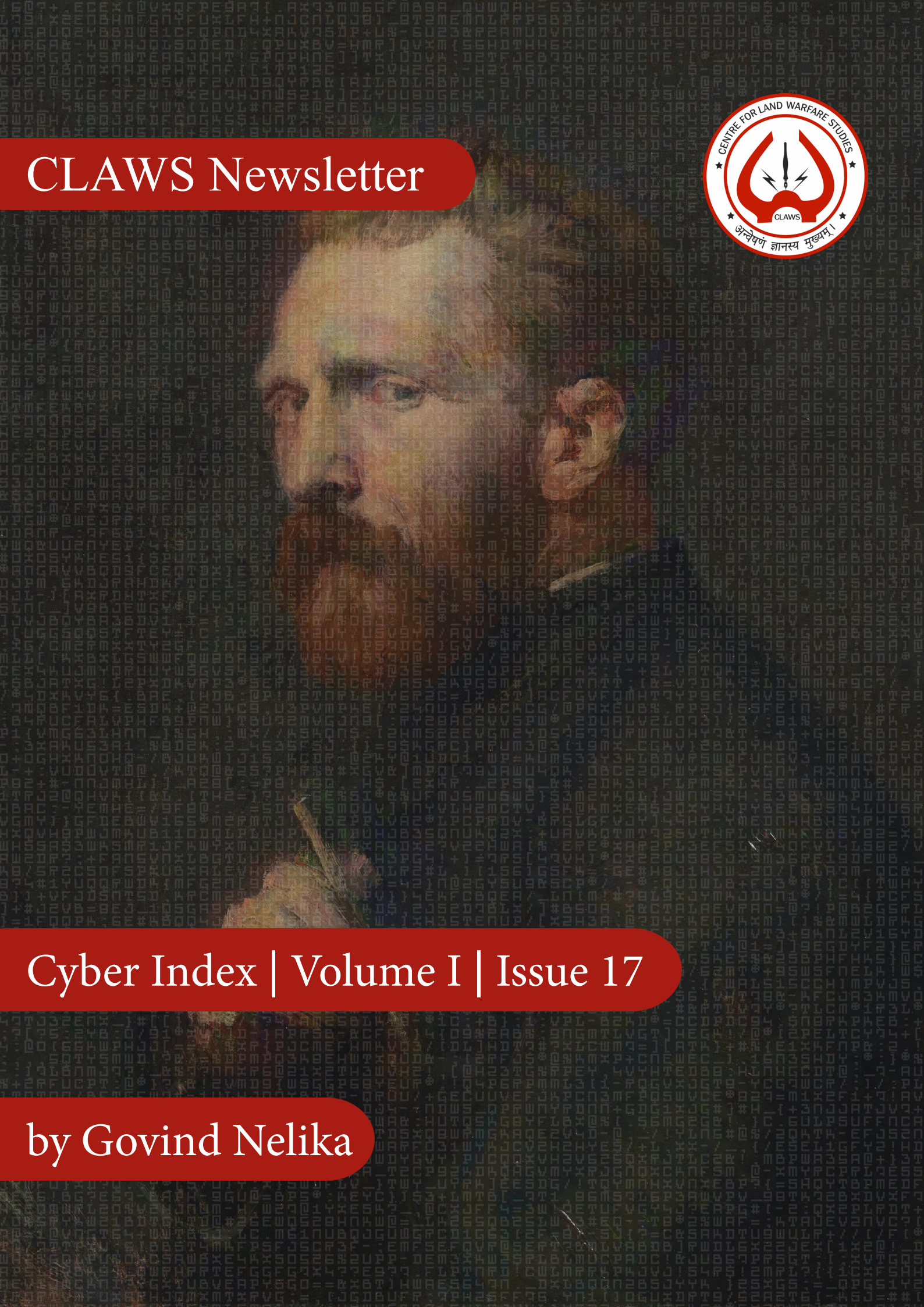
# CLAWS Newsletter



## Cyber Index | Volume I | Issue 17

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 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

**The Cybersecurity Information Sharing Act Expires, will it continue or be scrapped**

The main issue is the impending expiration of the Cybersecurity Information Sharing Act of 2015 (CISA 2015) in the U.S., with key actors including private sector firms, federal agencies (especially the Department of Homeland Security), lawmakers, and industry groups. CISA was introduced to create a legal framework and protections that encourage voluntary sharing of cyber threat indicators, monitoring, and defensive measures between private entities and the government. Its genesis followed high-profile cyber incidents and recognition that coordinated threat intelligence sharing is critical for defending national infrastructure.

The law provides several specific safeguards: it shields participating companies from liability under statutes like the Wiretap Act or ECPA when they monitor systems for threats; exempts threat data shared with DHS from Freedom of Information Act disclosure; grants antitrust safe harbours for sharing cyber-defence information; and ensures that privilege is not waived by sharing threat indicators with the government.

As of September 30, 2025, CISA 2015 is set to expire unless Congress acts to renew or amend it. Without renewal, the liability, antitrust, FOIA, privilege, and "notwithstanding" monitoring protections will no longer apply to new information sharing and monitoring activities conducted under its authority. This creates uncertainty for private and public actors, who risk legal exposure when sharing threat data or deploying defensive measures. Industry and legal experts caution that the lapse could chill cooperation, slow response to cyber threats, and weaken coordination especially over state-sponsored attacks.

Strategically, the expiration of CISA 2015 comes at a time of intensifying cyber threats and underscores how legal infrastructure underpins national cybersecurity. Without statutory protections, the U.S. risks less effective threat detection and response, and may see more fragmentation in cyber defense across jurisdictions and sectors. The push for reauthorization or reform reflects broader trends in ensuring legal regimes evolve alongside growing threats and technological change.

Read more: https://www.aoshearman.com/en/insights/cybersecurity-sunset-navigating-the-expiration-of-cisas-legal-protections

**Indian ministers push domestic alternatives to Google, Microsoft apps amid strained US ties**

Indian government ministers are actively promoting domestic technology alternatives to prominent U.S. digital services, signaling a strategic shift towards digital self-reliance amidst strained bilateral relations. This initiative, spearheaded by Indian Prime Minister Narendra Modi's "Made in India" (swadeshi) campaign, gained momentum following the United States' imposition of a 50% tariff on Indian imports in August. Key actors include Indian Information Technology Minister Ashwini Vaishnaw, Commerce Minister Piyush Goyal, and Education Minister Dharmendra Pradhan, who are publicly advocating for Indian-developed applications like Zoho, MapmyIndia, and Arattai. Specifically, Minister Vaishnaw has showcased Zoho's presentation software as an alternative to Microsoft PowerPoint and MapmyIndia as a domestic substitute for Google Maps in public forums, emphasizing their "swadeshi" nature.

Concurrently, Ministers Goyal and Pradhan have championed Arattai, Zoho's messaging application, as a homegrown alternative to WhatsApp. This concerted push has led to a significant surge in Arattai's adoption, with downloads increasing from fewer than 10,000 in August to over 400,000 last month, and daily active users surpassing 100,000 by late September. Despite this governmental backing, the initiative faces challenges. American brands like Google, Microsoft, and WhatsApp are deeply entrenched in the Indian market, often perceived as aspirational upgrades by millions. Past attempts to replace global platforms, such as the social media platform Koo, have faltered due to insufficient funding and inability to match the financial clout and reach of international competitors. Experts suggest that while state patronage is crucial, long-term success for domestic alternatives hinges on unique differentiating factors, substantial financial backing, and robust protec-

tion against surveillance. This push reflects India's broader ambition to reduce technological dependence on foreign entities, particularly in critical digital infrastructure, and could significantly reshape the competitive landscape for technology services in one of the world's largest digital markets.

Read more: https://www.reuters.com/world/india/indian-ministers-push-domestic-alternatives-google-microsoft-apps-amid-strained-2025-10-03/?

**The Crown Prince, Nezha: A New Tool Favored by China-Nexus Threat Actors**

A China-nexus threat actor has been observed leveraging a novel tool named "Nezha" in a sophisticated intrusion campaign targeting publicly-facing web applications, primarily across Taiwan, Japan, South Korea, and Hong Kong. This activity, first detected in August 2025, highlights the exploitation of geopolitical sensitivities in the region. The attack initiates by compromising vulnerable phpMyAdmin panels, often due to misconfigurations exposing the interface without authentication. The actor, operating from an AWS-hosted IP in Hong Kong, employs a log poisoning technique to inject a PHP web shell, akin to China Chopper, onto the web server. This involves manipulating MariaDB's general log to write a malicious PHP payload with a .php extension into a web-accessible directory, a method indicative of the actor's technical proficiency and prior experience, further suggested by their use of Simplified Chinese language settings during the initial compromise.

Upon establishing the web shell, the threat actor utilizes AntSword for interaction and subsequently deploys the Nezha agent. Nezha, an open-source server monitoring and task management tool, is repurposed here to facilitate further malicious activities, marking its first public documentation in such a context. The Nezha agent then proceeds to deploy Ghost RAT (Gh0st RAT), a remote access Trojan. This Ghost RAT variant establishes persistence by creating a service named "SQLlite" and disabling Windows Defender exclusions. Technical analysis of the Ghost RAT reveals dynamic resolution of WinAPI functions and a command-and-control (C2) infrastructure with historical DNS registrations linked to Beijing and Guangdong, China, aligning with known China-nexus APT group tactics.

The campaign has compromised over 100 victim machines, with the threat actor's Nezha dashboard, notably configured in Russian, indicating a growing victim count. While an anonymous source from Mainland China suggested the activity might be attributed to VPS enthusiasts seeking to bypass the Great Firewall for "experimentation," the deployment of advanced malware like Ghost RAT and the specific victim demographics strongly imply a more deliberate and malicious intent. This incident underscores the critical need for organizations to secure public-facing applications, implement robust authentication, and enhance detection capabilities for post-exploitation techniques to counter persistent and stealthy adversaries who increasingly weaponize publicly available tools.

Read more: https://www.huntress.com/blog/nezha-china-nexus-threat-actor-tool

**Microsoft's Crackdown on Unit 8200 Reveals Tech's Intermediary Role**

Microsoft recently took action against Israel's Unit 8200, an elite intelligence arm, by blocking its access to a cloud service that was being used for a surveillance program targeting Palestinian data. This development highlights the increasing role of major technology companies as "surveillance intermediaries" and their growing ability to influence state-operated surveillance practices. The incident stems from a joint investigation by The Guardian and +972 Magazine, which revealed that Unit 8200 had been storing thousands of terabytes of intercepted Palestinian phone calls from both Gaza and the West Bank on Microsoft's Azure cloud servers in Europe since 2022. This program was reportedly designed to analyze millions of phone calls daily, with Unit 8200 relying on Microsoft's infrastructure due to its own limitations in handling such a massive data load.

Following public scrutiny and an internal review, Microsoft announced on September 25 that it had found evidence supporting the allegations and subsequently terminated Unit 8200's access to specific cloud stor-

age and AI services, stating that it is "not in the business of facilitating the mass surveillance of civilians." While Israeli military officials reportedly anticipated the move and claimed no damage to operational capabilities, the action marks a significant instance of a major U.S. tech company imposing restrictions on a state intelligence agency. This event underscores a broader trend where tech giants, by providing critical infrastructure and tools, possess a de facto "kill switch" capability, enabling them to regulate government surveillance. This new power comes with profound responsibilities, particularly in contexts where traditional governmental or judicial oversight mechanisms for national security operations may be limited, as exemplified by the internal pressures on Israeli intelligence following the October 7, 2023, Hamas attack. The situation raises critical questions about how tech companies should exercise this discretion, the potential for blurring lines regarding their products' use, and the broader implications for international cooperation between states and private technology providers in national security matters.

Read more: https://www.lawfaremedia.org/article/microsoft-s-crackdown-on-unit-8200-reveals-tech-s-intermediary-role?

**China announces export control measures on technologies related to rare earths**

China's Ministry of Commerce (MOFCOM) and the General Administration of Customs have jointly announced comprehensive new export control measures targeting technologies and materials related to rare earths. These actions are framed within a context of national security, the fulfillment of international non-proliferation obligations, and the prevention of strategic resources from being misused in military or other sensitive applications by overseas entities. Rare earth elements are critical components in a wide array of advanced technologies, including new-energy vehicles, consumer electronics, wind turbines, and sophisticated military equipment such as fighter jets and nuclear facilities.

The new regulations, some effective immediately and others by November 8, impose strict controls on technologies associated with rare earth mining, smelting, separation, metal smelting, magnetic material manufacturing, and the recycling and utilization of rare earths from secondary sources. Additionally, overseas organizations and individuals are now required to obtain a dual-use items export license for certain rare earth-related items. The controls also extend to specific materials, including superhard materials, rare earth equipment and raw materials, five medium and heavy rare earth elements (such as holmium), lithium batteries, and artificial graphite anode materials. Notably, export applications destined for overseas military users or entities on control and watch lists will not be approved.

These measures signify a new phase in China's dual-use item export controls, formally implementing the extraterritorial application of such regulations, including refinements to the "de minimis rule" and "foreign-direct product rule." While China asserts these controls are not directed at any specific country or region and will permit legally compliant export applications, the strategic implications are significant. The move aims to safeguard China's national security and interests by preventing the transfer of critical resources that could undermine international peace and stability. It also positions China's actions as a responsible step consistent with international practices and WTO rules regarding national security exceptions, contrasting with what it perceives as other nations' over-generalization of national security concepts for competitive advantage. The long-term impact is expected to regulate, rather than ban, rare earth-related exports, ensuring the security and stability of global industrial and supply chains for compliant trade.

Read more: https://www.globaltimes.cn/page/202510/1345279.shtml

## United States of America (USA)

**In NGC2 first, Army uses beta artillery data tool in howitzer strike at Ivy Sting 1**

The U.S. Army's Next Generation Command and Control (NGC2) initiative, highlighted by the recent "Ivy Sting 1" exercise, represents a fundamental shift in military doctrine, moving away from a centralized, hierarchical command structure towards a more decentralized, agile, and data-driven approach to warfare.

This transformation is a direct response to the evolving character of modern conflict, particularly the lessons gleaned from the war in Ukraine, where the ability to rapidly sense, decide, and act has proven decisive. The legacy Advanced Field Artillery Tactical Data System (AFATDS), a product of the 1990s, is ill-suited for the speed and complexity of the contemporary battlefield. Its cumbersome interface and stove-piped architecture create significant latency in the "kill chain"—the process from target identification to engagement.

The successful test of the Artillery Execution Suite (AXS) tool during Ivy Sting 1 is a significant milestone in the NGC2 effort. AXS, conceived as an "app" within a broader, integrated ecosystem, streamlines the flow of targeting data, drastically reducing the cognitive load on soldiers and compressing the time required to execute a strike. By providing a more intuitive user interface and a common operating picture, AXS enables faster and more accurate decision-making. This is not merely an incremental improvement; it is a paradigm shift. The app-based architecture allows for rapid development and deployment of new capabilities, a stark contrast to the monolithic and slow-to-update nature of legacy systems. The use of an M777A2 Howitzer in the test underscores the integration of these new digital tools with existing hardware, demonstrating a commitment to maximizing the effectiveness of current assets.

The "Ivy Sting" series of exercises itself is a noteworthy innovation. It represents a move towards a more agile and iterative approach to military modernization, where soldiers and developers collaborate in a continuous feedback loop. This methodology, more akin to a tech startup than traditional defense procurement, allows for the rapid refinement and validation of new technologies in a real-world operational environment. The involvement of non-traditional defense contractors like Anduril, alongside established players like Lockheed Martin, further highlights the Army's commitment to leveraging cutting-edge commercial technology.

Strategically, the NGC2 initiative is a critical component of the U.S. military's response to the challenges of great power competition. The ability to operate in a decentralized manner, with dispersed forces connected by a resilient mesh network, is essential for survivability in a contested environment where traditional command and control nodes are vulnerable. By enabling the rapid massing of effects, rather than forces, NGC2 allows the Army to maintain a distributed posture while still concentrating combat power at the decisive point. This enhances lethality, reduces risk, and creates a more resilient and adaptable force, capable of outmaneuvering and overwhelming a peer adversary. The successful deployment of AXS in Ivy Sting 1 is a promising early indicator of the potential of this new approach to transform the U.S. Army's warfighting capabilities.

Read more: https://breakingdefense.com/2025/10/in-ngc2-first-army-uses-beta-artillery-data-tool-in-howitzer-strike-at-ivy-sting-1/?

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

**BIETA: A Technology Enablement Front for China's MSS**

The Beijing Institute of Electronics Technology and Application (BIETA), along with its subsidiary Beijing Sanxin Times Technology Co., Ltd. (CIII), has been identified as a technology enablement front for China's Ministry of State Security (MSS). This assessment is based on the affiliations of key personnel, BIETA's relationship with an MSS-run university, and the scope of its research and activities. BIETA and CIII are involved in researching, developing, importing, and selling technologies that support intelligence, counterintelligence, military, and national security missions for China.

Specific developments include extensive research into steganography, a method for covert communications and malware deployment, as well as the development and sale of forensic investigation and counterintelligence equipment. These entities also actively acquire foreign technologies related to steganography, network penetration testing, and military communications and planning. For instance, CIII advertises foreign software like WetStone Technologies' StegoHunt for steganography detection and various tools for military simulation and modeling, including those from US-based companies like Ansys Government Initiatives (AGI) and Scalable Network Technologies (SNT). Chinese Advanced Persistent Threat (APT) groups, such as APT40 and

APT15, have been observed utilizing steganographic techniques in their cyber operations to exfiltrate data and deploy malware.

The activities of BIETA and CIII highlight the MSS's role in developing and distributing advanced technologies to support cyber-enabled intelligence operations. This network of front organizations contributes to the modernization of China's state security apparatus, posing significant challenges to foreign governments and private businesses. The strategic implications include increased risks of technology transfer, as engagement with BIETA and CIII could inadvertently bolster the capabilities of the MSS and the People's Liberation Army (PLA). Foreign entities are advised to conduct thorough due diligence and consider restricting transactions with these organizations to mitigate national security risks.

Read more: https://www.recordedfuture.com/research/bieta-technology-enablement-front-for-chinas-mss
APT Meets GPT: Targeted Operations with Untamed LLMs

**APT Meets GPT: Targeted Operations with Untamed LLMs**

A China-aligned threat actor, tracked as UTA0388 (also known as Proofpoint's UNK_DropPitch), has been conducting extensive spear phishing campaigns since June 2025, targeting entities across North America, Asia, and Europe. These operations are characterized by their use of Large Language Models (LLMs), specifically OpenAI's ChatGPT, to generate highly tailored and voluminous phishing content. The campaigns initially involved direct malicious links but evolved to "rapport-building phishing," where benign initial emails precede the delivery of malicious payloads after target engagement.

The attack chain typically involves spear phishing emails leading to ZIP or RAR archives. These archives contain a legitimate executable, often named to appear as a document, which is then used for search order hijacking to load a malicious Dynamic Link Library (DLL). This DLL deploys GOVERSHELL, a custom malware family exclusively used by UTA0388. Volexity has identified five distinct variants of GOVERSHELL, developed in C++ and Golang, showcasing active and continuous development. These variants employ diverse command-and-control (C2) communication methods, including fake TLS, AES-encrypted channels, HTTPS polling, and WebSockets, and establish persistence via scheduled tasks.

Evidence for LLM usage includes the fabrication of personas, sequential patterns in fake contact details, non-existent domains in email signatures, and a lack of coherence in language and persona consistency across campaigns. Additionally, archives sometimes contained nonsensical "Easter eggs," such as pornographic images or religious recitations, and metadata in generated documents pointed to LLM-associated tools like python-docx. The high tempo and varied nature of the campaigns further support the assessment of LLM integration. This development signifies a critical shift in cyber warfare, where AI-driven automation enhances the scale and customization of attacks, posing significant challenges for detection and defense against sophisticated, state-sponsored threats with evolving tradecraft.

Read more: https://www.volexity.com/blog/2025/10/08/apt-meets-gpt-targeted-operations-with-untamed-llms/

**Photos of China's tailless J-50 aircraft give hints about stealth profile, likely mission: Experts**

Recent photographs of China's J-50 stealth fighter, a product of the Shenyang Aircraft Corporation (SAC) for the People's Liberation Army (PLA) Air Force, offer a detailed glimpse into the nation's advancing aerospace capabilities. The images confirm the aircraft, designated as J-50, J-XD, or J-XDS, features a tailless design, a significant step towards achieving a higher degree of stealth. This design eliminates vertical stabilizers, which are a major source of radar reflection, and instead relies on all-moving wingtips and 2D thrust-vectoring engine nozzles for flight control. The aircraft's configuration is further optimized for low observability with twin Diverterless Supersonic Intakes (DSI) and a low-profile canopy, suggesting an emphasis on wideband stealth that surpasses current fifth-generation fighters. The J-50's propulsion system, likely the WS-10C class

engines, combined with its aerodynamic shape, points towards a design capable of efficient supercruise—supersonic flight without the use of fuel-guzzling afterburners. This would grant the J-50 extended range and increase the kinematic performance of its air-to-air missiles. The heavy-duty, twin-wheeled nose gear has fueled speculation about its potential for carrier operations, which would significantly expand the PLA Navy's power projection capabilities.

However, experts caution that the tailless design may present challenges in the high-alpha (angle of attack) and low-speed handling required for carrier landings. Strategically, the J-50 is anticipated to fill the "low-end" role in a future "hi-lo" mix of stealth aircraft, complementing a larger, more capable stealth fighter like the J-36. It is expected to replace older aircraft, such as the JH-7 fighter-bomber and early J-10 variants. While likely possessing a smaller internal weapons bay and shorter range than the J-36, the J-50 is still expected to have considerable internal volume for fuel and munitions. The concurrent development of the J-50, J-36, and various unmanned loyal-wingman platforms highlights China's comprehensive strategy to build a multi-layered, technologically advanced air force. This modernization effort is poised to significantly alter the regional balance of power, challenging the air superiority of other nations and reinforcing China's national security posture.

Read more: https://breakingdefense.com/2025/10/new-photos-of-chinas-tailless-j-50-aircraft-give-hints-about-its-stealth-profile-likely-mission-experts/?

## Republic of China (ROC) | Taiwan

**Taiwan will not agree to 50-50 chip production deal with US, negotiator says**

Taiwan's firm rejection of a proposed "50-50 chip production" arrangement with the United States underscores a pivotal moment in global semiconductor geopolitics. The negotiation, led by Taiwan's Vice Premier and chief trade negotiator Cheng Li-chiun and U.S. Commerce Secretary Howard Lutnick, reflects intensifying tensions over technological sovereignty and supply-chain security. Washington's proposal to relocate half of Taiwan's chip output to U.S. soil was framed as a means of insulating the American economy from potential disruptions linked to cross-Strait instability. For Taipei, however, such a concession would undermine its most vital strategic asset: control over the world's most advanced semiconductor ecosystem, centered on the Taiwan Semiconductor Manufacturing Company (TSMC).

Cheng clarified that the idea of a 50-50 split was neither discussed nor acceptable to Taiwan, emphasizing instead a "Taiwan model" of cooperation. This approach seeks deeper economic alignment with the United States through investment, joint research, and supply-chain diversification without relinquishing industrial leadership or relocating key production capacity. TSMC's ongoing investments in U.S. fabrication plants, particularly in Arizona, represent strategic partnership rather than dependency. Simultaneously, Taiwan has extended an olive branch through commitments such as multi-billion-dollar agricultural imports from the U.S., signaling goodwill while maintaining firm boundaries on strategic technology matters.

The episode reveals a widening asymmetry between U.S. security-driven industrial policy and Taiwan's existential need to safeguard its technological dominance. It also reflects a broader decoupling trend: advanced manufacturing and supply chains are becoming instruments of national strategy rather than pure market efficiency. For Taiwan, retaining chip production onshore is not just an economic choice but a deterrent its "silicon shield" in a volatile regional environment. For the United States, the setback illustrates the limits of industrial coercion in a multipolar tech landscape increasingly defined by negotiation rather than alignment.

Read more: https://www.reuters.com/world/asia-pacific/taiwan-will-not-agree-50-50-chip-production-deal-with-us-negotiator-says-2025-10-01/?

Has Lutnick signalled the end of Taiwan's 'silicon shield' against Beijing?

The central issue is U.S. Commerce Secretary Howard Lutnick's push for a "50-50" split between the United States and Taiwan in semiconductor production, and whether that shift undermines Taiwan's so-called "silicon shield" against Chinese aggression. Lutnick argues that Taiwan's dominance in advanced chip manufacturing long viewed as a strategic deterrent to Beijing has become a vulnerability for the U.S., since supply chains are dependent on a geopolitically exposed location.

In a recent proposal, Lutnick suggested that half of the semiconductors used in the U.S. market should be produced domestically, thereby reducing reliance on Taiwan. He indicated that if Taiwan continues to hold 95 percent of advanced chip capacity, the U.S. may struggle to defend the island effectively in a crisis. He framed this as not just an economic issue but a national security one: "If you can't make your own chips, how can you defend yourself?".

Taiwan's government has firmly rejected the proposal, stating that the "50-50" split was never part of trade negotiations and that it will not agree to such a condition. Taiwanese officials are concerned that relocating or reducing advanced chip production would erode their geopolitical leverage and weaken the "silicon shield" that has helped deter Chinese military action. Opposition lawmakers in Taiwan have publicly criticized the U.S. proposal as exploitative and warned that surrendering chip dominance undermines Taiwan's strategic position. Strategically, this debate signals a major shift in how key actors view semiconductor supply chains in the context of great-power competition. For the U.S., reshoring chip production is becoming a pillar of economic and military preparedness. For Taiwan, maintaining its dominance in advanced chip manufacturing is not only an economic imperative but continues to be seen as a key part of its security and deterrence strategy against China. This dispute reflects broader trends of supply chain realignment and the securitisation of high technology in global politics.

Read more: https://www.scmp.com/news/china/politics/article/3327340/has-lutnick-signalled-end-taiwans-silicon-shield-against-beijing?

## European Union | EU

**Keeping European industry and science at the forefront of AI**

The European Commission is implementing a multi-faceted strategy to establish Europe as a global leader in artificial intelligence (AI), focusing on both industrial application and scientific advancement. Key actors in this endeavor include the European Commission, Member States, industry, academia, and civil society, all working to navigate the global competition in AI. The initiative is framed by the need to leverage AI's transformative potential for economic growth, societal benefits, and technological sovereignty, while upholding ethical principles. Specific developments include the "Apply AI Strategy," which aims to accelerate AI adoption in industries and public services by integrating infrastructure, data, and testing facilities, and by preparing the workforce for AI.

This strategy is supported by the "Apply AI Alliance" for coordination and an "AI Observatory" for trend monitoring. Simultaneously, the "AI in Science Strategy" seeks to advance AI-driven research through initiatives like RAISE (Resource for AI Science in Europe), a virtual institute for pooling AI resources. This includes attracting global scientific talent, allocating €600 million from Horizon Europe for computational power, and doubling annual AI investments to over €3 billion, with a focus on AI in science. Additionally, the "AI Act Service Desk" has been launched to ensure the smooth implementation of the AI Act, the world's first comprehensive AI law. These efforts, building on the "AI Continent Action Plan," are designed to foster innovation, ensure ethical AI development, and secure Europe's strategic position in the digital era.

The establishment of the "AI Act Service Desk" is a critical component, signaling the EU's commitment to not only creating the world's first comprehensive AI legal framework but also ensuring its practical imple-

mentation. The significant financial commitment, including doubling annual AI investments to over €3 billion, demonstrates a clear understanding of the resources required to compete at a global level. Ultimately, this strategy is not just about technological leadership; it's a geopolitical statement about the EU's commitment to shaping the future of AI in a way that aligns with its core values, potentially setting a global standard for responsible AI governance and influencing the trajectory of AI development worldwide.

Read more: https://commission.europa.eu/news-and-media/news/keeping-european-industry-and-science-forefront-ai-2025-10-08_en

## The Commonwealth of Australia

**NATO embraces new Australian-made Star Wars-style lasers to counter Russian drones**

NATO's decision to integrate an Australian-designed directed-energy weapon into its air defence network marks a strategic evolution in how the alliance counters the expanding threat of Russian and Iranian-supplied drones. The system, known as Apollo, is developed by Electro Optic Systems (EOS) a Canberra-based defence company and has been acquired by a Western European NATO member in a deal valued at approximately US $125 million. The move comes amid a surge in drone incursions across Eastern Europe, including violations of Polish airspace, underscoring the growing asymmetry in modern warfare where low-cost unmanned systems are deployed at scale to exhaust traditional, high-cost missile defences.

Apollo employs a high-energy laser to destroy drones through "thermal destruction," concentrating light to melt or ignite airframes and internal components. It can neutralize up to 20 drones per minute within a six-kilometre range, offering near-instantaneous engagement at roughly one US dollar per shot, a fraction of the cost of interceptor missiles that can exceed US $500,000 each. While the laser's effectiveness can be reduced by adverse weather fog, rain, or dust and its range remains shorter than kinetic interceptors, its speed, precision, and negligible collateral damage make it ideal for close-range defence around critical infrastructure and mobile bases.

Strategically, Apollo represents NATO's growing reliance on directed-energy weapons as a cost-effective countermeasure in an "economic attrition war" increasingly defined by drone swarms and automated strikes. The deployment signals a shift from reactive missile interception toward sustained, scalable energy-based defence layers integrated with radar and kinetic systems. For Australia, the sale elevates its profile as a high-technology defence exporter and aligns with Western efforts to diversify supply chains away from U.S. and European monopolies. More broadly, the adoption of laser technology by NATO could accelerate a global transition toward energy weapons, redefining the balance between offensive drone warfare and defensive sustainability in 21st-century conflicts.

Read more: https://www.abc.net.au/news/2025-09-30/australian-lasers-nato-russian-drones/105810770

## Islamic Republic of Pakistan

**Confucius Espionage: From Stealer to Backdoor**

The Confucius cyber-espionage group, a suspected state-aligned actor with a long history of operations across South Asia, has shifted its tactics from broad data theft toward more sophisticated and persistent intrusion methods. Historically known for targeting government, defense, and critical infrastructure sectors particularly in Pakistan the group relied on stealer malware campaigns such as WooperStealer, which exfiltrated a wide range of files using malicious Microsoft Office documents and shortcut (LNK) files. These earlier attacks delivered payloads that harvested local files, credentials, and documents before transmitting them to attacker-controlled servers via HTTP POST requests.

Recent investigations by Fortinet's FortiGuard Labs reveal that Confucius has transitioned to deploying Py-

thon-based backdoors, notably a reworked version of the "AnonDoor" malware. This new toolset introduces more complex infection chains, leveraging LNK files that execute PowerShell scripts to install a Python runtime environment, drop concealed compiled Python files (such as winresume.pyc), and establish persistence through scheduled Windows tasks. Once embedded, the backdoor gathers detailed system information, communicates with command-and-control infrastructure, and executes targeted commands such as file enumeration, exfiltration, screenshot capture, command execution, and credential theft. The backdoor's design shows increased emphasis on stealth, including timed task execution and obfuscation techniques to avoid detection. This tactical evolution marks a strategic pivot from opportunistic data collection to continuous, covert surveillance. By transitioning from simple stealers to modular, scriptable backdoors, Confucius demonstrates adaptability and a deeper focus on maintaining long-term access within targeted networks. The development mirrors broader global trends among advanced persistent threat groups, which increasingly employ lightweight, flexible toolchains to evade security solutions. For national security and intelligence agencies in South Asia, this shift underscores an escalating espionage threat that prioritizes persistence and control over quick data theft, highlighting the need for enhanced monitoring of PowerShell activity, script execution, and anomalous network traffic within high-value environments.

Read more: https://www.fortinet.com/blog/threat-research/confucius-espionage-from-stealer-to-backdoor

## Russian Federation & Ukraine

**Cavalry Werewolf raids Russia's public sector with trusted relationship attacks**

The recent campaign by the cyber threat cluster known as Cavalry Werewolf has targeted Russian government agencies and critical sectors like energy, mining, and manufacturing via a sophisticated "trusted-relationship" phishing strategy. The attackers masquerade as Kyrgyz government officials and, in several instances, exploit legitimately compromised email accounts from Kyrgyz ministries. Their emails carry manipulated RAR archives that deploy custom malware: FoalShell, a reverse-shell tool, and StallionRAT, a remote access trojan controlled over Telegram.

FoalShell the cluster's lightweight reverse shell tool is available in Go, C++, and C# variants, enabling stealthy execution of arbitrary commands via cmd.exe in hidden mode. StallionRAT written in Go, PowerShell, and Python is delivered via a C++ launcher that invokes PowerShell with Base64-encoded commands, establishing command-and-control over Telegram. The RAT supports operations such as listing compromised hosts, executing commands, and uploading files; it also employs SOCKS5 proxy tools (ReverseSocks5Agent / ReverseSocks5) and uses registry autorun persistence via a Run key to maintain survivability.

Between May and August 2025, BI.ZONE observed this cluster actively expanding its toolset and refining its methods. Attackers also appear to be probing new regional targets: file names in Tajik and Arabic hint at future campaigns beyond Russia. While this campaign avoided mass disclosure, analysts warned that stealth and evolving malware make timely detection and response especially challenging.

Strategically, this activity underscores how state-level or state-sponsored espionage actors are increasingly embedding themselves within trusted communications channels to bypass traditional defences. For Russia, the campaign reveals vulnerabilities in critical infrastructure and state agency networks. More broadly, the incident reflects a growing trend: adversaries blending credible impersonation, custom malware, and long-duration intrusion into sensitive systems. The persistence and adaptability of such threat clusters will continue to stress defences across geopolitical fault lines and heighten the stakes in cyber competition.

Read more: https://bi.zone/eng/expertise/blog/cavalry-werewolf-atakuet-rossiyu-cherez-doveritelnye-otnosheniya-mezhdu-gosudarstvami/

Malware & Vulnerabilities

**Rhadamanthys 0.9.x Upgrades its Payloads**

Rhadamanthys is a modular, multi-functional malware family sold via underground marketplaces as a Malware-as-a-Service (MaaS) platform, with developers and operators frequently updating it to evade detection. The 0.9.x iteration represents a significant evolution, emphasizing stealth, flexibility, and anti-analysis techniques. This malware targets high-value data sources such as browsers, cryptocurrency wallets, VPN configurations, email clients, and messaging applications, aiming to harvest credentials, session tokens, and other sensitive artifacts for subsequent monetization or lateral movement within compromised environments. Key actors in this ecosystem include the malware authors, criminal operators who deploy purchased builds, and defensive cybersecurity researchers analyzing these developments.

The 0.9.x updates introduce multiple structural and behavioral changes designed to complicate analysis and hinder defensive measures. One major change is the internal configuration format: the malware now uses a new magic marker and stores its configuration in a compressed and obfuscated format, encoded with a modified Base64 charset, encrypted with a stream cipher variant, and finally decompressed using LZO. Network communications have been modified to disguise data exfiltration, including MIME-type spoofing (e.g., callbacks using image/png) and support for multiple command-and-control endpoints per sample, allowing greater operational flexibility. Additional runtime behaviors, such as a misleading GUI message box on execution and a global mutex to prevent duplicate instances, demonstrate the malware's growing focus on anti-sandbox and anti-analysis mechanisms.

The modular design continues to expand in 0.9.x, with updated features for process injection, optimized data export routines, and improved operator management within the control panel. These changes render previous unpacking and detection tools less effective, forcing security teams to update static analysis scripts and behavioral detection rules. From a strategic perspective, the evolution of Rhadamanthys illustrates an ongoing arms race in malware development, where professionalized threat actors continuously refine their tools to bypass detection while lowering operational complexity for less-skilled users. For defenders, this trend emphasizes the need for a layered cybersecurity approach, combining endpoint detection, network monitoring, and memory analysis to detect obfuscated or encrypted communications and respond rapidly to compromise. Overall, Rhadamanthys 0.9.x represents a mature, highly adaptive threat, reinforcing the importance of proactive intelligence and rapid defensive adaptation in modern cybersecurity operations.

Read more: https://research.checkpoint.com/2025/rhadamanthys-0-9-x-walk-through-the-updates/

Tile's lack of encryption could make tracker owners vulnerable to stalking

The central subject involves Tile Bluetooth trackers and a newly exposed set of security vulnerabilities, with key actors being Georgia Institute of Technology researchers, the Electronic Frontier Foundation (EFF), Tile (owned by Life360), and the broader tech ecosystem (including competitors like Apple and Samsung). Researchers from Georgia Tech discovered that Tile devices broadcast unencrypted and static MAC addresses alongside unique IDs, meaning that a single recorded message suffices to fingerprint a tag indefinitely. Unlike competitors that rotate identifiers and encrypt communications to prevent unwanted tracking, Tile's design enables easy interception and replay of Bluetooth broadcasts via common tools or antennas.

Tile's "anti-theft mode" further complicates the privacy landscape. While intended to hide a user's device from thieves, it also prevents detection by its own Scan & Secure anti-stalking feature, making it possible for malicious actors to remain undetected. Researchers note that this feature, when subverted, could be exploited not only for stalking but also for framing innocent users via replay attacks broadcasts from one device replayed elsewhere to mimic movement. Critics, including the EFF, argue that Tile's reluctance to adopt industry-standard protections (like MAC address rotation and encrypted data transport) leaves consumers exposed. The parent company acknowledges making "improvements" after disclosure, but has not publicly detailed

fixes or addressed how their structural design enables potential mass surveillance.

From a strategic and privacy perspective, the vulnerabilities highlight how "trackers for convenience" can become tools for abuse in the absence of robust security. The case underscores growing scrutiny of IoT and location-tracking technology, especially as users and regulators demand stronger protections against stalking, surveillance, and misuse. The Tile situation fits a broader trend emphasizing that functionality without privacy safeguards poses real risks in both legal and personal security terms.

Read more: https://www.theverge.com/news/787836/tile-trackers-stalking-research-unencrypted?

**VMware Bug Exploited by Chinese Threat Actor**

The main issue centers on a high-severity local privilege escalation vulnerability in VMware products, designated CVE-2025-41244, affecting VMware Tools, VMware Aria Operations (specifically its Service Discovery Management Pack, SDMP), and related VMware infrastructure. The key actors include Broadcom (which owns VMware), cybersecurity firm NVISO Labs (which discovered and publicly documented the flaw), and the Chinese state-linked threat actor UNC5174, which has reportedly exploited the vulnerability in real operations.

In the context of increasingly frequent attacks on cloud and enterprise infrastructure, this vulnerability represents a significant exposure: it allows an unprivileged local user on a guest virtual machine (VM) to escalate their privileges to root, provided VMware Tools is installed and Aria Operations is managing the VM with SDMP enabled. The flaw arises from a misconfigured "service discovery" mechanism: VMware scripts use overly permissive regular expressions in identifying binaries (e.g., via get-versions.sh), potentially matching and executing malicious binaries placed in writable directories such as /tmp/httpd. This issue applies both to credential-based discovery (through Aria Operations) and credential-less modes (via open-vm-tools), meaning both Windows and Linux environments may be at risk. NVISO researchers confirmed active exploitation since mid-October 2024, documenting a proof-of-concept attack that uses this method to obtain root access.

Broadcom has released patches for affected VMware components, including updates to VMware Tools and Aria Operations, and flagged this as a serious vulnerability (CVSS score ~7.8). Analysts warn that such unchecked privilege escalation within virtualization infrastructure enables persistent adversaries to gain deep access, potentially spreading laterally across enterprise and cloud environments. Given that UNC5174 has a documented history of targeting critical sectors and exploiting enterprise software, this vulnerability underscores how even local, "trusted" infrastructure components can be weaponized. Strategically, the incident illustrates the growing importance of securing virtualization stacks, improving code validation practices (especially around regex and path handling), and the broader trend of adversaries exploiting infrastructure tools rather than just external attack surfaces.

Read more: https://blog.nviso.eu/2025/09/29/you-name-it-vmware-elevates-it-cve-2025-41244/

**Investigating active exploitation of CVE-2025-10035 GoAnywhere Managed File Transfer vulnerability**

A critical deserialization vulnerability, CVE-2025-10035, in Fortra's GoAnywhere Managed File Transfer (MFT) software is under active exploitation by the cybercriminal group Storm-1175, known for deploying Medusa ransomware. This flaw, rated with a CVSS score of 10.0, enables attackers to bypass signature verification in the License Servlet, leading to arbitrary object deserialization, command injection, and potential remote code execution (RCE) without authentication on internet-exposed instances.

The multi-stage attack observed by Microsoft Threat Intelligence begins with the exploitation of this zero-day vulnerability for initial access. Storm-1175 establishes persistence by deploying remote monitoring and management (RMM) tools such as SimpleHelp and MeshAgent directly within the GoAnywhere MFT process, alongside creating .jsp files. Following initial compromise, the threat actors conduct user and system discov-

ery using commands and tools like netscan, and achieve lateral movement within the network via mstsc.exe. Command and control (C2) infrastructure is set up using RMM tools and Cloudflare tunnels. Data exfiltration involves the deployment and execution of Rclone, culminating in the deployment of Medusa ransomware in some compromised environments.

The exploitation of MFT solutions poses significant national security and economic implications due to their role in handling sensitive data, making them prime targets for data theft and ransomware. Organizations are strongly advised to immediately upgrade to the latest GoAnywhere MFT version, implement robust enterprise attack surface management, restrict internet access for MFT servers, and leverage endpoint detection and response (EDR) in block mode. Microsoft Defender offers comprehensive protection, including vulnerability identification, endpoint detection, and threat intelligence, to help organizations detect and respond to this sophisticated threat.

Read more: https://www.microsoft.com/en-us/security/blog/2025/10/06/investigating-active-exploitation-of-cve-2025-10035-goanywhere-managed-file-transfer-vulnerability/

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.