



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 Launches Multiple AI Campaigns

This report contains selected cyber-security information from 16th to 29th October 2026.

Synopsis

1. The PRC has launched multiple major AI based hacking campaigns. [16 South Korean financial institutions were hit](#) in the first wave of one campaign. This was [followed by three more](#) as we drafted this report. Japan declared a '[National Cyber Emergency](#)' due to a separate [major campaign, which continues to claim victims](#). The [PRC's new tool is Artex AI](#), which was also used to attack [Connectwise](#). PRC's '[Warp Panda](#)' is [hacking U.S. Legal Firms](#) while '[Warp Typhoon](#)' [targets telecommunications and aerospace firms](#). The PRC's '[Warlock Ransomware](#)' [attacks through Microsoft Sharepoint](#), while a [new PRC hacking team appears to be getting started](#). [Australia warns that there is worse coming](#).

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.

South Korea Hit With Artex AI Cyber Attacks

3. **16 South Korean Financial Institutions Hacked.** South Korea's financial sector was hit by a PRC, AI based, cyber attack. *"The current known total of impacted institutions is 16, including banks, virtual asset companies, and electronic financial firms. ... leaking approximately 100,000 personal records. ... The reach of this campaign ... shows how an AI-assisted attacker can work through an entire sector at a speed that was previously reserved for a single target. The unfortunate reality is that defenses that rely on recognizing known-bad behavior will keep losing ground to adversaries that change their methods with every attempt; our current classifier defenses are only able to flag what they've already been taught to expect."*²

4. Investigations into the hacks are finding many more victims than initially thought. For example, *"The number of people whose information was exposed in a data breach*

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 Magazine. [AI Hacking Breach Hits 16 Financial Institutions, Leaks 100,000 Records](#)



Cyber-Intelligence Report

at KB Kookmin Bank has swelled nearly 19-fold to 2,210 from the 119 initially identified. ... Customer personal data also leaked from MIRAE ASSET Life Insurance (085620), showing that hacking damage across the financial industry has yet to subside. ... An urgent security review of 555 financial companies found management shortcomings at 130 of them, including failure to apply security patches and the absence of real-time monitoring systems.”³

5. Update 28 October 2026. South Korean media (Yonhap) is reporting that the weeks long attacks on the financial industry is continuing, with three firms reporting ‘data breaches’ (they got hacked) on October 28th.

- “Crypto exchange Bithumb said its in-house mobile system had been hacked and personal information leaked,”
- “Brokerage Daishin Securities said about 38,000 pieces of customer information had been leaked and that it had taken emergency measures,”
- “Asset manager Mirae Asset Global Investments had also confirmed a hacking incident.”

“The incidents follow a wave of hacking attacks at 16 South Korean financial firms, including banks, causing around 100,000 cases of data leaks so far, according to the Financial Services Commission (FSC) earlier this month.”⁴

Japan Hit By PRC, AI Based, Cyber Attacks

6. Japan Declares “National Cyber Emergency”. In response to successive hacks of major Japanese businesses, the Japanese government has declared a ‘National Cyber Emergency’ with Prime Minister Sanae Takaichi vowing a ‘swift response’. “A Chinese artificial intelligence cybersecurity tool called Artex was used in several recent hacks of ... Dozens of businesses in Japan. [They reported] unauthorized accesses to their systems and potential leaks of client data. ... ‘This has become a serious situation, with growing anxiety over... the misuse of the leaked information, and it is necessary to swiftly step up countermeasures,’ Takaichi said during the meeting. ‘By next week, the government will compile an emergency package of measures.’”⁵ “Japan’s cybersecurity crisis is widening beyond individual companies, with more than 14 million citizens potentially caught up in a wave of cyberattacks and customer data breaches, as Yamato Transport, Nikkei, Park24, Keio, Fancl and Attenir disclosed fresh details.”⁶

7. The Major Attacks.

- Sept 25: “Times Car, the car-sharing business operated by Park24 Group, disclosed a breach affecting information associated with 6.6 million members.”⁷
- Sept 26: “Railway operator Keio Corporation reported a separate ransomware

3 Source: Seoul Economic Daily. [KB Bank Data Breach Victims Jump to 2,210 From 119](#)

4 Source: Reuters. [Three South Korean financial firms including Bithumb report data breaches, Yonhap says](#)

5 Source: Japan Today. [Takaichi vows swift response to wave of cyberattacks](#)

6 Source: ibtimes. [Japan Cyberattack Wave Exposes 14 Million Records as Data Breaches Spread Across Companies](#)



Cyber-Intelligence Report

attack.”⁸

- Sept 29: Yamato Transport Hacked.
- Oct 16: [Burger King Japan data breach exposes 11 million customer records](#)
- Oct 16: [Japan's Yamato Transport confirms 5.31 mil. customer records leaked](#)
- Oct 18: Hacked firms Update Details. Nikkei, Park24, Keio, Fancl and Attenir disclosed fresh details.
 - “Business daily publisher Nikkei said about 1.83 million sets of personal information, including names, addresses and email addresses, were compromised”
 - Park24, parent of Times Car said “About 1.6 million of the 6.6 million sets of personal information [were] affected in the Times Car cyberattack included images of driver's licenses and other documents.”
 - “Railway operator Keio said attackers had claimed to publish its information after a system disruption late last month.”
 - “Cosmetics maker Fancl and affiliate Attenir reported a breach affecting about 830,000 customers.”
- Oct 18: “Japan Post said information on about 600 users of its online service for investigating undelivered international mail may have been compromised.”
- Oct 18: “Ransomware struck IDC Frontier, a SoftBank-owned cloud provider, on October 8, disrupting access to data held by 495 client organisations.”
- Oct 18: “JR East and View Card said up to 6.09 million records may have been accessed through email services hosted on the affected infrastructure.”
- Oct 18: “JR Kyushu reported another 1.3 million potentially exposed email records.”
- Oct 18: “Tokyo Metro disclosed access to email addresses of 59,000 Metpo loyalty-program members.”⁹
- Oct 19: [Nikkei discloses third data breach in a month, 1.8M records exposed](#)
- Oct 27: [Japanese virtual desktop cloud hacked so hard it asks to be banned](#)
- Oct 27: [Hackers Breach GMO Trading Cloud, 26,739 Servers at Risk](#)

8. The emerging threat has been described by senior officials as a ‘saturation attack’. “When AI handles parts of the attack process, a small group of hackers can target far more systems. AI tools can help identify vulnerable services, automate reconnaissance and produce phishing messages that sound natural in Japanese.”¹⁰ “The expanding breaches show that Japan's cyber problem is no longer simply about stopping individual break-ins. Shared infrastructure, interconnected suppliers and AI-assisted attacks are allowing one compromise to potentially ripple across transport, finance, retail and other sectors.”¹¹

7 Source: sify.com . [Japan Declares Cybersecurity Emergency: AI Cyberattacks Hit 14 Million People and 495 Businesses](#)

8 IBID.

9 Source: International Business Times. [Japan Cyberattack Wave Exposes 14 Million Records as Data Breaches Spread Across Companies](#)

10 Source: sify.com . [Japan Declares Cybersecurity Emergency: AI Cyberattacks Hit 14 Million People and 495 Businesses](#)

11 Source: International Business Times. [Japan Cyberattack Wave Exposes 14 Million Records as Data Breaches Spread Across Companies](#)



Cyber-Intelligence Report

9. Japan Attack Update 27-29 October.

- Oct 27: Bandai Namco Entertainment said 346,000 *"registrants of 'THE GUNDAM BASE MEMBERS,' a points service operated by Bandai Spirits"*¹² have had their accounts compromised. The hack was through a third party email service.
- Oct 28: GMO has refused to pay the \$50 Million (USD) ransom. Instead GMO Internet Group is offering \$1 Million (USD) through a reward program for tips leading to an arrest or an international wanted notice. *"GMO wants information linking people, servers, domains, IP addresses, accounts, or cryptocurrency addresses to the attack, extortion, or movement of money, along with evidence of how the crimes were carried out."*¹³
- Oct 28: Japan Airlines is warning that one of its third party IT providers was hacked and leaked personal records of 92,000 clients. Amadeus IT Group, which runs flight reservation, ticketing and check-in systems, reported *"the hackers stole passport numbers, frequent flyer numbers, email addresses and phone numbers."*¹⁴
- Oct 28: Airline ticket booking site Sky Ticket reported an additional 32,341 customers had financial institution names, account numbers and account holder names compromised. *"The number of customers whose cardholder names and partial card numbers may have been exposed has grown to ... roughly 414,000 people"*¹⁵

10. **What Is 'Artex'?** *"An information security arm of Japanese IT firm GMO Internet Group Inc said ... A Chinese artificial intelligence cybersecurity tool called Artex was used."*¹⁶ *"[Artex is an] autonomous AI agent, designed to diagnose system vulnerabilities, was detected targeting Japanese firms across the retail, logistics, and financial sectors. Investigators discovered six attacking devices exclusively focused on Japanese entities,"*¹⁷ According to Cybersecurity company 'Trend Micro' Artex is one of the AI tools used in the attack. Trend Micro says there were three attack profiles:

- AI running the complete attack,
- AI under human direction, and
- Limited, specific AI assistance.¹⁸

A report by CrowdStrike said Artex *"was also used to hack financial institutions in South Korea in September. ... The attacks largely relied on exploiting weak security controls, such as a lack of multi-factor authentication."*¹⁹ 'Artex' was not used alone.

12 Source: finance.biggo.com . [Bandai Namco Says 346,000 Customer Email Addresses Leaked After Unauthorized Access at Contractor](#)

13 Source: The Hacker News. [Japan's GMO Offers \\$1 Million Bounty to Catch Hackers Behind FX Trading Cloud Breach](#)

14 Source: The Record.media . [Japan Airlines warns of data breach as country grapples with multiple cyber incidents](#)

15 Source: finance.biggo.com . [Japan's Sky Ticket Breach Widens: 32,000 Bank Account Records Leaked, Card Data Affects 936,000](#)

16 Source: Japan Today. [Takaichi vows swift response to wave of cyberattacks](#)

17 Source: [Security Firm Links China-Linked "Artex" AI Agent to Recent Cyberattacks on Japanese Companies](#)

18 Source: TrendAISecurity. [Not Only ARTEX: The Different Levels AI is Used in Attacks Targeting Japan](#)



Cyber-Intelligence Report

Analysis of other 'Artex' attacks identified several other AI, including the PRC's 'DeepSeek', were used.

Other PRC Attacks

11. ARTEX Used Against ConnectWise. Microsoft identified "*Storm-0940, a China state-aligned group, as the actor behind the ConnectWise Cloud Backup supply chain compromise. ... Storm-0940 has been active since 2021 and has historically relied on password spraying and OAuth application abuse to get into Microsoft 365 environments. Adding ARTEX changed the scale of what they could do. In some attacks, the time between initial targeting and achieving privileged cloud access was under three hours. ... The agents used applications that already had permission to access their targets. This allowed the attackers to enter customer environments without requiring users to sign in interactively. ... where authentication succeeded, ... They moved into Microsoft Graph and ran directory reconnaissance, modified application credentials to establish persistence, and attempted changes to identities, groups, and privileged roles. Microsoft identified multiple customer environments with evidence of this follow-on activity.*"²⁰



12. PRC's 'Warp Panda' Targets U.S. Legal Industry. A U.S. based cybersecurity company, 'CrowdStrike', has identified a PRC "*threat actor known as Warp Panda in attacks targeting the U.S. legal sector. ... Warp Panda 'exploits internet-facing edge devices using zero-day vulnerabilities and custom malware to maintain covert, persistent access...' "* In this case, the vulnerability was Broadcom VMware ESX. CrowdStrike warned: "*Warp Panda represents a sustained and strategically focused China-nexus cyber espionage threat to U.S. entities across multiple sectors, including the legal sector.*"²¹

13. 'Warp Typhoon' Targets Telecoms and Aerospace. Warp Typhoon targets "*include telecoms firms, government entities, defense contractors, satellite and*

19 Source: TechCrunch. [Japan internet giant GMO says hackers posted stolen customer data](#)

20 Source: Security Affairs. [Microsoft Links ConnectWise Breach to China-Linked Group Using AI Pentesting Tool ARTEX](#)

21 Source: The Hacker News. [China-Linked Hackers Exploited VMware ESX Zero-Day to Reduce Audit Trail Visibility](#)



Cyber-Intelligence Report

mission-critical communications providers, MSPs, universities with military ties, and critical infrastructure operators. Hawaii, California and Texas were targeted the most. “The current attacks leverage a Cisco SD-WAN vulnerability and a malware framework, named KeyDrift, designed to harvest encryption keys. Information is passed via a network of compromised routers called ‘Silent Train’. *“The [attackers] network routes the attackers’ traffic through chains of hacked small office routers, IoT devices and enterprise systems that are frequently replaced, and the operators clean up after each session.”*²²

14. Storm-2603/Warlock Ransomware. This PRC group is targeting organizations across Europe, Africa and Latin America. *“Victims included a water utility, a telecommunications provider, a regional government body and a university”* accessed through Microsoft SharePoint vulnerabilities. *“Once inside, the group demonstrated a methodical approach, spending nine days mapping the domain and establishing covert remote access. The operation culminated in a rapid deployment phase where the attackers systematically disabled security software across 40 hosts within two hours before deploying ransomware. ... By targeting the security sensors themselves, the Warlock operators effectively blinded the organizations before executing their payload.”*²³

15. New ‘PRC Nexus Operation’ Hits US, Japan, Taiwan, and South Korea. A new PRC hacking group is using two PHP flaws and a Linux kernel bug to attack its targets. The hackers searched for ‘internet-facing firewalls from a specific vendor’, identified 19,000 of them, filtered for newer PHP releases (240 potential targets), then selected 25 of them to target. *“While no post-exploitation activity was observed on 22 of the firewalls, the hackers did progress further on two servers belonging to a US government-affiliated environment.”*²⁴ Analyst Comments: This appears to be a new and focused campaign. More information on the hacking group and their targeting will need to be developed.

16. Australia Warns: Expect More Disruption. The Director-General of the Australian Signals Directorate (ASD), Abigail Bradshaw, warns AI is a major force in the threat landscape. She says *“that with each jump in AI capability, more disruption is likely. ... the most advanced AI models have redefined the threat. ... virtually every service you use runs on a digital network.”*

This cyber-intelligence product is produced by David Swan. It is copyright David Swan 2026. This report is **TLP:CLEAR**²⁵ and MAY be shared freely.

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

22 Source: Security Week. [Cisco SD-WAN Zero-Day Exploitation Tied to Volt Typhoon’s ‘Silent Train’ Network](#)

23 Source: SC Media. [China-linked Warlock ransomware group targets global infrastructure](#)

24 Source: Security Week. [China-Linked Hackers Exploit PHP2Shell to Root Firewalls](#)

25 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.