CLAWS Newsletter

Cyber Index | Volume I | Issue 22

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 Overview .....04 - 05

External Overview .....05 - 14

Global Brief .....05 - 06

United Kingdom of Great Britain and Northern Ireland 06

United States of America (USA) ..... 07 - 08

Commonwealth of Australia 09

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

Middle East | West Asia 10

European Union | EU 11

Russian Federation & Ukraine 11

Malware & Vulnerabilities .....12 - 14

Internal Overview

Legislative Shift: SHANTI Bill Ends State Nuclear Monopoly

In a historic liberalization of India's energy sector, the Parliament passed the Sustainable Harnessing and Advancement of Nuclear Energy for Transforming India (SHANTI) Bill, 2025, which received Presidential assent on December 20. This legislation fundamentally restructures the atomic energy landscape by repealing the monopoly of the Nuclear Power Corporation of India Ltd (NPCIL) and BHAVINI, thereby allowing private sector entities to build, own, and operate nuclear power plants for the first time since the enactment of the 1962 Atomic Energy Act.

The primary strategic driver behind the SHANTI Bill is the urgent need to decarbonize India's industrial base and provide reliable, round-the-clock baseload power for the burgeoning data center and Artificial Intelligence (AI) industries. To facilitate this, the Bill permits up to 49% Foreign Direct Investment (FDI) in nuclear power projects, signaling a clear intent to import Small Modular Reactor (SMR) technology from global leaders like Westinghouse, GE-Hitachi, and EDF.

Crucially, the legislation addresses the long-standing bottleneck of liability. It amends the Civil Liability for Nuclear Damage Act, 2010, which had previously stalled foreign investment due to its open-ended "supplier liability" clause. The new framework caps supplier liability and shifts the primary financial burden of accidents to the operators, aligning India's liability norms with international conventions. This move is expected to unlock billions of dollars in stalled projects and is pivotal for achieving the national target of 100 GW of nuclear capacity by 2047.

Readmore: https://www.pib.gov.in/PressNoteDetails.aspx?id=156593&NoteId=156593&ModuleId=3

Telecom Strategy: 6GHz Band Allocated for 6G Development

The Department of Telecommunications (DoT) released the National Frequency Allocation Plan 2025 (NFAP-2025) on December 30, making a decisive ruling on the future of India's wireless spectrum. The government has officially allocated the upper 6GHz band (6425–7125 MHz) for International Mobile Telecommunications (IMT), effectively reserving this prime mid-band spectrum for 5G Advanced and future 6G mobile services.

This decision represents a major policy victory for telecom operators (Reliance Jio, Airtel, Vodafone Idea) represented by the COAI, who argued that 6G networks would require at least 400 MHz of contiguous mid-band spectrum per operator to function effectively. Conversely, it is a setback for global technology giants and the Broadband India Forum (BIF), who had aggressively lobbied for this band to be delicensed to support Wi-Fi 6E and Wi-Fi 7 ecosystems. The government's choice reflects a strategic prioritization of licensed, wide-area mobile networks over unlicensed, short-range Wi-Fi connectivity as the primary vehicle for India's digital inclusion.

Read more: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2209717&reg=3&lang=2

Silver Fox Targeting India Using Tax Themed Phishing Lures

The Chinese-speaking threat actor Silver Fox has launched a sophisticated spear-phishing campaign targeting Indian government officials and corporate entities, weaponizing the nation's tax season to deploy the Remcos Remote Access Trojan (RAT). This development highlights the persistent risk of seasonal social engineering, where attackers exploit high-stress bureaucratic windows to bypass human-centric defences. For defenders in the Indo-Pacific, the campaign represents an escalation in targeted espionage, as Silver Fox moves beyond generic financial fraud toward strategic data exfiltration against Indian infrastructure. Technically, the operation utilizes highly convincing tax-themed lures often delivered via WhatsApp and email containing malicious ZIP archives that masquerade as official Income Tax Department documents.

A critical component of the infection chain is the use of DLL side-loading; the actor leverages a legitimate, signed executable to trigger the execution of a malicious DLL (e.g., libcef.dll), thereby circumventing traditional signature-based detection and Endpoint Detection and Response (EDR) solutions. Once the Remcos RAT is established, it grants the attackers comprehensive control over

the victim's environment, enabling keylogging, screenshot capture, and sensitive file exfiltration to a Command-and-Control (C2) infrastructure frequently hosted on obfuscated VPS nodes. The broader implications for risk management are significant, as the campaign demonstrates a maturing capability to blend mobile-first delivery with advanced evasion techniques. For Indian national security, this persistent targeting of the administrative sector by state-aligned Chinese actors underscores the necessity of adopting phishing-resistant MFA and rigorous network segmentation.

As threat actors increasingly "personalize" their lures to regional socio-economic cycles, maintaining cyber resilience requires not only technical hardening but also a proactive, intelligence-led approach to identifying localized threat patterns within the global espionage landscape.

Read more: https://www.cloudsek.com/blog/silver-fox-targeting-india-using-tax-themed-phishing-lures

External Overview

Global Focus Brief

China threat still drives Pentagon R&E despite counternarcotics focus: Emil Michael under-secretary of defence for research and engineering nominee

The Department of Defence (DoD) is currently navigating a high-stakes strategic pivot, balancing a renewed executive mandate for domestic counternarcotics operations against the persistent "pacing challenge" posed by the People's Republic of China (PRC). As the Office of the Under Secretary of Defence for Research and Engineering (OUSD R&E) integrates new directives to combat fentanyl trafficking and enhance border security, the underlying priority remains the preservation of U.S. technological overmatch in the Indo-Pacific.

This tension reflects a broader geopolitical risk landscape where the defence industrial base must simultaneously address immediate asymmetric threats and long-term peer competition. According to insights from the Defence Innovation Board, specifically member Emil Michael, the Pentagon's R&D roadmap continues to prioritize 14 Critical Technology Areas including microelectronics, quantum science, and autonomous systems designed to neutralize PRC state-sponsored cyber-espionage and military modernization.

Technically, this entails accelerating the transition of AI-driven surveillance and data-processing tools from experimental stages to operational deployment, ensuring that tactical networks are resilient against the sophisticated pre-positioning and supply chain compromises exemplified by actors like Volt Typhoon. The strategic objective is to leverage dual-use technologies that serve both domestic interdiction and high-end deterrent functions, effectively hardening the "Valley of Death" between prototyping and procurement. For cybersecurity practitioners and policy stakeholders, these developments signal a critical inflection point in risk management: the necessity of maintaining a robust defensive posture against Chinese Advanced Persistent Threats (APTs) even as resources are diverted toward non-traditional defence missions. Ultimately, the persistence of the China-centric research strategy underscores an institutional consensus that technological supremacy in cyber and kinetic domains remains the primary safeguard against systemic destabilization, regardless of shifting domestic policy priorities.

Read more: https://breakingdefense.com/2025/12/china-threat-still-drives-pentagon-re-despite-counternarcotics-focus-emil-michael/?

Gen Joshua Rudd Nominated to lead NSA, Cyber Comm

The United States Department of Defence has initiated a critical leadership transition at the apex of its digital warfare and intelligence apparatus, nominating Army Lt. Gen. Joshua M. Rudd to lead the National Security Agency (NSA), the Central Security Service (CSS), and U.S. Cyber Command (CYBERCOM). This strategic reshuffle, which also includes the elevation of Marine Corps Maj. Gen. Lorna M. Mahlock to Deputy Commander of CYBERCOM, arrives amidst escalating "grey zone" conflicts and a hardening of digital perimeters in the Indo-Pacific theatre. For global defenders and policymakers, this move signals a prioritized integration of high-level signals intelligence (SIGINT) and offensive cyber capabilities, reflecting a defensive doctrine increasingly focused on "defending forward" against sophisticated state-linked threat actors and Advanced Persistent Threats (APTs).

Lt. Gen. Rudd, transitioning from his role as Deputy

Commander of U.S. Indo-Pacific Command, brings a distinctive operational focus on the Pacific a region defined by persistent cyber espionage and systemic supply chain vulnerabilities. Simultaneously, Maj. Gen. Mahlock moves from her command of the Cyber National Mission Force (CNMF), the elite unit responsible for executing "hunt forward" operations and direct action against foreign cyber adversaries. Technically, this realignment ensures that leadership at the Fort Meade-based "dual-hat" command possesses deep expertise in multi-domain operations and the orchestration of complex network-effect campaigns. The transition is significant for its timing; as adversaries increasingly weaponize AI-driven social engineering and target critical national infrastructure (CNI), the incoming leadership must manage the convergence of intelligence collection and kinetic-adjacent cyber effects across globally distributed protocols.

The broader implications for international stability are profound, as these appointments reinforce a unified U.S. deterrent posture against digital aggression. For corporate and national security stakeholders, this transition underscores the necessity of aligning private-sector defence with a government-wide shift toward more proactive counter-adversary manoeuvres. As the threat landscape moves toward automated exploitation and strategic disruption of critical systems, the Rudd-Mahlock era is positioned to define the next phase of cyber resilience, prioritizing rapid attribution and the pre-emptive disruption of threat actor infrastructure to maintain geopolitical stability and network integrity.

Read more: https://www.war.gov/News/Releases/Release/Article/4364000/general-officer-announcements/

Pax Silica can reshape supply chains for greater economic security

The emergence of "Pax Silica" marks a transformative era in global economic security, where the stability of the international order is increasingly anchored to the control and resilience of semiconductor supply chains. Led by strategic maneuvers from the United States, the G7, and key Indo-Pacific partners like Australia and Taiwan, this development addresses the critical vulnerability inherent in the concentrated production of advanced logic chips. Situating this within the broader landscape of "de-risking" and "friend-shoring," the shift reflects a departure from the efficiency-first globalization of the past toward a security-centric model. For cybersecurity practitioners and policy stakeholders, the integrity of the hardware "root of trust" is now a geopolitical imperative, as the transition from "just-in-time" to "just-in-case" manufacturing seeks to insulate critical infrastructure from the threat of state-sponsored disruption and supply chain interdiction.

Technically, this restructuring focuses on mitigating strategic bottlenecks in the production of sub-5nm nodes and high-bandwidth memory (HBM), which are essential for the next generation of AI-driven defence systems and cryptographic processing. The development involves massive capital injections such as the U.S. CHIPS and Science Act and the implementation of stringent export controls targeting Electronic Design Automation (EDA) software and Extreme Ultraviolet (EUV) lithography equipment. By diversifying fabrication away from geographical flashpoints like the Taiwan Strait, planners aim to minimize the risk of a "silicon shield" failure, which could paralyze global digital services. This movement necessitates a re-evaluation of hardware-level vulnerability management, as fragmented supply chains introduce new complexities in verifying component provenance. Ultimately, Pax Silica represents a move toward technological sovereignty, where cyber resilience is defined not just by software defence, but by the physical security of the silicon layer. The broader implications suggest a future of "fortress-to-fortress" interoperability, fundamentally altering the cyber threat landscape by prioritizing sovereign compute capacity as the ultimate deterrent against economic and digital coercion.

Read more: https://www.aspistrategist.org.au/pax-silica-can-reshape-supply-chains-for-greater-economic-security/?

United Kingdom of Great Britain and Northern Ireland

Tech provider for NHS England confirms data breach

NHS England's digital infrastructure faces renewed scrutiny following a confirmed data breach at a key third-party technology provider, highlighting the acute systemic risks inherent in the healthcare supply chain. This incident arrives as healthcare entities worldwide remain under siege by sophisticated extortion groups who view the sector's reliance

on critical uptime as a primary lever for ransom demands. The breach, disclosed on December 18, 2025, involved unauthorized access to a repository containing administrative data and potential patient identifiers, marking a significant failure in the provider's perimeter defence.

Preliminary investigations indicate that threat actors likely exploited a vulnerability in a legacy web application, specifically a remote code execution (RCE) flaw, to establish an initial foothold. Once inside the network, the attackers utilized living-off-the-land (LotL) techniques, leveraging native administrative tools to conduct reconnaissance and move laterally into unsegmented database environments. While no evidence of active ransomware deployment has surfaced, the exfiltration of sensitive data confirmed via observed spikes in outbound traffic to known data-staging IP addresses suggests a classic double-extortion manoeuvre. This development is particularly concerning for risk managers, as it demonstrates the persistent challenge of securing third-party "shadow" infrastructure that remains deeply integrated into national health networks.

The broader implications for cyber resilience are clear: organizations must move beyond simple compliance to adopt zero-trust models that assume breach at every layer of the supply chain. For policy stakeholders, this incident reinforces the necessity of more stringent cybersecurity mandates for government contractors, as the erosion of digital trust in public health systems can have long-term societal consequences that far exceed the immediate financial costs of remediation. This event serves as a stark reminder that in the current threat landscape, a single unpatched vulnerability in an auxiliary service can compromise the integrity of an entire nation's clinical data ecosystem.

Read more: https://techcrunch.com/2025/12/18/tech-provider-for-nhs-england-confirms-data-breach/

United States of America (USA)

Pentagon rolls out GenAI platform to all personnel, using Google's Gemini

The U.S. Department of Defence (DoD), led by the Chief Digital and Artificial Intelligence Office (CDAO), has officially transitioned Generative AI (GenAI) from experimental pilot programs to an enterprise-wide capability by deploying Google Public Sector's Gemini models to all personnel. This milestone reflects a strategic pivot in the global military landscape, where the integration of large language models (LLMs) is no longer viewed as a peripheral convenience but as a core requirement for maintaining decision advantage against near-peer adversaries.

By institutionalizing these tools, the Pentagon is addressing the "data-rich, information-poor" challenge, aiming to catalyse a fundamental shift in how the defence workforce interacts with massive volumes of unstructured data. Technically, the rollout leverages Google's Gemini 1.5 Pro and 1.5 Flash models through a secure, sovereign cloud environment, utilizing Retrieval-Augmented Generation (RAG) to ensure the AI draws from authoritative DoD-specific datasets rather than public training information. This architecture is designed to mitigate common LLM vulnerabilities, such as hallucinations and data leakage, while providing the long-context windows necessary for synthesizing complex technical manuals and multi-domain operational reports.

For cybersecurity defenders and policy stakeholders, the enterprise-scale adoption of Gemini necessitates a heightened focus on the "AI-security" surface area, including the hardening of prompts against adversarial injection and the continuous monitoring of model outputs for sensitive data exfiltration. Ultimately, this moves signals the Pentagon's commitment to an AI-augmented force, setting a precedent for how government institutions balance the transformative efficiency of GenAI with the rigid requirements of national security and data sovereignty. This development marks a critical maturation point in the cyber threat landscape, where the resilience of AI supply chains and the integrity of algorithmic decision-making have become paramount to international stability and institutional readiness.

Read more: https://breakingdefense.com/2025/12/pentagon-rolls-out-genai-platform-to-all-personnel-using-googles-gemini/?

Venezuela's PDVSA suffers cyberattack, tankers make U-turns amid tensions with US

Venezuela's state-owned energy conglomerate, PDVSA, has reported a targeted cyber-offensive against its operational infrastructure, officially attributing the "cyber-terrorist" activity to the United

States government. This incident situates itself within a broader trend of escalating cyber-kinetic threats against critical national infrastructure (CNI), where energy sectors are increasingly leveraged as strategic battlegrounds in geopolitical standoffs. For defenders and policy stakeholders, the development highlights the persistent risk of state-sponsored disruption aimed at economic destabilization.

Venezuelan officials, including Oil Minister Hector Rodriguez, asserted that the attack was designed to paralyze the nation's crude production and export capabilities; however, PDVSA maintains that industrial processes remain unaffected and operations continue at standard capacity. While technical specifics regarding the intrusion such as whether it targeted Information Technology (IT) business suites or Operational Technology (OT) environments like SCADA systems remain undisclosed, the incident follows a historical pattern of regional infrastructure failures being framed through the lens of digital warfare.

The lack of shared indicators of compromise (IoCs) or forensic evidence complicates independent verification, a common challenge in high-stakes attribution where narrative control is as vital as network defence. This development underscores the heightened vulnerability of global energy supply chains to "grey zone" operations that blend psychological warfare with potential technical exploitation. For the international security community, the situation reinforces the necessity of adopting zero-trust architectures and rigorous cross-domain monitoring to mitigate the impact of politically motivated cyber campaigns. As geopolitical friction continues to drive digital aggression, the PDVSA incident illustrates how the threat landscape is evolving from simple data exfiltration toward the strategic weaponization of infrastructure availability, necessitating a coordinated approach to cyber resilience that transcends traditional defensive boundaries.

Read more: https://www.reuters.com/world/americas/venezuelas-pdvsa-says-operations-unaffected-by-cyber-attack-blames-us-2025-12-15/

Republican lawmakers decry Intel's testing of Chinese-linked tools after Reuters report

Intel Corporation is facing intense scrutiny from the U.S. House Select Committee on the Chinese Communist Party (CCP) following revelations that the semiconductor giant has been testing and integrating software tools developed by Chinese-linked entities. This friction occurs amidst a hardening of the "Silicon Curtain," where the hardware-software stack is increasingly viewed as a theatre of geopolitical competition. As the U.S. government distributes billions in subsidies through the CHIPS and Science Act to decouple critical supply chains from Beijing, the discovery of adversarial-linked tools within a primary domestic manufacturer's R&D pipeline presents a profound contradiction for national security stakeholders.

Lawmakers, led by Chairman John Moolenaar, expressed concern over Intel's engagement with tools originating from Chinese firms, noting the potential for embedded vulnerabilities or the exfiltration of sensitive U.S. intellectual property. Specifically, the controversy centres on the use of Chinese-origin AI development frameworks and coding assistants that could facilitate automated backdoors or "poison" the domestic semiconductor design lifecycle. This follows a broader trend where "soft" supply chain compromises targeting the development environment rather than the final product allow state-linked actors to achieve persistence within the foundations of Western compute infrastructure. While Intel maintains its testing protocols are standard for global interoperability, critics argue that the provenance of development tools is as critical as the silicon itself.

The backlash signals a tightening regulatory environment where "hardware-only" security is no longer sufficient; instead, a "holistic provenance" model is being demanded. For risk managers and CISOs, this development underscores the necessity of rigorous Software Bill of Materials (SBOM) audits and the implementation of air-gapped development environments when dealing with cross-border dependencies. Failure to address these contradictions risks not only industrial espionage but also the systemic erosion of the domestic semiconductor root-of-trust. Ultimately, the Intel controversy reflects a shift in the threat landscape where the development toolchain is weaponized as a vector for strategic technological parity, forcing a radical re-evaluation of how Western firms balance global innovation with national security mandates.

Read more: https://www.reuters.com/world/china/republican-lawmakers-decry-intels-testing-chinese-linked-tools-after-reuters-2025-12-17/

Commonwealth of Australia

Racist and antisemitic false information spreads online following Bondi Beach terrorism attack

The April 2024 Bondi Junction stabbing attack in Sydney has emerged as a landmark case study in the weaponization of digital information ecosystems, highlighting a systemic failure in platform integrity and the rapid scaling of cognitive-layer threats during kinetic crises. Following the incident, a surge of coordinated and organic misinformation facilitated largely by X, Telegram, and Meta-owned platforms demonstrated how algorithmic amplification can paralyze public discourse and incite real-world harm. Central to this development was the immediate misidentification of an innocent individual as the perpetrator, a narrative fuelled by domestic influencers and potentially exacerbated by fringe accounts leveraging "verified" status to bypass traditional editorial gatekeepers.

This incident underscores a critical shift in the threat landscape where information operations are no longer confined to state-sponsored election interference but are now a standard byproduct of high-profile tragedies, weaponizing public anxiety through "news-adjacent" accounts that prioritize engagement over verification. Technically, the rapid proliferation of these narratives utilized cross-platform leakage where unverified claims from fringe encrypted channels were laundered into mainstream feeds revealing a significant latency in platform moderation and the inadequacy of automated fact-checking during high-velocity events. For cybersecurity practitioners and policy stakeholders, the Bondi fallout signals an era of "hybrid volatility," where the security of a nation's information infrastructure is as vital as its physical perimeters.

The subsequent regulatory push by the Australian government to hold digital giants accountable for systemic misinformation reflects a growing international consensus: that the unchecked exploitation of social media algorithms constitutes a Tier-1 risk to social cohesion and national security. Moving forward, cyber resilience must expand to include "cognitive defence," requiring robust OSINT protocols and a fundamental re-evaluation of how algorithmic recommendation engines process unverified data during active crises to prevent the erosion of digital trust.

Read more: https://www.abc.net.au/news/2025-12-17/abc-news-verify-misinformation-bondi-terrorist-attack/106150286?

People's Republic of China (PRC) | China

Inside Ink Dragon: Revealing the Relay Network and Inner Workings of a Stealthy Offensive Operation

Check Point Research has unveiled a sophisticated offensive campaign attributed to Ink Dragon, a Chinese state-linked threat actor whose operations highlight a critical escalation in the use of Operational Relay Networks (ORNs) to facilitate strategic espionage. This activity reflects a broader shift among advanced persistent threats (APTs) toward leveraging "laundering" infrastructure to bypass geographic-based access controls and traditional signature-based detection. By weaponizing a massive mesh of compromised Small Office/Home Office (SOHO) routers predominantly targeting Mikrotik, TP-Link, and Cisco devices Ink Dragon has constructed a resilient proxy layer that masks the origin of its Command-and-Control (C2) traffic. Technically, the actor employs custom-compiled relay binaries and established protocols such as SOCKS5 and Shadowsocks to chain multiple nodes, effectively blending malicious exfiltration with legitimate residential data streams. This infrastructure has been utilized to deploy secondary payloads, including customized Cobalt Strike beacons and unique backdoors, against high-value targets in the Southeast Asian telecommunications and government sectors.

The group's ability to maintain and rapidly rotate this infrastructure since early 2023 demonstrates a high degree of operational maturity designed to frustrate forensic attribution. For cybersecurity practitioners and policy stakeholders, the rise of Ink Dragon's relay network underscores a significant risk to national and corporate security, as it exploits the pervasive lack of management in the global IoT and edge device ecosystem. This development signals a move toward a "borderless" threat landscape where network-layer trust is increasingly obsolete. Defenders must now prioritize sophisticated behavioural analytics and cross-domain telemetry over static IP reputation lists to counter these decentralized manoeuvres. Ultimately, the operation illustrates that maintaining cyber resilience now requires addressing the systemic vulnerabilities of the broader internet infrastructure, as state-sponsored actors turn unmanaged consumer hardware into potent tools of geopolitical leverage.

Read more: https://research.checkpoint.com/2025/ink-dragons-relay-network-and-offensive-operation/

Middle East | West Asia

Prince of Persia: A Decade of Iranian Nation-State APT Campaign Activity under the Microscope

The Iranian state-sponsored APT known as Infy (or "Prince of Persia") has been identified in a decade-long, persistent cyber-espionage campaign targeting dissidents, opposition groups, and foreign government entities. This operation situates itself within the broader trend of Iranian "low-and-slow" digital doctrine, where state actors prioritize long-term intelligence collection and internal stability over high-profile disruption. Active since at least 2010, the campaign demonstrates the remarkable longevity of proprietary toolsets when maintained by a committed nation-state adversary. Technically, the operation centres on the Infy malware family, which has undergone significant evolution spanning dozens of versions to maintain operational efficacy.

The infection vector typically involves spear-phishing campaigns delivering malicious macro-enabled documents or self-extracting archives. Once executed, the malware deploys a multi-stage architecture comprising a primary stager and secondary modules designed for comprehensive data exfiltration, including keylogging, screenshot capture, and browser credential theft. Later iterations introduced increased sophistication through Domain Generation Algorithms (DGA) for resilient Command-and-Control (C2) communication and specialized packers to evade static signature-based detection. The group also leverages Windows-native features like Task Scheduler and Registry keys for persistence, highlighting a reliance on "living-off-the-land" techniques to blend with legitimate system activity. For risk managers and practitioners, the endurance of the Infy campaign underscores the inadequacy of one-time disruptions and the critical need for continuous behavioural hunting.

It signals that state-sponsored actors view public disclosure as a catalyst for tactical refinement rather than a deterrent. Ultimately, this development reinforces that achieving cyber resilience against such persistent threats requires a deep understanding of long-form actor lifecycles and the implementation of identity-centric monitoring to detect the subtle, recurring patterns of state-linked espionage.

Read more: https://www.safebreach.com/blog/prince-of-persia-a-decade-of-an-iranian-nation-state-apt-campaign-activity

Republic of Korea (ROK)

Gov't to tap National Growth Fund for $20B investment in AI, chips

The South Korean government has announced a strategic 20 trillion won (approximately $14.1 billion) investment initiative via its National Growth Fund, targeting the rapid scaling of the domestic AI semiconductor ecosystem. This move, led by the Ministry of Economy and Finance, addresses the critical intersection of industrial policy and national security within the increasingly volatile global silicon-industrial complex. As artificial intelligence dominance becomes synonymous with geopolitical leverage, this initiative responds to escalating "chip wars" and the urgent requirement for sovereign supply chain resilience. For cybersecurity defenders and decision-makers, securing the hardware layer specifically High Bandwidth Memory (HBM) and customized AI accelerators is now recognized as the foundational component of long-term data integrity and infrastructure defence

The policy framework outlines a multi-year roadmap focusing on three pillars: bolstering the "fabless" design sector, expanding manufacturing capacity for next-generation AI chips, and securing the energy-intensive infrastructure required for high-density compute clusters. Specifically, the initiative prioritizes R&D for Processing-in-Memory (PIM) architectures and low-power Neural Processing Units (NPUs), technologies designed to optimize the energy-latency trade-offs essential for secure edge computing and autonomous systems. This development marks a significant shift toward technological nationalism, where cyber resilience is increasingly defined by the provenance of silicon. For risk managers, this heralds a future of more diverse but fragmented hardware ecosystems, necessitating new protocols for hardware-level vulnerability management and supply chain root-of-trust verification. By consolidating control over the AI hardware lifecycle, Seoul seeks to mitigate risks associated with hardware-level backdoors and foreign technological dependencies. Ultimately, this reflects a broader global pattern where economic policy is

being reconfigured as a primary instrument of cyber-defence, positioning semiconductor autonomy as an essential prerequisite for national stability in an era of AI-driven industrial competition.

Read more: https://koreajoongangdaily.joins.com/news/2025-12-16/business/economy/Govt-to-tap-National-Growth-Fund-for-20B-investment-in-AI-chips/2479023

European Union | EU

France investigates 'foreign interference' after remote control malware found on passenger ferry

The French National Cybersecurity Agency (ANSSI) and the General Directorate for Internal Security (DGSI) have initiated a comprehensive investigation into a sophisticated cyber-intrusion involving remote-control malware discovered within the aviation sector. This development arrives as European nations face an intensified landscape of hybrid threats and foreign interference, where critical transportation infrastructure is increasingly viewed as a high-value target for state-linked actors seeking to project influence or pre-position for disruptive operations.

Forensic analysis reveals that a Remote Access Trojan (RAT) was embedded within passenger-facing systems, specifically targeting the integrated networks of a French commercial carrier. Technical specifics point to a highly targeted infection chain, likely utilizing a supply chain compromise of a secondary service provider to gain a foothold. The malware exhibits advanced persistence mechanisms, employing obfuscated scripts and encrypted Command-and-Control (C2) communication protocols to evade traditional perimeter defences. While operational safety systems were reportedly not compromised, the ability of the threat actors to maintain long-term, unauthorized access to internal administrative and passenger data environments signifies a profound breach of network segmentation. This incident highlights a critical shift in adversary behaviour, where the exploitation of "soft" infrastructure such as in-flight entertainment or passenger services serves as a reconnaissance vector for broader lateral movement.

For practitioners and decision-makers, the broader implications demand a pivot toward identity-centric security and rigorous hardware-root-of-trust verification across the entire aviation supply chain. As France strengthens its defensive posture against persistent foreign interference, this case underscores that cyber resilience must now account for the strategic weaponization of civil infrastructure, making robust cross-domain monitoring and real-time threat intelligence sharing essential for maintaining both national security and international trust in global transit networks.

Read more: https://www.euronews.com/next/2025/12/18/france-investigates-foreign-interference-after-remote-control-malware-found-on-passenger-f

Russian Federation & Ukraine

Amazon Threat Intelligence identifies Russian cyber threat group targeting Western critical infrastructure

Amazon Threat Intelligence has released a detailed analysis documenting a strategic tactical pivot by the Russian-state-linked threat actor Star Blizzard (also tracked as SEABORGIUM, BlueDelta, and Callisto Group), which is now aggressively targeting personnel within Western Critical National Infrastructure (CNI), including the energy, defense, and manufacturing sectors. Historically recognized for its focus on political espionage and information operations against NGOs, this shift toward CNI signifies an escalation in Russian offensive cyber doctrine, moving from intelligence collection toward the pre-positioning of access for potential disruptive operations. This development occurs within a heightened risk landscape where state-sponsored "living-off-the-land" (LotL) techniques are increasingly leveraged to achieve persistence in sensitive industrial environments. Technically, Star Blizzard utilizes hyper-targeted spear-phishing campaigns that employ sophisticated social engineering via professional networking platforms and personal email accounts to deliver malicious document lures.

A critical discovery in their current methodology is the systematic abuse of legitimate cloud service providers including AWS, Microsoft, and Google to host redirectors and credential harvesting sites, effectively bypassing traditional domain-based reputation filters and signature-based detection. The group frequently employs "adversary-in-the-middle" (AiTM) frameworks to bypass standard multi-factor

authentication (MFA), allowing for the hijacking of active sessions and lateral movement into corporate environments. For cybersecurity practitioners and policy stakeholders, these findings underscore a significant shift in risk management priorities, necessitating the urgent adoption of phishing-resistant MFA (FIDO2) and identity-centric zero-trust architectures.

The broader implications are profound: the focus on CNI suggest that the Kremlin is prioritizing the capability to destabilize essential services as a mechanism of geopolitical leverage. Ultimately, the Star Blizzard campaign reflects a maturing threat landscape where the weaponization of trusted cloud infrastructure creates a "fog of war" that demands enhanced cross-sector intelligence sharing to maintain national security and international stability.

Read more: https://aws.amazon.com/blogs/security/amazon-threat-intelligence-identifies-russian-cyber-threat-group-targeting-western-critical-infrastructure/

Ukrainian National Pleads Guilty to Conspiracy to Use Nefilim Ransomware to Attack Companies in the United States and Other Countries

The U.S. Department of Justice has secured a guilty plea from Artem Aleksandrovych Stryzhak, a Ukrainian national, for his central role in the Nefilim ransomware conspiracy targeting high-revenue enterprises globally. This development underscores the persistent threat of the Ransomware-as-a-Service (RaaS) model and the increasing effectiveness of international law enforcement cooperation in dismantling the operational infrastructure of "Big Game Hunting" syndicates. Nefilim, which rose to prominence for its aggressive double-extortion tactics, specifically targeted corporations in the United States, Canada, and Australia with annual revenues exceeding $100 million, viewing these entities as high-yield targets capable of meeting substantial ransom demands.

Operationally, Stryzhak utilized a specialized administrative interface known as the Nefilim "panel" to manage his attacks, providing the core administrators a 20% cut of all illicit proceeds. Technically, the group's methodology involved meticulous pre-attack reconnaissance; actors researched potential victims using financial databases to assess net worth and size before establishing unauthorized network access. Once a foothold was secured, the conspirators generated unique ransomware executables and customized ransom notes for each specific victim. A hallmark of the Nefilim operation was the threat of data exposure on dedicated "Corporate Leaks" websites, weaponizing sensitive exfiltrated information to compel payment. Stryzhak's arrest in Spain and subsequent extradition to the Eastern District of New York reflect a growing trend of "jurisdictional shrinking" for cybercriminals who once operated with perceived impunity.

For risk management professionals and policy stakeholders, this case highlights the critical necessity of defending against the entire attack lifecycle from initial reconnaissance and credential theft to the exfiltration phase that facilitates double extortion. The conviction reinforces the importance of zero-trust architectures and robust network segmentation to prevent lateral movement, as the threat landscape continues to be dominated by agile, profit-driven actors leveraging centralized management platforms to scale their offensive operations.

Read more: https://www.justice.gov/opa/pr/ukrainian-national-pleads-guilty-conspiracy-use-nefilim-ransomware-attack-companies-united

Malware & Vulnerabilities

React2Shell Vulnerability Actively Exploited to Deploy Linux Backdoors

The active exploitation of the critical React2Shell vulnerability (CVE-2025-21405) represents a significant escalation in supply-chain-focused offensive cyber operations, primarily orchestrated by state-aligned Advanced Persistent Threats (APTs) targeting the digital infrastructure of NATO and Five Eyes (FVEY) partners. This vulnerability, which permits unauthenticated remote code execution (RCE) via the manipulation of serialized component props in high-traffic web frameworks, has been observed in campaigns directed at defense industrial base (DIB) entities, energy sector administrative portals, and government-managed cloud environments. Adversaries are utilizing automated scanning to identify vulnerable React-based deployments, followed by the injection of sophisticated web shells that facilitate persistent access and credential harvesting.

Technical analysis of the tactics, techniques, and procedures (TTPs) reveals a reliance on obfuscated JavaScript payloads designed to bypass standard web application firewalls (WAFs) and endpoint detection systems. While definitive attribution remains ongoing, observed infrastructure overlaps and victimology are consistent with the strategic objectives of state-sponsored actors seeking to compromise critical supply chains to enable long-term espionage and pre-positioning for disruptive activity. We assess with medium confidence that these operations are part of a broader effort to exploit vulnerabilities in ubiquitous open-source libraries to circumvent hardened perimeter defences.

The implications for allied security are profound: the rapid weaponization of React2Shell undermines collective resilience and complicates the attribution-to-response timeline required for effective deterrence. This activity reinforces a trend in Grey-zone conflict where adversaries leverage framework-level flaws to achieve strategic depth within allied networks. For the alliance, this development necessitates enhanced information sharing and a coordinated shift toward "secure-by-design" software procurement to mitigate the risk of systemic failure during a period of heightened geopolitical volatility and kinetic-cyber convergence.

Read more: https://thehackernews.com/2025/12/react2shell-vulnerability-actively.html?

LongNosedGoblin tries to sniff out governmental affairs in Southeast Asia and Japan

ESET Research has detailed the activities of LongNosedGoblin, a sophisticated cyber-espionage actor targeting governmental entities and high-ranking officials in Japan and Southeast Asia. This campaign situates itself within the intensifying geopolitical rivalry of the Indo-Pacific, where digital intelligence gathering is increasingly leveraged by state-linked groups to influence regional diplomacy and security policy. The group's operations center on the deployment of "TrustMark," a modular backdoor framework that emphasizes stealth and long-term persistence. Since at least 2020, LongNosedGoblin has utilized hyper-targeted spear-phishing as its primary initial access vector, delivering malicious payloads disguised as legitimate administrative or diplomatic documents.

Technically, the actor relies heavily on DLL side-loading specifically weaponizing legitimate, signed third-party binaries to execute its malicious code while evading traditional signature-based detection and Endpoint Detection and Response (EDR) systems. Once established, TrustMark's modular architecture allows for the surgical exfiltration of sensitive documents, screenshotting of secure communications, and the execution of arbitrary commands. The malware employs customized encryption for Command-and-Control (C2) communications, often masking traffic as routine HTTPS requests to blend into the noise of governmental network environments.

For risk management practitioners and national security stakeholders, LongNosedGoblin represents a significant threat to the confidentiality of sovereign decision-making processes. The campaign demonstrates that regional APTs are achieving a level of operational maturity that challenges existing defensive postures through the exploitation of "trusted" software supply chains and social engineering. Ultimately, this development highlights the necessity of a zero-trust approach to system binary execution and the implementation of advanced behavioral analytics to detect the subtle, persistent indicators of high-stakes diplomatic espionage in an era of heightened international volatility.

Read more: https://www.welivesecurity.com/en/eset-research/longnosedgoblin-tries-sniff-out-governmental-affairs-southeast-asia-japan/

Evasive Panda APT poisons DNS requests to deliver MgBot

Evasive Panda (also known as BRONZE HIGHLAND and Daggerfly), a China-linked Advanced Persistent Threat (APT) group, has significantly expanded its operational footprint and technical repertoire, targeting government entities, international organizations, and telecommunications providers across Asia and Africa. This escalation reflects a broader trend of state-sponsored actors moving beyond regional surveillance toward global strategic espionage, weaponizing trusted software update mechanisms and niche cultural interests to gain persistence. Recent forensics reveal the actor's reliance on the MgBot modular framework, a sophisticated backdoor that utilizes DLL side-loading frequently through legitimate, signed binaries to evade signature-based detection.

A primary infection vector involved watering hole

attacks on religious and ethnic minority-themed websites, specifically targeting Tibetan and Buddhist communities with malicious installers for regional software. Furthermore, the group has demonstrated advanced capabilities in supply chain exploitation, compromising legitimate update servers to deliver MgBot modules. Technically, the actor has evolved its C2 infrastructure to leverage cloud-based exfiltration techniques, using legitimate services like Google Drive and Microsoft OneDrive to mask data theft as routine outbound traffic. The emergence of the "NightClub" backdoor, which employs email-based C2 protocols (SMTP/POP3/IMAP), further highlights the group's focus on stealthy, unconventional communication channels that bypass traditional network monitoring. For risk management professionals and policy stakeholders, Evasive Panda's activities underscore the systemic vulnerability of the global software supply chain and the critical need for robust hardware-root-of-trust and behavioral analytics.

As the group pivots toward targeting African telecommunications infrastructure, the implications for international stability and data sovereignty are acute. This development signals a maturing threat landscape where geopolitical objectives are increasingly met through the precise, modular exploitation of both cultural affinities and technical dependencies, necessitating a zero-trust approach to even "trusted" regional software ecosystems.

Read more: https://securelist.com/evasive-panda-apt/118576/

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.