CCRS Bit

July 2024

CONTENTS

Cybercrime

- Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024. Link
- Global Microsoft Meltdown Tied to Bad Crowdstrike Update. Link
- France: Telecom fiber optic networks sabotaged. Link
- The biggest data breaches in 2024: 1 billion stolen records and rising. Link
- AT&T says criminals stole phone records of 'nearly all' customers in new data breach. Link
- Phone, text message records of 'nearly all' AT&T customers stolen. Link
- Low-level cybercriminals are pouncing on CrowdStrike-connected outage. Link
- Major Russian banks hit with DDoS attacks as Ukraine claims responsibility. Link
- Illicit Crypto Ecosystem Report. Link
- US Crypto Exchange Gemini Reveals Breach. Link
- Indian crypto platform WazirX confirms $230 million stolen during cyberattack. Link
- Tether freezes $29 million of cryptocurrency connected to Cambodian marketplace accused of fueling scams. Link
- The $11 Billion Marketplace Enabling the Crypto Scam Economy. Link
- Phishing by Industry Benchmarking Report. Link
- AI-Powered Cybercrime report. Link
- Metacrime – can it be stopped? Link

- CSAM and the Role of Cryptocurrency. Link
- Report on Cyber-Related Child Sexual Abuse and Exploitation. Link
- The rise of deepfakes beyond social media. Link
  How to Protect Real Estate from Payment Redirection Scams. Link
- Chinese ‘cybercrime syndicate’ behind gambling sites advertised at European sporting events. Link
- Ransomware ecosystem fragmenting under law enforcement pressure and distrust. Link
- Ransomware Groups Fragment Amid Rising Cybercrime Threats. Link
- Dark Angels ransomware receives record-breaking $75 million ransom. Link
- BM: Cost of a breach reaches nearly $5 million, with healthcare being hit the hardest. Link
- Urgent Blood Appeal Issued in US After Ransomware Attack. Link
- Nearly 13 Million Australians Affected by MediSecure Attack. Link
- HealthEquity data breach affects 4.3M people. Link
- Debt collection agency says data breach affected more than 4 million people. Link
- Stolen GenAI Accounts Flood Dark Web With 400 Daily Listings. Link
- RockYou2024: 10 billion passwords leaked in the largest compilation of all time. Link
- Hacktivists Claim Leak of CrowdStrike Threat Intelligence. Link
- Up To 33 Million Authy User Cell Phone Numbers Exposed. Link

- Stolen credentials could unmask thousands of darknet child abuse website users. Link
- Russia-linked FIN7 hackers sell their security evasion tool to other groups on darknet. Link
- Google’s Nonconsensual Explicit Images Problem Is Getting Worse. Link
- The Digital Weaponry of Radicalisation: AI and the Recruitment Nexus. Link
- Policing Street Trolls: Navigating Cop Baiting and Digital Extremism. Link

Digital Investigation and Digital Evidence

- FBI Flies 65-Strong Cyber Action Team Across Globe To Fight Hackers. Link
- France launches large-scale operation to fight cyber spying ahead of Olympics. Link
- Europol coordinates global action against criminal abuse of Cobalt Strike. Link
- Website used for child pornography, prostitution and drug dealing taken down with support of Eurojust. Link
- Prolific DDoS Marketplace Shut Down by UK Law Enforcement. Link
- NCA infiltrates DDoS-for-hire site as suspected controller arrested in Northern Ireland. Link
- Interpol operation nabs 300 with links to West African cyber fraud. Link
- Call blocked: hard and fast action against 54 Spanish phone fraudsters. Link
- U.S. Seizes Domains Used by AI-Powered Russian Bot Farm for Disinformation. Link
- 300 arrests made in crackdown of West African cyber fraud group. Link
- Spanish police arrest three suspects linked to pro-Moscow NoName057(16) hackers. Link
- Police nab 17-year-old linked to group behind MGM Resorts cyberattack. Link
- U.S. Indicts alleged member of apt45 for Maui ransomware attacks. Link

- Australian charged for ‘Evil Twin’ WiFi attack on plane. Link
- Two Russians Convicted for Role in LockBit Attacks. Link
- Notorious Hacker Kingpin ‘Tank’ Is Finally Going to Prison. Link
- Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn. Link
- Bipartisan Senate bill calls for stronger Secret Service financial cybercrime probes. Link
- Taking action against antisemitism – close to 2 000 pieces of content flagged for removal. Link
- Meta bans 63,000 accounts belonging to Nigeria’s sextortionist Yahoo Boys. Link
- £7.7 million bounty offered in hunt for members of North Korea-backed hacking group. Link
- FCC wants major telecoms to step up rules around AI-generated robocalls. Link
- Using AI to Fight Trafficking Is Dangerous. Link

Digital Forensics

- Hard Disk Analysis Methodology. Link
- Exploring Host-Based Digital Forensics with Memory Analysis. Link
- Google Drive Forensics. Link
- Money Laundering and Cryptocurrency: Trends and new techniques for detection and investigation. Link
- Chainalysis Launches Public-Private Plans to Crack Down on Crypto Scams. Link
- A review of research in forensic investigation of cryptocurrencies. Link
- New AI algorithm flags deepfakes with 98% accuracy — better than any other tool out there right now. Link
- AI lie detectors are better than humans at spotting lies. Link
- OpenAI Disrupts Covert Influence Operations With The Help of OSINT. Link
- Hunting Lazarus: Expanding Indicators with Historic DNS. Link
- The Not-So-Secret Network Access Broker x999xx. Link
- Unmasked: The cybercriminal group targeting Spanish bank users with AI-powered phishing tools and Android malware. Link
- China-linked Daggerfly hackers update their toolset, likely after exposure. Link
- Qilin Revisited: Diving into the techniques and procedures of the recent Qilin Ransomware Attacks. Link

- Suspected Iranian state hackers use new malware to target Israeli organizations. Link
- Cyber Threat Intelligence: Illuminating the Deep, Dark Cybercriminal Underground. Link
- Dark Web Profile: APT40. Link
- Dark Web Profile: Eldorado Ransomware. Link
- Eldorado Ransomware: The New Golden Empire of Cybercrime? Link
- Dark Web Profile: Brain Cipher. Link
- BORN Group Supply Chain Breach: In-Depth Analysis of Intelbroker's Jenkins Exploitation. Link
- A curated list of resources for DFIR. Link
- OSINT Repos List. Link
- Image Raider - a reverse image tool. List
- BlueSpy - PoC to record audio from a Bluetooth device. Link
- SOCINT tools collection. Link
- OpenStreetMap - a geolocation tool. Link
- Cellebrite got into Trump shooter's Samsung device in just 40 minutes. Link

Digital Surveillance vs. Privacy

- Digital Rummaging. Link
- Human Rights Groups Raise Alarm Over UN Cybercrime Convention. Link
- How Venezuela became a model for digital authoritarianism. Link
- Policing by design: the latest EU surveillance plan. Link
- From wiretapping to geolocation data collection: AI mass surveillance for the Paris Olympics draws privacy concerns. Link
- Olympics' AI Security Stokes Backlash Over Mass Surveillance. Link
- At the Olympics, AI Is Watching You. Link
- CIA AI director Lakshmi Raman claims the agency is taking a 'thoughtful approach' to AI. Link
- Home routing and risks to lawful interception. Link
- How data brokers sell our location data and jeopardise national security. Link
- Apple Geolocation API Exposes Wi-Fi Access Points Worldwide. Link
- Georgia Prosecutors Stoke Fears over Use of Encrypted Messengers and Tor. Link
- WhatsApp and Signal messages at risk of surveillance following EncroChat ruling, court hears. Link
- Google Wants To Start Tracking 300 Million iPhone Users Within 5 Years. Link
- Bumble and Hinge allowed stalkers to pinpoint users' locations down to 2 meters, researchers say. Link

- US border agents must get warrant before cell phone searches, federal court rules. Link
- The new US border wall is an app. Link
- EFF Tells Minnesota Supreme Court to Strike Down Geofence Warrant As Fourth Circuit Court of Appeals Takes the Wrong Turn. Link
- Another European Parliament member says he's been targeted with commercial spyware. Link
- Apple warns iPhone users in 98 countries of spyware attacks. Link
- Apple warns Indian iPhone users of possible 'mercenary spyware' attack. Link
- WhatsApp: AWS leased infrastructure to NSO Group beginning in 2018. Link
- Tech giants say foreign spyware victims should be able to sue NSO Group in US. Link
- Israel's attempt to sway WhatsApp case casts doubt on its ability to deal with NSO spyware cases. Link
- Greek Court Clears State Institutions of Involvement With Illegal Spyware. Link
- Greek prosecutor closes spyware scandal probe, infuriating opposition and victims. Link
- Sanctioned and exposed, Predator spyware maker group has gone awfully quiet. Link
- The EU's Human Rights Sanction Regime could target malicious spyware vendors. Link
- Will the Brussels spyware scandal finally convince the EU to act? Link
- Curb your snooping, Commission tells EU governments. Link
- Spyware attributed to pro-Houthi hackers used against militaries across Middle East. Link

- Data breach exposes US spyware maker behind Windows, Mac, Android and Chromebook malware. Link
- Data breach exposes millions of mSpy spyware customers. Link
- Hacked, leaked, exposed: Why you should never use stalkerware apps. Link
- Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance. Link
- The UK's Home Office is building a "national facial matching service". Link
- NZ police struggle to delete unlawfully collected images. Link
- ‘It’s completely invasive’: New app lets you spy on SF bars to see if they’re poppin’. Link
- Meta to Pay Texas $1.4bn for Unlawful Biometric Data Capture. Link
- Senators to FTC: Car companies’ data privacy practices must be investigated. Link
- Your car is spying on you – but police won’t say if they’re using the data. Link
- FTC vs surveillance pricing. Link
- FTC launches probe into how companies use data to tailor what each customer pays. Link
- TracFone to pay $16 million to settle FCC cyber and privacy investigation. Link
- The Backlash Against AI Scraping Is Real and Measurable. Link
- Meta is training its AI with public Instagram posts. Artists in Latin America can’t opt out. Link
- AI trains on kids’ photos even when parents use strict privacy settings. Link
- Police Really Want a Cybertruck, Email Shows. Link

- The SFPD’s Intended Purchase of a Robot Dog Triggers Board of Supervisors’ Oversight Obligations. Link
- Hundreds of Tech Companies Want to Cash In on Homeland Security Funding. Here's Who They Are and What They're Selling. Link
- AI-Powered Super Soldiers Are More Than Just a Pipe Dream. Link
- Research Handbook on Warfare and Artificial Intelligence. Link
- The Hidden Ties Between Google and Amazon’s Project Nimbus and Israel's Military. Link
- Israel/OPT: Dutch Investor pushes for human rights safeguards to stop use of surveillance technology against Palestinians. Link

Cyber Security

- The Dark Side of Bug Bounty. Link
- Uncoordinated Vulnerability Disclosure: The Continuing Issues With CVD. Link
- Cyber ransom payments will need to be disclosed by businesses under new laws. Link
- Switzerland federal government requires releasing its software as open source. Link
- Teams of LLM Agents can Exploit Zero-Day Vulnerabilities. Link
- Hacker Shows How to Get Free Laundry For Life. Link
- Hackers could create traffic jams thanks to flaw in traffic light controller, researcher says. Link
- Latest Intel CPUs impacted by new Indirector side-channel attack. Link
- Chinese Espionage Group Upgrades Malware Arsenal to Target All Major OS. Link
- New Tactics from a Familiar Threat. Link
- Basta ransomware operator tactics undergo 'notable shift'. Link
- Microsoft spoofing flaw exploited in infostealer attacks. Link
- Malicious Python Packages Reveal Extensive Cybercriminal Operation Based in Iraq. Link
- MirrorFace Attack against Japanese Organisations. Link
- Iranian MuddyWater Upgrades Arsenal With New Custom Backdoor. Link

- DDoS Attack Triggers New Microsoft Global Outage. Link
- How Infostealers Pillaged the World's Passwords. Link
- New SMS Stealer Malware Targets Over 600 Global Brands. Link
- A Hacker 'Ghost' Network Is Quietly Spreading Malware on GitHub. Link
- Attackers Exploit URL Protections to Disguise Phishing Links. Link
- Computer viruses can spread by using ChatGPT to write sneaky emails. Link
- Beware the RAT: Android Remote Access malware strikes in Malaysia. Link
- Mandrake Spyware Infects 32,000 Devices Via Google Play Apps. Link
- New version of sophisticated spyware remained undetected on Google app store for two years. Link
- Magento Sites Targeted with Sneaky Credit Card Skimmer via Swap Files. Link
- Telegram zero-day for Android allowed malicious files to masquerade as videos. Link
- "EchoSpoofing" — A Massive Phishing Campaign Exploiting Proofpoint's Email Protection to Dispatch Millions of Perfectly Spoofed Emails. Link
- 'GhostEmperor' returns: Mysterious Chinese hacking group spotted for first time in two years. Link
- Mid-Year Doppelgänger Information Operations In Europe And The Us. Link
- Sunburst: US Judge Dismisses Most SEC Charges Against SolarWinds. Link
- Cybersecurity and the accountability black hole. Link

- Senate leader demands answers from CISA on Ivanti-enabled hack of sensitive systems. Link
- Nine Takeaways From Our Investigation Into Microsoft's Cybersecurity Failures. Link
- Lineaje raises $20M to help organizations combat software supply chain threats. Link
- ZeroTier raises $13.5M to help avert CrowdStrike-like network problems. Link
- Allies agree new NATO Integrated Cyber Defence Centre. Link
- OECD launches pilot to monitor application of G7 code of conduct on advanced AI development. Link
- It May Soon Be Legal to Jailbreak AI to Expose How it Works. Link
- Google's dark web monitoring service will soon be free for all users. Link