CLAWS Newsletter

Cyber Index | Volume II | Issue No. 2

by Govind Nelika

@govindnelika | https://claws.co.in/category/newsletter/

*CLAWS Cyber Index Newsletter is a concise brief delivering Strategic Insights on Global Cyber Threats, Policy Shifts, and Geopolitical Technology Developments.

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

Internal

Weaponized in China, Deployed in India: The Sync Future Espionage Targeted Campaign

In early December 2025, security researchers identified a sophisticated cyber-espionage campaign dubbed “SyncFuture,” which utilizes weaponized Chinese enterprise security software to target entities in India. The operation, attributed to state-linked threat actors, highlights a growing trend of “software repurposing,” where legitimate commercial tools in this case, the SyncFuture Terminal Security Management (TSM) system developed by Nanjing Zhongke Huasai Technology are converted into comprehensive espionage frameworks. By leveraging the trust associated with legitimate, signed Chinese security products, the actors achieve deep persistence and extensive data exfiltration capabilities while operating under the guise of standard administrative activity. This development underscores the escalating geopolitical tensions in the Indo-Pacific region and the increasing use of dual-use software to bypass traditional defensive perimeters.

The campaign begins with highly targeted phishing emails impersonating the Indian Income Tax Department, deploying lures titled “Tax Compliance Deficiency and Penalty Notice” to trick victims into downloading a malicious archive. The technical execution is notably advanced, employing DLL sideloading of a signed Microsoft binary to execute "MpGear.dll," a loader featuring multi-layered anti-debugging and timing checks. Once active, the malware utilizes file-less COM-based UAC bypasses and process masquerading to escalate privileges and blend into the Windows environment. A standout feature is its specialized evasion of Avast Free Antivirus; the malware uses automated GUI interaction and mouse simulation to navigate the antivirus interface and manually whitelist its own components. The final payload, the SyncFuture TSM, provides a robust command-and-control suite capable of real-time monitoring, file manipulation, and persistent service installation that remains active even in Safe Mode. For global defenders, this campaign illustrates the high risk posed by legitimate code-signing certificates and the necessity for behavioural monitoring that can detect the abuse of trusted management tools for covert intelligence gathering.

Read more: https://www.esentire.com/blog/weaponized-in-china-deployed-in-india-the-syncfuture-espionage-targeted-campaign

OpenAI CEO plans India visit as AI leaders converge at AI Impact Summit

OpenAI CEO Sam Altman’s planned visit to India for the AI Impact Summit marks a strategic inflection point in the global effort to harmonize frontier artificial intelligence (AI) development with robust regulatory and security frameworks. As AI integration penetrates critical infrastructure and democratic processes, this engagement between OpenAI, the Government of India, and a cohort of international AI leaders underscores the rising tension between rapid technological deployment and the necessity for sovereign guardrails. This development is particularly significant as India seeks to establish itself as a primary architect of AI ethics for the Global South, balancing the drive for innovation with the protection of its vast digital biometric and financial ecosystems.

The summit focuses on the operationalization of "Safe AI" principles, exploring the secure deployment of Large Language Models (LLMs) within public service delivery while mitigating systemic risks such as deepfakes and automated disinformation. Technical discussions are poised to centre on the security of sovereign AI stacks, emphasizing the hardening of API endpoints and the protection of fine-tuning datasets against poisoning or unauthorized exfiltration vulnerabilities that threaten the integrity of e-governance platforms. Furthermore, the visit highlights the imperative for "Security-by-Design" in autonomous systems, addressing the technical debt inherent in rapidly scaled LLM architectures. For risk management and policy stakeholders, Altman's engagement signals a shift toward a collaborative "Global AI Compact," aimed at stabilizing international norms regarding dual-use AI capabilities.

The broader implications for national security and international stability involve the creation of resilient, localized AI ecosystems that can withstand the adversarial manipulation of the information environment. Ultimately, this move reinforces the pattern of "tech-diplomacy," where the resilience of the global cyber threat landscape is increasingly determined by the alignment between Silicon Valley's frontier labs and the sovereign security requirements of major digital powers.

Read more: https://www.firstpost.com/tech/openai-ceo-plans-india-visit-as-ai-leaders-converge-at-ai-impact-summit-13972280.html

External

Global Focus Brief

No longer 'experimental': Navy to deploy drone boats this year, official says

The U.S. Navy is transitioning its Uncrewed Surface Vessel (USV) initiatives from experimental prototyping to formal operational deployment, signalling a pivotal shift in maritime power projection and the realization of a "hybrid fleet" architecture. Driven by escalating geopolitical tensions in the Indo-Pacific and the strategic necessity of Distributed Maritime Operations (DMO), this move addresses the requirement to augment traditional carrier strike groups with cost-effective, persistent autonomous platforms capable of high-risk intelligence, surveillance, and reconnaissance (ISR) and kinetic missions.

Rear Adm. Kevin Smith, the program executive officer for unmanned and small combatants, has confirmed that the Navy aims to deploy its first operational USVs by late 2026, marking the graduation of platforms like the Large USV (LUSV) and Medium USV (MUSV) from the experimental testbeds of Task Force 59.These systems leverage advanced Command and Control (C2) frameworks and modular sensor suites, utilizing Common Control System (CCS) architectures to ensure interoperability across the fleet. The transition necessitates hardening autonomous navigation software and secure data links against electronic warfare (EW) and cyber-interference, which remain primary vulnerabilities in contested littoral environments. For defense stakeholders and risk managers, this deployment represents a critical maturation of autonomous systems engineering, shifting the burden of maritime domain awareness to attritable robotic nodes.

However, the integration of these platforms into the tactical grid introduces complex cyber-resilience challenges, specifically regarding the integrity of AI-driven decision-making and the security of long-range telemetry. Ultimately, this operationalization cements autonomous robotics as a permanent fixture in modern naval warfare, forcing a re-evaluation of international maritime security protocols and escalation dynamics in congested theatres.

Read more: https://breakingdefense.com/2026/01/no-longer-experimental-navy-to-deploy-drone-boats-this-year-official-says/

Void Link: Evidence That the Era of Advanced AI-Generated Malware Has Begun

Check Point Research has identified "VOIDLINK," a sophisticated AI-generated malware framework that represents a pivotal evolution in the weaponization of Large Language Models (LLMs) by emerging threat actors. As the democratization of generative AI accelerates, VOIDLINK signifies a transition from human-dependent coding to an automated, malicious software development lifecycle (SDLC) capable of scaling attacks with unprecedented speed.

The framework functions as a modular ecosystem, utilizing LLM integration to autonomously generate, test, and refine polymorphic payloads tailored to specific target environments. Technically, VOIDLINK leverages a central orchestrator that issues prompt to LLM APIs to produce functional code in Python and Go, incorporating advanced evasion techniques such as dynamic API resolving, environment-aware anti-debugging logic, and semantic obfuscation to defeat static and heuristic analysis. Notable components include "VoidDrop," an intelligent downloader that performs pre-execution reconnaissance to detect virtualized environments, and "LinkSteal," a modular stealer targeting browser-stored credentials and localized cryptocurrency wallets. Furthermore, the framework's command-and-control (C2) architecture utilizes AI-tuned traffic shaping to mimic legitimate web services, effectively blending malicious exfiltration with routine HTTPS metadata. For defenders and decision-makers, this development underscores the diminishing returns of signature-based security and the critical necessity for behavioural, AI-augmented detection systems.

The operationalization of VOIDLINK suggests a future where cyber resilience must be maintained at machine speed to counter high-velocity, adaptive campaigns. Ultimately, this shift necessitates a fundamental re-evaluation of risk management protocols, as the barrier to entry for complex, multi-stage cyber-espionage and financial crime continues to collapse, challenging international stability and the integrity of global digital infrastructure.

Read more: https://research.checkpoint.com/2026/voidlink-early-ai-generated-malware-framework/

United Kingdom of Great Britain & Northern Ireland

China hacked Downing Street phones for years

British intelligence services have attributed a sustained, multi-year cyber-espionage campaign targeting 10 Downing Street to sophisticated threat actors linked to the Chinese state, marking a significant breach of the United Kingdom's executive communications. This development highlights the escalating sophistication of state-sponsored Advanced Persistent Threats (APTs) targeting high-value political leadership within the context of heightening geopolitical tensions between London and Beijing.

The incident underscores a critical shift in the threat landscape where mobile devices serve as the primary vector for long-term intelligence gathering, bypassing traditional perimeter defences. Investigative findings reveal that the compromise involved the deployment of advanced spyware likely utilizing zero-click exploits on both official and personal mobile handsets belonging to senior ministers and staff, with activity reportedly dating back to 2020. The tradecraft employed exhibited high levels of stealth, including the use of obfuscated command-and-control (C2) infrastructure and data exfiltration techniques designed to evade standard National Cyber Security Centre (NCSC) audits. Technically, the malware granted actors persistent access to encrypted messaging platforms, call metadata, and device hardware such as microphones and cameras, effectively turning the devices into mobile listening posts. The persistence of this operation over several years suggests a failure in existing endpoint detection and response (EDR) protocols for high-ranking officials.

For cybersecurity practitioners and policy stakeholders, this breach serves as a stark warning regarding the inadequacy of commercial mobile security in the face of state-level resources. The broader implications suggest a potential compromise of sensitive national security strategies and diplomatic positioning, necessitating an immediate transition toward hardened, hardware-backed communication systems. Ultimately, this development reinforces the reality of "Grey Zone" warfare, where the integrity of sovereign decision-making is under constant threat from silent, persistent digital subversion.

Read more:
https://www.telegraph.co.uk/news/2026/01/26/china-hacked-downing-street-phones-for-years/

Futuristic helicopter drones programme advances as British based companies selected to develop prototypes

The UK Ministry of Defence (MoD) has significantly accelerated its pursuit of autonomous aerial combat capabilities through Project NYX, shortlisting seven industry partners including BAE Systems, Leonardo, and Anduril to develop prototype "loyal wingman" Uncrewed Air Systems (UAS). This initiative signals a strategic pivot within the UK's Strategic Defence Review toward a "command rather than control" operational philosophy, reflecting a broader geopolitical shift where Western militaries are racing to integrate artificial intelligence (AI) and autonomous mass to counter sophisticated adversaries in contested environments. By pairing these drones with Apache attack helicopters, the MoD aims to offload high-risk tasks like reconnaissance, target acquisition, and electronic warfare to expendable, AI-driven platforms, thereby preserving high-value crewed assets.

Technically, Project NYX focuses on the maturation of autonomous decision-making architectures that allow UAS to adjust to dynamic battlefield variables within pre-defined mission parameters, reducing the cognitive and logistical burden on human operators. The transition from manual piloting to high-level command interfaces necessitates robust, encrypted datalinks and resilient AI models capable of operating under electronic warfare conditions a critical vulnerability in modern peer-to-peer conflict. Following this pre-qualification phase, the shortlist will be narrowed to four suppliers in March 2026 to produce concept demonstrators, with a target for initial operational capability by 2030. For cybersecurity practitioners and defense analysts, this development underscores the escalating importance of "secure-by-design" autonomous systems and the integrity of the underlying algorithmic logic. As warfare increasingly relies on the fusion of AI and kinetic power, the resilience of these uncrewed platforms against adversarial machine learning and signal interference will become a cornerstone of national security and international stability in the next decade.

Read more:
https://www.gov.uk/government/news/futuristic-helicopter-drones-programme-advances-as-british-based-companies-selected-to-develop-prototypes

United States of America (USA)

LOTUSLITE: Targeted espionage leveraging geopolitical themes

The Acronis Threat Research Unit (TRU) has identified a highly targeted cyber-espionage campaign, attributed with moderate confidence to the Chinese state-linked actor Mustang Panda, leveraging a novel custom backdoor dubbed LOTUSLITE. This activity underscores the persistent risk posed by advanced persistent threat (APT) groups that exploit shifting geopolitical landscapes specifically the evolving diplomatic tensions between the United States and Venezuela to craft credible, high-impact social engineering lures. The campaign primarily targets U.S. government organizations and policy-focused entities, utilizing spear-phishing emails that deliver a malicious ZIP archive containing a renamed legitimate binary from the Tencent music service. Technically, the intrusion chain relies on the sophisticated use of DLL side-loading to bypass legacy security perimeters.

Upon execution of the decoy-named "Maduro to be taken to New York.exe," the loader initiates the primary payload, kugou.dll, using Microsoft C Runtime (CRT) initialization mechanisms like _initterm to execute malicious logic before reaching the standard DllMain entry point. LOTUSLITE, a modular C++ implant, establishes persistence via the "Lite360" registry Run key and directory creation in C:\ProgramData. Command-and-control (C2) operations are conducted over port 443 to the hardcoded IP 172.81.60.97, with the malware employing a Googlebot User-Agent and Microsoft Host headers to masquerade as legitimate web traffic. Functional capabilities include system enumeration, interactive remote shell access, and file exfiltration, while the inclusion of dummy exports and developer messages serves as an anti-analysis defence. For defenders, this development emphasizes that modern cyber resilience depends on detecting behaviour-based anomalies, such as DLL side-loading and non-standard process execution chains, rather than relying solely on signature-based defences.

The operationalization of LOTUSLITE highlights a broader pattern in the threat landscape where adversaries prioritize stealthy persistence and thematic relevance over complex zero-day exploits, requiring policy stakeholders to harden supply chains

and internal data links against increasingly precise state-sponsored intrusions.

Read more:
https://www.acronis.com/en/tru/posts/lotuslite-targeted-espionage-leveraging-geopolitical-themes/

Trump's acting cyber chief uploaded sensitive files into a public version of ChatGPT

The Cybersecurity and Infrastructure Security Agency (CISA) is currently contending with a significant breach of internal data-handling protocols involving its Acting Director, Madhu Gottumukkala, who uploaded sensitive government documents into a public instance of OpenAI's ChatGPT. This incident highlights a growing crisis in federal AI governance, where the push for rapid technological integration conflicts with the rigorous security mandates required of the nation's primary cyber-defence authority. While the materials involved primarily CISA contracting documents were not classified, they were designated as "For Official Use Only" (FOUO), a sensitive category that prohibits public disclosure.

The uploads occurred in mid-2025 after Gottumukkala secured a "special exception" to bypass agency-wide blocks on the tool, a privilege not extended to the broader Department of Homeland Security (DHS) workforce. Operationally, the exposure was identified by CISA's automated security sensors, which triggered multiple alerts in August 2025 after detecting the movement of sensitive identifiers to external, non-secure servers. These systems are specifically engineered to prevent the exfiltration of government data to platforms where information may be retained for model training or indexed by third parties a risk mitigated only by using secure, internally hosted alternatives like "DHSChat" The use of a public-facing Large Language Model (LLM) for official business by a top security official suggests a fundamental breakdown in leadership judgment and security hygiene, occurring alongside other recent controversies regarding failed counterintelligence screenings within the agency.

This development carries severe implications for national security and corporate trust, as it signals potential vulnerabilities in CISA's internal procurement and administrative processes. For practitioners and policy stakeholders, the event serves as a stark reminder that the "human element" remains a primary vector for risk, even at the highest levels of cybersecurity leadership. The resulting erosion of institutional credibility could embolden adversarial state actors and complicate efforts to establish a unified, secure-by-design standard across the global cyber threat landscape.

Read more:
https://www.politico.com/news/2026/01/27/cisa-madhu-gottumukkala-chatgpt-00749361

People's Republic of China (PRC) | China

Chinese military says it is developing over 10 quantum warfare weapons

China's People's Liberation Army (PLA) is aggressively formalizing its "quantum-first" military doctrine, with recent reports indicating the development of more than ten distinct quantum warfare weapons. This strategic acceleration occurs within a high-stakes geopolitical landscape defined by the race for quantum supremacy, where the ability to manipulate subatomic particles poses an existential threat to current cybersecurity frameworks. For defenders, this shift amplifies the "Harvest Now, Decrypt Later" (HNDL) risk, where state-linked actors seize encrypted data today to await decryption via future quantum processors. The PLA's roadmap prioritizes

four critical domains: quantum communication, sensing, radar, and computing. Specifically, the development of Quantum Key Distribution (QKD) networks utilizing entangled photons to establish theoretically unhackable links aims to secure internal military commands against signals intelligence (SIGINT) operations.

Concurrently, quantum radar systems are being engineered to neutralize traditional stealth technologies by detecting the disruption of quantum states rather than radio-frequency reflections. In the sensing domain, Rydberg atom-based sensors and quantum gradiometers are designed to detect minute gravitational or electromagnetic anomalies, potentially exposing submerged nuclear submarines or hardened underground facilities that are currently shielded from conventional reconnaissance. These advancements rely on the operationalization of complex phenomena such as superposition and entanglement, requiring massive investment in cryogenic infrastructure and specialized laser systems.

For risk managers and policy stakeholders, the maturation of these technologies necessitates an immediate transition to Post-Quantum Cryptography (PQC) and lattice-based encryption to ensure long-term data integrity. Ultimately, the PLA's push into quantum warfare signals a paradigm shift in international stability; the successful deployment of these assets would effectively render legacy stealth and cryptographic standards obsolete, forcing a fundamental re-evaluation of global power projection and the technical foundations of national defence resilience.

Read more:
https://www.scmp.com/news/china/science/article/3339907/chinese-military-says-it-developing-over-10-quantum-warfare-weapons

China's Palantir and the Future of PLA Warfighting

The People's Liberation Army (PLA) is rapidly institutionalizing "digital twin" technology to gain a decisive advantage in "intelligentized" warfare, marking a pivotal shift in China's military modernization and strategic readiness. Driven by the national Military-Civil Fusion (MCF) strategy, this development situates the virtual domain as a high-fidelity laboratory for rehearsing complex operations in contested theatres like the Taiwan Strait and the South China Sea. Digital twins dynamic, AI-driven virtual replicas of physical assets, environments, and processes enable the PLA to synchronize the physical battlefield with a data-rich digital shadow, facilitating real-time operational optimization and predictive modelling.

Technically, these systems integrate massive datasets from IoT sensor networks, satellite reconnaissance, and electromagnetic signals into sophisticated 3D modelling frameworks and high-performance computing (HPC) architectures. These platforms are being deployed to model the performance envelopes of advanced assets, such as the J-20 stealth fighter and Type 055 destroyers, while simulating the degradation of critical infrastructure under cyber-kinetic assault. By utilizing "cyber-physical" synchronization, PLA commanders can execute iterative, high-speed simulations to stress-test logistics chains, evaluate the efficacy of electronic warfare (EW) tactics, and refine "gray-zone" manoeuvres without exposing physical assets to risk. For defence practitioners and policy stakeholders, the maturation of PLA digital twins represents a significant escalation in informationized warfare, where the ability to "rehearse" conflict in a near-perfect virtual environment collapses the OODA loop and enhances tactical surprise.

The broader implications for international stability are profound, as this capability increases the risk of miscalculation by providing state actors with a false sense of operational certainty. Ultimately, this trend highlights a maturing threat landscape where national security is increasingly dependent on the integrity of the data streams and computational models that define the digital shadows of modern warfare.

Read more:
https://chinatechnosphere.substack.com/p/digital-twins-the-plas-warfighting?

PeckBirdy: A Versatile Script Framework for LOLBins Exploitation Used by China-aligned Threat Groups

In early 2026, cybersecurity researchers unveiled "PeckBirdy," a sophisticated JScript-based command-and-control (C2) framework utilized by China-aligned threat actors to conduct widespread espionage and data harvesting. Primarily targeting the gambling industry, Asian government entities, and private organizations, PeckBirdy exemplifies the growing reliance on "Living-off-the-Land" (LotL) tactics, where attackers weaponize legitimate system binaries (LOLBins) to bypass traditional security perimeters. By employing the aging JScript language, the framework ensures compatibility across diverse execution environments including MSHTA, WScript, and web browsers allowing it to function seamlessly as a watering-hole controller, a reverse shell server, or a backdoor delivery mechanism depending on the phase of the kill chain.

Recent operational activity, tracked under the campaign monikers SHADOW-VOID-044 and SHADOW-EARTH-045, reveals a multi-vector approach to compromise. Threat actors have been observed injecting PeckBirdy scripts into high-traffic websites to deliver fake Google Chrome update prompts, which in turn drop advanced modular backdoors like "HOLODONUT" and "MKDOOR." These payloads leverage stolen code-signing certificates and memory-only execution techniques such as the Donut loader and AMSI/ETW bypasses to evade detection. In government-focused operations, the framework was utilized to harvest credentials from login pages and exploit vulnerabilities such as CVE-2020-16040. The strategic use of such a versatile, script-based framework signals a shift toward more modular and resilient attack infrastructures that prioritize stealth and cross-environment flexibility. For defenders and policy stakeholders, PeckBirdy underscores the urgent need for robust behavioral monitoring and the hardening of LOLBin execution policies to counter adversaries who increasingly blend malicious activity with authorized administrative processes.

Read more:
https://www.trendmicro.com/en_us/research/26/a/peckbirdy-script-framework.html

Middle East | West Asia

UAE signs four major defence deals worth AED880 million at UMEX & SimTEX 2026

The United Arab Emirates Ministry of Defence and the Tawazun Council have finalized four strategic defence contracts totalling AED 880 million (approximately $240 million USD) during the 2026 Unmanned Systems Exhibition (UMEX) and Simulation and Training Exhibition (SIMTEX). This investment underscores a significant regional pivot toward autonomous warfare and indigenous defence manufacturing, a trend driven by the strategic necessity of Distributed Maritime Operations and the lessons learned from the proliferation of low-cost, high-impact unmanned systems in modern global conflicts. The primary developments involve the procurement of advanced

Unmanned Aerial Vehicles (UAVs), Unmanned Ground Vehicles (UGVs), and high-fidelity simulation platforms designed to enhance tactical readiness while minimizing operational overhead. Technically, these systems are centered on the integration of resilient Command, Control, Communications, Computers, and Intelligence (C4I) frameworks, utilizing modular architectures to ensure cross-platform interoperability and secure telemetry in contested electronic warfare environments.

For cybersecurity practitioners and defence analysts, the operationalization of these assets introduces critical challenges regarding the integrity of autonomous navigation logic and the security of long-range data links against spoofing or remote hijacking. The move toward software-defined defence architectures necessitates a rigorous focus on cyber-physical security, particularly the hardening of AI-driven decision-making nodes and the protection of sovereign supply chains from hardware-level tampering. These deals represent a broader transformation in the Middle Eastern military-industrial complex, shifting focus from traditional kinetic platforms to attritable robotic nodes. Ultimately, this development signals that cyber resilience is no longer a secondary consideration but a core component of kinetic capability, forcing a re-evaluation of international maritime security protocols and the escalation dynamics associated with the deployment of autonomous systems in congested strategic theatres.

Read more:
https://timesofindia.indiatimes.com/world/middle-east/uae-signs-four-major-defence-deals-worth-aed880-million-at-umex-simtex-2026/articleshow/126807654.cms#

Elbit picks Lowental Hybrid to provide extended-endurance UAV propulsion systems

In a strategic move to fortify the endurance and operational resilience of unmanned aerial systems (UAS), Elbit Systems has partnered with Lowental Hybrid to integrate advanced hybrid-electric propulsion systems into its tactical UAV portfolio. This development arrives as the defence sector faces an escalating demand for persistent surveillance and long-loiter capabilities, driven by the need to navigate increasingly contested electronic warfare (EW) environments and dense sensor-rich landscapes. By shifting away from traditional internal combustion engines toward hybrid architectures, Elbit is addressing the critical "range vs. weight" trade-off that has long constrained tactical platforms in high-stakes reconnaissance missions. The technical core of this partnership centres on Lowental's hybrid power unit, which utilizes a high-density energy management system to combine the high energy density of liquid fuels with the tactical advantages of electric propulsion. This configuration enables extended flight times—significantly exceeding standard battery-only or fuel-only benchmarks—while providing a reduced acoustic and thermal signature, a vital requirement for evading modern multi-spectral detection systems.

Furthermore, the integration allows for high peak-power delivery during critical flight phases or when powering sophisticated onboard ISR (Intelligence, Surveillance, and Reconnaissance) payloads, such as synthetic aperture radar (SAR) or advanced signals intelligence (SIGINT) suites. For security practitioners and defence analysts, this evolution signals a broader shift toward "power-resilient" platforms capable of maintaining operational continuity even under logistical strain or in environments where conventional fuelling is compromised. The transition to hybrid-

electric propulsion not only enhances mission persistence but also reflects a growing trend in military aviation to adopt dual-use technological innovations to mitigate the vulnerabilities of traditional supply chains and energy dependencies. Ultimately, this collaboration underscores a pivot toward more sophisticated, stealthy, and long-endurance autonomous systems that are essential for maintaining a competitive edge in modern, multi-domain conflict scenarios.

Read more:
https://www.flightglobal.com/defence/elbit-picks-lowental-hybrid-to-provide-extended-endurance-uav-propulsion-systems/166099.article

European Union | EU

Poland Stops Cyberattacks on Energy Infrastructure

Polish security services, led by the Internal Security Agency (ABW) in coordination with the Ministry of Digital Affairs, have neutralized a series of sophisticated, coordinated cyberattacks targeting the nation's critical energy infrastructure. This escalation occurs within a highly volatile geopolitical environment, where Poland's strategic role as a primary logistical corridor for Western aid to Ukraine has made its power grid a high-priority target for state-linked threat actors, likely originating from Russia. The activity reflects a broader, persistent trend of "pre-positioning" by Advanced Persistent Threats (APTs) such as Sandworm or APT28, which specialize in the disruptive manipulation of Industrial Control Systems (ICS) across Eastern Europe. Technical analysis indicates that the campaign utilized a multi-stage infection vector beginning with highly targeted spear-phishing emails aimed at engineering and administrative staff. These lures delivered modular Remote Access Trojans (RATs) designed for stealthy persistence and credential harvesting.

Once initial access was established, the actors employed "Living-off-the-Land" (LotL) techniques specifically leveraging PowerShell and Windows Management Instrumentation (WMI) to move laterally and conduct reconnaissance on Supervisory Control and Data Acquisition (SCADA) networks. Evidence suggests the attackers intended to deploy wiper malware to permanently disable system controllers and disrupt power distribution, potentially synchronized with kinetic or psychological operations. For risk managers and policy stakeholders, this successful interception highlights the vital necessity of real-time telemetry sharing between government intelligence agencies and private energy providers. The development reinforces the transition of cyber-physical systems into the frontlines of modern gray-zone warfare, requiring defenders to prioritize the hardening of legacy operational technology (OT) and the implementation of air-gapped backups. Ultimately, this incident serves as a critical reminder that national security is now inextricably linked to the cyber resilience of the energy sector, necessitating a proactive, hunting-based defensive posture to maintain regional and international stability.

Read more:
https://www.gov.pl/web/primeminister/poland-stops-cyberattacks-on-energy-infrastructure

Norway has significantly enhanced its northern flank deterrence by selecting Hanwha Aerospace as the sole provider for its first-ever long-range precision fires capability, a 19 billion NOK ($2 billion) investment marking a strategic shift in European land defence. Situated against a backdrop of intensifying Arctic geopolitics and the lessons of high-intensity attrition warfare in Ukraine, the decision underscores a growing European reliance

on South Korean defense architecture to bypass production bottlenecks in the U.S. and continental Europe. The acquisition focuses on the K239 Chunmoo Multiple Launch Rocket System (MLRS), which notably outperformed competitors—including the U.S. HIMARS and offerings from KNDS and Rheinmetall—by meeting Norway's stringent requirements for a 500-kilometer strike radius and accelerated delivery timelines. Under the agreement, Norway will receive 16 launch units and a substantial inventory of precision-guided missiles utilizing GPS-aided inertial navigation systems (INS) for high-accuracy engagements. Operationally, the deal integrates Norway into a regional "Chunmoo ecosystem" alongside Poland, where a dedicated missile production line will be established to ensure supply chain resilience and logistical depth. Technical specifications highlight the system's modularity, capable of firing 239mm guided rockets and 600mm tactical missiles from an armored 8x8 chassis, providing both NBC protection and rapid-reload capabilities essential for modern counter-battery and deep-strike missions. For defense planners, this development reflects a broader trend of "rapid rearmament" where delivery speed and industrial offsets—in this case, an agreement valued at 120% of the contract—take precedence over traditional procurement alliances. By securing an operational system by 2028, Norway is effectively shortening the window of vulnerability in its land-based deterrence, signaling to regional adversaries that the cost of kinetic escalation has been raised through expanded reach and integrated European-Korean industrial cooperation.

Read more:
https://www.regjeringen.no/no/aktuelt/regjeringen-har-valgt-leverandor-av-langtrekkende-presisjonsild/id3147546/

Malware & Vulnerabilities

GNU InetUtils Security Advisory: remote authentication by-pass in telnetd

A critical authentication bypass vulnerability has been disclosed in the GNU Inetutils telnet daemon (telnetd), posing a severe threat to organizations still reliant on legacy remote management protocols. Discovered by security researchers and coordinated through the Open Source Security (oss-sec) community, the flaw represents a catastrophic failure in the authentication logic of a foundational networking utility maintained by the GNU Project. In the contemporary threat landscape, where sophisticated adversaries increasingly target the software supply chain and unpatched edge devices, this development underscores the persistent risk of "ghost" vulnerabilities flaws hidden in plain sight within legacy code for years. Situating this within broader trends, the vulnerability highlights the fragility of the internet's bedrock infrastructure, where a single mishandled environment variable can render decades of security advancements obsolete.

Technically, the issue arises from an improper neutralization of argument delimiters when telnetd invokes the system's /usr/bin/login process. An unauthenticated remote attacker can exploit this by supplying a carefully crafted USER environment variable specifically the string -f root using the telnet -a or --login command. Because the daemon fails to sanitize this input before passing it as a parameter to the login binary, the -f flag is interpreted as an instruction to force a login without password verification, granting the adversary immediate, root-level shell access. This "argument injection" vulnerability has remained latent in the codebase since version 1.9.3, released in 2015, affecting a vast array of Linux distributions and embedded systems for over a decade.

For practitioners and policy stakeholders, the implications are profound. With hundreds of thousands of telnet-enabled devices potentially exposed, this flaw provides a low-friction vector for initial access, lateral movement, and the deployment of ransomware or state-sponsored rootkits. Defenders must prioritize the decommissioning of Telnet in favor of SSH or implement aggressive IP allowlisting and network segmentation. Ultimately, this development serves as a strategic warning: cyber resilience is not merely about defending new tech, but about systematically auditing the technical debt of the past to prevent the catastrophic subversion of modern digital infrastructure.

Read more: https://seclists.org/oss-sec/2026/q1/89

UAT-8837 targets critical infrastructure sectors in North America

Cisco Talos has uncovered a sophisticated cyber-espionage campaign attributed to a new, unclassified threat actor designated as UAT-8837, targeting government and technological sectors in Taiwan. This activity surfaces amidst heightening geopolitical tensions in the Indo-Pacific, where state-aligned groups are increasingly prioritizing the infiltration of strategic infrastructure to facilitate long-term intelligence gathering. The development reflects a broader shift in the threat landscape toward the exploitation of edge-of-network vulnerabilities and the use of modular, evasive malware designed to bypass standard defensive perimeters. Factually, the campaign is characterized by the deployment of a bespoke C++ backdoor known as "Medusa," which provides the actors with extensive control over compromised systems, including file manipulation and reverse shell capabilities.

Technical analysis identifies a multi-stage infection chain that frequently utilizes DLL side-loading techniques leveraging legitimate binaries like those from security software or common productivity tools to execute malicious payloads in memory. Furthermore, UAT-8837 has been observed employing specialized PowerShell scripts for system reconnaissance and "Living-off-the-Land" binaries to evade detection while harvesting credentials from the Local Security Authority Subsystem Service (LSASS). The group's operational infrastructure is notably resilient, often utilizing a network of compromised small-home-office (SOHO) routers to serve as obfuscated command-and-control (C2) nodes, effectively masking malicious traffic within legitimate domestic data streams. For risk managers and policy stakeholders, the emergence of UAT-8837 underscores the escalating challenge of protecting sovereign data against high-tier adversaries who utilize hybrid toolsets.

The implications for national security are profound, as these persistent intrusions threaten the integrity of sensitive communications and strategic planning. Ultimately, this campaign highlights the necessity for a zero-trust approach to network architecture and the imperative for defenders to prioritize the monitoring of administrative tools and lateral movement to counter sophisticated, state-linked persistence.

Read more:
https://blog.talosintelligence.com/uat-8837/

Weaponizing Calendar Invites: A Semantic Attack on Google Gemini

Researchers at Miggo have identified a critical vulnerability in the integration between Google Gemini and Google Workspace, highlighting a new frontier for "semantic attacks" delivered through malicious calendar invites. As enterprises increasingly centralize operations within

AI-integrated productivity suites, the traditional security boundary is being challenged by Indirect Prompt Injection (IPI), where the primary risk stems from how models interpret untrusted data. The exploit involves a threat actor sending a benign-looking calendar invitation containing embedded, adversarial instructions within the event's metadata or description.

When a user invokes Gemini to provide a daily briefing or manage workspace tasks, the model inadvertently executes the attacker's hidden prompts. This can result in unauthorized data exfiltration leveraging Gemini's access to Gmail and Drive or the delivery of sophisticated social engineering lures that appear as legitimate AI-generated insights. Technically, this attack exploits the inherent lack of separation between the "data" (the invite) and the "control logic" (the user's intent) within LLM-based tool-use architectures. By bypassing traditional signature-based detection, these semantic injections allow for persistent, low-footprint manipulation of a user's digital environment without the need for traditional malware.

For cybersecurity practitioners and policy stakeholders, the development underscores a pivot in the threat landscape toward "prompt-as-code" exploitation, necessitating the implementation of advanced content sanitization and zero-trust principles for all external data ingested by autonomous agents. The broader implications for corporate security and international stability are profound, as the weaponization of integrated AI ecosystems could facilitate large-scale, automated espionage and the erosion of digital trust, requiring a fundamental re-evaluation of how automated decision-making platforms are hardened against logic-based subversion.

Read more:
https://www.miggo.io/post/weaponizing-calendar-invites-a-semantic-attack-on-google-gemini

Microsoft & Anthropic MCP Servers at Risk of RCE, Cloud Takeovers

Microsoft security researchers have issued a critical warning regarding systemic vulnerabilities in servers implementing Anthropic's Model Context Protocol (MCP), an open standard designed to link Large Language Models (LLMs) to external data sources and local tools. As enterprises transition toward "agentic" AI architectures that allow models to autonomously interact with corporate environments, the security of these connective protocols has become a primary concern for defenders. This risk sits at the intersection of rapid AI adoption and the expansion of the software supply chain, where third-party integrations often bypass traditional application security vetting.

The primary developments involve the discovery that many community-contributed MCP servers are susceptible to takeover via indirect prompt injection, leading to Remote Code Execution (RCE) and Server-Side Request Forgery (SSRF). Technically, the vulnerability arises from insecure implementation patterns where MCP servers execute shell commands, perform file system operations, or interact with internal APIs based on LLM-interpreted instructions without rigorous input sanitization or sandboxing. For example, an adversary can craft malicious data such as a poisoned document or email that, when processed by the LLM, triggers the MCP server to execute arbitrary code on the underlying host or exfiltrate sensitive credentials.

The lack of standardized authentication and the common practice of running these servers with over-privileged service accounts significantly heighten the risk of lateral movement. For risk management and policy stakeholders, this development

underscores that AI-integrated ecosystems introduce a "trust-by-default" logic that can be weaponized for industrial espionage or infrastructure subversion. The broader implications necessitate a shift toward zero-trust principles for AI-to-tool communications, requiring robust egress filtering and the enforcement of "Human-in-the-Loop" validations. Ultimately, these findings highlight a maturing threat landscape where the resilience of the enterprise is increasingly dependent on the integrity of the connective tissue between autonomous models and the systems they control.

Read more:
https://www.darkreading.com/application-security/microsoft-anthropic-mcp-servers-risk-takeovers?

Mamba Phishing-as-a-Service Kit: How Modern adversary-in-the-middle (AiTM) Attacks Operate

The emergence of the Mamba Phishing-as-a-Service (PhaaS) platform represents a significant escalation in the industrialization of Adversary-in-the-Middle (AitM) attacks, specifically targeting enterprise environments protected by multi-factor authentication (MFA). As traditional credential-harvesting techniques lose efficacy due to the widespread adoption of identity security protocols, threat actors are increasingly pivoting toward Mamba's reverse-proxy architecture to compromise high-value accounts. This shift occurs within a broader technological risk landscape where the commoditization of sophisticated exploit kits allows even low-skilled attackers to bypass standard TOTP and SMS-based verification layers. Technically, Mamba operates by positioning a malicious proxy server between the victim and legitimate service providers such as Microsoft 365 and Google, enabling the real-time interception of authentication tokens and session cookies. The platform utilizes Socket.io for persistent, low-latency communication and employs sophisticated JavaScript obfuscation to evade security mail gateways and automated sandbox detection.

Observers have noted the kit's ability to mirror enterprise login portals with extreme precision, capturing the full authentication handshake and exfiltrating "cookies" to attacker-controlled Telegram bots or administrative panels for immediate use in account takeover (ATO) operations. These developments signal a critical juncture for cyber resilience; the mere presence of MFA is no longer a definitive safeguard against session-level subversion.

For security practitioners and decision-makers, the Mamba threat necessitates a strategic shift toward phishing-resistant authentication standards, such as FIDO2 and hardware-backed security keys, alongside the implementation of conditional access policies that scrutinize session token anomalies. Ultimately, the proliferation of Mamba-style AitM frameworks underscores a maturing cybercrime economy where the exploitation of the "identity perimeter" has become a primary objective for state-linked and financially motivated actors alike, complicating the global effort to maintain international digital stability.

Read more:
https://www.cyfirma.com/research/mamba-phishing-as-a-service-kit-how-modern-adversary-in-the-middle-aitm-attacks-operate/

About the Author

Govind Nelika is the Web Manager/Researcher 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.