CCRS Bit

August 2024

CONTENTS

Cybercrime

- Cybercrime and sabotage cost German firms $300 bln in past year. Link
- Cyber Warfare Statistics: China and Russia Ranks the Most Dangerous Cyber Aggressive Countries. Link
- The global chip war could turn into a cloud war. Link
- Digital War in the Middle East: Cyber Threats in Israel-Iran Conflict. Link
- I Spy With My Little Eye: Uncovering an Iranian Counterintelligence Operation. Link
- After Iran Steals Sensitive Israeli Data, Israel Tries to Censor the Internet. Link
- Chinese government hackers targeted US internet providers with zero-day exploit, researchers say. Link
- Google TAG Uncovers Watering Hole Attacks on Mongolian Government Websites. Link
- Iranian cybercriminals are targeting WhatsApp users in spear phishing campaign. Link
- Exclusive: Russian spies hacked UK government data and emails earlier this year. Link
- Rivers of Phish - Sophisticated Phishing Targets Russia’s Perceived Enemies Around the Globe. Link
- Russian cyber snoops linked to massive credential-stealing campaign. Link
- Widespread QR code phishing targeted Microsoft 365 credentials. Link
- The biggest data breaches in 2024: 1 billion stolen records and rising. Link

- National Public Data leaked passwords online. Link
- National Public Data Published Its Own Passwords. Link
- National Public Data tells officials 'only' 1.3M people affected by intrusion. Link
- 32 Million Sensitive Records Exposed From Service Management Provider. Link
- Hacked GPS tracker reveals location data of customers. Link
- Hunters International ransomware gang threatens to leak US Marshals data. Link
- 332 Million Email Addresses Scraped from SOCRadar.io Published Online. Link
- Background check company breached, nearly 3 billion exposed in data theft. Link
- After nearly 3B personal records leak online, Florida data broker confirms it was ransacked by cyber-thieves. Link
- Plane tracker app FlightAware admits user data exposed for years. Link
- RansomHub hits 210 victims in just 6 months. Link
- Ransomware Victims Paid $460 Million in First Half of 2024. Link
- Six ransomware gangs behind over 50% of 2024 attacks. Link
- Understanding the ‘Morphology’ of Ransomware: A Deeper Dive. Link
- Over 950K compromised in BlackSuit ransomware attack against Connexure. Link
- How the ransomware attack at Change Healthcare went down: A timeline. Link
- From Protests to Profit: Why Hacktivists Are Joining the Ransomware Ranks. Link
- Hacktivists Target France in Retaliation for Arrest of Telegram Founder Pavel Durov. Link

- Cyber Threat Intelligence: Illuminating the Deep, Dark Cybercriminal Underground. Link
- Telegram: 'The dark web in your pocket'. Link
- Far-Right ‘Terrorgram’ Chatrooms Are Fueling a Wave of Power Grid Attacks. Link
- 'Malfunction' at Dutch defense ministry datacenter causing mass disruption. Link
- Green Berets storm building after compromising its Wi-Fi. Link
- Russia tells citizens to switch off home surveillance because the Ukrainians are coming. Link
- Check your IP cameras: There's a new Mirai botnet on the rise. Link
- Malware exploits 5-year-old zero-day to infect end-of-life IP cameras. Link
- Brazilian Ad Fraud Network 'Camu' Hits 2B+ Daily Bid Requests. Link
- 'Digital arrest' scams are big in India and may be spreading. Link
- Beware: scams involving fake correspondence from Europol. Link
- ‘Pig butchering’ scammers target BBC reporter. Link
- They Looked Like An Ordinary Texan Family. The FBI Says The Parents Are Pig Butcherers Who Stole $10 Million. Link
- New Phishing Attacks Target Eastern European Bank Users on iOS and Android. Link
- Sextortion Scams Now Include Photos of Your Home. Link
- Fake funeral “live stream” scams target grieving users on Facebook. Link
- SMS scammers use toll fees as a lure. Link

- Crypto scammers who hacked McDonald's Instagram account say they stole $700,000. Link
- Carbon black supplier Orion loses $60 million in business email compromise scam. Link
- 2024 Crypto Crime Mid-year Update Part 2: China-based CSAM and Cybercrime Networks On The Rise, Pig Butchering Scams Remain Lucrative. Link
- Money Laundering in the Digital Age: Exploring Virtual Assets Role. Link
- Cybercrime Rapper Sues Bank over Fraud Investigation. Link
- The rise of deepfakes beyond social media. Link
- Dad hacks database to fake death and avoid child support pay. Link
- USDoD Hacker Behind $3 Billion SSN Leak Reveals Himself as Brazilian Citizen. Link
- Newly Discovered Group Offers CAPTCHA-Solving Services to Cybercriminals. Link

Digital Investigation and Digital Evidence

- Investigating the Convergence of Cyberattacks and Disinformation. Link
- On the Offensive: Tracking Ransomware Gangs Across the Globe. Link
- United Nations treaty on cybercrime agreed by the Ad Hoc Committee. Link
- Bureaucratic initiative redefines German law enforcement cyber operations. Link
- Breaking Ground: The EU's First Far-Right Designation of 'The Base' and Its Impact on Online Content. Link
- Brazilian authorities launch OPERATION REDIRECT targeting illegal music sites responsible for malware distribution. Link
- The world's largest TV and movie piracy streaming ring is dead. Link
- Turkish intelligence dismantles global cyber espionage network. Link
- UK Shuts Down 'Russian Coms' Fraud Platform Defrauding Millions. Link
- Argentina Busts Crypto Ring Linked to North Korea, Seizes Millions. Link
- Feds bust minor league Radar/Dispossessor ransomware gang. Link
- Researcher sued for sharing data stolen by ransomware with media. Link
- Over $40 Million Recovered and Arrests Made Within Days After Firm Discovers Business Email Compromise Scam. Link

- Police hunt scammers after takedown of Russian Coms fraud platform. Link
- U.S. Secret Service Offers $2.5 Million Bounty for Capture of Top Wanted Hacker. Link
- Employee arrested for locking Windows admins out of 254 servers in extortion plot. Link
- DOJ Charges Nashville Man for Helping North Koreans Get U.S. Tech Jobs. Link
- Ransom Cartel, Reveton ransomware owner arrested, charged in US. Link
- WWH-Club credit card market admins arrested after cash spending spree. Link
- Behind the arrest of Telegram boss, a small Paris cybercrime unit with big ambitions. Link
- Telegram CEO Pavel Durov charged with allowing criminal activity. Link
- US accuses man of being 'elite' ransomware pioneer they've hunted for years. Link
- Ten people arrested, more than 100 charges laid in SIM swap scam: Toronto police. Link
- US indicts duo over alleged Swatting spree that targeted elected officials. Link
- U.S. charges Karakurt extortion gang’s “cold case” negotiator. Link
- 2 Men From Europe Charged With ‘Swatting’ Plot Targeting Former US President and Members of Congress. Link
- Guilty plea entered by ex-Verizon employee for spying for China. Link
- U.S. Army Intelligence Analyst Pleads Guilty to Charges of Conspiracy to Obtain and Disclose National Defense Information, Export Control Violations and Bribery. Link

- Owners of 1-Time Passcode Theft Service Plead Guilty. Link
- Russian man who sold logins to nearly 3,000 accounts gets 40 months in jail. Link
- Russian Citizen Sentenced to 40 Months for Selling Stolen Financial Information on the Criminal Internet Marketplace Slilpp. Link
- A UK court ordered a global asset freeze for the 'Cryptoqueen' and her OneCoin associates. Link
- Leader of International Malvertising and Ransomware Schemes Extradited from Poland to Face Cybercrime Charges. Link
- National Crime Agency threatens extraditions over rise in sextortion cases. Link
- Police officers are starting to use AI chatbots to write crime reports. Will they hold up in court? Link
- Google Has Unleashed Its Legal Fury on Hackers and Scammers. Link
- Defending the Digital Frontier: How Criminal Defense Lawyers Address Cybersecurity Crimes. Link

Digital Forensics

- Memory Forensics Tools Overview. Link
- Digital Detectives vs. Android 14: overcoming new forensic challenges. Link
- iOS 17- the "forever" setting that isn't… or is it? Link
- Unpacking iOS 18's New Privacy Features – A Digital Forensics Perspective. Link
- Skinny dipping into browser data - a tool and open plugin framework for parsing website/web app artefacts in browser data. Link
- Wireshark 4.4.0 Released – What's New! Link
- Threat Actors' Toolkit: Leveraging Sliver, PoshC2 & Batch Scripts. Link
- BlackSuit Ransomware. Link
- Magnet Forensics Acquires Medex Forensics, Strengthening Video Evidence Integrity. Link
- Criminal IP and Maltego Collaborate to Broaden Threat Intelligence Data Search. Link
- Decode: New Digital Forensics and Investigations Company Launched. Link
- CohnReznick Launches Digital Forensics Lab. Link
- Digital Forensics Market is expected to undergo a CAGR of 12.40% during the forecast period of 2021 to 2029. Link
- Digital Forensic Technology Market is Likely to Experience a Tremendous Growth in Near Future. Link
- TRACE - a digital forensic analysis tool that provides a user-friendly interface for investigating disk images. Link

- UFADE (Universal Forensic Apple Device Extractor) v0.9.1. Link
- DNS Spy: Tool that Monitors and Analyzes DNS Configurations in Real-Time. Link
- Intercepting Mobile Application Traffic with Caido and Frida. Link
- Obstracts: A Comprehensive Tool for Threat Intelligence and Risk Management. Link
- Prying Deep - An OSINT tool to collect intelligence on the dark web. Link
- Darkus - An Onion Website Searcher to Search Specific Words and Give You Back the Link Results. Link
- X-osint - an OSINT tool which gathers useful and yet credible valid information about a phone number, user's email address and IP address and more to come in future updates. Link
- Telegram OSINT. In-depth repository of Telegram OSINT resources covering, tools, techniques & tradecraft. Link
- The Ultimate Guide to the OSINT Framework. Link
- OSINT Methods for Image Investigations. Link
- Mapping and Geospatial Intelligence Tools. Link
- A collection of online resources and tools to assist with IMINT investigations. Link
- Face Eagle - Search among 4,190,640 face images. Link
- Chasing Shadows: Geolocate Images with Bellingcat's Shadow Finder Tool. Link
- Investigating the Target Online. Link
- OSINT Investigation Techniques for Missing Person Cases (Trace Labs). Link
- The Exciting Evolution of OSINT Tools: What’s Making Waves in 2024. Link

- The Essential Guide to OSINT: Top Tools for Modern Investigations. Link
- List of OSINT Repositories starred from GitHub. Link
- SMWYG-Show-Me-What-You-Got - This tool allows you to perform OSINT and reconnaissance on an organization or an individual. Link
- From Digital Forensics to Legal Claims: Leveraging Cybersecurity in Car Accident Cases. Link
- DHS guides cops on investigating crime committed using mDLs. Link
- REPORT Act revolutionizes child protection: A deep dive into legislative and digital forensic innovations. Link
- The AI revolution in forensics: Catching criminals in the digital age. Link
- AI And Digital Forensics Transforming Law Enforcement. Link
- Pindrop introduces voice deepfake detection tool, tracks down Harris spoof source. Link

Digital Surveillance vs. Privacy

- The UN Cybercrime Convention: Analyzing the Risks to Human Rights and Global Privacy. Link
- The UN Cybercrime convention is a victory for digital authoritarianism. Link
- How A Former Palantir Exec Built A Google-Like Surveillance Tool For The Police. Link
- Argentina will use AI to 'predict future crimes' but experts worry for citizens' rights. Link
- Expanded Police Surveillance Will Get Us "Broken Windows" on Steroids. Link
- Wir veröffentlichen den Entwurf zum neuem BKA-Gesetz. Link
- Intelligence bill would elevate ransomware to a terrorist threat. Link
- The 2024 Paris Olympics are gone, but AI surveillance may be here to stay. Link
- Privacy Impact Assessment for the CBP Commercial Telemetry Data Evaluation. Link
- EU pushes for new surveillance technology against migration, German police union asks for €35 million. Link
- Frontex goes drone shopping as EU looks to keep migrants out. Link
- The crowdfunding campaign for deadly Israeli military drones. Link
- Swarm Wars: The Shaky Rise Of AI Drones In Ukraine. Link
- Backyard Privacy in the Age of Drones. Link
- Colorado police department shows new ways to use drones for law enforcement. Link

- Locked In, Locked Out: How Data Breaches Shatter Refugees' Safety. Link
- Homeland Security Still Dreams of Face Recognition at the Border. Link
- The US wants to use facial recognition to identify migrant children as they. Link
- Canadian border agency launching immigration app with facial recognition, AWS tech. Link
- Israel is introducing new biometric technology on the border of West Bank: report. Link
- CBSA to use facial recognition app for people facing deportation: documents. Link
- Remote biometric surveillance and policing – a new frame of reference? Link
- Contactless fingerprint biometrics interoperability guidance updated. Link
- Police set facial recognition on collision course with AI Act in Germany. Link
- Careful procurement, data collection help avoid common biometrics challenges. Link
- Texas State Police Gear up for Massive Expansion of Surveillance Tech. Link
- The future of CCTV and policing. Link
- The Fifth Circuit Shuts Down Geofence Warrants—And Maybe A Lot More. Link
- A Ruling That Eliminates Important Privacy Rights in Many Stored Internet Contents—And The Legal Challenge to It. Link
- Audit: Decommissioned FBI electronic storage media plagued with security flaws. Link. Link

- FBI Wants More Access To Everything, Can’t Be Bothered To Protect The Stuff It Already Has. Link
- Mass hacking and fundamental rights: a missed opportunity for the CJEU? Link
- Google’s crack spyware hunter tracks down software that listens through targets’ phones. Link
- Russian government hackers found using exploits made by spyware companies NSO and Intellexa. Link
- State-backed attackers and commercial surveillance vendors repeatedly use the same exploits. Link
- Powerful Spyware Exploits Enable a New String of ‘Watering Hole’ Attacks. Link
- Britain and France to discuss misuse of commercial cyber intrusion tools. Link
- A Global Treaty to Fight Cybercrime—Without Combating Mercenary Spyware. Link
- Civil Society Joint Statement on the Use of Surveillance Spyware in the EU and Beyond. Link
- Judge says maker of Pegasus spyware does not need to provide sought-after Israeli witnesses in WhatsApp case. Link
- EFF to Ninth Circuit: Don’t Shield Foreign Spyware Company from Human Rights Accountability in U.S. Court. Link
- Chinese broadband satellites may be Beijing's flying spying censors, think tank warns. Link
- Is social media monitoring in the UK: the invisible surveillance tool increasingly deployed by government. Link
- UK police monitoring TikTok for evidence of criminality at far-right riots. Link
- UK: Big Tech platforms play an active role in fuelling racist violence. Link

- Video doorbells, CCTV, facial recognition: how the police tracked UK rioters. Link
- Suing Apple To Force It To Scan iCloud For CSAM Is A Catastrophically Bad Idea. Link
- Telegram really an encrypted messaging app? Link
- Signal Is More Than Encrypted Messaging. Under Meredith Whittaker, It's Out to Prove Surveillance Capitalism Wrong. Link
- Google and Meta struck secret ads deal to target teenagers. Link
- Apple's Huge "Dual Use" Face Swap App Problem Is Not Going Away. Link
- Meta's $1.4 billion settlement with Texas includes biometric safe harbor. Link
- Sensors can read your sweat and predict overheating. Here's why privacy advocates care. Link
- NFL to begin using face scanning tech across all of its stadiums. Link
- Twitch's Drop Ins Feature Turned On VTubers' Cameras Without Consent. Link
- Hacker Breaks Into GPS Tracker Tool, Looks Up User Locations. Link
- TELL BUMBLE: Don't sell or share users' data without their permission. Link
- Swipe Left for Identity Theft: An Analysis of User Data Privacy Risks on Location-based Dating Apps. Link
- Uber fined $325 million for moving driver data from Europe to US. Link
- Digital License Plates and the Deal That Never Had a Chance. Link Link

- Did your car witness a crime? Bay Area police may be coming for your Tesla — and they might tow it. Link
- The Wiretap: How Cops Got A Toyota Dealership To Spy On A Loaner Car For 3 Weeks. Link
- New Patent Application for Car-to-Car Surveillance. Link
- Texas Accuses GM, OnStar of Violating Drivers' Data Privacy. Link
- FTC Takes Action Against Security Camera Firm Verkada over Charges it Failed to Secure Videos, Other Personal Data and Violated CAN-SPAM Act. Link
- Conviction Secured For LAPD Officer Who Falsely Added People To PD's Gang Database. Link
- Detroit Man Secures $300,000 Payout For False Facial Recognition Arrest. Link
- Surveillance Watch, an interactive map and resource that documents the hidden connections within the opaque surveillance industry. Link

Cyber Security

- Computer Crash Reports Are an Untapped Hacker Gold Mine. Link
- Researchers find decades-old vulnerability in major web browsers. Link
- Israeli cyber researchers uncover critical vulnerability in networking system. Link
- Critical Flaw in Ivanti Virtual Traffic Manager Could Allow Rogue Admin Access. Link
- Routers from China-based TP-Link a national security threat, US lawmakers claim. Link
- Hackers could spy on cell phone users by abusing 5G baseband flaws, researchers say. Link
- U.S. CISA adds Dahua IP Camera, Linux Kernel and Microsoft Exchange Server bugs to its Known Exploited Vulnerabilities catalog. Link
- Microsoft's AI Can Be Turned Into an Automated Phishing Machine. Link
- Watch How a Hacker's Infrared Laser Can Spy on Your Laptop's Keystrokes. Link
- Hardware Backdoor Discovered in RFID Cards Used in Hotels and Offices Worldwide. Link
- Backdoor in Mifare Smart Cards Could Open Doors Around the World. Link
- Sinkclose' Flaw in Hundreds of Millions of AMD Chips Allows Deep, Virtually Unfixable Infections. Link

- White hat hacker shines spotlight on vulnerability of solar panels installed in Europe. Link
- Ecovacs home robots can be hacked to spy on their owners, researchers say. Link
- Tired of airport security queues? SQL inject yourself into the cockpit, claim researchers. Link
- Hundreds of LLM Servers Expose Corporate, Health & Other Online Data. Link
- Researchers Uncover Vulnerabilities in AI-Powered Azure Health Bot Service. Link
- Misconfiguration exposes suspected People Data Labs data. Link
- Hijacked: How Cybercriminals Are Turning Anti-Virus Software Against You. Link
- Researchers Uncover New Infrastructure Tied to FIN7 Cybercrime Group. Link
- Dark Web Profile: Dispossessor Ransomware. Link
- New APT Group Actor240524: A Closer Look at Its Cyber Tactics Against Azerbaijan and Israel. Link
- Cyclops: a likely replacement for Bellaciao. Link
- More advanced, stealthy LummaC2 malware variant emerges. Link
- LummaC2 infostealer uses obfuscated scripts via PowerShell to target endpoints. Link
- New Voldemort malware abuses Google Sheets to store stolen data. Link
- MINT STEALER: Running by a BulletProof Hoster. Link
- New QR Code Phishing Campaign Exploits Microsoft Sway to Steal Credentials. Link
- New Snake Keylogger Variant Slithers Into Phishing Campaigns. Link

- APT Group StormBamboo Attacks ISP Customers Via DNS Poisoning. Link
- Cyberattackers Exploit Google Sheets for Malware Control in Likely Espionage Campaign. Link
- BlackByte Ransomware Exploits VMware ESXi Flaw in Latest Attack Wave. Link
- CVE-2024-7971: North Korean APT Citrine Sleet Exploits Chromium Zero-Day. Link
- BlackByte blends tried-and-true tradecraft with newly disclosed vulnerabilities to support ongoing attacks. Link
- Black Basta and the Use of LLMs by Threat Actors. Link
- Fake Palo Alto GlobalProtect used as lure to backdoor enterprises. Link
- Unpatched AVTECH IP Camera Flaw Exploited by Hackers for Botnet Attacks. Link
- Iranian Hackers Use New Tickler Malware for Intelligence Gathering on Critical Infrastructure. Link
- Hacking a Secure Industrial Remote Access Gateway. Link
- TodoSwift: North Korean Cybercriminals Use Bitcoin Lure to Spread macOS Malware. Link
- Cryptocurrency Lures and Pupy RAT: Analysing the UTG-Q-010 Campaign. Link
- Digital Wallets Bypassed To Allow Purchase With Stolen Cards. Link
- Biotech company hacked in 2023 pays states $4.5 million over breached data. Link
- UK data watchdog to fine NHS vendor Advanced for security failures prior to LockBit ransomware attack. Link
- Indian telecom regulator orders crackdown on spam calls. Link
- On the Cyber Safety Review Board. Link

- NCSC to Build Nation-Scale Evidence Base for Cyber Deception. Link
- Here’s How we Made a Real-time Phishing Website Detector for MacOS. Link
- Google Play bug bounty program shutdown imminent. Link
- Conference presentation slides: - Black Hat USA 2024 slides (3-8 August,2024) - REcon 2024 Slides (28-30 Jun,2024) - Offensivecon 2024 (May 10-11,2024 Berlin) - Blackhat Asia 2024 (April 16-19, 2024 Marina Bay Sands / Singapore) – Blackhat. Link