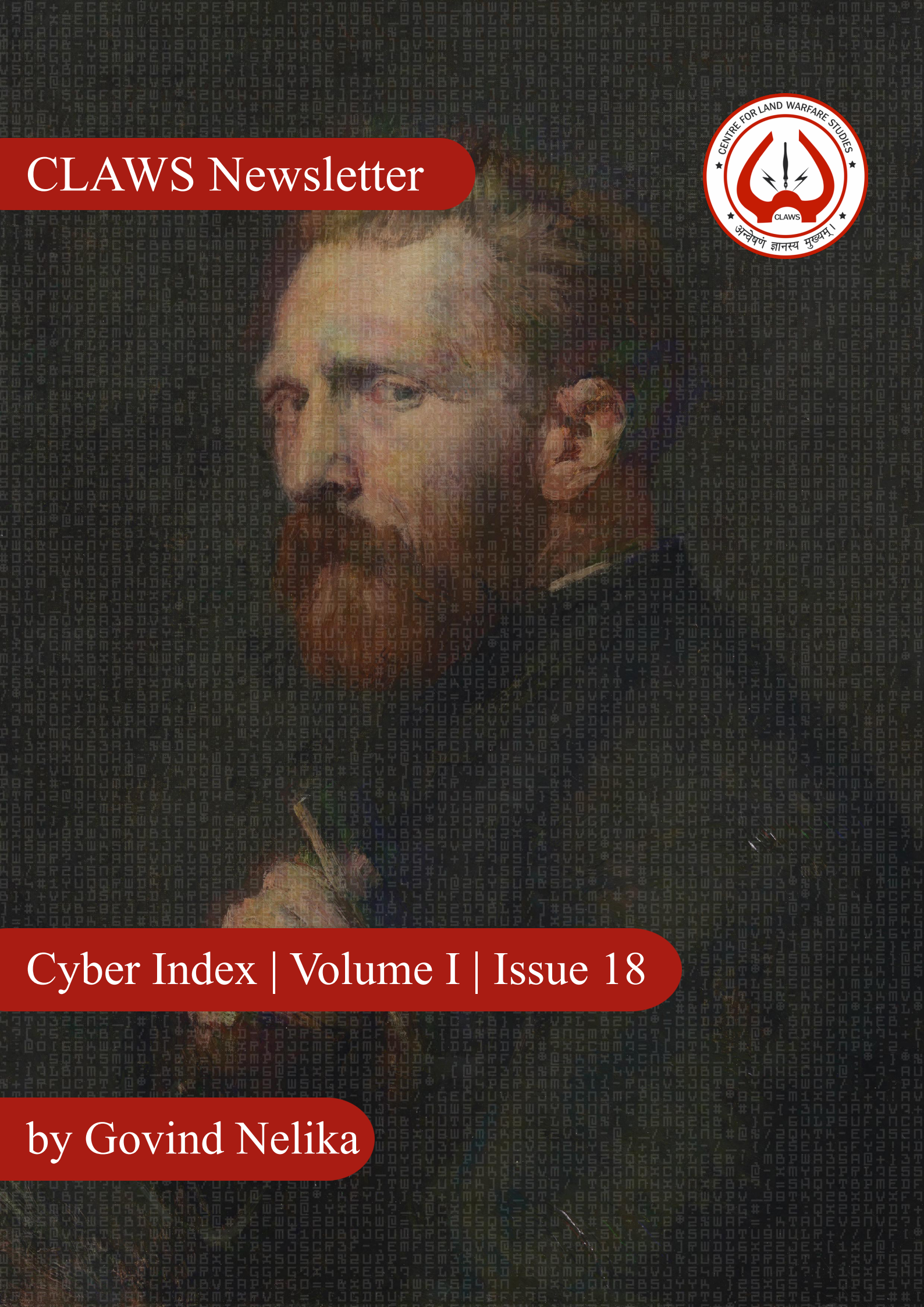
CLAWS Newsletter



Cyber Index | Volume I | Issue 18

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 04

United Kingdom of Great Britain and Northern Ireland 06

United States of America (USA) 08

People's Republic of China (PRC) | China 10

European Union | EU 12

The Commonwealth of Australia 12

Russian Federation 13

Democratic People's Republic of Korea (DPRK) 14

Malware & Vulnerabilities 14

Global Brief

IT Ministry proposes mandatory labelling of AI-generated content on social media

India's Ministry of Electronics and Information Technology (MeitY) has proposed sweeping amendments to its IT Rules, 2021, aimed at tightening regulation of AI-generated deepfake content. Under the draft framework, platforms with more than 5 million users will be required to obtain a user declaration when content is potentially synthetically generated, and use "reasonable and proportionate" technical measures to verify those declarations. Synthetic content must be clearly labelled: for images or video, a visible marker must cover at least 10 percent of the visual area, and for audio, an identifier must occupy at least the first 10 percent of playback. These labels must be permanently embedded and cannot be altered or removed by the platform. The draft also introduces a legal definition of "synthetically generated information" as any content artificially created or manipulated by computers in a way that appears authentic.

MeitY's justification for these rules points to the growing ease with which generative AI tools can produce "convincing falsehoods," and the risks posed by such misuse ranging from misinformation and electoral manipulation to impersonation and financial fraud. To strengthen accountability, the government is also introducing stricter due-diligence duties for those intermediaries that enable creation or modification of synthetic media. Meanwhile, takedown orders for content flagged as synthetic would require senior-level officials within government to issue the notice, ensuring greater oversight.

Stakeholder feedback on the draft is being solicited until November 6, 2025, and failure by platforms to comply could jeopardize the "safe-harbour" protections they enjoy under Indian law. Strategically, these proposed rules signal India's shift toward proactive governance of synthetic media, balancing innovation in AI with the need for transparency and user safety. By establishing legally enforceable labelling norms, the government is trying to preempt the weaponization of deepfakes a trend that has sparked rising concern globally and reinforce trust in digital public discourse.

Read more: https://www.thehindu.com/news/national/it-ministry-proposes-strict-rules-for-labelling-deepfakes-amidaimisuse/article70189322.ece

UN Convention against Cybercrime opens for signature in Hanoi, Viet Nam

The main subject is the new United Nations Convention against Cybercrime (also known as the "Hanoi Convention"), overseen by the United Nations Office on Drugs and Crime (UNODC) in collaboration with the Government of Hanoi, Viet Nam. The treaty arises from growing global concern over cyber-threats such as ransomware, online fraud, data theft and infrastructure attacks that span national borders and challenge existing legal and cooperative frameworks. Sixty-plus states gathered in Hanoi in October 2025 to open the instrument for signature, with seventy-two signing on the first day.

In practical terms, the Convention sets out to harmonise national laws by criminalising key cyber-offences including unauthorised access to information systems, data interference, the use of computer-systems to commit fraud or facilitate child sexual-exploitation, and attacks on critical infrastructure and it prescribes enhanced mechanisms for extradition, mutual legal assistance, and cross-border evidence sharing. While the exact text is not publicly dissected in full here, the institution of a supra-national legal instrument reflects recognition that cybercrime cannot be efficiently addressed by unilateral national law alone. The Convention will enter into force once a threshold of 40 ratifying states is reached.

Strategically, this development marks a significant milestone in international cyber-governance: for the first time a global treaty dedicated to cybercrime is open for signature, indicating a shift toward formalised multilateral frameworks in a space historically fragmented by regional conventions and bilateral treaties (such as the Budapest Convention on Cybercrime). The treaty's success could enhance law-enforcement coordination, streamline processes for cross-border investigations, and improve the ability to respond to cyber-threats in real

time. However, it also raises questions about national sovereignty, potential for surveillance or misuse, and how the safeguards for human rights will be implemented across diverse legal systems. Overall, the Hanoi Convention represents a major step in the trend toward globalising cyber-law and responding to the borderless nature of digital threats.

Read more: https://www.unodc.org/unodc/en/press/releases/2025/October/un-convention-against-cyber-crime-opens-for-signature-in-hanoi--viet-nam.html

China says it found evidence of U.S. cyber attack on state agency

China's Ministry of State Security has publicly accused the U.S. National Security Agency (NSA) of conducting a sustained cyber-espionage campaign against its National Time Service Center, a high-precision agency responsible for generating and broadcasting China's official standard time. According to Beijing, the campaign began in March 2022 and involved exploitation of a vulnerability in a foreign mobile-phone messaging service to access the personal devices of Time Center staff. Over time, attackers allegedly used stolen credentials to breach internal computer systems, and from 2023 into 2024 they even attempted to infiltrate the centre's ground-based, high-precision timing hardware

Chinese authorities claim they traced the activity to global private server networks used to obfuscate the origin of the attacks, warning that such intrusions posed a serious risk not only to China's timing infrastructure but also to vital national functions communication networks, financial systems, power grids, and defense all depend on precise time synchronization.

Although the Ministry insists it has "irrefutable evidence," it has not disclosed technical documentation or third-party verification of its claims. Meanwhile, the U.S. Embassy has not issued a public comment so far. Strategically, these allegations exacerbate already volatile U.S.–China cyber tensions, especially in light of broader disputes over trade, technology access, and national security. By framing the NSA as a threat to core timing infrastructure, China is underscoring the potentially systemic impact of cyber operations on critical systems. If validated, the claims could signal a significant escalation in state-level cyber conflict, highlighting not just espionage but possible sabotage routes that target precision-time services a foundational element for modern communications, finance, and power networks.

Read more: https://www.japantimes.co.jp/news/2025/10/19/asia-pacific/politics/china-evidence-us-cyber-attack/

Chinese arms makers urged to embrace AI technology in weapons development

The main subject of the development is China's state-run defence and arms-manufacturing complex particularly entities such as China North Industries Group Corporation (Norinco) and affiliated suppliers of the People's Liberation Army (PLA). A recent article in the magazine Modern Weaponry, published by Norinco, urges China's arms-makers to incorporate artificial intelligence (AI) into weapons development to improve efficiency and performance, while also cautioning that risks and uncertainties must be managed.
In context, China is deepening its "military-intelligentisation" drive seeking to integrate civilian high-tech innovation, dual-use AI capabilities, and military modernization under the broader framework of civil-military fusion. The impetus is both economic (competitive arms exports, cost-efficiency gains) and strategic (closing the technology gap, reshaping future warfare paradigms).

Specifically, the article highlights several technical pathways for AI integration: AI acting as an advisory or design-recommendation tool; leveraging historical and real-time sensor data to optimise design algorithms; using simulation and "digital twin" models of weapons systems for prediction of faults and improved testing; and applying AI to legacy systems such as artillery to refine firing tables and enhance accuracy. It emphasises that older systems with low automation present larger gain-potential when AI is applied. While the magazine encourages arms firms to "explore" and "optimise" AI in weapons design and production, it also warns that

blind optimism must be avoided, and strict oversight, security controls, and reliability verification are necessary.

Strategically, this push carries significant implications for global arms competition, military-industrial transformation, and regional security dynamics. The adoption of AI-enabled weapons development could accelerate China's defence-technology refresh, enhance the cost-performance profile of Chinese exports, and complicate arms-control regimes. At the same time, the explicit caution signals recognition of technology-risk, reliability, and governance issues. Overall, this development fits into broader trends of rising AI-military convergence, intensified great-power rivalry in defence innovation, and the erosion of a sharp divide between civilian technology and weapon systems.

Read more: https://www.scmp.com/news/china/military/article/3329069/chinese-arms-makers-urged-embrace-ai-technology-weapons-development?

United Kingdom of Great Britain and Northern Ireland

China stole 'vast amounts' of state secrets, says Cummings

The main actors in this episode are the United Kingdom's government agencies specifically the Cabinet Office and the National Cyber Security Centre (NCSC) and the People's Republic of China, which is alleged to have orchestrated a long-term cyber-intrusion into UK systems. Contextually, the revelation comes amid growing scrutiny of China's intelligence gather¬ing operations abroad, tensions surrounding tech-sovereignty, critical-infrastructure security and the UK's interplay between economic ties to China and national-security priorities. Former senior adviser Dominic Cummings claims that as early as 2020 he was notified that "vast amounts" of classified UK government data including intelligence-service material and restricted communications were accessed by Chinese actors via a network used for transmitting top-secret information.

He says the breach involved a data-transfer system code-named "Strap," used for the most sensitive content, and that this network had been compromised for years, facilitated by a Chinese-owned firm connected with the UK's infrastructure. In response, the government has publicly rejected the claim that its highest-level networks were compromised, stating there is no evidence of a campaign against the bespoke systems used for "Strap" material.

The divergence in accounts forms a dispute rather than a verified technical disclosure; specific methods of intrusion, malware tools or exfiltration paths are not publicly detailed and the allegations remain unconfirmed. Strategic implications are significant: if true, the episode would exemplify how state-backed actors can exploit trusted national-data-transfer systems and blur lines between espionage and supply-chain risk, thereby challenging assumptions about allied-state immunity. It also reflects a broader trend of elevated cyber-competition, where national-security frameworks must reckon with the dual pressures of economic engagement and digital defence.

Read more: https://www.telegraph.co.uk/news/2025/10/15/china-stole-state-secrets-massive-hack-cummings/

United States of America (USA)

US court bars NSO Group from installing spyware on WhatsApp

The case centers on NSO Group, an Israeli cyber-surveillance firm known for its Pegasus spyware, and Meta-owned WhatsApp, representing broader civil-society and privacy interests. In a U.S. federal court, Judge Phyllis Hamilton issued a permanent injunction barring NSO from targeting WhatsApp users, concluding that its operations cause "irreparable harm" and continue unabated. The legal battle stems from WhatsApp's 2019 lawsuit, which accused NSO of exploiting a vulnerability in the app to install Pegasus on about 1,400 devices, including those of journalists, human-rights activists, and government figures. The court found that NSO not

only violated federal and state hacking laws specifically the Computer Fraud and Abuse Act but also breached WhatsApp's terms of service. According to court findings, NSO reverse-engineered WhatsApp's code and repeatedly redesigned its spyware to evade detection and security patches, using "zero-click" mechanisms and missed-call exploits. While a prior jury judgment had awarded WhatsApp about US$168 million in damages, Judge Hamilton significantly reduced the punitive award to US$4 million, reasoning that the original figure lacked sufficient legal basis.

Strategically, this ruling represents a major accountability moment for the surveillance-tech industry, signaling that even powerful spyware vendors can face meaningful legal constraints. By halting NSO's ability to exploit encrypted platforms like WhatsApp, the court is reinforcing user privacy and pushing back on state or non-state actors who rely on commercial cyber-tools for covert surveillance. The decision may set a precedent for future litigation around mercenary spyware, influencing how such tools are regulated and deployed, especially when embedded in widely used civilian communication services.

Read more: https://economictimes.indiatimes.com/news/international/global-trends/us-court-bars-nso-group-from-installing-spyware-on-whatsapp/articleshow/124660671.cms?

ED 26-01: Mitigate Vulnerabilities in F5 Devices

CISA Orders Urgent Federal Response After F5 Source Code Breach Exposes Critical Infrastructure Risks
The primary subject is the U.S. federal government's cybersecurity response process overseen by the Cybersecurity and Infrastructure Security Agency (CISA), directed at vulnerabilities in equipment produced by F5 Networks especially its BIG-IP line of networking devices. The directive, labelled Emergency Directive 26-01 (ED 26-01), builds on escalating concerns over advanced cyber-threat actors exploiting critical infrastructure and government networks. It appears in the context of increasingly aggressive nation-state cyber campaigns exploiting network equipment and management interfaces areas of elevated risk for surveillance, data exfiltration, and persistent access.

Under ED 26-01, federal civilian agencies are required to perform an inventory of all F5 devices (including BIG-IP iSeries, rSeries, F5OS platforms and other variants network-exposed or publicly reachable), assess whether these systems are internet-accessible or accessible via networked interfaces, and remediate or replace vulnerable units accordingly. The directive was triggered because of a confirmed compromise of F5's internal systems, in which threat actors allegedly accessed portions of F5's source code, vulnerability information and other proprietary assets actions that provide attackers with a roadmap to design zero-day exploits or tailored attacks against F5 gear. According to CISA, successful exploitation of the impacted F5 gear could allow unauthorised access to embedded credentials, privileged administrative interface access, interception of application programming interface (API) flows, or full system takeover.

The required actions include:

(1) immediate inventory and identification of all F5 devices within agency networks;

(2) evaluation of whether network-exposed management or control interfaces exist;

(3) prioritised patching, hardening or removal of out-of-support or compromised devices;

(4) reporting back to CISA on status and remediation. The directive emphasises urgency because the stolen code and vulnerability information effectively lower the barrier for attackers to craft exploits tailored to these systems.

Strategically, this situation underscores how network-infrastructure vendors once viewed as marginal risk are now high-value targets for threat actors, because appliances like F5's are embedded deep within government and critical-infrastructure networks. It illustrates a broader trend of nation-state actors zeroing in on

supply-chain and infrastructure-hardware/software weaknesses, increasing the challenge of defending federal networks and allied systems. The successful exploitation of such devices would carry national-security, critical-infrastructure and intelligence implications; the directive signals that federal agencies are being compelled to adopt a more aggressive, proactive posture in identifying and remediating third-party infrastructure risk.

Read more: https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices

Chinese cyberspies snoop on Russian IT biz in rare east-on-east attack

The primary subject of the incident is the Chinese-linked advanced persistent threat (APT) known as Jewelbug, which targeted a Russian IT service provider and by extension, Russian technology and supply-chain infrastructure. According to cybersecurity firm Symantec, this operation ran from January to May 2025 and represents a striking departure from the historically tacit non-interference between Chinese and Russian intelligence cyber-activities.

In the broader context of rising cyber-espionage by state-backed actors, the move fits into Beijing's expanding footprint of intelligence collection and interference, and reflects a recalibration of target sets beyond traditional Western adversaries. Russian infrastructure especially service providers and software supply-chain dependencies now appears to be within the scope of Chinese cyber operations, suggesting both strategic ambition and shifting alliances. The exploitation of a Russian IT service firm opens opportunities not only for data theft but also for onward supply-chain compromise of the firm's customer base.

Technically, the attackers used a renamed version of Microsoft's debugger tool "cdb.exe" (renamed "7zup.exe") to execute shellcode, load malicious DLLs, and hijack processes. They also conducted credential dumps, scheduled-task persistence, and event-log clearing. Exfiltration of data was routed via Yandex Cloud a cloud platform commonly used in Russia providing plausible deniability and stealth.

Strategically, this development has serious implications: it signals that even states publicly aligned with China may find themselves targeted for exploitation, undercutting assumptions about friendly-state immunity from cyber intrusion. Moreover, penetration of a service provider raises supply-chain risks for downstream customers, amplifying potential damage. At an international level, the episode underscores a broader trend of sophisticated state-sponsored actors weaponising cloud infrastructure, legitimate administrative tools and supply-chain vectors to maximise stealth and scale.

Read more: https://www.theregister.com/2025/10/16/chinese_russian_cyber_espionage/

People's Republic of China (PRC) | China

Chinese team plans to test powerful chip on world's largest optical telescope in Spain

A research team from Tsinghua University in China is preparing to field-test a novel, ultra-compact optical computing chip, named Yuheng (also called "Rafael"), on the Gran Telescopio Canarias (GTC) in Spain. The GTC, a 10.4-meter single-aperture optical telescope located in the Canary Islands, is currently the world's largest of its kind. This development arises from a breakthrough in photonics and materials science: Yuheng can resolve light spectral features with a precision of under 0.1 nanometre about 100 times sharper than typical snapshot imagers and operate in real time.

It achieves this by using interference patterns and advanced AI algorithms to capture and decode the full color (spectral) information of incoming light, instead of physically splitting the light as conventional spectrographic instruments do. According to the researchers, in laboratory tests Yuheng was capable of capturing the spectral signatures of nearly 10,000 stars per second, a rate that, if replicated on a telescope, could dramatically accelerate our ability to map the Milky Way from an operation that would traditionally take millennia to one that could possibly be done in under a decade.

The team is now transitioning from prototype to an engineering-grade model, which they intend to integrate with the Gran Telescopio Canarias for on-sky experiments. Strategically, this represents a major step both for astronomy and for optical computing: if successful, Yuheng could transform how telescopes conduct spectral surveys, offering orders-of-magnitude improvements in efficiency. Moreover, the miniaturized, high-resolution chip has potential applications beyond astronomy in drones, robotics, and medical imaging highlighting China's push to fuse AI, photonics, and materials research to drive both scientific discovery and broader technological innovation.

Read more: https://www.scmp.com/news/china/science/article/3329364/chinese-team-plans-test-powerful-chip-worlds-largest-optical-telescope-spain?

'They're watching': How Monday's internet crash became China's training

The central subject is a large-scale internet service disruption specifically the major outage of Amazon Web Services (AWS) that occurred recently and the key actors involved include AWS, affected cloud-customers and infrastructure providers globally, and observers in the People's Republic of China, notably Chinese state-affiliated or state-led actors monitoring the event. In the context of heightened geopolitical tensions, increasing dependency on cloud services and digital infrastructure, and concerns over national-critical resilience, the outage serves both as a cautionary incident and as a potential training model for adversarial actors. Following the AWS network collapse, intelligence and cybersecurity analysts noted that Chinese cyber-operators appeared to treat the incident as a live case-study: they collected data on systems resilience, fail-over behaviour, DNS propagation issues and cloud-platform dependencies while the disruption unfolded.

The outage revealed how a single fault in a large-scale cloud provider could cascade into wide-ranging digital service failures, thereby illustrating systemic vulnerability. Technical detail includes disruptions in distributed-denial-of-service mitigation systems, routing anomalies, cloud-storage region replication failings and the knock-on effect on internet-connected services analysis indicates Chinese actors logged traffic patterns, incident-response timelines and public reaction as part of an iterative exercise

Strategically, this event carries significant national-security and international implications: it underscores the fragility of Western digital infrastructure, offers adversaries both reconnaissance data and operational lesson-sets, and reinforces a broader trend of state-linked actors using benign infrastructure failures to prepare for or simulate potential offensive campaigns. For defenders, it highlights the imperative of diversifying suppliers, improving resilience testing and anticipating that infrastructure incidents may be weaponised or studied by peer-state competitors.

Read more: https://www.smh.com.au/technology/they-re-watching-how-monday-s-internet-crash-became-china-s-training-20251021-p5n3zy.html

European Union | EU

Cybercrime-as-a-service takedown: 7 arrested

The primary subject is a sophisticated "cybercrime-as-a-service" network, dismantled in a coordinated law-enforcement action by Europol, Eurojust, and national authorities from Latvia, Austria, and Estonia. The operation codenamed SIMCARTEL uncovered a criminal infrastructure that rented out large pools of telephone numbers via SIM-box technology, enabling fraudsters to conceal their identities while committing a wide range of telecommunications-based crimes. During the October 10, 2025, crackdown, investigators arrested seven suspects (five Latvians among them), and seized 1,200 SIM-box devices and 40,000 active SIM cards. The network is believed to have facilitated more than 3,200 fraud cases: about 1,700 in Austria, causing losses of roughly €4.5 million, and 1,500 in Latvia, with around €420,000 lost. The infrastructure included five servers, two websites (notably gogetsms.com and apisim.com) used to provide the service, and more than 80 country-registered phone numbers. Beyond simple fraud, the SIM-farm enabled a variety of criminal activities

such as phishing, smishing, investment scams, extortion, migrant smuggling, and distribution of child sexual abuse content. Authorities also froze significant assets: €431,000 in bank accounts, USD 333,000 in crypto-currency, and seized four luxury vehicles.

This takedown is strategically significant because it strikes at the heart of a commercialized, scalable cyber-fraud capability: by dismantling infrastructure that offered anonymity and mass-account creation, law enforcement is disrupting cybercrime-as-a-service at its core. The operation underscores growing cross-border cooperation in fighting organized cybercrime and signals the EU's increasing capacity to target the enablers of large-scale fraud. It also highlights a wider trend: cybercriminal ecosystems are becoming modular and service-oriented, and law enforcement agencies are adapting with integrated, multinational responses.

Read more: https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested

The Commonwealth of Australia

ASD leads global strike on cyber crooks

The primary actor in this update is the Australian Signals Directorate (ASD), operating in conjunction with its domestic cyber-security wing the Australian Cyber Security Centre (ACSC) and allied intelligence and law-enforcement agencies. The context involves a rapidly intensifying global cyber-threat landscape in which both state-sponsored actors and organised cyber-criminal groups are leveraging more advanced methods and infrastructure to target critical services, government networks and supply-chains.

Within this environment, ASD has led an expansive "global strike" campaign to identify, disrupt and dismantle cyber-criminal infrastructure and networks, in many cases working in close partnership with foreign counterparts. Specific developments include offensive cyber-operations that disabled command-and-control nodes, seized illicit server infrastructure used for mass-data hosting and dark-web distribution, and imposed novel cyber-sanctions on entities supplying "bullet-proof hosting" services that facilitate large-scale data theft or ransomware operations.

The tradecraft observed spans credential harvesting, ransomware-extortion pipelines, illicit hosting of stolen personally-identifiable information (PII), and the exploitation of under-protected internet-facing infrastructure within supply-chains. For example, the ACSC's 2024-25 threat report notes that among critical-infrastructure entities, compromised assets/networks accounted for a majority of incidents, with denial-of-service (DoS) attacks and account-compromise also prominent. The continuing expansion of adversary capabilities such as use of AI tools within bot-nets, "living off the land" techniques and exploitation of edge devices has propelled the urgency of ASD's actions.

Strategically, this development underscores a shift in cyber-action from passive defence toward active disruption by government agencies, illustrating that national-security authorities are now prepared to strike at the infrastructure enabling cyber-criminal ecosystems rather than merely respond to individual incidents. This fits within broader global trends of intelligence agencies collaborating more closely, imposing legal and economic costs on malicious actors, and targeting the upstream enablers of cyber-threats thereby raising the bar for adversaries and altering the operational calculus of cyber-crime and state-sponsored activity.

Read more: https://www.theaustralian.com.au/special-reports/defence/asd-leads-global-strike-on-cyber-crooks/news-story/a2a68a1a0d74788173cda6b8c5c0c2f8

Russian Federation

Jewelbug: Chinese APT Group Widens Reach to Russia

The principal entity in this case is the Chinese-linked advanced persistent threat (APT) group known as Jew-

elbug (also referred to as REF7707, CL-STA-0049, Earth Alux), which has broadened its operations to target a Russian IT service provider. The intrusion, carried out between January and May 2025, marks a significant departure from the group's prior focus on Asia and Latin America and is especially notable given the traditional cyber-restraint between China-affiliated and Russian actors. Within the broader context of intensifying global cyber-espionage, supply-chain fragility and shifting geopolitical alignments, Jewelbug gained access to the provider's code repositories and software build systems indicative of a potential software supply-chain attack aimed at downstream Russian customers.

Technical tradecraft included use of a renamed Microsoft Console Debugger ("7zup.exe", masquerading cdb.exe) to execute shellcode, bypass application allow-listing, hijack DLL loaders, dump credentials (e.g., via LSASS/Mimikatz), schedule persistence tasks, clear Windows Event Logs, and exfiltrate data via a malicious "yandex2.exe" dropper to the Russian cloud service Yandex Cloud leveraging legitimate infrastructure to evade detection. Beyond Russia, Jewelbug concurrently targeted entities in South America, South Asia and Taiwan, deploying DLL sideloading, kernel driver exploitation (BYOVD / EchoDrv), and a bespoke backdoor using Microsoft Graph API and OneDrive as command-and-control channels. The operation underlines the group's expanding technical sophistication and strategic reach.

From a strategic and security perspective, the campaign underscores that even so-called allied states are not immune to each other's cyber-espionage, the criticality of supply-chain junctions in modern cyber-warfare, and the growing tendency of state-backed actors to operate stealthily via legitimate tools and cloud services. The broader trend suggests that national-security risk is increasingly diffuse spanning cloud platforms, software build ecosystems and trans-national supply chains requiring heightened vigilance and coordination across borders.

Read more: https://www.security.com/threat-intelligence/jewelbug-apt-russia

Operation MotorBeacon : Threat Actor targets Russian Automotive Sector using .NET Implant

A recently uncovered cyber campaign involves a previously unknown .NET malware dubbed CAPI Backdoor, which is being used to target Russia's automobile-commerce and e-commerce sectors. The research, conducted by SEQRITE Labs, describes a spear-phishing infection chain that commenced in early October 2025 via a malicious ZIP archive masquerading as a payroll recalculation document ("Перерасчет заработной платы 01.10.2025"). The ZIP contains a Windows shortcut (LNK) file which triggers execution of a malicious .NET DLL ("adobe.dll" / "client6.dll") using the legitimate rundll32.exe utility a classic misuse of a living-off-the-land binary.

Once executed, the CAPI Backdoor implants itself and establishes persistence by copying itself into the user's roaming app data folder and creating a startup shortcut, and also by scheduling a task that repeatedly runs via rundll32. Its functionality is extensive: it checks for administrative privileges, enumerates installed antivirus products via WMI, opens the decoy PDF to avoid suspicion, and connects to a command-and-control (C2) server over TCP (port 443) to fetch commands. These commands include data exfiltration (from browsers Chrome, Edge, Firefox), capturing screenshots, collecting user/system info, and managing connections. It also contains virtual-machine detection routines (via hypervisor queries, SMBIOS, PnP device checks, MAC address patterns, disk and GPU vendor enumeration) to evade sandbox analysis. The backdoor compresses stolen browser data (profiles, encrypted keys, bookmarks, history, etc.) into ZIP files and sends them to the C2 server; screenshots are also packaged and transmitted.

On the infrastructure side, SEQRITE observed use of a domain-generation algorithm (DGA) to create fake domains, initially redirecting to a domain impersonating carprice[.]ru (spelled carprlce[.]ru) to lend legitimacy. The C2 infrastructure was tracked to IP addresses under AS-REG (ASN 197695) and another node under ASN 39087 (P.a.k.t LLC). The hashes of key malicious files and network indicators have been documented; SEQRITE's own protections can detect this malware under the labels Trojan.49992.SL and RatCiR.

Strategically, this campaign is significant because it highlights a growing trend of highly targeted cyber espionage or crime operations aimed at critical sectors like Russian automotive commerce. By blending phishing, native Windows utilities, and stealthy .NET malware that harvests sensitive data and maintains persistence, the threat actor demonstrates sophisticated tradecraft. The targeting of financial-commerce and auto transactional systems may indicate motives ranging from intelligence gathering to economic sabotage. For national security, this raises concerns about deeper compromise of Russia's commercial infrastructure, while for the cybersecurity community, it underscores the importance of defending against supply-chain–style phishing attacks and living-off-the-land malware.

Read more: https://www.seqrite.com/blog/seqrite-capi-backdoor-dotnet-stealer-russian-auto-commerce-oct-2025/

Russian hackers leak documents linked to eight UK military bases as MoD launches probe

The incident centres on a cyberattack by a Russian-affiliated hacker group known as Lynx, which has purportedly breached the systems of the U.K. defence-contractor Dodd Group and leaked sensitive internal documents. The leaked files reportedly include personal data of employees, schematics and operational protocols for eight British military bases including sites housing U.S. F-35 fighter jets, a major RAF drone base, an ultra-secure radar facility, and locations where nuclear weapons are stored.

This leak unfolds amid a broader climate of heightened cyber risk between Russia and NATO-aligned nations, where defence supply chains and military infrastructure remain frequent targets. The hackers allegedly used ransomware tactics, demanding payment and threatening to make the stolen documents public a pattern consistent with other financially motivated or state-tolerated cyber operations.

Following the disclosure, the U.K. Ministry of Defence (MoD) confirmed it is investigating the claim of a data breach involving Dark Web publication of its internal documents. The Dodd Group acknowledged that it experienced an unauthorized intrusion, saying it promptly contained the incident and brought in digital-forensics experts.

Strategically, this event underscores the evolving nature of cyber-espionage, where state-linked actors may combine intelligence gathering with financial extortion. The targeting of military infrastructure not just operational communications but detailed base schematics raises serious national security concerns. It highlights how hybrid threat actors exploit both technological access and commercial vulnerabilities in defence contracting to achieve geopolitical leverage. For Western security services, the leak portends a growing threat: adversaries may weaponize stolen defense data in political, military, or economic leverage campaigns.

Read more: https://theins.ru/en/news/286028

Democratic People's Republic of Korea (DPRK)

DPRK Adopts EtherHiding: Nation-State Malware Hiding on Blockchains

The subject of this development is a North Korean state-linked cyber threat group, identified by Google Threat Intelligence as UNC5342, which has started using a technique called EtherHiding to embed malware in public blockchains marking the first observed use of this tactic by a nation-state. Contextually, this comes amid ongoing geopolitical tensions and international sanctions on North Korea, motivating its cyber operators to adopt increasingly resilient methods to steal cryptocurrency and generate revenue. Since February 2025, UNC5342 has integrated EtherHiding into its long-running "Contagious Interview" campaign, which lures developers with fake job interviews and technical assessments, distributing malicious loaders disguised as legitimate software.

In practice, EtherHiding works by embedding malicious JavaScript payloads into smart contracts on block-

chains such as Ethereum and BNB Smart Chain. These contracts act as decentralized, immutable command-and-control (C2) servers: the malware's loader script, injected into a compromised site, issues read-only blockchain calls (like eth_call) to fetch the hidden payload without generating any transaction or gas fees. Once retrieved, the payload typically a loader called JADESNOW decrypts and executes a more persistent backdoor, INVISIBLEFERRET, which can exfiltrate sensitive data, hijack credentials, and steal cryptocurrency. The malicious smart contracts have been updated repeatedly on-chain at low cost, reflecting operational flexibility, while UNC5342 uses centralized API providers (rather than directly hosting blockchain nodes) to query on-chain data, letting them effectively pivot or reconfigure their infrastructure without being easily blocked.

Strategically, this represents a significant shift: by abusing blockchain technology itself as a host for malware, UNC5342 gains a highly resilient, takedown-resistant infrastructure difficult to disrupt via conventional cybersecurity measures. EtherHiding's use by a state-backed actor underscores evolving cyber tactics where decentralized technologies enable persistent and covert operations. For defenders, this raises serious implications: traditional domain- and IP-based blocking may prove ineffective, and mitigating this threat will likely require enterprise-scale controls, such as managed browser environments (e.g., Chrome Enterprise) and strict download policies, combined with threat intelligence and proactive monitoring of blockchain-based abuse.

Read more: https://cloud.google.com/blog/topics/threat-intelligence/dprk-adopts-etherhiding

Malware & Vulnerabilities

Tracking Malware and Attack Expansion: A Hacker Group's Journey across Asia

A FortiGuard Labs investigation has identified a cyberthreat actor expanding a persistent malware campaign across Asia, with operations tracked moving from Mainland China to Taiwan, Japan, and most recently Malaysia. Initially observed in January 2025 deploying the "Winos 4.0" backdoor in Taiwan via spear-phishing, the group subsequently shifted to a different malware family HoldingHands and scaled its attacks. The phishing lures used in this campaign include PDF documents masquerading as official Taiwanese Ministry of Finance communications, embedding links that lead to malicious payloads hosted on Tencent Cloud. Fortinet analysts connected related attacks by correlating infrastructure identifiers (such as Tencent Cloud app IDs), shared domain naming conventions (many containing "tw"), and reused command-and-control (C2) servers.

In Japan, a phishing PDF redirects victims to a Japanese-language page, which in turn delivers a digitally signed EXE that sideloads the malware. That executable carries debug paths ("BackDoor.pdb") linking it to HoldingHands, reinforcing the connection with earlier campaigns. More recently, the group has shifted to Malaysia, where the same infrastructure (including domains like twczb[.]com) resolves to previously observed IP addresses. In this variant, malware is installed via a multi-stage flow that abuses Windows Task Scheduler, making detection by behavior-based security tools more difficult.

The malware chain involves a malicious "dokan2.dll" loader (named after a legitimate open-source DLL) that loads a shellcode loader, which in turn unpacks encrypted payloads into files under C:\Windows\System32. These include a malicious TimeBrokerClient.dll, msvchost.dat, and other encrypted components. Defense evasion is achieved via anti-VM checks like RAM size verification and privilege escalation via TrustedInstaller impersonation. The final payload is injected into a taskhostw.exe process running under a user's desktop session by duplicating a logged-on user's access token and then periodically reinjecting if the process exits.

The HoldingHands payload also supports dynamic updating of its C2 server, by reading a registry value (HKEY_CURRENT_USER\SOFTWARE\HHClient\AddrStrChar), and a command to terminate its own execution. The threat actor's use of layered obfuscation, code reuse, infrastructure overlap, and signed executables underscores operational sophistication.
Strategically, this cross-border malware operation reflects a growing trend of regionally pivoting cyber espionage or crime groups that maintain persistence by evolving tools and tactics. The ability to reuse infrastructure

and pivot targets across multiple Asian jurisdictions shows a long-term, adaptive campaign rather than isolated incidents. For national-security and cyber-defense stakeholders, the activity signals a need for cross-border intelligence sharing, stronger phishing resilience, and enhanced monitoring of anomalous scheduled-task or DLL side-loading activity especially for infrastructure users in government, finance, or critical services across the Asia-Pacific region.

Read more: https://www.fortinet.com/blog/threat-research/tracking-malware-and-attack-expansion-a-hacker-groups-journey-across-asia

BeaverTail and OtterCookie evolve with a new Javascript module

The main subject of this incident is a North Korea–linked threat group, commonly referred to as Famous Chollima (also tracked under names like CL-STA-0240, UNC5342, and Void Dokkaebi), which has evolved its malware arsenal by merging two previously distinct tool families: BeaverTail and OtterCookie. This development unfolds against the backdrop of the group's long-running "Contagious Interview" campaign, in which they impersonate recruiters to lure job seekers particularly developers into installing malicious software under the guise of technical tests.

In the latest variant, dubbed OtterCookie v5, the threat actor has combined BeaverTail's browser information-stealing capabilities with OtterCookie's remote-command and control features, and added a powerful keylogger module along with screenshot capture. The infection begins when a target installs a trojanized Node.js application (e.g., a fake "Chessfi" client) or a malicious npm package ("node-nvm-ssh") delivered via the official npm registry. During installation, a post-install hook executes a JavaScript loader chain (index.js → file15.js) that eventually unpacks a large obfuscated payload combining BeaverTail and OtterCookie logic.

Once active, the malware establishes a persistent Socket.IO-based connection to a command-and-control (C2) server, which enables a modular set of operations: exfiltrating browser profiles and cryptocurrency wallet data (from extensions like MetaMask), performing remote shell commands, harvesting clipboard content, capturing keystrokes, taking periodic screenshots, and installing remote-access software (AnyDesk). It can also deploy a secondary Python backdoor called InvisibleFerret to maintain long-term access. To evade detection, the malware uses obfuscation (via Obfuscator.io), XOR-based encoding, and sandbox-detection techniques.

Strategically, this convergence of BeaverTail and OtterCookie into a unified, highly modular JavaScript malware represents a significant sophistication in North Korea's cyber operations. By using fake recruitment processes and supply-chain tactics (npm packages), the threat actor is targeting not just individual developers but potentially valuable crypto-asset infrastructure. The enhanced surveillance capabilities (keylogging, screenshots) signal a shift toward deeper espionage, while the long-term persistence via InvisibleFerret suggests the goal is sustained system compromise. Overall, this development underscores a broader trend of nation-state actors blending financial crime, social engineering, and advanced malware to achieve strategic gains while staying under the radar.

Read more: https://blog.talosintelligence.com/beavertail-and-ottercookie/

PassiveNeuron: a sophisticated campaign targeting servers of high-profile organizations

The PassiveNeuron campaign, identified by Kaspersky's Global Research & Analysis Team (GReAT), represents a sophisticated cyber-espionage operation that has been targeting Windows Server systems in government, financial, and industrial organizations across Asia, Africa, and Latin America since at least December 2024. After a six-month hiatus, operations resumed through August 2025, involving a multi-stage infection chain and advanced implants. Attackers initially compromise systems possibly via Microsoft SQL Server vulnerabilities, SQL injections, or credential abuse and attempt to deploy web shells; when these efforts are blocked, they fall back on a complex DLL-loader architecture. The first-stage loader is a deceptively named DLL (e.g., wlbsctrl.dll, TSMSISrv.dll, oci.dll) placed in the System32 folder, leveraging Phantom DLL Hi-

jacking to auto-load under legitimate Windows processes and achieve persistence. These DLLs are artificially inflated to over 60–100 MB to evade detection. They also perform checks on the host's MAC address hash to ensure the malware only runs on intended targets, thwarting sandbox analysis.

The campaign deploys three main payloads: Neursite, a modular C++ backdoor capable of system reconnaissance, process control, proxying traffic, and loading plugins for shell access, file management, and socket communication; NeuralExecutor, a .NET implant obfuscated with ConfuserEx, which supports multiple communication channels (TCP, HTTP(S), named pipes, WebSockets) and dynamically loads .NET assemblies from its command-and-control (C2) infrastructure; and Cobalt Strike, the commercial red-teaming tool repurposed here for post-exploitation, lateral movement, and persistence. Attackers inject their final payload into legitimate system processes (e.g., WmiPrvSE.exe or msiexec.exe) via shellcode execution, sometimes using VMProtect for further obfuscation.

Attribution remains tentative; Kaspersky notes some function names in samples use Cyrillic characters potential false flags but based on tactics, techniques, and procedures, they assess a low-confidence link to a Chinese-speaking threat actor. Strategically, PassiveNeuron underscores a growing trend in APT activity: server systems especially Internet-exposed ones are prime targets, and threat actors are leveraging deeply stealthy, multi-stage implants to sustain long-term access. For defenders, this emphasizes the critical need to reduce server attack surfaces, enforce rigorous patch management (especially on SQL servers), monitor for anomalous DLL behavior, and deploy layered detection (e.g., behavioral EDR) to catch these tailored espionage campaigns.

Read more: https://securelist.com/passiveneuron-campaign-with-apt-implants-and-cobalt-strike/117745/

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.