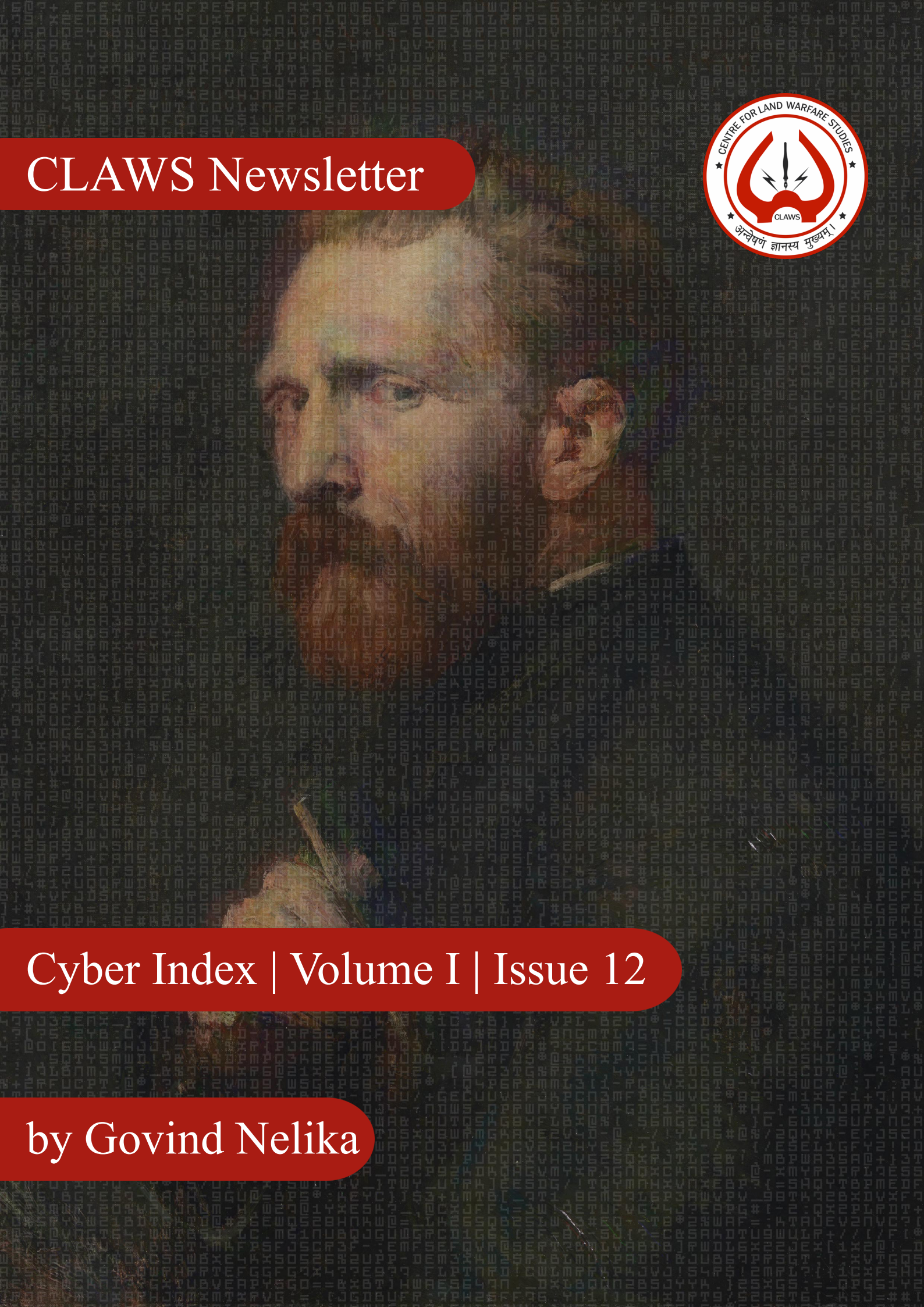
CLAWS Newsletter



Cyber Index | Volume I | Issue 12

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 04

United States of America (USA) 08

People's Republic of China (PRC) | China 09

Republic of China (ROC) | Taiwan 11

Europe 11

The Commonwealth of Australia 12

West Asia 13

Malware & Vulnerabilities 14

Global Brief

China Threat Actor Storm-2603 active exploitation of Microsoft on premises SharePoint vulnerabilities

Microsoft has disclosed the active exploitation of several zero-day vulnerabilities in on-premises Microsoft SharePoint Server instances by a suspected state-aligned threat actor. The attacks, which began in April 2024 and continued into mid-2025, exploited unpatched SharePoint servers to gain initial access to enterprise networks. The actor used a sequence of flaws most notably CVE-2023-29357 (a privilege escalation vulnerability) chained with CVE-2023-24955 (a remote code execution flaw) to execute arbitrary code in the context of SharePoint web applications, thereby establishing persistent footholds in affected environments.

Following exploitation, the attackers deployed custom web shells to maintain access and conducted reconnaissance, credential harvesting, and lateral movement operations. These activities targeted primarily government and defence organizations, as well as critical infrastructure operators across North America and Europe. The attackers leveraged legitimate administrative tools and manipulated SharePoint's built-in functionalities to avoid detection, making forensic analysis and attribution challenging. Indicators of compromise include suspicious child processes spawned by SharePoint IIS worker processes, as well as anomalous authentication attempts tied to forged JSON Web Tokens (JWTs).

Microsoft Threat Intelligence attributes this campaign to a highly capable actor exhibiting hallmarks of a state-sponsored group, although no formal attribution has been made public. In response, Microsoft collaborated with its Detection and Response Team (DART) and security partners to disrupt the campaign and issue security guidance, detection rules, and mitigations for affected systems. The company has urged all organizations running on-premises SharePoint to apply the latest security patches and review historical activity for signs of compromise.

This incident underscores the persistent risk posed by unpatched enterprise software and the strategic targeting of collaborative platforms in espionage campaigns. It highlights how state-aligned actors exploit niche vulnerabilities to penetrate hardened environments, contributing to an ongoing trend where critical software infrastructure becomes a vector for geopolitical cyber operations and long-term intelligence gathering.

Read more: https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

Euro-Atlantic and Indo-Pacific united in response to hybrid threats

The Euro-Atlantic and Indo-Pacific regions are increasingly coordinating their responses to hybrid threats as part of a broader strategic convergence aimed at defending democratic institutions and critical infrastructure from coercive tactics employed by authoritarian states. Key actors in this alignment include NATO, the European Union, and Indo-Pacific partners such as Australia, Japan, South Korea, and India. These efforts reflect growing concern over state-sponsored influence operations, disinformation campaigns, cyber intrusions, and economic coercion particularly from China, Russia, and North Korea that aim to destabilize open societies and weaken alliances without triggering conventional military conflict.

Recent initiatives demonstrate an evolving network of cross-regional cooperation that spans cybersecurity, military interoperability, technology standards, and counter-disinformation efforts. For example, NATO's new outreach to Indo-Pacific democracies includes deeper information sharing and coordinated responses to cyber incidents and foreign interference, while the EU is expanding its cybersecurity and strategic communications partnerships with regional allies. Japan and South Korea have hosted and participated in joint cyber exercises with European partners, and Australia has strengthened its cybersecurity dialogue with both NATO and the EU. These moves reflect a shared recognition that hybrid threats by design exploit vulnerabilities in both digital infrastructure and the information environment, often through legal grey zones and asymmetrical tactics that complicate attribution and response.

The unification of Euro-Atlantic and Indo-Pacific security agendas marks a shift toward a more globalize and multidomain understanding of national security. It underscores that threats to sovereignty and democrat ic resilience in one region have ripple effects globally, particularly in a digitally interconnected world. A authoritarian actors deploy hybrid strategies that blend cyber warfare, economic pressure, and narrative ma nipulation, democratic coalitions are countering with a mix of resilience-building, defensive interoperability and strategic deterrence. This cross-regional solidarity signals a transformation in collective defence thinking reflecting the necessity of integrated approaches to complex, non-traditional threats.

Read more: https://www.aspistrategist.org.au/euro-atlantic-and-indo-pacific-united-in-response-to-hybrid-threats/

Amazon to shut down Shanghai AI research lab

Amazon has announced the closure of its Shanghai-based artificial intelligence research lab, the Amazon We Services (AWS) AI Lab Shanghai, marking a significant strategic shift amid increasing geopolitical and reg ulatory pressures between China and the United States. The lab, which focused on advanced AI technologie including machine learning models, natural language processing, and computer vision, was part of Amazon' broader effort to enhance its global AI capabilities. The decision affects approximately 200 employees an comes at a time when U.S. tech firms are reassessing their operational exposure in China due to growing con cerns over data security, intellectual property protection, and potential regulatory entanglements.

This development is framed by broader U.S.–China tensions over emerging technologies, particularly in th fields of AI, semiconductors, and cloud computing, where Washington has implemented export controls an investment restrictions to limit China's access to cutting-edge technologies. These measures have created more complex environment for American companies operating in China, especially those in sensitive sectors Amazon's move reflects a recalibration of risk management strategies by Western firms operating in a jurisdic tion where domestic data laws such as China's Data Security Law and Personal Information Protection Law impose stringent controls on how data is stored, accessed, and transferred.

The closure of the Shanghai lab also follows a trend among major U.S. tech companies including Google Meta, and Microsoft that have reduced or restructured their research footprints in China to avoid legal expo sure and reputational risks. Strategically, the decision underscores a decoupling of U.S. corporate R&D infra structure from China in high-tech domains, potentially reducing future collaborative innovation but insulatin companies from compliance and espionage risks. The shift has national security implications as AI become a central component of both commercial competitiveness and military modernization, and may accelerate th bifurcation of global AI ecosystems into separate spheres of influence aligned with national interests.

Read more: https://asia.nikkei.com/Business/Technology/Amazon-to-shut-down-Shanghai-AI-research-lab

How China's Patriotic 'Honkers' Became the Nation's Elite Cyberspies

A growing convergence between state-aligned cyber espionage units and nationalist hacktivist groups i China is reshaping the global cyber threat landscape, as demonstrated by the evolving relationship betwee pro-Beijing hacker collectives and Chinese intelligence services. Notably, the group known as the "Honke Union" once an independent, nationalist hacking collective has increasingly aligned with state cyber opera tions, blurring the boundary between patriotic activism and coordinated cyber-espionage. This transformatio reflects a broader strategic shift within China's cyber doctrine, wherein informal or semi-autonomous actor are leveraged as force multipliers by state intelligence agencies, particularly in campaigns targeting foreig governments, critical infrastructure, and technology firms.

Recent investigations have revealed growing overlaps in tools, tactics, and operational targets between Honk er-affiliated hackers and established Chinese advanced persistent threat (APT) groups such as APT41 an APT27. These actors have been implicated in sophisticated operations involving zero-day vulnerabilities, cus tom malware frameworks, credential theft, and long-term network infiltration across targets in the U.S., Tai

wan, Japan, and Western Europe. The Honker Union, originally active in retaliatory defacements and DDoS attacks, now exhibits technical signatures and strategic behaviour consistent with professional cyberespionage, including stealthy data exfiltration and intelligence gathering.

This convergence has coincided with China's intensified efforts to expand its cyber influence amid escalating geopolitical tensions with the United States and its allies, particularly over Taiwan, semiconductor supply chains, and the South China Sea. By cultivating a cyber-ecosystem that fuses nationalist fervor with operational sophistication, Chinese state organs benefit from plausible deniability while extending the reach and agility of their cyber campaigns.

The fusion of hacktivism and state-backed cyber espionage poses significant challenges to attribution, deterrence, and defence, particularly for democratic nations whose critical infrastructure and political institutions are increasingly targeted. It underscores a strategic trend where national security is inseparable from information dominance, and where cyber operations are deeply embedded in geopolitical competition.

Read more: https://www.wired.com/story/china-honkers-elite-cyber-spies/

Vietnam's public security ministry takes over state stake in FPT Telecom

Vietnam's Ministry of Public Security has formally assumed control of the state's equity stake in FPT Telecom, one of the country's leading telecommunications and internet service providers. This transfer, approved by the Prime Minister, involves over 50 million shares equivalent to approximately 21% of the company previously held by the State Capital Investment Corporation (SCIC). The shift in ownership aligns with broader governmental efforts to restructure and centralize oversight of strategic national assets, particularly those involving critical infrastructure such as telecommunications.

FPT Telecom plays a vital role in Vietnam's digital infrastructure, operating extensive broadband networks, data centers, and international internet connections. The transfer of ownership to the Ministry of Public Security suggests a heightened focus on cybersecurity, surveillance capabilities, and the protection of sensitive communications amid rising regional and global cyber threats. The ministry has increasingly expanded its scope beyond traditional policing to include oversight of digital and information security, particularly in sectors seen as critical to national sovereignty and internal stability.

This development occurs against a backdrop of growing geopolitical tensions and increased cyber-espionage activity in Southeast Asia. Vietnam has faced persistent challenges from foreign state-backed actors targeting government institutions and infrastructure, prompting a recalibration of national security priorities. By integrating telecommunications infrastructure more directly under the Ministry of Public Security, the government aims to strengthen its control over data flows and pre-empt potential vulnerabilities in information networks. Strategically, the move signals Vietnam's intent to consolidate its digital sovereignty and enhance its resilience against external manipulation or interference in its communication systems. It also reflects a broader trend among states in the Asia-Pacific region to assert tighter governmental control over key technology sectors. As global power competition increasingly extends into cyberspace, this transfer underscores Vietnam's evolving approach to managing the intersection of technology, security, and national interest.

Read more: https://news.tuoitre.vn/vietnams-public-security-ministry-takes-over-state-stake-in-fpt-telecom-103250717145217228.htm

Microsoft, US national lab tap AI to speed up nuclear power permitting process

Microsoft and the U.S. Department of Energy's Idaho National Laboratory (INL) have partnered to deploy artificial intelligence in accelerating the regulatory approval process for nuclear power projects, a move that reflects growing governmental and private-sector alignment on expanding nuclear energy capacity to meet climate and energy security goals. The collaboration focuses on using large language models (LLMs) to automate the review and analysis of complex regulatory documents, including technical reports, safety protocols,

and licensing materials submitted to the Nuclear Regulatory Commission (NRC). By training AI tools on decades of nuclear permitting documentation, the system is designed to flag inconsistencies, streamline paperwork, and reduce the time required for agency review potentially cutting years off the traditional timeline for nuclear plant approval.

This initiative arises amid increasing geopolitical and economic pressures to diversify energy sources and reduce reliance on carbon-intensive fuels. With many nations seeking to achieve net-zero emissions by mid-century, nuclear energy has re-emerged as a strategic option due to its reliability and low-carbon output. However, regulatory bottlenecks often involving multi-year licensing procedures remain a key barrier to the timely deployment of next-generation reactors, such as small modular reactors (SMRs) and other advanced designs. The joint Microsoft-INL effort is intended not to replace human regulators, but to enhance decision-making by augmenting technical analysis and document processing capabilities. The AI systems developed are being tested for accuracy, bias mitigation, and compliance with federal safety standards, ensuring that automated tools remain transparent and accountable.

Strategically, this project signals a broader convergence of digital transformation and national energy policy. By integrating AI into nuclear infrastructure development, the U.S. seeks to maintain leadership in civilian nuclear technology, boost domestic energy resilience, and potentially offer a model for other countries facing similar regulatory challenges. It also reflects a wider global trend of leveraging AI in critical infrastructure to improve efficiency and strategic agility.

Read more: https://www.reuters.com/business/energy/microsoft-us-national-lab-tap-ai-speed-up-nuclear-power-permitting-process-2025-07-16/

China Is Putting Data Centers in the Ocean to Keep Them Cool

China is advancing its artificial intelligence (AI) and data infrastructure capabilities by developing undersea data centers designed to reduce energy consumption and bolster computing power. Spearheaded by Chinese tech firms in collaboration with local governments and state-backed research institutions, the project involves submerging container-sized data modules beneath coastal waters, where naturally low ocean temperatures assist in passive cooling of high-performance computing systems. These submerged facilities are engineered to support energy-intensive AI operations, including model training and real-time inference, while lowering carbon emissions and operational costs.

This technological push aligns with China's broader national strategy to become a global leader in AI and digital infrastructure, as outlined in its multi-year plans for innovation and industrial modernization. Traditional land-based data centers face increasing scrutiny over energy usage, especially given the country's carbon neutrality targets and regional power shortages. By relocating AI workloads offshore, China aims to address these environmental and logistical constraints while enabling scalability in AI development. Each underwater module can house hundreds of servers and be deployed rapidly, with modular designs allowing for easier expansion and integration into coastal smart city grids.

From a security and geopolitical perspective, the initiative also enhances data sovereignty and strategic control over computational assets. Undersea facilities offer additional physical protection from natural disasters and potential sabotage, and their placement within territorial waters ensures state jurisdiction over data flows and infrastructure. Furthermore, the integration of AI infrastructure into maritime zones dovetails with China's increasing emphasis on dual-use technologies that serve both civilian and defence applications. This development underscores a global shift in how nations and corporations' approach digital infrastructure amid rising demand for AI capabilities, energy constraints, and concerns over cyber and physical resilience. China's undersea data centres represent a convergence of environmental engineering, digital ambition, and strategic autonomy, potentially setting a precedent for next-generation infrastructure in the AI age.

Read more: https://www.scientificamerican.com/article/china-powers-ai-boom-with-undersea-data-centers/

United States of America (USA)

America's New AI Action plan the gist

The U.S. federal government's newly unveiled "America's AI Action Plan," backed by President Donald Trump and issued under Executive Order 14179, with support from key agencies including the Office of Management and Budget, OSTP, NIST, the FTC, FCC, and Department of Commerce. This plan is structured around three pillars: Accelerating AI Innovation, Building American AI Infrastructure, and Leading in International AI Diplomacy and Security.

The context for this initiative includes intensifying global competition with China for AI leadership, concerns over U.S. economic competitiveness, and divergent regulatory philosophies compared to the previous administration. Rather than prioritizing risk mitigation, the U.S. is now placing deregulation at the center of its AI industrial strategy.

Key developments include a directive to federal agencies to identify and roll back regulations perceived as burdensome such as privacy or misinformation-related provisions to stimulate faster deployment and adoption of AI. The plan warns that federal AI funding may be withheld from states that enact stringent AI regulations, and instructs agencies to consider state regulatory climates in grant allocations. Other actionable steps include streamlining environmental permitting for data center and semiconductor construction, fast-tracking energy infrastructure projects, and promoting open-source and "open-weight" AI ecosystems

The plan also calls for the export of the full U.S. AI technology stack to allied nations, the tightening of export controls on AI compute technologies, and alignment of international governance standards with American values. Additionally, it mandates federal procurement be restricted to AI systems deemed ideologically neutral and free of bias.

Strategically, the initiative marks a pronounced policy shift toward maximizing AI-driven economic growth and technological dominance over regulatory caution. By foregrounding deregulation and permitting incentives, it positions AI as a cornerstone of U.S. industrial renewal and global leadership. The plan reflects broader trends in techno-nationalism and industrial policy, where technology governance becomes a tool of statecraft and raises critical questions regarding consumer protection, equity, and environmental safeguards. Future tensions may emerge between federal priorities and state-led AI oversight, influencing the trajectory of AI governance in a contested global arena

Read more: https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

China hawks rattled over Trump's 'dangerously inconsistent' chip pivot

The focus is on the Trump administration's sudden reversal of restrictions on Nvidia's H20 AI chips, a move that has alarmed U.S. security "china hawk" lawmakers. Initially banned under prior export controls to limit Beijing's access to high-performance AI hardware, approvals were reversed after direct lobbying by Nvidia CEO Jensen Huang who reportedly secured assurances that sales would align with broader trade negotiations. This change occurs amid deepening U.S.–China geopolitical tensions and high-stakes economic competition centered on leadership in AI and semiconductor capabilities. H20 chips used extensively for AI inference workloads are viewed by critics as enabling enhancements to China's military intelligence, surveillance, and technological ecosystem. National security experts and former government officials have warned the export poses strategic risks.

Technically, the key issue is whether providing lower-tier but still advanced chips like the H20 to Chinese entities may erode the effectiveness of export control policy. Proponents argue that permitting such exports creates dependency on U.S. tech stacks, while critics see it as unsafe bargaining leverage tied to a trade concession on rare-earth magnet exports.

The reaction from hawkish figures including legislators across party lines reflects frustration at what they describe as a pattern of policy inconsistency and transactional governance. Concerns center on the credibility of U.S. export control regimes and the message sent to both industry and global competitors.

Strategically, this reversal underscores the tensions between commercial and security imperatives in U.S. China policy. On one hand, Silicon Valley and industry stakeholders see continued access to Chinese markets as essential. On the other, national security voices warn that even limited exports could undercut America's AI advantage and embolden Beijing's technological ascent. The episode vividly illustrates the broader trend of politicized trade instruments and the fragility of export controls in a polarized environment raising the risk that future policy shifts may further erode global enforcement norms.

Read more: https://subscriber.politicopro.com/article/2025/07/china-hawks-rattled-over-trumps-dangerously-inconsistent-chip-pivot-00454619

Huang downplays role in China chip ban reversal

The primary subject of the development is Jensen Huang, CEO of NVIDIA, and his public stance on the company's role in the context of U.S.–China tech tensions, particularly in the area of artificial intelligence. Amid ongoing geopolitical and economic frictions between Washington and Beijing, U.S. export controls on advanced semiconductors have directly affected NVIDIA's ability to supply its high-performance AI chips, such as the A100 and H100, to Chinese clients. These restrictions are part of broader national security measures aimed at preventing China's military and surveillance apparatus from gaining access to leading-edge computing technologies. Huang, speaking during a forum in Singapore, downplayed NVIDIA's centrality to China's AI ambitions, suggesting that the country possesses robust talent, strong data access, and alternative pathways to develop competitive AI capabilities even in the absence of U.S. chip technologies.

Huang's remarks serve to reposition NVIDIA as a neutral commercial entity caught in the crossfire of political decisions beyond its control, while implicitly acknowledging the challenges created by decoupling trends in the semiconductor sector. His comments also reflect a shift in tone, distancing the company from narratives that portray it as a linchpin in the global AI arms race. At a technical level, the export restrictions target chips with high processing throughput, large memory bandwidth, and advanced parallel computing capabilities essential components for training large-scale AI models, including generative AI and autonomous systems.
Strategically, Huang's position illustrates the complicated dynamics multinational technology firms face as they navigate between two increasingly adversarial superpowers. While the U.S. aims to constrain China's access to critical computing power, China is accelerating efforts to build domestic alternatives and deepen its AI ecosystem. This incident underscores the fragility of global tech supply chains and signals the intensifying bifurcation of the AI development landscape, where commercial innovation is increasingly entangled with national security priorities and geopolitical competition.

Read more: https://www.perplexity.ai/page/huang-downplays-role-in-china-v.Tb2pVaQKGRyNWwvgJI_g

People's Republic of China (PRC) | China

Chips, smart devices produced overseas could have designed backdoors to steal sensitive info: MSS

The Chinese Ministry of State Security (MSS) has issued a pointed warning regarding the growing cybersecurity risks posed by embedded technical backdoors in digital systems, highlighting their potential to compromise not only individual privacy and corporate data but also national security. A technical backdoor refers to hidden access paths embedded in hardware or software that bypass conventional authentication protocols. While sometimes included for legitimate reasons such as debugging or post-sale maintenance these access points, if not properly secured or removed, can be exploited by malicious actors to gain unauthorized control over systems. The MSS emphasized that some foreign-made chips, smart devices, and software may be inten-

tionally designed with such backdoors, enabling remote control capabilities such as unauthorized activation of cameras and microphones or surreptitious data collection. These functions could be triggered by specific signals sent by the original manufacturer or compromised by third parties.

The ministry also warned of advanced tactics used to compromise devices, including tampering with software update mechanisms, injecting malicious code into open-source repositories, and corrupting components in the supply chain all methods capable of delivering persistent surveillance tools without detection. The MSS stressed that these practices represent a significant and covert threat, capable of undermining critical national infrastructure and leaking classified information.

In light of these risks, the MSS advocated for the adoption of domestically produced chips and operating systems, particularly in sensitive or confidential sectors, to reduce dependency on foreign technologies that could harbour hidden vulnerabilities. The advisory aligns with China's broader push for technological self-reliance amid escalating global cybersecurity concerns and geopolitical tensions. As cyber threats increasingly originate from complex global supply chains, this warning underscores the strategic importance of securing digital infrastructure through greater transparency, independent verification, and localized development to safeguard national sovereignty and information integrity.

Read more: https://www.globaltimes.cn/page/202507/1338833.shtml

Chinese AI firm MiniMax targets $4 billion-plus valuation in Hong Kong IPO

Chinese artificial intelligence firm MiniMax has confidentially filed for an initial public offering (IPO) in Hong Kong, marking a significant move by one of China's most promising AI startups amid intensifying global competition and evolving regulatory landscapes. Backed by major domestic tech players such as Alibaba, MiniMax is known for developing advanced generative AI systems, including large language models and multimodal platforms capable of synthesizing text, images, and speech. The IPO, expected to raise several hundred million dollars, would position the company as a leading contender in China's race to achieve technological parity with U.S. AI giants such as OpenAI, Anthropic, and Google DeepMind.

The timing of the filing coincides with increased scrutiny of Chinese tech firms' overseas listings, driven by both domestic data security concerns and geopolitical frictions with the United States. To navigate this environment, MiniMax has opted for a listing in Hong Kong, which is increasingly viewed as a strategic financial bridge for Chinese firms seeking international capital while remaining within the regulatory reach of Beijing. The decision also reflects China's broader effort to cultivate a robust domestic AI ecosystem by encouraging capital formation within its own jurisdictional sphere.

MiniMax's technology portfolio includes foundational models trained on extensive Chinese-language datasets, aimed at enterprise solutions, digital assistants, and content generation platforms. The company's growth is emblematic of the surge in investment across China's AI sector, supported by state policies promoting indigenous innovation, data localization, and reduced dependency on foreign semiconductors and cloud infrastructure.

Strategically, the IPO reinforces China's ambition to lead in AI development as a pillar of economic competitiveness and national security. It also signals a maturing of the domestic AI sector, where private companies are increasingly assuming a central role in driving foundational technology innovation. MiniMax's move underscores the shifting dynamics of global tech finance, where capital, regulation, and innovation are tightly interwoven with geopolitical strategy.

Read more: https://www.reuters.com/world/asia-pacific/chinese-ai-firm-minimax-files-confidentially-hong-kong-ipo-sources-say-2025-07-16/

Republic of China (ROC) | Taiwan

China-Aligned Espionage Actors Ramp Up Taiwan Semiconductor Industry Targeting

China-aligned cyber-espionage groups have intensified targeting of Taiwan's semiconductor sector through a series of sophisticated phishing campaigns aimed at compromising sensitive intellectual property and industrial infrastructure. Proofpoint researchers have attributed these operations to multiple advanced persistent threat (APT) actors, notably TA423 and the lesser known but active cluster identified as "UNGRAVEL." These groups employ tailored spear-phishing emails impersonating government agencies, trade organizations, and industry stakeholders to deliver custom malware payloads, including Chinoxy and other backdoors designed for persistent access and data exfiltration.

The operations exploit social engineering tactics to deceive high-value individuals in Taiwan's semiconductor supply chain, including engineers, executives, and researchers. Attack vectors often leverage geopolitical narratives or regulatory topics to increase credibility. Once inside the targeted systems, attackers establish command-and-control (C2) infrastructure to survey internal networks, extract proprietary chip design files, and monitor communications potentially enabling strategic theft of critical technologies central to Taiwan's global leadership in advanced chip fabrication.

This campaign occurs amid escalating cross-strait tensions, with Taiwan's semiconductor dominance particularly through companies like TSMC viewed as a strategic asset by both Taipei and foreign powers. As semiconductors underpin critical sectors including defence, AI, and consumer electronics, hostile attempts to undermine Taiwan's semiconductor ecosystem represent a significant national security risk. These cyber-operations align with China's broader strategy of technological self-sufficiency and military-civil fusion, which seeks to reduce dependency on foreign chip suppliers while absorbing cutting-edge capabilities.

Strategically, the surge in targeted cyber intrusions highlights the evolving threat landscape in which cyber-espionage functions as a tool of statecraft. It reflects broader trends of asymmetric competition in the Indo-Pacific, where digital aggression complements geopolitical posturing. Taiwan's semiconductor sector remains not only a technological linchpin but also a flashpoint for intelligence operations, making cybersecurity a frontline concern for regional stability and global supply chain integrity.

Read more: https://www.proofpoint.com/us/blog/threat-insight/phish-china-aligned-espionage-actors-ramp-up-taiwan-semiconductor-targeting

Europe

Global operation targets NoName057(16) pro-Russian cybercrime network

A coordinated international law enforcement operation led by Europol has disrupted the activities of the pro-Russian cybercrime network known as NoName057(16), a threat actor responsible for widespread distributed denial-of-service (DDoS) attacks against critical infrastructure across Europe and North America. The operation involved cyber units from law enforcement agencies in Germany, the United States, the United Kingdom, Poland, Finland, and other EU member states, and targeted the network's infrastructure, digital assets, and support channels. Authorities seized multiple servers and took down websites and Telegram channels used by the group to coordinate attacks and claim responsibility.

NoName057(16) emerged in early 2022 as a loosely affiliated, ideologically driven hacktivist collective that aligned with Russian geopolitical objectives, particularly in the context of the war in Ukraine. The group primarily conducted DDoS attacks against government websites, transport systems, media outlets, financial institutions, and energy companies in countries supporting Ukraine. Their operations utilized a volunteer-based DDoS-as-a-service model known as "DDosia," incentivizing participation with cryptocurrency rewards. Attack vectors included volumetric traffic floods and application-layer attacks, often launched with automated

tools distributed to participants through encrypted channels.

The dismantling of NoName057(16)'s infrastructure represents a significant tactical disruption to an operation that has contributed to the hybrid warfare landscape by blending cyber aggression with propaganda. The group's activities exemplify the convergence of cybercrime and state-aligned ideological motivations, blurring the distinction between independent actors and state-sponsored campaigns.

Strategically, this operation underscores the growing emphasis on international cyber law enforcement collaboration to counter asymmetric digital threats targeting civil infrastructure. It also signals a commitment by Western security agencies to protect democratic institutions from politically motivated cyber disruption. The case highlights broader trends in cyber warfare, where ideologically aligned hacktivist networks function as informal proxies in geopolitical conflicts, raising the stakes for both digital sovereignty and public-sector cyber resilience.

Read more: https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network

Italian cybersecurity firm Exein sees defence boost as it closes funding round

Italian cybersecurity firm Exein has completed a significant funding round aimed at accelerating the deployment of its embedded security solutions, particularly for defence and critical infrastructure applications. The company specializes in securing Internet of Things (IoT) and edge computing environments by embedding security protocols directly into device firmware a method that allows real-time threat detection, response, and mitigation at the hardware level without relying on external security layers. This approach is increasingly critical as global militaries and industrial systems adopt next generation connected devices that expand the attack surface for cyber adversaries.

The funding sourced from a mix of institutional investors and defence-oriented backers reflects a growing recognition of firmware-level vulnerabilities as a strategic security gap. Exein's platform employs lightweight, runtime security modules and AI-driven anomaly detection to safeguard embedded systems across sectors including aerospace, energy, and autonomous vehicles. These capabilities are particularly relevant in defence settings where operational continuity, low latency, and tamper resistance are paramount. The company also adheres to open-source principles, which enhances transparency and accelerates adoption in sensitive sectors where code auditability and trust are essential.

This development comes amid heightened geopolitical instability, especially in Europe, where NATO-aligned nations are seeking to bolster cybersecurity in response to escalating threats from state and non-state actors. Supply chain attacks, firmware backdoors, and zero-day vulnerabilities have all emerged as vectors of concern, particularly for military and dual-use technologies. Exein's solutions offer a proactive layer of security by embedding defence mechanisms at the silicon and OS level bypassing some of the limitations of traditional perimeter-based defences. Strategically, the funding positions Exein as a critical enabler of sovereign cybersecurity capabilities in the European defence ecosystem. It underscores a broader shift toward pre-emptive, embedded security architecture as a standard for protecting critical systems in an era of pervasive connectivity and rising cyber warfare.

Read more: https://ciso.economictimes.indiatimes.com/amp/news/next-gen-tech/italian-cybersecurity-firm-exein-sees-defence-boost-as-it-closes-funding-round/122574520

The Commonwealth of Australia

Australia adopts AS IEC 62443 as national cyber security standard to protect critical infrastructure

Australia has formally adopted the international cybersecurity framework AS/IEC 62443 as its national stan-

dard for securing critical infrastructure, marking a significant advancement in the country's approach to safeguarding industrial control systems (ICS) and operational technology (OT) environments. The initiative, led by the federal government in coordination with the Australian Cyber Security Centre (ACSC) and Standards Australia, aims to standardize protections across sectors deemed essential to national security and economic stability including energy, water, transport, health, communications, and defence.

The AS/IEC 62443 standard, developed by the International Electrotechnical Commission (IEC), provides a layered, risk-based methodology for securing automation and control systems against a range of cyber threats. It outlines requirements for system design, secure integration, access control, asset inventory, incident response, and ongoing lifecycle management. By implementing this standard nationally, Australia seeks to improve resilience against increasingly sophisticated threats, including ransomware, supply chain compromise, and state-sponsored cyber operations that target vulnerabilities in ICS and SCADA (Supervisory Control and Data Acquisition) systems.

The decision comes amid growing global concern about the cyber vulnerability of critical infrastructure, particularly following recent high-profile disruptions such as the Colonial Pipeline ransomware attack in the United States and widespread targeting of OT networks by advanced persistent threat (APT) groups. For Australia, which faces an increasingly contested regional cyber environment, standardizing industrial cybersecurity practices helps ensure interoperability, consistency, and preparedness across jurisdictions and industries.

Strategically, the national adoption of AS/IEC 62443 positions Australia as a proactive actor in the international cybersecurity landscape and supports its broader cyber resilience and digital sovereignty objectives. It reflects a shift toward harmonizing with global best practices while reinforcing national oversight. As cyber-physical systems become more integral to economic and defence operations, embedding robust, standardized security frameworks will be essential to deterring adversaries and maintaining operational integrity across critical sectors.

Read more: https://www.cyberdaily.au/security/12391-australia-adopts-as-iec-62443-as-national-cyber-security-standard-to-protect-critical-infrastructure

West Asia

New malware samples exfiltrate WhatsApp data to target Iran regime's enemies

A new cyber espionage campaign linked to Iran's state-aligned threat actor MuddyWater has been identified targeting individuals in the Middle East, with a particular focus on data exfiltration from the WhatsApp messaging platform. MuddyWater, also known as Static Kitten or MERCURY, is affiliated with Iran's Ministry of Intelligence and Security (MOIS) and is known for its persistent targeting of regional adversaries, including government officials, academics, and activists. The campaign utilizes Android malware embedded in malicious mobile applications, which impersonate legitimate services or security tools to lure victims into installation.

Once installed, the malware gains extensive permissions on the infected device, enabling it to bypass security mechanisms and access sensitive data. Its core capabilities include harvesting contacts, SMS messages, call logs, device metadata, and specifically, WhatsApp communications and media. The malware achieves this by abusing Android's accessibility services and internal file system access, exfiltrating both user-generated and received content from the app's storage directories. Command-and-control (C2) infrastructure controlled by the attackers is used to exfiltrate stolen data and receive updates, with indicators suggesting ongoing development to enhance stealth and persistence.
This operation demonstrates a tactical evolution in MuddyWater's methods, shifting from traditional spear-phishing and desktop malware toward mobile-focused espionage that aligns with broader regional trends of smartphone dependency and surveillance. The focus on WhatsApp, a widely used encrypted messaging platform, indicates an emphasis on circumventing end-to-end encryption by targeting endpoints directly rather than transmission interception.

Strategically, the campaign reflects Iran's continued emphasis on cyber-enabled intelligence collection in a geopolitically volatile region. It underscores the growing use of mobile malware by state actors to bypass encrypted communications and highlights vulnerabilities in personal device security in high-threat environments. This development fits within a broader pattern of asymmetric cyber operations aimed at undermining regional adversaries through targeted surveillance and digital intrusion.

Read more: https://therecord.media/malware-exfiltrates-whatsapp-iran-muddywater

Malware & Vulnerabilities

Crims hijacking fully patched SonicWall VPNs to deploy stealthy backdoor and rootkit

SonicWall's Secure Mobile Access (SMA) 100 series VPN appliances have become the focus of a sophisticated cyber campaign conducted by the threat actor UNC6148, which has been tracked by Google's Threat Intelligence Group and Mandiant. These appliances, including models SMA 210, 410, and 500v, are widely deployed and in many cases are end-of-life, making them attractive targets due to known vulnerabilities and legacy exposure. Despite being fully patched, several devices were compromised through a combination of previously stolen administrative credentials and one or more suspected zero-day vulnerabilities.

The attackers deployed a stealthy rootkit dubbed OVERSTEP, which manipulates the device's boot process via the /etc/ld.so.preload configuration to gain persistence. This rootkit enables credential harvesting, command execution via web logs, and hides its own activity by filtering system outputs and modifying filesystem behaviour. Simultaneously, SonicWall disclosed a critical vulnerability, CVE-2025-40599, affecting the SMA 100 series a high-severity authenticated arbitrary file upload flaw in the web management interface. While this specific vulnerability has not yet been tied to active exploitation, it could be used for remote code execution by attackers who gain administrative access.

UNC6148's exploitation strategy hinges on prior access to OTP seeds and passwords, allowing them to bypass multifactor authentication and regain control even after devices are patched. The OVERSTEP rootkit's capability to persist across reboots and operate without detection presents a particularly dangerous threat vector. The campaign highlights a broader and escalating risk associated with edge infrastructure, especially VPN appliances, which serve as gateways into sensitive enterprise environments. The strategic implications of this campaign are considerable: it demonstrates how even updated systems can be undermined through credential reuse and persistent malware, and it reinforces the urgent need for organizations to rotate credentials, perform forensic reviews, decommission vulnerable appliances, and implement zero-trust access models. This operation reflects a growing trend of advanced actors targeting VPNs and remote access devices for espionage, data theft, and long-term infiltration.

Read more: https://www.theregister.com/2025/07/16/sonicwall_vpn_hijack/

Critical Golden dMSA Attack in Windows Server 2025 Enables Cross-Domain Attacks and Persistent Access

A critical design flaw in Microsoft's Windows Server 2025 has exposed enterprise environments to a severe identity compromise technique dubbed the "Golden dMSA" attack. The vulnerability centres on delegated Managed Service Accounts (dMSAs), a feature introduced by Microsoft to enhance security over traditional service accounts by binding them to specific machines and managing their passwords through Active Directory. Security researchers from Semperis, led by Adi Malyanker, discovered that the mechanism used to generate dMSA passwords specifically the ManagedPasswordId is based on a time-derived structure that limits entropy to just 1,024 possible combinations. This allows attackers to brute-force valid password values with minimal computational effort. If an adversary gains elevated privileges on a single Domain Controller, such as SYSTEM, Domain Admin, or Enterprise Admin access, they can extract the Key Distribution Service (KDS) root

key a master secret used across the entire forest for generating service account passwords. With the KDS root key in hand, attackers can enumerate dMSA accounts via LDAP or API calls, guess the password ID, and then generate valid passwords offline.

These credentials can be used with Kerberos authentication or techniques like Pass-the-Hash and Overpass-the-Hash to assume identities and move laterally across domains. The implications are severe: the attack enables indefinite and undetectable control over all dMSA and gMSA accounts across the Active Directory Forest. Compounding the threat, the KDS root key does not expire, and no logging is enabled by default to detect its access, making early detection nearly impossible without proactive auditing. Semperis released a proof-of-concept tool named GoldenDMSA to simulate and analyse the attack in controlled settings. Strategically, this vulnerability exemplifies the growing risks associated with centralized identity infrastructures and highlights the urgent need for robust cryptographic hygiene, fine-grained access controls, and the implementation of zero-trust security principles in modern enterprise environments.

Read more: https://thehackernews.com/2025/07/critical-golden-dmsa-attack-in-windows.html

LARVA-208's New Campaign Targets Web3 Developers

The report highlights a cyber espionage and credential theft campaign by the financially oriented threat actor known as LARVA 208 (also called EncryptHub or Water Gamayun), which is now targeting Web3 developers. Traditionally focused on IT personnel via phishing calls and emails, the group has shifted to a refined operation that weaponizes social engineering through fake AI collaboration platforms. Victims are approached via recruitment style outreach through platforms such as X, Telegram, and Web3 focused job boards like Remote3 with invitations to interviews or portfolio reviews. These invitations direct developers to "Norlax AI": a typosquatting clone of the legitimate AI workspace Teampilot.ai. The fake site lends credibility with unique invitation codes and realistic interfaces.

Once logged in, victims receive a false audio error prompt, incentivizing them to download an alleged Realtek HD Audio Driver. In reality, the executable contains embedded PowerShell commands that silently retrieve the Fickle stealer from attacker controlled C2 servers hosted via FFv2 bulletproof hosting infrastructure, associated with the broader Luminous Mantis network. Fickle systematically harvests system metadata (OS version, hardware, installed software, processes), geolocation and IP data, crypto wallet credentials, development environment access, and user identity details all exfiltrated to a backend system known as SilentPrism. In parallel with this novel delivery channel, LARVA 208 has continued to deploy older techniques such as malicious .LNK shortcut files that invoke PowerShell via appended commands to download the same Fickle payload from domains like Filebin or bitacid.net.

By targeting developers in the Web3 space who often control smart contract repositories, deployment infrastructure, and cryptographic keys LARVA 208 is exploiting a decentralized workforce that lacks centralized IT protections. The combination of realistic social engineering, trusted platforms, and tailored lures enables the group to bypass conventional detection methods. Strategically, this represents a notable shift from ransomware centric monetization toward credential and data theft, achieving faster profits with lower infrastructure footprint. The campaign underscores a growing trend: threat actors pivoting to high value, niche technical targets where compromise can yield direct access to financial assets and intellectual property.

Read more: https://catalyst.prodaft.com/public/report/larva-208s-new-campaign-targets-web3-developers/overview#heading-1000

The Dark Side of Romance: SarangTrap Extortion Campaign

A sophisticated cyber campaign orchestrated by unidentified threat actors has emerged, targeting mobile users globally through a large-scale operation dubbed "SarangTrap." The campaign, identified by cybersecurity firm Zimperium, deployed over 250 malicious Android applications and more than 80 phishing domains disguised

as legitimate dating and social media platforms. Its primary targets include emotionally vulnerable individuals, particularly those using dating services, but also users of cloud storage and car service apps.

The attackers utilized convincing phishing tactics such as mimicking app store interfaces and brand logos to lure victims into downloading malware. On Android, users were prompted to enter an "invitation code," reinforcing the illusion of exclusivity and delaying malicious behaviour to evade dynamic security analyses. Once the code was verified, the app requested extensive permissions access to SMS, files, contacts, and photos under false pretenses. In the background, the malware exfiltrated sensitive data to attacker-controlled servers, compressing images using the Luban library and sending device identifiers, full contact lists, private photos, and messages. On iOS, attackers bypassed App Store restrictions by tricking users into installing malicious configuration profiles, allowing similar access to sensitive data.

The malware featured well-crafted user interfaces that masked its true intent, showing dummy content such as SMS previews and image selectors. The campaign's scope and coordination were reflected in spikes in domain registrations over time, suggesting planned rollouts and evolving evasion strategies. A notable real-world case in South Korea illustrates the campaign's psychological manipulation, where a user was emotionally exploited and extorted after installing a fake dating app. This campaign represents a shift in mobile cyber threats merging emotional and social engineering with technical stealth. It highlights the growing intersection of psychological manipulation and digital extortion, posing significant implications for user privacy and cybersecurity resilience. The operation underlines the need for advanced mobile threat defence systems capable of detecting behavioural anomalies, phishing tactics, and profile-based iOS intrusions, especially in an era of increasingly personalized and socially engineered cyberattacks.

Read more: https://zimperium.com/blog/the-dark-side-of-romance-sarangtrap-extortion-campaign

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.