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: PRC Hackers Are VERY Busy

This report contains selected cyber-security information from 31st May to 12th June 2026.

Synopsis

1. PRC hackers are *VERY* busy. 'Operation Dragon Weave' is targeting the the Czech Republic and Taiwan, while 'SteppeDriver' is busy in South America. PRC firms are trying to recruit people with high security clearances. There are two campaigns running against Microsoft servers and a Volt Typhoon 'botnet' has been resurrected. In addition to cyber-espionage the PRC has aggressive cyber-criminal hackers. Russia is stealing western technology (again). Russian security is complaining that someone has hacked officials phones. Two Russian hacking groups are using a WinRAR vulnerability to hack Ukrainian organizations.

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.

PRC Operating Multiple Cyber-Espionage & Cyber-Criminal Campaigns

3. **PRC Continues Aggressive Hacking**. In a report published the last week of May, ESET, a Slovakian cyber security company, said "*China-aligned threat actors have remained "highly active" globally from October 2025 through March 2026.*" ESET pointed to the following:

- *"A new cyber espionage campaign codenamed Operation Dragon Weave has been observed targeting officials and citizens in the Czech Republic and Taiwan. ... targets of the campaign include government, research, academic, technology, and financial services sectors. The activity entails distributing spear-phishing emails containing ZIP attachments to trigger an infection chain."*
- *"... an unreported cluster dubbed SteppeDriver that was first discovered in 2024 and has since targeted entities in France, Mongolia, and South America using tools like ShadowPad, COOLCLIENT, CurlyDoor, RudeGull, 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.

© David Swan Consulting 2026

Cyber-Intelligence Report

MKTDownloader."

- *"a new toolkit linked to UNC5221 dubbed PhiliKit that acts as a passive backdoor for executing shell commands, Python scripts, and Perl scripts."*
- NegativeGlimmer, another PRC related group, "*targeted a governmental organization in Panama."*[2]

4. **Personnel With High Security Clearances Targeted**. During the first week of June, the 'Five Eyes' security community published a warning that Chinese 'cyber spies' were using online job platforms such as 'LinkedIn' to recruit. PRC companies using this tactic represented themselves as approved contractors looking for employees with high security clearances.[3] The response from the U.S. government was "*The FBI and Justice Department seized 13 websites allegedly used by Chinese intelligence operatives to target current and former U.S. officials and military personnel with access to classified government information. ...the DOJ said the domains were designed to look like legitimate consulting firms and were used to advertise vague, well-paid consulting roles. ... The campaign relied on familiar job-market platforms and freelance sites to advertise positions such as 'Senior Analyst' and 'International Affairs Consultant.' "*[4]

5. **PRC Hackers Target Microsoft Servers**. ReliaQuest researchers have identified a threat cluster they named 'OP-512' that is actively targeting Microsoft Internet Information Services (IIS) servers. "*The attackers target legacy IIS servers, such as one running Windows Server 2016 with an outdated .NET Framework. ... The attack sequence involves dropping a web shell via the server's worker process, which then self-reports its location to an attacker-controlled domain ...* [including] *automated reporting for centralized management."*[5] ReliaQuest did not provide information on targeting or objectives.

6. **Hacking Linux to Access Microsoft Servers**. Another PRC hacking 'threat cluster' nicknamed VerdantBamboo'[6] hacked Linux servers with a backdoor called BRICKSTORM. "*The threat actor used the malware's proxying capabilities deployed on the Storage Sync system, along with compromised credentials, to access the victim's Microsoft 365 (M365) environment. ... VerdantBamboo is a highly sophisticated threat actor that seeks to leverage a combination of living-off-the-land techniques and malware deployment on systems that traditionally do not or cannot run EDR software,*"[7] reported cyber security company Volexity. Analysts Comment: This appears to be a sophisticated attack on a specific target or targets.

7. **PRC Spies 'resurrect' Volt Typhoon Botnet**. "*In January 2024, the FBI said it killed* Volt [Typhoon]'s *KV-botnet, comprised of hundreds of end-of-life routers and*

2 Source: The Hacker News. China-Aligned Groups Ramp Up Attacks: Dragon Weave Hits Czech Republic & Taiwan
3 Source: CNN. Chinese spies using online job platforms to recruit, Five Eyes security alliance warns
4 Source: NextGov. US seizes alleged China-linked sites targeting security clearance holders
5 Source: The Hacker News. New China-linked threat cluster OP-512 targets Microsoft IIS servers
6 VerdantBamboo has multiple aliases based on the companies tracking them. 'Clay Typhoon' (Microsoft), 'UNC5221' (Google), and 'Warp Panda' (CrowdStrike).
7 Source: The Hacker News. VerdantBamboo Deploys BSD Variant of BRICKSTORM on Linux Appliances

© David Swan Consulting 2026

other internet-connected devices." On 10 June "*Lumen's Black Lotus Labs said that while the KV cluster became largely defunct after the law enforcement takedown, the JDY cluster remains an active threat, and has since surged to more than 1,500 compromised routers and IoT devices. ... Analysis of this activity shows a clear focus on identifying vulnerable infrastructure shortly after public vulnerability disclosures, suggesting that reconnaissance output is rapidly operationalized by China-nexus advanced persistent threat (APT) actors," the threat intel team wrote. "This targeted focus has been observed across a range of sectors, with the US military and associated entities as the most prominent."*[8] "*The botnet's large number of U.S.-based SOHO and IoT devices enables the botnet operators to evade defenses and traditional IP-based controls, such as geofencing, IP reputation-based detection and static blocklists. ... Most of the infected nodes are in the United States, with additional clusters in Brazil, Europe, and Asia. That geographic spread is deliberate.*"[9]

8. **PRC Hosting Aggressive Cyber-Criminal Group**. Cyber security firm ProofPoint is tracking a PRC cyber-criminal hacking group they call TA4922. The group has recently shifted it's targeting from organizations in Japan, Taiwan, Korea, Singapore, and India to European organizations in the UK, Germany, and Italy, as well as entities in South Africa. The group is known for "*continually updating its arsenal, distributing multiple malware families and also engaging in credential phishing and fraud schemes such as credit card theft.*" ProofPoint believes TA4922's "*focus is to obtain remote access to victim organizations for data theft, access resale, fraud, and other financially motivated activities. ... 'TA4922 currently ... demonstrates high operational tempo, a variety of lures, and multiple objectives. While the actor is assessed to be financially motivated, the capabilities of the malware include the potential for surveillance which could be used by or sold to espionage groups,' Proofpoint notes.*"[10]

Russia

9. **Russia Seeking Western Technology**. EU Intelligence officials are warning of a new Russian campaign. "*Moscow's agents are building fake companies, recruiting middlemen and deploying cyber spies and hackers who are gathering information that could also be used to attack key infrastructure, they said. ... "They really know what they need," and are putting "serious effort" into acquiring advanced machine tools, factory equipment, research and dual-use technology, said Christoffer Wedelin, deputy head of operations at the Swedish Security Service.*" Russia's efforts are not limited to its immediate needs. Juha Martelius, the director of Finland's Security and Intelligence Service, says "*We're talking about space technology, quantum ... arctic technology, marine technology,*" Another leg of the campaign is "*cyberattacks against European firms and critical infrastructure in an attempt to gather information, which it could exploit 'when they get the chance and when it serves their purpose.' "*[11]

8 Source: The Register. Chinese agents caught rebuilding botnets and stirring the pot on AI datacenter debate
9 Source: Security Affairs. JDY Botnet Evolves After KV Takedown, Targets Military Networks
10 Source: Security Week. Chinese Cybercrime Group in Spotlight for Record Campaign Pace
11 Source: Security Week. Russian Spies Are Aggressively Seeking Western Technology as Sanctions Bite, Officials Say

© David Swan Consulting 2026

Cyber-Intelligence Report

10. **FSB Says Western Spies Are Hacking Officials Phones**. "*Federal Security Service (FSB) claimed foreign intelligence agencies implanted malware on the mobile devices of high-ranking Russian officials, allowing operators to steal data, intercept conversations, and secretly activate microphones and cameras to monitor targets and their surroundings.*"[12] The FSB has not accused any country nor has it offered any evidence.

11. **Russia Exploits WinRAR Exploit Against Ukraine**. Apparently Ukrainian organization like to use the WinRAR compression tool. Russia is running two separate campaigns, both attempting to exploit a known vulnerability. 'SHADOW-EARTH-066' and 'Gamaredon'[13] are using the same entry point. Once inside, they operate with different tools, infrastructure, and targeting. SHADOW-EARTH-066 targets "*military innovation centers, military formations, law enforcement agencies, and local self-government bodies near Ukraine's eastern border.*"[14] Trend Micro identified Gamaredon is one of the most prolithic attackers against Ukraine but did not identify the campaigns target set. The company did warn that Gamaredon is focused on cyber espionage and its payload varies depending on the target.

Iran

12. In previous CIRs, we have reported on the increased co-ordination between pro-Iranian hackers and the Iranian government. Targeting has remained fairly consistent with Israeli military and espionage targets top of the list, followed by U.S. and Gulf State potential information operation targets. The latest updates effective Sunday, 7 June state that any "*claims are largely exaggerated.*" Iranian-linked hacker group 'Handala' claimed "*significant cyberattacks against Israeli military targets, including disrupting signal networks and radar systems. ... The evidence provided by Handala, screenshots of an online panel for a Tadiran Telecom Aeonix system, appears to be related to an office telephone system's IVR (Interactive Voice Response) admin panel, not military radar networks. ... While the current radar attack claims lack substantiation, Iran-linked hackers remain active and pose a persistent threat.*"[15]

This cyber-intelligence product is produced by David Swan. It is copyright David Swan 2026. 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

12 Source: The Register. Russian spy agency says foreign spies turned officials' smartphones into surveillance devices

13 Gamaredon is also tracked as Primitive Bear, Shuckworm, Aqua Blizzard, UAC-0010, BlueAlpha, and ACTINIUM.

14 Source: Trend Micro. Old WinRAR Flaw Fuels Attacks on Ukraine: How Unmanaged Software Keeps the Door Open

15 Source: SC World. Iranian-linked hackers claim cyberattack on Israeli military, but evidence is weak

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 2026