CCRS Bit

June 2024

CONTENTS

Cybercrime

- Here's What We Can Learn (and Do) About Cybercrime from FBI's Latest Internet Crime Report. Link
- Insider threat: Months after being fired, former employee accessed company's computer test system and deleted servers, causing it to lose S$918,000. Link
- ID Verification Service for TikTok, Uber, X Exposed Driver Licenses. Link
- China-Backed Hackers Exploit Fortinet Flaw, Infecting 20,000 Systems Globally. Link
- UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion. Link
- Snowflake Breach Exposes 165 Customers' Data in Ongoing Extortion Campaign. Link
- Kimsuky Using TRANSLATEXT Chrome Extension to Steal Sensitive Data. Link
- WA man set up fake free WiFi at Australian airports and on flights to steal people's data, police allege. Link
- Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools. Link
- The Scourge of Ransomware Victim Insights on Harms to Individuals, Organisations and Society. Link
- Ransomware Is 'More Brutal' Than Ever in 2024. Link
- Chinese hackers are increasingly deploying ransomware, researchers say. Link

- Cyberespionage Groups Attacking Critical Infrastructure with Ransomware. Link
- Infosys McCamish Systems ransomware attack affected more than 6 million people. Link
- LockBit Ransomware Claims 33 TB of US Federal Reserve Data for Ransom. Link
- Threat Actor Claims to Sell Critical Vulnerabilities in Interpol and FBI Login Pages. Link
- SPECTR Malware Targets Ukraine Defense Forces in SickSync Campaign. Link
- Russian hackers claim cyberattack on Spanish defence company. Link
- Crimson Palace: Chinese Hackers Steal Military Secrets Over 2 Years. Link
- Threat Actor Claims to Sell Data of Indonesian Military Intelligence Agency and INAFIS (Indonesia Automatic Fingerprint Identification System). Link
- Pakistani Hacking Team 'Celestial Force' Spies on Indian Gov't, Defense. Link
- Pakistani Hackers Use DISGOMOJI Malware in Indian Government Cyber Attacks. Link
- Cleveland City Hall Shuts Down After Cyber Incident. Link
- Andariel Hackers Target South Korean Institutes with New Dora RAT Malware. Link
- Indonesian Directorate General of Civil Aviation Database is Allegedly Leaked. Link
- French Diplomatic Entities Targeted in Russian-Linked Cyber Attacks. Link
- London Hospitals Cancel Operations Following Ransomware Incident. Link

- Threat Actor Claims to Sell Access to European Biomedical Company with U.S. Contracts, Offering 6TB of Data. Link
- Qilin Ransomware Leaks 400GB of NHS and Patient Data on Telegram. Link
- Medical-Targeted Ransomware Is Breaking Records After Change Healthcare's $22M Payout. Link
- Sustained Campaign Using Chinese Espionage Tools Targets Telcos. Link
- IntelBroker Allegedly Breached T-Mobile. Link
- Russian Power Companies, IT Firms, and Govt Agencies Hit by Decoy Dog Trojan. Link
- Microsoft informs customers that Russian hackers spied on emails. Link
- Frontier says 750,000 Social Security numbers accessed during April cyberattack. Link
- IntelBroker Hacker Claims Apple Breach, Steals Source Code for Internal Tools. Link
- TeamViewer Confirms Security Breach by Russian Midnight Blizzard. Link
- Thousands of UEFA Customer Credentials Sold on Dark Web. Link
- Live Nation Confirms Massive Ticketmaster Data Breach. Link
- North Korean Hackers Target Brazilian Fintech with Sophisticated Phishing Tactics. Link
- New Medusa Android Trojan Targets Banking Users Across 7 Countries. Link
- Threat Actor Allegedly Leaks 70 GB of KYC Data from CredRight. Link
- Threat Actor Claims to Sell Access to an UK Bank Server. Link
- Santander customers' private data put up for sale for $2m by hackers. Link

- Kraken Crypto Exchange Hit by $3 Million Theft Exploiting Zero-Day Flaw. Link
- 8220 Gang Exploits Oracle WebLogic Server Flaws for Cryptocurrency Mining. Link
- Hotel Kiosks Vulnerability Exposed Guest Data, Room Access. Link
- Location Tracker Firm Tile Hit by Data Breach, Hackers Access Internal Tools. Link
- Check-in terminals used by thousands of hotels leak guest info. Link
- BreachForums back online — or it is a honeypot? Link
- Developing: BreachForums down, ShinyHunters' and forum Telegram channels deleted? Link
- A Ransomware Builder Advertised on a Dark Web Forum. Link
- Threat Actor Claims to Sell 0day Sandbox Escape RCE in Chrome Browser. Link

  'AI Call Center Software' Is Powering a Scam Call Center. Link
- Rising Wave of QR Code Phishing Attacks: Chinese Citizens Targeted Using Fake Official Documents. Link
- Cybercrime and identity fraud: an Olympic challenge. Link
- My daughter voiced sadness on TikTok and was fed self-harm videos. Link
- CISO Guide to Deepfake Scams. Link
- Does GPT-4 risk accelerating cybercrime? Link
- AI Boosts Cybercrime, INTERPOL Warns. Link
- Deloitte predicts losses of up to $40B from generative AI-powered fraud. Link
- Deepfake Creators Are Revictimizing GirlsDoPorn Sex Trafficking Survivors. Link

- CDT, CCRI, and NNEDV Announce Multistakeholder Working Group to Address Non-Consensual Intimate Images. Link
- EU leaders have failed to tackle child sexual abuse crisis online. Link
- Commission demands details from porn platforms on protections for minors and illegal content. Link
- Treacherous Internet: Cyber-Criminalization of LGBT People. Link
- Neo-Nazis Are All-In on AI. Link
- Embargo Ransomware Group: The Interview. Link
- Road to redemption: GhostSec's hacktivists went to the dark side. Now they want to come back. Link
- Impacts of Geopolitics to Cyberspace: Sweden Faces Intensifying Hacktivist Attacks. Link
- eBay Removes Listing for StingRay Cellphone Spying Tech. Link
- This stuff is illegal But you can still buy it anyway. Here are 10 wild Amazon gadgets you can purchase. Link
- Bangladeshi police agents accused of selling citizens' personal information on Telegram. Link
- An AirTags Stalking Sting Operation. Link
- The UN Cybercrime Draft Convention Remains Too Flawed to Adopt. Link

Digital Investigation and Digital Evidence

- Western Law Enforcement Agencies are Going on the Cyber Offensive. Link
- War Crime Prosecutions Enter a New Digital Age. Link
- ICC probes cyberattacks in Ukraine as possible war crimes. Link
- Federal criminal investigation involving Perry Johnson & Associates data breach. Link
- French police shut down chat website reviled as 'den of predators'. Link
- Feds seize domains linked to crypto investment scam preying on New York's Russian diaspora. Link
- Interpol, FBI Disrupt Moldova-Based Cyber Ring . Link
- USD 257 million seized in global police crackdown against online scams. Link
- 'Operation Endgame' Hits Malware Delivery Platforms. Link
- Europol's Hunt Begins for Emotet Malware Mastermind. Link
- US boosts reward for info on 'Missing Cryptoqueen' Ruja Ignatova to $5 million. Link
- FBI obtains 7,000 LockBit ransomware decryption keys. Link
- Four arrested for allegedly attempting to sabotage Interpol criminal search system. Link
- More arrests stemming from Desjardins data breach. Link
- Scattered Spider Boss Cuffed in Spain Boarding a Flight to Italy. Link
- British national with possible links to high-profile phishing campaigns arrested in Spain. Link

- Ukraine Police Arrest Suspect Linked to LockBit and Conti Ransomware Groups. Link
- Two Ukrainians suspected of helping Russia spread propaganda, hack military phones. Link
- Indonesia arrests over 100 foreigners in Bali suspected of participating in cybercrime. Link
- Bulgarian hacker "Emil Külev" arrested and detained. Link
- Man arrested over 'honey trap' WhatsApp messages sent to British politicians. Link
- Two people arrested in connection with investigation into homemade mobile antenna used to send thousands of smishing text messages to the public. Link
- Singapore Extradites Suspected Cybercrime Scammers from Malaysia. Link
- 4 FIN9-linked Vietnamese Hackers Indicted in $71M U.S. Cybercrime Spree. Link
- Owners of "Empire Market" Charged in Chicago With Operating $430 Million Dark Web Marketplace. Link
- Russian National Indicted for Cyber Attacks on Ukraine Before 2022 Invasion. Link
- Doctor charged for unauthorized access to personal information of pediatric patients at Texas Children's Hospital. Link
- Chinese nationals plead guilty to running Zambia scam operation. Link
- ViLe Cybercrime Group Members Plead Guilty to Hacking DEA Portal. Link
- Arrested Data Security Officer Admits To Hacking 93 Websites. Link
- Russian hackers sanctioned by European Council for attacks on EU and Ukraine. Link

- Israel’s cyber chief calls for international front against Iranian hackers. Link
- Inside a Violent Gang's Ruthless Crypto-Stealing Home Invasion Spree. Link
- The phone fixer. Link
- The Unusual Espionage Act Case Against a Drone Photographer. Link

Digital Forensics

- Changing Perceptions Of Large And Complex Investigations. Link
- Navigating the complex world of cell phone forensics: How multiple SIMs and eSIMs impact investigations. Link
- Maximising Data Collection With SaaS Innovations. Link
- How Did That Photo Get On That iPhone. Link
- Wireshark: Ethereal Network Analysis for the Cloud SOC. Link
- The art of concealment: how hackers hide malware. Link
- Investigating A Malware Attack Using Binalyze AIR's Investigation Hub. Link
- Tracking Down Notorious Ransomware Actors with CTI 2.0. Link
- Extracting WhatsApp Database (or any app data) from Android 12/13 using CVE-2024-0044. Link
- CRITICAL: SystemBC Historical Bot Infections Special Report. Link
- Criminal IP Unveils Fraud Detection Data Products on Snowflake Marketplace. Link
- AI Chatbot Fools Scammers & Scores Money-Laundering Intel. Link
- Semantics 21: Advancing AI For Victim Identification. Link
- New multilingual audio deepfake detection coming to Reality Defender. Link
- Microsoft admits no guarantee of sovereignty for UK policing data. Link
- Police Scotland engages public on biometric data rights amid cloud storage concerns. Link

- How to easily find, organise and manage your OSINT tools. Link
- How Law Enforcement Can Adapt to the Ever-Changing OSINT Landscape. Link
- Everything About Social Media Intelligence (SOCMINT) and Investigations. Link
- Geolocating a Gang Leader Wanted by the FBI: An OSINT Explainer. Link
- Offensive OSINT s05e06 - Open Source Surveillance - Free advanced Open Street Map search. Link
- OSINTQUEST - Investigation Platform Free online tool. Link
- TotalRecall - extracts and displays data from the Recall feature in Windows 11, providing an easy way to access information about your PC's activity snapshots. Link
- Phunter - OSINT tool allowing you to find various information via a phone number. Link
- EnsembleData - Scrape TikTok, Instagram data API. Link
- Social Media Tools. Link
- Deepware - Scan & Detect Deepfake Videos. Link
- OSINT Method for Map Investigations. Link
- Worldwide Web: An Analysis of Tactics and Techniques Attributed to Scattered Spider. Link
- Dark Web Profile: BlackSuit Ransomware. Link
- Dark Web Profile: Qilin (Agenda) Ransomware. Link
- Dark Web Profile: SpaceBears. Link
- Dark Web Profile: dAn0n Hacker Group. Link
- Dark Web Profile: IntelBroker. Link
- RansomHouse: Stolen Data Market, Influence Operations & Other Tricks Up the Sleeve. Link
- Tracking Adversaries: The Qilin RaaS. Link

- Dissecting Propaganda: Using AI to Cut Through North Korean TV Spin. Link
- Truth, Trust, and AI: Justice and Accountability for International Crimes in the Era of Digital Deception. Link
- Fake or Real? Detecting AI Images from a Forensic Lens. Link

Digital Surveillance vs. Privacy

- Into the Void: Special Operations Forces after the War on Terror. Link
- Weaponisation of the FATF Standards: A Guide for Global Civil Society. Link
- Security, Surveillance, and Government Overreach – the United States Set the Path but Canada Shouldn't Follow It. Link
- Policing by design: the latest EU surveillance plan. Link
- Automating the fortress: digital technologies and European borders. Link
- Travelers to EU may be subjected to AI lie detector. Link
- Germany beefs up border security ahead of UEFA Championship. Link
- FedEx's Secretive Police Force Is Helping Cops Build An AI Car Surveillance Network. Link
- The Age of the Drone Police Is Here. Link
- US police launch drone programs, but no FRT on UAS – yet. Link
- An Israeli company is hawking its self-launching drone system to U.S. police departments. Link
- Cheap and lethal: the Pentagon's plan for the next drone war. Link
- The Lords of Silicon Valley Are Thrilled to Present a 'Handheld Iron Dome'. Link
- The DJI Drone Ban: A Uniquely American Clusterfuck. Link
- The House Ban On DJI Drones Is Mindless Anticompetitive Fear Mongering. Link

- UK could ban Hikvision CCTV cameras amid surging sales and security concerns. Link
- Amazon-Powered AI Cameras Used to Detect Emotions of Unwitting UK Train Passengers. Link
- False Promise of Biometrics. Link
- Threat Actor Claims to Sell 0day Vulnerability for Dahua Cameras. Link
- Robots integrate biometrics for parcel delivery, security, and military operations. Link
- German lawmakers call for bans on biometric surveillance. Link
- Berlin Group adopts working paper on facial recognition technology. Link
- Surveillance technology from Saxony: Secret facial recognition in five German federal states. Link
- Sweden wants to let police use facial recognition technology. Link
- Brazil's data privacy regulator looks at biometrics and facial recognition in new report. Link
- Kansas law enforcement upgrades to Idemia ABIS. Link
- Clearview AI Is So Broke It's Now Offering Lawsuits Plaintiffs A Cut Of Its Extremely Dubious Future Fortunes. Link
- Clearview facial recognition searches double, database reaches 50B images. Link
- Evansville Police officer resigned following investigation of misuse of A.I. technology. Link
- Five Eyes biometric data sharing increases by over 100X with little transparency. Link
- AWS says it's keeping its word on cops' use of Rekognition, docs differ. Link

- The Next Generation of Cell-Site Simulators is Here. Here's What We Know. Link
- Other people's smartphones are spying on your router. How to stop it. Link
- This undisclosed WhatsApp vulnerability lets governments see who you message. Link
- New Branding, Same Scanning: "Upload Moderation" Undermines End-to-End Encryption. Link
- EU's 'Going Dark' Expert Group Publishes 42-Point Surveillance Plan For Access To All Devices And Data At All Times. Link
- After Pushback From Service Providers, Australian Regulators Strip Encryption Breaking Demands From Online Safety Bill. Link
- Georgia Prosecutors Stoke Fears Over Use Of Encrypted Messengers And Tor. Link
- By Whose Authority? Pegasus targeting of Russian & Belarusian-speaking opposition activists and independent media in Europe. Link
- Government and military officials fair targets of Pegasus spyware in all cases, NSO Group argues. Link
- Sanctioned and exposed, Predator spyware maker group has gone awfully quiet. Link
- After Pegasus was blacklisted, its CEO swore off spyware. Now he's the king of Israeli AI. Link
- US private equity firm in talks to buy cyberattack co Paragon. Link
- Polish investigators seize Pegasus spyware systems as part of probe into alleged abuse. Link
- Polish Parliament strips official of immunity, clearing path for prosecution in spyware scandal. Link

- The inside view of spyware’s 'dirty interference,' from two recent Pegasus victims. Link
- Sanctions for Spyware. Link
- Cyber intelligence company Variston changes tack. Link
- Lawsuit Filed Challenging Constitutionality Of Vast Network Of Illinois License Plate Readers. Link
- The Mystery of AI Gunshot-Detection Accuracy Is Finally Unraveling. Link
- Houston, Texas Poised To Become The Next Major City To Drop ShotSpotter. Link
- Caution: External Exposure of License Plate Recognition Systems May Lead to Personal Information Leakage. Link
- New ALPR Vulnerabilities Prove Mass Surveillance Is a Public Safety Threat. Link
- Cops Released a Car’s Travel History to a Total Stranger. Link
- Hacker Accesses Internal ‘Tile’ Tool That Provides Location Data to Cops. Link
- 'Junk inferences' by data brokers are a problem for consumers and the industry itself. Link
- Google Leak Reveals Thousands of Privacy Incidents. Link
- Google Chrome: Agree to 'privacy feature', but get tracking! Link
- Google Maps Timeline Data to be Stored Locally on Your Device for Privacy. Link
- Microsoft Delays AI-Powered Recall Feature for Copilot+ PCs Amid Security Concerns. Link
- Lawsuit Claims Microsoft Tracked Sex Toy Shoppers With 'Recording in Real Time' Software. Link
- My Memories Are Just Meta's Training Data Now. Link

- NOYB Urges Immediate Action Against Meta's Data Use for AI Training. Link
- Introducing Apple Intelligence, the personal intelligence system that puts powerful generative models at the core of iPhone, iPad, and Mac. Link
- Former head of NSA joins OpenAI board. Link
- AI trained on photos from kids' entire childhood without their consent. Link
- AI Tools Are Secretly Training on Real Images of Children. Link
- Mastercard To Expand Digital Biometric ID and "Behavioral Biometrics". Link
- Yet Another ID Verification Service Breached, Exposing Private Info Collected On Behalf Of Uber, TikTok & More. Link
- Mall of America deploys Corsight facial recognition after gun incidents. Link
- This Will Certainly End Well: Retailers Are Equipping Employees With Body Cameras To Limit Theft. Link
- Shopping app Temu is "dangerous malware," spying on your texts, lawsuit claims. Link
- McDonald's pauses AI voice ordering system developed with IBM. Link
- Privacy fears sap potential of female fertility tech start-ups. Link

Cyber Security

- 2023 Hacked Website & Malware Threat Report. Link
- Phishing for Gold: Cyber Threats Facing the 2024 Paris Olympics. Link
- Global Revival of Hacktivism Requires Increased Vigilance from Defenders. Link
- Global DDoS Attack Landscape: Insights from Q1 2024. Link
- Your Phone's 5G Connection Is Vulnerable to Bypass, DoS Attacks. Link
- Top 10 VPN Vulnerabilities (2022 – H1 2024). Link
- ZKTeco Biometric System Found Vulnerable to 24 Critical Security Flaws. Link
- Scores of Biometrics Bugs Emerge, Highlighting Authentication Risks. Link
- AuthenticID develops proprietary algorithms to mitigate biometric injection attacks. Link
- Ransomware Attackers May Have Used Privilege Escalation Vulnerability as Zero-day. Link
- Black Basta Ransomware May Have Exploited MS Windows Zero-Day Flaw. Link
- New SnailLoad Attack Exploits Network Latency to Spy on Users' Web Activities. Link
- New “Snowblind” Android Malware Steals Logins, Bypasses Security Features. Link
- New Fickle Stealer Exploits Software Flaws to Steal Crypto, Browser Data. Link

- Celebrity TikTok Accounts Compromised Using Zero-Click Attack via DMs. Link
- China-Backed Hackers Exploit Fortinet Flaw, Infecting 20,000 Systems Globally. Link
- AI Company Hugging Face Detects Unauthorized Access to Its Spaces Platform. Link
- NiceRAT Malware Targets South Korean Users via Cracked Software. Link
- Hackers Exploit Legitimate Websites to Deliver BadSpace Windows Backdoor. Link
- Hackers exploit critical D-Link DIR-859 router flaw to steal passwords. Link
- Oyster Backdoor Spreading via Trojanized Popular Software Downloads. Link
- LightSpy Spyware's macOS Variant Found with Advanced Surveillance Capabilities. Link
- Craxs Rat, the master tool behind fake app scams and banking fraud. Link
- Commando Cat: A Novel Cryptojacking Attack Abusing Docker Remote API Servers. Link
- Cloaked and Covert: Uncovering UNC3886 Espionage Operations. Link
- RansomHub: New Ransomware has Origins in Older Knight. Link
- Boolka Unveiled: From web attacks to modular malware. Link
- The Travels of “markopolo”: Self-Proclaimed Meeting Software Vortax Spreads Infostealers, Unveils Expansive Network of Malicious macOS Applications. Link
- Chinese Hackers Deploy SpiceRAT and SugarGh0st in Global Espionage Campaign. Link
- What a show! An amplified Internet scale DNS probing operation. Link

- New Wi-Fi Takeover Attack—All Windows Users Warned To Update Now. Link
- New Phishing Campaign Deploys WARMCOOKIE Backdoor Targeting Job Seekers. Link
- Hackers Detail How They Allegedly Stole Ticketmaster Data From Snowflake. Link
- Statement from National Security Advisor Jake Sullivan on the Global Effort to Strengthen the Cybersecurity of Energy Supply Chains. Link
- Microsoft Chose Profit Over Security and Left U.S. Government Vulnerable to Russian Hack, Whistleblower Says. Link
- US government sanctions Kaspersky executives. Link
- Citing national security, US will ban Kaspersky anti-virus software in July. Link
- FCC wants major telecoms to step up rules around AI-generated robocalls. Link
- New US Treasury strategy targets crypto scams and real estate money laundering. Link
- ODNI releases ic information technology roadmap. Link
- Meta tried to discredit researchers who identified fraudulent ads in its platforms. Link
- Zero-day vulnerability market tries to restructure. Link