CLAWS Cyber Index

15 - 30 March 2024

CLAWS Cyber Index

Multidomain Studies
Cyber Vertical

Govind Nelika
Websitemanager/Researcher, CLAWS

Lock Bit ransomware leader vows revenge

The leader of the Lock Bit ransomware group, known as LockBitSupp, vowed to continue his operations despite the group's recent takedown by international law enforcement. The takedown, which occurred in February 2024, resulted in the seizure of LockBit's platform, hacking tools, cryptocurrency accounts, and source code, effectively disrupting the group's four-year ransomware rampage. LockBit has been linked to numerous attacks on hospital systems and critical infrastructure, including significant incidents in Canada and the United States (Dina Temple-Raston, 2024).

Russia Sanctions Americans due to Russo-Phobic Policies

Russia has imposed new sanctions on hundreds of Americans, including prominent journalists and cybersecurity experts, as part of its response to what it perceives as "Russo phobic policies" supported by the United States. The sanctions target individuals involved in activities that Russia deems as "anti-Russian actions," such as reporting on cybersecurity issues. The list of sanctioned individuals includes journalists like Robert F. Worth from the New York Times Magazine and Jeff Seldin from the Voice of America, as well as cybersecurity columnists from the Washington Post, such as Ellen Nakashima, Joseph Menn, Joseph Marks, and Tim Starks. These sanctions are seen as a response to legal restrictions imposed by the U.S. on Russian citizens supporting the Kremlin and the war against Ukraine, which Russia refers to as a special military operation (Antoniuk, 2024).

U.S Sanctions Russian Nationals for alleged disinformation Campaign

The U.S. Treasury Department has sanctioned two Russian nationals, Ilya Andreevich Gambashidze and Nikolai Aleksandrovich Tupikin, along with two companies, Social Design Agency and Company Group Structure, for their alleged involvement in a disinformation campaign. This campaign is believed to have been aimed at impersonating legitimate media outlets. The companies are accused of creating websites and social media accounts that mimic government organizations and European media outlets, with the goal of amplifying content. In the fall of 2022, it is reported that Tupikin and Gambashidze created around 60 fake news websites, fictitious social media accounts, and staged videos as part of this campaign. Both Structura and Social Design Agency were previously sanctioned by the European Union for their involvement in Doppelgänger. The U.S. government has also linked these entities to a disinformation campaign across Latin America, aimed at undermining support for Ukraine and discrediting the U.S. and NATO (Greig, 2024).

Elon Musk's SpaceX to build spy satellite network for US intelligence under classified contract

SpaceX, the aerospace manufacturer and space transportation company founded by Elon Musk, is reportedly building a network of spy satellites for the U.S. intelligence agency, according to sources familiar with the matter. This development marks a significant expansion of SpaceX's role in the defense sector, beyond its existing capabilities in launching satellites for various commercial and governmental purposes. The spy satellite network is part of a broader effort by the U.S. intelligence community to enhance its surveillance capabilities, particularly in the context of global security challenges. While specific details about the nature of the spy satellites, their intended missions, or the scale of the project are not disclosed in the source, the involvement of SpaceX indicates a growing collaboration between the private sector and government agencies in space-related projects (Roulette, 2024).

Japan doubles defence tie-ups with private sector in AI powered drones

Japan has significantly increased its defence ties with the private sector, particularly in the areas of drones and artificial intelligence (AI), according to reports. This move is part of Japan's broader strategy to enhance its defence capabilities and leverage private sector innovation to address emerging security challenges. The expansion of defence ties with the private sector reflects Japan's recognition of the importance of integrating cutting-edge technologies into its defence arsenal. Drones and AI are seen as key technologies that can enhance surveillance, reconnaissance, and precision strikes, making them attractive areas for collaboration

CLAWS Cyber Index

between the government and private companies. The collaboration between Japan's defence agencies and private sector entities is expected to accelerate the development and deployment of advanced defence technologies. This includes the use of drones for surveillance and reconnaissance missions, as well as the application of AI for enhancing the capabilities of these drones, such as improved target identification and autonomous decision-making (Takeuchi, 2024).

China warns foreign hackers infiltrating business and government networks

China has issued warnings about foreign hackers infiltrating hundreds of business and government networks, highlighting the rampant attacks by overseas agencies in recent years. This comes as Beijing broadens the scope of its anti-espionage law to include online attacks and prepares to expand penalties for data violations. The top spy agency in China is urging Chinese citizens to enhance their cybersecurity measures in response to these threats. The Ministry of State Security (MSS) has provided examples of typical attacks, such as a hi-tech enterprise being blackmailed after its infosystem and data were encrypted and controlled by a foreign hacking group, interrupting daily operations. The MSS also mentioned that hackers often use phishing emails, targeted software loopholes, and injected code to gain access to a victim's device. It urged people and organizations to report any attacks or ransom threats to national security authorities (Wong, 2024).

G7 industry ministers agree to cooperate on AI, supply chains, presidency says

The G7 countries have agreed to align their rules on artificial intelligence (AI) during the Italian presidency, according to a statement from the Italian Presidency. This move is part of the G7's efforts to ensure that AI technologies are developed and used in a way that is safe, ethical, and beneficial for society. The alignment of rules on AI among the G7 countries reflects a collective commitment to addressing the challenges posed by AI, including issues related to privacy, security, and the ethical use of AI. The G7's focus on aligning rules on AI is significant, given the rapid advancements in AI technology and its potential impact on various aspects of society, including healthcare, transportation, and security. By working together to establish common standards and guidelines, the G7 aims to ensure that AI technologies are developed and used in a manner that is consistent with the values and principles of the member countries (Reuters, 2024).

New Variant of Acid Rain Malware detected

A new variant of the data-wiping malware Acid Rain, known as Acid Pour, has been detected targeting Linux x86 devices. This malware is specifically designed for Linux x86 systems and is compiled as an ELF binary, which is different from the original Acid Rain malware that targeted MIPS architectures. Acid Pour is capable of erasing content from RAID arrays and Unsorted Block Image (UBI) file systems by specifying file paths like "/dev/dm-XX" for RAID arrays and "/dev/ubiXX" for UBI file systems. The malware was first identified in the context of the Russo-Ukrainian war, where it was used against KA-SAT modems from U.S. satellite company Viasat. The cyber attack was attributed to Russia by the Five Eyes nations, along with Ukraine and the European Union (Hackernews, 2024).

Europe's Commission initiates investigation on companies using Generative AI

The European Commission has initiated investigations into three major entities under the Digital Services Act (DSA), focusing on generative AI, consumer protection practices, and compliance with the EU's new content rules. These investigations are part of the Commission's efforts to ensure that online platforms adhere to the bloc's regulations, particularly concerning the spread of deepfake content and the protection of sensitive data. The Commission has sent requests for information to major social media and search companies, including AliExpress, LinkedIn, Facebook, Snapchat, TikTok, YouTube, X (formerly Twitter), Instagram, Google, and Bing. These requests are the first step towards an official investigation into how these companies are handling generative AI, which has been linked to the creation of deepfake videos and other manipulated content. The companies have already signed voluntary commitments to combat electoral threats associated with generative AI, but the Commission is seeking more detailed information on their measures to mitigate such risks TH: This marks the first time a Chinese e-commerce company has been targeted for potential DSA enforcement (Scott, 2024).

CLAWS Cyber Index

North Korea linked group employs cyber-attack on South Korea

The North Korea-linked threat group Kimsuky, also known as APT43, Emerald Sleet, and Velvet Chollima, has conducted a sophisticated and multistage cyberattack against South Korean entities, as detailed in the Dark Reading article. This campaign, named "DEEP#GOSU," is characterized by its eight-stage attack chain, which is significantly longer than typical cyberattacks that usually involve five or fewer stages. The attackers employed a strategy of "living off the land," using legitimate cloud services and evasive malware to conduct cyber espionage and financial crimes. The attack began with the execution of a LNK file attached to an email, which downloaded PowerShell code from Dropbox. This initial stage set the foundation for the attacker's toolkit, which included the installation of various .NET assemblies, legitimate code components for .NET applications. The attackers also utilized LNK files, command scripts downloaded from Dropbox, and code written in PowerShell and VBScript to execute offensive operations. Despite the use of legitimate services like Dropbox and Google Docs for command and control (C2) communication, the attackers actively aimed to evade detection, employing techniques such as shutting down security tools and adding payloads to exclusions (Lemos, 2024).

APT Earth Krahang compromises 48 government organizations across five continents.

Chinese linked APT group known as Earth Krahang, which has compromised 48 government organizations across five continents. This group, also known as APT40, has been active since at least 2015 and has targeted entities in various sectors, including government, military, and critical infrastructure. Earth Krahang's modus operandi involves spear-phishing campaigns, exploiting vulnerabilities in software, and using stolen credentials to gain unauthorized access to systems. The group has been particularly adept at leveraging zero-day vulnerabilities, with targets in North America, Europe, Asia, Africa, and Australia. The group's ability to operate across different continents and sectors demonstrates the evolving landscape of cyber threats (Nelson, 2024).

The "GoFetch" Vulnerability in Apple M-Series, what to know.

The "GoFetch" vulnerability in Apple M-series chips has been identified as a significant security flaw that could potentially leak secret encryption keys. This vulnerability is a result of a microarchitectural side-channel attack that exploits the data memory-dependent prefetcher (DMP) feature of the chips. The DMP is designed to optimize memory access by predicting future memory access patterns and prefetching data accordingly. However, this feature can be exploited to reveal sensitive data from the CPU cache, undermining the security of cryptographic operations. The attack requires the attacker and the victim to have processes co-located on the same machine and CPU cluster. The vulnerability allows an attacker to monitor microarchitectural side channels, such as cache latency, to extract secret keys used during cryptographic operations. This poses a serious threat to the security of data, as it bypasses the protections offered by constant-time programming against timing side-channel attacks. To mitigate this vulnerability, researchers suggest treating access to the host system's graphics card via the browser as a sensitive resource, requiring websites to seek user permission before use. Additionally, Apple's data-independent timing (DIT) feature, which ensures that certain instructions are completed in a constant amount of time, can help prevent timing-based leakage. However, this feature is not available on all M-series processors, and developers are advised to avoid conditional branches and memory access locations based on the value of secret data to effectively block adversaries from inferring secrets. Given the fundamental nature of the flaw, it cannot be fixed in existing Apple CPUs. Developers of cryptographic libraries are urged to take steps to prevent conditions that allow "Go Fetch" to succeed, which may introduce a performance hit. Users are also advised to keep their systems up to date to mitigate the risk of exploitation (Newsroom, 2024).

GitHub Developers Complex Supply Chain Cyberattack

The sophisticated supply chain cyberattack targeted members of the Top.gg GitHub organization and individual developers, aiming to inject malicious code into the code ecosystem. The attackers employed a variety of techniques, including hijacking GitHub accounts with stolen cookies, contributing malicious code via verified commits, establishing a counterfeit Python mirror, and releasing tainted packages on the PyPI registry. They also utilized a typo squatting technique with a fake Python mirror-domain to deceive users, tampering with popular Python packages like Colorama to conceal malicious code within seemingly legitimate software. This allowed the attackers to expand their reach beyond

CLAWS Cyber Index

GitHub repositories and exploit high-reputation GitHub Top.gg accounts to increase the credibility of their actions (Eddy, 2024).

Meta Is Preparing for Indian General Elections 2024

Meta is taking significant steps to prepare for the Indian General Elections 2024, focusing on limiting misinformation, removing voter interference, and enhancing transparency and accountability on its platforms. The company has around 40,000 people globally working on safety and security, with more than $20 billion invested in teams and technology since 2016. This includes 15,000 content reviewers who review content across Facebook, Instagram, and Threads in more than 70 languages, including 20 Indian languages. As the election approaches, Meta will activate an Elections Operations Center to identify potential threats and put mitigations in place in real time. Meta is closely engaged with the Election Commission of India via the Voluntary Code of Ethics joined in 2019, providing a high priority channel to flag unlawful content. The company is also focusing on addressing online misinformation by removing serious kinds of misinformation from its platforms and working with independent fact-checking organizations. It is making it easier for fact-checking partners across India to find and rate content related to the elections, using keyword detection and onboarding them to the new research tool, Meta Content Library (Meta, 2024).

UN Adopts resolution on AI

The UN General Assembly adopted a landmark resolution on artificial intelligence (AI) on March 11, 2024. This resolution emphasizes the promotion of "safe, secure, and trustworthy" AI systems, aiming to benefit sustainable development for all. The resolution was led by the United States and was co-sponsored by more than 120 other Member States. It highlights the importance of respecting, protecting, and promoting human rights in the design, development, deployment, and use of AI. This is the first time the Assembly has adopted a resolution on regulating the emerging field of AI. The resolution also recognizes the potential of AI systems to accelerate progress towards achieving the 17 Sustainable Development Goals (Nations, 2024).

New Zealand alleges China sponsored threat actors in Parliament breach

The New Zealand government has expressed concerns to China regarding its involvement in a state-sponsored cyber hack on New Zealand's parliament in 2021. This comes amid global accusations against China for widespread cyber espionage campaigns. New Zealand's Foreign Minister Winston Peters denounced foreign interference and urged China to refrain from such activities. The New Zealand government linked the cyber-attack to a Chinese state-sponsored actor known as Advanced Persistent Threat 40 (APT40). China has vehemently denied these accusations, calling them groundless and rejecting any interference in other countries' affairs. Additionally, New Zealand highlighted the departure of seven citizens who provided training to China's military, posing a significant national security risk. Similar cyber-attacks attributed to state-sponsored actors have also been condemned in the past, including those from Russia. The United States and Britain have recently filed charges against China for cyber espionage, labelling the hacking group responsible as Advanced Persistent Threat 31 (APT31). Australia also joined in condemning such actions, emphasizing the threat to democratic institutions and processes (Craymer, 2024).

Zero Day Exploits increase by 50% in 2023

In 2023, the number of zero-day exploits observed in the wild jumped by 50% compared to 2022, with Google researchers identifying 97 zero-day vulnerabilities exploited, up from 62 in 2022. This increase was attributed to a variety of factors, including the sophistication of attacks by nation-state hackers and cybercriminals, and the role of commercial spyware vendors (CSVs) in exploiting vulnerabilities (Maddie Stone, 2024).

CLAWS Cyber Index

Works Cited

Antoniuk, D. (2024, March 15). *Russia targets hundreds of Americans with new sanctions, including cyber journalists* at The Dark Reading. Retrieved March 17, 2024, from https://therecord.media/russia-new-sanctions-on-cyber-journalists-americans

Craymer, L. (2024, March 26). *New Zealand accuses China of hacking parliament, condemns activity at Reuters.* Retrieved March 28, 2024, from https://www.reuters.com/technology/cybersecurity/new-zealand-says-parliamentarian-entities-hit-2021-by-malicious-cyber-activity-2024-03-25/

Dina Temple-Raston, e. a. (2024, March 15). E*xclusive: After LockBit's takedown, its purported leader vows to hack on*. The Record. Retrieved March 16, 2024, from https://therecord.media/after-lockbit-takedown-its-purported-leader-vows-to-hack-on?

Eddy, N. (2024, March 25). *GitHub Developers Hit in Complex Supply Chain Cyberattack.* The Darkreading. Retrieved March 25, 2024, from https://www.darkreading.com/application-security/github-developers-hit-in-complex-supply-chain-cyberattack

Greig, J. (2024, March 21). *Two Russians sanctioned by US for alleged disinformation campaign.* The Record. Retrieved March 22, 2024, from https://therecord.media/russians-sanctioned-disinformation-social-design-agency-company-group-structura

Hackernews, T. (2024, March 19). *Suspected Russian Data-Wiping 'AcidPour' Malware Targeting Linux x86 Devices.* The Hackernews.Retrieved March 20, 2024, from https://thehackernews.com/2024/03/suspected-russian-data-wiping-acidpour.html?

Lemos, R. (2024, March 19). *North Korea-Linked Group Levels Multistage Cyberattack on South Korea.* Darkreading. Retrieved March 21, 2024, from https://www.darkreading.com/vulnerabilities-threats/north-korea-linked-group-level-multistage-cyberattack-on-south-korea

Maddie Stone, J. S. (2024, March 27). *A review of zero-day in-the-wild exploits in 2023*. Google Blog. Retrieved March 29, 2024, from https://blog.google/technology/safety-security/a-review-of-zero-day-in-the-wild-exploits-in-2023/

Meta. (2024, March 19). *How Meta Is Preparing For Indian General Elections 2024*. About FB. Retrieved March 21, 2024, from https://about.fb.com/news/2024/03/how-meta-is-preparing-for-indian-general-elections-2024/

Nations, U. (2024, March 21). *General Assembly adopts landmark resolution on artificial intelligence*. UN News. Retrieved March 23, 2024, from https://news.un.org/en/story/2024/03/1147831

Nelson, N. (2024, March 19). *Chinese APT 'Earth Krahang' Compromises 48 Gov't Orgs on 5 Continents*. from Darkreading. Retrieved March 19, 2024, https://www.darkreading.com/threat-intelligence/chinese-apt-earth-krahang-compromised-48-gov-orgs-5-continents

Newsroom. (2024, March 25). *New "GoFetch" Vulnerability in Apple M-Series Chips Leaks Secret Encryption Keys. T*hehackernews. Retrieved March 25, 2024, from https://thehackernews.com/2024/03/new-gofetch-vulnerability-in-apple-m.html

Reuters. (2024, March 15). *G7 industry ministers agree to cooperate on AI, supply chains, presidency says.* Reuters. Retrieved March 16, 2024, from https://www.reuters.com/world/g7-agreed-align-rules-ai-italian-presidency-says-2024-03-14/

Roulette, J. (2024, March 16). *Exclusive: Musk's SpaceX is building spy satellite network for US intelligence agency, sources say.* Reuters. Retrieved March 17, 2024, from https://www.reuters.com/technology/space/musks-spacex-is-building-spy-satellite-network-us-intelligence-agency-sources-2024-03-16/

Scott, M. (2024, March 14). *Europe's content police have a new target: Generative AI.* Politico. Retrieved March 25, 2024, from https://www.politico.eu/article/european-commission-opens-three-dsa-investigations/

Takeuchi, Y. (2024, March 15). *Japan doubles defense tie-ups with private sector in drones, AI.* Asia Nikkei. Retrieved March 16, 2024, from https://asia.nikkei.com/Politics/Defense/Japan-doubles-defense-tie-ups-with-private-sector-in-drones-AI

Wong, H. (2024, March 21). *China warns foreign hackers are infiltrating 'hundreds' of business and government networks.* The South China Morning Post. Retrieved March 21, 2024, from https://www.scmp.com/news/china/politics/article/3256216/china-warns-foreign-hackers-are-infiltrating-hundreds-business-and-government-networks

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.