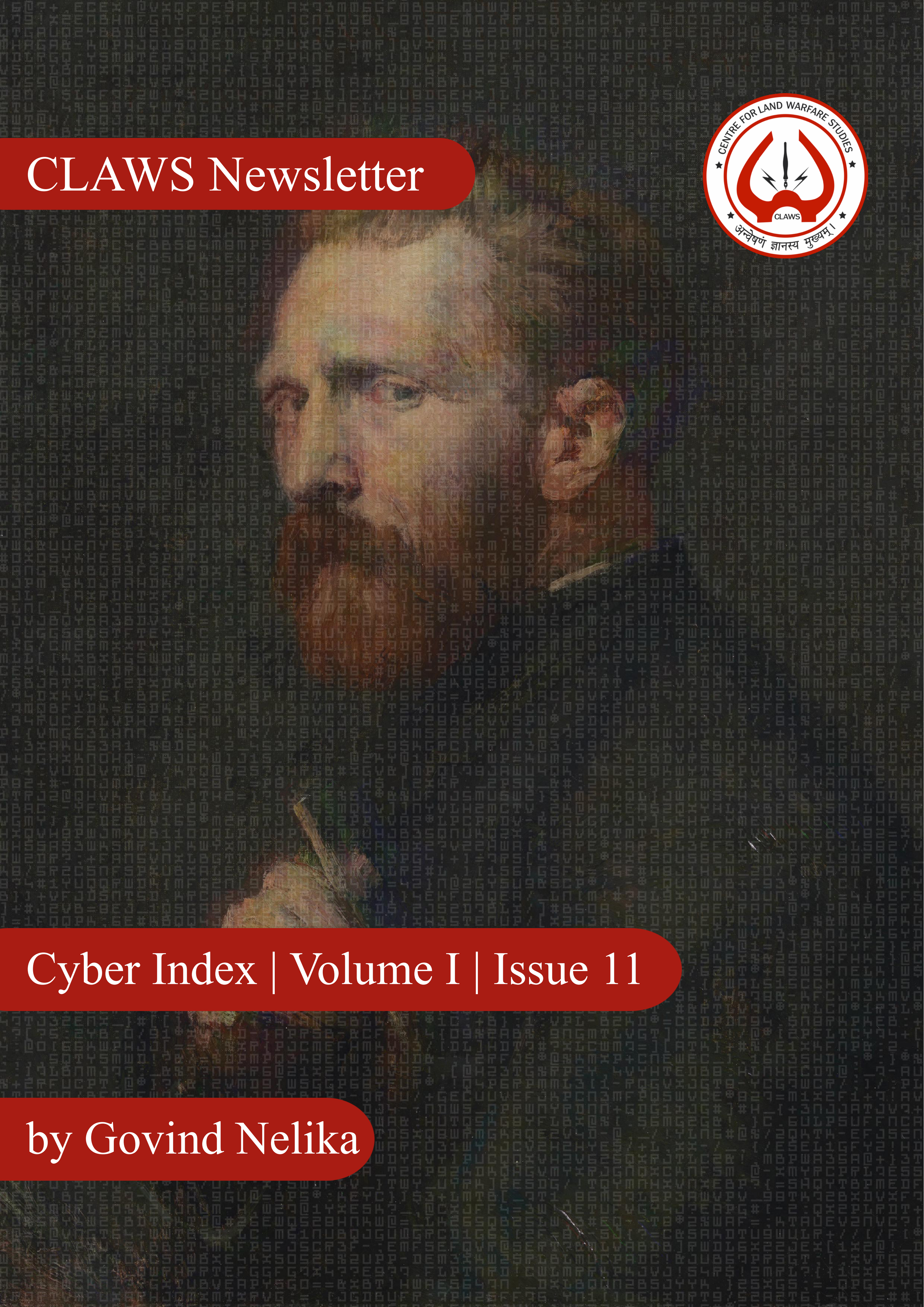

CENTRE FOR LAND WARFARE STUDIES

CLAWS

अन्वेषणं ज्ञानस्य मुख्यम्।

CLAWS Newsletter

Cyber Index | Volume I | Issue 11

by Govind Nelika

About us

The Centre for Land Warfare Studies (CLAWS) is an independent think tank based in New Delhi, India, dedicated to strategic studies and land warfare in the Indian context. Established in 2004 and registered under the Societies Registration Act, 1860, CLAWS operates as a membership-based organization governed by a Board of Governors and an Executive Council, under the Aegis of the Indian Army.

With a futuristic outlook and a policy-oriented approach, CLAWS focuses on national security issues, conventional military operations, and sub-conventional warfare. The Centre closely monitors regional conflicts and military developments within India's strategic frontiers, particularly in South Asia.

Committed to fostering strategic culture and informed policymaking, CLAWS disseminates its research to armed forces personnel, policymakers, members of the strategic community, and interested civilians. By facilitating in-depth studies and discussions, CLAWS contributes to shaping India's defense policies and military preparedness.

The CLAWS Newsletter is a newly fortnightly series under the leadership of Dr. Tara Kartha, Director Research & Academics. The newsletter features insightful content curated by CLAWS researchers, each specializing in their respective verticals. This initiative aims to provide in-depth analysis, strategic insights, and updates on key issues.

Contents

Global Brief

Behind the Clouds: Attackers Targeting Governments in Southeast Asia Implement Novel Covert C2 Communication

Unit 42 of Palo Alto Networks has identified a covert cyber espionage campaign, dubbed CL STA 1020, targeting government agencies in Southeast Asia via a novel Windows backdoor named HazyBeacon. The campaign, active since late 2024, is aimed at harvesting sensitive data such as tariff positions and trade dispute information, exploiting legitimate cloud services to hide its activities. Attackers use DLL sideloading, planting a malicious mscorsvc.dll alongside the legitimate mscorsvw.exe, which then initiates C2 communication over HTTPS to attacker-controlled AWS Lambda URLs a novel method that blends malicious traffic with usual cloud usage. This C2 channel fetches payloads including file-collection tools and Google Drive/Dropbox uploaders (igfx.exe, GoogleDriveUpload.exe, etc.), used to collect and exfiltrate target documents before hiding traces. Persistence is maintained through a newly created Windows service, msdnetsvc, ensuring the backdoor remains active after reboot.

By exploiting serverless infrastructure, the threat actors capitalize on trusted AWS domains to evade detection, while leveraging common cloud platforms for exfiltration, making network based detection challenging without behavioral analysis. The campaign reflects a broader trend of fileless, cloud centric intrusion tactics, where adversaries increasingly harness legitimate services for stealth and scalability. For defenders, effective detection requires enhanced monitoring of cloud resources, anomaly-based inspections of AWS communications, and alerting on unusual services such as DLL sideloading or new service registrations.
Strategically, CL STA 1020 underscores how state-aligned APT operations are evolving blending traditional malware techniques with innovative C2 channels via trusted infrastructure. These tactics amplify intelligence-gathering capabilities while complicating attribution and detection. The emergence of serverless based backdoors marks a pivotal shift in cyber espionage tradecraft and signals the urgent need for cloud-aware defence mechanisms across national security and public sector domains.

Read more: https://unit42.paloaltonetworks.com/windows-backdoor-for-novel-c2-communication/

Japan and EU envision satellite network to cut reliance on US, SpaceX

Japan and the European Union are collaborating on the development of a joint satellite network aimed at reducing dependence on U.S.-based providers, particularly SpaceX, for space-based infrastructure. The initiative reflects growing concerns over strategic autonomy in the context of rising geopolitical tensions and vulnerabilities in global supply chains. As nations increasingly rely on satellite communications for critical infrastructure—ranging from defense and disaster response to telecommunications and economic data exchange—relying on a small number of foreign commercial providers has raised alarms about sovereignty and resilience. The proposed network would include next-generation low-Earth orbit (LEO) satellites designed to provide secure, high-speed communications and bolster navigation and Earth observation capabilities. Both Japan and the EU view this partnership as a step toward ensuring independent access to space and safeguarding key technological ecosystems against disruptions or coercive pressure from major global powers.

Technical planning includes integrating advanced cybersecurity and quantum encryption measures to protect against cyberattacks and surveillance, while ensuring interoperability with existing satellite systems. The effort is part of broader strategies such as the EU's IRIS² project and Japan's ambitions under its Basic Space Plan. The development will likely involve domestic aerospace and telecommunications firms from both regions, with joint research and infrastructure funding. Strategically, the project reinforces both regions' commitment to multilateral cooperation in securing the global commons, while asserting greater independence in an increasingly contested space domain. It also represents a growing trend of regional space partnerships seeking alternatives to dominant actors such as the United States, China, and Russia. If successful, the network could serve as a model for similar collaborative efforts among democracies seeking to protect their interests in the new space race. The project has far-reaching implications for national security, economic resilience, and the balance of power in space-based infrastructure.

Read more: https://asia.nikkei.com/Business/Aerospace-Defense-Industries/Japan-and-EU-envision-satellite-network-to-cut-reliance-on-US-SpaceX

Russia field-testing new AI drone powered by Nvidia's Jetson Orin supercomputer

Ukrainian military intelligence has confirmed that Russia is field testing a highly advanced autonomous strike drone, designated MS001, an upgraded variant of the Iranian Shahed 136/Geran 2 loitering munition. Core to this development is its integration of Nvidia's handheld Jetson Orin AI supercomputer capable of 67 TOPS inference and 102 GB/s memory bandwidth enabling real time thermal imaging and object recognition, and granting the drone the ability to identify, prioritize, and strike targets without external input. Equipped with a CRPA antenna to resist GPS spoofing or jamming, FPGA based adaptive logic, a thermal imager, and encrypted telemetry radios, the drone retains the original navigation and flight controller systems of its predecessor while adding a high definition Ezcap video encoder for 60 fps digital streaming.

Operational testing took place near Sumy, where at least one unit was downed for technical analysis. Ukrainian officials describe it as a "digital predator" capable of independent target selection and engagement, even when GPS is unavailable. The drone also supports swarm coordination and resilience in contested environments, potentially enabling coordinated, multi unit operations with minimal human intervention.

This marks a significant evolution in unmanned aerial systems by shifting autonomy from remote piloting to onboard AI decision making. Militarily, MS001 represents a breakthrough in strike systems: its autonomous targeting and resistance to electronic countermeasures suggest Russia is overcoming Western export controls by sourcing Nvidia chips via third party channels. Strategically, the deployment of AI powered "digital predator" drones underscores the intensifying arms competition in the Ukraine conflict and points to a global trend toward autonomous, hybrid warfare. Such capabilities demand urgent reassessment of air defence, electronic warfare, and policy on lethal autonomous weapons signalling a new era in drone enabled conflict.

Read more: https://www.techspot.com/news/108579-russia-field-testing-new-ai-drone-powered-nvidia.html?

Republic of India | Bharat

TAG 140 Targets the Government of India Via 'ClickFix Style' Lure

TAG 140, an APT group linked to Pakistan's Transparent Tribe, has launched a targeted cyber espionage campaign against key Indian government ministries using a new Remote Access Trojan (RAT) called "DRAT V2." Identified by researchers at Recorded Future, the campaign is delivered via spear phishing emails and a spoofed Ministry of Defence portal, using a ClickFix style lure to execute malicious scripts that install DRAT V2 through the BroaderAspect .NET loader. DRAT V2, now Delphi compiled, features a custom TCP C2 protocol and enhanced capabilities for system reconnaissance, data theft, and command execution. The campaign reflects TAG 140's modular malware strategy and highlights growing cyber tensions in the Asia Pacific, underscoring the need for strong phishing defences, script monitoring, and network traffic analysis.

The operation underscores TAG-140's strategy of "modular malware rotation", layering BroaderAspect and DRAT variants to maintain agility and evade attribution ([recordedfuture.com][2]). By targeting critical infrastructure ministries using tailored phishing campaigns and lightweight RATs, the group enhances its espionage and surveillance reach across high value networks.

Strategically, this campaign exemplifies the intensifying cyber competition in the Asia-Pacific region, where state-linked actors exploit social engineering and persistent malware to infiltrate government systems. It reflects broader trends in APT operations: custom malware development, flexible command and control frameworks, and focused attack chains aimed at sensitive national infrastructure. Defence against DRAT V2 requires vigilant phishing awareness, mshta.exe monitoring, registry audits, and network analysis for unusual

TCP connections and Base64-encoded traffic patterns.

Read more: https://www.darkreading.com/threat intelligence/tag 140 indian government clickfix lure?

United States of America (USA)

US defence firms to 'remain vigilant' against Iranian cyber activity, agencies warn

The main subject is a joint cybersecurity alert issued on June 30, 2025, by four U.S. government entities CISA, FBI, NSA, and the Department of Defence's DC3 warning of heightened cyber threat activity from Iranian state affiliated actors and allied hacktivist groups targeting critical U.S. infrastructure. The alert emphasizes Defence Industrial Base organizations engaged with Israeli research or defence firms as particularly vulnerable.

The broader context includes lingering geopolitical tensions following recent conflicts, including the Israel–Hamas war, which CISA notes has triggered spikes in disruptive cyber warfare like website defacements, data leaks, and increased DDoS activity. Technologically, the Iranian cyber adversaries are exploiting weakly secured systems favouring legacy software, unpatched CVEs, default credentials, and internet exposed industrial control systems (ICS/OT).

Specific findings highlight routine methods such as automated password guessing, hash cracking with online tools, and using default manufacturer passwords for initial access. On ICS/OT environments, attackers are deploying diagnostic or engineering tools to penetrate operator interfaces, PLCs, HMIs, third party vendor systems, and leveraging these to disrupt or sabotage industrial processes. Iranian affiliated hacktivist groups have engaged in hack and leak operations, defacements, and DDoS, with a likely escalation in the context of ongoing regional tensions.

Further, these state aligned actors have been observed collaborating with criminal ransomware affiliates coordinating access and encryption in exchange for payment, alongside leak and extortion tactics. Historical precedent is provided: in late 2023–early 2024, IRGC linked actors exploited default password PLCs and HMIs in sectors like water, energy, and healthcare, affecting U.S. organizations directly.

On the defensive front, the agencies strongly recommend critical infrastructure organizations disconnect OT/ICS systems from the public internet, enforce strong unique passwords or MFA, patch known CVEs, disable insecure remote access protocols, monitor logs, enforce RBAC, and prepare incident response and business continuity plans.

Strategic implications are clear: Iran's cyber capabilities are advancing in sophistication, blending state goals with hacktivist disruption and cybercrime collaboration. The alert underscores that even in the absence of a fully coordinated campaign, opportunistic exploitation poses a clear threat to U.S. critical sectors. This reflects a broader trend of weaponized cyber espionage and hybrid tactics by state affiliated adversaries emphasizing heightened vigilance, resilience, and defensive preparation in national security strategy.

Read more: https://www.cisa.gov/resources tools/resources/iranian cyber actors may target vulnerable us networks and entities interest

DARPA picks Bell Textron to build runway-independent X-Plane

The U.S. Defence Advanced Research Projects Agency (DARPA) has selected Bell Textron to design and build a next-generation experimental aircraft under its SPRINT (Speed and Runway Independent Technologies) X-plane program. This initiative aims to develop a high-speed, vertical take-off and landing (VTOL) platform that eliminates the need for conventional runways while achieving jet-like cruise speeds. The key objective is to combine the operational flexibility of a helicopter with the speed and range of a fixed-wing aircraft, providing the U.S. military with new strategic options for rapid response and distributed operations in contested environments. Bell Textron, known for its tiltrotor technologies such as the V-22 Osprey and V-280 Valor, is expected to leverage its expertise in propulsion integration and flight control to deliver a novel aircraft capable of sustained speeds above 400 knots.

DARPA's focus on runway independence and agility reflects broader concerns over the vulnerability of large airbases in future conflicts, particularly in the Indo-Pacific region, where dispersed and mobile logistics are critical for maintaining operational advantage. The SPRINT program will culminate in a flight demonstration scheduled for 2027, and it is designed to validate key technologies such as thrust vectoring, adaptive wing configurations, and high-lift systems. The aircraft must achieve rapid transition between vertical and horizontal flight while operating in austere environments with limited infrastructure.

Strategically, this effort aligns with the Pentagon's vision of agile combat employment (ACE) and the push toward distributed airpower, especially in scenarios where adversaries possess advanced anti-access/area denial (A2/AD) capabilities. Bell's selection also highlights continued investment in future vertical lift capabilities beyond traditional rotorcraft. If successful, the SPRINT X-plane could serve as a testbed for follow-on platforms across all military services, reshaping how forces are deployed, supported, and sustained in dynamic conflict zones.

Read more: https://breakingdefense.com/2025/07/darpa-picks-bell-textron-to-build-runway-independent-x-plane/?

Senate panel OKs Trump's national cyber director nominee

Sean Cairncross, President Trump's nominee for National Cyber Director, has been approved by the Senate Homeland Security Committee in an 11–4 vote, moving his nomination to the full Senate. The National Cyber Director plays a key role in coordinating federal cybersecurity policy and inter agency strategy. Cairncross, a political strategist and former Millennium Challenge Corporation CEO, lacks technical cybersecurity experience but emphasizes his leadership and organizational background. While critics express concern over his limited cyber expertise and potential federal workforce cuts, supporters including former National Cyber Director Chris Inglis highlight his management skills and ability to drive policy coordination. His nomination reflects a broader shift toward prioritizing executive oversight and inter agency alignment in national cyber strategy amid evolving digital threats.

Read more: https://www.scworld.com/brief/senate panel oks trumps national cyber director nominee

US Treasury Sanctions Global Bulletproof Hosting Service Aeza Group for Enabling Cybercriminal Activity

Aeza Group, a Russia based bulletproof hosting (BPH) provider, and its affiliates have been sanctioned by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) in coordination with the UK National Crime Agency. The sanctions target Aeza Group, its UK front company Aeza International Ltd., Russian subsidiaries Aeza Logistic LLC and Cloud Solutions LLC, and four executives CEO Arsenii Penzev, General Director Yurii Bozoyan, Technical Director Vladimir Gast, and part owner Igor Knyazev who collectively facilitated cybercriminal operations.

Technically, Aeza operated by leasing IP addresses via their UK branch and providing backbone infrastructure for command and control servers, malware distribution, and secure cryptocurrency cash outs. Blockchain analysis revealed a TRON based crypto wallet linked to the group, which moved over $350,000 through exchanges and darknet related financial flows.

By targeting the infrastructure rather than only individual hackers, OFAC's action under Executive Orders 13694 and related amendments aims to choke the supply chains enabling large scale cyber operations. All U.S. based assets of the sanctioned entities and individuals are frozen, and U.S. persons are barred from engaging with them. This builds on earlier sanctions against providers like ZServers and is part of a strategic trend toward dismantling facilitation networks that underpin ransomware, data theft, and illicit online marketplaces. Strategically, these measures reflect a broadened approach in cybersecurity enforcement shifting focus from chasing threat actors to dismantling the support infrastructure that empowers them. This action strengthens global efforts to degrade cybercriminal ecosystems, integrate sanctions with crypto tracing intelligence, and guard critical sectors from escalating digital threats.

Read more: https://www.trmlabs.com/resources/blog/treasury_sanctions_global_bulletproof_hosting_service_aeza_group_for_enabling_cybercriminal_activity

People's Republic of China (PRC) | China

North American APT-Q-95 targeting China identified by cybersecurity firm Qianxin

The Chinese cybersecurity firm Qianxin has revealed the operations of a highly sophisticated advanced persistent threat (APT) group, codenamed NightEagle (APT-Q-95), believed to be a North America-based state-sponsored actor targeting China's critical industries. This group has conducted cyber-espionage campaigns against high-value sectors including semiconductors, quantum computing, artificial intelligence (particularly large language models), and military technology. NightEagle's hallmark is its use of rapidly shifting infrastructure—constantly rotating domains and IP addresses—and exploiting unknown zero-day vulnerabilities in Microsoft Exchange servers to implant memory-resident malware undetectable by conventional antivirus tools.

The group employs modified versions of the open-source tunneling tool Chisel, repurposed to maintain persistent command-and-control (C2) connections via scheduled tasks. The primary delivery mechanism includes fake processes like SynologyUpdate.exe contacting disguised domains such as synologyupdates.com. Once inside a network, the attackers use ASP.NET-based memory loaders (e.g., App_Web_cn.dll) injected into Exchange's IIS service to create virtual URL paths that execute payloads through server-side deserialization, granting them remote access to emails and sensitive data. Notably, the malware operates exclusively during nighttime Beijing hours (9 p.m. to 6 a.m.), consistent with working hours in the U.S. Pacific time zone, suggesting a Western origin. Analysis indicates that every domain was tailored for a unique target, with attackers adapting malware and infrastructure per campaign.

NightEagle's infrastructure is tied to U.S.-based cloud providers including DigitalOcean and Akamai, and its domain registrations were traced to the registrar Tucows. The group's activities correlate with major geopolitical events and shifts in Chinese AI research development, showing a strategic interest in emerging technologies.

Strategically, this campaign illustrates a high-level convergence of espionage tradecraft, technical innovation, and geopolitical targeting. It highlights the evolving threat landscape where APTs increasingly combine zero-day exploits, fileless malware, and AI-related reconnaissance to compromise national security assets. The disclosure underscores the importance of real-time threat intelligence, deep packet inspection, and cross-platform visibility for detecting sophisticated intrusions.

Read more: https://raw.githubusercontent.com/RedDrip7/NightEagle_Disclose/36d0366a5d8d4c-b2ee95b0276d0f5690e13e3f6e/Exclusive%20disclosure%20of%20the%20attack%20activities%20of%20the%20APT%20group%20NightEagle.pdf

Award-winning data scientist She Yiyuan takes job in China after decades in US

She Yiyuan, an award-winning statistician and data scientist, has returned to China after nearly two decades at Florida State University to take up a prestigious chair professorship at Westlake University's School of Science and Institute for Theoretical Sciences in Zhejiang Province. A recipient of the U.S. National Science

Foundation's esteemed Career Award and a fellow of major statistical bodies including the American Statistical Association, Institute of Mathematical Statistics, and International Statistical Institute—She brings world-class expertise in high-dimensional statistics, machine learning, optimization, and robust data analysis. His multidisciplinary research integrates statistics, mathematics, and computer science to produce novel machine-learning methods and tools applied across fields such as biomedicine and economics.

This move occurs amid intense global competition in AI and advanced technology, where China is actively recruiting overseas talent to enhance its strategic capabilities. Westlake University emphasises that strengthening statistics—a foundational discipline for AI and data science supports national ambitions in emerging high-tech sectors. She's appointment aligns with broader efforts to elevate China's research institutions and close the innovation gap with Western countries.

Strategically, his return underscores China's talent repatriation campaign, leveraging the expertise of scientists educated abroad to accelerate domestic development in AI, big data, and high-performance computing. It signals a sustained push toward self-reliance in core technologies, reflecting global trends in technology competition where nations vie for leadership in foundational science. His presence at Westlake is likely to advance China's theoretical and applied research, foster interdisciplinary collaboration, and bolster its position within the international scientific community.

Read more: https://www.scmp.com/news/china/science/article/3317558/award-winning-data-scientist-she-yiyuan-takes-job-china-after-decades-us

China discovers significant source of lithium ores

China has announced the discovery of a significant lithium ore deposit in Linwu County, Hunan Province, positioning itself even more strategically in the global race for critical minerals. The Jijiaoshan mining area, where the find occurred, holds an estimated 490 million tonnes of lithium ore containing approximately 1.31 million tonnes of lithium oxide. This deposit is classified as an altered granite-type lithium deposit, a category known for its large-scale and economically viable extraction potential. In addition to lithium, the site also contains rubidium, tungsten, and tin—valuable minerals used in various high-tech and industrial applications. The discovery was made possible by advances in geological survey technologies and the culmination of years of exploration led by the Mineral Resources Survey Institute of Hunan Province.

According to experts, such as Professor Xu Yiming, the deposit is expected to bolster Chenzhou's ambitions in expanding its new-energy industry, aligning with China's broader push toward electric vehicles (EVs), energy storage, and renewable technologies. As lithium is a key input in batteries for EVs, smartphones, and grid-scale storage, this discovery has important economic and geopolitical implications. It enhances China's already considerable leverage in the global supply chain for critical energy transition materials. The China Geological Survey previously reported that the nation's lithium reserves now account for 16.5% of the global total, ranking second globally. This find strengthens China's position in global lithium markets at a time when major economies are striving to secure stable and sustainable supplies amid rising demand. The strategic importance of this discovery extends beyond industrial value; it reinforces China's ability to influence the pace and cost of global electrification efforts, and may intensify geopolitical competition over resource control and technology supply chains as the world accelerates its shift to green energy.

Read more: https://english.news.cn/20250708/8282522a30df4d8691dca91c24e3994c/c.html

Republic of China (ROC) | Taiwan

Silver Fox Suspected in Taiwanese Campaign Using DeepSeek Lure

The recent cyber espionage campaign attributed to the China linked threat group Silver Fox has targeted Taiwanese organizations and individuals through the use of trojanized installers for widely used Chinese language applications, including the R1 large language model by DeepSeek, WPS Office, and Sogou Search. This operation reflects ongoing geopolitical tensions between China and Taiwan, with cyber capabilities increasingly deployed as tools of state influence and surveillance. The attackers utilized spoofed Mandarin language websites that mimic official download portals to distribute malware laced software, effectively weaponizing the growing popularity of generative AI tools to increase infection rates.

Upon execution, the malicious installers deploy Sainbox RAT a modified variant of the Gh0st remote access trojan alongside the Hidden rootkit, enabling extensive system compromise. These tools grant attackers remote command execution, credential harvesting, data exfiltration, and long term persistence. Silver Fox is known for its use of DLL sideloading and bring your own vulnerable driver (BYOVD) techniques to escalate privileges on compromised Windows hosts. The malware exhibits strong obfuscation, encrypted command and control communications, and adaptability across sectors, allowing stealthy infiltration into government, healthcare, and industrial networks.

Security researchers observed that the campaign did not focus on specific organizations but rather used a wide net approach that resulted in infections across multiple sensitive sectors in Taiwan. Victims included entities handling medical records, government communications, and intellectual property, raising concerns about the potential for espionage, surveillance, and data manipulation.

This operation exemplifies the convergence of AI tool proliferation and advanced persistent threat (APT) operations, with threat actors exploiting public trust in new technologies to execute covert intrusions. Strategically, it underscores the national security challenges posed by hybrid cyber operations blending misinformation, malware delivery, and state aligned targeting. The incident highlights the need for strengthened software provenance verification, robust endpoint monitoring, and regional cybersecurity cooperation to deter and detect such increasingly sophisticated state backed intrusions.

Read more: https://www.darkreading.com/cyberattacks data breaches/silver fox suspected taiwanese campaign deepseek?

Europe

Chinese Hacker, Wanted By US For Stealing COVID-19 Data, Arrested in Italy

Italian law enforcement, in cooperation with U.S. authorities, has arrested a Chinese national named Xu Zewei at Milan's Malpensa Airport on July 3, 2025, in connection with a high-profile cyber espionage operation targeting COVID 19 vaccine research. Xu, 33, allegedly worked under China's Ministry of State Security and its Shanghai State Security Bureau, as part of the notorious Hafnium hacking group. Between February 2020 and June 2021, he is accused of infiltrating U.S. universities and research labs particularly those in Texas and North Carolina using Microsoft Exchange Server vulnerabilities and sophisticated web shells to steal sensitive immunology and virology data. Federal prosecutors have unsealed a nine-count indictment from the Southern District of Texas charging Xu with conspiracy, wire fraud, unauthorized computer access, and aggravated identity theft.

His arrest follows more than a year on the run alongside co-conspirator Zhang Yu, who remains at large. U.S. officials contend the operation targeted over 12,700 U.S. entities and thousands of academic and biomedical institutions, aligning with state-directed efforts to boost China's medical research capabilities. Xu now faces extradition proceedings in Italy, which could strain diplomatic dynamics as Italy balances its NATO alliance with economic ties to China. Strategically, the arrest demonstrates enduring international resolve to hold foreign cyber operatives accountable, reinforces the global law enforcement response to state-sponsored hacking, and underscores the necessity of securing critical research infrastructure against advanced persistent threats.

Read more: https://www.ndtv.com/world-news/chinese-hacker-wanted-by-us-for-stealing-covid-data-arrested-in-italy-8852167

West Asia

Iranian Ransomware Crew Blurs the Line Between Profit and Proxy Attacks

The central focus is on Pay2Key.I2P, an Iranian linked ransomware crew operating a Ransomware as a Service (RaaS) platform that blends profit driven extortion with state aligned cyber operations. Emerging from its predecessor, Pay2Key tied to Iran backed APT group Fox Kitten Pay2Key.I2P has escalated activity amid regional tensions with Israel and the United States, reportedly amassing over USD 4 million in ransom payments within four months. To intensify geopolitical targeting, the group recently increased affiliate payouts to 80% for attacks against U.S. and Israeli entities, framing these operations as ideological responses to military aggression against Iran.

Pay2Key.I2P recruits its operators on Russian language cybercrime forums and has formed operational ties with Mimic ransomware developers, whose codebase partially derives from the disbanded Conti gang. By mid June, the group had executed more than 50 ransomware campaigns, some of which utilized wiper style tools disguised as encryptors merging sabotage techniques typical of state cyber operators with extortion tactics. This dual use model allows plausible deniability: ransomware creeps into a victim's environment under the guise of financially motivated crime, while covertly achieving state aligned goals.

Technically, the operation follows a classic RaaS playbook: affiliate operators carry out attacks and share ransom revenues, but the inclusion of wiper components signals a shift toward destructive cyber capabilities. This approach may involve initial data exfiltration for double extortion, enhanced with destructive payloads if payment demands are not met. Strategically, Pay2Key.I2P exemplifies the hybridization of cyber threat models, where state aligned espionage and sabotage converge with criminal monetization. This fusion strengthens Iran's cyber posture, enabling attacks that are both ideologically motivated and financially self sustaining, while obscuring attribution. The phenomenon amplifies the international cybersecurity challenge: defenders must now anticipate cyber threats that seamlessly integrate espionage, sabotage, and extortion demanding comprehensive detection, response strategies, and global cooperation.

Read more: https://www.halcyon.ai/blog/iranian ransomware crew blurs the line between profit and proxy attacks

Malware & Vulnerabilities

Unmasking AsyncRAT: Navigating the labyrinth of forks

ESET researchers have mapped the sprawling ecosystem of AsyncRAT, an open-source remote access trojan released in 2019, which has become a prolific framework spawning numerous forks and variants exploited by cybercriminals. Originally written in C#, AsyncRAT shares cryptographic roots with earlier RATs like Quasar but introduced enhanced modularity and stealth, enabling dynamic adaptation and widespread abuse. Analysis reveals prominent offshoots such as DcRat and VenomRAT, which dominate campaigns and extend capabilities—DcRat, for example, employs Message Pack for data serialization and patches security features like AMSI and ETW, while offering plugins for webcam access, microphone recording, Discord token theft, and even embedded ransomware via AES-256 encryption.

Beyond mainstream variants, lesser-known forks like NonEuclid RAT introduce niche features including jump-scare payloads, USB infection modules, clipboard hijacking (to steal cryptocurrency), and brute-forcing routines. These forks maintain a shared foundational structure—encrypted configuration using AES-256 with base64 encoding—while diverging through varied salts, certificates, plugin architectures, and obfuscation techniques. ESET outlines systematic methods to dissect and distinguish forks: analysing version labels, salt values, embedded certificates, and packet patterns for command-and-control (C2) infrastructure.
This proliferation illustrates a broader malware trend: open-source frameworks act as breeding grounds for rapid innovation and customization, lowering entry barriers for threat actors and raising detection challenges.

Key tactics across these RAT variants include process injection, disabling security telemetry, credential theft, lateral movement, and file encryption. By acknowledging this intricate “labyrinth of forks,” defenders can better target shared behaviour patterns and infrastructure characteristics rather than relying solely on signature-based detection. Strategically, the evolving AsyncRAT network highlights the necessity for behavioural and threat intelligence-driven defences to counter increasingly modular and adaptable malware architectures that threaten enterprise and critical systems globally.

Read more: https://www.welivesecurity.com/en/eset-research/unmasking-asyncrat-navigating-labyrinth-forks/

SEO Poisoning Campaign Targets 8,500+ SMB Users with Malware Disguised as AI Tools

A large scale SEO poisoning campaign, attributed to cybercriminals, has targeted over 8,500 small and medium sized business (SMB) users by surreptitiously leveraging search engine results to distribute malware disguised as legitimate software and AI tools. Researchers at Arctic Wolf discovered that fake websites masquerading as trusted download portals for utilities like PuTTY and WinSCP appear high in search results, tricking users into installing a malicious loader known as Oyster (also called Broomstick or CleanUpLoader). Once executed, Oyster establishes persistence by creating a scheduled task that launches a malicious DLL (twain_96.dll) via rundll32.exe, using DllRegisterServer to maintain its foothold.

The campaign also exploits popular AI and collaboration related search terms such as ChatGPT, Zoom, Teams, Outlook, Excel, and Word to distribute additional malware loaders, including Vidar Stealer, Lumma Stealer, and Legion Loader, through obfuscated installer chains. These installers packaged within password protected ZIPs and NSIS or MSI wrappers utilize AutoIt scripts or batch execution to bypass file size and detection thresholds. A parallel tactic involves hijacking search engine results for tech support domains, inserting attacker controlled contact numbers via parameter injection to channel victims into call based scams. The campaign exploits both organic search poisoning and malvertising and even extends to social media platforms like Facebook to lure users into installing malware laced apps under the guise of legitimate tools.

This operation illustrates the evolving sophistication of SEO poisoning, which capitalizes on user trust in search results and well known brand names. By weaponizing AI tool searches and trusted software names, attackers significantly increase their reach within both enterprise and consumer environments. The strategic implications are profound: organizations must verify software sources rigorously, employ behavioural download monitoring, and maintain user awareness to counteract these layered social engineering tactics. This trend reflects a broader shift toward blending conventional malvertising methods with AI themed lures to facilitate stealthy malware distribution at scale posing an urgent challenge for cybersecurity defences.

Read more: https://thehackernews.com/2025/07/seo poisoning campaign targets 8500.html

RondoDox Unveiled: Breaking Down a New Botnet Threat

A newly uncovered botnet threat known as RondoDox has emerged, targeting internet connected digital video recorders (DVRs) and industrial routers through the exploitation of unpatched vulnerabilities. The primary systems affected include TBK DVR models 4104 and 4216, as well as Four Faith industrial routers such as the F3x24 and F3x36 series. These devices, often deployed in retail, warehouse, and small business environments, are typically overlooked in cybersecurity planning, making them ideal targets for botnet activity. RondoDox leverages two known command injection vulnerabilities CVE 2024 3721 in TBK DVRs and CVE 2024 12856 in Four Faith routers to enable remote code execution and unauthorized device takeover.

Once inside the systems, RondoDox deploys a range of obfuscated binaries across multiple architectures, including MIPS, ARM, and x86_64, using shell scripts to identify writable file paths before payload delivery. The malware ensures persistence through the installation of init scripts and scheduled cron jobs, while removing shell history to cover its tracks. It employs XOR based obfuscation to evade detection by conventional antivirus systems. When activated as part of the botnet, compromised devices are used for distributed denial of service (DDoS) attacks across HTTP, TCP, and UDP protocols. To further mask its activities, the malware disguises traffic as legitimate communication associated with gaming platforms such as Fortnite, Minecraft, and Discord, or VPN tools like OpenVPN and WireGuard.

The strategic implications of RondoDox are significant, underscoring the growing threat posed by increasingly sophisticated IoT targeting malware. By compromising large numbers of vulnerable edge devices, actors behind RondoDox can facilitate proxy services, amplify DDoS campaigns, and sustain covert command and control operations. This development reflects a broader trend in the cybersecurity landscape, where attackers exploit weakly defended IoT infrastructure for scalable, low profile attacks. It highlights the urgent need for robust firmware patching, network segmentation, and anomaly based intrusion detection in both enterprise and industrial environments.

Read more: https://www.fortinet.com/blog/threat research/rondobox unveiled breaking down a botnet threat

Critical Vulnerability in Anthropic's MCP Exposes Developer Machines to Remote Exploits

A critical security vulnerability within Anthropic's Model Context Protocol (MCP) Inspector a developer facing tool discovered by independent cybersecurity researchers. The Inspector, part of Anthropic's open source MCP ecosystem, was found susceptible to remote code execution (RCE) via a cross site request forgery (CSRF) flaw (CVE 2025 49596), compounded by an outdated browser vulnerability nicknamed "0.0.0.0 Day." MCP Inspector serves as a locally hosted web interface (using Server Sent Events, or SSE) on default port 6277, and lacked authentication or origin checks between its client and proxy until version 0.14.1.

In context, as AI development tools like MCP gain broader adoption among enterprise and open source communities, shifting core logic to local web based proxies opens novel attack surfaces. The Inspector's proxy listens on all interfaces (0.0.0.0), making it reachable both from localhost and local networks. Attackers crafting malicious web pages exploit "0.0.0.0 Day," then leverage CSRF to send SSE commands to the proxy, effectively triggering arbitrary system level commands on a developer's machine. DNS rebinding techniques further enable bypassing same origin defenses, escalating the threat significantly.

The vulnerability was responsibly disclosed in April 2025 and swiftly patched in version 0.14.1 on June 13, which introduced session tokens, origin validation, and stricter authentication between client and proxy. However, the broader MCP ecosystem remains at risk: a related flaw (CVE 2025 6514, CVSS 9.6) in the mcp remote component similarly enables full RCE when clients connect to untrusted MCP servers, demonstrating a pattern of insecure defaults.

Strategically, these issues highlight the accelerating convergence of AI development workflows and web based tooling an environment where traditional browser based web threats can rapidly escalate to system level compromise. The vulnerabilities underscore the need for robust security hygiene in open source AI frameworks: authenticated inter process communication, proper origin enforcement, limiting network exposure, and default secure configurations. With AI platforms becoming foundational in both enterprise and research contexts, such lapses could invite supply chain exploits, insider threats, or lateral movement attacks making the secure design of developer tooling integral to broader cyber resilience.

Read more: https://thehackernews.com/2025/07/critical vulnerability in anthropics.html?

Okta observes v0 AI tool used to build phishing sites

Okta Threat Intelligence has identified a significant shift in phishing tactics, with v0, a generative AI web development tool from Vercel, being repurposed by threat actors to rapidly generate high fidelity phishing sites. In these attacks, adversaries employ natural language prompts to replicate login pages for platforms like Okta, Microsoft 365, and cryptocurrency services importing brand specific logos and assets and hosting everything on Vercel’s own infrastructure to evade detection.

This development arrives amid rising concerns over the misuse of generative AI tools, where streamlined deployment and open source clones (e.g., DIY GitHub repositories) are lowering the technical barriers for low skill actors. Attackers can now produce convincing phishing sites in under 30 seconds, significantly increasing the speed, scale, and scale and quality of credential stealing campaigns.

Okta researchers validated the threat by reproducing the technique using v0 and observed that all elements including sign in forms, visuals, and code were hosted on trusted platforms to bypass anti phishing systems that rely on blacklist detection or suspicious domain signals. Although there have been no confirmed cases of credential theft yet, the potential for large scale compromise and rapid weaponization underscores the severity. In response, Okta advocates urgent adoption of phishing resistant, passwordless authentication mechanisms, such as Okta FastPass, which cryptographically binds a user’s authenticator to the legitimate site domain, nullifying credential harvesting via look alike pages . Additional countermeasures include device trust policies, step up authentication based on anomaly detection, and enhanced security training tailored to AI generated phishing threats.

Implications: This trend marks a strategic inflection point in cybercrime generative AI is no longer merely assisting phishing (e.g., crafting emails) but enabling rapid, automated deployment of phishing infrastructure. Traditional detection and user awareness approaches are increasingly inadequate. To counter these emerging risks, organizations must embrace passwordless and phishing resistant identity solutions, integrate continuous anomaly monitoring, and coordinate shared threat intelligence especially as adversaries leverage AI’s scalability to democratize sophisticated attack capabilities.

Read more: https://www.okta.com/newsroom/articles/okta observes v0 ai tool used to build phishing sites/

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.

The views expressed and suggestions made are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.