable cross-border transfers beyond the reach of Western restrictions. The NCA says Smart's operators even worked with individuals linked to Russian intelligence services, including a UK-based Bulgarian group led by Orlin Roussev, later convicted of spying across Europe on Moscow's behalf. The networks also helped Russian clients illegally move money into the UK to invest."[3]

5. **Cyber Scams Now Powered By Artificial Intelligence (AI)**. There has been speculation that hackers have been using AI to "*make old scams faster, smarter, and more convincing than ever.*" Trend Research reports "*cybercriminals are using AI to supercharge scam operations, making them easier to run and harder to detect. ... criminals are using GenAI to produce text, images, video, and voices that, when combined, can become a well-coordinated and automated scam operation through the replication and investigation of an AI-powered scam assembly line.*" The documentation shows the automation process using a legitimate process manager called n8n. "*Together, these technologies create a self-sustaining fraud ecosystem, one that operates around the clock, scheduling posts, promoting deals during peak shopping hours, and responding instantly to buyers, all without human oversight.*"[4]

6. **PRC Operating AI-Controlled Cyber-Espionage Campaign**. PRC hackers used "*(AI) technology developed by Anthropic ... to an unprecedented degree – using AI not just as an advisor, but to execute the cyber attacks themselves.*"[5] The result was attacks on "*about 30 global targets spanning large tech companies, financial institutions, chemical manufacturing companies, and government agencies.*" Some of the attacks were successful. "*Anthropic said the threat actor turned Claude into an 'autonomous cyber attack agent' to support various stages of the attack lifecycle, including reconnaissance, vulnerability discovery, exploitation, lateral movement, credential harvesting, data analysis, and exfiltration.*" In a new twist, the hackers had the AI document the attacks so the successful results could be handed off to a human team for further exploitation. "*Anthropic has since banned the relevant accounts and enforced defensive mechanisms to flag such attacks.*" Anthropic has discovered, and disrupted, another sophisticated attack. "*Over the past two months, OpenAI and Google have also disclosed attacks mounted by threat actors leveraging ChatGPT and Gemini, respectively.*"[6]

7. **Businesses Don't Seem to Be Learning**.

> **80 percent of IT leaders overestimate cybersecurity readiness**
> "*The survey of 600 leaders across industries finds 80 percent of cybersecurity and IT decision-makers claim they can detect and contain a cyber incident in under eight hours. ... External benchmarks ... show attackers dwell inside environments undetected for an average of 181 days and breaches take 60 days to contain.*"[7]

3 Source: The Register. Russia-linked crooks bought a bank for Christmas to launder cyber loot
4 Source: Trend Micro. Reimagining Fraud Operations: The Rise of AI-Powered Scam Assembly Lines
5 Source: Anthropic. Disrupting the first reported AI-orchestrated cyber espionage campaign
6 Source: The Hacker News. Chinese Hackers Use Anthropic's AI to Launch Automated Cyber Espionage Campaign
7 Source: betanews. 80 percent of IT leaders overestimate cybersecurity readiness

© David Swan Consulting 2025

Cyber-Intelligence Report

43% of businesses experienced a cyberattack in past year
"*Recent (UK) government figures reveal that 43% of businesses reported experiencing a cyber breach or attack in the past year.*"[8]

Ontario And Alberta Investigation Finds Inadequate Safeguards In PowerSchool Student Data Breach
"*The regulators conclude that PowerSchool and several Ontario [and Alberta] school boards did not have adequate safeguards and oversight in place for the personal information of students and staff that was compromised in the incident.*"[9]

People's Republic of China (PRC)

8. **PRC's APT24 Continues Three Year Cyber-Espionage Campaign**. A PRC hacking group known as APT24 and sometimes 'Pitty Tiger' is using a malware called 'BADAUDIO' to establish persistent remote access to compromised networks. Historically they have targeted "*government, healthcare, construction and engineering, mining, non-profit, and telecommunications sectors in the U.S. and Taiwan*"[10], stealing the intellectual property that makes organizations competitive. Recently APT24 has pivoted, using supply chain attacks targeting organizations in Taiwan. The attacks include breaching a Taiwanese digital marketing firm, effectively hijacking more than 1,000 domains.

9. **PRC's Campaign To Hack Chinese Organizations**. 'PlushDaemon' is a PRC Hacking group that has been targeting Chinese organizations that use popular Chinese software products. The compromised products are: "*the Sogou Pinyin Method input editor, the Baidu Netdisk cloud service, multipurpose instant messenger Tencent QQ, and the free office suite WPS Office.*" Researchers at ESET report that PlushDaemon "*hijacks network traffic using a specially designed implant, re-routes legitimate software update requests to its own infrastructure, and then serves victims malicious substitutes. ... The majority of PlushDaemon's victims have been in mainland China or Hong Kong, such as one Taiwanese electronics manufacturer located in the mainland, and a Beijing university. Other targets have come from Taiwan, Cambodia, New Zealand, and the US.*"

Russia

10. **Russian Port Operator Hit With Multi-Day DDoS Attack**. On 14 November Russian Port Operator 'Port Alliance' said it was in day three of a multi-day DDoS attack targeting its critical infrastructure. Port Alliance reported "*the hackers used a botnet of more than 15,000 unique IP addresses from around the world — including some within Russia — and continuously changed tactics to evade security defenses. ... All key systems remain operational, and port and terminal business processes have not been affected … Port Alliance operates six maritime terminals along key transport routes, with an annual cargo turnover of coal and mineral fertilizers exceeding 50*

8 Source: In-Cumbria. 43% of businesses experienced a cyberattack in past year
9 Source: MobileIDWorld. Ontario And Alberta Investigation Finds Inadequate Safeguards In PowerSchool Student Data Breach
10 Source: The Hacker News. APT24 Deploys BADAUDIO in Years-Long Espionage Hitting Taiwan and 1,000+ Domains

© David Swan Consulting 2025

Cyber-Intelligence Report

million tonnes."[11]

11. **NoName057(16) Attacks Danish Government Resources**. Russia's hacker group NoName057(16) launched a series of attacks on Denmark on 13 and 14 November. The attacks targeted Danish digital services including government agencies and defense industries. The objective appeared to be to "*block access to websites and influence the political process.*"[12] The website for Denmark's 'Great Belt Bridge' was also attacked and went down on the 14th. *"Jørn Guldberg, an IT security specialist with the Danish Society of Engineers (IDA), said ... They rarely aim to steal data – it's about visibility and symbolism. But they are also part of a broader pattern in which cyberattacks are used as a political pressure tool."*[13]

Iran

13. **Amazon Links Digital Spying To Physical Strikes**. Amazon has documented two cases of Iran's use of Digital Spying to prepare for 'cyber-enabled kinetic targeting'. In the first example, Iranian APT 'Imperial Kitten' compromised a ship's Automatic Identification System (AIS), then it hacked additional maritime vessels including shipboard CCTV cameras. This was followed by searching for AIS data on a specific ship, which was targeted by a Houthi missile strike. In the second case, Iranian APT 'MuddyWater', part of the Iranian Ministry of Intelligence and Security, compromised an Israeli server used for 'live CCTV streams from Jerusalem'. "*Researchers believe this was used to collect real-time visual intelligence of potential targets in the city in preparation for a June 23 missile attack launched by Iran.*"[14] Amazon believes using cyber-enabled kinetic targeting will become increasingly common.

14. **Iranian Hackers Targeting Victims Families – To Increase Pressure**. The Israel National Digital Agency (INDA) is warning that Iran's APT42 *" 'is systematically targeting high-value senior defense and government officials using personalized social engineering tactics.' What's notable about the effort is that it also extends to the targets' family members, creating a broader attack surface that exerts more pressure on the primary targets."*[15]

This cyber-intelligence product is produced by David Swan. It is copyright David Swan 2025. This report is **TLP:CLEAR**[16] and MAY be shared freely.

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

11 Source: The Record. Cyberattack on Russian port operator aimed to disrupt coal, fertilizer shipments
12 Source: unn.ua. Pro-Russian hackers attacked Danish government resources on the eve of elections – CPD
13 Source: thelocal.dk. New cyberattack on Denmark targets Great Belt Bridge website
14 Source: Security Week. Amazon Details Iran's Cyber-Enabled Kinetic Attacks Linking Digital Spying to Physical Strikes
15 Source: The Hacker News. Iranian Hackers Launch 'SpearSpecter' Spy Operation on Defense & Government Targets
16 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 2025