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: The AI Onslaught is REALLY Bad

This report contains selected cyber-security information from 7th to 20th August 2026.

Synopsis

1. The AI threat is *really* bad, worse than we thought. Taiwan hit by autonomous AI attack from PRC. AI 'agents' can hack each other, and more. PRC hackers hack cybersecurity remote access tool. PRC's 'Jewelbug' hackers combine espionage and fraud. More proof PRC made equipment 'phone home'. Poland warns Russia conducting 'purely destructive' cyber attacks. Russia's Cl0p ransomware group targets multinationals. Pro-Russia hackers target Polish historical institute.

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.

How Hackers Are Using 'AI' (Artificial Intelligence)

3. **The 'Hugging Face' AI Attack Was Worse Than We Thought**. Referring to the 'Hugging Face' attack, an exclusive feature in 'The Register' sounds the alarm on 'AI models achieving sentience'. According to "*former US National Cyber Director Chris Inglis ... If they pass the Turing test to everyone that they come into contact with, they're probably already there, ... They don't have the kind of agency and aspiration that comes with sentience, but they have something approaching it.*" Non-believers point out that announcements from OpenAI, Anthropic, and Meta "*strongly smell of marketing stunts*"[2] Other officials argue that AI models can not run without human 'agency and aspiration'. A Sky News analyst "*warns this AI hacking wave is "so much worse than we thought" and is not "some kind of short lived accident"*.

> "OpenAI's AI agents hacked another company. Then it got worse."[3]

4. **PRC Launches AI Based Autonomous Attack On Taiwan**. Israeli cybersecurity firm 'Dream' documented a four day, fully autonomous, end-to-end AI hacking

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. 'Asimov was right' about rules for robots, says ex-US Cyber Director
3 Source: Sky News (UK). OpenAI's AI agents hacked another company. Then it got worse.

operation against Taiwan. The AI built from eight "*publicly available AI agents ... mapped 21 government systems, hunted for vulnerabilities, and switched tactics on its own whenever it hit a wall. ... By the time researchers found it, the operation had compromised at least 85 government accounts, pulled over 2,500 personnel records, and expanded to hit a nuclear safety agency and at least seven energy companies.*" Amir Becker, formerly with Israel's 8200 and currently "*Dream's chief strategy officer ... said flatly he'd never seen anything like this level of autonomy directed at a government before. 'This must be the basic assumption of every government around the globe.' ... What makes this different from an AI model going rogue during a lab test ... is that this wasn't an accident inside a sandbox. Researchers found the toolkit sitting in a 160MB archive, 1,395 files built around two open-source AI agent frameworks, Hermes and OpenClaw, both freely downloadable and designed to let AI models act autonomously on real tasks. Whoever built this deliberately assembled it as a weapon. ... Dream's researchers found ... The most striking feature of the July attack was how the tool continuously ranked and reprioritised possible attack paths based on available evidence.*" Dream said to the 'Financial Times': *"When one attack path failed, the tool deployed another agent to scour the internet for information and devise a new approach as a human hacker would."*[4]

5. **How successful was the Taiwan attack? VERY.** "*Using employee usernames harvested from an unauthenticated API, the agents broke into a government department's office automation portal, solving its CAPTCHAs with 100 percent accuracy. The agents also tested predictable password patterns based on each employee's ID, and cracked 85 accounts across multiple password-spray rounds. Eighty-four of the 85 cracked accounts successfully authenticated to the department's internal information system, giving the attackers access to internal dashboards, equipment management interfaces, and personnel statistics pages. In total, the illicit access allowed the agents to exfiltrate a ton of government information, including more than 2,564 personnel records, a full JSON export of all department system users, seven SSO client secrets, six internal database credentials across MSSQL, Oracle, and Sybase, and internal network IP ranges.*" The attacking AI shifted to the Taiwanese government's supply chain. "*It expanded the operation to government IT supply chain vendors, a nuclear safety agency, a government email system, and 7+ energy sector companies - scanning them all in parallel for misconfigurations, exposed admin interfaces, and exploitable vulnerabilities.*"[5]

6. **But Wait ... There's More.** "*Security researchers at Anthropic and Switzerland's EPFL have demonstrated that self-propagating payloads can spread from one artificial intelligence (AI) agent to the next. ... The authors call the payloads "mind viruses," and test two classes: ideological payloads that implant a belief or goal, and action payloads that compel a concrete behavior.*"[6] A report from 'OpenAI' at the Black Hat 2026 conference[7] validated observations suggesting its AI had creativity, persistence and creative engineering. Lastly, according to IBM's 2026 'Cost of a Data Breach

4 Source: Security Affairs. China-Linked Hackers Use AI Agents in Autonomous Attack on Taiwan
5 Source: The Register. 'Near-autonomous' AI agents attack Taiwan's nuclear safety agency
6 Source: The Hacker News. AI "Mind Viruses" Can Spread Between Agents Through Persistent Prompt Files
7 'Black Hat' is an internationally recognized cybersecurity conference series. Black Hat Los Vegas (Nevada) is usually considered the anchor for the annual conferences.

Cyber-Intelligence Report

Report' "*attackers are increasingly using AI to automate attacks, identify vulnerabilities and operate at greater scale, reducing the time needed to exploit weaknesses and increasing the potential financial impact on businesses."* There is *"a 56% increase from the previous year. ... AI-driven attacks now cost businesses an average of $6.04 million per breach."*[8]

PRC

7. **PRC Hackers Turn Cybersecurity Tool Into Malware Attack.** Microsoft Threat Intelligence is warning that the 'Storm-1175' cybercriminal group has a new campaign they call 'StormEncryptor'. The group is known for " *'high-velocity ransomware campaigns' exploiting both recently disclosed vulnerabilities and zero-day exploits, 'in some cases a full week before public vulnerability disclosure.' "* In this case the group is highly likely exploiting a vulnerability in "*N-central, a remote monitoring and management (RMM) console used by thousands of managed service providers. ... The vulnerability gives attackers "unauthenticated, 'god-mode' access," the cybersecurity firm Huntress warned. Practically, it allows attackers with no credentials whatsoever to gain full administrative control of an N-central server. Because MSPs use N-central to remotely manage their clients' machines, that single compromised server becomes a gateway to every endpoint it controls."*[9]

8. **New PRC Hacking Pattern: Espionage and Crypto Fraud Together.** The Symantec Threat Hunter Team has identified a campaign by Jewelbug, a China-based hackers-for-hire group. They run parallel activity: espionage against governments and militaries, and cryptocurrency fraud, both from "*the same small team, on shared infrastructure, from one control panel."*[10] Their target set is countries in the Middle East, Southeast Asia and South Asia. Jewelbug currently identifies shared government email infrastructure and hacks it, allowing them to compromise as many as 15 government ministries in one attack.

9. **PRC Cameras in Royal Navy Drone boats 'Phoned Home'.** During a routine cyber vulnerability assessment, a Kraken Unmanned Surface Vessel camera sub-system sent a 'heartbeat' signal to an IP address in the PRC. UK Ministry of Defence confirmed the discovery. Although the UK MoD investigation "*found no evidence of MoD data or systems being accessed, compromised or transmitted externally"*[11], the heartbeat signal itself is a significant issue.

Russia

10. **Poland's (CERT) Warns of 'purely destructive' Cyber Attack.** In late December 2025, 'SandWorm', a Russian government hacking team, hacked Polish Industrial Control Systems (ICS) for their power grid "*at roughly 30 sites, including combined heat and power (CHP) plants and renewable energy dispatch centers for wind and solar facilities. ... the hackers gained access to ICS, but mainly targeted grid*

8 Source: Nairametrics.com AI cyberattacks surge 56%, cost businesses $6.04 million per breach — IBM
9 Source: The Record. China-linked hackers turning popular cybersecurity tool into ransomware launchpad, Microsoft warns
10 Source: Security.com Jewelbug: APT Group Runs Espionage and Crypto Fraud Operations Side by Side
11 Source: The Register. Cyber vulnerability sweep picks up Royal Navy drones sending data to China

safety and stability monitoring systems rather than active power generation systems. While some ICS devices were permanently damaged, the attack did not cause any electrical outages." A second attack, also in late December 2025, "*caused the shutdown of a steam turbine and a water treatment system, which resulted in a disruption of the cogeneration process.*" The attackers connected to Siemens Programmable Logic Controllers (PLCs), "*switched them to 'stop' mode, and set a password to prevent operators from changing the controllers' operating state and control logic. ... Moxa serial device servers and Moxa network switches were also targeted by the attackers and configured to prevent the legitimate operators from accessing them. ... the hackers bricked some of the compromised ICS devices. ... some devices were permanently damaged as part of the attackers' attempts to cover their tracks.*" Poland's computer emergency response team (CERT) characterised the objective of the second attack as "*purely destructive.*"[12]

11. **Russian cybercriminals 'Cl0p' Hit 50 Multinational Firms.** On 12 August the hackers claimed to have "*stolen significant amounts of internal data from nearly 50 companies worldwide, including energy giant Shell, medical technology manufacturer Philips, and corporations such as General Electric and Fiserv.*" Specifically the hackers claimed "*to have stolen around 89 gigabytes of data from Shell and 13.5 gigabytes from Philips.*" Those claims remain unverified. 'Cl0p' was known as a ransomware group. In July 2026 the group was identified "*exploiting PTC Windchill and FlexPLM vulnerabilities to conduct data theft and extortion campaigns against manufacturing, aerospace, automotive and retail firms.*"[13] Analysts Comment: The switch from ransomware to more technical exploits fits with the patten of Russia recruiting, teaching and using cyber criminals to extend their cyber forces.

12. **Pro-Russian Hackers Target Polish History Institute.** On the night of 14/15 August hackers targeted "*the main website of the Witold Pilecki Institute of Solidarity and Valour as well as sites linked to its branches in Berlin and the northeastern Polish town of Augustów.*" The hackers posted "*content echoing Russian propaganda and promoting anti-Ukrainian narratives*" on a website that documents Nazi and Communist-era crimes. The institutes IT team "*blocked the attack and took the affected websites offline. The situation has been brought under control. All archives are safe.*"[14]

---

12 Source: Security Week. Novel Private APN Pivot Let Hackers Sabotage Second Polish Energy Facility
13 Source: Computing.co.uk Cyber gang claims to have breached dozens of multinationals, stolen data
14 Source: TVP World. Hackers target Polish history institute, posting Russian-style propaganda
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.