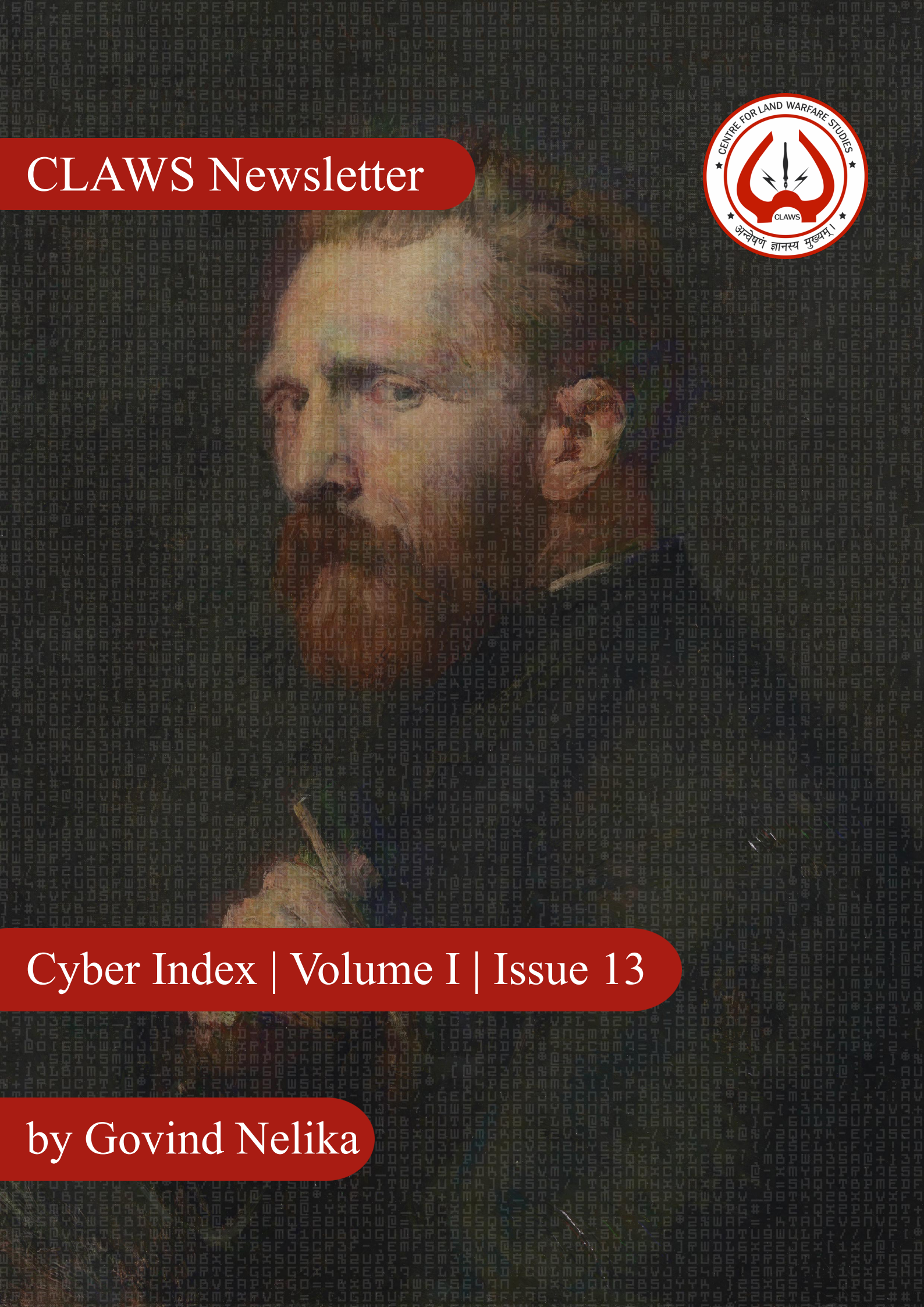
CLAWS Newsletter



Cyber Index | Volume I | Issue 13

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 fortnightly series 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

Global Brief

China state media says Nvidia must provide 'security proofs' to regain trust

China's state media has demanded that U.S. chipmaker Nvidia provide clear security assurances for its H20 artificial intelligence chips after regulators raised concerns that the products could contain hidden backdoors or vulnerabilities. The Cyberspace Administration of China recently summoned the company to explain these risks, reflecting growing suspicion of foreign technology amid intensifying U.S.-China competition over advanced semiconductors. Nvidia has denied the existence of backdoors and emphasized its commitment to cybersecurity, but the calls from outlets like People's Daily underscore Beijing's insistence on tighter oversight of imported technology. The dispute highlights China's push for greater technological self-reliance, while for Nvidia it poses potential challenges in maintaining access to a key market that accounts for significant global chip demand. More broadly, the episode illustrates how national security concerns are increasingly shaping global technology supply chains and raising barriers for international companies operating across geopolitical fault lines.

Read more: https://www.reuters.com/world/china/china-state-media-says-nvidia-must-provide-security-proofs-regain-trust-2025-08-01/?

Chinese biz using AI to hit US politicians, influencers with propaganda

The primary subject of this briefing is GoLaxy, a Beijing-based tech company whose advanced AI tools are being used in influence operations targeting U.S. politicians and social media figures. Key actors include GoLaxy allegedly founded by a state-affiliated scientific institute and backed by Sugon, a Chinese supercomputing company and U.S. national security officials, as well as researchers at Vanderbilt University, who uncovered internal documents detailing the firm's covert capabilities.

This activity unfolds against a backdrop of intensifying geopolitical information warfare, where AI-enhanced propaganda operations are increasingly replacing manual troll farms. The evolution reflects broader tensions between democratic societies and authoritarian states seeking narrative control.

According to the leaked documents, GoLaxy employs systems such as DeepSeek and a so-called "Smart Propaganda System" (GoPro) to assemble detailed profiles of at least 117 U.S. lawmakers and over 2,000 American influencers and thinkers. It monitors millions of posts daily across platforms like Weibo, Facebook, and X, constructing nuanced personal profiles and tailoring persuasive content in real time. This allows rapid deployment and morphing of messaging aligned with Beijing's policy objectives.

The documents also reveal active operations in Hong Kong, Taiwan, and now targeting U.S. discourse. The AI system is designed to detect political developments, automatically generate compelling counter-messaging, and adapt instantaneously, even during fast-moving events. GoLaxy meanwhile publicly claims it only uses open-source data and denies government linkage exposing a layer of plausible deniability even as the internal evidence indicates otherwise.

Strategically, the rise of GoLaxy signals a shift in influence operations: from labor-intensive tactics to scalable, AI-driven systems capable of sophisticated messaging and real-time adaptation. This poses a formidable challenge to defenders of democratic information ecosystems. U.S. officials citing testimony from former NSA director Gen. Paul Nakasone warn this marks a new frontier in gray-zone conflict, requiring urgent investment in AI-powered detection and cooperation across private and academic sectors to keep pace with evolving synthetic threats.

Read more: https://www.theregister.com/2025/08/08/golaxy_ai_influence/

At missile defence conference, the first rule of Golden Dome is don't talk about Golden Dome

The primary subject is the Pentagon's ambitious Golden Dome missile defence initiative, spearheaded b Space Force General Michael Guetlein under the direction of the Trump administration, aiming to deliver comprehensive, multi-layered shield protecting the continental U.S., Hawaii, and Alaska. Key actors includ the Missile Defence Agency (MDA), senior Defence Department leadership, and major industry players suc as Lockheed Martin, Northrop Grumman, RTX, and emerging tech firms.

This initiative emerges amid heightened geopolitical concerns over missile threats from near-peer rivals lik China and Russia and is framed as a decisive shift toward homeland defence paralleling historical precedent like Reagan's Strategic Defence Initiative. It reflects technological challenges and complexity: Golden Dom envisions a four-tiered architecture combining space-based sensors and interceptors, radars, ground-base interceptors (e.g., Next Generation Interceptors, THAAD, Patriot), and potentially directed-energy weapon such as lasers, all networked and orchestrated via advanced AI-enhanced fire control systems.

However, public discussion of Golden Dome remains tightly controlled: at the recent Space and Missil Defense Symposium in Huntsville, officials were instructed to avoid mentioning the program, with session scrapped and replaced by an industry-only event closed to media access. Nonetheless, defence contractor publicly promoted their relevance Lockheed Martin emphasizing integration of combat-proven systems, an Northrop Grumman underscoring industry readiness even as the Pentagon side-stepped questions on detail and feasibility.

Strategically, Golden Dome signals a novel escalation in U.S. missile defence posture, integrating space based capabilities with terrestrial systems under AI control. Its secrecy indicates both operational security an the high-stakes optics of defence programming. For defence contractors, it represents a potentially histori procurement opportunity. Internationally, the initiative may spark renewed arms-race dynamics in space an reshape how nations perceive deterrence and defence in the emerging era of multi-domain threats.

Read more: https://breakingdefence.com/2025/08/at-missile-defence-conference-the-first-rule-of-golden-dome-is-dont-talk-about-golden-dome/?

Dutch National Cyber Security Centre (NCSC-NL) Citrix NetScaler ADC Vulnerability

The primary subject is a critical Citrix NetScaler ADC and Gateway vulnerability, tracked as CVE-2025 6543, which has been actively exploited to breach multiple critical Dutch organizations. Key actors includ the Dutch National Cyber Security Centre (NCSC-NL), Citrix (as vendor issuing patches), and sophisticate threat actors behind the exploitation. This unfolds in a broader context of persistent security threats to gatewa appliances that handle high-value access such as VPN, ICA proxy, and AAA services.

Investigations revealed that from early May 2025 nearly two months before the vulnerability was publicl disclosed the flaw was being exploited as a zero-day, enabling unauthenticated remote code execution, deploy ment of web shells, and deliberate deletion of logs to obscure the intrusions. Affected versions include Citri NetScaler ADC and Gateway builds prior to 14.1-47.46, 13.1-59.19, and specified 13.1-FIPS/NDcPP releases while older End-of-Life versions remain especially at risk.

By July 16, NCSC-NL detected signs of abuse and began notifying affected organizations. These organiza tions, including the Public Prosecution Service, suffered operational disruption and needed forensic respons to uncover malicious web shells and hidden administration accounts. In its follow-up update on August 13 NCSC-NL introduced two new detection scripts via GitHub, along with revised Indicators of Compromis (IOCs), urging organizations to adopt a defense-in-depth strategy, including patching, session termination network segmentation, logging, and forensic readiness (ncsc.nl).

This incident underscores the strategic threat posed by sophisticated zero-day exploitation of widely deploye network appliances. It highlights the importance of timely patching, coordinated incident response, and lay

ered defences. More broadly, it reveals how adversaries can penetrate critical infrastructure through trusted gateway systems, necessitating urgent attention to foundational resilience and proactive monitoring across enterprise networks.

Read more: https://www.ncsc.nl/actueel/nieuws/2025/07/22/casus-citrix-kwetsbaarheid

United States of America (USA)

Commission to study how the US could go about making a Cyber Force

The primary focus centres on the newly established Commission on Cyber Force Generation, formed through a collaboration between the Center for Strategic and International Studies (CSIS) and the Cyberspace Solarium Commission 2.0 (affiliated with the Foundation for Defence of Democracies). This commission brings together seasoned leaders including Lt. Gen. Ed Cardon (former commander of Army Cyber Command), Michael Sulmeyer (the Pentagon's first Senate-confirmed cyber policy lead), and representatives from both military and civilian cyber sectors to plan how an independent U.S. Cyber Force could be implemented, should the political decision to create one arise.

Amid growing concern over operational readiness and structural inefficiencies in the military's approach to cyberspace, the commission does not debate whether a Cyber Force is needed, but focuses on the practical aspects of making it a reality such as defining its organizational structure, core responsibilities, and legal authorities, while drawing on inputs from government, industry, and civil society. The commission builds on momentum stirred by language in the 2025 National Defence Authorization Act, which calls for an evaluation of alternative organizational models for cyber elements within the Armed Forces, including a new Cyber Force but notably omits an outright directive to establish one.

Traditional service branches (Army, Navy, Air Force, Marine Corps, Space Force) currently supply cyber mission teams to U.S. Cyber Command, but disparate training, retention, and career structures have led to persistent readiness shortfalls. The commission's preparatory work is intended to reduce "downstream risk," avoid institutional friction, and accelerate implementation should political backing materialize.

Strategically, this initiative reflects recognition that the cyber domain has matured into a distinct warfighting environment, demanding specialized, agile organizational structures analogous to other military domains. For U.S. national security, the commission's work signals shifting consensus toward investing in frameworks capable of delivering cyber superiority or at least parity amid intensifying global cyber competition.

Read more: https://breakingdefence.com/2025/08/commission-to-study-how-the-us-could-go-about-making-a-cyber-force/?

U.S Army seeks AI/ML tools to tame crowded airspace under NGC2 push

The United States Army, in coordination with the Program Executive Office Intelligence Electronic Warfare & Sensors (PEO IEW&S) and Program Manager Next Generation Command and Control (NGC2), has issued a Request for Information (RFI) seeking industry input on artificial intelligence and machine learning solutions to transform airspace management. The initiative responds to the growing cognitive burden on commanders as they navigate increasingly complex, multi-domain battlefields. Against the backdrop of rapid unmanned aerial system (UAS) proliferation, contested and congested airspace, and dynamic mission requirements, the Army is exploring AI-driven technologies that enhance situational awareness, streamline deconfliction, and enable faster, data-driven decision-making.

The RFI outlines two primary objectives: near-term "fight tonight" capability demonstrations of solutions that are operationally ready today, and a long-term vision to integrate scalable AI/ML tools into NGC2 systems for adaptive airspace management. Specific challenges identified include integrating manned and unmanned aircraft, coordinating fires and air defence effects, sustaining operations in environments affected by jamming

or electronic warfare, and processing large volumes of operational data in real time. The Army is particularly interested in solutions that support dynamic allocation of airspace, real-time conflict detection and resolution, predictive mission planning, resilience against adversary countermeasures, and sustainable management approaches.

Vendors are asked to describe core AI/ML techniques, such as supervised learning, reinforcement learning, or predictive analytics, and address deployment scalability, technology readiness, cybersecurity compliance, and integration risks. Responses should also provide cost estimates, licensing models, and proposed contracting incentives. A notable opportunity includes delivering a minimum viable product (MVP) for demonstration at the Joint Pacific Multinational Readiness Center (JPMRC) Exercise 26-01 by November 2025, aimed at supporting the 25th Infantry Division's UAS operations in contested environments.

Strategically, this effort underscores the Army's recognition that effective airspace control is central to multi-domain dominance. By leveraging AI/ML, the Army seeks not only to reduce commander workload but also to establish resilient, adaptive systems that can outpace adversaries in the increasingly data-intensive battlespace.

Read more: https://sam.gov/workspace/contract/opp/90e7ea130d474afa8adaaa5ccc8ff768/view

Two Chinese Nationals Arrested on Federal Complaint Alleging They Illegally Shipped to China Sensitive Microchips Used in AI Applications

The central focus of this briefing is a federal criminal complaint brought by the U.S. Department of Justice against two Chinese nationals Chuan Geng, a lawful permanent resident of Pasadena, and Shiwei Yang, an undocumented individual from El Monte who are accused of exporting tens of millions of dollars' worth of sensitive AI-capable microchips to China without authorization. The U.S. Attorney's Office for the Central District of California is leading the case under the Export Control Reform Act, a statute designed to curb exports of strategic technologies and carries penalties of up to 20 years in prison.

From October 2022 to July 2025, through their small El Monte–based company ALX Solutions Inc., established shortly after tightened export licensing requirements came into effect, the defendants allegedly exported advanced graphical processing units including high-end Nvidia chips without securing necessary licenses from the U.S. Department of Commerce. At least 20 shipments, including one in December 2024 falsely labeled to avoid scrutiny, were routed through transshipment points in Singapore and Malaysia, common intermediaries used to conceal shipments destined for China. Financial records indicate that while ALX Solutions did not receive payments from declared intermediaries, it was paid directly by companies based in China and Hong Kong among them a $1 million transfer in January 2024.

At initial court proceedings in Los Angeles, Geng surrendered and was released on a $250,000 bond; Yang remains in custody pending a detention hearing. Arraignment for both is set for September 11.

Strategically, this case underscores the U.S. government's intensified enforcement of export controls amid escalating technological and geopolitical competition with China. It highlights vulnerabilities in private-sector compliance pathways and the urgency of safeguarding dual-use technologies vital to AI advancement. More broadly, the proceedings signal a robust commitment to enforcing national security mandates governing advanced semiconductor exports reinforcing deterrence and providing a legal precedent in the fight against illicit technology transfers.

Read more: https://www.justice.gov/usao-cdca/pr/two-chinese-nationals-arrested-federal-complaint-alleging-they-illegally-shipped-china

Citizen Lab director warns cyber industry about US authoritarian descent

Ronald Deibert, founder and director of the University of Toronto's Citizen Lab, delivered a pointed message at Black Hat USA 2025, urging the cybersecurity community to recognize and resist what he terms a "dramatic descent into authoritarianism" within the United States, where technology and governance are increasingly merging into what he describes as a "fusion of tech and fascism". Traditionally, cybersecurity professionals have sidestepped political entanglements, but Deibert warns that this stance is no longer viable as democratic norms erode and tech platforms from Meta to Google and Apple risk enabling authoritarian trends by downsizing their vital threat intelligence teams that have historically detected spyware abuses like Pegasus.

Deibert highlighted a growing "market failure" in protecting civil society, which cannot afford high-end cybersecurity defences, making it especially vulnerable as institutional safeguards vanish and attacks intensify. Indicator actions such as the marginalization of figures like former CISA director Chris Krebs following his defence of election integrity, and public appeals from his successor Jen Easterly illustrate an alarming politicization of cybersecurity leadership. Deibert argues that preserving democratic integrity will depend on solidarity across the cybersecurity community, continued pro bono support for independent watchdogs, and defence of public-interest research entities like Citizen Lab, which he notes might not survive in current conditions if these trends persist.

Strategically, Deibert reframes cybersecurity as a frontline defence of democracy, not merely an exercise in technical protection. As surveillance technologies and state-aligned tech platforms proliferate, the call-to-action challenges industry professionals to safeguard digital rights and civic freedoms emphasizing that the future resilience of democratic societies depends on their choices and willingness to act.

Read more: https://techcrunch.com/2025/08/06/citizen-lab-director-warns-cyber-industry-about-us-authoritarian-descent/

People's Republic of China (PRC) | China

Chinese researchers suggest lasers, sabotage to counter Musk's Starlink

The main subject centers on the advanced countermeasures being researched by Chinese government and military scientists, aimed at neutralizing or mitigating the perceived threat posed by SpaceX's Starlink satellite constellation. Key actors include the People's Liberation Army, state-linked universities such as the National University of Defense Technology, and various state-backed scientific bodies publishing in peer-reviewed journals. The backdrop for these initiatives is the growing integration of Starlink operated by a private U.S. company closely tied to American defence institutions into national security infrastructures. This integration intensified following Starlink's pivotal role in supporting battlefield communications in Ukraine, raising alarm over reliance on a privately controlled, geopolitically sensitive network. In response, Chinese researchers have proposed a range of sophisticated technical methods: deploying stealth submarines equipped with space-targeting lasers, developing custom attack satellites using ion-thruster propulsion systems, orchestrating supply-chain sabotage to disrupt Starlink's manufacturing or deployment, and launching small corrosive-satellite "tailers" designed to damage Starlink units in orbit through chemical or physical means.

Additional strategies include the use of ground-based optical telescopes for continuous tracking, deep-fake generation to mislead or create false targets, and electromagnetic or laser dazzling operations to blind and disable satellite sensors. Concurrently, China is accelerating its own mega-constellation efforts such as Guowang and Qianfan aimed at establishing competing low-earth-orbit networks of comparable scale and functionality. These developments underscore a broader geopolitical and technological shift: the weaponization of space assets, growing emphasis on directed-energy and non-kinetic counterspace technologies, and a race for technological sovereignty. Strategically, this marks a tangible escalation in space-domain competition, highlighting the need for resilient satellite architectures and frameworks capable of withstanding both physical and cyber-threats in an increasingly contested orbital environment.

Read more: https://telecom.economictimes.indiatimes.com/news/portal-in-portal/satcom/chinas-bold-strategies-to-counter-starlink-lasers-sabotage-and-military-innovation/123011896

China plots pathway to tech supremacy through brain-computer interfaces

The Chinese government, led by multiple state bodies including the Ministry of Industry and Information Technology, the National Development and Reform Commission, and city-level administrations like Beijing and Shanghai initiating a comprehensive roadmap to develop brain–computer interface (BCI) technology as a key "future industry." This initiative unfolds against the backdrop of geopolitical competition in advanced neuroscience and artificial intelligence, as well as domestic ambitions under strategies like "Made in China 2025" that prioritize technological self-reliance.

The policy framework calls for significant breakthroughs in BCI technology by 2027 and the establishment of advanced industrial, technological, and standards infrastructure. The goal by 2030 is to cultivate two to three globally influential enterprises and develop a secure, reliable industry ecosystem. Key measures include accelerated deployment of BCI applications across healthcare, industrial manufacturing, consumption, smart living, education, sports, and safety sectors. The guidelines prioritize advancements in core hardware and software, including BCI chips, ultralow-power communications chips, implantable and non-implantable devices (such as headbands, ear-worn, or smart glasses), decoding algorithms, and reliable data transmission technologies. Standards development and regulatory oversight over brain data collection and usage are being fast-tracked to ensure safety and interoperability.

Provincial plans reinforce the national strategy: Beijing's 2025–30 action plan targets the incubation of 3–5 global BCI leaders and over 100 specialized technology firms; Shanghai's strategy aims for full clinical application of BCI products by 2030. Meanwhile, progress in clinical BCI innovation is advancing rapidly: Chinese Institute for Brain Research and NeuCyber NeuroTech have already implanted semi-invasive wireless chips (Beinao No. 1) in human patients three to date with plans for more and eventual trials involving up to 50 patients.

Strategically, this campaign underscores China's ambition to lead in human–machine integration by aligning neuroscience, clinical research, and industrial policy. It reflects a transition from exploratory R&D to commercialization and cross-sector deployment, raising implications for global competition in neurotechnology, ethical governance of neurodata, and emerging domains of military and civilian convergence in BCI applications.

Read more: https://www.scmp.com/news/china/science/article/3321136/china-plots-pathway-tech-supremacy-through-brain-computer-interfaces?

Republic of China (ROC) | Taiwan

'China's Instagram' Xiaohongshu used to steer Taiwan public opinion: Taipei official

The central subject of this briefing is the covert digital influence campaign orchestrated by state-linked entities in the People's Republic of China, employing platforms such as Instagram and its local analogues Xiaohongshu and Douyin to shape public opinion in Taiwan, as identified by officials in Taipei. This operation unfolds amid heightened cross-strait tensions, where Beijing increasingly relies on nuanced psychological and informational tools rather than overt military confrontation, aiming to sway Taiwan's youth and broader public through cultural and lifestyle content.

Chinese "content farms" and coordinated online networks have deployed a multi-layered strategy: faux user accounts post innocuous lifestyle, fashion, or pop-culture content, which are then amplified through fan pages and dummy accounts eventually infiltrating legitimate public groups to subtly seed pro-Beijing narratives. These patterns align with the "four-level structure" of cognitive warfare previously used by the mainland to shape perceptions ranging from morale to political identity. Such operations exploit Taiwan's high internet

usage and reliance on digital media for news and entertainment, particularly among younger demographics who are less likely to verify content critically. Platforms like Xiaohongshu often dubbed "Chinese Instagram" and Douyin are especially potent vectors, given their popularity and algorithmic reach.

Taipei's regulatory agencies have flagged these orchestrated influence efforts as a form of cognitive warfare embedded in social media consumption. Although overt political messaging is rare, the cultural and ideological framing in lifestyle content gradually aligns audiences with pro-unification narratives, softening resistance to Beijing's broader narratives

The implications are considerable: Beijing's campaign underscores the evolving nature of modern influence operations, where subtle cultural levers replace traditional propaganda in democratic societies. For Taiwan, this raises urgent challenges in preserving social cohesion, democratic resilience, and national identity. It also reinforces the need for enhanced media literacy, stronger content oversight, and a fortified societal response to the subtle encroachments of digital cognitive warfare.

Read more: https://asia.nikkei.com/politics/international-relations/taiwan-tensions/china-s-instagram-used-to-steer-taiwan-public-opinion-taipei-official

Three former employees of TSMC detained

The primary focus is on Taiwan Semiconductor Manufacturing Company (TSMC), one of the world's leading semiconductor firms, and three of its former engineers, who have been detained under suspicion of compromising classified technology related to the production of cutting-edge 2-nanometer chips. The key actors include the Taiwan High Prosecutors' Office, which is conducting the investigation under the National Security Act, and TSMC, which self-reported the suspected breach and is cooperating fully with authorities to safeguard its trade secrets. This incident emerges against a backdrop of heightened global competition for semiconductor dominance, where Taiwan's advanced chipmaking capabilities especially at the 2 nm node are of immense strategic and economic value.

Authorities have detained one ex-TSMC engineer surnamed Chen, along with two others recently dismissed from the company (including one surnamed Wu), imposing restrictions on their communications. The investigation, initiated on July 25 following a disclosure by TSMC, centres on potential unauthorized dissemination of core chipmaking technology possibly involving clandestine data transfer to third parties. The advanced nature of the 2-nm process, scheduled for its first tape-out next month, underscores the sensitive, high-value nature of the information involved.

This marks the first known application of the National Security Act's provisions that prohibit the unauthorized reproduction, use, or disclosure of Taiwan's core national technologies. While prosecutors have yet to establish whether these individuals acted on behalf of a foreign government or commercial competitor, the move signals Taiwan's determination to shield its critical high-tech assets from espionage or industrial theft. Strategically, the case highlights the vulnerability of pivotal innovation centres to insider threats and underscores the urgency of reinforcing internal data safeguards. For Taiwan, and globally, the episode is a stark reminder that safeguarding semiconductor leadership demands not only technological excellence but also robust legal, organizational, and security frameworks against intellectual property exfiltration.

Read more: https://www.taipeitimes.com/News/front/archives/2025/08/06/2003841548

Russian Federation

Russia blocks calls via WhatsApp and Telegram as it tightens control over the internet

Roskomnadzor, Russia's media and internet regulator, decided to partially restrict voice (and in some cases video) calls on globally popular encrypted messaging platforms WhatsApp and Telegram. This action is part

of a broader, escalating push by the Russian government toward internet control and "digital sovereignty." Authorities framed the restrictions as necessary for combating crime citing platforms' use in fraud, extortion, sabotage, and terrorism and denounced the services for failing to cooperate with law enforcement investigations. Technical disruptions to call functionality have been confirmed: users report poor audio quality, complete inability to place calls in some cases, particularly for WhatsApp, while Telegram calls remain barely functional. Russia's control extends beyond these platforms: users across the country have experienced widespread mobile internet shutdowns, access to foreign sites has been throttled or blocked, VPNs are frequently disrupted, and a national "white list" of approved services is being enforced.

Simultaneously, the Kremlin is promoting use of Max, a state-backed multifunctional messaging app, set for preinstallation on all smartphones sold in Russia and deeply integrated with government services. Critics warn that Max bypasses encryption and enables state surveillance casting it as a tool for curbing independent communication.

Strategically, this selective throttling of encrypted communications marks a subtle but powerful shift in Russia's internet governance: rather than outright bans, targeted disruptions are used to weaken public reliance on independent platforms while bolstering acceptance of state-controlled alternatives. For digital rights and privacy stakeholders, the development underscores new pressure points in the contested arena of encrypted messaging, where limitations on voice though leaving text intact can significantly degrade communication resilience and democratic expression.

Read more: https://www.euronews.com/next/2025/08/14/russia-blocks-calls-via-whatsapp-and-telegram-as-it-tightens-control-over-the-internet

The Commonwealth of Australia

Australia's NBN picks Amazon's Project Kuiper over Starlink for remote internet

The central focus is on NBN Co, Australia's government-owned national broadband provider, and its strategic decision to partner with Amazon's Project Kuiper for the rollout of satellite-based internet service, instead of opting for SpaceX's Starlink. This initiative comes against the backdrop of Australia's enduring challenge of providing reliable broadband to rural, remote, and regional communities areas not served by terrestrial infrastructure and the looming decommissioning of NBN's aging Sky Muster geostationary satellites, which currently support around 300,000 premises but suffer from high latency and limited bandwidth. NBN Co conducted a rigorous procurement process involving regulatory, legal, technical, and commercial assessments, ultimately expressing confidence in Kuiper's ambitious deployment and substantial investment backing estimated at around US$15 billion.

Project Kuiper, Amazon's low-Earth orbit (LEO) satellite constellation, currently has 78 satellites in orbit following recent launches and intends to deploy over 3,200 in total providing significantly lower latency and higher throughput compared to both Sky Muster and Starlink. The service is expected to launch in Australia by mid-2026, beginning in Tasmania and proceeding north, with speeds potentially reaching up to 400 Mbps for residential users and up to 1 Gbps for enterprises. Meanwhile, Sky Muster will remain operational until around 2032 to ensure continuity during the phased transition. Strategically, NBN Co's choice of Kuiper over the more established Starlink reflects a concerted effort to balance performance, affordability, and sovereign control of critical infrastructure particularly amid concerns about political risks inherent in over-reliance on a single U.S. provider. The shift to LEO satellite technology aligns with broader global trends of deploying resilient, low-latency networks to bridge the digital divide. By preparing to deliver "city quality broadband" to isolated communities, this move positions Australia to more equitably integrate remote populations into the national digital economy, supporting education, telehealth, remote work, and emergency services.

Read more: https://www.timeslive.co.za/news/sci-tech/2025-08-05-australias-nbn-picks-amazons-project-kuiper-over-starlink-for-remote-internet/

Australian Information Commissioner takes civil penalty action against Optus

The central focus is on Singtel Optus Pty Limited (and its subsidiary Optus Systems), a major Australian telecommunications provider, and the Australian Information Commissioner, acting through the Office of the Australian Information Commissioner (OAIC). In August 2025, the Commissioner launched civil penalty proceedings in the Federal Court of Australia following a catastrophic data breach in September 2022. Over a three-year period from approximately October 17, 2019, to September 20, 2022 Optus allegedly failed to take reasonable steps to protect the personal information of roughly 9.5 million current, former, and prospective customers, resulting in a "serious interference with privacy" under section 13G of the Privacy Act 1988.

The breach exposed sensitive identifiers including passport and driver's license numbers, Medicare and email details and led to some data being posted on the dark web. The OAIC emphasized that the inadequacy of Optus's cybersecurity and information risk management systems was disproportionate to the company's size, scope of customer data, and risk profile. The Commissioner has alleged one contravention per individual affected, potentially exposing Optus to penalties of up to AUD 2.22 million per breach, though the heightened maximum penalty of AUD 50 million per breach introduced in December 2022 does not apply retroactively.

Optus has expressed regret to customers and claims to be reviewing the allegations, while affirming its continued investment in cybersecurity. Strategically, this regulatory escalation signals a significant shift toward accountability in data protection within Australia's digital economy. For organizations handling large-scale personal data, the case underscores the urgency of robust risk governance and preventative cybersecurity measures. More broadly, it heralds a new era in privacy enforcement, where failures to uphold trust and safeguard data may result in severe financial and reputational consequences.

Read more: https://www.oaic.gov.au/news/media-centre/australian-information-commissioner-takes-civil-penalty-action-against-optus

West Asia

Microsoft launches probe after Israeli mass surveillance claims

Microsoft and its decision to launch an external investigation following allegations that Unit 8200, Israel's military intelligence wing, exploited Microsoft's Azure cloud platform to conduct mass surveillance of Palestinians in the West Bank and Gaza. The probe was initiated after a collaborative investigative report by The Guardian, +972 Magazine, and Local Call revealed that Unit 8200 allegedly recorded "millions of calls per hour" and stored them using a custom, segregated Azure suite created by Microsoft's Israel office. This revelation alarmed executives at Microsoft's U.S. headquarters, who feared that local staff might have concealed the scope of this activity and its implications.

Microsoft reaffirmed that storing data derived from broad or mass surveillance of civilians in these territories would violate its terms of service and engaged the U.S. law firm Covington & Burling to oversee the investigation. This marks Microsoft's second external review involving its ties to Israeli military entities. A prior inquiry earlier in the year concluded that there was no evidence of Azure being used to target or harm Gaza civilians. The current probe explicitly addresses the more detailed and concerning allegations emerging from the recent media disclosures.

Inside Microsoft, the issue has sparked activist pressure, particularly from an employee-led campaign called No Azure for Apartheid, which accuses the company of complicity in human rights abuses and calls for severing all ties with the Israeli military. Sources suggest that leadership is urgently reevaluating data stored in Azure, especially as concerns mount that the surveillance infrastructure may have been used to identify targets for strikes in Gaza. Microsoft has committed to publicly sharing the factual outcomes of the investigation.

Strategically, this development underscores the growing scrutiny on tech companies' responsibility for how

their platforms and complex ties to security agencies may enable surveillance or conflict. It reflects broader concerns about cloud-enabled surveillance, corporate ethics in wartime contexts, and the need for transparent governance of digital infrastructure in contested regions. The findings could reshape how global tech firms manage geopolitical risks and privacy obligations moving forward.

Read more: https://www.arabnews.com/node/2611959/amp

Malware & Vulnerabilities

Before ToolShell: Exploring Storm-2603's Previous Ransomware Operations

The main subject centers on Storm-2603, a newly identified threat actor linked to recent ransomware operations exploiting the "ToolShell" vulnerability chain in Microsoft SharePoint servers. Key actors include Storm-2603 itself tracked alongside known Chinese-affiliated APTs such as Linen Typhoon (APT27) and Violet Typhoon (APT31) and cybersecurity researchers at Check Point Research (CPR) and Unit 42, who have closely examined its tactics, techniques, and procedures (TTPs).

Contextually, these campaigns unfold amid widespread exploitation of four critical SharePoint vulnerabilities (CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, CVE-2025-53771), collectively dubbed "ToolShell," which facilitate full remote code execution on on-premises servers. Storm-2603 appears to operate at the intersection of espionage-style APT behavior and financially motivated ransomware deployment, underscoring a hybrid threat model.

Researchers uncovered that Storm-2603 employs a custom command-and-control (C2) framework named ak47c2, featuring both HTTP-based and DNS-based backdoor clients "ak47http" and "ak47dns." These tools use XOR and hexadecimal encoding to obfuscate commands and data, with DNS communication broken into small fragments and reassembled on the server side. Attacks also deploy multiple ransomware strains such as LockBit Black and Warlock (X2anylock) often bundled and delivered through DLL sideloading and MSI installers, accompanied by use of legitimate tools like masscan, PsExec, and SharpHostInfo for reconnaissance and lateral movement. Notably, the threat actors integrate BYOVD ("Bring Your Own Vulnerable Driver") tactics installing a signed third-party driver to disable endpoint defences via IOCTL commands.

These findings highlight significant strategic and security implications. Organizations with on-premises SharePoint deployments face elevated risk from sophisticated, multi-layered ransomware threats. For cybersecurity stakeholders, the Storm-2603 model underscores the necessity of proactive patching, comprehensive threat detection, layered defence architectures, and rapid incident response. Internationally, this trend reflects a growing convergence of state-linked APT methods with cybercriminal tactics, blurring traditional lines and escalating risk across sectors.

Read more: https://research.checkpoint.com/2025/before-toolshell-exploring-storm-2603s-previous-ransomware-operations/

Frozen in transit: Secret Blizzard's AiTM campaign against diplomats

The central subject of this briefing is a cyberespionage operation conducted by the Russian-linked threat actor known as Secret Blizzard, targeting foreign embassies in Moscow. Key actors include Secret Blizzard (also tracked under the Turla group), diplomatic personnel, and Microsoft Threat Intelligence, which identified and analyzed the campaign. This effort unfolds within a broader geopolitical context: the strategic value of diplomatic communications, the heightened vulnerabilities of embassy networks especially those reliant on local Internet service providers and the persistent risk of nation-state cyber operations aimed at intelligence collection.

Technically, Secret Blizzard has executed an adversary-in-the-middle (AiTM) intrusion dubbed "Frozen in

Transit," using a custom malware tool called ApolloShadow. This tool enables the attacker to install a trusted root certificate on devices, effectively intercepting and redirecting traffic through attacker-controlled websites while masquerading as legitimate. By compromising TLS or SSL trust chains, AiTM positioning allows for credential harvesting, session hijacking, and sustained persistence on diplomatic systems. The campaign has been active since at least 2024 and continues to pose a high espionage threat to embassies and diplomatic networks in Moscow, especially those depending on local connectivity.

The implications of this covert operation are significant. By compromising diplomatic devices at the TLS-trust level, the actors may gain long-term access to sensitive communications, compromise credentials, and mislead or manipulate officials undetected. The ability to maintain persistent footholds through root-certificate implants underscores the sophistication of the campaign and highlights the challenges of securing diplomatic and high-value targets in sovereign environments. Strategically, this reflects the growing use of stealthy interception-based methods beyond phishing or malware drops within state-sponsored espionage. For at-risk organizations such as embassies, international NGOs, and governmental agencies, it underscores an urgent need for hardened network defences, certificate validation practices, zero-trust architectures, and vigilant threat detection tailored to intercept-based threats.

Read more: https://www.microsoft.com/en-us/security/blog/2025/07/31/frozen-in-transit-secret-blizzards-aitm-campaign-against-diplomats/

New 'Shade BIOS' Technique Beats Every Kind of Security

The primary focus is on an emerging and highly sophisticated hardware-based attack technique known as Shade BIOS, unveiled by security researchers from FFRI Security, led by Kazuki Matsuo. This technique represents a significant evolution in firmware exploitation, allowing malware to execute entirely outside traditional operating system (OS) environments and beyond the reach of conventional security tools like antivirus, endpoint detection and response (EDR), or extended detection and response (XDR) systems. Unlike UEFI rootkits or bootkits which depend on the OS to carry out malicious activities and therefore remain somewhat visible to defensive mechanisms Shade BIOS breaks this dependency by keeping the BIOS portion of firmware active in memory even after the OS has loaded, establishing a parallel execution environment safe from detection.

Technically, Shade BIOS deceives the OS loader into preserving the BIOS memory region during system initialization, instead of discarding it as usual. This enables the BIOS to manage memory and hardware drivers independently, allowing it to perform tasks such as file I/O, command execution, and device interaction all without any interface with the compromised OS or exposure to monitoring tools. Its deployment could theoretically span virtually all PCs, servers, or motherboards across different brands and operating systems, leveraging UEFI's universality to amplify reach and stealth.

The implications are profound: security mechanisms that rely on detecting anomalies within the OS or its boot process would be rendered ineffective, as Shade BIOS exists fundamentally outside their scope. This breakthrough underscores the reinvigorated threat of firmware-level attacks and the necessity of incorporating low-level hardware integrity checks into defensive strategies. As enterprises and infrastructure increasingly depend on layered security, this development signals an urgent need for firmware validation tools, runtime BIOS integrity monitoring, and partnerships with hardware vendors to mitigate future attacks at the most foundational level of computing architecture.

Read more: https://www.darkreading.com/endpoint-security/shade-bios-technique-beats-security?

11 Malicious Go Packages Distribute Obfuscated Remote Payloads

A sophisticated software supply-chain attack targeting the Go development ecosystem, revealed by the Threat Research Team at Socket. Eleven malicious Go modules ten still active on the Go Module registry were identi-

fied, with eight deliberately crafted as typosquats that mimic legitimate package names, exploiting developers' reliance on Go's decentralized module system SocketSC Media.

Against a backdrop of evolving open-source threats, these packages deploy an index-based string array obfuscation routine that effectively conceals malicious behavior from static analysis. At runtime, each module silently invokes a system shell using constructs like exec.Command("/bin/sh", "-c", <obfuscated>), fetching a secondary payload from .icu and .tech command-and-control (C2) domains specifically paths like /storage/de373d0df/a31546bf. Notably, six of these C2 URLs remain reachable, granting threat actors on-demand access to any developer or CI environment that imports the compromised modules.

The second-stage payloads comprise ELF binaries on Linux and PE executables on Windows. These payloads gather system metadata, extract browser data, and send it back to C2 servers. To evade sandbox detection, they often begin with a one-hour delay before execution. These techniques expose both Linux build servers and Windows workstations to stealthy credential harvesting and environment infiltration.

Strategically, this campaign highlights the risks inherent in Go's open package distribution model where direct imports from GitHub and namespace ambiguity enable malicious modules to masquerade as trusted dependencies. The incident underscores the urgent need for developers to adopt real-time dependency scanning, conduct thorough audits, maintain curated package registries, and apply anomaly detection within CI/CD pipelines. More broadly, it reflects the expanding threat landscape in software supply chains, where even minor or obscure code components can become vectors for widescale compromise.

Read more: https://socket.dev/blog/11-malicious-go-packages-distribute-obfuscated-remote-payloads

Data Dump From APT Actor Yields Clues to Attacker Capabilities

The central focus is on a significant intelligence breach in which independent hackers known as "Saber" and "cyb0rg" infiltrated and extracted data from a nation-state-level advanced persistent threat (APT) operator, referred to as "KIM." The operator is suspected of affiliations with either the North Korea–linked Kimsuky group or a Chinese-aligned cyber-espionage team. This breach occurred amid a broader escalation of cyber espionage activity targeting sensitive national security targets, including South Korea's government agencies. The hackers compromised both a virtual workstation and a virtual private server (VPS) used by the APT operator, exfiltrating logs from phishing campaigns targeting the South Korean Defense Counterintelligence Command and the Supreme Prosecutor's Office. They also obtained nearly 20,000 browser history entries, internal documentation, credentials, command files, source code, and attack tools. Among the specialized malware disclosed were a TomCat remote kernel backdoor, a custom Cobalt Strike beacon, the "RootRot" backdoor via Ivanti Control, Android Toybox payload variants, and exploits like Bushfire. The leak provides a rare window into the attacker's tactics, techniques, and procedures, revealing command-and-control infrastructure, day-to-day operations, and campaign breadth.

Analysis by cybersecurity researchers confirms the data's authenticity. Indicators suggest that while the phishing kit and domain similarities hint at Kimsuky influence, browsing behavior and language point to Chinese operators, possibly mimicking Kimsuky to sow confusion. The disclosure significantly enriches the cyber threat intelligence community's understanding of nation-state espionage, offering tangible artifacts that can enhance detection, attribution, and defensive measures.

Strategically, this incident highlights both the operational depth of state-aligned cyber actors and the growing vulnerabilities within APT infrastructure. For defenders, this emphasizes the necessity of leveraging leaked intelligence to refine indicators of compromise, urgency in patching defensive gaps, and improved collaboration across intelligence and security organizations to stay ahead in the evolving cyber-espionage landscape
.
Read more: https://www.darkreading.com/threat-intelligence/data-dump-apt-actor-attacker-capabilities?

ShinyHunters Targets Salesforce Amid Clues of Scattered Spider Collaboration

ShinyHunters and Scattered Spider whose recent campaign patterns suggest emerging collaboration, amplifying the severity of ongoing data extortion threats. ShinyHunters, known for large-scale data breaches of high-profile companies, has resumed operations with phishing campaigns targeting Salesforce environments at major firms including Google, weaving in aggressive credential harvesting and voice phishing tactics. Scattered Spider, a financially motivated ransomware and intrusion group active since 2022, originally specialized in social engineering attacks, especially voice-based deception, and executing complex CRM hacks.

Recent analyses by ReliaQuest identify significant overlaps between both groups. Shared attack infrastructure, phishing domain patterns (such as ticket-brand-themed domains), synchronized targeting timelines, and blends of social engineering techniques strongly indicate operational convergence. The combined strategy marries ShinyHunters' capacity for broad data theft with Scattered Spider's refined, high-pressure infiltration methods. This complicates attribution, as indicators of compromise (IoCs) once unique to a single group are now shared, undermining traditional detection systems.

This alliance is manifesting in elaborate phishing campaigns impersonating tools like Salesforce or Okta, designed to harvest credentials or gain initial access in ways that mimic legitimate enterprise tools. The financial services and technology sectors are now priority targets, as phishing domains increasingly impersonate these verticals.

Strategically, the apparent teaming of ShinyHunters and Scattered Spider marks a turning point in cyber extortion: threat groups are now forming hybrid coalitions to enhance operational reach and camouflage attack attribution. Organizations must shift to proactive defense postures prioritizing detection of behavioral patterns over simple indicator matching with heightened vigilance against phishing, credential abuse, and CRM platform compromise. This trend signals a broader evolution in cybercrime where collaboration and tool-sharing enable more resilient, adaptive, and destructive campaigns across industries.

Read more: https://reliaquest.com/blog/threat-spotlight-shinyhunters-data-breach-targets-salesforce-amid-scattered-spider-collaboration/

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.