JULY 2025

NEWSLETTER

They want what you've got. don't give it to them

Infosources™

CYBERESPIONAGE

CRITICAL INFRASTRUCTURE

CYBERCRIME

RANSOMWARE

GEOPOLITIC

REPORTS

CYBERESPIONAGE

Canada Bans Chinese Surveillance Giant Hikvision Over National Security Concerns

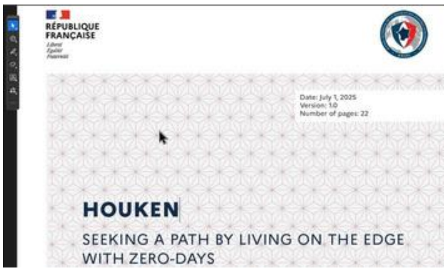
▶ SUBSCRIBE

Canada has ordered Hikvision, a major Chinese video surveillance firm, to cease all operations in the country following a national security review. The government also banned the use and purchase of Hikvision products across federal agencies, citing risks tied to the company's Chinese state connections. Hikvision denies the allegations, calling the decision unfair and politically motivated, mirroring similar moves by the United States amid rising geopolitical tensions.

Chinese Cyberespionage Targets France's Critical Infrastructure

▶ SUBSCRIBE

In late 2024, a stealthy Chinese cyber campaign quietly infiltrated the French government's digital perimeter, leveraging a trio of Ivanti CSA zero-days to breach systems across multiple strategic sectors — government, telecoms, media, finance, and transport. It wasn't just another APT sighting. What emerged instead was a broader picture of China's evolving cyber playbook: not only highly technical and persistent, but increasingly modular, commercialized, and deniable.



RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Date: July 1, 2025
Version: 1.0
Number of pages: 22

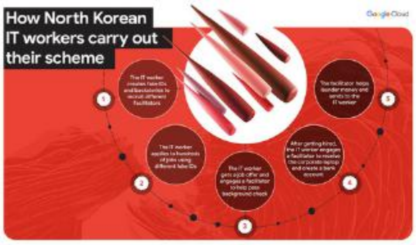
HOUKEN

SEEKING A PATH BY LIVING ON THE EDGE WITH ZERO-DAYS

North Korean IT Worker Scheme Exposed: Microsoft and Cybersecurity Firms Disrupt AI-Powered Job Fraud Network

▶ SUBSCRIBE

A quiet but deeply strategic cyber operation by North Korea has been unfolding across the U.S. and European tech sectors, exploiting the growing reliance on remote work and the rapid evolution of generative AI. Under the guise of freelance developers and software engineers, North Korean operatives — aided by U.S.-based facilitators — have embedded themselves into legitimate companies, using stolen identities and AI tools to pass as qualified candidates.



How North Korean IT workers carry out their scheme

Google Cloud

1 The IT worker creates false IDs and backstories to recruit different facilitators

2 The IT worker applies to hundreds of jobs using different false IDs

3 The IT worker gets a job offer and engages a facilitator to help pass background check

4 After getting hired, the IT worker engages a facilitator to receive the corporate laptop and create a bank account

5 The facilitator helps launder money and sends to the IT worker

Iranian-Linked Hackers Leak Thousands of Israeli Military CVs: Strategic Exposure Through Hybrid Warfare

▶ SUBSCRIBE

In a striking escalation of hybrid warfare, Iranian-affiliated hackers have leaked thousands of detailed résumés belonging to current and former members of Israel's most sensitive military and intelligence units. More than a data breach, the operation exposes the structural vulnerability of Israel's defense-to-tech pipeline—where elite IDF experience forms the foundation of civilian cybersecurity and AI industries. By targeting this overlap, Iran is not only gathering long-term intelligence but also aiming to discredit, destabilize, and erode the deterrent edge of the Israeli security apparatus.

Operation “AUTHENTIC ANTICS” — GRU Espionage Tool Targeting Western Infrastructure

▶ SUBSCRIBE

In July 2025, the United Kingdom publicly exposed a covert cyber espionage operation attributed to Russia’s military intelligence service, the GRU. At the heart of this campaign is a newly identified malware tool—AUTHENTIC ANTICS—developed and deployed by the notorious hacking group APT28 (also known as Fancy Bear or Forest Blizzard). The malware is engineered to silently infiltrate Microsoft cloud environments, stealing credentials and authentication tokens to enable long-term access to email accounts and sensitive cloud services.

UK Identifies Russian GRU’s “AUTHENTIC ANTICS” Malware in Email Espionage Campaign
AUTHENTIC ANTICS

Singapore Faces Active Cyber Espionage Threat from UNC3886

▶ SUBSCRIBE

In recent years, Singapore has emerged as a frequent target of advanced persistent threat (APT) actors, particularly state-sponsored cyber espionage groups. The most recent and pressing example is the ongoing intrusion campaign attributed to UNC3886, a China-linked threat actor known for its stealthy operations and focus on high-value strategic targets. On July 18, 2025, Singaporean authorities publicly identified UNC3886 for the first time, warning that the group is actively compromising parts of the nation’s critical information infrastructure.

Extensive Use of Chinese Surveillance Technology in Ireland Sparks Security Debate

▶ SUBSCRIBE

Across Ireland, Hikvision surveillance cameras — made by a Chinese state-linked firm — are widely deployed in sensitive public sites, from hospitals and universities to courthouses and government buildings. Unlike countries such as the US, UK, and Australia that have banned Hikvision from critical infrastructure due to national security concerns, Ireland has issued no guidance or restrictions. Despite reassurances from suppliers and claims that advanced functions like facial recognition are disabled, the lack of a coordinated response raises alarms.

CRITICAL INFRASTRUCTURE

Scattered Spider’s Expanding Warpath: From Casinos to Clouds to Cockpits

▶ SUBSCRIBE

Scattered Spider, a notorious cybercriminal group, is expanding its operations beyond tech and finance into U.S. aviation, insurance, and manufacturing. Confirmed by the FBI, these attacks exploit social engineering to bypass security, posing a growing threat to critical infrastructure.

Prescription for Deception: How Imposter Scams Are Targeting America's Health Data

▶ SUBSCRIBE

A new wave of cybercrime is exploiting one of the most trusted sectors in American life—healthcare. Posing as federal health fraud investigators or legitimate insurance reps, scammers are tricking patients and providers into handing over sensitive data. Behind these impersonation scams lies a calculated use of fear, urgency, and institutional mimicry to breach personal privacy and hijack financial information. As health data becomes a prime target, the lines between cybercrime and public trust grow dangerously thin.

Iranian Hackers Threaten U.S. Stability with Propaganda and Infrastructure Attacks Amid Rising Tensions

▶ SUBSCRIBE

As geopolitical tensions between the United States and Iran escalate, U.S. cybersecurity agencies are sounding the alarm over a surge in Iranian cyber operations aimed at destabilizing political institutions and threatening critical infrastructure. Recent developments highlight not only Tehran's use of cyber propaganda to influence public perception—particularly through efforts to smear political figures like former President Donald Trump—but also a growing pattern of attacks targeting vital sectors such as energy, transportation, and defense. These activities, attributed to Iranian state-sponsored groups and affiliated hacktivists, reflect a broader strategic posture designed to disrupt, discredit, and retaliate against perceived adversaries through increasingly aggressive digital means.

CYBERCRIME

International Crypto Fraud Network Laundered $540 Million Before Spanish Authorities Dismantled It

▶ SUBSCRIBE

Spanish law enforcement, aided by Europol and international partners, dismantled a global cryptocurrency fraud network that laundered over $500 million and victimized thousands. The investigation exposed complex laundering schemes spanning multiple countries and remains ongoing amid growing concerns over evolving online fraud.

International Crypto Fraud Network Laundered $540 Million Before Spanish Authorities Dismantled It

▶ SUBSCRIBE

Mohammed Umar Taj, a suspended IT worker from Yorkshire, was sentenced to over seven months in prison after deliberately disrupting his employer's network. Following his suspension in July 2022, the company failed to immediately revoke his network access, allowing Taj to alter login credentials and multi-factor authentication settings. This sabotage locked out the company and its clients in Germany and Bahrain, causing around £200,000 in financial losses and damaging the business's reputation. Taj pleaded guilty to unauthorized acts intended to impair computer operations. Authorities highlighted the wide-reaching impact of his actions beyond the UK. Interestingly, Taj is also currently listed as director of an electrical company.

Transnational Scam Centers and Human Trafficking Expansion into West Africa

▶ SUBSCRIBE

The global expansion of transnational scam centers has taken a new and troubling turn, with West Africa emerging as a significant node in a cybercriminal infrastructure once concentrated in Southeast Asia. Driven by organized crime networks, technological innovation, and human trafficking, this evolving ecosystem poses both regional and international security threats. The following unstructured report analyzes recent developments, strategic shifts, and operational patterns observed in this expanding illicit industry.

ONLINE SCAMS AND HUMAN TRAFFICKING
FROM REGIONAL CRIME THREAT TO GLOBAL HUMAN TRAFFICKING CRISIS
PRIMARY TRAFFICKING HUBS
SECONDARY TRAFFICKING HUBS
OTHER AFFECTED COUNTRIES
INTERPOL

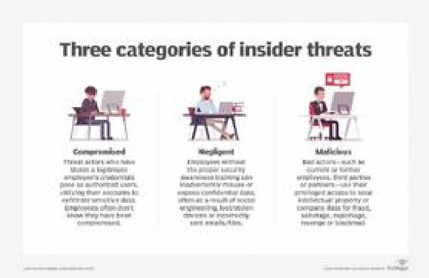
How Organized Crime Leverages Insider Weaknesses

▶ SUBSCRIBE

Insider threats have long been seen as isolated acts by disgruntled employees, but this outdated view no longer reflects reality. Today, insider exploitation has evolved into a global, organized phenomenon driven by cybercriminal networks and state-sponsored actors who infiltrate organizations by manipulating trusted employees through coercion, bribery, or deception. The human element has become the most critical vulnerability in corporate and national security.

From North Korean operatives posing as IT contractors in major companies to ransomware groups bribing employees to deploy malware, these campaigns are deliberate, industrialized, and weaponized. This article examines the tactics and geopolitical forces behind this shift, emphasizing the urgent need for organizations to move from reactive security to proactive resilience in a world where trust itself is the ultimate attack surface.

The old stereotype of the lone rogue insider is over. Today, your employees are the frontline—and without adaptation, they could become your greatest point of failure.



Three categories of insider threats

Compromised

Threat actors who have stolen a legitimate employee's credentials pose as authorized users, utilizing their accounts to exfiltrate sensitive data. Employees often don't know they have been compromised.

Negligent

Employees without the proper security awareness training can inadvertently misuse or expose confidential data, often as a result of social engineering, lost/stolen devices or incorrectly sent emails/files.

Malicious

Bad actors—such as current or former employees, third parties or partners—use their privileged access to steal intellectual property or company data for fraud, sabotage, espionage, revenge or blackmail.

Allegations of Algorithmic Manipulation: France Opens Criminal Probe into Elon Musk’s X

▶ SUBSCRIBE

French prosecutors have launched a criminal investigation into X (formerly Twitter) over allegations of algorithmic manipulation and unauthorized data extraction. The probe, led by the J3 cybercrime unit, follows formal complaints from a French MP and a senior official who suspect that X’s ranking systems were intentionally distorted to serve political interests and gather user data unlawfully. The investigation focuses on two charges:

1. Tampering with automated data systems as part of an organized group, and
2. Fraudulent extraction of data.

The case raises broader concerns about foreign interference, algorithmic opacity, and compliance with EU digital laws, as X continues expanding into financial services within Europe.

RANSOMWARE

Ransomware’s Shockwave: How Cyber Insurers Rethink Security Assessments and Risk-Sharing Models

▶ SUBSCRIBE

Ransomware has forced a deep transformation in how cyber insurers assess and manage risk. As double extortion and ransomware-as-a-service models surged, insurers shifted from outdated questionnaires to real-time scans and integrations. This evolution reshaped their partnerships with clients, introducing new incentives, security benchmarks, and a rebalancing of risk in the age of persistent cyber extortion.

Pay2Key.I2P: The Iranian Ransomware-as-a-Service Model Blending Ideology with Profit

▶ SUBSCRIBE

In early 2025, a significant evolution in Iran-linked cyber operations emerged with the reappearance of Pay2Key under a new identity: Pay2Key.I2P. More than just a ransomware variant, this latest deployment signals a strategic shift in the modus operandi of Iranian-affiliated threat actors, merging state-aligned ideological objectives with financially motivated cybercrime at scale. Hosted entirely on the Invisible Internet Project (I2P)—a first for any known Ransomware-as-a-Service (RaaS) operation. This RaaS platform is not operating in isolation. It reflects a broader alignment between Iranian APTs like Fox Kitten (aka Lemon Sandstorm) and well-known ransomware crews such as BlackCat (ALPHV), RansomHouse, and NoEscape. Their collaborative infrastructure marks a turning point in how cyberwarfare intersects with global cybercrime markets. The report is offering insight into how ransomware is being weaponized not only for profit but also for state-backed digital confrontation.

Ingram Micro under Siege: A Strategic breach of the Global Tech Supply Chain

▶ SUBSCRIBE

On July 3, 2025, a sophisticated ransomware attack crippled Ingram Micro, the world's largest IT distributor, exposing deep vulnerabilities within the global tech supply chain. The cybercriminal group SafePay exploited weaknesses in remote access infrastructure, triggering widespread operational outages and sending shockwaves through partners, clients, and markets. As millions of dollars are lost daily and reputations hang in the balance, the incident underscores the urgent need for stronger cybersecurity defenses, smarter infrastructure, and strategic resilience. The fallout reveals not only the fragility of interconnected digital systems, but also the new stakes facing businesses and investors in an era of intelligent cyber threats.

GEOPOLITIC

Russia Labels Recorded Future an “Undesirable Organization” Amid Accusations of Supporting Ukraine

▶ SUBSCRIBE

Recorded Future

Russia has labeled U.S. cybersecurity firm Recorded Future as an "undesirable organization," accusing it of aiding Ukraine and conducting intelligence work against Russian military operations. The designation bans the company from operating in Russia. Recorded Future’s CEO welcomed the move as a compliment. This marks the first time a cybersecurity firm has received such a label, typically reserved for NGOs or media. The company, soon to be acquired by Mastercard for $2.6 billion, is a major global threat intelligence provider.

Putin’s AI-Driven Disinformation Machine: Operation Overload and the New Arms Race for Truth

▶ SUBSCRIBE

A Russian-aligned disinformation campaign is harnessing the power of consumer-grade artificial intelligence to flood digital platforms with false narratives at an unprecedented scale. Known as Operation Overload—or Matryoshka and linked by some to Storm-1679—this campaign has rapidly evolved since 2023 into a high-volume, AI-enabled propaganda engine. Targeting democratic societies, especially Ukraine, the campaign spreads doctored videos, fake images, and misleading narratives designed to polarize public opinion, interfere in elections, and amplify social divisions. By exploiting widely available AI tools, its operators have shifted toward a faster, cheaper, and multilingual model of influence that circumvents traditional verification systems and overwhelms the global information ecosystem. The result is a dramatic escalation in coordinated online manipulation—one that challenges how societies prepare for and defend against foreign influence operations in the age of generative AI.

© Social media/east2west news

Africa at a Digital Crossroads: Cyber Conflict, AI Threats, and Sovereignty in the Balance

▶ SUBSCRIBE

As digital infrastructure becomes the backbone of modern governance, economic development, and geopolitical influence, African states find themselves at a dangerous inflection point. On one side lies the promise of modernization—expanded digital public services, economic growth, and greater global integration. On the other, a rapidly expanding threat landscape shaped by cybercriminals, hostile state actors, and the disruptive power of artificial intelligence.

In this volatile environment, Morocco's recent cyberattacks—targeting national databases and compromising millions of sensitive records—signal more than a localized security breach. They reflect a triple convergence of forces reshaping Africa's digital future:

Firstly, the growing use of cyber capabilities as tools of geopolitical confrontation, particularly in the context of the tense rivalry between Morocco and Algeria and their respective international alignments. Secondly, the continent-wide explosion of cybercrime and AI-powered fraud, exploiting institutional weaknesses and outpacing traditional defense mechanisms. Third, the uneven but increasingly urgent efforts across Africa to build resilient digital sovereignty, secure public infrastructures, and train a new generation of cybersecurity professionals.

This report explores the Moroccan cyber breach through these three interwoven lenses, situating the attack within broader patterns of regional disruption, technological acceleration, and structural fragility. It aims to show how a single act of digital aggression can expose systemic vulnerabilities—and why the stakes now reach far beyond national borders.

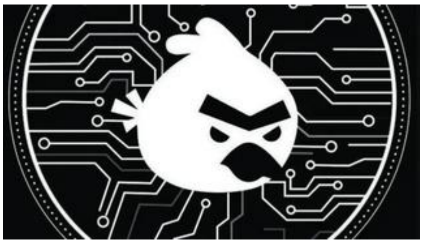
Nobitex Hack: A Cyberattack at the Crossroads of Geopolitics, Sanctions Evasion, and Financial Warfare

▶ SUBSCRIBE

The June 2025 takedown of Iran's largest crypto exchange, Nobitex, by the hacker group Predatory Sparrow, marks a turning point in the convergence of cyberwarfare, financial sabotage, and geopolitical coercion. This was not a heist but a deliberate act of digital scorched earth — aimed at collapsing Iran's crypto-based sanctions evasion architecture and shaking public confidence in the regime's control over its financial future. In destroying rather than stealing, the attackers redefined the strategic utility of cyber operations: making economic annihilation more potent than profit and transforming backend infrastructure into a battlefield. What unfolded was not just a data breach — it was a weaponized message to Tehran that even its last financial escape hatches can be burned from within.

خرید و فروش امن بیت‌کوین و ارزهای دیجیتال

به بزرگترین بازار ارز دیجیتال ایران بپیوندید



Operation "AUTHENTIC ANTICS" — GRU Espionage Tool Targeting Western Infrastructure

UK Identifies Russian GRU's "AUTHENTIC ANTICS" Malware in Email Espionage Campaign
AUTHENTIC ANTICS

In July 2025, the United Kingdom publicly exposed a covert cyber espionage operation attributed to Russia's military intelligence service, the GRU. At the heart of this campaign is a newly identified malware tool—AUTHENTIC ANTICS—developed and deployed by the notorious hacking group APT28 (also known as Fancy Bear or Forest Blizzard). The malware is engineered to silently infiltrate Microsoft cloud environments, stealing credentials and authentication tokens to enable long-term access to email accounts and sensitive cloud services.

This attribution marks a significant escalation in the UK's confrontation with Russian hybrid threats. It follows a joint investigation by Microsoft and the NCC Group and coincides with a sweeping round of British government sanctions against multiple GRU units and officers. These developments underscore the evolving nature of cyber conflict: silent, persistent, state-directed, and increasingly integrated into broader geopolitical campaigns.

The following unstructured report compiles all available intelligence surrounding AUTHENTIC ANTICS, its discovery, capabilities, attribution, and implications for national and organizational cybersecurity. It reflects the broader strategic confrontation between democratic states and state-sponsored cyber operations, and the ongoing need to defend against persistent, well-resourced actors operating in the grey zone of international conflict.

REPORT

RANSOMWARE TRENDS AND THREAT ACTORS: INTELLIGENCE INSIGHTS FROM THE 2025 ZSCALER THREATLABZ REPORT

▶ SUBSCRIBE

Between April 2024 and April 2025, ransomware activity escalated dramatically, reaching record levels in both frequency and impact. Zscaler's cloud infrastructure intercepted over 10.8 million ransomware attempts—an unprecedented 145.9% increase year-over-year—marking the sharpest spike observed since tracking began. Simultaneously, public ransomware extortion cases surged by 70.1%, reflecting a decisive pivot toward data theft as the preferred mechanism of coercion.

This operational shift has seen ransomware actors increasingly abandon encryption in favor of data exfiltration, exploiting the reputational, regulatory, and operational risks faced by victim organizations. Data theft volumes rose 92.7% across key ransomware families, with several groups—most notably Hunters International—committing entirely to non-encryption, extortion-only campaigns.

Despite large-scale law enforcement actions, including Operation Endgame, the ransomware ecosystem remained resilient and adaptive. Thirty-four new ransomware groups emerged during the analysis period, while established operations like Clop, Akira, and DragonForce expanded in both scale and sophistication. Generative AI is now playing a tactical role in this evolution, enabling attackers to accelerate phishing, malware development, and automated data processing.

Target selection continues to prioritize high-leverage sectors. Manufacturing, technology, and healthcare remained top targets, while the oil and gas sector experienced an extraordinary 935% increase in attacks. Geographically, the United States accounted for over half of all incidents, though notable growth was observed in India, Israel, and across the Asia-Pacific region.

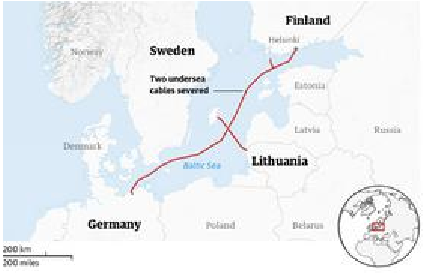
This report provides in-depth analysis of these developments, profiles dominant and emerging ransomware families, explores the operational methodologies in use, and highlights strategic recommendations for defenders—especially in leveraging AI and Zero Trust architectures to preempt and contain ransomware threats.

Cutting the Lines: Hybrid conflict and the battle for global connectivity

SUBSCRIBE

Global connectivity relies on a hidden yet indispensable layer of infrastructure: undersea fiberoptic cables. These cables, which carry more than 99% of intercontinental data traffic, form the backbone of the digital economy and global communications. Every day, over $10 trillion in financial transactions depend on their uninterrupted operation. Yet in recent years, this critical system has faced an alarming rise in disruptions—some accidental, others increasingly suspected to be deliberate.

Across Europe, especially in the Baltic Sea, a dense web of cables and pipelines has become a focal point for suspicious maritime incidents. While some outages stem from routine fishing or anchoring activity, a growing body of evidence suggests coordinated sabotage by state-linked actors, masked as normal maritime operations. These patterns signal a shift toward hybrid tactics—where physical infrastructure is quietly targeted below the threshold of open conflict. Intelligence agencies, NATO, and regional governments have taken notice, but institutional responses remain fragmented.



Source: TeleGeography

In parallel, the Asia-Pacific—home to one of the world's most concentrated submarine cable networks—faces its own vulnerabilities. Slow repair times, regulatory bottlenecks, and limited maintenance capacity have created a dangerous gap between infrastructure growth and operational resilience. Some island nations, like Tonga or Taiwan's Matsu Islands, have endured prolonged outages with major economic and security consequences. As geopolitical rivalries intensify, concerns over ownership, access, and sabotage risks are driving new alignments and infrastructure strategies.

Meanwhile, the global financial sector—the most data-dependent industry of all—remains critically underprepared. While there are playbooks for cyberattacks and financial crises, no equivalent framework exists for managing extended cable outages. Market volatility, transactional delays, and systemic risks loom large if multiple disruptions occur simultaneously.

The Kongsberg HUGIN Large Uncrewed Underwater Vehicle – is an autonomous submersible capable of surveillance tasks down to extreme depths. (Image: Kongsberg)

This report analyzes the escalating risks to undersea infrastructure through a regional and sectoral lens. It maps the technical, political, and economic fault lines emerging across Europe and the Indo-Pacific, highlights the strategic motivations behind suspected sabotage, and assesses the readiness of financial and regulatory institutions. As cables become contested terrain in both geopolitical and economic terms, strengthening their resilience must become a global priority—before the next outage triggers a crisis that can no longer be dismissed as hypothetical.