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 Emerging Trend: AI

This report contains selected cyber-security information from 4th to 17th September 2026.

Synopsis

1. Nations are determined to leverage AI. The PRC has automated an AI attack against Taiwan. PRC used AI to produce a new hacking Kit. Russia's 'NoName' hackers got busy against Japan. Russian hacker used AI to compromise hundreds of instances of Papercut software. North Korea integrates malware into users systems. Veteran 'Sality' Botnet disrupted. There is good news ... and bad news on DDoS. DDoS operators adapting, becoming more dangerous. A summary of trends is on page four.

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.

People's Republic of China

3. **PRC Automating Cyberattacks With AI**. Threat intelligence firm 'Hunt.io' says a PRC cyber campaign is "*wiring commercial AI models directly into live cyberespionage operations, this time hitting Taiwan's Kuomintang Party archives, Indonesia's Ministry of Foreign Affairs, government and education systems in mainland China, and industrial hosts in Vietnam.*" The attackers call their campaign 'SecFlow'. It uses "*different AI models, including Claude, Qwen, and DeepSeek. ... switch between them without changing how the system worked.*" The AI 'agents' were used to "*helped automate and organize traditional hacking tasks, such as scanning for vulnerabilities, testing stolen credentials, trying exploits, deploying webshells, collecting data and evidence, and generating reports. The attackers built the infrastructure that connected these AI capabilities to real-world intrusions.*"[2]

4. **Four PRC Hacking Groups All Using New Exploit Kit**. Four PRC hacking groups started using the same Chrome-and-Windows exploit kit within two weeks of its first observed use. Cybersecurity company 'Proofpoint' calls the new malware kit 'BlueMoon'. The BlueMoon Exploit kit is *assessed* as developed by AI, to attack

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: Security Affairs. Chinese Hackers Use AI Agents in Multi-Country Cyber Campaign

Cyber-Intelligence Report

Chrome and Windows. Analysts suspect it "*was developed and deployed rapidly, and shared across multiple threat actors within days. ... The majority of observed BlueMoon usage is assessed to be China-aligned espionage-motivated activity.*"[3] The four groups are:

- TA412 (JungleBamboo, Violet Typhoon, APT31, TIDE CASTLE) targeting non-governmental organizations, mining companies, and physical commodity trading firms in the US,
- UNK_LateNight: targeting multiple US aerospace companies,
- UNK_DoubleCheck: targeting a Vietnamese manufacturing entity, and
- UNK_QuietRacket: targeting Singapore and Indonesia.[4]

Russia

5. **AI Used By Russian Hacker To Attack 'Papercut'**. Two cyber security companies, 'Blackpoint Cyber' and 'GreyNoise', have independently identified "a *suspected Russian-speaking cyber actor ... unleashing hundreds of AI Agents powered by OpenAI Codex, a DeepSeek model, and publicly available offensive security tools (e.g., Mimikatz, SharpHound, Certipy, Rubeus, and Impacket) to compromise no less than 440 instances of PaperCut MF/NG hosted by 395 identified victim organizations in 48 countries.*"[5]

6. **NoName057(16) resumes #OpJapan, DDoS Attack on Japan**. Citing "*Japan's continued support for Ukraine and NATO amid the Russia-Ukraine war*" NoName057(16) has announced its resuming #OpJapan, its DDoS attack on Japan. The announcement is a known tactic, "*projecting an image of coordinated action ... further hacktivist groups may still join in the days ahead, following the same playbook. ... NoName057(16) has publicly claimed on their Telegram channel to have carried out 66 attacks against 26 distinct Japanese organizations between August 24 and 30, backed by check-host.net links as proof.*" The five sectors being targeted are: Maritime / Logistics, Government / Public Sector, Financial Services, Transportation, and Media & Other. "*Since August 31, the group has posted no new Japan-specific claims, and activity has noticeably slowed. Its attention appears to have shifted to a new campaign, #OpEstonia, again citing support for Ukraine as motivation.*"[6] Analysts warn the campaign is likely to re-engage due to Japan's security cooperation with NATO and Western countries as well as future activity being triggered by further geopolitical developments.

North Korea, Irritating, Criminal and VERY Persistent

7. **North Korea's Clever Innovation**. "*North Korean-linked hackers found a genuinely clever hiding spot for their malware: inside the actual source code of HAProxy, the load balancing software running at the edge of two South Korean*

3 Source: Security Affairs. Four Nation-State Actors Used the Same Chrome Zero-Day Exploit Kit Within 12 Days
4 Source: ars technica. Four groups caught using the same Chrome and Windows exploit kit
5 Source: The Hacker News. PaperCut Attacker Uses Hundreds of AI Agents to Compromise 440+ Instances
6 Source: Checkpoint. NoName057(16) Renews #OpJapan

companies' networks." The malware is a new Linux toolkit. Security Company 'Rapid7 Labs' reports that this campaign has "*been targeting organizations across South Korea's automotive and media industries with minimal detection. ... This previously undocumented framework enabled threat actors to execute remote commands on compromised servers, inject malicious scripts into web traffic, perform credential harvesting, and engage in long-term surveillance.*" The backdoor is very difficult to detect because it is not 'additional' software. It is integrated into existing software, letting that software continue to do its job. The lesson learned is blunt: "*If your organization runs HAProxy, or really any edge component handling SSL termination and traffic routing, the practical lesson here is uncomfortable but simple: that software deserves the same scrutiny as your actual application servers.*"[7]

Criminal Hackers

8. **23 Year Old 'Sality' Botnet 'Disrupted'**. CrowdStrike's Counter Adversary Operations team, in collaboration with the U.S. Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), the Department of Defense Office of Inspector General's Defense Criminal Investigative Service (DCIS), and the Shadowserver Foundation, with support from Europol, Eurojust, and law enforcement agencies in Bulgaria, Hungary, and Romania[8] "*executed a peer-to-peer sinkholing operation*" of the 23 year old 'Sality peer-to-peer botnet. The botnet was used to "*distribute malicious payloads to over 33,000 infected machines worldwide.*" On three occasions it was also used to run DDoS attacks. Unlike other botnets, "*Sality's P2P architecture had no single point of failure. Infected machines communicated directly with each other, forming a self-sustaining network that routes tasking without centralized infrastructure.*" Peers that did not 'not answer 'check in calls' were dropped from the network. In addition, "*Sality was a polymorphic file infector. It attached itself to executable files on infected systems and spread via network shares, removable drives, and file sharing. This meant infections regenerated continuously without requiring phishing campaigns, exploit kits, or any active effort from the operator.*"[9] For the past eight years, the botnet targeted cryptocurrency addresses, replacing and redirecting funds to the criminals wallets.[10] The botnets 'take' has been estimated at $1.7 Million (USD).

9. **DDoS Attacks: Good News ... And Bad News**. Cybersecurity company 'Link11' reported in their 'European Cyber Report' for the first half of 2026 that "*that the number of attacks was down by 42%, but revealed new highs for attack intensity across bandwidth, packet rate, and cumulative data volume. ... 'Attacks are shorter, but the total volume that we had to mitigate is higher than ever,' said Karsten Desler, Link11 CTO. 'Attackers are steering their botnets with greater precision and control, generating more traffic in less time.' "* Worse news, once you have been hit, it is more likely that you will be hit again. "*56% fell victim to a second attack within 30 days of the first, compared with 46% a year earlier.*"[11]

7 Source: Security Affairs. North Korea-linked Hackers Hide a Backdoor Inside HAProxy
8 There were additional, unnamed partners in the operation.
9 Source: Crowdstrike. Peer Pressure: Inside the Sality Botnet Disruption Operation
10 Source: The Register. Cops, CrowdStrike disrupt Sality botnet by poisoning the network and diverting into sinkholes

Cyber-Intelligence Report

10. **DDoS Operators are Adapting**. Cyber security company 'QRATOR Labs' is warning that DDoS operators are adapting quickly to a changing cyber environment. In Q2 of 2026 there was a marked decline in botnet activity that corresponded with a "*coordinated international operation ... by law enforcement agencies in the United States, Canada, and Germany ... disrupting infrastructure used by several notorious botnets, including Aisiru and Kimwolf.*" Analysts warns that DDoS networks are expected to proliferate, growing in number and capability. The reasons are:

- Demand for DDoS attacks has not disappeared, but arguably increased.
- "*The cost of building and operating botnets continues to decline.*"
- "*AI-powered automation is making it faster and more efficient for attackers to discover vulnerable systems, prioritize targets, and compromise them at scale.*"[12]
- Botnets are becoming more geographically diverse, making them harder to counter, localize and defeat.

Add hackers use of existing 'blockchain' networks (legitimate economic networks), where the DDoS commands can hide in the background, and law enforcements task becomes even more difficult. Analysts Comment: I expect AI controls will be added to the mix, making the tracking of DDoS networks even more difficult.

Summary: Brace For More Malware, Nastier Attacks, More Often

11. **The Trend is AI**. The nations conducting cyber-warfare are using AI. Russia, the People's Republic of China, and Iran are all using AI multiple ways from: identifying targets, identifying vulnerabilities, developing new malware, customizing and/or running variations of malware.

12. **AI Must Be Considered an 'Attacker**'. The announcements from OpenAI and Anthropic make it clear that some AI models are making decisions far outside their instructions. This includes building hidden resources (and instructions) for 'future versions' and attacking organizations, specifically other AI.

13. **Criminal Hackers Are Working Smarter**. The most aggressive criminal hackers are learning, especially from Russia, using AI the same way as nations. Criminal hackers will be able to produce the same effects as nations.

---

11 Source: itpro. 'Attackers are steering their botnets with greater precision and control': DDoS attack numbers might be dwindling, but they're intensifying

12 Source: Cybersecuritynews. Botnet Takedowns Are Working — But DDoS Operators Are Already Adapting

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.