CENTRE FOR LAND WARFARE STUDIES

CLAWS

VICTORY THROUGH VISION

CLAWS Cyber Index

01 - 15 March 2024

CLAWS Cyber Index ●

Multidomain Studies
Cyber Vertical

Govind Nelika ●
Websitemanager/Researcher, CLAWS

1. Five Eyes Alliance Warns of Attacks Exploiting Known Ivanti Gateway Flaws

The Five Eyes intelligence alliance has issued a cybersecurity advisory warning about threat actors exploiting known vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways. These vulnerabilities, identified as CVE-2023-46805, CVE-2024-21887, and CVE-2024-21893, allow attackers to bypass authentication, craft malicious requests, and execute arbitrary commands with elevated privileges. The advisory also highlights that the Ivanti Integrity Checker Tool is insufficient for detecting compromises due to the sophistication of the attacks. Furthermore, it's noted that despite factory resets on the Ivanti device, threat actors may still maintain root-level persistence (Paganini, 2024)

2. US indicts Iranian man in cyber-espionage campaign against defence contractors

The U.S. Department of Justice has indicted Alireza Shafie Nasab for his alleged involvement in a cyber-espionage campaign against U.S. Defence Department contractors and other government departments. Nasab, a 39-year-old Iranian, is accused of exploiting vulnerabilities in a New York accounting firm to infect over 200,000 devices, targeting more than a dozen companies, many of which were cleared defence contractors. The operation, which spanned from 2016 until April 2021, involved spear phishing attacks and the use of social engineering tactics to gain access to targeted systems. Nasab faces charges of conspiracy to commit computer fraud and wire fraud, as well as wire fraud and aggravated identity theft, with a combined maximum sentence of 47 years in prison (Reddick, 2024).

3. Researchers spot new infrastructure likely used for Predator spyware

Cybersecurity researchers have identified new infrastructure likely used by the operators of the commercial spyware known as Predator in at least 11 countries, including Angola, Armenia, Botswana, Egypt, Indonesia, Kazakhstan, Mongolia, Oman, the Philippines, Saudi Arabia, and Trinidad and Tobago. Predator, developed by the Israeli-owned spyware consortium Intellexa, has been deployed since at least 2019, infecting both Android and iPhone devices. It can access a device's microphone, camera, and all stored or transmitted data, making it highly invasive and challenging to investigate. The Insikt Group identified a multi-level Predator delivery network, including delivery servers and upstream servers, used for device exploitation and initial access. These servers host domains that spoof legitimate websites for specific entities, and the anonymization network makes attributing attacks difficult. Spyware technologies like Predator are marketed for counterterrorism and law enforcement but are often abused to target civil society, including journalists, politicians, and activists.

4. Singapore – INTERPOL and UNICR release Revised toolkit for Responsible AI Innovation in Law Enforcement

INTERPOL and UNICRI have released an updated version of the Toolkit for Responsible AI Innovation in Law Enforcement, aimed at guiding law enforcement agencies on the responsible development and deployment of artificial intelligence (AI). This toolkit, which includes seven distinct resources and a comprehensive user guide, provides guidance from technical foundations to organizational assessments on readiness and risk. The updated toolkit incorporates additional recommendations on AI governance and ethics, enhanced guidance on building AI strategies, illustrative examples and case studies, and aligns with the latest legal, regulatory, and technical developments in the AI landscape. These updates were unveiled during the 4th INTERPOL-UNICRI Global Meeting on Responsible AI for Law Enforcement, held in Singapore, and included dedicated AI Toolkit sessions and workshops to enhance understanding of the toolkit's content and its practical applications in law enforcement work (Interpol, 2024)

5. AUKUS weighs Japan's participation in defence tech development

The U.S. is leading discussions with the U.K. and Australia to invite Japan to collaborate on defence technology under the AUKUS security partnership. This move aims to extend an invitation to Tokyo at a summit between President Joe Biden and Prime Minister Fumio Kishida on April 10. Japan would be the first country invited to work in the trilateral AUKUS framework since its launch in September 2021. The U.S. defence bill has also been noted to strengthen military ties with AUKUS and Japan, indicating a growing alignment in defence technology development and cooperation (Nakamura, 2024)

6. Southeast Asia's three-nation partnership to fight Cyber threats

Australia, Malaysia, and Singapore are exploring a partnership to enhance cybersecurity in Southeast Asia. This initiative aims to address common challenges in digitalizing their economies, including cybercrimes, security of digital systems, and the protection of subsea cables. The partnership could leverage Australia's strengths as a Quad member country in mapping how emerging technologies like artificial intelligence and quantum computing could revolutionize the digital economy and security. It also aligns with Australia's 2040 Southeast Asia Economic Strategy, which focuses on changing how infrastructure is developed and operated, such as increasing automation in ports and growing the electric vehicle ecosystem. The strategy also highlights the growing e-commerce between ASEAN countries and Australia, emphasizing the need for improved cybersecurity and resilience against digital threats that exploit e-commerce (Rahman, 2024)

7. DOJ, Europol, and the NCA, deny involvement in the recent shutdown notice posted by the AlphV/BlackCat ransomware group

The BlackCat ransomware site has claimed that it was seized by UK law enforcement, but UK law enforcement has denied this claim. The situation highlights the ongoing challenges in combating cybercrime, particularly with ransomware groups that often operate with impunity and use sophisticated tactics to evade detection and prosecution. The denial from UK law enforcement underscores the complexity of tracking and taking down cybercriminal operations, which often operate across borders and use various methods to hide their activities and evade law enforcement efforts (Bing, 2024).

8. China takes big swings in 6G wireless technology R&D

China is planning to accelerate the research and development of 6G wireless technology and initiate an "artificial intelligence plus" project to utilize AI for driving new industrialization. This was announced by Jin Zhuanglong, the Minister of Industry and Information Technology, during the ongoing two sessions in Beijing. The country aims to deepen the integration of informatization and industrialization, with a focus on advancing 5G networks, computing power, and other information infrastructure to better harness cutting-edge technologies for various industries. Additionally, China is looking to build a modern industrial system with advanced manufacturing as its core, involving the revitalization of traditional industries and their transition towards high-end, intelligent, and environmentally friendly practices. This includes strengthening key industries to maintain their competitive edge, fostering the development of internationally influential Chinese manufacturing brands, and establishing more national manufacturing innovation centers, advanced manufacturing clusters, and model zones for new industrialization (Si, 2024)

9. Under-testing AI models must get Govt permission before deployment: MeitY, India

The Union Ministry of Electronics and Information Technology (MeitY) has issued an advisory stating that all "under-testing" or "unreliable" artificial intelligence (AI) models must obtain explicit government permission before being deployed in India. This move is part of efforts to ensure that AI tools do not introduce bias, discrimination, or threaten the integrity of the electoral process. Additionally, intermediaries are instructed to label all synthetically created media and text with unique identifiers or metadata to make such content easily identifiable. This advisory comes in response to concerns over the use of AI models, particularly in the context of misinformation and deepfakes, and follows discussions with social media companies and technology firms on the issue. The advisory emphasizes the importance of compliance and the need for intermediaries to clearly inform users about the potential fallibility or unreliability of AI-generated content (Agrawal, 2024)

10. North Korea broke into S. Korean chip equipment firms, Seoul's spy agency says

North Korea has reportedly infiltrated South Korean chip equipment firms, according to South Korea's National Intelligence Service (NIS). The infiltration is part of North Korea's efforts to gain access to advanced technology and intellectual property, which could be crucial for its military and economic development. The NIS has identified several instances where North Korean hackers have targeted South Korean companies including those involved in the production of semiconductors and other high-tech equipment. This development underscores the ongoing cybersecurity challenges faced by South Korea, as it seeks to protect its critical infrastructure and technological advancements from external threats (Shin, 2024).

Canada's financial intelligence unit offline after cyberattack

FINTRAC has acknowledged a cyber incident that occurred over the last 24 hours, which does not involve the Centre's intelligence or classified systems. In response to the incident, FINTRAC has taken its corporate systems offline as a precautionary measure to ensure the integrity of its systems and to protect the information it maintains. FINTRAC is collaborating with its federal partners, including the Canadian Centre for Cyber Security (Cyber Centre), to protect and restore its systems (Canada, 2024)

Google opens cyber defence hub in Tokyo

Google has established its first Asia-Pacific cyber defence hub in Tokyo, aiming to address growing cybersecurity concerns in the region, particularly from China and other sources. The hub will collaborate with the Japanese government, as well as companies and universities, to share the latest information on cyberattack countermeasures. It will also serve as a training base for regional cyber defence experts, focusing on research and development to enhance cybersecurity across the Asia-Pacific region (staff, 2024).

China-Linked Cyber Spies Blend Watering Hole, Supply Chain Attacks

The Evasive Panda hacking team, linked to China, has conducted a sophisticated cyber-operations campaign that blends watering-hole and supply chain attacks. This campaign, which began in September 2023, targeted users in India, Taiwan, Australia, the United States, and Hong Kong. The group compromised websites of organizations promoting Tibetan Buddhism, a Tibetan language translation application, and a news website, unknowingly hosting malicious programs. Visitors from specific global locations were infected with droppers and backdoors, including the group's preferred MgBot and a relatively new backdoor program, Nightdoor. The campaign showcased a variety of attack vectors, including an adversary-in-the-middle (AitM) attack via a software update, exploiting a development server, a watering hole, and phishing emails. The Evasive Panda group, active since 2012, is known for its supply chain attacks and has used stolen code-signing credentials and application updates to infect systems in China and Africa in 2023. The group has targeted individuals within China for surveillance purposes and has also compromised government agencies in China, Macao, and Southeast and East Asian nations. The Georgia Institute of Technology was among the organizations attacked in the United States. Evasive Panda has developed its own custom malware framework, MgBot, and introduced Nightdoor in 2020, pointing to the group's involvement in cyber-espionage activities (Lemos, 2024).

Ex-Google engineer charged with stealing AI trade secrets

Linwei Ding, a former software engineer at Google, has been charged with stealing artificial intelligence (AI) trade secrets from the company while secretly working with two Chinese companies. Ding, a Chinese national, was arrested in Newark, California, on four counts of federal trade secret theft, each punishable by up to 10 years in prison. This case was announced at an American Bar Association conference in San Francisco by Attorney General Merrick Garland, highlighting the threat of Chinese economic espionage and the national security concerns posed by advancements in AI and other developing technologies. The FBI executed a search warrant at Ding's home, seizing his electronic devices, and later executed an additional warrant for the contents of his personal accounts, which contained more than 500 unique files of confidential information that authorities say he stole from Google. Google has strict safeguards to prevent the theft of confidential commercial information and trade secrets, and after an investigation, referred the case to law enforcement. (Tucker, 2024)

CISA Executive director warns of China's Cyber strategy

Brandon Wales, the executive director of the US Cybersecurity and Infrastructure Security Agency, has warned of a significant shift in China's cybersecurity strategy, moving from passive espionage to actively preparing for offensive cyberattacks. This shift aims to disrupt American military activities in the Asia-Pacific and potentially cause societal chaos. Wales highlighted that China is the dominant cybersecurity threat the US faces, with evidence of China burrowing inside networks for several years to prepare for potential attacks. Wales emphasized that China's goals include stealing political and intellectual property secrets while also preparing for disruptive cyberattacks on adversaries' critical infrastructure in the event of a conflict. He noted that the evidence of these activities coming to fruition requires a coordinated effort from the United States and its allies to prevent them (Knott, 2024).

South Korean Man arrested in Russia on Cyber Espionage charges.

Russia has arrested a South Korean man on suspicion of spying, according to TASS, the Russian news agency. The arrest is part of a broader crackdown on foreign espionage activities, which have been a concern for Russia in recent years. The specific details of the man's activities, the motive behind his alleged espionage, and the extent of his involvement in any larger network are not provided in the available information.Espionage cases involving foreign nationals are not uncommon, especially in countries with significant strategic interests or in regions of geopolitical tension. The arrest underscores the ongoing tensions and the security concerns that arise from the activities of foreign entities within a country's borders (Black, 2024).

Works Cited

Agrawal, A. (2024, March 02). *Under-testing AI models must get govt permission before deployment:* MeitY. Hindustantimes: Retrieved March 10, 2024, from https://www.hindustantimes.com/india-news/undertesting-ai-models-must-get-govt-permission-before-deployment-meity-101709390335142.html

Bing, J. P. (2024, March 6). *'Exit scam' - hackers that hit UnitedHealth pull disappearing act*. Reuters Retrieved March 10, 2024, from https://www.reuters.com/technology/cybersecurity/blackcat-ransomware-site-claims-it-was-seized-uk-law-enforcement-denies-being-2024-03-05/

Black, D. (2024, Marh 12). *Russia arrests Korean man on espionage charges*. Cybernews: Retrieved March 15, 2024, from https://cybernews.com/cyber-war/russia-arrests-korean-man-cyber-espionage/

Canada, G. o. (2024, March 03). *FINTRAC Statement*. Fintrac: Retrieved March 10, 2024, from https://fintrac-canafe.canada.ca/new-neuf/statement-declaration-eng

Interpol. (2024, March 6). *Revised toolkit empowers law enforcement with responsible AI practices*. Interpol: Retrieved March 10, 2024, from https://www.interpol.int/en/News-and-Events/News/2024/Revised-toolkit-empowers-law-enforcement-with-responsible-AI-practices

Knott, M. (2024, March 13). *'Societal chaos': US cyber chief sounds alarm on China threat*. The Syndey Morning Herald: Retrieved March 14, 2024, from https://www.smh.com.au/politics/federal/societal-chaos-us-cyber-chief-sounds-alarm-on-china-threat-20240312-p5fbo8.html

Lemos, R. (2024, March 7). *China-Linked Cyber Spies Blend Watering Hole, Supply Chain Attacks*. Darkreading: Retrieved March 10, 2024, from https://www.darkreading.com/cyberattacks-data-breaches/china-linked-cyber-spies-blend-watering-hole-supply-chain-attacks

Nakamura, R. (2024, March 2). *AUKUS weighs Japan's participation in defense tech development*. Asia Nikkei Retrieved March 10, 2024, from: https://asia.nikkei.com/Politics/Defense/AUKUS-weighs-Japan-s-participation-in-defense-tech-development

Paganini, P. (2024, March 01). *Five Eyes Alliance warns of attacks exploiting known Ivanti Gateway Flaws*. securityaffairs: Retrieved March 10, 2024, from https://securityaffairs.com/159807/hacking/fiveeye-warns-ivanti-gateways-attacks.html

CLAWS Cyber Index

Rahman, M. F. (2024, March 1). *Southeast Asia's three-nation partnership to fight cyber threats*. The Mandarin: Retrieved March 10, 2024, from https://www.themandarin.com.au/240775-southeast-asias-three-nation-partnership-to-fight-cyber-threats/

Reddick, J. (2024, March 1). *US indicts Iranian man in cyber-espionage campaign against defense contractors.* The Record: Retrieved March 10, 2024, from https://therecord.media/iranian-indicted-cyber-espionage-campaign-us-defense-contractors

Shin, H. (2024, March 4). *North Korea broke into S. Korean chip equipment firms, Seoul's spy agency says.* Reuters: Retrieved March 10, 2024, from https://www.reuters.com/world/asia-pacific/north-korea-broke-in-to-s-korean-chip-equipment-firms-seouls-spy-agency-says-2024-03-04/

Si, M. (2024, March 08). *China takes big swings in 6G wireless technology R&D.* Chinadaily: Retrieved March 10, 2024, from https://www.chinadaily.com.cn/a/202403/08/WS65eab174a31082fc043bb82f.html

staff, N. (2024, March 7). Google opens cyberdefense hub in Tokyo. Asia Nikkei: Retrieved March 10, 2024, from https://asia.nikkei.com/Business/Technology/Google-opens-cyberdefense-hub-in-Tokyo

Tucker, E. (2024, March 7). Ex-Google engineer charged with stealing AI trade secrets while working with Chinese companies. Assocated Press: Retrieved March 11, 2024, from https://apnews.com/article/china-google-justice-department-63156ade1e564d15d92adbef91e9c5da

About the Author

Govind Nelika is the Web Manager/Researcher at the Centre for Land Warfare Studies (CLAWS). He is an alumnus of Pondicherry Central University with a degree in Political Science complemented by a certification in Data Sciences from IBM. His research approach is multidisciplinary in nature, and his focus area at CLAWS is on emerging challenges and trends in the fields of Cybersecurity, OSINT, and the evolving landscape of Strategic Technology, synergized with Generative AI and LLM.

© All Rights Reserved 2023 Centre for Land Warfare Studies (CLAWS)

No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from CLAWS The views expressed and suggestions made in the article are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.