CLAWS Newsletter

Cyber Index | Volume I | Issue 7

by Govind Nelika

About us

The Centre for Land Warfare Studies (CLAWS) is an independent think tank based in New Delhi, India, dedicated to strategic studies and land warfare in the Indian context. Established in 2004 and registered under the Societies Registration Act, 1860, CLAWS operates as a membership-based organization governed by a Board of Governors and an Executive Council, under the Aegis of the Indian Army.

With a futuristic outlook and a policy-oriented approach, CLAWS focuses on national security issues, conventional military operations, and sub-conventional warfare. The Centre closely monitors regional conflicts and military developments within India's strategic frontiers, particularly in South Asia.

Committed to fostering strategic culture and informed policymaking, CLAWS disseminates its research to armed forces personnel, policymakers, members of the strategic community, and interested civilians. By facilitating in-depth studies and discussions, CLAWS contributes to shaping India's defense policies and military preparedness.

The CLAWS Newsletter is a newly fortnightlyseries under the leadership of Dr. Tara Kartha, Director Research & Academics. The newsletter features insightful content curated by CLAWS researchers, each specializing in their respective verticals. This initiative aims to provide in-depth analysis, strategic insights, and updates on key issues.

Contents

Opening News

Pahalgam attack: Code of war - India and Pakistan take their battle to the (web)front

In the aftermath of the Pahalgam terror attack in April 2025, tensions between India and Pakistan have escalated into the cyber domain, marking a significant shift in their longstanding rivalry. Pakistan-sponsored hacker groups, notably 'Cyber Group HOAX1337' and 'National Cyber Crew,' have intensified cyber offensives against Indian military websites and databases. Targets have included institutions such as Army Public School Nagrota, Sunjuwan, and the Army Institute of Hotel Management, with several sites defaced to mock victims of the Pahalgam incident. These actions are perceived as calculated provocations aimed at testing India's restraint and challenging its cybersecurity infrastructure.

India has responded by bolstering its cyber defences and issuing advisories to critical sectors, including finance and defence, to remain vigilant against potential breaches. The Indian Computer Emergency Response Team (CERT-In) has reported a significant uptick in cyber threats targeting both governmental and private entities. This cyber confrontation underscores the evolving nature of modern warfare, where state and non-state actors leverage digital platforms to conduct espionage, disseminate misinformation, and disrupt critical infrastructure. The international community watches closely, recognizing that such cyber skirmishes between nuclear-armed neighbours have broader implications for regional stability and global cybersecurity norms.

Read more: https://economictimes.indiatimes.com/news/india/code-of-war-india-and-pakistan-take-their-battle-to-the-webfront/articleshow/120842154.cms

US approves HawkEye 360 sale to boost India's surveillance

The U.S. State Department approved a $131 million Foreign Military Sale to India, involving advanced maritime surveillance technology from HawkEye 360, a Virginia-based geospatial analytics firm. This deal includes SeaVision software, technical assistance, training, and logistical support, aiming to enhance India's maritime domain awareness in the Indo-Pacific region. HawkEye 360 operates a constellation of satellites in Low Earth Orbit that detect and geolocate radio frequency (RF) emissions, enabling the tracking of vessels that disable their Automatic Identification System (AIS) to avoid detection. This capability is crucial for monitoring illegal activities such as smuggling and unauthorized fishing within India's Exclusive Economic Zone.

The acquisition aligns with India's strategic objectives to bolster its surveillance capabilities amid regional security challenges. It also reflects the strengthening defense partnership between the U.S. and India, supporting shared goals of maintaining stability and security in the Indo-Pacific. The integration of HawkEye 360's technology is expected to augment India's existing surveillance assets, including P-8I reconnaissance aircraft and Sea Guardian drones, providing a more comprehensive maritime monitoring framework.

Read more: https://timesofindia.indiatimes.com/india/us-approves-hawkeye-360-sale-to-boost-indias-surveillance/articleshow/120859058.cms

The Artemis generation: Space diplomacy's next giant leap

The Lowy Institute's Interpreter published an article by Philip Citowicki discussing the evolving landscape of space diplomacy, particularly in the context of NASA's Artemis program. The Artemis II mission, scheduled for April 2026, aims to carry four astronauts on a lunar flyby, marking a significant step in renewed lunar exploration efforts. This mission is part of a broader initiative to establish a sustainable human presence on the Moon and potentially Mars, fostering international collaboration in space exploration. The article emphasizes the importance of diplomatic engagement and the establishment of norms and agreements to ensure peaceful and cooperative activities in space, amidst increasing interest and competition among nations. It also highlights the role of emerging spacefaring nations and the need for inclusive governance structures to manage the

shared domain of outer space effectively.

Read more: https://www.lowyinstitute.org/the-interpreter/artemis-generation-space-diplomacy-s-next-giant-leap

Amid lawmaker concerns, CYBERCOM head says SOCOM-like model is best way forward

Lieutenant General William Hartman, acting commander of U.S. Cyber Command (CYBERCOM) and interim director of the National Security Agency (NSA), advocated for restructuring CYBERCOM to mirror the U.S. Special Operations Command (SOCOM) model. This proposal emerged during a House Armed Services Subcommittee hearing, where Hartman presented findings from a Department of Defence (DoD) analysis mandated by the 2023 National Defence Authorization Act. The analysis evaluated three organizational models: establishing a separate cyber force, maintaining service-specific cyber units, and adopting a SOCOM-like unified command structure.

Hartman endorsed the SOCOM-like model, emphasizing its potential to enhance operational efficiency and inter-service coordination. However, lawmakers, including Representatives Don Bacon and Richard McCormick, expressed concerns about the implications of such a restructuring, particularly regarding oversight and resource allocation. The debate underscores the complexities of organizing cyber capabilities within the DoD, balancing the need for unified command with the distinct operational cultures of individual services. Internationally, this discussion reflects broader challenges faced by allied nations in structuring their cyber forces to address evolving threats, highlighting the importance of adaptable and cohesive cyber defence strategies.

Read more: https://breakingdefense.com/2025/05/amid-lawmaker-concerns-cybercom-head-says-socom-like-model-is-best-way-forward/?

Trump administration to rescind and replace Biden-era global AI chip export curbs

The Trump administration announced the rescission of a Biden-era regulation that imposed stringent export controls on advanced artificial intelligence (AI) chips. The original rule, set to take effect on May 15, aimed to limit the export of sophisticated AI chips to various countries, including allies, to prevent technological advancements in adversarial nations like China. However, the Trump administration deemed the regulation overly complex and bureaucratic, opting to replace it with a more streamlined global licensing regime.

This policy shift is expected to benefit major U.S. chip manufacturers, such as NVIDIA, AMD, and Intel, by facilitating broader international sales and reducing regulatory burdens. The decision has been welcomed by countries like India, where cloud service providers and data center operators rely heavily on U.S.-made AI hardware for technological development. By easing export restrictions, the U.S. aims to strengthen its economic ties with allied nations while maintaining a strategic stance against China's technological ambitions. This move underscores a balancing act between safeguarding national security interests and promoting global technological collaboration.

Read more: https://www.bis.gov/press-release/department-commerce-rescinds-biden-era-artificial-intelligence-diffusion-rule-strengthens-chip-related

https://economictimes.indiatimes.com/tech/technology/trump-administration-to-rescind-and-replace-biden-era-global-ai-chip-export-curbs/articleshow/120987078.cms?

NCSC CEO, UK urges fresh perspective on cyber security as a contest

At CYBERUK 2025, Dr. Richard Horne, CEO of the UK's National Cyber Security Centre (NCSC), delivered a keynote underscoring the urgent need to reframe cybersecurity as a persistent contest shaped by rapidly evolving threats. Horne emphasized that the UK must adapt to adversaries like China and Russia, whose state-

backed cyber operations pose continuous risks to critical infrastructure and democratic stability. He acknowledged the global nature of these threats, referencing recent warnings from allies such as the United States, Canada, and Australia, which have all reported heightened espionage activities linked to Chinese state-sponsored groups. Canada, for example, raised alarms about Beijing's large-scale data collection efforts, while the U.S. has dismantled Chinese-linked botnets like those operated by Flax Typhoon.

European partners, including France and Denmark, have also seen increased targeting of their telecom and government networks. Horne advocated for a unified international response that includes intelligence sharing, resilient digital infrastructure, and strategic public-private partnerships. His call to action reflects a shared recognition among Western nations that cyber resilience must become a central pillar of national security policy, not only to deter aggression but to safeguard global digital stability in an era of geopolitical competition.

Read more: https://www.ncsc.gov.uk/speech/cyberuk-2025-ncsc-ceo-keynote-speech

Claude AI Exploited to Operate 100+ Fake Political Personas in Global Influence Campaign

In May 2025, Anthropic disclosed that its Claude AI chatbot was exploited by unidentified actors to orchestrate over 100 fake political personas across Facebook and X (formerly Twitter). This "influence-as-a-service" operation engaged tens of thousands of real users, disseminating politically aligned narratives favouring or opposing interests in regions including the U.A.E., Iran, Kenya, and parts of Europe. Claude was utilized not only for content generation but also to determine the timing and nature of interactions, such as comments, likes, and shares based on each persona's political alignment.

The campaign employed a structured JSON-based system to manage these personas, ensuring consistent behaviour and enabling efficient scaling across platforms. Additionally, the bots were programmed to respond with humor and sarcasm when challenged about their authenticity, enhancing their perceived legitimacy. Anthropic's findings underscore the potential for AI tools to be repurposed for sophisticated influence operations, highlighting the need for robust frameworks to detect and mitigate such threats as AI technologies become more accessible.

Read more: https://thehackernews.com/2025/05/claude-ai-exploited-to-operate-100-fake.html?

Malware, Threat Actors & Vulnerabilities

ETH Zurich researchers discover new security vulnerability in Intel processors

The researchers from ETH Zurich's Computer Security Group, led by Professor Kaveh Razavi, disclosed a critical vulnerability in Intel processors termed Branch Privilege Injection (BPI), designated as CVE-2024-45332. This flaw arises from Branch Predictor Race Conditions (BPRC), where asynchronous operations within the CPU's branch predictor can be exploited to bypass hardware-enforced privilege boundaries. By leveraging this vulnerability, attackers can inject malicious branch predictions from user mode, enabling the unauthorized reading of sensitive memory contents across privilege levels. The vulnerability affects all Intel processors released since 2018, encompassing a wide range of devices from personal computers to data centre servers .

The implications of this discovery are profound, particularly for cloud computing environments where multiple users share the same physical hardware. The ability to breach isolation between users undermines the foundational security assumptions of multi-tenant systems. Given Intel's significant market presence, this vulnerability necessitates urgent attention from both hardware manufacturers and software developers to implement effective mitigations. The ETH Zurich team's findings highlight the ongoing challenges in securing speculative execution mechanisms and underscore the need for continued research into hardware-level security vulnerabilities.

Read more: https://ethz.ch/en/news-and-events/eth-news/news/2025/05/eth-zurich-researchers-discov-

er-new-security-vulnerability-in-intel-processors.html

China-Nexus Nation State Actors Exploit SAP NetWeaver (CVE-2025-31324) to Target Critical Infrastructures

The Cybersecurity firm EclecticIQ reported that Chinese state-sponsored advanced persistent threat (APT) groups—specifically UNC5221, UNC5174, and CL-STA-0048—exploited a critical zero-day vulnerability (CVE-2025-31324) in SAP NetWeaver's Visual Composer component to target critical infrastructure globally. This unauthenticated file upload flaw enables remote code execution, allowing attackers to deploy web shells and establish persistent access to compromised systems. Analysis revealed that attackers utilized tools like Nuclei for mass scanning and documented 581 compromised SAP instances, with an additional 1,800 domains identified as potential future targets. The presence of Chinese-language file names and specific tradecraft patterns reinforced attribution to Chinese-speaking operators. These operations are assessed to be linked to China's Ministry of State Security (MSS) or affiliated entities, aiming to exfiltrate sensitive data and maintain long-term access to high-value networks. The exploitation of such widely used enterprise platforms underscores the strategic focus of these APT groups on critical infrastructure sectors. This campaign highlights the pressing need for organizations to implement robust cybersecurity measures, promptly apply security patches, and enhance monitoring to detect and mitigate such sophisticated threats.

Read more: https://blog.eclecticiq.com/china-nexus-nation-state-actors-exploit-sap-netweaver-cve-2025-31324-to-target-critical-infrastructures

New Noodlophile Stealer Distributes Via Fake AI Video Generation Platforms

Morphisec Threat Labs uncovered a novel cyber threat involving the Noodlophile Stealer, a previously undocumented infostealer malware disseminated through counterfeit AI video generation platforms. Cybercriminals, exploiting the burgeoning interest in AI tools, created deceptive websites and social media campaigns—particularly on Facebook—offering free AI-powered video editing services. Unsuspecting users, enticed by these offers, were prompted to upload personal media files and subsequently download what they believed were AI-processed videos. Instead, they received a ZIP archive containing a malicious executable disguised with misleading file extensions.

Upon execution, the malware deployed the Noodlophile Stealer, which harvested browser credentials, cryptocurrency wallet information, and other sensitive data. In some instances, it also installed XWorm, a remote access trojan, granting attackers deeper control over the compromised systems. The malware communicated with its operators via Telegram bots, facilitating covert data exfiltration. Further investigation revealed that Noodlophile is part of a malware-as-a-service (MaaS) scheme, with its developer, likely of Vietnamese origin, actively promoting it on cybercrime forums.

This campaign underscores a significant shift in cyberattack strategies, leveraging the public's enthusiasm for AI technologies as a vector for malware distribution. It highlights the need for heightened vigilance among users and the importance of robust cybersecurity measures to counteract increasingly sophisticated social engineering tactics.

Read more: https://www.morphisec.com/blog/new-noodlophile-stealer-fake-ai-video-generation-platforms/

Threat Actor SocGholish deploys Mintsloader malware

The Recorded Future's Insikt Group uncovered MintsLoader, a sophisticated multi-stage malware loader employed by threat actors TAG-124 and SocGholish. MintsLoader is engineered to deliver secondary payloads, notably GhostWeaver, while evading detection through advanced obfuscation, sandbox evasion, and domain generation algorithms (DGAs). Its second-stage PowerShell scripts are designed to detect and avoid virtualized environments, complicating analysis and hindering automated detection systems. The malware's use of

DGAs to generate daily command-and-control (C2) domains based on system dates further challenges traditional monitoring and blocking strategies.

GhostWeaver, the primary payload delivered by MintsLoader, utilizes self-signed X.509 certificates resembling those used by AsyncRAT variants, leading to potential misclassification and complicating threat attribution. The persistent use of such sophisticated techniques by MintsLoader indicates a trend towards increased professionalization within the cybercriminal ecosystem. This evolution enhances the resilience and efficiency of malicious operations, posing significant challenges to national security and critical infrastructure. However, it also presents opportunities for defenders to develop more effective detection and disruption strategies. Recorded Future's Malware Intelligence Hunting has been instrumental in identifying new MintsLoader samples and associated C2 domains, providing actionable intelligence to bolster defences against such advanced threats.

Read more: https://www.recordedfuture.com/research/uncovering-mintsloader-with-recorded-future-malware-intelligence-hunting

Horabot Unleashed: A Stealthy Phishing Threat

FortiGuard Labs identified a resurgence of the Horabot malware campaign, a sophisticated phishing operation targeting Spanish-speaking users, particularly in Latin America. The campaign employs deceptive emails masquerading as invoices, containing malicious HTML attachments that initiate a multi-stage infection process. Upon opening, these attachments download additional payloads, including VBScript, AutoIt, and PowerShell scripts, which perform system reconnaissance, credential theft, and the installation of banking trojans. Horabot leverages Outlook COM automation to propagate by sending phishing emails from compromised accounts, facilitating lateral movement within networks. The malware exhibits advanced evasion techniques, such as detecting virtual environments and specific antivirus software, to avoid analysis and detection. Its operations have been observed in countries including Mexico, Guatemala, Colombia, Peru, Chile, and Argentina. The campaign underscores the evolving tactics of cyber threat actors in exploiting trusted communication channels and highlights the necessity for organizations to implement robust email security measures, user education, and advanced threat detection capabilities to mitigate such threats.

Read more: https://www.fortinet.com/blog/threat-research/horabot-unleashed-a-stealthy-phishing-threat

Middle East

Iranian Threat Actor Maintain Two – Year Intrusion for two years

The Fortinet's FortiGuard Incident Response (FGIR) team disclosed a prolonged cyber intrusion targeting critical national infrastructure (CNI) in the Middle East. The intrusion persisted from at least May 2023 to February 2025, with signs of compromise dating back as far as May 202,1 attributed to an Iranian state-sponsored threat group. The operation, characterized by extensive espionage and network prepositioning tactics, aimed to establish persistent access for potential future strategic advantages. The attackers exploited vulnerabilities in Microsoft Exchange servers to infiltrate networks, employing advanced techniques to maintain a low profile and evade detection. This incident underscores the escalating sophistication of state-sponsored cyber operations and their focus on vital sectors such as energy, transportation, and telecommunications. The breach not only threatens the operational integrity of essential services but also poses significant risks to regional stability and international relations. It highlights the imperative for robust cybersecurity measures, continuous monitoring, and international collaboration to safeguard critical infrastructure against evolving cyber threats.

Read more: https://www.fortinet.com/blog/threat-research/fortiguard-incident-response-team-detects-intrusion-into-middle-east-critical-national-infrastructure

Saudi Arabia launches Humain to develop AI, may seek US partnership and favour from Donald Trump

Saudi Arabia launched "Humain" a state-backed artificial intelligence (AI) initiative spearheaded by Crown Prince Mohammed bin Salman and funded by the nation's $940 billion Public Investment Fund. This move aligns with Saudi Arabia's Vision 2030, aiming to diversify its economy beyond oil by establishing the kingdom as a global AI leader. Humain's objectives include developing advanced AI infrastructure, such as next-generation data centers, cloud platforms, and high-performance computing systems, with a focus on creating Arabic-language large language models tailored for the Middle East.

The initiative coincided with former U.S. President Donald Trump's visit to Riyadh, during which significant U.S.-Saudi tech collaborations were announced. Notably, Nvidia agreed to supply over 18,000 of its latest AI chips to Humain, while AMD and Amazon Web Services committed to multi-billion-dollar investments to bolster Saudi Arabia's AI capabilities. These partnerships reflect a strategic shift in U.S. policy, moving from stringent export controls to fostering AI collaborations with Gulf nations. While these developments enhance U.S.-Saudi technological ties and position Saudi Arabia as a burgeoning AI hub, they also raise questions about the geopolitical implications of advanced technology proliferation in the Middle East and the potential challenges in balancing international partnerships with national security concerns.

Read more: https://www.indiatoday.in/technology/news/story/saudi-arabia-launches-humain-to-develop-ai-may-seek-us-partnership-and-favour-from-donald-trump-2724119-2025-05-13

Marbled Dust leverages zero-day in Output Messenger for regional espionage

Microsoft Threat Intelligence reported that the Türkiye-affiliated threat actor Marbled Dust exploited a zero-day vulnerability (CVE-2025-27920) in Output Messenger, a widely used enterprise messaging platform, to conduct espionage operations targeting Kurdish military entities in Iraq. The vulnerability, a directory traversal flaw in the Output Messenger Server Manager, allowed authenticated users to upload malicious files into the server's startup directory, facilitating the deployment of custom malware. Marbled Dust leveraged this flaw to install Go-based backdoors, such as OMServerService.exe and OMClientService.exe, enabling persistent access, data exfiltration, and user impersonation. The attackers likely obtained initial access through credential harvesting techniques, including DNS hijacking and the use of typosquatted domains, consistent with their previous tactics.

This campaign signifies a notable escalation in Marbled Dust's capabilities, transitioning from exploiting known vulnerabilities to deploying zero-day exploits, thereby enhancing their operational effectiveness. The incident underscores the critical need for organizations, especially those in geopolitically sensitive regions, to promptly apply security patches and implement robust cybersecurity measures to defend against sophisticated state-sponsored threats. The collaboration between Microsoft and Srimax, the developer of Output Messenger, led to the release of patches addressing both CVE-2025-27920 and an additional vulnerability, CVE-2025-27921, highlighting the importance of coordinated responses in mitigating such threats.

Read more: https://www.microsoft.com/en-us/security/blog/2025/05/12/marbled-dust-leverages-zero-day-in-output-messenger-for-regional-espionage/

Russia – Ukraine

North Korean APT Targets Russia & Ukraine

Proofpoint identified a strategic shift in the operations of TA406, a North Korean state-sponsored threat actor also known as Opal Sleet and Konni. Historically focused on Russian targets, TA406 redirected its cyber-espionage efforts toward Ukrainian government entities, likely aiming to gather intelligence on Ukraine's political climate and military posture amid the ongoing Russian invasion. This pivot aligns with North Korea's deploy-

ment of troops to support Russia in late 2024, suggesting an interest in assessing the conflict's trajectory and potential implications for its forces.

TA406's campaign utilized spear-phishing emails impersonating fictitious think tank personnel, embedding malicious HTML and CHM files that executed PowerShell scripts upon user interaction. These scripts conducted extensive reconnaissance, collecting system information and establishing persistence through scheduled tasks and autorun scripts. Additionally, TA406 employed credential harvesting tactics, sending fake Microsoft security alerts from ProtonMail accounts to lure targets into divulging login credentials via compromised domains.

The group's focus on strategic intelligence gathering, rather than direct military targeting, underscores the multifaceted nature of cyber threats in modern conflicts. TA406's activities highlight the importance of robust cybersecurity measures, particularly for government entities, to safeguard against sophisticated state-sponsored espionage operations.

Read more: https://www.proofpoint.com/us/blog/threat-insight/ta406-pivots-front

United Kingdom of Great Britain and Northern Ireland

Britain warns that China is becoming a 'cyber superpower'

In May 2025, senior UK officials, including Cabinet Office Minister Pat McFadden and National Cyber Security Centre (NCSC) head Richard Horne, warned that China is rapidly emerging as a "cyber superpower," posing a significant national security threat. Speaking at the CYBERUK conference, McFadden emphasized China's advanced cyber capabilities and its deep integration into global supply chains, making economic decoupling impractical. Horne highlighted ongoing concerns about persistent cyber activities originating from China, including espionage campaigns like Salt Typhoon targeting the telecommunications sector.

These operations are part of a broader strategy by the Chinese Communist Party, leveraging a comprehensive ecosystem of state and commercial actors to conduct cyber intrusions and data exfiltration. International partners, such as Denmark, France, and Canada, have reported similar espionage activities, with Canada noting China's acquisition of vast amounts of data on global political figures and citizens. The UK's stance reflects a dual approach: engaging with China economically while bolstering cyber defences through alliances like the Five Eyes. This situation underscores the need for enhanced cybersecurity measures and international collaboration to address the evolving cyber threat landscape.

Read more: https://therecord.media/britain-warns-china-is-becomming-a-cyber-superpower

United States of America (USA)

DISA turns to AI, automation to bridge workforce gaps, attempts to stay on track with JWCC Next

The U.S. defence Information Systems Agency (DISA) announced a strategic shift towards leveraging artificial intelligence (AI), machine learning (ML), and automation to address workforce shortages impacting critical initiatives, notably the Joint Warfighting Cloud Capability (JWCC) Next program. Jeff Marshall, Director of DISA's J9 Hosting and Compute Center, highlighted that recent federal workforce reduction programs, including the Deferred Resignation Program and Voluntary Early Retirement Authority (VERA), have led to significant personnel gaps. To mitigate these challenges, DISA plans to implement generative AI tools to identify operational deficiencies and prioritize areas where automation can enhance efficiency. This approach aims to realign the JWCC Next project, a successor to the $9 billion JWCC contract facilitating the Department of Defence's acquisition of commercial cloud services, which has experienced delays due to staffing constraints. The integration of AI and automation not only seeks to streamline DISA's operations but also reflects a broader trend within defence agencies to adopt advanced technologies for maintaining mission read-

iness amid evolving workforce dynamics. This development underscores the increasing reliance on AI-driven solutions to sustain critical defence infrastructure and operations in the face of human resource limitations.

Read more: https://breakingdefense.com/2025/05/disa-turns-to-ai-automation-to-bridge-workforce-gaps-attempts-to-stay-on-track-with-jwcc-2-0/?

Pentagon's AI metals program goes private to boost Western supply

The U.S. Department of Defense transitioned its AI-driven critical minerals forecasting initiative to the Critical Minerals Forum (CMF), a nonprofit consortium comprising over 30 entities, including mining firms and manufacturers like Volkswagen, MP Materials, and South32. Developed with support from DARPA, the AI model analyzes more than 70 datasets to predict supply and pricing trends for essential minerals such as rare earth elements, nickel, and cobalt. This move aims to enhance market transparency and reduce Western dependence on dominant suppliers, notably China.

The CMF plans to utilize this model to guide long-term investment decisions, considering potential market shocks like export restrictions. Data contributions come from entities like FactSet, Benchmark Mineral Intelligence, and the U.S. Commerce Department. While some experts question the model's predictive capabilities, proponents argue it offers valuable insights for supply chain resilience. The initiative also seeks international collaboration, with countries rich in critical minerals, such as Zambia and the Democratic Republic of Congo, exploring participation. By fostering a more transparent and diversified global supply chain, the program holds significant implications for national security, industrial strategy, and international relations.

Read more: https://www.reuters.com/business/autos-transportation/pentagons-ai-metals-program-goes-private-bid-boost-western-supply-deals-2025-05-01/

Unsophisticated Cyber Actor(s) Targeting Operational Technology

On May 6, 2025, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the Federal Bureau of Investigation (FBI), issued an alert highlighting a surge in cyberattacks targeting Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems within the U.S. energy and transportation sectors. These attacks, often executed by unsophisticated actors employing basic intrusion techniques, exploit vulnerabilities stemming from poor cyber hygiene and exposed assets. Consequences of such breaches include system defacement, unauthorized configuration changes, operational disruptions, and potential physical damage. CISA emphasized the urgency for critical infrastructure operators to implement mitigations, such as disconnecting Operational Technology (OT) systems from public internet access, changing default passwords, and securing remote access with robust authentication measures.

Internationally, similar threats have been observed. In Europe, pro-Russian hacktivist groups have targeted critical infrastructure sectors, including water and wastewater systems, dams, energy, and food and agriculture, employing unsophisticated techniques to manipulate ICS equipment and create nuisance effects. While these attacks are often limited in sophistication, they pose physical threats against insecure and misconfigured OT environments.

These developments underscore the global nature of cyber threats to critical infrastructure and the necessity for international collaboration in enhancing cybersecurity measures. Implementing best practices and sharing threat intelligence across borders are essential steps in mitigating the risks posed by both sophisticated and unsophisticated cyber actors.

Read more: https://www.cisa.gov/news-events/alerts/2025/05/06/unsophisticated-cyber-actors-targeting-operational-technology

US arrests two alleged leaders of the 764 group

The U.S. Department of Justice announced the arrests of Leonidas Varagiannis (aka "War") and Prasan Nepal (aka "Trippy"), alleged leaders of the transnational child exploitation network known as "764." Varagiannis, a U.S. citizen residing in Thessaloniki, Greece, and Nepal, from High Point, North Carolina, are accused of orchestrating a global enterprise that targeted minors through coercion, manipulation, and psychological abuse. The network, characterized by its nihilistic and violent extremist ideology, aimed to destabilize societal structures by exploiting vulnerable populations, particularly children. Members of 764 allegedly produced and distributed child sexual abuse material (CSAM), encouraged self-harm among victims, and utilized digital platforms to recruit and indoctrinate individuals into their extremist beliefs.

The group's operations extended across multiple countries, leveraging encrypted communication channels to evade detection. The arrests of Varagiannis and Nepal mark a significant step in dismantling one of the most disturbing online child exploitation enterprises encountered by federal authorities. This case underscores the critical need for international collaboration in combating cyber-enabled child exploitation and highlights the evolving nature of threats posed by ideologically driven online networks. The Department of Justice emphasized its commitment to prosecuting individuals involved in such heinous activities and safeguarding children from exploitation.

Read more: https://www.justice.gov/opa/pr/leaders-764-arrested-and-charged-operating-global-child-exploitation-enterprise

The FBI's Brett Leatherman gives the latest 'Typhoon' forecast

The FBI disclosed ongoing efforts to counter Chinese state-sponsored cyber threats, notably the Flax Typhoon group. Flax Typhoon, linked to China's Ministry of State Security, orchestrated a vast botnet operation compromising over 260,000 devices globally, including routers, cameras, and other Internet of Things (IoT) devices. These compromised devices were leveraged to infiltrate critical infrastructure sectors, exfiltrate sensitive data, and facilitate further cyber-espionage activities. The FBI, in collaboration with international partners, executed a court-authorized operation to dismantle this botnet, effectively severing the threat actors' control over the infected devices. This action followed similar operations against other Chinese-linked groups, such as Volt Typhoon and Salt Typhoon, which have targeted U.S. telecommunications and government networks.

The persistent activities of these groups underscore the strategic emphasis placed by Chinese state-sponsored actors on cyber capabilities to advance national interests. The implications for national security are profound, highlighting the necessity for robust cybersecurity measures, international cooperation, and continuous monitoring to safeguard critical infrastructure and sensitive information from sophisticated cyber threats.

Read more: https://therecord.media/fbi-interview-china-hacking-volt-salt-flax-typhoon?

Yemeni National Charged in Federal Indictment Alleging He Sent 'Black Kingdom' Malware

The U.S. Department of Justice indicted Rami Khaled Ahmed, a 36-year-old Yemeni national also known as "Black Kingdom," for orchestrating a global ransomware campaign targeting U.S. entities. Between March 2021 and June 2023, Ahmed and his co-conspirators deployed the "Black Kingdom" ransomware to exploit vulnerabilities in Microsoft Exchange servers, compromising approximately 1,500 computer systems. Victims included a medical billing company in California, a ski resort in Oregon, a Pennsylvania school district, and a Wisconsin health clinic. The malware either encrypted or claimed to exfiltrate data, demanding $10,000 in Bitcoin for restoration, with payments directed to cryptocurrency wallets controlled by the attackers. The FBI, with assistance from New Zealand Police, is investigating the case. If convicted, Ahmed faces up to five years in federal prison for each of the three charges: conspiracy, intentional damage to a protected computer, and threatening damage to a protected computer. This case underscores the persistent threat of ransomware to critical infrastructure and highlights the challenges of international cybercrime enforcement, particularly

when perpetrators operate from jurisdictions with limited extradition agreements.

Read more: https://www.justice.gov/usao-cdca/pr/yemeni-man-charged-federal-indictment-alleging-he-sent-black-kingdom-malware-extort

Botnet Dismantled in International Operation, Russian and Kazakhstani Administrators Indicted

The U.S. Department of Justice announced the dismantling of a sophisticated botnet operated by Russian and Kazakhstani nationals, which had compromised thousands of computers worldwide. The botnet, designed to harvest personal and financial data, was utilized for various cybercrimes, including identity theft and financial fraud. The operation involved deploying malware that infiltrated victims' systems, allowing the perpetrators to exfiltrate sensitive information and conduct unauthorized transactions. This international cybercriminal enterprise posed significant threats to global cybersecurity, affecting individuals, businesses, and government entities. The collaborative effort between U.S. law enforcement and international partners underscores the importance of cross-border cooperation in combating cyber threats. The successful takedown of the botnet not only disrupts the malicious activities of the involved threat actors but also serves as a deterrent to similar cybercriminal operations. This case highlights the evolving nature of cyber threats and the necessity for continuous advancements in cybersecurity measures to protect national security and maintain the integrity of international digital infrastructure.

Read more: https://www.justice.gov/usao-ndok/pr/botnet-dismantled-international-operation-russian-and-kazakhstani-administrators

About the Author

Govind Nelika is the Researcher / Web Manager / Outreach Coordinator 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. In recognition of his contributions, he was awarded the Chief of Army Staff (COAS) Commendation Card on Army Day 2025 for his work with CLAWS.