CLAWS Newsletter

Cyber Index | Volume II | Issue 01

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

Transparent Tribe Launches New RAT Attacks Against Indian Government and Academia

Transparent Tribe (APT36), a prolific state-sponsored threat actor linked to Pakistan, has intensified its cyber espionage operations against Indian governmental, academic, and strategic sectors through the deployment of a sophisticated, multi-stage malware delivery chain. Situated within the volatile geopolitical landscape of South Asia, these campaigns underscore the adversary's commitment to refining its toolkit to circumvent increasingly robust regional defences.

The latest activity involves spear-phishing emails containing ZIP archives that harbor weaponized Windows shortcut (LNK) files. These files masquerade as legitimate PDF advisories including one notably mimicking a National Cyber Emergency Response Team of Pakistan (PKCERT) document to lure victims into execution. Technically, the infection process leverages the Living-off-the-Land (LotL) binary mshta.exe to execute memory-resident HTML Application (HTA) scripts, thereby minimizing the malware's file-system footprint. A distinguishing feature of this campaign is its adaptive persistence mechanism, which dynamically alters its installation path and execution method based on the presence of specific antivirus solutions such as Kaspersky, Quick Heal, or Avast.

The core payload, a Delphi-based DLL RAT, facilitates a comprehensive suite of espionage capabilities, including file exfiltration, remote shell access via cmd.exe, and screen capture. To further evade network-level detection, the malware utilizes reversed endpoint strings, such as /retsiger (register) and /taebtraeh (heartbeat), for communication with command-and-control (C2) infrastructure like dns.wmiprovider[.]com. Simultaneously, reports indicate reciprocal activity from Indian-linked actors like Patchwork, who are utilizing the StreamSpy trojan against Pakistani defense targets. For defenders and policy stakeholders, these developments highlight the shifting nature of regional cyber conflict, where the reliance on memory-only execution and AV-aware persistence necessitates a transition from static signature-based defense to advanced behavioral analysis and rigorous identity-centric security architectures to maintain long-term cyber resilience.

Read more: https://thehackernews.com/2026/01/transparent-tribe-launches-new-rat.html?

External

Global Focus Brief

DARPA Seeks Universal Translator Between Different Kinds of Quantum Computer

The Defence Advanced Research Projects Agency (DARPA) has launched a strategic initiative to bridge the widening gap between disparate quantum computing architectures by developing a "universal translator" capable of cross-platform algorithmic execution. As the global race for quantum supremacy accelerates, the lack of standardization across hardware modalities including superconducting circuits, trapped ions, and neutral atoms presents a significant bottleneck for both national security and industrial applications. This fragmentation currently necessitates that quantum software be painstakingly "hand-tuned" for specific hardware gate sets and qubit connectivity topologies, creating a brittle ecosystem where strategic progress is siloed within individual hardware wins. DARPA's objective is to create an automated compilation and transpiration framework that abstracts high-level quantum circuits from their underlying physical implementations.

Technically, this involves mapping logical operations to architecture-specific physical gates while optimizing for varying connectivity constraints, such as the nearest-neighbour limitations of superconducting chips versus the all-to-all connectivity of ion traps. By managing architecture-specific noise profiles and error-handling requirements through this middleware layer, the program aims to ensure that cryptographically relevant algorithms and complex simulations can be ported seamlessly across an evolving hardware landscape. For defenders and strategic decision-makers, this development signals a critical shift toward a software-defined quantum future, mitigating the risks of hardware lock-in and long-term technical debt in the lead-up to the post-quantum era. The success of such a framework would enhance national cyber resilience by ensuring that critical defence applications remain operational regardless of which physical modality ultimately

scales, thereby stabilizing the technological risk landscape during a period of intense geopolitical competition and rapid cryptographic transition.

Read more: https://www.mitchellaerospacepower.org/darpa-seeks-universal-translator-between-different-kinds-of-quantum-computer/

Musk's AI tool Grok will be integrated into Pentagon networks, Hegseth says

The integration of xAI's "Grok" large language model into the United States Department of Defense (DoD) unclassified and classified networks marks a paradigm shift in the military's adoption of generative artificial intelligence for national security operations. Announced by Defense Secretary Pete Hegseth, this initiative forms the centerpiece of a newly unveiled "AI acceleration strategy" aimed at dismantling bureaucratic barriers and ensuring American dominance in algorithmic warfare. This development arrives amid a high-stakes technological risk landscape where "sovereign AI" is increasingly viewed as a critical component of state power, following the DoD's earlier selection of Google's Gemini to power its internal platform, GenAI.mil. Under the new strategy, the Chief Digital and Artificial Intelligence Office (CDAO) will exercise authority to enforce "data decrees," making mission-critical data available across federated IT systems for rapid AI exploitation.

While the $200 million multi-contract award involving xAI, OpenAI, Anthropic, and Google underscores a commitment to agentic AI workflows, the deployment of Grok which has recently faced scrutiny for generating sexualized imagery and unfiltered algorithmic outputs introduces significant technical and reputational risks to the defense ecosystem. For practitioners and decision-makers, the reliance on commercially developed models within sensitive environments necessitates rigorous auditing of training data integrity and defensive posture against adversarial machine learning, such as prompt injection and data poisoning. Furthermore, the move highlights a growing trend toward the "privatization" of defense capabilities, where the reliability of state intelligence increasingly hinges on the safety guardrails and ethical standards of private-sector partners. Ultimately, the successful integration of these tools into mission systems will define the future of cyber resilience and international stability, as the boundary between commercial innovation and military-grade capability continues to dissolve.

Read more: https://www.theguardian.com/technology/2026/jan/13/elon-musk-grok-hegseth-military-pentagon

Diffraqtion's quantum camera for space apps draws $4.2M round

Diffraction, a pioneer in quantum-enhanced sensing, has secured a $4.2 million seed funding round to accelerate the operationalization of its specialized quantum camera technology for space-based applications. This development arrives at a critical juncture in the "New Space" race, where the convergence of orbital congestion and heightening geopolitical tensions has made Space Domain Awareness (SDA) a top-tier priority for national security and commercial operators. Traditional satellite imaging is increasingly constrained by classical diffraction limits and noise interference; however, Diffraction's approach leverages quantum-correlated photon detection to achieve super-resolution imaging and high-sensitivity detection in extreme low-light environments. For defenders, this technology provides a vital capability to identify, characterize, and monitor "silent" or non-cooperative orbital assets that would remain obscured by conventional optical sensors.

Technically, the platform utilizes diffractive quantum imaging (DQI) to bypass the Rayleigh criterion, allowing for the resolution of fine-scale structural details on distant satellites even under suboptimal signal-to-noise ratios. By integrating these sensors into the satellite infrastructure, decision-makers can achieve near-real-time verification of orbital anomalies, significantly mitigating the risk of undetected "grey-zone" activities or proximity-based cyber-physical threats in space. The broader implications for international stability are significant: as the orbital environment becomes increasingly transparent to quantum-enabled surveillance, the potential for verifiable attribution grows, potentially deterring clandestine operations against critical space infrastructure.

This shift toward quantum-native sensing marks a departure from legacy observation methods and

underscores a larger trend where the security of the high frontier is defined by the precision of its data pipelines. For practitioners and policy stakeholders, Diffraction's progress signals that the "quantum edge" is moving from the laboratory to the operational tactical environment, necessitating a recalibration of how orbital risks are assessed and managed in a contested celestial domain.

Read more: https://www.fiercesensors.com/sensors/diffraqtions-quantum-camera-space-apps-draws-42m-round

Doomsday for Cybercriminals — Data Breach of Major Dark Web Forum

The cybercriminal underground is reeling following a catastrophic data breach of BreachForums, the preeminent successor to RaidForums and a central clearinghouse for illicit data sales and black-hat activity. On January 9, 2026, a database containing 323,986 user records was leaked via the shinyhunte[.]rs domain, an act of "re-victimization" that exposes the identities and operational details of a global network of threat actors. This event occurs amidst a volatile landscape where "The Com" ecosystem—a decentralized, youth-led collective specializing in SIM-swapping and corporate extortion—has increasingly fractured under both international law enforcement pressure and internal betrayal. The leaked MySQL dump, specifically the hcclmafd2jnkwmfufmybb_users table, points to a compromise of the MyBB forum software, likely through a previously rumored zero-day vulnerability or a severe server misconfiguration.

The exposed data includes administrative metadata, argon2i hashed passwords, PGP keys, and last-login IP addresses, providing a definitive resource for deanonymization by security researchers and government agencies. A central figure in this disruption, an actor using the pseudonym "James," accompanied the leak with a nihilistic manifesto targeting global power structures, including the FBI and major technology corporations, further complicating the attribution and motive behind the breach. For defenders and intelligence analysts, this "Doomsday" event serves as a critical inflection point in the dark web lifecycle, signaling the inherent fragility of illicit digital marketplaces. The broader implications for risk management are profound: as these platforms collapse, the associated data becomes a public record, enabling a massive wave of retroactive attribution and legal action against active threat groups.

This development underscores a growing trend where the infrastructure of the aggressors has become as vulnerable as that of their targets, potentially chilling the operations of emerging cyber-extortionists while offering a rare, transparent window into the internal mechanics of modern cybercrime syndicates.

Read more: https://www.resecurity.com/es/blog/article/doomsday-for-cybercriminals-data-breach-of-major-dark-web-foru

United States of America (USA)

Pentagon to Invest $1 billion in L3Harris Rocket Motor Business

The U.S. Department of Defence (DoD) has initiated a strategic $1 billion investment in the rocket motor business of L3Harris Technologies, specifically focusing on the Aerojet Rocketdyne division, to fortify the domestic solid rocket motor (SRM) industrial base. This move addresses a critical bottleneck in the Western defence supply chain: the limited production capacity for propulsion systems essential to high-demand munitions, including the GMLRS, Javelin, and emerging hypersonic interceptors. Situated within the broader context of reshoring critical technologies to counter near-peer capabilities in the Indo-Pacific and Europe, the investment reflects a shift toward industrial resilience in response to the fragility exposed by recent global conflicts. The funding is expected to modernize manufacturing facilities and scale up advanced production techniques, such as additive manufacturing for complex engine components and automated propellant casting.

These technological upgrades are designed to enhance throughput while simultaneously improving the "cyber-physical" security of the manufacturing process, protecting against industrial espionage and unauthorized subversion of propulsion flight-control software. By incentivizing dual-sourcing and reducing reliance on a narrow set of providers, the Pentagon is actively mitigating the risk of systemic failure within the defence industrial base (DIB). For

analysts and policy stakeholders, this development emphasizes that modern national security is increasingly tethered to supply chain integrity and the ability to rapidly scale kinetic manufacturing under duress.

The broader implications suggest a long-term move toward a "hardened" industrial ecosystem where technological redundancy serves as a primary deterrent against geopolitical coercion. This effort fits into a larger pattern of securing the physical and digital foundations of the "arsenal of democracy," ensuring that strategic missile stockpiles remain viable and resilient against both kinetic and non-kinetic threats in an era of sustained international friction.

Read more: https://dsm.forecastinternational.com/2026/01/13/pentagon-to-invest-1-billion-in-l3harris-rocket-motor-business/

Human-machine teaming in battle management: A collaborative effort across borders

The United States Air Force, in coordination with strategic allies from the United Kingdom and Australia, has accelerated the operationalization of Human-Machine Teaming (HMT) within global battle management architectures to address the complexities of high-end, multi-domain conflict. This initiative arrives as a pivotal response to the escalating demand for Joint All-Domain Command and Control (JADC2), where the sheer volume of data in contested environments particularly in the Indo-Pacific outpaces traditional human cognitive limits. By integrating advanced Artificial Intelligence (AI) and Machine Learning (ML) algorithms into command-and-control (C2) nodes, the partnership seeks to automate sensor-to-shooter loops while ensuring human-in-the-loop oversight for strategic and ethical validation. Recent operational testing at Nellis Air Force Base has specifically focused on "algorithmic interoperability," testing the ability of AI-driven decision aids to synchronize target prioritization across disparate national data sets without compromising sovereign encryption standards.

Technically, the effort leverages cloud-native environments and edge computing to facilitate real-time data fusion from a variety of fifth-generation platforms and legacy systems. A primary focus involves the development of open-architecture protocols and standardized data schemas, allowing AI agents to perform automated reconnaissance and threat assessment while maintaining resilience against electronic warfare (EW) and signal degradation. These exercises also emphasize the security of the underlying data pipelines, addressing the risk of adversarial "data poisoning" or prompt injection that could subvert autonomous decision-making. For defenders and policy stakeholders, these advancements signal a shift toward a software-defined military posture where "decision superiority" is the primary deterrent. The broader implications for national security and international stability are significant: as HMT becomes foundational to collective defense, cyber resilience must move beyond endpoint protection to encompass the integrity of the entire algorithmic ecosystem. This development underscores a larger trend in the threat landscape where the security of the human-machine interface against cognitive and technical subversion is now a prerequisite for mission success and regional stability.

Read more: https://www.nellis.af.mil/News/Article/4370792/human-machine-teaming-in-battle-management-a-collaborative-effort-across-borders/

People's Republic of China (PRC) | China

UAT-7290 targets high value telecommunications infrastructure in South Asia

The China-linked advanced persistent threat (APT) group known as Mustang Panda tracked by Cisco Talos under the designation UAT-7290 has launched a sophisticated and enduring espionage campaign targeting government entities and strategic sectors across Southeast Asia. This development situates itself within a broader trend of escalating cyber-enabled statecraft in the South China Sea region, where regional tensions drive a continuous demand for high-value intelligence. The campaign is notable for its tactical refinement, shifting away from generic delivery methods toward highly modular, multi-stage infection chains designed to bypass modern endpoint detection and response (EDR) systems.

Technical analysis reveals that UAT-7290 primarily utilizes a "living-off-the-land" (LotL) strategy,

leveraging legitimate but vulnerable binaries, such as components of the PotPlayer media player, to facilitate DLL side-loading. In a typical infection sequence, a malicious loader frequently disguised within archives containing geopolitical-themed lures is used to deploy a custom C++ backdoor. This implant is capable of extensive system reconnaissance, directory enumeration, file exfiltration, and the execution of arbitrary shell commands. To maintain persistence, the actor exploits mshta.exe and creates specialized scheduled tasks that periodically beacon to a command-and-control (C2) infrastructure hosted on IP ranges specifically selected to blend with regional traffic patterns. Furthermore, the group demonstrates operational maturity by employing sophisticated obfuscation techniques to mask its C2 communication protocols and internal metadata, frustrating forensic reconstruction.

For defenders and policy stakeholders, the persistent activity of UAT-7290 underscores the limitations of signature-based defence in the face of state-sponsored actors who can rapidly iterate their toolsets. The implications for national security and corporate resilience are profound: as Mustang Panda refines its ability to maintain low-and-slow access to government networks, the focus of risk management must shift toward deep behavioural analytics and a zero-trust approach to "trusted" third-party binaries.

This campaign represents a larger pattern of sustained strategic competition in the cyber domain, where the long-term integrity of regional digital infrastructure is increasingly compromised by sophisticated, state-aligned persistence.

Read more: https://blog.talosintelligence.com/uat-7290/

The Great VM Escape: ESXi Exploitation in the Wild

A critical escalation in hypervisor-based threats has surfaced with the technical analysis of a VMware ESXi virtual machine (VM) escape exploit, representing a foundational risk to the virtualized infrastructure that serves as the backbone of global enterprise data centers. This development arrives amid a broader strategic shift where sophisticated threat actors, particularly ransomware syndicates such as Akira and LockBit, have moved from targeting individual endpoints to compromising the virtualization layer to achieve maximum operational paralysis. Hypervisor escapes are considered the "Holy Grail" of exploitation because they shatter the guest-to-host isolation boundary, allowing an adversary with limited access to a single VM to gain arbitrary code execution on the underlying ESXi host. By compromising the hypervisor, attackers bypass guest-level security controls and gain total visibility and control over every virtualized workload, including sensitive databases and domain controllers.

Technical analysis reveals that the exploit targets memory corruption vulnerabilities within the VMX process the host-side component responsible for managing guest execution typically by triggering heap overflows or use-after-free conditions through emulated hardware interfaces. Specifically, vulnerabilities in the virtual USB controller, SVGA device, or network interface cards (NICs) are frequently leveraged to achieve the escape. Once the guest-to-host boundary is breached, the attacker can execute shellcode with the privileges of the ESXi user, facilitating the deployment of host-level ransomware or the exfiltration of raw VMDK files.

This "infrastructure-native" approach renders traditional guest-resident EDR and antivirus solutions largely ineffective, as the intrusion occurs beneath the monitored operating system. For risk management professionals and policy stakeholders, this trend necessitates a paradigm shift that prioritizes hypervisor hardening and immediate patching of management planes.

As the cyber threat landscape moves toward higher-level abstraction attacks, maintaining international stability and corporate resilience will increasingly depend on securing the "identity and infrastructure" perimeters, ensuring that a single guest compromise does not translate into a catastrophic, site-wide failure.

Read more: https://www.huntress.com/blog/esxi-vm-escape-exploit

China's digital defense drills

China's Ministry of Public Security (MPS) and the Cyberspace Administration of China (CAC) have

significantly intensified state-mandated "Cyber Shield" (Dianwang) exercises, signaling a strategic pivot toward a "Whole-of-Nation" defensive posture. This development occurs against a backdrop of escalating geopolitical friction and the imperative to secure Critical Information Infrastructure (CII) against sophisticated foreign intelligence actors. These drills, which often span weeks, involve a highly coordinated ecosystem of government bodies, state-owned enterprises (SOEs), and private-sector tech giants, effectively blurring the lines between domestic security and national defense. Factually, the exercises utilize elite state-sponsored "Red Teams" to launch unannounced, high-fidelity simulations against Blue Team defenders across sectors including energy, finance, and telecommunications. Operational details highlight a focus on advanced persistence, specifically targeting industrial control systems (ICS/SCADA) and exploiting software supply chain vulnerabilities. Technically, these simulations emphasize the use of automated vulnerability scanning, zero-day exploitation frameworks, and lateral movement techniques designed to test the limits of real-time detection and incident response protocols.

By mandating the participation of top-tier cybersecurity researchers, China is effectively centralizing its vulnerability discovery pipeline, ensuring that critical exploits are disclosed to the state before they reach global databases. This centralized model poses a substantial challenge to international risk management, as it accelerates the professionalization of China's defensive capabilities while simultaneously sharpening its offensive potential. For global practitioners and policy stakeholders, these drills underscore a broader trend of "digital sovereignty," where state-level resilience is achieved through the integration of civilian expertise into military-grade defense strategies.

The resulting increase in domestic cyber resilience not only complicates foreign signals intelligence operations but also establishes a new benchmark for national-level cyber readiness, requiring a recalibrated understanding of international stability in an increasingly fragmented digital landscape.

Read more: https://netaskari.substack.com/p/chinas-digital-defense-drills

Republic of China (ROC) | Taiwan

Chinese cyberattacks on Taiwan infrastructure averaged 2.6 million a day in 2025, report says

Taiwan's critical infrastructure is navigating an era of unprecedented digital siege as state-linked cyberattacks from the People's Republic of China (PRC) surged to an average of 26 million daily incidents throughout 2025. This escalation represents more than traditional espionage; it reflects a strategic shift toward high-volume, automated disruption and pre-positioning within essential service networks, including energy, telecommunications, and government administration. As cross-strait tensions remain a focal point of global geopolitical risk, these operations underscore the weaponization of the "Grey zone," where cyber activity serves to erode public trust and test the limits of national resilience without crossing the threshold into kinetic warfare.

Operational data reveals a sophisticated tactical blend, prominently featuring "living-off-the-land" (LotL) techniques to bypass traditional signature-based detection and the exploitation of zero-day vulnerabilities in edge networking equipment. Threat actors have increasingly targeted Industrial Control Systems (ICS) and operational technology (OT) protocols, seeking to establish persistent access that could be activated during a crisis. The sheer scale of these probes—averaging over 18,000 attempts per minute—necessitates a move away from manual triage toward AI-driven defensive automation and zero-trust architectures. For global defenders and policy stakeholders, Taiwan's experience serves as a critical case study in the evolution of state-sponsored attrition.

The broader implications for international stability are profound: the persistence and volume of these attacks signal a permanent shift in the cyber threat landscape, where the goal is no longer just the theft of data but the systematic exhaustion of defensive capacity. This development mandates a revaluation of risk management strategies, emphasizing that cyber resilience is now a cornerstone of national security and the preservation of global supply chain integrity in an increasingly volatile digital theatre.

Read more: https://www.reuters.com/world/

china/chinese-cyberattacks-taiwan-infrastructure-averaged-26-million-day-2025-report-2026-01-05/

Middle East | West Asia

Reborn in Rust: Muddy Water Evolves Tooling with RustyWater Implant

The Iran-linked threat actor MuddyWater (also known as APT33 or Static Kitten), believed to operate on behalf of the Ministry of Intelligence and Security (MOIS), has significantly modernized its offensive toolkit with the introduction of "RustyWater," a sophisticated new implant developed in the Rust programming language. This development occurs within a broader technological landscape where advanced persistent threats (APTs) are increasingly transitioning from traditional languages like C++ to memory-safe, cross-platform languages such as Rust and Go to enhance operational efficiency and systematically bypass signature-based detection. MuddyWater's strategic focus remains centered on Middle Eastern governmental and telecommunications sectors, where regional geopolitical tensions drive a persistent need for high-fidelity intelligence.

Technically, RustyWater serves as a versatile backdoor designed for stealthy reconnaissance and initial foothold maintenance. The implant leverages Rust's inherent performance and modularity to perform comprehensive system profiling, including the collection of hostnames, user account details, and active process lists. For command-and-control (C2) operations, the malware utilizes HTTP/HTTPS protocols, frequently employing obfuscated headers to blend with legitimate web traffic. Notable capabilities include the ability to execute arbitrary shell commands, facilitate bidirectional file transfers, and update its own configuration to avoid hardcoded indicators of compromise (IoCs). The move to Rust specifically complicates reverse engineering efforts for security analysts relying on legacy automated sandboxing, as the language produces complex binaries that can evade traditional heuristic engines.

For risk management and defense stakeholders, the emergence of RustyWater underscores the necessity of moving beyond static indicators toward a defense-in-depth model rooted in deep behavioral analytics and endpoint visibility. The evolution of MuddyWater's arsenal highlights a larger pattern in the threat landscape where state-aligned actors are professionalizing their development pipelines to increase the longevity of their intrusions. Ultimately, maintaining regional cyber resilience in the face of such adaptive adversaries requires a shift toward zero-trust principles and the proactive monitoring of non-standard binary execution within sensitive network environments.

Read more: https://www.cloudsek.com/blog/reborn-in-rust-muddywater-evolves-tooling-with-rustywater-implant

European Union | EU

34 arrests in Spain during action against the 'Black Axe' criminal organisation

The Spanish National Police, in coordination with Europol's European Cybercrime Centre (EC3), has dismantled a major operational cell of the Black Axe criminal organization, resulting in the arrest of 34 individuals across several Spanish provinces. Originally a Nigerian-based fraternity, Black Axe has evolved into a formidable transnational syndicate specializing in high-volume financial cybercrime, situating this development at the intersection of traditional organized crime and modern digital exploitation. This crackdown is particularly significant given the current risk landscape, where industrial-scale Business Email Compromise (BEC) and social engineering continue to bypass sophisticated technical perimeters by targeting human trust. The investigation revealed that the network successfully laundered nearly €5 million through a complex web of shell companies and "money mule" accounts, effectively obfuscating the proceeds of romance scams, investment fraud, and targeted corporate intrusions.

Tactically, the group employed sophisticated phishing kits to harvest credentials and intercept financial communications, often using identity theft to establish credible fraudulent personas. During the synchronized raids, law enforcement seized high-end hardware, forged identification documents, and substantial cash reserves, pointing to a highly organized logistical structure. For defenders and corporate decision-makers, this operation serves as a stark reminder that cyber resilience must extend beyond software

patching to encompass robust financial controls and rigorous identity verification protocols. The broader implications for international security are profound; as West African-linked syndicates like Black Axe professionalize their digital operations, the necessity for cross-border intelligence sharing and "follow-the-money" forensic strategies becomes paramount. This successful disruption underscores a critical pattern in the threat landscape: the convergence of cyber-enabled fraud with globalized money laundering infrastructures, requiring a unified, multi-jurisdictional response to protect the integrity of the international financial system and mitigate long-term technical and economic risks.

Read more: https://www.europol.europa.eu/media-press/newsroom/news/34-arrests-in-spain-during-action-against-black-axe-criminal-organisation

Russian Federation & Ukraine

GRU-Linked BlueDelta Evolves Credential Harvesting

BlueDelta, a prolific threat group attributed to the Russian General Staff Main Intelligence Directorate (GRU), has significantly advanced its credential harvesting operations targeting strategic government and defense organizations throughout Europe. This activity is situated within the broader landscape of Russian cyber espionage efforts designed to secure an intelligence advantage during the prolonged conflict in Ukraine, emphasizing the continued vulnerability of NATO-aligned entities to state-linked intrusions. The group, frequently tracked as APT28 or Forest Blizzard, has refined its methodology to exploit vulnerabilities in widely deployed webmail platforms, moving away from easily detectable phishing to more seamless web-based exploitation. Recent tactical shifts include the weaponization of cross-site scripting (XSS) flaws in Roundcube webmail software specifically CVE-2023-43770 and CVE-2023-5631 to execute malicious JavaScript within victim sessions. This capability allows the adversary to automate the theft of session tokens and user credentials while bypassing traditional multi-factor authentication (MFA) triggers.

To enhance their evasion, BlueDelta leverages legitimate third-party services like Mockbin and Webhook.site as command-and-control (C2) and exfiltration nodes, effectively camouflaging their operations within standard enterprise web traffic. This move toward modular, high-stealth infrastructure highlights a sophisticated effort to circumvent signature-based detection and complicates forensic analysis. For national security analysts and corporate defenders, the evolution of BlueDelta underscores the critical need for an "identity-first" security posture and the aggressive patching of public-facing communication software. The broader implications for international stability are stark; as these actors achieve deeper persistence within diplomatic networks, the risk of strategic miscalculation increases. Strengthening cyber resilience in this environment requires a transition toward behavioural analytics that can identify the subtle indicators of session hijacking and the unauthorized use of legitimate development tools for exfiltration.

Read more: https://www.recordedfuture.com/research/gru-linked-bluedelta-evolves-credential-harvesting

Malware & Vulnerabilities

Unveiling VoidLink – A Stealthy, Cloud-Native Linux Malware Framework

The emergence of VoidLink, a sophisticated and modular Linux-based command-and-control (C2) framework identified by Check Point Research, signals a critical evolution in the landscape of cloud-native cyber espionage. Attributed to high-tier, Chinese-affiliated developers, the framework is specifically engineered for "cloud-first" environments, reflecting a broader strategic shift as state-aligned actors professionalize their operations against Linux-centric infrastructure. VoidLink is written primarily in the modern Zig programming language and utilizes a modular architecture inspired by Cobalt Strike's Beacon Object Files (BOF), supporting over 30 post-exploitation plugins.

These modules target high-value assets, including SSH keys, git credentials, and instance metadata via vendor-specific APIs for AWS, Azure, GCP, Alibaba, and Tencent. Technically, the framework demonstrates an exceptional level of operational security (OPSEC), employing an "adaptive stealth" mechanism that profiles the host environment for security products and kernel hardening measures to

calculate a risk score, subsequently tuning its evasion behavior. Its payload includes a multi-path rootkit system that dynamically deploys eBPF hooks, Linux Kernel Modules (LKM), or LD_PRELOAD based on the target's kernel version, effectively shielding malicious processes and network sockets from standard monitoring.

Communication is managed through a proprietary "VoidStream" protocol, which camouflages C2 traffic within legitimate-looking HTTP/2, WebSocket, or DNS packets. By prioritizing the exploitation of container ecosystems and developer workstations, VoidLink creates a potent launchpad for cross-cloud lateral movement and supply-chain compromise. For security practitioners and policy stakeholders, this development highlights the inadequacy of traditional, Windows-centric defense models in a fragmented, cloud-first reality. The broader implications for international stability are profound; as professionalized, modular frameworks like VoidLink lower the threshold for persistent cloud-resident espionage, maintaining cyber resilience will increasingly depend on deep-visibility kernel monitoring and identity-centric cloud security architectures.

Read more: https://research.checkpoint.com/2026/voidlink-the-cloud-native-malware-framework/

Microsoft disrupts global cybercrime subscription service responsible for millions in fraud losses

Microsoft's Digital Crimes Unit (DCU), in a landmark coordinated effort with law enforcement agencies across the United States, the United Kingdom, and Germany's ZIT, has successfully disrupted RedVDS, a prolific cybercrime-as-a-service (CaaS) subscription platform that has facilitated at least $40 million in fraudulent losses since early 2025. This operation, which marks Microsoft's first such legal action in the UK, targets the foundational infrastructure that allows low-level actors to execute high-impact financial crimes with minimal technical overhead. RedVDS specialized in providing disposable virtual desktops often running unlicensed Windows environments for as little as $24 per month, offering attackers a cheap, scalable, and anonymized launchpad for malicious activity. The platform was a primary engine for sophisticated business email compromise (BEC) and real estate payment diversion scams, with more than 191,000 organizations compromised globally. Technically, the service enabled the transmission of roughly one million phishing messages daily and was increasingly integrated with generative AI tools, including voice cloning and face-swapping technologies, to enhance the realism of social engineering campaigns. By seizing key domains and dismantling the marketplace's server infrastructure, Microsoft and its partners, including co-plaintiffs H2-Pharma and the Gatehouse Dock Condominium Association, have severely degraded a major node in the AI-enabled fraud ecosystem.

The disruption highlights a critical trend in the threat landscape: the professionalization of fraud through specialized infrastructure providers who shield malicious traffic from detection. For security practitioners and policy stakeholders, the operation reinforces the necessity of aggressive public-private partnerships and the use of civil litigation to neutralize the economic incentives of cybercrime. Ultimately, this development underscores that modern cyber resilience requires moving beyond perimeter defence to actively dismantling the shared infrastructure that fuels large-scale, automated deception campaigns.

Read more: https://blogs.microsoft.com/on-the-issues/2026/01/14/microsoft-disrupts-cybercrime/

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.