CCRS Bit

November 2023

CONTENTS

Cybercrime

- The Evolution Of E-Crime: From Hacking To Cyberwarfare. Link
- The Untold Story of the Boldest Supply-Chain Hack Ever. Link
- Inside Job: How a Hacker Helped Cocaine Traffickers Infiltrate Europe's Biggest Ports. Link
- How an Indian startup hacked the world. Link
- Indian Hack-for-Hire Group Targeted U.S., China, and More for Over 10 Years. Link
- Shadowy Hack-for-Hire Group Behind Sprawling Web of Global Cyberattacks. Link
- Microsoft: Lazarus hackers breach CyberLink in supply chain attack. Link
- Espionage: Chinese hacker group was in the network of the Dutch chip manufacturer NXP for years. Link
- A Hacker Faked His Own Death–Then Claimed To Have Sold Marriott Customer Data To Russians, FBI Says. Link
- ChatGPT: OpenAI Attributes Regular Outages to DDoS Attacks. Link
- Same threats, different ransomware. Link
- LockBit ransomware group assemble strike team to breach banks, law firms and governments. Link
- Rackspace Ransomware Costs Soar to Nearly $12M. Link
- Ransomware Attack Targets WS_FTP Vulnerability: Over 4,000 Servers Exposed. Link
- World's largest commercial bank ICBC confirms ransomware attack. Link
- Step-by-step through the Money Message ransomware. Link

- The threat of ransomware in the food supply chain: a challenge for food defence. Link
- Cancer treatments cancelled after Canadian hospitals hit by ransomware attack. Link
- VX-Underground malware collective framed by Phobos ransomware. Link
- Fraudsters make $50,000 a day by spoofing crypto researchers. Link
- Spy Trojan SpyNote Unveiled in Attacks on Gamers. Link
- Lazarus hackers breached dev repeatedly to deploy SIGNBT malware. Link
- Overheating datacenter stopped 2.5 million bank transactions. Link
- Fidelity National Financial shuts down network in wake of cybersecurity incident. Link
- Russian Hackers Linked to 'Largest Ever Cyber Attack' on Danish Critical Infrastructure. Link
- Denmark Hit With Largest Cyberattack on Record. Link
- Greater Paris wastewater agency dealing with cyberattack. Link
- Australia locks down ports after ‘nationally significant’ cyberattack. Link
- Chinese APT groups target dozens of Cambodian government orgs. Link
- Mustang Panda Hackers Targets Philippines Government Amid South China Sea Tensions. Link
- Angreifer stören Navigation im Flugverkehr. Link
- Hackers are taking over planes’ GPS — experts are lost on how to fix it. Link
- Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology. Link

- Russia ushers in a new era of cyber-physical attack. Link
- Ukraine Tracks a Record Number of Cyber Incidents During War. Link
- US-based entity trains hackers to crash Russian Servers. Link
- MuddyC2Go: New C2 Framework Iranian Hackers Using Against Israel. Link
- Apple warns Armenians of state-sponsored hacking attempts. Link
- The state of Maine disclosed a data breach that impacted 1.3m people. Link
- Cyberattack on North Carolina county allowed hackers to access data. Link
- US Cybersecurity Lab Suffers Major Data Breach. Link
- Personal info of Canadian Armed Forces, RCMP stolen in cyberattack. Link
- Massive ransomware attack hinders services in 70 German municipalities. Link
- Pharmacy provider Truepill data breach hits 2.3 million customers. Link
- Hackers breach healthcare orgs via ScreenConnect remote access. Link
- Data Breach Exposes 1.2 Million Patients at Chicago Healthcare Provider. Link
- 2.2 Million Impacted by Data Breach at McLaren Health Care. Link
- Welltok data breach impacted 8.5 million patients in the U.S. Link
- Hacker Leaks Vaccination Records of Over 2 Million Turkish Citizens. Link
- NoEscape gang adds two more medical entities to their leak site. Link

- Women sue plastic surgery after hack saw their naked photos posted online. Link
- App used by hundreds of schools leaking children's data. Link
- Cyberattackers leaked data of 27,000 NYC Bar Association members. Link
- Potentially hundreds of UK law firms affected by cyberattack on IT provider CTS. Link
- Cyberattack on legal tech provider causing widespread disruption to UK law firms. Link
- North Texas water utility serving 2 million hit with cyberattack. Link
- Slovenian Electrical Utility HSE Suffers Ransomware Attack. Link
- Vietnam Post exposes 1.2TB of data, including email addresses. Link
- Samsung says hackers accessed customer data during year-long breach. Link
- General Electric Probes Security Breach as Hackers Sell DARPA-Related Access. Link
- Toyota Financial Services discloses unauthorized activity on systems after the Medusa ransomware gang claimed to have hacked the company. Link
- Rights warriors claim online ad auction data is a danger to national security. Link
- Password Breach of Game Developer Zynga Compromises 170 Million Accounts. Link
- Children’s tablet has malware and exposes kids’ data, researcher finds. Link
- Scam or Mega Chatbot? Investigating the New AI Chatbot Called Abrax666. Link

- How Netflix crushed the Latin American password black market. Link
- Mortgage giant Mr. Cooper says customer data exposed in breach. Link
- Hacker Leaks 800,000 Scraped Chess.com User Records. Link
- Boeing confirms cyberattack amid LockBit ransomware claims. Link
- The LockBit ransomware group published data allegedly stolen from the aerospace giant Boeing in a recent attack. Link
- Data from 35M LinkedIn Users Freely Shared on Hacking Forum. Link
- Round 4: Hacker returns and puts 26Mil user records for sale on the Dark Web. Link
- Schweiz: Cyberkriminelle veröffentlichen Daten der Steuerverwaltung im Darknet. Link
- Virtual Kidnapping: AI Tools Are Enabling IRL Extortion Scams. Link
- From bad to worse: stalking, threats, and chilling effects. Link
- How Hackers Are Using AI To Steal Your Bank Account Password. Link
- Chinese Scammers Cloning Websites for Massive Gambling Scam in Asia-Pacific Region. Link
- A Spy Wants to Connect With You on LinkedIn. Link
- Microsoft Warns of Fake Skills Assessment Portals Targeting IT Job Seekers. Link
- Thornaby: Woman targeted in £13k train station QR code scam. Link
- Crypto scam: Inside the billion-dollar 'pig-butchering' industry. Link

- $9 million seized from "pig butchering" scammers who preyed on lonely hearts. Link
- Researchers Expose Gaza Charity Crypto Scam. Link
- Rebel offensive in Myanmar takes aim at online scam industry. Link
- Hackers pose as officials to steal secrets and cryptocurrency for North Korea. Link
- Breaking: Nerayoff Follows Through, Releases 2015 Vitalik Buterin Recordings and Alleges Ethereum Corruption, Fraud. Link
- Fraudsters make $50,000 a day by spoofing crypto researchers. Link
- Fake crypto apps bring real losses to leading app marketplace users. Link
- Scammers Exploit Crypto Hype with Fake Token Factory, Stealing Millions. Link
- Scammers Use Fake Ledger App on Microsoft Store to Steal $800,000 in Crypto. Link
- KyberSwap DEX Hacked for $48 Million, Attacker Teases Negotiations. Link
- Ethereum feature abused to steal $60 million from 99K victims. Link
- What Ethereum Smart Contract Hacking Looks Like. Link
- More than $100 million stolen from Poloniex crypto platform. Link
- KyberSwap says $54.7 million of user cryptocurrency stolen during attack. Link
- Monero’s community wallet loses all funds after attack. Link
- Crypto firm Kronos Research says $26 million stolen after cyberattack. Link

- Microsoft: BlueNoroff hackers plan new crypto-theft attacks. Link
- Polish court discovers secret cryptomining rigs hidden throughout building. Link
- The Crypto Launderers: Crime and Cryptocurrencies from the Dark Web to DeFi and Beyond. Link
- Illicit Financial Flows from Cyber-Enabled Fraud. FATF Report. Link
- Giant AI Platform Introduces 'Bounties' for Deepfakes of Real People. Link
- AnyDream: Secretive AI Platform Broke Stripe Rules to Rake in Money from Nonconsensual Pornographic Deepfakes. Link
- Children making AI-generated child abuse images, says charity. Link
- Deepfakes could supercharge health care's misinformation problem. Link
- Microsoft offers politicians protection against deepfakes. Link
- Meta, Google to Talk Deepfake Election Threats in Senate Forum. Link
- Why fighting deepfakes in the 2024 election is…complicated. POLITICO Tech Podcast. Link
- Slovak election targeted by pro-Kremlin deepfake hoax. Link
- Adobe sells fake AI-generated Israel-Hamas war images – then the news ran them as real. Link
- For teen girls victimized by 'deepfake' nude photos, there are few, if any, pathways to recourse in most states. Link
- Goodbye Omegle: how the anonymous chatroom traumatized our teen years. Link
- Hackers Use Online Casinos to Gamble Mountains of Cash They Steal from Victims. Link

- 'Hunters International' Cyberattackers Take Over Hive Ransomware. Link
- Facebook approved an Israeli ad calling for assassination of pro-Palestine activist. Link
- How Kopeechka, an Automated Social Media Accounts Creation Service, Can Facilitate Cybercrime. Link
- The Mirai Confessions: Three Young Hackers Who Built a Web-Killing Monster Finally Tell Their Story. Link
  Hacker Conversations: Chris Wysopal, AKA Weld Pond. Link
- Approaching stealers devs : a brief interview with LummaC2. Link
- Exclusive interview with a phone phreak legend: Matthew Weigman. Link
- Exclusive: Hacker breaks silence following a decade behind bars in Cybernews documentary. Link
- Approaching stealers devs: a brief interview with Meduza. Link
- The Story of Karim Baratov. Cloak and Dagger Episode. Link
- Meet the Unique New "Hacking" Group: AlphaLock. Link
- Approaching stealers devs : a brief interview with Recordbreaker. Link
- Darknet Diaries EP: D3f4ult. Link
- Cybercrimeology EP 98- The Ecosystem: Understanding Cybercrime and Cybersecurity. Link
- “Smashing Security” episode 348: “Hacking for chimp change, and AI chatbot birthday”. Link
- Netflix documentary “Cyberbunker: The Criminal Underworld”. Link
- DW Documentary. Billion dollar fraud on the Internet. Link

Digital Investigation and Digital Evidence

- Alleged covert wiretap on Russian messaging service blown by expired TLS certificate. Link
- Thousands of new honeypots deployed across Israel to catch hackers. Link
- Crypto AG (Switzerland) - Which algorithms were used and how did the backdoors work? Link
- Ransomware Mastermind Uncovered After Oversharing on Dark Web. Link
- How Interpol traced the identity of 'the woman with the flower tattoo'. Link
- Protecting Victims From Stalkerware And Tech-Enabled Abuse. Forensic Focus podcast. Link
- REKTify: Identifying millions in stolen cryptocurrency. Link
- Cops Are Giving People Free Car Tracking Devices to Combat Thefts. Link
- History and evolution of open source intelligence. Link
- ASINT: AI-Assisted Analysis: The Future of Intelligence Work. Link
- Why For Today's Cyber Investigations We Need to Combine Intelligence Disciplines. Link
- Countering transnational dissident cyber espionage. Link
- Scattered Spider Casino Hackers Evade Arrest in Plain Sight. Link
- Nine arrested as part of investigation into money laundering and smishing. Link

- Europol arrest hackers allegedly behind string of ransomware attacks. Link
- 'Untouchable': Associates React to Arrest of Drug Trafficker Turned 'Encryption King'. Link
- Inside the FBI and DOJ Takedown of Qakbot, the “Swiss Army Knife” of Malware. Link
- U.S. Takes Down IPStorm Botnet, Russian-Moldovan Mastermind Pleads Guilty. Link
- FBI Shuts Down Notorious IPStorm Botnet, Arrests Mastermind Sergei Makinin after Four-Year Cybercrime Spree. Link
- The Federal Bureau of Investigation (FBI) dismantled the infrastructure behind the illegal botnet proxy service IPStorm. Link
- FBI struggled to disrupt dangerous casino hacking gang, cyber responders say. Link
- Australia Breaks Apart Crime Network Handling Nearly $1 Billion in Cryptocurrency. Link
- Major Phishing-as-a-Service Syndicate 'BulletProofLink' Dismantled by Malaysian Authorities. Link
- Europol and Local Forces Disband Multi-Million Dollar Vishing Ring. Link
- Europol Busts Major Online CSAM Racket in Western Balkans. Link
- Ukrainian and Czech police bust $9 million bank fraud gang. Link
- Taiwanese Crypto Exchange Bitgin under Investigation for Potential Money Laundering. Link
- Actions across Europe against online fraud with cryptocurrencies. Link
- Treasury Designates Virtual Currency Money Launderer for Russian Elites and Cybercriminals. Link

- Leader of $70M Cryptocurrency and Binary Options Fraud Schemes Extradited to the U.S. Link
- Assistant head teacher caught with 11,500 child abuse images. Link
- DOJ announces arrests in ‘high-end brothel network’ used by elected officials, military officers and others. Link
- Two Russian Nationals Charged For Conspiring To Hack The Taxi Dispatch System At JFK Airport. Link
- SEC charges SolarWinds CISO with fraud for misleading investors before major cyberattack. Link
- Indictment against Binance and its founder, Changpeng "CZ" Zhao. Link
- Binance CEO Pleads Guilty, Agrees to Pay $50 Million Fine. Link
- Russian and Moldovan National Pleads Guilty to Operating Illegal Botnet Proxy Service that Infected
- Tens of Thousands of Internet-Connected Devices Around the World. Link
- US teenager pleads guilty to his role in credential stuffing attack on a betting site. Link
- Wisconsin Man Pleads Guilty To Hacking Fantasy Sports And Betting Website. Link
- US Man Sentenced to Over 21 Years for Dark Web Distribution of CSAM. Link
- Man Sentenced to Life in Prison for Running Four Dark Web Child Exploitation Websites. Link
- Hacker Sentenced to 30 Months for SIM Swapping Conspiracy Resulting in Theft of Nearly $1 Million in Cryptocurrency. Link

- An Israeli hacker has been sentenced to 80 months in prison in the US for his role in a massive spear-phishing campaign. Link
- Ukrainian gets 8-year sentence for running marketplace for Americans' data. Link
- Sam Bankman-Fried found guilty of defrauding FTX customers out of billions. Link
- Man Sentenced to Four Months in Prison for Offering Phishing Panels via Telegram. Link
- Los Angeles SIM Swapper Sentenced to 8 Years in Prison. Link
- U.S. Treasury Sanctions Russian Money Launderer in Cybercrime Crackdown. Link
- Sinbad crypto mixer flagged by Elliptic sanctioned and seized. Link
- Following Investigations by Tether, OKX, and the U.S. Department of Justice, Tether Voluntarily Freezes 225M in Stolen USDT Linked to International Crime Syndicate. Link
- Nearly £2 million of stolen cryptocurrency to be paid back to victims. Link
- 'Hello Sir/Ma'am': Person Linked to Scam Asks FBI for His Seized Cryptocurrency Back. Link
- Omegle: 'How I got the dangerous chat site closed down'. Link
- EUCRIM has pre-published several articles on the hotly debated topic of electronic evidence in criminal and administrative punitive matters. Link
- The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice. Link
- Mutual Admissibility of Evidence and Electronic Evidence in the EU. Link
- The E-evidence Package. Link

- Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings. Link
- Electronic Evidence Collection in Cases of the European Public Prosecutor's Office. Link
- Trusted Cross-Border Data Flows: A National Security Priority. Link
- Exploring challenges with law enforcement access to data. Link
- Appeals Court: Bad Cloud Data Warrant Good Enough To Jail Someone For Crime Cops Weren't Even Investigating. Link
- USA seeks bilateral deals for access to European "criminal, terrorist, and identity records". Link
- Council and EU Parliament reach deal to advance police cooperation in Europe. Link
- Civil Liberties Committee adopted its position: Child sexual abuse online: effective measures, no mass surveillance. Link
- Committee on Civil Liberties, Justice and Home Affairs, REPORT on the proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. Link
- Announcing Lantern: The First Child Safety Cross-Platform Signal Sharing Program. Link
- Pentagon seeks to rapidly build up information-warfare force. Link
- UN Cybercrime Treaty - Summary of the GI-TOC's key positions. Link
- Cybercrime and violent crime are converging: here's how to deal with it. Link
- The effects of online ad campaigns on DDoS-attacks: A cross-national difference-in-differences quasi experiment. Link

Digital Forensics

- The platform matters: a comparative study on Linux and Windows ransomware attacks. Link
- In Search of Extraction Techniques for Pair-Locked iOS Devices. Link
- Enhancing Mobile Investigations: A Focus On Screenshots And Screen Recording. Link
- iOS 15 Image Forensics Analysis and Tools Comparison - Processing details and general device information. Link
- Exploring forensic evidence and detection methods for remote monitoring and management (RMM) tooling. Link
- Prioritizing Digital Evidence Management System over Physical Disks. Link
- Remote collection of Windows Forensic Artifacts using KAPE and Microsoft Defender for Endpoint. Link
- GPT vs malware analysis: challenges and mitigations. Link
- Applied Emulation - Analysis of MarsStealer. Link
- BPFDoor Evasive Linux Backdoor and Malware Forensic Investigation Presentation. Link
- Awesome-Hardware-and-IoT-Hacking. Link
- Seven Use Cases Where AI can be a Hero to Digital Forensics. Link
- TheDFIRReport Assistant: Fetches and discusses the latest reports from TheDFIRReport's website. Link
- Hack The Box just released FREE DFIR labs. Link
- The DFIR, OSINT & Blue Team CTFs and Challenges section of the Free & Affordable Training site has been updated! Link

- fastfire/deepdarkCTI Collection of Cyber Threat Intelligence sources from the deep and dark web. Link
- CovenantDecryptor: designed to decrypt the communication data of Covenant traffic - Extract_privatekey script retrieves the p and q primes from a minidump file to construct an RSA private key. Link
- Forbidden-Buster - A Tool Designed To Automate Various Techniques In Order To Bypass HTTP 401 And 403 Response Codes And Gain Access To Unauthorized Areas In The System. Link
- How Hackers Hide From Memory Scanners - demo of the technique "PeFluctuation". Link
- ShellGhost: A memory-based evasion technique which makes shellcode invisible from process start to end. Link
- .NET Assembly Obfuscation for Memory Scanner Evasion. Link
- HBSQLI - Automated Tool For Testing Header Based Blind SQL Injection. Link
- TrafficWatch - TrafficWatch, A Packet Sniffer Tool, Allows You To Monitor And Analyze Network Traffic From PCAP Files. Link
- jasperan/whatsapp-osint: WhatsApp spy - logs online/offline events from ANYONE in the world. Link
- Wireshark 4.2.0 has been released. Link
- Atola Adds RAID 6 Support To Its TaskForce Imagers. Link
- Anti-forensic Techniques: Feasibility and Efficiency against Forensic Tools. Link
- Machine Learning in Anti-Money Laundering (AML) Risk Mitigation and Tracing. Link
- How to Recognize AI-Generated Pictures, Videos, and Audio. Link
- VirusTotal have uploaded malicious modules used in campaign Operation Triangulation. Link

- Modern Asian APT groups' tactics, techniques and procedures (TTPs). Link
- LockBit 3.0 Ransomware Case Study: A Huge Cybersecurity Risk. Link
- From Akamai to F5 to NTLM... with love. Link Malware spotlight – into the trash: analyzing LitterDrifter. Link
- eSentire Threat Intelligence Malware Analysis: SolarMarker: To Jupyter and Back. Link
- Stealc Stealer. Link
- win32.tiktok.man.trojan. Link
- How BPF-Enabled Malware Works. Link
- CISA, FBI, and MS-ISAC Release Advisory on Rhysida Ransomware. Link
- Good Day Ransomware malware analysis. Link
- Ransomware manager: Investigation into farnetwork, a threat actor linked to five strains of ransomware. Link
- A deep dive into Phobos ransomware, recently deployed by 8Base group. Link
- How AI is shaping malware analysis. Link

Digital Surveillance vs. Privacy

- The Shapeshifting Crypto Wars. Link
- What We Must Ask About Surveillance State Failures. Link
- A New US Privacy Bill Seeks to End Warrantless Police and FBI Spying. Link
- Surveillance Bill Draft Would Require Warrant for FBI Searches. Link
- Reauthorizing Mass Surveillance Shouldn’t be Tied to Funding the Government. Link
- FBI Director: FISA Section 702 warrant requirement a 'de facto ban'. Link
- FBI boss: Taking away our Section 702 spying powers could be 'devastating'. Link
- UK Government Leaders Say Investigatory Powers Act Isn’t Awful Enough, Announce Plans To Make It Worse. Link
- UK Lawmakers Demand Pause on Live Facial Recognition Technology. Link
- Big Brother Watch’s Briefing on the Investigatory Powers (Amendment) Bill for the House of Lords, Second Reading. Link
- Große Koalition in Hessen will Vorratsdatenspeicherung und Gesichtserkennung. Link
- Knesset beschließt mehr Überwachung in Israel. Link
- Customs and Border Protection acquired ‘huge amount of surveillance power’. Link
- Does ICE Data Surveillance Violate Human Rights Law? The Answer is Yes, and It’s Not Even Close. Link

- Frontex illegally processing migrants' data, EU watchdog says. Link
- Migration Pact: EU lawmakers flirt with racial profiling in final negotiations. Link
- The (human) cost of Artificial Intelligence and Surveillance technology in migration. Link
- @EuroMedRights& @StatewatchEU report: AI in Border Control and Surveillance. Link
- Silicon Valley is piling into the business of snooping. Link
- Web browsing data collected in more detail than previously known, report finds. Link
- Secretive White House Surveillance Program Gives Cops Access to Trillions of US Phone Records. Link
- US Spies Are Buying Americans' Private Data. Congress Has a New Chance to Stop It. Link
- Report: Unregulated Data Brokers Sell Military Family Info For Pennies. Link
- Data brokers are selling US service members' secrets, researchers find. Link
- Lexisnexis sold powerful spy tools to U.S. Customs and border protection. Link
- Unsealed FTC Complaint Shows Data Broker Kochava Hoovered Up Oceans Of Sensitive Data On Millions Of Americans. Link
- A Spy Agency Leaked People's Data Online—Then the Data Was Stolen. Link
- Statewatch New Report: Europe's hidden security crisis: How data about European defence personnel and political leaders flows to foreign states and non-state actors. Link
- Patternz sammelt Daten von Milliarden von Menschen. Link
- Germany Raises Red Flags About Palantir's Big Data Dragnet. Link

- Do Qualcomm chips pass private information to the US government? Link
- Patient privacy fears as US spy tech firm Palantir wins £330m NHS contract. Link
- Private UK health data donated for medical research shared with insurance companies. Link
- 'Shocking' scale of UK government's secret files on critics revealed. Link
- CCTV Video Surveillance and Crime Control: The Current Evidence and Important Next Steps. Link
- The NYPD is using drones 3 times more than it did last year. Link
- There's a new sheriff in Times Square … and it's an NYPD robot. Link
- Datenschutzbeauftragte kritisiert Berliner Bodycam-Pläne. Link
- Police and protest in the digital age – a post-Soviet comparison of citizen-police relations. Link
- How China targets civil society abroad. Link
- Rio de Janeiro: A test for the intelligence of smart cities. Link
- What San Diego Must Consider Before Resurrecting Streetlight Surveillance. Link
- International police facial recognition system: Parliament must ensure democratic debate. Link
- Remote Biometric Identification and Emotion Recognition in the Context of Law Enforcement. Link
- The EU wants to make facial recognition history — but it must be done for the right reasons. Link
- UK Policing Minister Advocates for More Facial Recognition. Link

- Police Use of Face Recognition Is Sweeping the UK. Link
- Police urged to double use of facial recognition software. Link
- UK police plan national roll-out of facial-recognition phone app. Link
- Live Facial Recognition for Law Enforcement: The European Union's Regulatory Approach Should be Informed by UK Police's Practice. Link
- The French national police is unlawfully using an Israeli facial recognition software. Link
- AI Cameras Took Over One Small American Town. Now They're Everywhere. Link
- 'Wholly ineffective and pretty obviously racist': Inside New Orleans' struggle with facial-recognition policing. Link
- Does A.I. Lead Police to Ignore Contradictory Evidence? Link
- Vidéosurveillance algorithmique à la police nationale : des faits passibles du droit pénal. Link
- Beijing reportedly asked Hikvision to identify fasting students in Muslim-majority province. Link
- Russia considers multiplying the size of its face surveillance network. Link
- Ukraine's 'Secret Weapon' Against Russia Is a Controversial U.S. Tech Company. Link
- Watchdog bites back against blockage of $9M fine on US selfie-scraper Clearview AI. Link
- Clearview AI tops 40 billion reference images in facial recognition database. Link
- Spyware are still having a 'ball' despite a decade of warnings. Link
- NSO continues its outreach to U.S. officials, including Secretary of State Antony Blinken. Link

- Israeli spyware firm NSO demands “urgent” meeting with Blinken amid Gaza war lobbying effort. Link
- Israel's NSO unleashes controversial spyware in Gaza conflict. Link
- Blacklisted spyware firm looks for inroads amid war in Gaza. Link
- Predatorgate scandal in Greece: RSF denounces the political sabotage of the investigation. Link
- Apple Warns Top Indian Opposition Leaders, Journalists About ‘State-Sponsored’ Attack on Phone. Link
- Democracy needs privacy: ban rights-violating spyware in India now. Link
- Apple sends experts to India after hacker threat warning. Link
- Android spyware delivered through infected news site targets Urdu speakers in Kashmir. Link
- Spyware Targeting Against Serbian Civil Society. Link
- Tuta Is An Independent Company And Not Linked To Five Eyes Secret Services. Link
- EU urged to drop new law that could allow member states to intercept and decrypt global web traffic. Link
- EU Tries To Slip In New Powers To Intercept Encrypted Web Traffic Without Anyone Noticing. Link
- Johnson's use of anti-pornography software raises cybersecurity questions. Link
- We must stop AI replicating the problems of surveillance capitalism. Link
- Generative AI Is Making Companies Even More Thirsty for Your Data. Link
- With AI, Big Tech is No Longer Pretending to Care. Link

- ChatGPT Has Been Turned Into A Social Media Surveillance Assistant. Link
- ChatGPT Is Apparently a Great Surveillance Tool. Link
- CBP Is Testing Palmer Luckey's AI-Powered Surveillance Towers in the Great Lakes. Link
- EDPS published the "Study on the essence of the fundamental rights to privacy and to protection of personal data. Link
- Ombudsman: European Commission's concealment of secret 'expert list' on CSAM regulation constitutes 'maladministration'. Link
- EU lawmakers criticize lack of action to tackle spyware abuses. Link
- noyb files complaint against EU Commission over targeted chat control ad campaign. Link
- A coalition of 6 organisations takes EU's dangerous terrorist content regulation to court. Link
- ECNL joins CSO coalition in court case against EU's terrorist content regulation. Link
- The CNIL issues ten new sanctions under its simplified procedure. Link
- Inside a Six-Month Espionage Campaign at Facebook. Link
- This Is the Ops Manual for the Most Tech-Savvy Animal Liberation Group in the US. Link
- Lidl staff to wear body cameras after surge in shoplifting. Link
- Court rules automakers can record and intercept owner text messages. Link
- Why I'm Not Getting a Humane AI Pin. Link
- Surveillance Tech Companies Are Writing Press Releases For Cops. Worse, News Agencies Are Publishing Them. Link

Cyber Security

- The second quantum computing revolution: new report from Europol. Link
- Chinese researchers claim they can break 2048-bit RSA using quantum computers, entire tech world at risk. Link
- In a first, cryptographic keys protecting SSH connections stolen in new attack. Link
- European Telecom Body to Open-Source Radio Encryption System. Link
- #BSidesMunich23, #7SYNs Edition (re)presents: Tayla Sellschop's "Bio-Lock The future and ethics around DNA Cryptography". Link
- Coverage Advisory for CVE-2023-47246 SysAid Zero-Day Vulnerability. Link
- MOVEit hackers leverage new zero-day bug to breach organizations (CVE-2023-47246). Link
- Google TAG revealed that threat actors exploited a Zimbra Collaboration Suite zero-day (CVE-2023-37580) to steal emails from governments. Link
- Disclosure of Vulnerable Bitcoin Wallet Library — Unciphered. Link
- If you created a bitcoin wallet before 2016, your money may be at risk. Link
- Reptar: a vulnerability in Intel processors. Link
- Randstorm: You Can't Patch a House of Cards. Link
- Randstorm Exploit: Bitcoin Wallets Created b/w 2011-2015 Vulnerable to Hacking. Link

- DeFi vulnerability leading to $6.7M exploit ‘not detected’ by auditors. Link
- Cybercriminals Using Telekopye Telegram Bot to Craft Phishing Scams on a Grand Scale. Link
- Advanced fuzzing unmasks elusive vulnerabilities. Link
- BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses. Link
- Experts Uncover Passive Method to Extract Private RSA Keys from SSH Connections. Link
- MultiSource Analysis of the Top MITRE ATT&CK Techniques by Cyentia and TidalCyber. Link
- FBI shares tactics of notorious Scattered Spider hacker collective. Link
- NetSupport RAT Infections on the Rise - Targeting Government and Business Sectors. Link
- DarkGate and PikaBot Malware Resurrect QakBot's Tactics in New Phishing Attacks. Link
- TA402 Uses Complex IronWind Infection Chains to Target Middle East-Based Government Entities. Link
- Ransomware Actors Continue to Gain Access through Third Parties and Legitimate System Tools. Link
- Israel warns of BiBi wiper attacks targeting Linux and Windows. Link
- Cybercrime, DarkGate now abuses Microsoft Teams and SharePoint. Link
- Abusing Microsoft access linked table feature to perform ntlm forced authentication attacks. Link
- Malvertiser copies PC news site to deliver infostealer. Link
- Cybercrime service bypasses Android security to install malware. Link

- Fast-acting cyber gangs increasingly disabling telemetry logs. Link
- A nasty Python package continues a trend of targeting developers. Link
- LummaC2 v4.0 Malware Stealing Data with Trigonometry to Detect Human Users. Link
- NodeStealer Malware Hijacking Facebook Business Accounts for Malicious Ads. Link
- FBI Alert: Silent Ransom Group Utilizes Callback Phishing for Network Hacks. Link
- Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology. Link
- Russian Cyber Espionage Group Deploys LitterDrifter USB Worm in Targeted Attacks. Link
- Russian hackers use Ngrok feature and WinRAR exploit to attack embassies. Link
- New Jupyter Infostealer Version Emerges with Sophisticated Stealth Tactics. Link
- Imperial Kitten Deploys Novel Malware Families in Middle East-Focused Operations. Link
- Malware that steals Facebook accounts. Link
- CherryBlos, the malware that steals cryptocurrency via your photos - what you need to know. Link
- CanesSpy Spyware Discovered in Modified WhatsApp Versions. Link
- Hamas Telegram in the immediate wake of their 7 October terrorist attack(s): part 1 – activity levels. Link
- Researchers Uncover Undetectable Crypto Mining Technique on Azure Automation. Link
- Crooks leverage Google quiz messages as part of bitcoin scam. Link

- Kinsing Malware Exploits Apache ActiveMQ Vulnerability to Mine Cryptocurrency. Link
- MGM Casino Hack and Realities of Social Engineering Attacks. Link
- Reflective call stack detections and evasions. Link
- DPRK Crypto Theft | macOS RustBucket Droppers Pivot to Deliver KandyKorn Payloads. Link
- Here's How Violent Extremists Are Exploiting Generative AI Tools. Link
- Flipper Zero can still crash iPhones running the latest version of iOS 17. Link
- Predator AI | ChatGPT-Powered Infostealer Takes Aim at Cloud Platforms. Link
- Hacking Google Bard - From Prompt Injection to Data Exfiltration. Link
- New Study Suggests ChatGPT Vulnerability with Potential Privacy Implications. Link
- Google mitigated the largest DDoS attack to date, peaking above 398 million rps. Link
- Mitigation Guide: Healthcare and Public Health (HPH) Sector. Link
- FCC Reveals Some Vague Rules That Pretend To Tackle SIM Hijacking Fraud. Link
- The NSA Seems Pretty Stressed About the Threat of Chinese Hackers in US Critical Infrastructure. Link
- EU Tightens Cybersecurity Requirements for Critical Infrastructure and Services. Link
- Europe is trading security for digital sovereignty. Link
- UK National Cyber Force operations to become 'more embedded' with policing. Link
- Intel Faces 'Downfall' Bug Lawsuit. Link

- AlphV files an SEC complaint against MeridianLink for not disclosing a breach to the SEC (2). Link
- SEC Charges Against SolarWinds CISO Send Shockwaves Through Security Ranks. Link
- SEC Suit Ushers in New Era of Cyber Enforcement. Link
- Optus loses court bid to keep report into cause of 2022 cyber-attack secret. Link
- Acuity Who? Attempts and Failures to Attribute 437GB of Breached Data. Link
- Denied Ransom, Frustrated Hackers Report Victim to Police for Failure to Report Data Breach. Link
- Dragos Says No Evidence of Breach After Ransomware Gang Claims Hack via Third Party. Link
- EasyJet hack investigation abandoned because of 'limited resources'. Link
- If entities continue to obfuscate and lie, it's time to mandate more transparency in breach disclosures. Link
- Healthcare startups scramble to assess fallout after Postmeds data breach hits millions of patients. Link
- Royal Mail spent £10m on cyber measures after LockBit attack. Link
- 'I employ a lot of hackers': how a stock exchange chief deters cyber-attacks. Link
- Measures taken following the unprecedented cyber-attack on the ICC. Link
- EU policymakers prepare to close on cybersecurity law for connected devices. Link
- Book: The Android Malware Handbook: Detection and Analysis by Human and Machine. Link