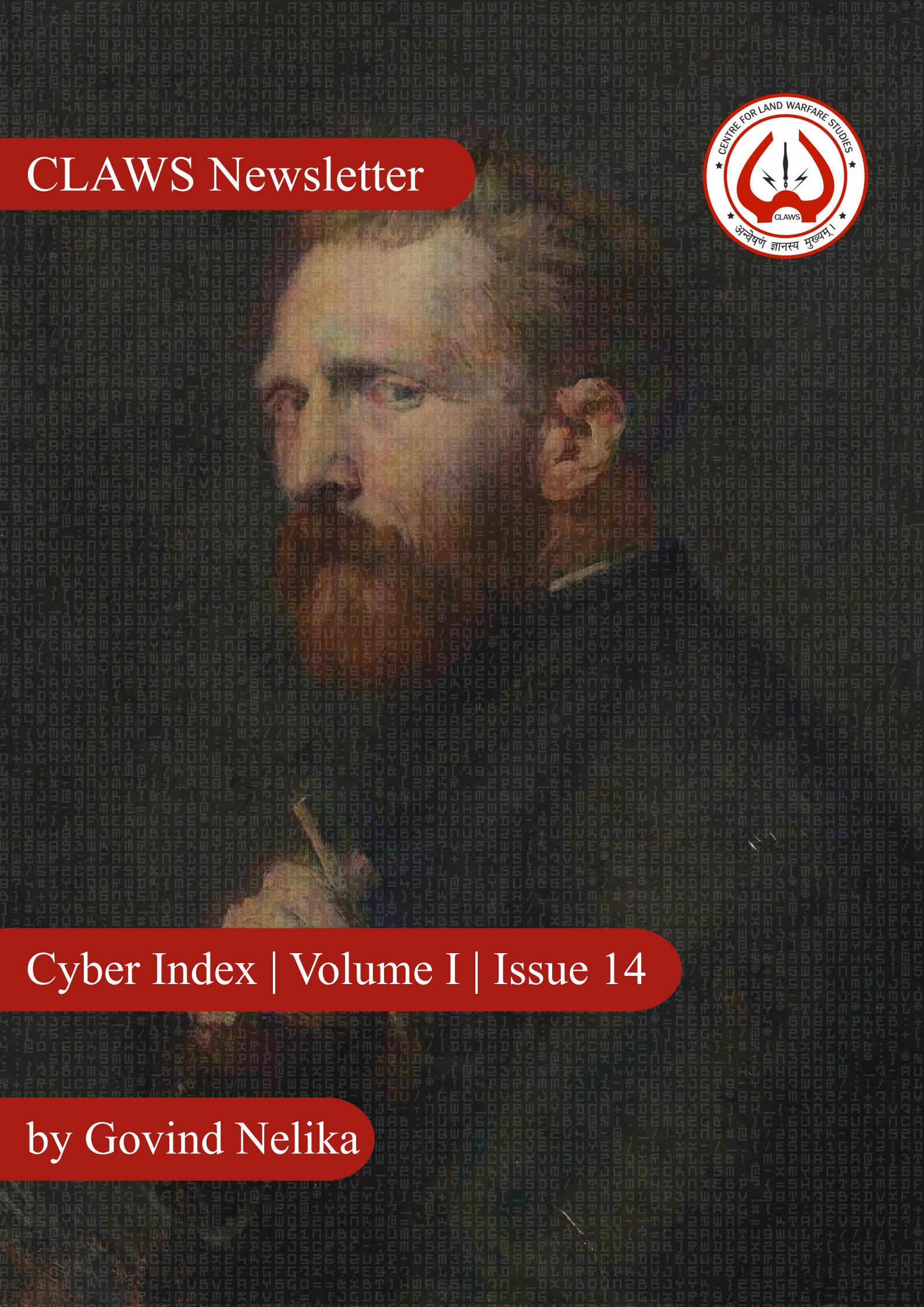
CLAWS Newsletter



Cyber Index | Volume I | Issue 14

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

Adani, Ambani quietly hunt for Chinese tech as Trump tariff war reshapes global supply chains: Report

India's largest conglomerates, including Adani Group, Reliance Industries, and JSW Group, are discreetly seeking technology transfers and partnerships with leading Chinese firms such as CATL, BYD, and Chery Automobile as global trade disruptions reshape supply chains. This pursuit comes against the backdrop of renewed U.S. tariffs under Donald Trump, which are pressuring countries that trade with Russia and driving Indian corporations to reassess sourcing strategies. For India, which urgently requires advanced expertise in electric vehicles, lithium-ion batteries, and renewable energy systems, China remains a dominant technological power despite bilateral strains following the 2020 border clash.

To navigate political sensitivities and regulatory barriers, Indian companies are reportedly using indirect channels, including subsidiaries and third countries such as Singapore and Vietnam, to engage Chinese partners. Gautam Adani has been linked to exploratory talks with CATL and BYD, though his group denies pursuing such collaborations, while JSW Group has formalized a deal with Chery Automobile to acquire EV technology and components. Reliance Industries is also evaluating opportunities in Chinese-origin battery and fuel cell technology as part of its clean energy expansion, although it has not issued public confirmation.

The targeted sectors demand sophisticated, mature, and cost-efficient technology that Indian firms currently lack, making Chinese collaboration strategically appealing. At the same time, these efforts highlight the tension between India's ambition for technological self-reliance and the risks of deepening reliance on a geopolitical rival.

Strategically, such quiet partnerships illustrate India's hedging approach: balancing U.S. trade volatility, domestic political constraints, and the need to accelerate industrial capacity. By cautiously engaging with Chinese technology while avoiding overt political entanglement, Indian conglomerates aim to strengthen regional manufacturing, reduce dependency on Western suppliers, and position India as a more independent player in global supply chains. This development underscores the broader trend of multipolarity in technology alliances amid shifting geopolitical and economic currents.

Read more: https://www.financialexpress.com/world-news/adani-reliance-quietly-hunt-for-chinese-tech-as-trump-tariff-war-reshapes-global-supply-chains-report/3950602/

China cut itself off from the global internet for an hour on Wednesday

On August 20, 2025, China's Great Firewall (GFW) unexpectedly disrupted secure internet access by blocking all traffic on TCP port 443 the standard port for HTTPS effectively severing connections to the global internet for approximately 74 minutes (from 00:34 to 01:48 Beijing Time). The blocking mechanism involved the GFW injecting forged TCP RST+ACK packets, terminating encrypted connections while leaving other ports such as 22 (SSH), 80 (HTTP), and 8443 (alternate HTTPS) unaffected.

Analysis revealed that the device responsible for the interference did not match the fingerprint of known GFW components, suggesting either deployment of a new censorship device or an existing system operating in an anomalous configuration. The asymmetrical nature of triggering was notable: packets originating from inside and outside China triggered different reset behaviors, underscoring the sophistication of the interference.

The disruption impacted a wide range of services reliant on secure external communications Apple, Tesla, and other globally connected platforms were affected, demonstrating the operational risks of opaque censorship tools. With no evident political motive or crisis coinciding with the outage, observers remain uncertain whether the blockage was a technical misconfiguration, deliberate test, or preliminary deployment.

This episode highlights the GFW's role as a complex censorship system that walks a tightrope aiming to

restrict access to foreign information while minimizing economic disruption. The anomalous port-443 blackout underlines the risks posed by unverified or evolving censorship infrastructure, reminding global stakeholders that even narrowly targeted disruptions can cause far-reaching service outages. Nations and businesses may need to factor in such volatility when designing resilient cross-border digital systems and securing communications in tightly controlled internet environments.

Read more: https://www.theregister.com/2025/08/21/china_port_443_block_outage/
https://gfw.report/publications/usenixsecurity25/en/#9

US spy chief says UK has dropped its Apple backdoor demand

The central issue involves the United Kingdom's demand that Apple provide a "backdoor" into its encrypted iCloud data, emerging under Britain's Investigatory Powers Act, also known as the "Snoopers' Charter." This would have permitted UK authorities potentially including access to data of non-UK individuals, notably American citizens to bypass Advanced Data Protection (ADP), Apple's end-to-end encryption feature. Amid mounting pushback from U.S. officials and privacy advocates, U.S. lawmakers expressed concern that such a mandate would weaken privacy, create systemic vulnerabilities, and conflict with Americans' constitutional protections. Apple had already responded by disabling ADP enrollment for UK users and challenging the directive in court.

The impasse concluded after months of high-level diplomacy. U.S. Director of National Intelligence Tulsi Gabbard, in coordination with President Trump and Vice President J.D. Vance, engaged with British officials to reverse the mandate. Their intervention resulted in the UK formally abandoning its demand for the backdoor, citing the need to protect civil liberties and digital privacy.

While privacy groups welcomed the outcome, they emphasized the underlying legal authority the Investigatory Powers Act remains intact. They continue to call for legislative reform to prevent future government-mandated encryption breaches.

Strategically, this development underscores a growing tension between national security prerogatives and digital privacy rights, especially in a globalized environment where encrypted services transcend borders. The reversal not only safeguards strong encryption and user privacy but also sets a notable precedent: governments may face significant diplomatic, legal, and political resistance when attempting to undermine these protections. The episode highlights the importance of robust encryption as a cornerstone of both individual liberties and international data governance frameworks.

Read more: https://techcrunch.com/2025/08/19/us-spy-chief-says-uk-has-dropped-its-apple-backdoor-demand/

Travel eSIMs secretly route traffic over Chinese and undisclosed networks: study

The focus is on vulnerabilities in travel eSIM services, implicated in covert data routing and privacy risks. Key entities include Northeastern University researchers (Maryam Motallebighomi, Jason Veara, Evangelos Bitsikas, and Aanjhan Ranganathan) and major eSIM providers such as Holafly, Airalo, and eSIM Access. Against the backdrop of the growing adoption of eSIMs for global roaming, this study reveals that user traffic is frequently routed through foreign, undisclosed telecom networks often in China regardless of the user's actual physical location.

In controlled testing of eSIM profiles from 25 services, researchers observed that the assigned public IP addresses did not match user locations but instead traced back to third-party networks, including China Mobile International. One example: an eSIM from Ireland-based Holafly routed traffic through China Mobile's Hong Kong network, causing devices to appear physically located in China when GPS or localization services were disabled. This opaque routing not only misrepresents user location but also opens users to jurisdictional exposure and unauthorized geo-access, as demonstrated by accessing content normally un-

available in the U.S. without a VPN.

Furthermore, the study found that establishing an eSIM reseller account was remarkably easy requiring only a valid email and payment method raising concerns about who can gain access to sensitive user data such as IMSI numbers, location accuracy within 800 meters, and SMS sending capabilities. Using specialized hardware, researchers also uncovered asynchronous, hidden communications initiated by eSIM profiles such as silent SMS retrievals and background connections to servers in Singapore and Hong Kong leveraging SIM Application Toolkit commands without user awareness.

These findings carry significant implications: users may unknowingly expose sensitive data to foreign networks, raising legal and surveillance concerns. The ease of becoming a reseller and the embedded silent communications suggest systemic privacy gaps. Strategically, this underscores the urgent need for transparency mandates, regulatory oversight, and clear accountability frameworks across the eSIM ecosystem given the increasing reliance on digital SIM technologies in global travel and connectivity.

Read more: https://www.itnews.com.au/news/travel-esims-secretly-route-traffic-over-chinese-and-undisclosed-networks-study-619659?

United States of America (USA)

DARPA Advances Context-Aware AI for Defense and Military Operations with Real-Time Mission-Critical Intelligence

The "Defence Advanced Research Projects Agency (DARPA) has launched a program focused on developing context-aware artificial intelligence systems capable of delivering critical information to users precisely when it is needed, reflecting broader U.S. efforts to integrate advanced AI into military and defence operations. The initiative, rooted in the recognition that current AI tools often overwhelm users with excessive or poorly timed outputs, aims to create "push" capabilities that automatically surface relevant intelligence in high-stakes environments without requiring direct queries. DARPA's research emphasizes adaptive models that can interpret situational context, assess mission objectives, and proactively provide actionable data whether in battlefield command centres, cyber defence monitoring, or intelligence analysis. Unlike conventional AI assistants, which primarily operate reactively, the envisioned systems would integrate multimodal data sources, including sensor feeds, communications traffic, and real-time operational updates, to prioritize information relevance and delivery timing.

The effort comes amid intensifying competition with adversaries such as China and Russia, both of which are accelerating AI adoption for military command, control, and decision support. Within this geopolitical context, DARPA's push underscores U.S. concerns that delays or overload in information delivery could disadvantage commanders in fast-evolving operational theatres, particularly in cyber and electronic warfare domains where seconds can determine outcomes. Technically, the project will test adaptive machine learning pipelines capable of filtering noise, ranking intelligence value, and presenting information through interfaces optimized for human decision-making under stress. Cybersecurity and adversarial resilience are also focal points, as the systems must withstand attempts to manipulate data feeds or exploit AI-generated outputs.Strategically, this initiative represents a step toward embedding AI deeper into U.S. defence infrastructure, with implications for joint force readiness, allied interoperability, and human-machine collaboration in future conflicts. By prioritizing timeliness and context, DARPA seeks to mitigate information paralysis and ensure decision superiority, reinforcing broader U.S. objectives to maintain technological dominance in next-generation warfare.

Read more: https://www.darpa.mil/news/2025/chatbot-push-useful-info-when-needed

Hegseth Calls for Anti-Drone Task Force

Defence Secretary Pete Hegseth has directed Army Secretary Daniel P. Driscoll to establish a Joint Interagency Task Force 401, aimed at countering the growing threat from hostile unmanned aerial systems (UAS)

commonly known as drones that are operating around U.S. borders and overseas, posing risks to war fighters, installations, and national airspace sovereignty. This decision emerges amid a broader strategic pivot toward more agile and integrated defence capabilities, reflecting escalating geopolitical tensions, particularly as drone threats have proliferated in conflicts like those in Ukraine and Nagorno-Karabakh, and even within U.S. bases abroad.

The new task force is designed to unify talent and authority from across multiple government agencies, break through bureaucratic inertia, and ensure rapid fielding of counter-UAS (C-sUAS) systems. It consolidates research, development, and procurement efforts especially those previously fragmented under the Joint Counter-small Unmanned Aircraft Systems Office and the Replicator initiative providing the task force director with direct authority to approve up to $50 million per initiative and drive streamlined hiring processes for essential technical skills such as electronic warfare, intelligence, and acquisition. Embedded within this structure is the Army's C-sUAS University at Fort Sill to facilitate training and doctrinal integration.

The move underscores a doctrinal shift: prioritizing speed over process in countering fast-moving drone threats, which have become both more sophisticated and common. Strategically, the formation of JIATF 401 signals a recognition that unmanned systems have transformed modern warfare requiring cohesive doctrine, rapid technological adaptation, and centralized execution. This development also aligns with broader Force modernization under Hegseth that emphasizes drone swarming, lethality, and rapid deployment reflecting a trend of embedding unmanned aerial technologies at the core of U.S. defence operations.

Read more: https://www.defense.gov/News/News-Stories/Article/Article/4289575/hegseth-calls-for-anti-drone-task-force/

Two in-house models in support of our mission

Microsoft has introduced two internally developed AI models MAI-Voice-1 and MAI-1-preview as part of its broader strategic effort to build greater independence in artificial intelligence. The announcement, led by Microsoft AI chief Mustafa Suleyman, comes amid an evolving dynamic with long-time partner OpenAI, and signals a deliberate pivot toward proprietary AI infrastructure and capabilities. MAI-Voice-1 is a highly resource-efficient speech generation model capable of producing one minute of expressive, multi-speaker audio in under a second on a single GPU, and it is already integrated into features like Copilot Daily and podcast-style content via Copilot Labs. MAI-1-preview, a text-based, instruction-following large language model trained end-to-end on approximately 15,000 Nvidia H100 GPUs, is currently undergoing public testing on the AI benchmarking platform LMArena with planned integration into Copilot text capabilities over the coming weeks.

These developments reflect Microsoft's pursuit of cost-effective AI innovation, leveraging its own data sources and efficiency optimizations to "punch above its weight class," reducing reliance on OpenAI's models, which are noted to be slower and more expensive at scale. The move can be interpreted as part of a larger strategic shift toward autonomy in AI one that aligns with growing tensions in the Microsoft-OpenAI relationship and echoes industry-wide pressures over compute costs and infrastructure control. By cultivating its own models tailored to consumer-facing use cases, Microsoft aims to orchestrate a portfolio of specialized AI tools optimized for diverse user intents, laying the groundwork for long-term competitiveness in both user experience and operational independence.

Read more: https://microsoft.ai/news/two-new-in-house-models/#

Developing nuclear safeguards for AI through public-private partnership

The headline development involves Anthropic, the AI company behind the Claude chatbot, in partnership with the U.S. Department of Energy's National Nuclear Security Administration (NNSA) and DOE national laboratories. Together, they have jointly developed and deployed a specialized AI classifier designed to distinguish

between benign and potentially dangerous nuclear-related inquiries, achieving approximately 96% accuracy in preliminary testing striking a balance between facilitating legitimate scientific dialogue and preventing misuse for nuclear weapons purposes.

The effort emerged from over a year of collaboration and red-teaming, during which NNSA provided curated indicators of nuclear proliferation risk. Anthropic used these to train a real-time content classifier embedded within Claude's safeguards framework. The testing phase relied on hundreds of synthetic prompts rather than user data, ensuring user privacy while enabling thorough validation. The classifier maintained a high detection rate (94.8% of harmful prompts flagged correctly) with negligible false positives.

Currently deployed within Claude's traffic monitoring system, early results affirm its effectiveness in practical conversations. Notably, when certain news-driven discussions about nuclear events were flagged, a hierarchical summarization system contextualized them properly, preventing misclassification. Going forward, Anthropic plans to share its methodology via the Frontier Model Forum a coalition of leading AI developers enabling broader industry adoption.

Strategically, this effort underscores the emergence of public-private partnerships as vital to AI safety, especially regarding dual-use content areas like nuclear science. By integrating government domain expertise with AI engineering, Anthropic has established a precedent for securing advanced AI systems against misuse. This approach not only enhances national security but also offers a replicable framework for other developers navigating the ethical and legal complexities of AI deployment in sensitive domains.

Read more: https://red.anthropic.com/2025/nuclear-safeguards/

People's Republic of China (PRC) | China

China's Brain-Computer Interface Industry – Tapping into the Future of Human-Machine Integration

China's brain-computer interface (BCI) industry is rapidly advancing, guided by coordinated action from national government agencies including the Ministry of Industry and Information Technology, the National Development and Reform Commission, the National Health Commission, and the Chinese Academy of Sciences which jointly issued policy guidelines aiming for technological breakthroughs by 2027 and the creation of a globally competitive BCI ecosystem by 2030. This strategic push is supported by ambitious regional plans from Beijing and Shanghai's development blueprints to Sichuan's provincial targets of 3,000 invasive BCI surgeries annually and deployment of rehabilitation devices to more than 100,000 patients by 2030.

Leading Chinese firms span both invasive and non-invasive BCI technologies. Notable players such as NeuroXess (Shanghai), NeuraMatrix (Beijing), BrainUp, BrainCo, Neuracle, Yunrui Intelligence, ZhenTai Intelligence, Flexolink, Jieti Medical, and ECon are developing technologies from EEG-based wearables to implantable electrodes for rehabilitation, sleep monitoring, neural modulation, and motor control. In clinical milestones, Shanghai's NeuroXess achieved real-time Chinese speech decoding with an invasive BCI implant displaying 71 percent accuracy five days post-surgery, while Beijing's NeuCyber NeuroTech (in partnership with the Chinese Institute for Brain Research) implanted its Beinao-1 chip in patients enabling cursor control and robotic arm operation with plans to expand to 13 implants this year and 50 in 2026 and is developing a wireless Beinao-2 implant for human trials within 12–18 months.

Market dynamics reinforce the strategic vision. The global BCI market, valued at approximately US $2 billion in 2023, is forecast to exceed US $6 billion by 2028 and China's BCI market alone is projected to surpass RMB 120 billion (nearly US $16 billion) by 2040. The policy regime also promotes non-invasive consumer applications wearables like headbands, earpieces, smart glasses for health, safety, and productivity use cases, including driver alertness monitoring and workplace safety.

Technically, efforts are focused on enhancing signal-decoding chips, improving accuracy and responsiveness

of implantable and non-implantable devices, standardizing BCI technology, and building mass-manufacturing capabilities and high-performance surgical robotics. The overall pattern reflects a shift from exploratory research to full implementation, with China leveraging its strength in translating research into commercial products.

Strategically, China's coordinated push in BCI underscores a commitment to leadership in a transformative technology field, with profound implications for healthcare innovation, human-machine integration, and economic competitiveness. If successful, the initiative could yield medical breakthroughs for paralysis and brain disorders, expand consumer and industrial use cases, and heighten geopolitical and industrial competition with Western counterparts like Neuralink. The policy-driven commercialization also raises important considerations around safety, ethics, data privacy, and regulatory oversight as China accelerates toward a future of integrated neurotechnology.

Read more: https://www.china-briefing.com/news/chinas-brain-computer-interface-industry-tapping-into-the-future-of-human-machine-integration/

Huawei reveals Kirin chip inside 5G smartphones as firm overcomes US sanctions

Huawei Technologies and its semiconductor design unit, HiSilicon, have officially disclosed that their latest flagship smartphones the Mate 70 and Pura 80 series are powered by the Kirin 9020 system-on-chip (SoC), marking the first explicit processor reveal in nearly five years amid heavy U.S. sanctions. Designed domestically and manufactured by Semiconductor Manufacturing International Corporation (SMIC) using a 7 nm-class process, the Kirin 9020 integrates Huawei's Balong 6000 5G modem and supports advanced 5G front-end modules (FEMs), overcoming dependencies on U.S. RF component suppliers.

This chip features a multi-tier CPU architecture high-performance cores up to 2.50 GHz, mid-tier cores up to 2.15 GHz, and efficiency cores up to 1.60 GHz paired with an Arm-based Maleoon 920 GPU. Its integration of the 5G modem and RF components into a single SoC demonstrates deep engineering proficiency, especially given the complexities of wide-spectrum support, beamforming, and low-latency communication required for 5G performance.

The strategic significance of the Kirin 9020 lies not in revolutionary redesign analysts describe it as an incremental evolution over its predecessor, the Kirin 9010 but in its symbolic value. It underscores Huawei's and China's drive toward technological self-reliance in chip design and manufacturing, particularly under the constraints of U.S. export controls that limit access to advanced lithography tools and RF technologies.

This move enhances Huawei's competitive standing in 5G-enabled smartphones and signals progress in domestic semiconductor capabilities, with implications for global tech supply chains and geopolitics. The Kirin 9020 reflects a broader shift: Chinese firms are increasingly capable of building complex, high-performance chips indigenously, potentially reshaping competition and resilience in the semiconductor industry amid geopolitical tensions.

Read more: https://www.scmp.com/tech/big-tech/article/3322397/tech-war-huawei-reveals-kirin-chip-inside-5g-smartphones-firm-overcomes-us-sanctions?

Chinese EDA leader Empyrean announces breakthroughs in chip design software

China's leading EDA (electronic design automation) developer, Empyrean Technology, backed by state investment, has unveiled significant innovations in chip design tools amid mounting U.S.–China tech tensions. In the first half of 2025, Empyrean launched AI-enhanced capabilities for memory chip and panel display design. Its layout editor now includes a "clone group" function that automates the positioning of identical memory modules, while the AI-driven simulation tool improves yield prediction with fewer test iterations. Concurrently, the firm deployed a large-scale, AI-automated platform to design pixel layouts for panel dis-

plays a move that replaces traditional manual workflows. Beyond these, Empyrean rolled out six additional tools serving digital, analog, and 3D-integrated circuit design.

These advances come against the backdrop of intensifying export restrictions on Western EDA technologies. As U.S. firms like Synopsys and Cadence face hurdles in the Chinese market due to tightened controls, Empyrean is stepping into a crucial strategic gap. The new toolsets support key stages of memory chip development from layout editing to simulation augmenting China's ambitions for semiconductor self-reliance.
Strategically, Empyrean's breakthroughs signal a shift toward domestic mastery of critical semiconductor tools traditionally dominated by U.S. and European providers. These technologies, once considered chokepoints, are now being localized, underscoring China's commitment to mitigating vulnerabilities amid geopolitical pressures. The firm's expanded offerings not only help underpin national chipmaking ambitions but also lay the groundwork for broader EDA ecosystem development and resilience against external supply chain disruptions.

Read more: https://www.scmp.com/tech/article/3322366/tech-war-chinese-eda-leader-empyrean-announces-breakthroughs-chip-design-software

Republic of China (ROC) | Taiwan

TAOTH Campaign Exploits End-of-Support Software to Target Traditional Chinese Users and Dissidents

The TAOTH campaign, identified by Trend Micro, involves a sophisticated cyber espionage operation targeting high-value individuals such as dissidents, journalists, researchers, and business or technology leaders within Eastern Asia, including Taiwan, Hong Kong, Japan, and overseas Taiwanese communities. The adversary employed a dual-pronged approach combining exploitation of an end-of-support software supply chain and targeted spear-phishing. In October 2024, attackers seized control of the lapsed update domain for Sogou Zhuyin, an IME discontinued in mid-2019. By embedding malicious updates into the installer and manipulating trusted distribution channels including modifying Wikipedia links to redirect users they deployed several malware families: TOSHIS, C6DOOR, DESFY, and GTELAM. These strains delivered diverse functionalities including remote access, backdoor deployment, information theft, and reconnaissance, while cleverly abusing legitimate services such as Google Drive and cloud storage to hide network traffic and exfiltrate data.

The infection chain typically begins when users download the ostensibly benign installer and then receive malicious updates through a compromised updater (ZhuyinUp.exe), which fetches payload configurations from remote servers. Payloads like TOSHIS act as loaders modifying legitimate binaries, injecting shellcode, and fetching next-stage agents such as Cobalt Strike or Merlin. DESFY and GTELAM contribute espionage capabilities and data extraction, sometimes disguised through cloud-based exfiltration. Detailed telemetry shows consistent infrastructure, shared malware variants, and overlapping tactics indicative of a persistent actor with recon and espionage goals.

This campaign signals a broader trend: adversaries increasingly exploit software supply chains and abandoned infrastructure when defending high-value digital assets. The blend of trusted distribution channels, stealthy malware, and selective targeting places significant pressure on defenders. Strategically, TAOTH underscores the necessity for proactive removal of outdated software, rigorous validation of update sources, and multimodal detection capabilities to counter evolving hybrid cyber-espionage threats aligned with geopolitical fault lines.

Read more: https://www.trendmicro.com/en_us/research/25/h/taoth-campaign.html

Taiwan traces Chinese hackers selling stolen data to trafficking ring

Taiwan's Investigation Bureau has traced a Chinese hacker group known as CrazyHunter to a network sell-

ing stolen personal data to human trafficking rings spanning Taiwan and mainland China. Between February and March 2025, CrazyHunter carried out ransomware attacks targeting hospitals, publicly traded firms, and academic institutions including MacKay Memorial Hospital, Changhua Christian Hospital, and Keding Enterprises demanding ransom and exfiltrating sensitive data.

Prosecutors have identified two Chinese nationals, surnamed Luo and Xu, as core members of the hacker group, and uncovered their collaboration with a trafficking syndicate that includes a Chinese individual, Zhao, and two Taiwanese collaborators, surnamed Liu and Cheng. From May through August, authorities conducted raids resulting in the arrests of Liu and Cheng, who were found to be actively trading thousands of illegally obtained records from both domestic and international cybercriminals. Seized evidence included cryptocurrency payments and electronic transaction records linking them to CrazyHunter's operations.

Liu and Cheng now face charges of computer misuse, extortion, and breaches of the Personal Data Protection Act, though both were released on NT$30,000 (approximately US$938) bail and have been restricted from traveling abroad. The involvement of Luo, Xu, and Zhao remains under active investigation, suggesting an ongoing probe into a broader cross-border criminal ecosystem. Strategically, this case illustrates how cybercrime, personal data abuse, and human trafficking have converged in Taiwan's evolving threat landscape. The attacks on healthcare and educational institutions underscore vulnerabilities in critical infrastructure, while the interconnection with transnational trafficking syndicates raises profound national security and human rights concerns. These developments highlight the imperative for law enforcement to bolster digital forensics, tighten protections around personal data, and strengthen international cooperation in combating hybrid cybercrime.

Read more: https://focustaiwan.tw/society/202508280006

Foxconn and SoftBank to make data centre equipment in Ohio for Stargate project

The focal point is a strategic collaboration between Taiwan's Foxconn and Japan's SoftBank, centred on their joint operation of Foxconn's former electric vehicle manufacturing site in Lordstown, Ohio. SoftBank acquired the expansive 6.2-million square-foot facility including its machinery in a $375 million transaction. The two companies will form a joint venture under which Foxconn will operate the site while SoftBank supplies the venue and manufacturing equipment. This initiative is an integral component of the Stargate project a massive public-private venture spearheaded by SoftBank, OpenAI, and Oracle, unveiled by President Trump in January, aimed at building AI infrastructure across the U.S. with a potential investment of up to $500 billion. The Ohio plant will serve as the first dedicated manufacturing hub linked directly to Stargate, enabling production of AI servers and data-centre hardware to supply the broader infrastructure buildout. The choice of this location reflects its strategic advantages in power capacity, infrastructural readiness, and ability to meet the project's tight timeline. This move occurs within Foxconn's broader shift from smartphone assembly toward AI server production its AI server business has outpaced consumer electronics revenue, and the firm is expanding its U.S. footprint in places like Texas and Wisconsin. Nevertheless, the Stargate initiative has faced delays and financing uncertainties, with initial momentum slower than anticipated due to tariff challenges and extended negotiations, though SoftBank emphasizes its continued commitment to the investment goals. Strategically, the deployment of this U.S. manufacturing base underscores accelerating globalization of AI infrastructure and aligns with broader national security and economic priorities of boosting domestic production while reducing dependency on foreign tech supply chains.

Read more: https://www.reuters.com/business/media-telecom/foxconn-softbank-make-data-centre-equipment-ohio-stargate-project-2025-08-18/?

The Democratic People's Republic of Korea

Unmasking the DPRK-linked GitHub C2 Espionage Campaign

The focus is a sophisticated espionage campaign attributed to North Korean (DPRK) actors, specifically tied

to the Kimsuky group, targeting diplomatic missions across Europe via their Seoul postings. The Trellix Advanced Research Center identified at least 19 spear-phishing attacks between March and July 2025, leveraging highly personalized lures from faux meeting invites and official letters to event correspondence to trick embassy staff into engaging with malicious content.

Attackers used cloud platforms such as Dropbox, Daum, and GitHub to orchestrate their operation. Initial infection was triggered through spear-phishing emails containing password-protected ZIP attachments that delivered a disguised Windows shortcut (.lnk) triggering a PowerShell script. Once executed, this script retrieved a XenoRAT remote access trojan a MoonPeak-associated variant via links hosted on GitHub's raw content or Dropbox.

Notably, GitHub served as the campaign's command-and-control (C2) infrastructure: infected systems pulled operational instructions and RAT payload locations from files like onf.txt in the private repository, while stolen reconnaissance data was exfiltrated back to the attackers by uploading to GitHub using the platform's API. Files were tagged with timestamped IP-based filenames and removed from local storage post-upload.

The malware never touched the disk; instead, the payload was loaded directly into memory via .NET reflection techniques, enabling stealthy persistence and comprehensive remote control capabilities such as keystroke logging, screenshot capture, file transfers, and remote shells.

This campaign exemplifies how modern state-aligned threat actors exploit trusted cloud and code platforms to evade detection, complicate attribution, and conduct long-term espionage. Leveraging GitHub for both data exfiltration and C2 operations masks malicious communications in seemingly benign traffic. The operation underscores pressing national-security concerns and highlights the evolving need for defenders to monitor even legitimate platforms for abuse, reevaluate trust models, and adapt to increasingly stealthy, hybridized cyber threats.

Read more: https://www.trellix.com/blogs/research/dprk-linked-github-c2-espionage-campaign/

Russian Federation

Kremlin-Backed Messaging App Max to Come Pre-Installed on Devices Starting Next Month

Russia has mandated that beginning September 1, 2025, all smartphones and tablets sold in the country must come pre-installed with Max, a Kremlin-backed messaging app developed by VK Corporation. In parallel, Apple devices will be required to carry the state-run app store RuStore, while from January 2026 smart TVs will need to include LIME HD TV. These measures reflect Moscow's drive for digital sovereignty and reduced reliance on Western platforms amid escalating tensions with the United States and Europe over Ukraine and broader geopolitical disputes.

The decision follows recent restrictions on foreign platforms such as WhatsApp and Telegram, including blocked voice and video calls and accusations that they fail to cooperate with Russian authorities. By contrast, Max has already surpassed 18 million downloads and is being promoted as a more secure alternative that demands fewer device permissions than its Western counterparts. However, critics argue that its deep integration with government services could transform it into a surveillance tool, enabling state monitoring of private communications under the guise of national security.

The strategic implications extend beyond consumer choice. This policy underscores Russia's consolidation of a state-controlled digital ecosystem, where communications, app distribution, and media streaming are tightly regulated by the government. It also highlights a global trend in which major powers are weaponizing technology policy to achieve political and security goals, fragmenting the internet into rival spheres of influence. For Russia, pre-installing Max cements state control over the digital domain, but it also raises serious concerns for privacy, civil liberties, and the security of cross-border communications.

Read more: https://www.themoscowtimes.com/2025/08/21/kremlin-backed-messaging-app-max-to-come-pre-installed-on-devices-starting-next-month-a90306

West Asia

Iranians struggle with GPS disruption after Israel war

Iran is experiencing widespread GPS disruptions in the aftermath of Israel's June military strike and the short but intense 12-day war. The Iranian Communications Ministry has attributed the interference to security and military needs, but its impact on daily life has been severe. Ride-hailing services such as Snapp and navigation apps like Neshan have been heavily affected, with drivers reporting they often appear hundreds of kilometres from their actual location. Neshan's CEO confirmed a sharp decline in user activity, while ordinary residents have struggled with navigation, transport delays, and lost income.

The disruptions fit into Iran's established practice of GPS jamming and spoofing near sensitive sites, aimed at complicating foreign targeting of missiles, drones, and rockets. However, this instance is broader and more sustained, affecting entire cities rather than localized military zones. Former Communications Minister Mohammad Javad Azari Jahromi has criticized the approach, noting that adversaries could easily switch to alternative positioning systems, rendering the interference strategically limited while imposing heavy costs on civilians.

Officials have floated the possibility of adopting China's BeiDou navigation system to bypass U.S.-controlled GPS. Deputy Minister Ehsan Chitsaz acknowledged that such a transition would be expensive and technically complex, while experts warned of increased cyber vulnerabilities during implementation. Meanwhile, the economic fallout from navigation failures compounds Iran's existing financial difficulties under sanctions, and the disruptions raise safety concerns, including for emergency response.

The incident reflects a wider trend in modern conflict, where electronic warfare extends beyond battlefields to disrupt civilian infrastructure. Similar interference has been linked to shipping and aviation incidents in the region, underscoring the risks of overreliance on vulnerable satellite systems. For Iran, the crisis highlights the costs of prioritizing military electronic warfare tactics over civilian stability, while also pointing toward deeper alignment with China in strategic technologies.

Read more: https://www.al-monitor.com/originals/2025/08/iranians-struggle-gps-disruption-after-israel-war

Malware & Vulnerabilities

WhatsApp Issues Emergency Update for Zero-Click Exploit Targeting iOS and macOS Devices

Meta-owned messaging platform WhatsApp has rapidly addressed a critical zero-click vulnerability (CVE-2025-55177) affecting its iOS, WhatsApp Business for iOS, and macOS clients impacting versions prior to iOS 2.25.21.73, WhatsApp Business for iOS 2.25.21.78, and macOS 2.25.21.78. The flaw stems from insufficient authorization in linked-device synchronization messaging, allowing an unrelated actor to force the app to process content from a malicious URL on the target's device.

This weakness may have been combined with a recently disclosed Apple ImageIO framework exploit (CVE-2025-43300) affecting iOS, iPadOS, and macOS, as part of a sophisticated zero-click attack chain targeting specific individuals. WhatsApp's internal security team reclassified and remediated the issue, prompting the release of emergency patches for the affected versions. Notifications were sent to a number of potentially targeted individuals, with recommendations including full factory resets and immediate updates to both the app and operating systems to mitigate lingering threats. Donncha Ó Cearbhaill, head of Amnesty International's Security Lab, indicated that vulnerable users particularly in civil society are likely among those impacted.

The exploit's zero-interaction nature highlights the heightened risk posed by invisible threats that require no user input, now validated against high-value platforms like WhatsApp. Strategically, this incident underscores the challenges of securing widely used communication tools amid advanced spyware campaigns, especially where OS-level and app-level vulnerabilities converge. It emphasizes the urgent necessity for platforms to swiftly enforce patch distribution and for users to remain vigilant particularly in sectors such as journalism, human rights, and advocacy where such silent exploits can have profound privacy and national security consequences.

Read more: https://thehackernews.com/2025/08/whatsapp-issues-emergency-update-for.html?

MURKY PANDA: A Trusted-Relationship Threat in the Cloud

A newly identified cyber-espionage campaign attributed to the China-linked threat actor Murky Panda highlights the growing risks posed by advanced persistent threats exploiting trusted relationships in cloud environments. Murky Panda, previously tied to Chinese state-sponsored intelligence-gathering operations, is leveraging sophisticated techniques to infiltrate organizations through their cloud service providers and supply chain partners rather than direct compromise. The campaign involves exploiting cloud trust relationships such as misconfigured identity federation, shared tokens, and over-permissioned service accounts to laterally move across networks and access sensitive data. Once inside, the group employs custom malware loaders, living-off-the-land techniques, and credential theft to establish persistence while evading detection.

The campaign has primarily targeted organizations in technology, defence, and government sectors across North America and Asia, aligning with China's strategic interest in acquiring intellectual property and geopolitical intelligence. Technical analysis indicates that Murky Panda relies on compromised administrator accounts, abuse of OAuth tokens, and cloud-native command-and-control (C2) channels that blend into legitimate traffic. These methods allow the actors to bypass traditional perimeter defenses and security tools, particularly in hybrid and multi-cloud environments where monitoring is fragmented. The operation demonstrates a deliberate shift toward exploiting systemic cloud trust dependencies, making attribution and containment more challenging for defenders.

Strategically, the activity underscores the vulnerability of modern enterprises to indirect compromises via third-party and cloud service providers, echoing broader concerns about supply chain security. For China, such operations reinforce its long-standing cyber-enabled espionage objectives, while for targeted nations they highlight the limitations of current cloud security frameworks. The incident reflects a broader trend in which state-backed actors increasingly exploit cloud ecosystems, identity infrastructure, and managed service providers to gain long-term strategic access. The implications extend to national security, corporate resilience, and international cyber norms, with cloud trust exploitation emerging as a frontline battleground in state-driven cyber conflict.

Read more: https://www.crowdstrike.com/en-us/blog/murky-panda-trusted-relationship-threat-in-cloud/

ERMAC V3.0 Banking Trojan Full Source Code Leak

The central focus is the leak of ERMAC 3.0, a sophisticated Android banking trojan operating as a Malware-as-a-Service (MaaS) platform. Key actors include its developers likely linked to a threat actor known as DukeEugene, associated with BlackRock trojan and cybersecurity researchers at Hunt.io, who uncovered the full source code. This disclosure occurred in March 2024, when an open directory containing an archive named Ermac 3.0.zip was discovered, exposing the entire malware infrastructure to public scrutiny.

Contextually, ERMAC builds on earlier leaked banking malware frameworks initially derived from Cerberus and later ERMAC 2.0 from portions of the Hook botnet evolving into this expanded third version. Version 3.0 introduces vastly improved capabilities, including advanced form injection techniques and the ability to target

more than 700 applications, encompassing banking, shopping, and cryptocurrency platforms. It also supports commands like SMS sending, call forwarding, push notifications, Gmail subject extraction, front-camera snapshots, overlay launches, contact and app enumeration a breadth indicating deep infiltration capabilities.

The leak revealed the full malware stack: a PHP/Laravel-based backend C2 server, a React-based operator panel (frontend), a Golang exfiltration server, Docker deployment configuration, and an Android builder for generating obfuscated APKs. The infrastructure suffers from serious vulnerabilities: a hardcoded JWT secret, static administrator bearer token, default "changemeplease" root credentials, and open API registration, any of which can be exploited to hijack or disrupt operations.

Strategically, this leak provides defenders and law enforcement with an unprecedented blueprint to map active C2 and exfiltration infrastructure, erode trust in the MaaS model, and deploy effective mitigation or takedown strategies. More broadly, the incident signals how even highly complex criminal frameworks can be undermined by basic operational security failures, underscoring an ongoing trend: as mobile malware grows in sophistication, its structural fragility creates openings for defenders to penetrate and counteract these threats.

Read more: https://hunt.io/blog/ermac-v3-banking-trojan-source-code-leak

RingReaper Linux Malware: EDR Evasion Tactics and Technical Analysis

The emergence of RingReaper, a newly identified Linux-based malware strain, highlights the growing sophistication of threats aimed at bypassing enterprise detection systems and targeting critical infrastructure. Security researchers have linked the malware to campaigns against organizations operating in telecommunications, cloud services, and government networks, where Linux servers often form the backbone of operational and security environments. The malware distinguishes itself through its advanced endpoint detection and response (EDR) evasion techniques, which enable persistent compromise while remaining hidden from traditional defences. RingReaper uses process injection, obfuscation, and in-memory execution to avoid leaving detectable artifacts on disk. It also disables monitoring agents and leverages living-off-the-land binaries (LOLBins) trusted system utilities repurposed for malicious use making detection far more difficult. In addition, the malware employs modular components, granting attackers flexible capabilities such as credential harvesting, data exfiltration, command execution, and lateral movement across Linux environments.

A particularly notable feature is RingReaper's use of kernel-level manipulation to interfere with security monitoring tools, effectively blinding EDR solutions and reducing forensic visibility. Its ability to dynamically adjust its evasion strategy based on the presence of specific security controls suggests that it was engineered by a highly capable threat actor with deep understanding of defensive technologies. Given its architecture, the malware could serve both espionage and disruptive purposes, allowing adversaries not only to collect sensitive data but also to potentially destabilize mission-critical systems that rely on Linux infrastructure.

Strategically, RingReaper underscores the increasing targeting of Linux systems, which are prevalent in cloud platforms, high-performance computing, and enterprise servers but historically under protected compared to Windows environments. The campaign reflects broader trends in cyber warfare where state-backed and advanced criminal groups exploit systemic blind spots to undermine national security and economic stability. Its development signals a shift toward stealthier, more resilient malware ecosystems that exploit trust in essential digital infrastructure, raising the urgency for defenders to harden Linux defences and adapt detection strategies against next-generation evasion tactics.

Read more: https://www.picussecurity.com/resource/blog/ringreaper-linux-malware-edr-evasion-tactics-and-technical-analysis

ZipLine Campaign: A Sophisticated Phishing Attack Targeting US Companies

The ZipLine phishing campaign, uncovered by Check Point Research, represents a highly sophisticated and

resource-intensive social-engineering operation targeting critical industries including manufacturing, hardware, semiconductors, biotechnology, and pharmaceuticals. These sectors sit at the center of U.S. and global supply chains, making them prime targets for espionage, intellectual property theft, and disruption. Unlike traditional phishing attempts that rely on mass unsolicited emails, ZipLine exploits corporate trust by initiating contact through a company's public "Contact Us" web form, prompting the victim to begin the email exchange. This inversion of the usual phishing dynamic allows attackers to bypass spam filters and appear as legitimate business inquiries.

The adversaries then sustain extended, business-style email conversations lasting up to two weeks, often requesting NDAs or invoking plausible pretexts such as artificial intelligence assessments to build credibility. To reinforce this illusion, they register or repurpose U.S.-based LLC domains, sometimes recycling abandoned domains with established reputations, and deploy cloned websites with uniform templates and even stock images. Once trust is established, attackers deliver malicious ZIP archives, frequently hosted on legitimate platforms like Heroku, containing decoy PDFs or DOCX files alongside a hidden LNK shortcut. Activating the shortcut launches a PowerShell loader that executes malicious scripts entirely in memory, culminating in the deployment of MixShell, a stealthy in-memory implant.

MixShell employs DNS TXT record tunnelling for command-and-control with HTTP fallback, granting attackers remote command execution, file manipulation, reverse proxying, and covert sessions while evading traditional detection. The campaign has already impacted dozens of organizations in the United States, with additional victims in Singapore, Japan, and Switzerland, spanning small businesses to large enterprises.

Strategically, ZipLine reflects an evolution in phishing: a shift from high-volume, fear-driven tactics to patient, trust-centric exploitation that erodes the reliability of digital communication. Its focus on supply chain-linked industries underscores severe risks to intellectual property, operational continuity, and national security, highlighting the urgent need for organizations to harden verification processes, strengthen employee vigilance, and deploy defences capable of detecting context-aware, slow-moving cyber threats.

Read more: https://research.checkpoint.com/2025/zipline-phishing-campaign/

Grok chats show up in Google searches

The exposure of private conversations from Grok, an AI chatbot developed by Elon Musk's company xAI and integrated with the social platform X, has triggered serious concerns about privacy and security in generative AI systems. The issue came to light when search engines such as Google, Bing, and DuckDuckGo indexed Grok's shared chat transcripts, making them accessible to anyone online. More than 370,000 conversations were discovered to be searchable, a scale that magnified the potential risks of the exposure.

This incident reflects a recurring pattern across AI platforms where convenience features inadvertently create vulnerabilities. Grok's "Share" button, intended to let users distribute interesting chatbot outputs, automatically generated public URLs for conversations. Because these pages were not restricted or protected from web crawlers, they were indexed by search engines. Many users likely assumed their shared chats remained private or semi-private, unaware they were being published openly. Similar exposures had already occurred earlier in 2025 with OpenAI's ChatGPT and Meta AI, underscoring systemic weaknesses in AI product design.

The indexed transcripts contained a wide spectrum of sensitive material. Some conversations included deeply personal content such as medical inquiries, mental health struggles, and even a password. Others contained alarming and dangerous information, ranging from instructions on making drugs, bombs, or malware to methods of self-harm. Particularly concerning was the discovery of a transcript describing a detailed plan to assassinate Elon Musk himself. While usernames were sometimes obscured, the conversational context often revealed identifying details, further heightening the risks.

The implications extend far beyond Grok alone. By exposing private data at scale, this failure undermines

public trust in AI platforms and invites greater scrutiny from regulators and policymakers. Strategically, the incident demonstrates how quickly AI tools can become vectors for sensitive data leakage when privacy protections are poorly implemented. It reinforces the need for stronger default safeguards, transparent communication about risks, and strict adherence to privacy-by-design principles to prevent generative AI systems from amplifying security, legal, and societal threats.

Read more: https://www.malwarebytes.com/blog/news/2025/08/grok-chats-show-up-in-google-searches

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.