CLAWS Cyber Index

01 - 15 April 2024

CLAWS Cyber Index

Multidomain Studies
Cyber Vertical

Govind Nelika ●
Websitemanager/Researcher, CLAWS

1. Pentagon unveiled Defence Industrial Base (DIB) Cybersecurity Strategy

The Pentagon has unveiled its first-ever Defence Industrial Base (DIB) Cybersecurity Strategy to enhance the cybersecurity and resilience of its massive industrial base. This strategy, which spans from fiscal years 2024 through 2027, aims to protect the DIB from cyber threats by improving best practices within the industrial base. The strategy outlines four topline goals, each containing a subset of objectives, such as the ability to recover from a cyberattack. A key component of this strategy is the Cybersecurity Maturity Model certification program, which aims to raise cybersecurity standards among contractors to ensure compliance and resilience. The strategy's implementation will focus on addressing the vulnerabilities that could lead to breaches, emphasizing the importance of quickly patching vulnerabilities to prevent a "feeding frenzy" among cybercriminals. This approach underscores the Pentagon's commitment to safeguarding its industrial base against cyber threats, ensuring the resilience and security of the nation's defence capabilities (Matishak, 2024).

2. Federal Court upholds FCC right to ban Chinese surveillance tech

A federal appeals court has upheld the Federal Communications Commission's (FCC) right to ban video surveillance products made by Chinese-owned companies Hikvision and Dahua. The decision is based on the Secure Equipment Act (SEA) of 2021, which was enacted to counteract the national security threat posed by telecommunications equipment that could be accessed by the Chinese government. The FCC's ban on Hikvision and Dahua products is justified under this law, as these companies' products could potentially be used by China to surveil U.S. critical infrastructure. However, the court also noted that the FCC's definition of critical infrastructure was deemed too broad and arbitrary. The FCC's order stated that the ban applies to equipment used for public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes. The court found that the FCC's interpretation of critical infrastructure was overly broad, particularly in its use of the term "connected to" when defining critical infrastructure. The court emphasized that it is implausible that every system or asset connected to sectors like food and agriculture or water supply is critical to U.S. national security (Smalley, 2024).

3. Android Apps used as proxy "PROXYLIB"

Android apps have been identified as turning Android phones into proxies for cybercriminals. This operation, codenamed PROXYLIB, involves the use of a software development kit (SDK) from LumiApps, which contains the proxyware functionality. The malicious apps utilize a native Golang library to achieve this, transforming the user's device into a proxy node without their knowledge. The apps were found on the Google Play Store and have since been removed by Google (Arntz, 2024).

4. Indian MEA rescues 250 Indians from 'cyber slavery'

The Indian Ministry of External Affairs (MEA) has been actively collaborating with Cambodian authorities to rescue and repatriate Indian citizens who have been trapped in Cambodia, allegedly being forced to carry out cyber frauds. This initiative comes in response to reports that over 5,000 Indians are trapped in Cambodia, where they are said to be held against their will and compelled to engage in illegal cyber activities. The government estimates that these individuals have duped people in India of at least Rs 500 crore over the past six months. As of the latest update, the MEA has successfully rescued and repatriated about 250 Indians, with 75 of these rescues occurring in the last three months. This collaborative effort between the Indian government and Cambodian authorities is a significant step in addressing the issue of cyber slavery and ensuring the safety and well-being of Indian citizens abroad (Indianexpress, 2024).

CLAWS Cyber Index

5. China-linked Hackers Deploy New 'UNAPIMON' Malware

China-linked hackers have deployed a new malware named UNAPIMON, which is part of a threat activity cluster known as Earth Freybug. This group, which has been active since at least 2012, focuses on espionage and financially motivated activities, targeting organizations across various sectors and countries. Earth Freybug is considered a subset of APT41, a China-linked cyber espionage group also known by several other names. The group employs a combination of living-off-the-land binaries (LOLBins) and custom malware, along with techniques like dynamic-link library (DLL) hijacking and application programming interface (API) unhooking. The malware deployment begins with the use of a legitimate executable associated with VMware Tools ("vmtoolsd.exe") to create a scheduled task using "schtasks.exe" and deploy a file named "cc.bat" on the remote machine. The method of injecting malicious code into "vmtoolsd.exe" is not fully understood, but it's suspected to involve exploiting external-facing servers (Thehackernews, 2024).

6. CISA issue notice on Compromise of Sisense Customer Data

The Cybersecurity and Infrastructure Security Agency (CISA) has issued an alert regarding a compromise of customer data at Sisense, a company that provides data analytics services. This incident was discovered by independent security researchers and has led to CISA collaborating with private industry partners to address the situation. The compromise potentially exposes or uses credentials to access Sisense services, prompting customers to reset their credentials and secrets to mitigate the risk. CISA is actively involved in the response to this incident, especially concerning impacted critical infrastructure sector organizations. It encourages customers to investigate any suspicious activity involving credentials that may have been exposed or used to access Sisense services and and report any findings to CISA. This proactive approach aims to protect the affected organizations and the broader infrastructure sector from potential cyber threats (CISA, 2024).

7. Iran Threat Actor MuddyWater adopts C2 infrastructure

The Iranian threat actor known as MuddyWater has adopted a new command-and-control (C2) infrastructure named DarkBeatC2, marking the latest tool in its arsenal. This group, also known by aliases such as Boggy Serpens, Mango Sandstorm, and TA450, is believed to be affiliated with Iran's Ministry of Intelligence and Security (MOIS) and has been active since at least 2017. MuddyWater is known for orchestrating spear-phishing attacks that lead to the deployment of various legitimate Remote Monitoring and Management (RMM) solutions on compromised systems. The group has previously used other C2 frameworks, including SimpleHarm, MuddyC3, PhonyC2, and MuddyC2Go. (Thehackernews, 2024).

8. China tests US voter fault lines and ramps AI content to boost its geopolitical interests

The Microsoft Threat Analysis Center (MTAC) has published insights into China's use of AI and cyber operations to influence elections and advance its geopolitical interests. The report highlights China's employment of fake social media accounts to understand U.S. voter fault lines and the increased use of AI-generated content to sow division and influence public opinion. This strategy is part of China's broader influence operations (IO) targeting the South Pacific islands, the South China Sea region, and the U.S. defense industrial base. In the Taiwanese presidential election in January 2024, there was a notable surge in the use of AI-generated content by CCP-affiliated actors, marking the first time Microsoft Threat Intelligence observed a nation-state actor using AI content to influence a foreign election. The group, known as Storm-1376, used AI-generated fake audio and memes to influence the election, including a suspected AI-gener-

CLAWS Cyber Index

audio of Foxconn owner Terry Gou endorsing another candidate, which was quickly removed by YouTube (Watts, 2024).

9. Germany to launch cyber military branch

Germany has initiated a significant military reform with a new command structure, aiming to enhance its readiness for potential conflicts, particularly in response to Russia's invasion of Ukraine in 2022. The Defence Minister, Boris Pistorius, announced plans for a major restructuring of the Bundeswehr, including the establishment of a fourth branch specializing in cyber warfare. This new branch, known as the Cyber and Information Domain Service (CIR), will focus on defending against cyberattacks, protecting electronic infrastructure, and countering disinformation and other hybrid threats. The expansion of the military's branches to include cyber warfare is a strategic move to address the evolving nature of warfare and the increasing importance of cybersecurity in modern conflicts (DW, 2024).

10. Android Espionage Campaign Targeting India and Pakistan

A new Android espionage campaign, identified as SpyLoan, has been spotted targeting users in India and Pakistan. This campaign involves the use of deceptive apps designed to steal sensitive information from Android devices. The SpyLoan scams are part of a broader trend of cyber espionage activities, where attackers use malicious apps to compromise user data and gain unauthorized access to personal and financial information. The SpyLoan scams typically involve the distribution of apps that appear to offer legitimate services, such as loans or financial advice, but are actually designed to collect user data. Once installed, these apps can access a wide range of information, including contact lists, messages, and financial details. The collected data is then used for various purposes, including identity theft, financial fraud, and cyber espionage (Poireault, 2024).

11. Apple warns users of "mercenary spyware" attack

Apple has issued a warning to users about a "mercenary spyware" attack that has impacted India and 91 other countries. This warning is part of Apple's efforts to protect its users from cyber threats and to raise awareness about the potential risks associated with such attacks. The term "mercenary spyware" refers to malicious software that is designed to collect sensitive information from users without their knowledge or consent. This type of attack can target a wide range of devices and platforms, including those running Apple's iOS operating system. The warning from Apple is a proactive measure to inform users about the ongoing threat and to provide guidance on how to protect themselves. It is important for users to be vigilant about the apps they download and the permissions they grant to these apps. Apple advises users to only download apps from trusted sources, such as the App Store, and to regularly update their devices to the latest software versions to ensure they have the latest security patches (Aryan, 2024).

12. Chinese owned Semiconductor company targeted by ransomware

Nexperia, a Chinese-owned semiconductor company based in the Netherlands, has been targeted by a ransomware attack. The attackers, identified as a group named Dunghill Leak, uploaded stolen confidential documents to a darknet extortion site. This incident was announced by Nexperia in a statement, revealing that unauthorized access to certain IT servers occurred in March 2024. The company has engaged Fox-IT to investigate the details of the attack, with no further details disclosed at this time. This is not the first time Nexperia has faced cybersecurity challenges; it previously clashed with the British government over the acquisition of the UK's largest microprocessor factory, the Newport Wafer Fab, amid a global semiconductor supply shortage. The British government ordered Nexperia to sell at least 86% of the acquired company, citing national security concerns related to the potential reintroduction of compound semiconductor activities at

CLAWS Cyber Index

the Newport site. Nexperia sold the Newport Wafer Fab to Vishay Intertechnology, a US-based firm, for $177 million last month (Martin A. , 2024)..

Work Cited

Arntz, P. (2024, April 01). *Free VPN apps turn Android phones into criminal proxies.* Malwarebytes Retrieved April 03, 2024, from https://www.malwarebytes.com/blog/news/2024/04/free-vpn-apps-turn-android-phones-into-criminal-proxies

Aryan, A. (2024, April 12). *Apple warns users of "mercenary spyware" attack; India, 91 other countries impacted*. The Economic Times Retrieved April 13, 2024, from https://economictimes.indiatimes.com/tech/technology/exclusive-apple-warns-users-of-mercenary-spyware-attack-india-91-other-countries-impacted/articleshow/109210976.cms?from=mdr

CISA. (2024, April 11). *Compromise of Sisense Customer Data*. CISA Retrieved April 13, 2024, from https://www.cisa.gov/news-events/alerts/2024/04/11/compromise-sisense-customer-data

DW. (2024, April 04). *Germany launches military reform with new command structure.* DW Retrieved April 06, 2024, from https://www.dw.com/en/germany-launches-military-reform-with-new-command-structure/a-68740863

Indianexpress, T. (2024, March 31). *Collaborating closely with Cambodia, rescued 250 Indians: MEA on 'cyber slavery'.* The Indianexpress Retrieved April 01, 2024, from https://indianexpress.com/article/india/collaborating-closely-with-cambodia-rescued-250-indians-mea-on-cyber-slavery-9242557/

Martin, A. (2024, April 15). *Chinese-owned semiconductor company Nexperia hit by ransomware attack.* The Record Retrieved April 15, 2024, from https://therecord.media/nexperia-semiconductor-company-ransomware-incident?

Matishak, M. (2024, March 29). Pentagon lays out strategy to improve defense industrial base cybersecurity. The Record Retrieved April 01, 2024, from https://therecord.media/pentagon-unveils-first-ever-defense-industrial-base-strategy?

Poireault, K. (2024, April 11). *New Android Espionage Campaign Spotted in India and Pakistan*. Infosecurity Magazine Retrieved April 13, 2024, from https://www.infosecurity-magazine.com/news/android-espionage-campaign-india/

Smalley, S. (2024, April 4). *Court upholds FCC right to ban tech from Chinese-owned telecom companies*.The Record Retrieved April 06, 2024, from https://therecord.media/court-upholds-fcc-ban-on-hikvision-dahua-products?

Thehackernews. (2024, April 02). *China-linked Hackers Deploy New 'UNAPIMON' Malware for Stealthy Operations.* Thehackernews Retrieved April 04, 2024, from https://thehackernews.com/2024/04/china-linked-hackers-deploy-new.html?

CLAWS Cyber Index

Thehackernews. (2024, April 12). Iranian MuddyWater Hackers Adopt New C2 Tool 'DarkBeatC2' in Latest Campaign. Thehackernews Retrieved April 13, 2024, from https://thehackernews.com/2024/04/iranian-muddywater-hackers-adopt-new-c2.html?

Watts, C. (2024, April 4). *China tests US voter fault lines and ramps AI content to boost its geopolitical interests*. Mircrosoft Blog Retrieved April 5, 2024, from https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/

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.