CCRS Bit

February 2024

CONTENTS

Cybercrime

- A New Age of Hacktivism. Link
- Cloudflare Breach: Nation-State Hackers Access Source Code and Internal Docs. Link
- Russia-Aligned TAG-70 Targets European Government and Military Mail Servers in New Espionage Campaign. Link
- Iran-Linked UNC1549 Hackers Target Middle East Aerospace & Defense Sectors. Link
- Chinese hackers hid in US infrastructure network for 5 years. Link
- Anonymous spies on FBI / UK Police hacking investigation conference call. Link
- DDoS attack on Pennsylvania court system knocks out filing systems, bail payment site. Link
- Chinese hackers infect Dutch military network with malware. Link
- Hacker exposed weakness in German electronic ID, magazine reports. Link
- New Wave of 'Anatsa' Banking Trojans Targets Android Users in Europe. Link
- The Cheap Radio Hack That Disrupted Poland’s Railway System. Link
- Ransomware Groups Are Bouncing Back Faster From Law Enforcement Busts. Link
- Feds hack LockBit, LockBit springs back. Now what? Link
- Ransomware payment rates drop to new low – now 'only 29% of victims' fork over cash. Link

- The Scourge of Ransomware Victim: Insights on Harms to Individuals, Organisations and Society. Link
- Hyundai Motor Europe hit by Black Basta ransomware attack. Link
- Hackers uncover new TheTruthSpy stalkerware victims: Is your Android device compromised? Link
- 20+ hospitals in Romania hit hard by ransomware attack on IT service provider. Link
- Ransomware gang seeks $3.4 million after attacking children's hospital. Link
- Data breach at French healthcare services firm puts millions at risk. Link
- US health tech giant Change Healthcare hit by cyberattack. Link
- 1.3 Million-Record Database of Netherlands COVID-19 Testing Lab Exposed Online. Link
- Pharmaceutical giant Cencora says data was stolen in a cyberattack. Link
- Health insurance data breach affects nearly half of France's population, privacy regulator warns. Link
- Bank of America warns customers of data breach after vendor hack. Link
- 'World's biggest casino' app exposed customers' personal data. Link
- 200,000 Facebook Marketplace user records leaked on hacking forum. Link
- Unsecured Database Leaks 153 GB of Filipino Student and Family Data. Link
- Credit Union Service Leaks Millions of Records and Passwords in Plain Text. Link
- Congressional hearing on "Crypto Crime in Context". Link

- New ‘Pig Butchering’ Crypto Scams From A Law Enforcement Viewpoint. Link
- SpyNote Android Spyware Poses as Legit Crypto Wallets, Steals Funds. Link
- North Korean hackers now launder stolen crypto via YoMix tumbler. Link
- The latest ‘Woj bomb’ was just a scam NFT tweet from a hacked account. Link
- Security Researcher Allegedly Hacked Apple’s Backend, Scammed $2.5 Million. Link
- Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’. Link
- ‘Everyone looked real’: multinational firm’s Hong Kong office loses HK$200 million after scammers stage deepfake video meeting. Link
- The On-chain Footprint of Southeast Asia’s ‘Pig Butchering’ Compounds: Human Trafficking, Ransoms, and Hundreds of Millions Scammed. Link
- How cyberscams are drawing China into Myanmar’s civil war. Link
- Deepfake scammer walks off with $25 million in first-of-its-kind AI heist. Link
- Cybersecurity expert says the next generation of identity theft is here: 'Identity hijacking'. Link
- Fake Funeral Live Stream Scams Are All Over Facebook. Link
- The Metropolitan Police’s Crypto team presented The Little Book of Crypto Crime. Link
- The Anatomy of a Scam: The Shoebox Incident. Link
- International Law Enforcement Agencies Issue Joint Warning about Global Financial Sextortion Crisis. Link

- FBI: 'Financial sextortion' of teens is a 'rapidly escalating threat.' How parents can protect their kids. Link
- Instagram and Facebook knowingly platform parents who sexually exploit children for profit, say reports. Link
- Taylor Swift fake nudes show this harassment could happen to anyone. Link
- As AI porn generators get better, the stakes get higher. Link
- Deepfake face swap attacks on ID verification systems up 704% in 2023. Link
- Behind Asia's cyber slavery. DW Documentary. Link
- Inside the weird, shady world of click farms. Link
- Gaming and Extremism: The Radicalization of Digital Playgrounds. Link
- Gen Z Spies: Are Gamers a Bigger Threat Than Foreign Operatives? Link
- Gone in 20 seconds: how ‘smart keys’ have fueled a new wave of car crime. Link
- Anonymous: a cult of personality that could soon fail. Link
- Russian Language Cybercriminal Forums – Analyzing the Most Active And Renowned Communities. Link
- “This Forum is a Bunch of Communists and They Set Me Up”, LockBit Spills the Tea Regarding Their Recent Ban on Russian-Speaking Forums. Link
- Top 10 Deep Web and Dark Web Forums. Link

Digital Investigation and Digital Evidence

- The Crucial Role of Intelx.io in Crypto Investigations. Link
- The On-chain Footprint of Southeast Asia's 'Pig Butchering' Compounds: Human Trafficking, Ransoms, and Hundreds of Millions Scammed. Link
- Rethinking Open-Source Intelligence for Security in Commercial Settings. Link
- Offensive OSINT s05e04 - Open Source Surveillance - Username search. Link
- INTERPOL-led operation targets growing cyber threats. Link
- Taiwan money laundering trials spotlight Asian cyberscam sector. Link
- TRM's Kyle Armstrong Sits Down with Former FBI Section Chief Bryan Smith to Discuss the Evolution of Crypto Tracing at the FBI. Link
- Chinese hackers fail to rebuild botnet after FBI takedown. Link
- US offers $10 million reward for info on Hive ransomware gang members. Link
- U.S. DoJ Dismantles Warzone RAT Infrastructure, Arrests Key Operators. Link
- U.S. Government disrupts botnet used by Russian GRU hackers. Link
- Police Seized 50,000 Bitcoin From Operator Of The Now-Defunct Piracy Site Movie2k. Link
- Knight ransomware source code for sale after leak site shuts down. Link

- A Global Police Operation Just Took Down the Notorious LockBit Ransomware Gang. Link
- After LockBit takedown, police try to sow doubt in cybercrime community. Link
- Authorities Claim LockBit Admin "LockBitSupp" Has Engaged with Law Enforcement. Link
- US offers $15 million bounty for info on LockBit ransomware gang. Link
- Interpol arrests more than 30 cybercriminals in global 'Synergia' operation. Link
- US announces another arrest in BTC-e cybercrime case. Link
- Teen arrested in massive string of swatting attacks. Link
- Executive alleged to be behind EncroChat encrypted phone network arrested. Link
- Hacker arrested for selling bank accounts of US, Canadian users. Link
- Cryptojacker arrested in Ukraine over EUR 1.8 million mining scheme. Link
- Darknet Drug Dealers Arrested After Packages of Meth-Laced Adderall Repeatedly Returned to Sender. Link
- Russia arrests three alleged SugarLocker ransomware members. Link
- Charges filed in DDoS-for-hire attacks, including Baltimore schools incident. Link
- Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally. Link
- FBI's Most-Wanted Zeus and IcedID Malware Mastermind Pleads Guilty. Link
- Joshua Schulte: Former CIA hacker sentenced to 40 years in prison. Link

- Portland Man Sentenced to Federal Prison for Role in SIM Swapping Identity Theft and Fraud Scheme. Link
- DraftKings Hacker Sentenced to 18 Months in Prison. Link
- Bitsonic chief sentenced to 7 years for crypto theft in South Korea. Link
- Assistant moderator of dark web child sexual abuse site is sentenced. Link
- US sanctions Iranians behind CNI cyber attacks. Link
- YouTube, Discord, and Lord of the Rings Led Police to a Teen Accused of a US Swatting Spree. Link
- How We Were Able to Infiltrate Attacker Telegram Bots. Link
- Stalkerware apps PhoneSpector and Highster appear shut down after NY settlement. Link
- FCC moves to outlaw AI-generated robocalls. Link
- How Artificial Intelligence Can Use To Fight Cybercrime? Link
- Legal implications of automated suspicious transaction monitoring: enhancing integrity of AI. Link
- Google and CSA Singapore Combat Android Fraud With New Pilot. Link
- Automating CSAM Investigation, Cybercrimeology EP102. Link
- This Website Tracked Hate Crimes in India. Then the Government Took It Offline. Link
- Using AI to monitor the internet for terror content is inescapable – but also fraught with pitfalls. Link
- Belgien setzt Überwachungs-KI der deutschen Medienaufsicht ein. Link
- Leveraging AI LLMs to Counter Social Engineering: A Psychological Hack-Back Strategy. Link
- Treasury Publishes 2024 National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing. Link

- The Legality of SKY ECC Evidence: A Controversy Over Privacy and Fair Trials. Link
- In-Depth: EncroChat Defendants Say Post Office Scandal Gives Them Hope. Link
- Intelligence services unlawfully investigated entire population groups. Link
- How the FBI and CISA look to mature the government's top ransomware task force. Link
- Deputy Prime Minister hosts first global conference targeting 'hackers for hire' and malicious use of commercial cyber tools. Link
- Draft UN Cybercrime Treaty Could Make Security Research a Crime, Leading 124 Experts to Call on UN Delegates to Fix Flawed Provisions that Weaken Everyone's Security. Link

Digital Forensics

- Bullshit Hunting: Digital Forensics Edition. Link
- The Lazy Guide To Reverse RPC. Link
- Advanced CyberChef Techniques for Configuration Extraction - Detailed Walkthrough and Examples. Link
- BPF Memory Forensics with Volatility 3. Link
- Forensic Duel: Exploring Deleted WhatsApp Messages—iOS vs Android. Link
- Here is Apple's official 'jailbroken' iPhone for security researchers. Link
- 5 simple tricks to quickly analyze a larger list of URLs. Link
- Deep Links & WebViews Exploitations Part I. Link
- Deep Links & WebViews Exploitations Part II. Link
- AWS Ransomware. Link
- Skrapa - a new tool that scans memory quickly by filtering on memory attributes. Link
- FormThief - a project designed for spoofing Windows desktop login applications using WinForms and WPF. Link
- BypassAV - a map that lists the essential techniques to bypass anti-virus and EDR. Link
- The-OSINT-Newsletter. Link
- CloakQuest3r - Uncover the true IP address of websites safeguarded by Cloudflare & Others. Link
- Spy.pet - Explore Discord's data with over 300 million users and still growing. Link
- MrHandler - Linux Incident Response Reporting. Link

SploitScan - A Sophisticated Cybersecurity Utility Designed

To Provide Detailed Information On Vulnerabilities And Associated Proof-Of-Concept (PoC) Exploits. Link

- SiCat - an advanced exploit search tool designed to identify and gather information about exploits from both open sources and local repositories effectively. Link

Digital Surveillance vs. Privacy

- Stingrays, Simulators, Surveillance, and Silverados. Link
- Is Clarence Darrow Dead? The Public and Government Information Stockpiles. Link
- House unveils new warrantless surveillance bill. Link
- A bunch of internal Chinese government documents leaked on GitHub. Link
- Interesting Thread on a massive dump from a Chinese Ministry of Public Security (MPS) private industry contractor called iSoon (aka Anxun). Link
- Data From Chinese Security Services Company i-Soon Linked to Previous Chinese APT Campaigns. Link
- No real safeguards for new Europol data powers, says data protection authority. Link
- MEPs have given their final approval to a law on aligning the Customs Information System with data protection rules. Link
- Automated data exchange in Prüm II: The EU's securitisation mindset keeps encroaching on our fundamental rights. Link
- Do AI systems have politics? Predictive optimisation as a move away from the rule of law, liberalism and democracy. Link
- In conversation: Bruce Schneier on AI-powered mass spying. Link
- When Eyes in the Sky Start Looking Right at You. Link
- Welcome To Chula Vista, Where Police Drones Respond To 911 Calls. Link
- Wie die EU von Geodaten profitieren kann. Link

- Judge allows case against geolocation data broker Kochava to proceed. Link
- San Francisco Police's Live Surveillance Yields Almost 200 Hours of Spying-Including of Music Festivals. Link
- London Underground Is Testing Real-Time AI Surveillance Tools to Spot Crime. Link
- Met Police to scrap and replace 'racist' Gangs Violence Matrix. Link
- Here Are the Secret Locations of ShotSpotter Gunfire Sensors. Link
- Temporary ePrivacy derogation: Companies like Facebook must never indiscriminately scan people's private messages. Link
- EFF Helps News Organizations Push Back Against Legal Bullying from Cyber Mercenary Group. Link
- Phone Spy Tool Pitched for 'Riot Detection' in NYC. Link
- Spyware leak offers 'first-of-its-kind' look inside Chinese government hacking efforts. Link
- New spyware attacks exposed: civil society targeted in Jordan. Link
- Brussels spyware crisis expands: Two MEPs hit in phone-hacking security breach. Link
- Government agrees law to protect confidential journalistic material from state hacking. Link
- Court of Appeal strikes out Saudi Government case in Pegasus spyware claim brought by UK based dissident Ghanem Al-Masarir. Link
- Announcement of a Visa Restriction Policy to Promote Accountability for the Misuse of Commercial Spyware. Link
- Government hackers targeted iPhone owners with zero-days, Google says. Link
- Meta details actions against eight spyware firms. Link

- Israeli government absent from London spyware conference and pledge. Link
- Global Coalition and Tech Giants Unite Against Commercial Spyware Abuse. Link
- How the makers of Predator spyware hid behind a Czech Nanny. Link
- Meta e Google hanno messo nel mirino gli spyware made in Italy. Link
- Poland launches Pegasus spyware probe. Link
- US to restrict visas for those who misuse commercial spyware. Link
- Pegasus - The enemy reads along. Documentary. Link
- Buying Spying: How the commercial surveillance industry works and what can be done about it. Link
- Understanding private surveillance providers and technologies. Link
- The 'cynical space' where aid, tech, and militaries intersect. Link
- Biden executive order seeks to cut China off from Americans' sensitive data. Link
- Dictators Used Sandvine Tech to Censor the Internet. The US Finally Did Something About It. Link
- ORG submits complaints about intrusive liveramp adtech system. Link
- Privacy International. EdTech: Surveillance Tracker. Link
- Why law enforcement should prioritise enhancing existing biometric modalities over exploring new ones: A necessity under the EU AI Act. Link
- Police real-time remote biometric ID in the AI Act. Link

- Global: Amnesty International publishes an introduction to defending the rights of refugees and migrants in the digital age. Link
- Biometric Data, Data Protection Authorities, and Migrants: A Complex Nexus. Link
- 'A privacy nightmare': the $400m surveillance package inside the US immigration bill. Link
- UK to replace physical biometric immigration cards with e-visas. Link
- Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework. Link
- Amazon defends facial-recognition tech sale to FBI despite moratorium. Link
- Gardaí to spend estimated €2.1 million on trial run of body worn cameras in four locations. Link
- A Vending Machine Error Revealed Secret Face Recognition Tech. Link
- Facial recognition service says it is for suspicious lovers, not stalking. Link
- Police Turn to AI to Review Bodycam Footage. Link
- Bodycam Maker Axon Is on a Mission to Surveil America with AI. Link
- The thorny push to put body cameras on hospital and retail workers. Link
- Wyze says camera breach let 13,000 customers briefly see into other people's homes. Link
- Your AI Girlfriend Is a Data-Harvesting Horror Show. Link
- Tumblr and WordPress to Sell Users' Data to Train AI Tools. Link

- Google Update Shows How Bard AI May Work With Your Messages App. Link
- FTC to ban Avast from selling browsing data for advertising purposes. Link
- Palestine: 300 academics call for halt to EU research funding that violates international law. Link
- Italian Data Regulator Slams EU-Funded AI Projects. Link
- "Illegal to break encryption," the European Court of Human Rights rules. Link
- ECtHR: Judgment Škoberne v. Slovenia - systematic and indiscriminate retention of telecommunications data, amid proceedings against judge for bribery. Link
- ECtHR: Judgment Podchasov v. Russia - Legislation at issue providing extremely broad duty of retention and as such rendering the interference exceptionally wide-ranging and serious; Inadequate and insufficient safeguards against abuse relating to law-enforcement authorities' access to stored Internet communications and related communications data; Statutory obligation to decrypt end-to-end encrypted communications disproportionate. Link
- European Parliament just adopted the new rules on transparency and targeting of political advertising. Link

Cyber Security

- A year in the cybersecurity trenches with Mandiant Managed Defense. Link
- CrowdStrike 2024 Global Threat Report. Link
- Microsoft, Navigating cyberthreats and strengthening defenses in the era of AI. Link
- Threat Intelligence Report: GoldPickaxe Malware Family and GoldFactory Cybercrime Group. Link
- YouTuber breaks BitLocker encryption in less than a minute using $5 Raspberry Pi Pico. Link
- EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras. Link
- Apple's iMessage Is Getting Post-Quantum Encryption. Link
- Signal Finally Rolls Out Usernames, So You Can Keep Your Phone Number Private. Link
- The Picus Red Report: the Top 10 Most Prevalent MITRE ATT&CK Techniques - The Rise of Hunter-Killer Malware. Link
- Patterns and Targets for Ransomware Exploitation of Vulnerabilities: 2017-2023. Link
- Raspberry Robin malware evolves with early access to Windows exploits. Link
- Lazarus hackers exploited Windows zero-day to gain Kernel privileges. Link
- Exploiting Windows' vulnerabilities with Hyper-V: A Hacker's swiss army knife. Link
- Keylogging in the Windows kernel with undocumented data structures. Link

- CVE-2024-21412: Water Hydra Targets Traders With Microsoft Defender SmartScreen Zero-Day. Link
- Cross Window Forgery: A Web Attack Vector. Link
- A Catastrophe For Control: Understanding the ScreenConnect Authentication Bypass (CVE-2024-1709 & CVE-2024-1708). Link
- New Fortinet RCE bug is actively exploited, CISA confirms. Link
- SEO Poisoning to Domain Control: The Gootloader Saga Continues. Link
- SSD Advisory – TP-Link NCXXX Authentication Bypass. Link
- Static Analysis Automation for Hunting Vulnerable Kernel Drivers. Link
- Flatlined: analyzing pulse secure firmware and bypassing integrity checking. Link
- Pikabot Loader Detailed Analysis. Link
- Cybercriminals Weaponizing Open-Source SSH-Snake Tool for Network Attacks. Link
- Uncovering The IOCs: Ivanti Connect Secure VPN Exploitation. Link
- The Unknown Unknowns: Post-Exploitation Activities of Ivanti CS/PS Appliances. Link
- Cutting Edge, Part 3: Investigating Ivanti Connect Secure VPN Exploitation and Persistence Attempts. Link
- Automated local DNS cache poisoning using Android while charging via computer. Link
- VoltSchemer attacks use wireless chargers to inject voice commands, fry phones. Link
- Hello Lucee! Let us hack Apple again? Link
- New hack clones fingerprints just by listening to fingers swipe screens. Link

- iPhone Under Attack: U.S. Government Issues 21 Days To Comply Warning. Link
- Zero Click Account Takeover. Link
- Zero-Click Apple Shortcuts Vulnerability Allows Silent Data Theft. Link
- Dusting Off Old Fingerprints: NSO Group's Unknown MMS Hack. Link
- Banking Trojans Target Latin America and Europe Through Google Cloud Run. Link
- iOS Trojan Collects Face and Other Data for Bank Account Hacking. Link
- AI in the wrong hands: New iOS Trojan challenges face recognition. Link
- Exploring Encrypted Attacks Amidst the AI Revolution. Link
- Yes, Telegram Is A Very Serious Threat To Your Phone. Link
- Face Swap Injection Attacks Surged by 704% in H2 2023, AI-Based Verification Techs Are Essential: Report. Link
- MIVD reveals Chinese espionage methods in the Netherlands. Link
- How I Hacked the Dutch Government: Exploiting an Innocent Image for Remote Code Execution. Link
- New Zardoor backdoor used in long-term cyber espionage operation targeting an Islamic organization. Link
- TinyTurla Next Generation - Turla APT spies on Polish NGOs. Link
- Ex-Employee's Admin Credentials Used in US Gov Agency Hack. Link
- State-backed hackers are experimenting with OpenAI models. Link
- Microsoft: Nation-state hackers are exploiting ChatGPT. Link

- Microsoft Catches APTs Using ChatGPT for Vuln Research, Malware Scripting. Link
- Chinese Hackers Using Deepfakes in Advanced Mobile Banking Malware Attacks. Link
- Malicious AI models on Hugging Face backdoor users' machines. Link
- How are attackers using QR codes in phishing emails and lure documents? Link
- The near-term impact of AI on the cyber threat. Link
- Protecting Transnational Critical Information Infrastructure: Vitality, Vulnerability and Diplomacy. Link
- 'Safety by design' could prevent domestic abuse through smart devices. Link
- Post Office IT insider and the software decision that lit the Horizon scandal. Link
- What Companies & CISOs Should Know About Rising Legal Threats. Link
- MicroStrategy hack: Fake MSTR AirDrop costs users $440K. Link
- Canada Moves to Ban the Flipper Zero Over Car Hacking Fears. Link
- White House Targets Software Provider Accountability. Link
- What's New in the NIST Cybersecurity Framework 2.0. Link
- NSA Cybersecurity Year in Review 2023. Link
- Cyber Resilience 2024. Link
- Report on the cybersecurity and resiliency of the EU communications infrastructures and networks. Link
- Geopolitical Cyber Risk: Cyber Operations in Modern Warfare. Link