CLAWS Newsletter

Cyber Index | Volume II | Issue 10

by Govind Nelika

@govindnelika
govind-nelika-4217969b

https://claws.co.in/category/newsletter/

* CLAWS Cyber Index Newsletter is a concise Bi-Monthly 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

CERT-IN Releases comprehensive Blueprint to defend Against AI Vulnerablities

The Indian Computer Emergency Response Team (CERT-In) has released a comprehensive 38-page technical advisory titled "Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure," signaling an aggressive overhaul of national defensive doctrine to counter automated cyber warfare. This strategic intervention addresses a fundamental shift in the threat landscape, where adversaries increasingly weaponize generative AI, large language models (LLMs), and autonomous agents to automate reconnaissance, discover unknown software flaws, and dynamically generate evasive malware. By compressing the time window between a vulnerability's public disclosure and its functional weaponization from days to mere hours, AI-assisted exploitation threatens critical national infrastructure, financial networks, and digital public infrastructure (DPI) across vital sectors. To neutralize this compressed cyber kill chain, CERT-In's blueprint outlines a strict, phased remediation framework that challenges traditional, compliance-driven quarterly patch management cycles. Under the new recommendations, organizations are urged to contain and patch known exploited vulnerabilities affecting internet-facing or "crown-jewel" assets within an aggressive 12-hour window.

Other critical externally exposed flaws must be mitigated within 24 hours, while internal high-value systems must be resolved within three days. To meet these accelerated timelines, the guidance advocates for a five-stage Continuous Threat Exposure Management (CTEM) cycle encompassing scoping, discovery, prioritization, validation, and mobilization backed by agentic Security Operations Centers (SOCs) that utilize machine learning for real-time telemetry correlation and automated anomaly detection. Furthermore, the blueprint mandates deep supply chain visibility through the implementation of Software Bills of Materials (SBOM) and AI Bills of Materials (AIBOM) to trace open-source package and model dependencies. Ultimately, this framework establishes a repeatable blueprint for modern cyber resilience by forcing security teams to transition to an "assume breach" operational posture. By enforcing rapid remediation, daily exposure validation, and robust AI model governance, defenders can mitigate adversarial techniques such as data poisoning and prompt injection, systematically reducing attacker dwell time in an era of automated, large-scale cyber operations.

Read more: https://www.cert-in.org.in/PDF/Blueprint_for_Defending_against_AI_Assisted_Exploitataion.pdf

Tata Electronics and ASML Announce Strategic Partnership to Advance the Semiconductor Manufacturing Ecosystem in India

In an era defined by intensifying geostrategic competition over hardware sovereign control and supply chain resilience, Tata Electronics and Dutch semiconductor giant ASML have entered into a strategic partnership to anchor India's nascent semiconductor manufacturing ecosystem. Signed as a Memorandum of Understanding (MoU) on May 16, 2026, the alliance responds directly to growing geopolitical vulnerabilities within the global tech stack, where high-reputation logic chip dependencies are increasingly threatened by cross-border disruptions and state-sponsored industrial espionage. For enterprise defenders and national security decision-makers, securing the hardware-level trust architecture represents the foundational baseline for all downstream software, cyber deterrence, and critical infrastructure resilience. Under the operational terms of the pact, ASML will deploy its comprehensive suite of advanced lithography tools and holistic solutions to facilitate the construction and rapid deployment of Tata's upcoming 300 mm (12-inch) commercial semiconductor fabrication facility in Dholera, Gujarat.

Representing an $11 billion investment, the facility is designed to manufacture legacy nodes ranging from 28nm to 110nm in partnership with Taiwan's PSMC, explicitly targeting downstream applications in automotive, mobile, and artificial intelligence (AI) ecosystems. Beyond hardware deployment, the framework establishes a joint commitment to building domestic research and development (R&D) infrastructure and a

specialized lithography talent pipeline to mitigate intellectual property risks and operational vulnerabilities. For global risk managers, this development signals a shifting paradigm in hardware risk mitigation, driving the decentralization of critical technology stacks away from historical Asian maritime flashpoints. By integrating ASML's industry-standard lithography infrastructure with India's scaling engineering capacity, the initiative highlights an accelerating move toward trusted foundry models, establishing verified, diverse, and resilient supply lines essential for protecting sovereign communications, military systems, and enterprise data backbones from hardware-level tampering or supply restrictions.

Read more: https://www.asml.com/en/news/press-releases/2026/tata-electronics-and-asml-announce-strategic-partnership

Short Range Ballistic Missile Agni-1 successfully test-launched

In a significant reinforcement of its regional deterrence posture, India's Ministry of Defence and the Strategic Forces Command (SFC) successfully test-fired the short-range ballistic missile (SRBM) 'Agni-1' from the Integrated Test Range in Chandipur, Odisha. This deployment validation occurs amid escalating geopolitical tensions in the Indo-Pacific and a rapidly evolving regional risk landscape, where maintaining a "minimum credible deterrence" is paramount for national security decision-makers balancing conventional and asymmetric threats. Developed by the Defence Research and Development Organisation (DRDO), the Agni-1 features a operational range of 700 km to 1,200 km, precisely engineered to bridge the tactical capability gap between the shorter-range Prithvi-II and the longer-range Agni-II.

The mid-tier strategic asset is highly versatile, capable of delivering both conventional and nuclear payloads. Operationally, the test validated all technical parameters of the platform, which is optimized for high mobility and rapid deployment via specialized road-mobile transporter erector launchers (TELs) as well as rail-based configurations. This successful launch follows a broader pattern of accelerated strategic testing by New Delhi, occurring just weeks after an advanced Agni variant equipped with Multiple Independently Targetable Re-entry Vehicle (MIRV) technology was trailed in the Indian Ocean Region. For security practitioners and risk analysts, the successful validation of the canisterized, highly mobile Agni-1 underscores India's focus on survivability and reduced reaction times against potential first-strike scenarios. Ultimately, the development demonstrates a mature strategic capability, consolidating India's defence preparedness and stabilizing its deterrence architecture within a highly contested electronic and kinetic theatre.

Read more: https://timesofindia.indiatimes.com/india/india-successfully-test-launches-agni-1-ballistic-missile/articleshow/131265957.cms

Raksha Mantri holds bilateral talks with Minister of National Defence, Republic of Korea in Seoul

In an era defined by fragmenting supply chains and escalating geostrategic friction in the Indo-Pacific, India and the Republic of Korea (RoK) have finalized a series of bilateral defence agreements establishing a formalized framework for cooperation across critical technology and cyber domains. Signed in Seoul by Indian Defence Minister Rajnath Singh and South Korean National Defence Minister Ahn Gyu-back, the pacts position joint defence cyber capabilities alongside joint training and UN peacekeeping operations as core pillars of a multi-dimensional strategic partnership. This development underscores a broader trend wherein nation-states are increasingly anchoring regional security architectures in joint technological defence to counter sophisticated multi-vector threats and state-sponsored offensive cyber activity. Operationally, the agreements aim to link the two nations' innovation ecosystems via the newly discussed India-Korea Defense Innovation Accelerator Ecosystem (KIND-X) roadmap, targeting mutual development and export of next-generation defensive software, artificial intelligence, autonomous platforms, quantum computing, and semiconductor security frameworks.

The bilateral initiative also yielded industry-level agreements between corporate giants Larsen & Toubro (L&T) and Hanwha Co. Ltd., demonstrating a concerted push to align private sector manufacturing capabilities

with public sector resilience goals. For global risk managers and defensive stakeholders, this pact highlights a shifting threat landscape where conventional warfare boundaries are blurring into cyberspace. By formalizing a defence cyber alliance and pooling deep technological capabilities leveraging South Korea's advanced electronics sector alongside India's vast engineering talent and scaling startup ecosystem both nations seek to insulate critical infrastructures from cross-border disruption. Ultimately, the partnership reflects a growing imperative among technologically capable democracies to build trusted digital supply chains and robust cyber deterrence frameworks, signalling that long-term regional stability in a shifting global landscape is now inextricably tied to collective cyber resilience.

Read more: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2263304&reg=3&lang=2

Pune co successfully tests 300km-range Suryastra rockets off Odisha; Army procuring its launcher systems

In a significant development demonstrating the growing role of private-sector defence firms in regional deterrence architectures, Pune-based NIBE Limited has successfully executed the consecutive live-fire demonstration of the "Suryastra" precision long-range rocket system. Conducted on May 18 and 19, 2026, at the Integrated Test Range (ITR) in Chandipur, Odisha, the trials underscore India's aggressive push for indigenous hardware autonomy (Atmanirbhar Bharat) amid intensifying border tensions and a heightened reliance on localized supply chains. For military operators and defensive planners, this system directly bridges a critical operational gap between traditional tactical field artillery and heavier, more cost-prohibitive ballistic missile platforms. Factual, operational details from the testing confirm the successful flight of two distinct variants the EXTRA rocket, which commands a 150 km range, and the Predator Hawk variant, striking at distances up to 300 km.

Architecturally, the system achieved exceptional terminal accuracy, registering a Circular Error Probable (CEP) of just 1.5 meters and 2 meters respectively, which positions it among the most precise deep-strike assets globally. The Suryastra utilizes India's first indigenous, universal multi-caliber rocket launcher platform, built onto an all-terrain tactical truck chassis. This gives mobile artillery crews vital "shoot-and-scoot" functionality, enabling them to fire a full salvo and rapidly relocate before hostile counter-battery sensors can calculate an interception vector. Backed by a preliminary emergency procurement order placed by the Indian Army in January for the weapon's launcher and munitions packages, the validation of this platform signals a broader shift in the strategic risk landscape. By integrating highly mobile, precise, and modular deep-strike platforms into front-line arsenals, national defence architectures can effectively enhance localized resilience, reduce reliance on vulnerable foreign defence supply links, and force state-linked threat actors to recalibrate their regional escalation calculations.

Read more: https://timesofindia.indiatimes.com/defence/news/pune-co-successfully-tests-300km-range-suryastra-rockets-off-odisha-army-procuring-its-launcher-systems/articleshow/131225560.cms

External

Global Focus Brief

JIATF 401 Drone Defence Marketplace Broadens Allied Access to Counter-Drone Capabilities

The U.S. Department of War's Joint Interagency Task Force 401 (JIATF-401) has launched an international "Drone Defense Marketplace," an online procurement clearinghouse designed to drastically accelerate allied and partner nation access to combat-proven Counter-Unmanned Aircraft Systems (C-UAS). This strategic expansion comes amid a paradigm shift in modern multi-domain warfare, where the proliferation of cheap, automated, and swarm-capable aerial threats challenges traditional, cost-prohibitive air defense structures globally. Directed by Army Brig. Gen. Matt Ross, the initiative aims to institutionalize defense-supply chains,

ensuring that international allies can rapidly integrate affordable, AI-driven kinetic and electronic mitigation capabilities into their localized force-protection doctrines. The newly established digital marketplace streamlines foreign military sales by offering pre-vetted, high-rate production systems, notably featuring Perennial Autonomy's suite of autonomous interceptors, including the fixed-wing Merops, the Bumblebee FPV quadcopter, and the pneumatic-launched Hornet drone.

Technically, the marketplace serves as a standardized verification node to guarantee interoperability; all listed platforms must adhere to uniform interface standards that feed directly into established military command and control (C2) frameworks, facilitating automated target handoff while retaining human-in-the-loop oversight for lethal validation. Furthermore, the catalog prioritizes systems engineered with advanced terminal-guidance machine learning algorithms and robust electronic warfare (EW) resistance, specifically evaluating platforms on their ability to maintain localized radio frequency (RF) sensing and computer-vision tracking in GPS-denied environments. Ultimately, this procurement move carries major implications for international stability and collective cyber-kinetic resilience. By shifting C-UAS acquisition from slow, localized experimentation into a scalable, high-volume allied ecosystem, the Pentagon is building a unified front against asymmetric aerial warfare. For defense decision-makers and risk management stakeholders, this platform establishes a repeatable blueprint to fortify critical infrastructure and forward operating bases globally, neutralizing low-tier aerial threats before they can disrupt strategic regional security.

Read more: https://www.war.gov/News/News-Stories/Article/Article/4497147/jiatf-401-drone-defense-marketplace-broadens-allied-access-to-counter-drone-cap/

GitHub update on stolen data from thousands of internal repositories

In a high-impact development highlighting the critical risks facing modern software supply chains, GitHub disclosed a cyberattack resulting in the unauthorized exfiltration of approximately 3,800 internal repositories. The incident was initiated on May 18, 2026, when a GitHub employee's device was compromised via a "poisoned" third-party Visual Studio Code (VS Code) extension. This initial breach vectors directly into the escalating trend of threat actors targeting developer environments and identity management pipelines to breach high-reputation code repositories, using corrupted ecosystem dependencies to manipulate trusted platforms. While GitHub's initial response effectively isolated the compromised endpoint and removed the malicious extension version, subsequent investigations forced a significant escalation in defensive measures on May 26, 2026, due to potential threat actor interactions with core repository data. Out of an abundance of caution, GitHub initiated an emergency rotation of its cryptographic foundations, most notably the GitHub Enterprise Server (GHES) GPG signing key used to validate binary integrity during manual updates.

Administrators running GHES instances are required to urgently deploy a specialized bash script (rotate-gpg.sh) across single-node and high-availability cluster topologies to update the GPG public keys stored within admin and root accounts; failure to execute this rotation will cause all future version upgrades and security patches to fail package verification. Although customer code repositories hosted on GitHub Enterprise Cloud remain unaffected, some internal logs containing excerpts of historical customer support interactions were exposed. Ultimately, this breach underscores a systemic vulnerability where a single endpoint compromise can jeopardize institutional signing infrastructure. For risk managers and security architects, it stresses the imperative of moving beyond traditional perimeter security to enforce strict least-privilege constraints on developer extensions, mandate zero-trust identity verification for code-signing operations and maintain rigid patch compliance across on-premises enterprise servers to mitigate cascading downstream supply chain compromises.

Read more: https://github.blog/security/investigating-unauthorized-access-to-githubs-internal-repositories/

Disrupting Fox Tempest: A cybercrime service that turned "verified" software into a pathway for ransomware

In a decisive offensive legal and technical intervention, Microsoft's Digital Crimes Unit has unsealed a lawsuit in the U.S. District Court for the Southern District of New York to neutralize "Fox Tempest," a prolific malware-signing-as-a-service (MSaaS) operation. Operating since May 2025, the illicit platform has weaponized the fundamental trust architectures of the internet by providing cybercriminals with a highly specialized, high-cost mechanism to bypass initial access blocks. This operation aligns with a broader modular trend in the cybercrime economy, where sophisticated enablers remove operational friction for distributed threat groups, drastically altering the risk landscape for enterprise defenders. Behind the scenes, Fox Tempest operators used fabricated identities and corporate impersonation to systematically create hundreds of fraudulent Microsoft accounts, exploiting development platforms like Microsoft Artifact Signing to obtain legitimate, high-reputation code-signing credentials.

Cybercriminals uploaded payloads via the web portal signspace[.]cloud to bind valid digital signatures to prominent information stealers and loaders, including Oyster, Lumma Stealer, and Vidar. Co-conspirators like Vanilla Tempest used this signed malware to bypass Antivirus and Endpoint Detection and Response (EDR) systems, establishing the initial access necessary to deploy devastating double-extortion ransomware variants like Rhysida, INC, Qilin, and Akira against critical infrastructure globally. Microsoft's multi-layered disruption dismantled Fox Tempest's infrastructure by seizing its core domain, taking down hundreds of third-party-hosted virtual machines, and blocking an external repository hosting the underlying code. The operational takedown highlights the critical vulnerability of the public-key infrastructure (PKI) ecosystem to automated credential abuse. For risk managers and security operations teams, this development underscores that checking binary validity alone is insufficient; countering modern cybercrime requires proactive behavioral detection for search engine manipulation, malicious ad networks, and post-exploitation anomalies, ensuring that trust mechanisms themselves are not used to slip past perimeter defences.

Read more: https://blogs.microsoft.com/on-the-issues/2026/05/19/disrupting-fox-tempest-a-cybercrime-service/

United States of America (USA)

Secretary of the Army hosts Defense Critical Infrastructure Summit at Fort Bragg

Secretary of the Army Dan Driscoll, alongside the XVIII Airborne Corps, federal interagency partners, and private-sector utility providers, has convened the inaugural Defense Critical Infrastructure (DCI) Summit at Fort Bragg, North Carolina, signaling an aggressive push to fortify the domestic foundations of military power projection. This strategic mobilization unfolds amid a highly volatile global threat landscape where nation-state adversaries increasingly target civilian industrial control systems (ICS) and commercial supply chains to degrade military readiness before a single shot is fired. Because the overwhelming majority of U.S. military installations rely entirely on privately owned regional utilities, securing these external dependencies has become a national security imperative. Led by Driscoll, Principal Cyber Advisor Brandon Pugh, and Acting Under Secretary of Energy Alex Fitzsimmons, the high-level summit addressed four critical operational vulnerabilities: physical threats from low-cost unmanned aerial systems (UAS), multi-vector cyber impacts on power grids, force projection dependencies, and information-sharing latency between military commanders and local municipalities.

To mitigate these vectors, organizers established a coordinated defense framework aimed at accelerating joint crisis response and embedding engineering redundancies directly into local electrical grids, water treatment facilities, and gas distribution lines. On the technical front, defense stakeholders prioritized the deployment of scalable counter-UAS capabilities to safeguard vulnerable homeland infrastructure and mandated the adoption of standardized, high-speed telemetry channels to eliminate reporting delays during active disruptions. Ultimately, this summit marks a significant departure from isolated installation security toward a unified, whole-of-government defensive ecosystem. For risk management professionals, corporate utility operators, and military strategists, this development establishes an actionable model for public-private resilience. By systematically auditing commercial infrastructure gaps and synchronizing tactical operational parameters with civilian providers, the Pentagon aims to insulate critical infrastructure from asymmetric disruption, ensuring sustained power-projection capabilities and robust homeland defense against increasingly sophisticated cyber and kinetic adversaries.

Read more: https://www.army.mil/article/292545/secretary_of_the_army_hosts_defense_critical_infrastructure_summit_at_fort_bragg

Department of Commerce Announces Letters of Intent With 9 Companies for $2 Billion to Accelerate U.S. Leadership in Quantum Computing

In a watershed development reshaping the geopolitical landscape of cryptographic defense and computational dominance, the U.S. Department of Commerce has announced nine letters of intent totaling $2.013 billion in federal incentives under the CHIPS and Science Act. Released on May 21, 2026, the initiative targets the critical frontier of utility-scale, fault-tolerant quantum computing, which carries profound strategic implications for national security, critical infrastructure resilience, and the future viability of public-key cryptography. For enterprise defenders and intelligence agencies, this massive capitalization effort accelerates the timeline toward a post-quantum reality, forcing an urgent shift away from traditional encryption protocols to counter the long-term threat of state-sponsored “harvest now, decrypt later” operations. Operationally, the Department’s funding strategy partitions the $2 billion across multiple technological modalities to solve systemic engineering bottlenecks. On the infrastructure tier, $1.375 billion is dedicated to building foundational domestic manufacturing capacity through two secure quantum foundries: IBM receives $1 billion to establish a subsidiary specialized in quantum-grade superconducting wafers, while GlobalFoundries is allocated $375 million to pioneer a multi-modality foundry supporting superconducting, trapped ion, photonic, topological, and silicon spin architectures.

Concurrently, $638 million is distributed among seven hardware developers to mitigate hardware-level vulnerabilities and errors; specifically, Atom Computing and Infleqtion ($100M each) will scale neutral-atom arrays, D-Wave ($100M) and Rigetti ($100M) will optimize superconducting qubit counts and advanced dielectric packaging, PsiQuantum ($100M) will develop low-loss photonic packaging, Quantinuum ($100M) will target trapped-ion optical bottlenecks, and Diraq ($38M) will advance silicon-

spin logic arrays. For risk managers and policymakers, this milestone signals that global technology supply chains are definitively decoupling. By engineering a trusted, sovereign quantum ecosystem, the U.S. aims to insulate core defense architectures from foreign hardware dependencies, establishing a rigid technological baseline essential for maintaining strategic stability and digital supply chain integrity in an increasingly adversarial global arena.

Read more: https://www.nist.gov/news-events/news/2026/05/department-commerce-announces-letters-intent-9-companies-2-billion

Joint Interagency Task Force 401 Awards $500 Million Counter-UAS Contract

The U.S. Department of War's Joint Interagency Task Force 401 (JIATF-401) has awarded a three-year, $500 million Indefinite Delivery/Indefinite Quantity (IDIQ) contract to Perennial Autonomy, marking an aggressive shift in military doctrine toward low-cost, artificial intelligence-driven kinetic drone defence. Driven by asymmetric threat landscapes in Ukraine and the Middle East, where adversaries deploy waves of inexpensive one-way attack drones like the Shahed-136, defence planners face an unsustainable cost-exchange ratio when using million-dollar air defence missiles against cheap aerial threats. Directed by Army Brig. Gen. Matt Ross, JIATF-401's enterprise-wide procurement effort addresses this operational vulnerability by mass-producing attritable air-to-air kinetic interceptors. Under this contract, the Pentagon will scale and field three operationally proven autonomous platforms: the flagship Merops fixed-wing interceptor, the Bumblebee FPV quadcopter, and the Hornet pneumatic-launched, mid-range strike drone.

These platforms incorporate cutting-edge technical suites featuring onboard computer vision, localized radio frequency (RF) sensing, and advanced terminal-guidance machine learning algorithms that facilitate automated target identification, tracking, and autonomous collision-course manoeuvres. To ensure survivability in heavily contested electromagnetic combat zones, Perennial Autonomy engineered these platforms with high-integrity, electronic warfare (EW)-resistant communications, bypassing traditional commercial GPS dependencies. While executing autonomous navigation and terminal tracking, the platforms continuously feed data into existing multi-domain military command and control (C2) architectures, preserving a human-in-the-loop framework for final lethal force authorization. Ultimately, this procurement signals a fundamental restructuring of modern force protection and layer-defence strategies. By transitioning combat-tested, AI-enabled interceptor hardware from localized experimentation into formalized, high-volume U.S. military doctrine, defence stakeholders are establishing a repeatable blueprint for neutralizing low-tier aerial threats at scale. This development guarantees long-term cyber and kinetic resilience for frontline critical infrastructure, forward operating bases under U.S. Central Command, and strategic power-projection platforms worldwide against increasingly sophisticated, swarm-capable autonomous adversaries.

Read more: https://www.war.gov/News/News-Stories/Article/Article/4495165/joint-interagency-task-force-401-awards-500-million-counter-uas-contract/

République française | The French Republic

France's Passport Agency Got Hacked 19 million Citizens' Identity Records Are Now for Sale

In a severe escalation of threat activity targeting core civil infrastructure, France's National Agency for Secure Documents (ANTS) suffered a massive data breach potentially exposing the personal records of up to 19 million citizens. Operating under the French Ministry of the Interior, the ANTS portal (ants.gouv.fr) acts as the centralized gateway for processing passports, national identity cards, and driver's licenses. The incident highlights an aggressive, evolving threat landscape wherein threat actors increasingly target sovereign identity frameworks and centralized administrative hubs to acquire high-fidelity, government-verified identity datasets for downstream operations. Operationally, the breach was detected on April 15, 2026, and officially acknowledged by the ministry five days later. Shortly thereafter, threat actors operating under the aliases "breach3d" and "ExtaseHunters" advertised the stolen telemetry on BreachForums, claiming an exfiltrated corpus of 18 to 19 million records.

While the ministry confirmed that uploaded document scans were not compromised, the exfiltrated cache contains critical identity vectors: full names, dates and places of birth, postal addresses, phone numbers, email addresses, and unique internal

account identifiers. Technical analysis points to a highly critical Insecure Direct Object Reference (IDOR) vulnerability within the ANTS application programming interface (API), which allowed the actors to systematically harvest account metadata by merely manipulating request parameters without requiring advanced authentication. The threat actors further signaled deep infrastructure penetration by posting a screenshot of an internal CHEOPS law enforcement portal defaced with the text "WE ARE STILL HERE." For defense teams and national security stakeholders, the ANTS compromise underscores the permanent risk of structural identity theft; unlike static passwords, government-verified birth and geographic details cannot be rotated. This incident demands that risk managers prepare for a surge in highly targeted, multi-channel social engineering, synthetic identity creation, and credential-stuffing campaigns across both public and private sectors.

Read more: https://www.gblock.app/articles/france-ants-passport-breach-19m

People's Republic of China (PRC) | China

Joint Statement of the Russian Federation and the People's Republic of China

In a development accelerating the geopolitical fracturing of the global technology stack, the Russian Federation and the People's Republic of China have executed a comprehensive Joint Statement aimed at codifying their strategic alliance across critical cyber and technology domains. Issued during a high-profile bilateral summit on May 20, 2026, the document signals a concerted effort by Moscow and Beijing to institutionalize an alternative digital governance model, challenging Western supremacy in infrastructure control and cryptographic standard-setting. For global enterprise security leaders and defence stakeholders, this formalized technological pact establishes a powerful collaborative framework designed to build operational resilience against unilateral sanctions and coordinate responses to state-sponsored offensive threat actions. Operationally, the agreement focuses heavily on achieving full ICT supply chain independence, accelerating the development of indigenous core software, open-source architectures, and semiconductor fabrication pathways free from Western dependencies.

Factual and precise text within the strategic roadmap outlines extensive cooperation between national intelligence apparatuses and state-linked corporate entities to standardize cross-border data routing protocols, advance artificial intelligence (AI) safety parameters, and align sovereign cloud infrastructures. Crucially, the pact expands joint military-technical training to protect critical industrial assets and operational technology (OT) from external disruption, while actively promoting a doctrine of "cyber-sovereignty" within international bodies like the United Nations. For risk management practitioners, this alignment deepens the complexity of the cyber threat landscape, effectively creating a unified techno nationalist bloc capable of pooling zero-day research and intelligence capabilities. Ultimately, the development underscores that cyber resilience is no longer an isolated technical mandate but an extension of geopolitical strategy, forcing multinational organizations to navigate an increasingly bifurcated internet ecosystem where hardware and software compliance rules are starkly divided along geopolitical lines.

Read more: http://kremlin.ru/supplement/6487

Amid A Global Memory Chip Supply Crunch, Is China the Answer?

An escalating global memory chip supply crunch is forcing major Western hardware manufacturers like Apple and Dell into a critical strategic bind, testing the boundaries of U.S. export controls against commercial realities. This dilemma unfolds amid intensifying geopolitical tensions and a highly protective trade environment, where the United States has increasingly weaponized supply chain restrictions to curtail China's technological and military self-reliance. Despite the U.S. government explicitly designating two of China's leading domestic memory suppliers as Chinese military companies subjecting them to stringent regulatory scrutiny and trade barriers the sheer scale of the worldwide component shortage has prevented Western tech giants from entirely discarding Chinese semiconductor infrastructure. At the core of the development are state-backed semiconductor firms that have rapidly scaled production capabilities to fill the global vacuum in vital memory modules, presenting a highly cost-competitive lifeline for consumer electronics and enterprise server supply chains. Operationally, Western firms are forced to carefully balance these commercial supply benefits against severe compliance risks, knowing that

integrating components from restricted entities could trigger retaliatory regulatory penalties from Washington or expose hardware architectures to long-term national security vulnerabilities. For risk management professionals, corporate decision-makers, and policy stakeholders, this supply chain friction underscores the persistent fragility of decoupling strategies within highly integrated hardware ecosystems.

It demonstrates that when severe component shortages collide with geopolitical blockades, market demands frequently drive vendors toward legally precarious workarounds to sustain manufacturing volumes. Ultimately, this development signals that achieving absolute technological decoupling remains an elusive goal for defenders; as long as critical hardware elements remain concentrated within Chinese industrial clusters, global enterprise resilience and international tech-sector stability will remain deeply entangled with Beijing's manufacturing output.

Read more: https://www.thewirechina.com/2026/05/24/amid-a-global-memory-chip-supply-crunch-is-china-the-answer/

New Chinese surveillance leaves foreigners nowhere to hide

An unsecured database leak has exposed a massive escalation in state-sponsored surveillance by China's Public Security Bureau (PSB), expanding traditional counterintelligence into an automated, data-fused dragnet explicitly targeting foreign nationals, particularly journalists from "Five Eyes" nations. Discovered by cybersecurity researcher NetAskari via a leaked test dashboard for the Zhangjiakou PSB, the "Dynamic Management and Control Platform for Foreigners" marks a critical shift toward "holographic profiling." While historical state surveillance relied on disparate closed-circuit television networks under initiatives like the "Xueliang" (Bright Eyes) project, this modern framework leverages algorithmic data fusion. The platform aggregates unstructured real-time inputs including facial-recognition ticket gates at ski resorts, precise high-speed rail carriage and seat assignments, mobile payment logs, and fuel consumption metrics to construct predictive, 24/7 behavioural dossiers. Operational backend telemetry reveals that high-priority foreign assets are systematically labelled with a "trackable" real-time tag.

The moment an individual crosses into a monitored jurisdiction, automated indicators trigger early-warning notifications to local law enforcement, mapping out interpersonal relationships and generating automated network graphs based on physical proximity captured on camera. For defenders and risk management stakeholders, this intelligence development illustrates the weaponization of commercial data-aggregation techniques into counter-espionage infrastructure. By replacing human-intensive tailing operations with tire-less relationship-modeling algorithms evidenced by local procurement programs like the Shanghai Putuo PSB's "Holistic Personnel Archive System" the Chinese state has effectively eliminated operational anonymity within its borders. Consequently, international corporations, diplomatic missions, and non-governmental organizations must urgently reassess their operational security protocols; traditional countersurveillance tradecraft is rendered obsolete when physical transit, financial actions, and social networks are fully ingested into a centralized, predictive big-data engine designed to neutralize source confidentiality and corporate espionage defences.

Read more: https://www.dw.com/en/new-chinese-surveillance-leaves-foreigners-nowhere-to-hide/a-77246713

Российская Федерация, Rossiyskaya Federatsiya | Russian Federation

Kazuar: Anatomy of a nation-state botnet

In an exhaustive technical analysis, Microsoft Threat Intelligence has exposed the architectural evolution of "Kazuar," a sophisticated, custom-engineered cyberespionage malware family actively operated by the Russian state-sponsored threat group Secret Blizzard (formerly Turla). Historically focused on government, diplomatic, and military targets in Europe, Central Asia, and Ukraine, the threat actor has shifted away from monolithic backdoor frameworks toward highly modular peer-to-peer (P2P) botnet ecosystems. This structural pivot directly counters defender reliance on tracking native tools (living-off-the-land techniques), embedding operational stealth and infrastructure resilience natively into the malware to ensure long-term persistence and intelligence collection. Delivered via environmental-bound droppers like Pelmeni, Kazuar distributes its operational footprint across three specialized

modules: Kernel, Bridge, and Worker.

The Kernel acts as the central orchestrator, executing anti-analysis routines and managing up to 150 embedded configuration types, including specific exfiltration timeframes and extensive bypasses for the Antimalware Scan Interface (AMSI) and Event Tracing for Windows (ETW). Crucially, to evade network anomalies, Kazuar introduces an internal decentralized leadership election protocol using Windows Mailslots. Only the single elected "leader" Kernel maintains outbound communication via the Bridge module utilizing HTTP, WebSockets, or Exchange Web Services (EWS) while secondary "client" Kernels enter a silent state and receive delegated tasks locally over AES-encrypted named pipes. Simultaneously, Worker modules execute specialized surveillance payloads, including automated file harvesting, screenshot captures, and keylogging. Ultimately, Kazuar's shift to an interconnected, self-electing P2P architecture signals an advanced trend in nation-state cyber warfare toward highly resilient, low-observability infrastructure. For security operations centers and corporate risk managers, countering these stealthy botnets requires moving beyond standalone file hashes to monitor core behavioral markers, such as unusual inter-process communication (IPC) routines, local named pipe traffic, and leader-election anomalies within critical network sectors.

Read more: https://www.microsoft.com/en-us/security/blog/2026/05/14/kazuar-anatomy-of-a-nation-state-botnet/

Україна | Republic of Ukraine

Spear-phishing campaign targeting government organizations, orchestrated by the state-linked threat group UAC-0057

The Computer Emergency Response Team of Ukraine (CERT-UA) has issued an urgent technical advisory detailing a sweeping spear-phishing campaign targeting government organizations, orchestrated by the state-linked threat group UAC-0057 (also known as UNC1151). Occurring amid the protracted cyber-kinetic defence landscape in Eastern Europe, this activity illustrates the persistent focus of state-sponsored actors on executing long-term intelligence-gathering operations against public administration sectors. Operatives are leveraging compromised email accounts to distribute malicious PDF documents disguised as online course certificate notifications from the prominent educational platform Prometheus. Once an unsuspecting target opens the PDF and clicks the embedded link, a malicious ZIP file downloads containing a JavaScript file classified as "OYSTERFRESH." This initial stager displays a decoy document while writing an encoded and obfuscated malware variant, "OYSTERBLUES," directly into the Windows operating system registry.

Concurrently, it downloads and executes a decoder utility named "OYSTERSHUCK," which systematically unwraps OYSTERBLUES using string reversal, ROT13 transformation, and standard URL decoding. Once operational, the OYSTERBLUES component profiles the compromised endpoint harvesting the hostname, user account metadata, operating system version, system uptime, and active process lists before transmitting the telemetry via HTTP POST requests to a command-and-control (C2) server. The C2 infrastructure, obfuscated behind Cloudflare using top-level domains like .icu, responds with remote JavaScript payloads executed locally via the eval function, which analysts note frequently drops subsequent Cobalt Strike beacons for full network exploitation. For risk management professionals and defence stakeholders, this persistent campaign highlights the critical importance of endpoint attack surface reduction. Mitigating this specific threat requires enforcing strict Group Policy Objects (GPOs) to restrict wscript.exe execution for standard user profiles and rigorously monitoring anomalous outbound HTTP POST traffic, as bypassing credential perimeters via trusted third-party themes continuously tests national and corporate cyber resilience.

Read more: https://cert.gov.ua/article/6315762

Enter the Killer Robots: The Ukrainian Forging the Future of Warfare

In a definitive paradigm shift mirroring the broader transformation of modern asymmetric conflict, Ukraine's Ministry of Defense, under the leadership of newly appointed Defense Minister Mykhailo Fedorov, has institutionalized a comprehensive roadmap to embed artificial intelligence natively into front-line combat systems. The strategic pivot addresses an increasingly critical threat landscape where conventional warfare boundaries are overlapping into electronic warfare (EW) and localized internet blocking, forcing a dependency

on autonomous technologies to counter heavy GPS jamming and state-sponsored signal interference. Factual and operational details highlight Ukraine's launch of the Defense AI Center "A1," an advanced operational hub designed with British governmental backing to accelerate tactical decision-making and automate data-driven procurement. Architecturally, the initiative relies heavily on transitioning from manually operated drones to decentralized, AI-driven autonomous platforms and uncrewed ground vehicles (UGVs) equipped with computer-vision targeting and resilient optical navigation.

These systems utilize machine-learning algorithms to process battlefield telemetry in real time, enabling drones such as the newly deployed Hornet and fiber-optic variants to successfully lock onto, track, and strike targets completely independent of satellite connectivity or human intervention once a jamming threshold is breached. Simultaneously, the ministry has formalized automated data logging across its strategic Drone Line program to track target-attrition metrics and analyze operational vulnerabilities, an automated framework that reportedly contributed to a significant surge in adversary casualty rates throughout early 2026. For global defense planners and cybersecurity architects, the militarization of autonomous edge-computing platforms underscores the urgent evolution of the risk landscape. By removing the vulnerable radio-frequency links that traditional EW assets exploit, this AI-centric doctrine signals that future cyber-physical resilience will depend on securing local neural networks and building trusted, self-sustaining hardware supply chains capable of executing automated defense at machine speed.

Read more: https://www.nytimes.com/2026/05/15/world/europe/mykhailo-fedorov-ukraine-ai.html

Middle East | West Asia

Seedworm: Iran-Linked Hackers Breached Korean Electronics Maker in Global Spying Campaign

Symantec and Carbon Black threat intelligence teams have uncovered a sprawling global espionage campaign conducted by the Iranian state-linked cyber threat group Seedworm (also tracked as MuddyWater or Static Kitten), which successfully breached a major South Korean electronics manufacturer and at least eight other organizations across four continents during the first quarter of 2026. Attributed to Iran's Ministry of Intelligence and Security (MOIS), this multi-theater offensive underscores an aggressive geopolitical shift by Tehran to expand its traditional Middle Eastern footprint into a global intelligence-gathering dragnet. By targeting key high-tech, industrial manufacturing, public sector, and financial organizations, the threat actors seek to harvest highly sensitive intellectual property, extract proprietary technical research, and establish strategic chokepoints for downstream supply chain access. Factually, the campaign began around February 20, 2026, when Seedworm operatives established an initial foothold inside the South Korean electronics maker's network, maintaining undetected persistence for nearly a week. Technically, the group's tradecraft highlighted a disciplined move away from raw command-line executions toward quieter, runtime-orchestrated operations. Attackers leveraged a node.exe-based loader chain to drop an array of malicious Node.js and PowerShell scripts tasked with automated reconnaissance, screenshot capture, Security Account Manager (SAM) hive credential theft, and privilege escalation.

To bypass standard endpoint detection and response perimeters, the actors relied heavily on living-off-the-land binaries to execute dynamic DLL sideloading. Specifically, they dropped malicious components masquerading as valid libraries next to legitimately signed third-party executables, abusing Fortemedia's audio utility (fmapp.exe) to load fmapp.dll, and a SentinelOne security component (sentinelmemoryscanner.exe) to execute sentinelagentcore.dll. Both hijacked binaries ultimately ran ChromElevator, a public post-exploitation tool used to scrape sensitive user credentials, session cookies, and payment information from Chromium-based browsers, while simultaneously establishing persistent SOCKS5 reverse-proxy tunnels for interactive data exfiltration. Ultimately, this campaign introduces profound long-term risk management challenges for global supply chain resilience, corporate competitiveness, and international stability. By weaponizing trusted endpoint security binaries and commercial tools, Seedworm demonstrates that file-centric and signature-based defenses are insufficient against state-sponsored intelligence operations. Enterprise security leaders and defenders must urgently adopt rigorous, identity-first behavioral analytics and strict application whitelisting controls to counter this highly quiet, industrialized subversion of trust across

interconnected networks.

Read more: https://www.security.com/threat-intelligence/iran-seedworm-electronics

Fast and Furious – Nimbus Manticore Operations During the Iranian Conflict

Checkpoint Research has exposed an aggressive surge in cyber operations conducted by the Islamic Revolutionary Guard Corps (IRGC)-affiliated threat actor Nimbus Manticore (also tracked as UNC1549) during Operation Epic Fury, a U.S. military campaign against Iran initiated on February 28, 2026. This activity underscores a growing trend where nation-state groups rapidly adapt their software development lifecycles and distribution tactics to maintain high operational availability during active kinetic conflicts. Moving away from standard DLL sideloading, Nimbus Manticore deployed a sophisticated multi-wave campaign targeting defense, aviation, and software sectors across the United States, Europe, and the Middle East by exploiting AppDomain hijacking. This defensive evasion technique abuses legitimate .NET applications, such as Microsoft-signed binaries and hijacked Zoom installers, by planting Trojanized .config files to force the .NET runtime into loading malicious code within trusted system contexts. In a significant shift from traditional spear-phishing lures, the actors also utilized search engine optimization (SEO) poisoning, compromising search engine rankings on Bing and DuckDuckGo via keyword stuffing and domain-linking networks to redirect users seeking legitimate database tools to a malicious domain, getsqldeveloper[.]com.

Technically, the group debuted a previously undocumented, highly modular 64-bit Windows backdoor named "MiniFast." Strikingly, MiniFast's codebase features excessive error handling, defensive programming logic, and verbose method naming conventions that strongly indicate the integration of large language models (LLMs) and AI-assisted malware development. The implant establishes persistence by hijacking legitimate scheduled tasks, verifies its parent process architecture to evade sandbox detection, and communicates with command-and-control (C2) servers via JSON-formatted telemetry. For risk management professionals and enterprise decision-makers, this evolution signals a dangerous convergence of AI-accelerated malware production and advanced delivery vectors. Mitigating these risks requires strict verification of .NET application directories, application whitelisting, and monitoring for anomalous scheduled task modifications, as state-sponsored entities increasingly use automation to bypass traditional endpoint perimeters.

Read more: https://research.checkpoint.com/2026/fast-and-furious-nimbus-manticore-operations-during-the-iranian-conflict/

Introducing Showboat: A new malware family taunts defences and targets international telecom firms

Lumen Technologies' Black Lotus Labs, in collaboration with PricewaterhouseCoopers (PwC) Threat Intelligence, has uncovered a previously undocumented Linux-based post-exploitation framework dubbed "Showboat," which has been actively targeting international telecommunications providers and internet service providers since at least mid-2022. Attributed to multiple threat activity clusters aligned with the People's Republic of China (PRC) with strong ties to Chengdu-based infrastructure and tactical overlaps with the espionage group Calypso (aka Bronze Medley) this campaign underscores a critical geopolitical shift toward long-term surveillance of foreign critical infrastructure. By compromising telecommunications firms, state-sponsored actors aim to establish persistent, stealthy chokepoints to monitor downstream traffic, exploit supply chain relationships, and compromise high-value targets across interconnected global networks. Technically, Showboat operates as a highly modular ELF binary designed to secure an initial foothold and facilitate east-west lateral movement inside compromised local area networks (LANs). Once executing on a victim's system, the backdoor gathers comprehensive host configurations including operating system information, process lists, and desktop screenshots which it transmits to a command-and-control (C2) server via XOR-encrypted configuration files.

To evade standard network monitoring and security perimeters, the malware can hide its own system process, mask communications by potentially routing over port 53 (DNS), and utilize external dead-drop sites like Pastebin for dynamic code retrieval. Furthermore, the framework integrates custom SOCKS5 proxy and "portmap" functionalities, appending localized parameters like "SKS" or "MAP" to its callback URLs to interact with

internal, non-internet-facing segments. Analysts tracked the primary operational cluster through a unique self-signed X.509 certificate and identified spoofed infrastructure, such as singtelcom[.]site and kaztelecom[.]shop, which impersonated legitimate regional providers. Ultimately, this discovery highlights the advanced resource-pooling strategy utilized by Chinese threat groups, where modular toolsets like Showboat, ShadowPad, and NosyDoor are distributed through a centralized digital quartermaster to optimize operational efficiency. For security decision-makers and defence practitioners, mitigating this risk requires strict perimeter enforcement and rigorous monitoring of unusual internal lateral traffic, as the systematic exploitation of core networking infrastructure severely compromises downstream confidentiality and international cyber resilience.

Read more: https://www.lumen.com/blog/en-us/introducing-showboat-a-new-malware-family-taunts-defenses-and-targets-international-telecom-firms

Malware & Vulnerabilities

Multiple Vulnerabilities in NGINX Could Allow for Remote Code Execution

In a security development carrying substantial risk for global web infrastructure, the Multi-State Information Sharing and Analysis Center (MS-ISAC) issued a high-severity advisory (2026-051) detailing multiple vulnerabilities in F5's NGINX software suite. Given NGINX's critical role as a ubiquitous web server, reverse proxy, and load balancer, this security flaws present an immediate initial access vector for threat actors seeking to compromise internet-facing applications. The threat landscape has grown acutely volatile following independent confirmation from security firm VulnCheck that the most severe flaw, a heap-based buffer overflow tracked as CVE-2026-42945, is currently being actively exploited in the wild, alongside a public proof-of-concept exploit published by DepthFirst. Technically, CVE-2026-42945 resides within the ngx_http_rewrite_module component, where an unpropagated is_args flag during consecutive rewrite and set sequences triggers an undersized buffer allocation; subsequent processing copies attacker-controlled escaped URI data past the heap boundary, enabling unauthenticated remote code execution (RCE) on systems where Address Space Layout Randomization (ASLR) is bypassed or disabled.

The advisory documents three other critical flaws affecting major operational modules: CVE-2026-42946 in the scgi and uwsgi modules, where state mismatches induce massive cross-buffer pointer subtractions that crash worker processes; CVE-2026-40701, an asynchronous use-after-free bug in the SSL resolver module; and CVE-2026-42934, an off-by-one out-of-bounds read error within the charset parsing engine. Affected software ranges from legacy NGINX Open Source (versions 0.6.27 to 1.30.0) and NGINX Plus to enterprise deployments of NGINX Ingress Controllers and App Protect WAF platforms. For enterprise defenders and risk managers, these developments emphasize the systemic threat posed by infrastructure-level flaws, where successful RCE yields complete systemic administrative rights depending on worker process configurations. Organizations must urgently prioritize applying vendor-supplied patches, enforce strict network segmentation, and ensure anti-exploitation defenses like ASLR and least-privilege service configurations are universally enabled to mitigate cross-boundary network escalation.

Read more: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-nginx-could-allow-for-remote-code-execution_2026-051

The Microsoft Security Response Center (MSRC) | Statement

The Microsoft Security Response Center (MSRC) has issued a stern public condemnation targeting independent security researchers over a series of uncoordinated zero-day vulnerability drops, signalling a fracturing relationship between large tech vendors and the bug-hunting community. This escalation sits at the center of an intensifying debate over Coordinated Vulnerability Disclosure (CVD) frameworks, which defenders rely on to patch systems before malicious actors can operationalize exploits. The immediate trigger was the public release of proof-of-concept (PoC) code for six unpatched Windows vulnerabilities dubbed RedSun (CVE-2026-41091), UnDefend (CVE-2026-45498), BlueHammer (CVE-2026-33825), YellowKey (CVE-2026-45585), GreenPlasma, and MiniPlasma by a researcher operating under the alias "Nightmare Eclipse" (or Chaotic Eclipse). The researcher dropped the zero-days publicly following claims of mistreatment by Microsoft, including portal account

deletion and withheld bounty payments.

Microsoft has retaliated by working around the clock to develop emergency updates and explicitly declaring that its Digital Crimes Unit (DCU) will coordinate with global law enforcement to pursue legal action against actors who publish uncoordinated exploit code. This aggressive stance has drawn sharp pushback from prominent industry figures who argue that treating vulnerability disclosure as a criminal matter threatens to alienate the global research community and push independent analysts toward full public disclosure or underground monetization channels. For risk management professionals and enterprise decision-makers, this dispute highlights a systemic threat to the patch management pipeline; when communication breakdowns between vendors and researchers lead to retaliatory zero-day releases, defenders are stripped of their lead time, forcing security teams to scramble against immediate exploit availability. Ultimately, enforcing threat-hunting perimeters and maintaining strict defense-in-depth controls are critical as the digital ecosystem navigates the fragile, legal gray areas of modern vulnerability intelligence.

Read more: https://www.microsoft.com/en-us/msrc/blog/2026/05/a-shared-responsibility-protecting-customers-through-coordinated-vulnerability-disclosure

The FIFA World Cup 2026 Scam: CTM360 Reveals the full story

Cybersecurity researchers at CTM360 have exposed an expansive, highly structured cyber fraud ecosystem aggressively scaling to exploit the global buildup to the FIFA World Cup 2026. This surge underscores a persistent cybercrime trend where threat actors treat high-profile international sporting events as massive monetization horizons, leveraging brand impersonation and fan urgency to bypass standard psychological defences. According to the advisory, analysts identified more than 7,000 World Cup-themed domains, with a staggering 4,500 registered between December 2025 and April 2026 alone. Operating through the "Fraud Navigator" lifecycle, these campaigns systematically orchestrate infrastructure setup, social media impersonation, and fraudulent payment redirection. Attackers rely heavily on lookalike .com domains (89% of the ecosystem) mimicking official ticket sales, hospitality packages, and tourism services to trick users into submitting credit card data via fake checkout systems. Furthermore, threat actors are heavily utilizing major social platforms to execute multi-stage social engineering schemes, engaging victims directly via private messages before sending them to external payment channels.

Beyond financial fraud, the threat landscape has expanded into severe mobile malware distribution; researchers observed malicious Android APKs disguised as free IPTV streaming applications delivering the "BTMob" malware family. Once installed via sideloading, BTMob abuses Android accessibility services to intercept one-time passwords (OTPs), harvest SMS messages, capture screen telemetry, and steal cryptocurrency credentials. For risk management professionals, corporate security teams, and consumers, this development demands aggressive brand protection monitoring and strict endpoint perimeter enforcement. Mitigating these risks requires proactive blocking of typosquatted infrastructure, continuous takedowns of unauthorized social profiles, and educating users against installing unverified applications, as the industrialized convergence of financial fraud and high-capability spyware continuously threatens data confidentiality and broader digital resilience.

Read more: https://www.ctm360.com/reports/fifa-world-cup-2026-scams-surge-fraud-networks

Exploitation of Knowledge Deliver via View State Deserialization Vulnerability

Google Cloud's Mandiant and Google Threat Intelligence Group (GTIG) have exposed the active, zero-day exploitation of a critical security flaw in Knowledge Deliver, a prominent Learning Management System (LMS) developed by Digital Knowledge and widely deployed across Japan. Tracked as CVE-2026-5426, the flaw allows unauthenticated remote code execution (RCE) and positions learning management frameworks as primary supply chain vectors for broader enterprise compromise. This development aligns with a hazardous cyber threat trend wherein state-linked or highly capable financial threat actors systematically audit web development documentation and vendor software templates to uncover hardcoded secrets, allowing them to weaponize trusted codebases to compromise downstream client networks. Technically, the vulnerability is rooted in Digital Knowledge's reliance on a standardized web.config

file distributed across installations prior to February 24, 2026.

This deployment template contained identical, pre-shared ASP.NET machineKey values used by the underlying framework to sign and encrypt ViewState data. By leveraging these publicly exposed cryptographic keys, an unauthenticated attacker can craft a malicious __VIEWSTATE payload using public utilities like ysoserial.net and force the host server into deserializing untrusted input via standard HTTP POST requests. Incident response telemetry from late 2025 revealed that adversaries used this mechanism to deploy a .NET-based in-memory variant of the Godzilla web shell (tracked as BLUEBEAM) under the IIS worker process (w3wp.exe) context. This initial foothold enabled lateral movement, unauthorized file tampering to insert remote script loaders, and the ultimate drop of Cobalt Strike BEACON payloads to compromise connected user workstations. Security posture leaders must recognize that the systemic reuse of vendor static secrets neutralizes traditional network perimeters; identifying these intrusions demands rigorous log correlation specifically auditing Windows Application Event ID 1316 for "invalid ViewState" errors coupled with strict machine key rotation, immediate configuration file encryption, and continuous behavioural monitoring of anomalous web server child processes.

Read more: https://cloud.google.com/blog/topics/threat-intelligence/knowledgedeliver-viewstate-deserialization-vulnerability/

GlassWorm Exploited Unicode Shadows in VS Code Supply Chains

A malicious supply chain campaign targeting the Open VSX Registry has deployed a highly sophisticated malware framework dubbed "GlassWorm," which cleverly weaponizes Unicode blind spots to infect developer ecosystems. Uncovered initially by KOI Security and reverse-engineered by Endor Labs, the campaign distributed multiple malicious Visual Studio Code (VS Code) extensions that achieved more than 35,000 downloads before detection. GlassWorm marks an alarming evolution in software supply chain risks and defense evasion; while traditional security tools catch obvious obfuscation, this threat actor bypassed standard integrated development environment (IDE) warnings by abusing a specific subset of Unicode characters known as Variation Selectors (VS17 to VS256) and Private Use Area code points. Because these characters do not visually render in common code editors, the underlying payload remained entirely invisible to casual human review. Technically, the malware's package.json initiates a time-gated activation routine to evade dynamic sandbox environments. Once a configured cooldown period passes, an initialization script activates native binary decoders customized for Windows, Linux, and macOS.

These decoders execute simple offset arithmetic (codepoint - base_offset + 16) on the invisible Unicode strings, translating them into a Base64-encoded JavaScript payload. Upon executing the payload via eval(), GlassWorm establishes highly resilient, decentralized command-and-control (C2) infrastructure, polling transaction memos on the Solana blockchain and parsing encoded Google Calendar event titles for fallback IP routing. The final-stage malware functions as a powerful credential harvester—targeting over 70 cryptocurrency wallets alongside sensitive GitHub, NPM, and Open VSX tokens—while transforming the compromised developer workstation into a covert operational node hosting a SOCKS proxy and Hidden VNC (HVNC) server. Ultimately, the GlassWorm campaign demonstrates that relying on visual code audits or standard static analysis is no longer sufficient to guarantee pipeline integrity. For security decision-makers and DevOps teams, neutralizing this threat requires enforcing automated pre-commit hooks that strictly flag unusual Unicode ranges and continuously monitoring anomalous developer workstation telemetry, as state-linked and sophisticated financial actors increasingly turn trusted programming tools into invisible beachheads for broader enterprise infiltration.

Read more: https://www.endorlabs.com/reports/invisible-threats-glassworm-unicode-vscode

About the Author

Govind Nelika is a Researcher, Web Manager, and Outreach Coordinator at the Centre for Land Warfare Studies (CLAWS), working on national security issues at the intersection of technology, cybersecurity, and geopolitics. His research focuses on hybrid warfare, digital influence operations, semiconductor geopolitics, AI-enabled conflict, and cyber governance, with publications covering topics such as U.S.–China tech rivalry, the Quad's cyber dynamics, and emerging risks in AI and supply chains. He previously worked at Pondicherry University under the UGC-SAP (DRS II) programme in the Department of Politics & International Studies, progressing from Project Fellow to Project Associate. He holds a degree in Political Science and a Data Science certification from IBM. Earlier in his career, he gained research and digital management experience with the Regional Centre of Expertise, Trivandrum (affiliated with the United Nations University), and the Bureau of Police Research & Development (BPRD), Ministry of Home Affairs where he conducted research on cybercrime trends in India. He was awarded the Chief of Army Staff (COAS) Commendation Card on Army Day 2025 for his contributions to CLAWS