CCRS Bit

April 2024

CONTENTS

Cybercrime

- Mapping the global geography of cybercrime with the World Cybercrime Index. Link
- World-first "Cybercrime Index" ranks countries by cybercrime threat level. Link
- WEF Cybercrime Atlas: Researchers are creating new insights to fight cybercrime. Link
- Most cybercriminal threats are concentrated in just a few countries, new index shows. Link
- Nigeria & Romania Ranked Among Top Cybercrime Havens. Link
- Russia and Ukraine Top Inaugural World Cybercrime Index. Link
- Europol offers law enforcement agencies data on Europe's most threatening crime networks. Link
- The Blackorbird Annual Threat Assessment 2024. Link
- Latrodectus: This Spider Bytes Like Ice. Link
- Debunking NotPetya's cyber catastrophe myth. Link
- The LockBit's Attempt to Stay Relevant, Its Imposters and New Opportunistic Ransomware Groups. Link 'Large volume' of data stolen from UN agency after ransomware attack. Link
- Decade-old malware haunts Ukrainian police. Link
- UNDP, City of Copenhagen Targeted in Data-Extortion Cyberattack. Link
- US says Russian hackers stole federal government emails during Microsoft cyberattack. Link

- “IntelBroker” Claims Geospatial Intelligence Firm Space-Eyes Breach, Exposing Sensitive US National Security Data. Link
- Hackers accessed more than 19,000 accounts on California state welfare platform. Link
- Hackers stole 340,000 Social Security numbers from government consulting firm. Link
- DOJ data on 341,000 people leaked in cyberattack on consulting firm. Link
- Hackers claim to breach database containing thousands of Russian criminal records. Link
- Hackers Linked to Russia’s Military Claim Credit for Sabotaging US Water Utilities. Link
- Food and agriculture sector hit with more than 160 ransomware attacks last year. Link
- Change Healthcare Faces Another Ransomware Threat—and It Looks Credible. Link
- US cancer center data breach exposes info of 827,000 patients. Link
- Hacker Leaks 8.5M U.S. Environmental Protection Agency (EPA) Contact Data (UPDATED). Link
- Personal information of millions of AT&T customers leaked online. Link
- The Post and Courier hacked; Black Suit claims to have 500 GB of data. Link
- When a breach goes from 25 documents to 1.3 terabytes…Link
- Ukrainian hacktivists claim to breach Russian drone developer. Link
- Chipmaker Nexperia confirms breach after ransomware gang leaks data. Link

- German database company Genios confirms ransomware attack. Link
- FIN7 cybercriminals targeted large U.S. automotive manufacturer last year. Link
- Where Hackers Find Your Weak Spots. Link
- A Spy Site Is Scraping Discord and Selling Users' Messages. Link
- Sensitive passport data of Germans published online. Link
- Hackers are threatening to leak World-Check, a huge sanctions and financial crimes watchlist. Link
- Crypto FOMO Is Back. So Are the Scam. Link
- How Cryptocurrency Revitalized Commercial CSAM. Link
- Malware dev lures child exploiters into honeytrap to extort them. Link
- Students turning to cyberfraud as huge phishing site infiltrated, police reveal. Link
- Fraudsters Exploit Telegram's Popularity For Toncoin Scam. Link
- At least a dozen Westminster insiders targeted in WhatsApp phishing attack. Link
- Deepfakes Are Coming for the Financial Sector. Link
- AI-Powered Cyber Attacks – The Alarming 85% Global Surge. Link
- The Clock is Ticking to Protect Vulnerable Groups from AI-Driven Cybercrime. Link
- Creating sexually explicit deepfake images to be made offence in UK. Link
- AI extremism technologies, tactics, actors. Link
- How Ethical Hacking Practices Are Affected by the Legislation. Link

- How big tech and silicon valley are transforming the military-industrial complex. Link
- Google won't say anything about Israel using its photo software to create Gaza "hit list". Link
- The Invisible War: Inside the electronic warfare arms race that could shape course of war in Ukraine. Link
- Inside a Modern Murder-for-Hire Ring in NYC. Link
- How Ukraine's volunteer hackers have created a 'coordinated machine' around low-level attacks. Link
- The other players who helped (almost) make the world's biggest backdoor hack. Link
- Instilling the Hacker Mindset Organizationwide. Link
- The Mystery of 'Jia Tan,' the XZ Backdoor Mastermind. Link
- North Korea Hacked Him. So He Took Down Its Internet. Link

Digital Investigation and Digital Evidence

- Cybercrime Makes Techno Cops a Commodity. Link
- Public Private Partnerships to Combat Ransomware: An inquiry into three case studies and best practices. Link
- Investigating child sexual abuse material availability, searches, and users on the anonymous Tor network for a public health intervention strategy. Link
- Voice Phishing Syndicates Unmasked An In-Depth Investigation and Exposure. Link
- Rewards Up To $10 Million For Information On Iranian Hackers. Link
- Infiltrating ransomware gangs on the dark web. Link
- International police operation infiltrates LabHost phishing website used by thousands of criminals. Link
- INTERPOL-led operation targets growing cyber threats. Link
- Founders and CEO Of Cryptocurrency Mixing Service Arrested And Charged With Money Laundering And Unlicensed Money Transmitting Offenses. Link
- Zambia Busts 77 People in China-Backed Cybercrime Operation. Link
- Crypto miner arrested for skipping on $3.5 million in cloud server bills. Link
- U.S. and Australian Police Arrested Firebird Rat Author and Operator. Link
- Moldovan Botnet Operator Indicted for Role in Conspiracy to Unlawfully Access Thousands of Infected Computers Throughout the United States. Link

- US charges Samourai cryptomixer founders for laundering $100 million. Link
- Global Cybercriminal Duo Face Imprisonment After Hive RAT Scheme. Link
- Magecart-style hackers charged by Russia in theft of 160,000 credit cards. Link
- Analysis of the apt31 indictment. Link
- Ex-FSB officer sentenced to 9 years in prison for helping Russian hackers. Link
- Former Security Engineer Sentenced to Three Years for Hacking Two Decentralized Exchanges. Link
- Mango Markets swindler convicted for brazen $110 million crypto manipulation scheme. Link
- Another insider in OneCoin cryptocurrency scam gets prison sentence. Link
- U.S. Treasury Sanctions Iranian Firms and Individuals Tied to Cyber Attacks. Link
- European collaboration on digital crime. Link
- British police investigating 'honey trap' WhatsApp messages sent to MPs. Link
- Police forces check intelligence and criminal databases after errors discovered in O2 phone data. Link
- Cops can force suspect to unlock phone with thumbprint, US court rules. Link
- Now, mobile forensic vans proposed for evidence collection at crime scenes 24x7. Link
- Axon releases Draft One, AI-powered report-writing software. Link
- Der Quick-Freeze kommt. Link
- Police Scour LockBit Ransomware Evidence, Turning Up 200 Leads. Link

- Legal implications of automated suspicious transaction monitoring: enhancing integrity of AI. Link
- Israeli authorities link 42 crypto addresses to terrorism. Link
- SIRIUS and An Garda Síochána advance collaboration in cross-border access to electronic evidence. Link
- A template for creating and sharing ground truth data in digital forensics. Link
- Presenting Digital Evidence that Holds up in Court. Link
- Trial court to decide guidelines for releasing Chula Vista Police drone video. Link
- Chula Vista Loses on Police Drone Video in Landmark State High Court Decision. Link
- Beyond the Windshield: Dashcam Forensics - A Quick Overview. Link
- Jill Dando murder revelation over Man X's striking resemblance to Serbian secret services assassin. Link
- Spoliated Video Footage Leads to Jury Instruction Sanction and More Thoughts on Linked Attachments. Link
- Expert in odometer tampering case says he cannot pinpoint individuals behind fraudulent activity. Link
- Bitcoin Fog Case Confirms Chainalysis Analytics is Reliable and Admissible in Court. Link
- Movie industry demands US law requiring ISPs to block piracy websites. Link
- FCC looks to limit how domestic violence abusers use connected cars. Link
- Japanese police create fake support scam payment cards to warn victims. Link

- Using Remote Sensing Data in Urban Crime Analysis: A Systematic Review of English-Language Literature from 2003 to 2023. Link
- Hope Revived for UN Cybercrime Treaty as Negotiations Set to Resume. Link
- Lords debate amendment to law on use of computer evidence in light of Post Office scandal. Link
- Book. Dark Wire. The Incredible True Story of the Largest Sting Operation Ever. Link

Digital Forensics

- Digital Forensics: The Good, the Bad, and the AI-Generated. Link
- CISA Releases Malware Analysis System for Public Use. Link
- Static Analysis of Malware. Link
- New Lattice Cryptanalytic Technique. Link
- Hidden files using Alternative Data Streams - this is what the cops look for. Link
- What DFIR experts need to know about the current state of the Unified Audit Log. Link
- DeRR.p. Investigating Power Events on Samsung Devices. Link
- How Did That Photo Get On That iPhone. Link
- Handbook of windows forensic artifacts across multiple Windows version with interpretation tips with some examples. Link
- Magnet Forensics Announces Magnet One, A Revolutionary Platform For The Pursuit Of Justice. Link
- Maltego Acquires PublicSonar and Social Network Harvester to Propel Vision of An All-in-One Investigation Platform. Link
- Atola Insight Forensic Gets iSCSI Support for Remote Imaging. Link
- Introducing XRY 10.9, XAMN 7.9, And XEC 7.9 From MSAB. Link
- Powershell Digital Forensics And Incident Response (DFIR) – Essential Scripts For Windows Cyber Defense. Link
- Azure Governance Visualizer Accelerator. Link
- Microsoft-Extractor-Suite. A PowerShell module for acquisition of data from Microsoft 365 and Azure. Link

Microsoft-Analyzer-Suite. A collection of PowerShell scripts for analyzing data from Microsoft 365 and Microsoft Entra ID. Link

- New Microsoft Incident Response guide helps simplify cyberthreat investigations. Link
- forensictools: A toolkit designed for digital forensics. Link
- MasterParser. A powerful DFIR tool designed for analyzing and parsing Linux logs. Link
- Lionel Notari's iOS Unified Logs Acquisition Tool. Link
- Blauhaunt. A tool collection for filtering and visualizing logon events. Link
- Indetectables Toolkit. The essential toolkit for reversing, malware analysis, and cracking. Link
- Mindmaps to help bug bounty Hunters, pentesters, and offensive/defensive security Professionals. Link
- Sysreptor. Fully customisable, offensive security reporting solution designed for pentesters, red teamers and other security-related people alike. Link
- Darknet Resources You Need to Use When Doing Cyber Threat Intelligence - Part 1 of Many. Link
- Leaked Credentials. How to look for Leaked Credentials. Link
- Lookyloo. A web interface that allows users to capture a website page and then display a tree of domains that call each other. Link
- Free Online Tools for Looking up Potentially Malicious Websites. Link
- Phunter. An OSINT tool allowing you to find various information via a phone number. Link
- Deepware. Scan & Detect Deepfake Videos. Link

- DroneXtract. A digital forensics suite for DJI drones. Link
- DJI Mavic 3 Drone Research Part 1: Firmware Analysis. Link
- DJI Mavic 3 Drone Research Part 2: Vulnerability Analysis. Link
- Free OSINT Tools. Link
- Hurricane Electric BGP Toolkit Search IPs, domains and ASNs associated with specific companies. Link
- Geolocation Revolutionized: GEOSPY AI's Cutting-Edge Technology. Link
- Geospatial Querying Using GeoHashes and GridDB. Link
- OpenSource Surveillance. A tool to gather intelligence for given city or country. Link
- VIDEO OSINT cheat sheet. Link
- Reddit OSINT: User Investigations. Link
- Leaked passwords database search tool. Link
- DFIR Report's cloud-based DFIR Labs offer a hands-on learning experience, using real data from real intrusions. Link
- Case Study: Ukrainian Cyber Police Fights Crime with Maltego. Link
- BBC Studio Documentary Unit produces Murder Case: The Digital Detectives for Channel 4. Link

Digital Surveillance vs. Privacy

- Open letter: European Commission's decision to allow data flows to Israel alarms privacy experts. Link
- Written submission: Civil society shows evidence gaps in "Going Dark" group proposal for access to data for law enforcement. Link
- Congress has a chance to rein in police use of surveillance tech. Link
- With a mysterious surveillance target identified, calls for Congress to change course. Link
- Statement: House Votes to Expand Warrantless Surveillance. Link
- U.S. House Vote Narrowly Allows Rampant Abuses of Warrantless Spying Authority to Continue. Link
- House passes bill to limit personal data purchases by law enforcement, intelligence agencies. Link
- France's latest foreign interference bill questions democratic control over surveillance services. Link
- France's Surveillance Bill Expands amid Privacy Debates. Link
- The Air Force Bought a Surveillance-Focused AI Chatbot. Link
- Drones, the air littoral, and the looming irrelevance of the U.S. Air force. Link
- 'Lavender': The AI machine directing Israel's bombing spree in Gaza. Link
- IDF colonel discusses 'data science magic powder' for locating terrorists. Link

- Israel reportedly using facial recognition and Google Photos to conduct mass surveillance in Gaza. Link
- War by algorithm raises new moral dangers. Link
- Exclusive: Google Workers Revolt Over $1.2 Billion Contract With Israel. Link
- US law proposed for DHS to make a plan for integrating AI into border control. Link
- Between privacy and border control: Tech in the Migration Pact. Link
- The colonial biometric legacy at heart of new EU asylum system. Link
- The Hellenic Data Protection Authority fines the Ministry of Migration and Asylum for the "Centaurus" and "Hyperion" systems with the largest penalty ever imposed to a Greek public body. Link
- Polizeiliche Datenanalyse: Innenausschuss diskutiert Palantir-Alternativen. Link
- IREX.ai Successfully Launches Peru’s First Real Smart-City. Link
- Polizei Bayern will Palantir den Weg ebnen. Link
- After shooting, MSU promised safety. It delivered surveillance. Link
- Sneaky Drivers Dodging Toll Cameras Cost Authorities Millions. Link
- Eye in the Sky: Backyard Trapeze Artist Fights to Halt Use of Aerial Photos for Code Inspection. Link
- Paris tests AI surveillance ahead of Olympics. Link
- We all lose if the Olympic surveillance state becomes the norm. Link
- Lords to challenge controversial DWP benefits bank account surveillance powers. Link

- The TRUTH about Bank Privacy. Link
- Outlook is Microsoft's new data collection service. Link
- How Tech Giants Cut Corners to Harvest Data for A.I. Link
- 'Reverse' searches: The sneaky ways that police tap tech companies for your private data. Link
- Police warn partnership with tech industry 'at risk' over end-to-end encryption. Link
- Police Can Spy on Your iOS and Android Push Notifications. Link
- The not-so-silent type: Vulnerabilities across keyboard apps reveal keystrokes to network eavesdroppers. Link
- Google to Delete Billions of Browsing Records in 'Incognito Mode' Privacy Lawsuit Settlement. Link
- Security bugs in popular phone-tracking app iSharing exposed users' precise locations. Link
- Israel Tried to Keep Sensitive Spy Tech Under Wraps. It Leaked Abroad. Link
- Markets Matter: A Glance into the Spyware Industry. Link
- Apple alerts users in 92 nations to mercenary spyware attacks. Link
- Apple drops term 'state-sponsored' attacks from its threat notification policy. Link
- Promoting Accountability for the Misuse of Commercial Spyware. Link
- Poland: Gov't to notify around 30 people subjected to Pegasus surveillance. Link
- Poland's prosecutor general says previous government used spyware against hundreds of people. Link
- Spain: Court reopens investigation in Pegasus spying scandal. Link

- Starry Addax targets human rights defenders in North Africa with new malware. Link
- Intruders beware: New face-detecting AI security cam fires paintballs and teargas. Link
- ShotSpotter Keeps Listening for Gunfire After Contracts Expire. Link
- How G.M. Tricked Millions of Drivers Into Being Spied On (Including Me). Link
- The Future of Biometric Technology for Policing and Law Enforcement. Link
- Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies. Link
- Colorado approves a bill to protect biological data, including neural data. Link
- 96% of US hospital websites share visitor info with Meta, Google, data brokers. Link
- Proposed FTC Order will Prohibit Telehealth Firm Cerebral from Using or Disclosing Sensitive Data for Advertising Purposes, and Require it to Pay $7 Million. Link
- Protection of personal data: according to Advocate General Pikamäe, the supervisory authority has an obligation to act when it finds a breach in the course of investigating a complaint. Link
- FTC Issues $5.6M in Refunds to Customers After Ring Privacy Settlement. Link
- Book. The Cambridge Handbook of facial recognition in the modern state. Link

Cyber Security

- XZ backdoor story – Initial analysis. Link
- Open Source Security (OpenSSF) and OpenJS Foundations Issue Alert for Social Engineering Takeovers of Open Source Projects. Link
- Toward greater transparency: Adopting the CWE standard for Microsoft CVEs. Link
- Google paid $10 million in bug bounty rewards last year. Link
- Price of zero-day exploits rises as companies harden products against hackers. Link
- 1,200+ Vulnerabilities Detected In Microsoft Products In 2023. Link
- Thousands of Qlik Sense Servers Open to Cactus Ransomware. Link
- Large-scale brute-force activity targeting VPNs, SSH services with commonly used login credentials. Link
- Teetering on the Edge: VPNs, Firewalls' Nonexistent Telemetry Lures APTs. Link
- Over 1,400 CrushFTP servers vulnerable to actively exploited bug. Link
- Beware! Zero-Click RCE Exploit For IMessage Circulating On Hacker Forums. Link
- “Mobile NotPetya”: Spyware Zero-Click Exploit Development Increases Threat of Wormable Mobile Malware. Link
- Chinese Keyboard Apps Open 1B People to Eavesdropping. Link

- Over 92,000 exposed D-Link NAS devices have a backdoor account. Link
- Various Botnets Pummel Year-Old TP-Link Flaw in IoT Attacks. Link
- US government says security flaw in Chirp Systems' app lets anyone remotely control smart home locks. Link
- The spam came from inside the house: How a smart TV can choke a Windows PC. Link
- AI-as-a-Service Providers Vulnerable to PrivEsc and Cross-Tenant Attacks. Link
- Satellite Hacking Demystified. Link
- Hackers Exploit Old Microsoft Office 0-Day To Deliver Cobalt Strike. Link
- From OneNote to RansomNote: An Ice Cold Intrusion. Link
- Okta Warns Of Credential Stuffing Attacks Using Proxy Services. Link
- Chinese Botnet As-A-Service Bypasses Cloudflare & Other DDoS Protection Services. Link
- New SSLoad Malware Combined With Tools Hijacking Entire Network Domain. Link
- Fake Facebook MidJourney AI page promoted malware to 1.2 million people. Link
- Microsoft Warns: North Korean Hackers Turn to AI-Fueled Cyber Espionage. Link
- Hack to the Future: Using LLMs as attacking agents in real networks. Link
- Android Malware Brokewell With Complete Device Takeover Capabilities. Link
- WithSecure uncovers Kapeka, a new malware with links to Russian nation-state threat group Sandworm. Link

- LockBit 3.0 Variant Generates Custom, Self-Propagating Malware. Link
- New DragonForce Ransomware Emerged From The Leaked LOCKBIT Builder. Link
- Redline Stealer Malware Evolves with Sneaky New Tricks, Spreads Globally. Link
- Fileless .NET Based Code Injection Attack Delivers AgentTesla Malware. Link
- 5000+ CrushFTP Servers Hacked Using Zero-Day Exploit. Link
- EM eye: eavesdropping on security camera via unintentional RF emissions. Link
- KageNoHitobito Ransomware Attacking Windows Users Around The Globe. Link
- Godfather Banking Trojan Spawns 1.2K Samples Across 57 Countries. Link
- Cybercriminal Campaign Spreads Infostealers, Highlighting Risks to Web3 Gaming. Link
- eXotic Visit campaign: Tracing the footprints of Virtual Invaders. Link
- Researchers Uncover That UK.GOV Websites Sending Data To Chinese Ad Vendor Analysts. Link
- FCC to probe 'grave' weaknesses in phone network infrastructure. Link
- Feds finally decide to do something about years-old SS7 spy holes in phone networks. Link
- JCDC Working and Collaborating to Build Cyber Defense for Civil Society and High-Risk Communities. Link
- Joint Statement on the Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression. Link

- Cyber Resilience Act Requirements Standards Mapping - Joint Research Centre & ENISA Joint Analysis. Link
- NIST Researchers Use Cellphone Compass to Measure Tiny Concentrations of Compounds Important for Human Health. Link
- US supreme court ruling suggests change in cybersecurity disclosure process. Link
- Exposure Management: The Evolution of Vulnerability Management. Link
- NATO to launch new cyber center to contest cyberspace 'at all times'. Link
- Book. Hacked: The Secrets Behind Cyber Attacks. Link
- BlackHat ASIA 2024-Slides. Link