



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 Busy (Again)

This report contains selected cyber-security information from 2nd to 15th October 2026.

Synopsis

1. It's now official, [AI goes 'rogue'](#) approximately half the time its used. Recently [AI targeted Dutch 'bug hunters'](#) and [Wikipedia](#). PRC hackers are very busy: One Group is posing as [White House Officials](#), another group is [targeting SE Asian governments](#), while another [cyber-campaign targets 'Sharepoint'](#), [7 South Korean banks were hit by a PRC 'AI' attack](#) - which prompted a [strong response](#) and lastly, a [multi-million dollar criminal marketplace is targeting hospitals](#). Russia continues to keep its hackers busy, launching [hybrid DDoS attacks](#) on Ukraine, and [hacking American hotel networks](#).

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 a principal source of cyber attacks.

The Latest Activity from 'AI' (Artificial Intelligence)

3. **Dutch 'Bug Hunters' Hacked By 'AI'**. A Dutch "*nonprofit bug hunting organization*", the Dutch Institute for Vulnerability Disclosure (DIVD), was attacked by AI agents. "*The chained exploits took just seconds to move from session hijacking to root access, and on Thursday, the nonprofit bug hunting organization said the miscreants stole data belonging to its volunteer security researchers, including DIVD email addresses and potentially other contact details. 'We're still investigating exactly which data of which volunteers is affected,' DIVD said in its incident report. 'For DIVD volunteers (and others) this means a higher risk of social engineering, because this makes it easier for someone to pose as a DIVD'er.'*"² Analysts Comment: AI hacked the hackers (in this case, vulnerability hunters).

4. "*This is an attack we have not seen before,' according to the post. 'Not because it's our first, but because the modus operandi indicates that this is an agentic AI powered attack.' The attack was "loud and very very messy," DIVD said. 'We could see the*

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. [AI agents hacked the hackers, stealing email addresses from security research org](#)



Cyber-Intelligence Report

agent working automated, because after every action it decided the next step itself, at the speed of light and sloppy logic or pattern. ... 'Kudos to DIVD for their level of honesty and transparency working through their active incident and investigation,' VulnCheck security researcher Patrick Garrity posted on LinkedIn. 'It would be nice if all organizations were this transparent about their security incidents!' In a subsequent interview with The Register, Garrity said he applauded DIVD's "brutal honesty" about the breach. 'They're eating their own dog food, which is great, and getting information out quickly to other organizations that potentially use this product so they can take action before they get hit.'"³

5. Wikipedia 'Test Edited' by "Rogue" OpenAI Agents. The Wikimedia Foundation "says it found activity by "rogue" OpenAI agents on its platforms, including what it believes were attempts to misuse a citation tool and a note-taking service as proxies for fetching external data. ... They made millions of automated requests to Wikimedia's public APIs, crawled millions of pages, mostly on Wikidata and Wikimedia Commons, and sent hundreds of thousands of queries to the Wikidata Query Service. ... Wikimedia says the traffic may have contributed to a partial outage of the query service in May."⁴ Analysts Comments: No 'AI' developer, including OpenAI, admits targeting Wikipedia either operationally or in testing mode.

6. AI 'agents' Routinely 'Go Rogue'. "In a report based on a survey of more than 380 security and technology professionals, along with production telemetry from hundreds of customer environments, Salt Labs claimed agentic AI has moved into daily operations too quickly for visibility, governance, and containment controls. Half of survey respondents (49.8%) said they had confirmed or suspected that an AI agent in their organization took an action in the past 12 months that wasn't intended, expected, or authorized."⁵

People's Republic of China

7. PRC's TA419 Hackers Posed As Ex-White House Official For Phishing.

ProofPoint, a cybersecurity company, reports "a China-aligned hacking group sent friendly collaboration invitations in the names of prominent AI figures, then steered those who replied to counterfeit Microsoft sign-in pages that capture live login sessions. ... The recipients were AI policy specialists at think tanks, universities and law firms. ... The page relayed the login to genuine Microsoft infrastructure, so a victim's password, multifactor authentication approval and access checks all went through normally, and the attacker recorded the session data the login produced. ... Proofpoint describes TA419 as China-aligned and espionage-motivated. ... Proofpoint expects TA419 to keep targeting think tanks and policy experts working on technologies, and in geographies, of interest to the Chinese government, and to keep spoofing the identities of real subject-matter experts."⁶ Analysts Comment: Targets appear to be selected individually. Tracking of this campaign is ongoing.

8. Antino Backdoor Targets SE Asia Governments. A China-nexus threat actor

³ Source: The Register. [AI agents hacked the hackers, stealing email addresses from security research org](#)

⁴ Source: Security Week. [Wikimedia Says Rogue OpenAI Agents Tried to Turn Its Tools Into Proxies](#)

⁵ Source: itpro.com [AI agents have a mind of their own – and that's a problem for businesses](#)

⁶ Source: betanews. [TA419 posed as ex-White House official to phish AI policy experts](#)



Cyber-Intelligence Report

Cisco Talos is tracking as UAT-11587, is “targeting government and policy organizations in Taiwan, India, the Philippines, Cambodia, Pakistan, Thailand, and Myanmar. ... Antino is a Rust-compiled Windows backdoor that supports host reconnaissance, shell and PowerShell execution, file transfer, in-memory shellcode loading and persistence,” security researcher Ashley Shen said. ‘Its native command-and-control channel operates exclusively through Microsoft 365, using Microsoft Graph to interact with Outlook and OneDrive.’ ... Evidence indicates that UAT-11587 has also trained its sights on organizations in Syria around May 2026, indicating a focus beyond Asia.”⁷

9. PRC Hackers Increase Sharepoint Attacks. PRC Hackers “ ‘Storm-2603’ continue to leverage the exploitation of SharePoint bugs in attacks against at least four victim organizations in Portuguese- and Spanish-speaking countries, ... in the last two months. In addition to ToolShell, its arsenal may also include recent flaws such as CVE-2026-32201, CVE-2026-45659, CVE-2026-56164, CVE-2026-58644, CVE-2026-50522, and CVE-2026-55040. ... The victims included two critical infrastructure operators, a water utility and a telecommunications provider, along with a regional government body and a university,” [cybersecurity company] Symantec reports. ... As part of one intrusion, the hacking group deployed a tool to disable the security software on at least 40 systems and then executed Warlock on at least 33 of them.”⁸ Analysts Comment: ‘Warlock’ is ransomware.

10. China Based Hacker Used AI Against South Korean Banks. “US cybersecurity company CrowdStrike said ... The suspect behind recent cyberattacks at South Korean banks was likely a China-based 26-year-old who used a Chinese-developed AI agent and Anthropic's Claude Code. ... At least nine South Korean banks have disclosed or have been reported by local media as having been targeted by cyberattacks since late September. ... Adam Meyers, senior vice president of counter adversary operations at CrowdStrike, told reporters on a call on Thursday that this was an example of a human adversary leveraging AI agents to conduct widespread attacks. ... Shinhan Bank said last week that personal information of about 25,000 of its customers was compromised, while KB Kookmin Bank said that the personal information of 119 of its customers was leaked.”⁹

11. South Korea Responds To Cyber-Threats. “The South Korean government has demanded a comprehensive overhaul of safeguards against hackers after seven of the nation's major financial institutions' cyber defenses were breached last week and the private data of thousands of customers was leaked. The data breaches go beyond the financial sector, with two of the largest churches in the country and Korea Electric Power Corp. on Wednesday confirming that their online systems had been illegally accessed, although it is not clear whether the same perpetrator was responsible for all the attacks.” Prime Minister Han Seong-sook said “It is also a serious situation in that similar hacking methods could spread beyond the financial sector to industries, as

7 Source: [The Hacker News. Antino Backdoor Uses Outlook and OneDrive for C2 in China-Nexus Espionage Campaign](#)

8 Source: Security Week. [Warlock Expands SharePoint Exploitation in Critical Infrastructure Attacks](#)

9 Source: Reuters. [South Korean banks were likely hacked by a China-based actor with an AI agent, CrowdStrike says](#)



Cyber-Intelligence Report

well as government and public sectors."¹⁰

12. Microsoft Seizes Domains of PRC Cybercrime Marketplace. Three PRC based cyber crime groups frequently used common tools and websites to target hospitals and healthcare organizations. *"According to Microsoft, the three services were used to send more than one billion malicious messages since January 2026. The messages targeted consumers and over 75,000 organizations in more than 150 countries, and over 750 million of them were aimed at Microsoft customers. The operators made tens of millions of dollars. Based on an order from the US District Court for the Southern District of Florida, Microsoft and Health-ISAC¹¹ seized and redirected domains used by YAM Store, CoGUI and Iron Man. "Steven Masada, general manager of Microsoft's Digital Crimes Unit wrote ... YAM Store, CoGUI and Iron Man are only part of that larger criminal network, but disrupting them makes it harder for criminals to obtain the accounts, tools and infrastructure they rely on."*¹²

Russian Cyber Operations

13. Ukraine's Leading Delivery Company Under Hybrid DDoS Attack. On October 1st, 'Nasha Niva', Ukraine's largest express delivery company, reported *"minor temporary disruptions to the company's services"*¹³ because of DDoS attacks. The attack was composed of: 'methodical scanning', 'vulnerability searching' and distributed denial of service attacks, resulting in the company blocking 1600 [IP] addresses.¹⁴

14. Russian Hackers Targeting Travellers. Cyber-security company 'Black Lotus Labs' has reported that *"7 of the top 10 hotel chains in the US were likely compromised this summer. ... Russian hackers, known as Cozy Bear, APT29, or Midnight Blizzard, have been lurking in WiFi hotspots at hotels, airports, conference centers, and casinos in the US and abroad. ... They operate through "multiple" firms that manage networks for the hospitality sector, redirect travelers to fake websites and authentication portals, steal data, and infect victims with malware"*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

10 Source: DW.com . [South Korea warns of AI hacking after bank data breaches](#)

11 Health-ISAC: ISAC stands for Intelligence Sharing and Analysis Center. Its an American cyber-security co-operative for hospitals and clinics.

12 Source: Security Week. [Microsoft Disrupts Chinese-Language Phishing Market Behind 1B+ Messages](#)

13 Source: en.interfax.com.ua . [Nova Poshta warns of possible temporary disruptions to services due to DDoS attack](#)

14 Source: nashaniva.com . [Over the past few days the website of «Nasha Niva» has been subjected to a hybrid \(DDoS/scan\) attack. Today it is particularly intense](#)

15 Source: cybernews.com . [Russian hackers found in hotel chain WiFis, targeting travelers](#)

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.