CCRS Bit

August 2023

CONTENTS

Cybercrime

- The Weird, Big-Money World of Cybercrime Writing Contests. Link
- How fame-seeking teenagers hacked some of the world’s biggest targets. Link
- Evolution of Cybercriminal Operations in 2023. Link
- MOVEit, the biggest hack of the year, by the numbers. Link
- Unmasking Trickbot, One of the World’s Top Cybercrime Gangs. Link
- ‘Five Eyes’ nations release technical details of Sandworm malware ‘Infamous Chisel’. Link
- Lazarus Group's infrastructure reuse leads to discovery of new malware. Link
- Researchers uncover new Lazarus group malware details. Link
- Lazarus Group exploits ManageEngine vulnerability to deploy QuiteRAT. Link
- New "Whiffy Recon" Malware Triangulates Infected Device Location via Wi-Fi Every Minute. Link
- Ransomware on the Move: Evolving Exploitation Techniques and the Active Pursuit of Zero-Days. Link
- Ransomware Wipes Out Data Access for 'Majority' of Cloud Provider's Customers. Link
- Monti Ransomware Returns with New Linux Variant and Enhanced Evasion Tactics. Link
- International ransomware gangs are evolving their techniques. The next generation of hackers will target weaknesses in cryptocurrencies. Link

- LogicMonitor customers hacked in reported ransomware attacks. Link
- Cybercriminals Increasingly Using EvilProxy Phishing Kit to Target Executives. Link
- Cyber Criminals Targeting Victims through Mobile Beta-Testing Applications. Link
- Hackers steal Signal, WhatsApp user data with fake Android chat app. Link
- Over 100K hacking forums accounts exposed by info-stealing malware. Link
- Rust-based Realst Infostealer Targeting Apple macOS Users' Cryptocurrency Wallets. Link
- New Downfall attacks on Intel CPUs steal encryption keys, data. Link
- Hackers exploit WinRAR zero-day bug to steal funds from broker accounts. Link
- Most DDoS attacks tied to gaming, business disputes, FBI and prosecutors say. Link
- A New Supply Chain Attack Hit Close to 100 Victims—and Clues Point to China. Link
- Classiscam fraud-as-a-service expands, now targets banks and 251 brands. Link
- FBI: Lazarus hackers readying to cash out $41 million in stolen crypto. Link
- Telekopye: Hunting Mammoths using Telegram bot. Link
- The CoinsPaid Hack Explained: We Know Exactly How Attackers Stole and Laundered $37M USD. Link
- Crypto investor data exposed by a sim swapping attack against a Kroll employee. Link

- Criminals Pose as Non-Fungible Token (NFT) Developers to Target Internet Users with an Interest in NFT Acquisition. Link
- Researcher Exposes Cryptocurrency Scam Network of 300 Domains. Link
- How crypto scammers are embracing new AI technology. Link
- Cybercriminals train AI chatbots for phishing, malware attacks. Link
- Deepfake Fraud Surges More Than 1,000 Percent, Insiders Say It's Just the Beginning. Link
- Warning: Humans cannot reliably detect speech deepfakes. Link
- Google and Universal Music negotiate deal over AI 'deepfakes'. Link
- 3 Cryptocurrency Firms Suffer Data Breach After Kroll SIM Swapping Attack. Link
- 10 Million Likely Impacted by Data Breach at French Unemployment Agency. Link
- Scraped data of 2.6 million Duolingo users released on hacking forum. Link
- Mom's Meals discloses data breach impacting 1.2 million people. Link
- 68k Phishing Victims are Now Searchable in Have I Been Pwned, Courtesy of CERT Poland. Link
- Data From The Qakbot Malware is Now Searchable in Have I Been Pwned, Courtesy of the FBI. Link
- Data breach at French govt agency exposes info of 10 million people. Link
- US govt contractor Serco discloses data breach after MoveIT attacks. Link

- LinkedIn accounts hacked in widespread hijacking campaign. Link
- Millions of Americans' health data stolen after MOVEit hackers targeted IBM. Link
- Hackers Threaten Patients Following a Massive Cyberattack on a Hospital. Link
- Colorado warns hackers stole 16 years of public school data in ransomware attack. Link
- Parsing the UK electoral register cyberattack. Link
- Leaked Secrets and Unlimited Miles: Hacking the Largest Airline and Hotel Rewards Platform. Link
- Paramount discloses data breach following security incident. Link
- In Airbnb, Cybercriminals Find a Comfortable Home for Fraud. Link
- Crooks Using Stealers and Stolen Cookies to Hack Airbnb Accounts. Link
- A Huge Scam Targeting Kids
  With Roblox and Fortnite 'Offers' Has Been Hiding in Plain Sight. Link
- New malware from North Korea's Lazarus used against healthcare industry. Link
- Exclusive: North Korean hackers breached top Russian missile maker. Link
- Russia-backed hackers used Microsoft Teams to breach government agencies. Link
- The Cheap Radio Hack That Disrupted Poland's Railway System. Link
- Cuba ransomware uses Veeam exploit against critical U.S. organizations. Link

- Japanese watchmaker Seiko breached by BlackCat ransomware gang. Link
- Major US Energy Company Hit by QR Code Phishing Campaign. Link
- Chinese hackers accused of using Barracuda bug against federal, local US agencies. Link
- Hacktivists fund their operations using common cybercrime tactics. Link
- Final negotiations on UN cybercrime treaty underway in New York. Link
- U.S. government board looks to curb teen enthusiasm for cybercrime. Link
- Europe’s Sweeping New Rules for Big Tech Are About to Kick In. Here’s What to Know. Link
- How a hacking crew overtook a satellite from inside a Las Vegas convention center and won $50,000. Link
- Critiquing the U.S. characterization, attribution and retaliation laws and policies for cyberattacks. Link

Digital Investigation and Digital Evidence

- How the FBI goes after DDoS cyberattackers. Link
- Burner phones. Pizza crust. DNA on burlap. A New York architect was charged with killing 3 women in Gilgo Beach serial killings cold case. Link
- NATO probes hacktivist crew's boasts of stolen portal data. Link
- US government to investigate China's Microsoft email breach. Link
- Interpol takes down 16shop phishing-as-a-service platform. Link
- Cybercrime: 14 arrests, thousands of illicit cyber networks disrupted in Africa operation. Link
- Operation Narsil disrupts network of child abuse websites designed to generate profits from advertising. Link
- Notorious phishing platform shut down, arrests in international police operation. Link
- Alleged cybercrime hub raided in Pasay; around 650 held including foreigners. Link
- Closing ranks on West African organized crime: more than EUR 2 million seized in Operation Jackal. Link
- FBI Identifies Cryptocurrency Funds Stolen by DPRK. Link
- FBI, Partners Dismantle Qakbot Infrastructure in Multinational Cyber Takedown. Link
- US and Poland shut down Lolek Hosted bulletproof hosting platform. Link

- LOLEKHosted admin arrested for aiding Netwalker ransomware gang. Link
- Hong Kong police arrest 6 men in connection with crackdown on HK$175 million fraud syndicate. Link
- 10 persons arrested for their suspected involvement in banking-related malware scam cases. Link
- Two Men Arrested Following Poland Railway Hacking. Link
- Chinese National Arrested in Sydney for Involvement in $100M Crypto Scam. Link
- Five foreign nationals charged with defrauding Australians. Link
- Tornado Cash Founders Charged With Money Laundering And Sanctions Violations. Link
- Bitfinex Hacker and Wife Plead Guilty to Money Laundering Conspiracy Involving Billions in Cryptocurrency. Link
- International Cyber Fraudster Sentenced to More Than 8 Years in Federal Prison. Link
- Lapsus$: Court finds teenagers carried out hacking spree. Link
- Pennsylvania Resident Sentenced To Three Years In Prison For Role In Conspiracy To Defraud And Extort Cryptocurrency Executives. Link
- Basics of Cryptocurrency Investigations. Link
- A new and simplified way to request nonpublic gTLD Registration Data. Link
- Group-IB supports international police operation targeting 16shop, a popular phishing-as-a-service platform. Link
- ADF Supports International Justice Mission in the Fight against Human Trafficking. Link
- Binance says intel shared with authorities led to capture of senior ISIS members in Asia. Link

- Operation Venetic: Corrupt police worker admits tipping-off criminal over secret nationwide investigation. Link
- Accuracy of cell phone location data debated in murder case. Link
- Digitalize it: digital evidence at the ICC. Link

Digital Forensics

- Best Practices in Mobile Forensics: Separating Extraction and Analysis. Link
- The Transformative Impact of Digital Forensics on Cybersecurity. Link
  Bypassing Bitlocker using a cheap logic analyzer on a Lenovo laptop. Link
- How To Scan A Mobile Device With Mobile Device Investigator. Link
- EDRaser: powerful tool for remotely deleting access logs, Windows event logs, databases. Link
- Breaking into iOS 16.5: Extracting the File System and Keychain. Link
- Hope for the Best, Prepare for the Worst: How to prepare for cloud DFIR. Link
- OSINT Data to Support Subpoenaing Internet Service Providers. Link
- Android & AirTags (Part II). Link
- Viewing CCTV after Acquisition. Link
- The Role of AI in Digital Forensics and Cybersecurity. Link
- 6 Ways AI Can Revolutionize Digital Forensics. Link
- Seven Use Cases Where AI can be a Hero to Digital Forensics. Link
- Forensic analysts can be wrong about the USB Drives attached to a computer in evidence. Link
- Phishing the anti-phishers: Exploiting anti-phishing tools for internal access. Link

- Clop ransomware now uses torrents to leak data and evade takedowns. Link
- Thousands of Android Malware Apps Using Stealthy APK Compression to Evade Detection. Link
- Cyber Criminals Exploiting Google Drive, OneDrive to Hide Malicious Traffic. Link
- Velociraptor: Open-source digital forensics and incident response. Link
- Cartographer: a Ghidra plugin for mapping out code coverage data. Link
- Wireshark 4.0.8 Release: What's New! Link
- XRY 10.6.1 Release: support for iOS 17 beta, wider device range, and multiple app enhancements. Link
- Oxygen Corporate Explorer Introduces Remote Device Collector. Link
- Digital Evidence Investigator PRO (DEI PRO) From ADF Solutions. Link
- MOBILedit Forensic version 9.2 with brand-new powerful Samsung Security Bypassing. Link
- Maltego Version 4.5.0. Link
- Magnet Forensics Acquires Griffeye, A Leading Digital Media Forensics Software Firm. Link
- Magnet Forensics Partners With Jamf To Simplify Digital Investigations Of Apple Endpoints. Link
- Cellebrite Enhances Evidence & Workflow Management Tech for Digital Forensics and Investigative Units with New Capabilities. Link
- Katalysen Ventures announces deal with fast-growing digital forensics company VALEGA Chain Analytics. Link
- Cado Security accelerates APAC presence with new channel partner. Link

- Digital Forensics Market 2023 Growth Drivers and Future Outlook. Link
- Tackling Cybercrime with Digital Forensic Laboratory as a Service: A New Era in Telecommunications. Link
- Gandhinagar University Inaugurates State's 1st AI Blockchain-Driven Cyber Security And Digital Forensics Lab. Link
- The Free On-Demand Course "iOS Forensics with Belkasoft" Starts September 15th. Link
- DFSP # 391 – Investigation Lifecycle. Link

Digital Surveillance vs. Privacy

- Researchers watched 100 hours of hackers hacking honeypot computers. Link
- Hackers Are Selling Hacked Police Emails to Try to Grab Personal Data From TikTok, Facebook. Link
- UN cybercrime treaty risks becoming a 'global surveillance pact'. Link
- NSA orders employees to spy on the world "with dignity and respect". Link
- The Secret Weapon Hackers Can Use to Dox Nearly Anyone in America for $15. Link
- EXCLUSIVE: Hacking tool Flipper Zero tracked by intelligence agencies, which fear white nationalists may deploy it against power grid. Link
- UK MPs warn against growing use of smart tech in domestic abuse. Link
- The A.I. Surveillance Tool DHS Uses to Detect 'Sentiment and Emotion'. Link
- This AI Watches Millions Of Cars Daily And Tells Cops If You're Driving Like A Criminal. Link
- Worldcoin's Targeting of Developing Countries in Biometric Data Collection Raises Privacy Concerns. Link
- How EU's plan to digitising travel documents might affect you. Link
- Changes to UK Surveillance Regime May Violate International Law. Link
- UK data bill favours big business and 'shady' tech firms, rights group claims. Link

- Government targeting UK minorities with social media ads despite Facebook ban. Link
- China's Draft Rules Would Force User Consent for Facial Recognition Technology, With Expected Government Exceptions. Link
- Afghanistan: Installing thousands of cameras risks creating total surveillance state. Link
- Why LinkedIn is a snooper's paradise. Link
- Cellebrite asks cops to keep its phone hacking tech 'hush hush'. Link
- The Scourge of Commercial Spyware—and How to Stop It. Link
- Spyware maker LetMeSpy shuts down after hacker deletes server data. Link
- A Brazilian phone spyware was hacked and victims' devices 'deleted' from server. Link
- Zoom might use your calls and data to train AI. Link
- Zoom CEO admits mistake as terms-of-service changes raise AI fears. Link
- YouTube Ads May Have Led to Online Tracking of Children, Research Says. Link
- X wants permission to start collecting your biometric data and employment history. Link
- Popular open source project Moq criticized for quietly collecting data. Link
- The New York Times prohibits using its content to train AI models. Link
- Meta refreshes promise to roll out default end-to-end encryption in Messenger this year. Link
- The Internet Is Turning Into a Data Black Box. An 'Inspectability API' Could Crack It Open. Link

- The New York subway’s ride tracker has a scary security loophole. Link
- I Tracked an NYC Subway Rider's Movements with an MTA ‘Feature’. Link
- FBI Seizure of Mastodon Server Data is a Wakeup Call to Fediverse Users and Hosts to Protect their Users. Link
- PSNI data breach: 'Family fears for my safety as a police officer'. Link
- Possible Multi-Billion Dollar Lawsuit Aimed at Google’s “Incognito Mode” Ruled a Triable Issue Due to Consumer Privacy Concerns. Link
- Google 'wiretapped' tax websites with visitor traffic trackers, lawsuit claims. Link
- Norway to fine Meta nearly $100,000 a day over data use. Link
- Victory! Ninth Circuit Allows Human Rights Case to Move Forward Against Cisco Systems. Link
- Law Firm Must Name Clients Affected by 2020 Cyberattack, Judge Says. Link
- Tesla says data breach impacting 75,000 employees was an insider job. Link
- Leaseweb is restoring ‘critical’ systems after security breach. Link
- US tech firms offer data protections for Europeans to comply with EU big tech rules. Link
- Danish cloud host says customers ‘lost all data’ after ransomware attack. Link
- Discord starts notifying users affected by March data breach. Link
- Ad firm plans to use people’s data in a maneuver to sink data privacy bill. Link

- Information Commissioner's Office and The Alan Turing Institute published Guidance on AI to assist in explaining AI decisions and their consequences. Link
- ICO Guidance on biometric data. Link
- Crackdowns on Encrypted Messaging Don’t ‘Help the Children’. Link

Cyber Security

- The FBI and domestic and international partners released a joint Cybersecurity Advisory (CSA) listing the most frequently exploited vulnerabilities by malicious cyber actors in 2022. Link
- Hackers Compromised ChatGPT Model with Indirect Prompt Injection. Link
- ChatGPT Security Concerns: Credentials on the Dark Web and More. Link
- Researchers Uncovered a New Flaw in ChatGPT to Turn Them Evil. Link
- VMware Aria vulnerable to critical SSH authentication bypass flaw. Link
- 16 Zero-Day Vulnerabilities Discovered in CODESYS Affect Millions of Industrial Devices. Link
- Hackers Launch MiTM Attack to Bypass VMware Tools SAML Authentication. Link
- Critical MikroTik RouterOS Vulnerability Exposes Over Half a Million Devices to Hacking. Link
- New BitForge cryptocurrency wallet flaws lets hackers steal crypto. Link
- How API authentication vulnerabilities are at the center of cloud security concerns. Link
- Ivanti warns customers another zero-day is under active attack. Link
- AVID: AI Vulnerability Database - an open-source, extensible knowledge base of AI failures. Link

- Hackers use VPN provider's code certificate to sign malware. Link
- Hackers Can Exploit Skype Vulnerability to Find User IP Address. Link
- Akira ransomware targets Cisco VPNs to breach organizations. Link
- Hackers can abuse Microsoft Office executables to download malware. Link
- EvilProxy phishing campaign targets 120,000 Microsoft 365 users. Link
- Microsoft signing keys keep getting hijacked, to the delight of Chinese threat actors. Link
- Hackers use public ManageEngine exploit to breach internet org. Link
- DarkGate Loader Delivered Through Stolen Email Threads to Lure Victims. Link
- Hackers use open source Merlin post-exploitation toolkit in attacks. Link
- CISA says hackers are exploiting a new file transfer bug in Citrix ShareFile. Link
- MalDoc in PDFs: Hiding malicious Word docs in PDF files. Link
- Lockbit 3.0 Builder Leaked: Anyone Can Blend Ransomware. Link
- Knight ransomware distributed in fake Tripadvisor complaint emails. Link
- TP-Link smart bulbs can let hackers steal your WiFi password. Link
- Hackers increasingly abuse Cloudflare Tunnels for stealthy connections. Link

- New stealthy techniques let hackers gain Windows SYSTEM privileges. Link
- XLoader Malware Variant Targets MacOS Disguised as OfficeNote App. Link
- China-Linked BadBazaar Android Spyware Targeting Signal and Telegram Users. Link
- A Fake Signal App Was Planted On Google Play By China-Linked Hackers. Link
- Russian Hackers Employ Telekopye Toolkit in Broad Phishing Attacks. Link
- About 2000 Citrix NetScalers Were Compromised in Massive Attack Campaigns. Link
- Malicious Campaigns Exploit Weak Kubernetes Clusters for Crypto Mining. Link
- LinkedIn accounts hacked in widespread hijacking campaign. Link
- Spoofing an Apple device and tricking users into sharing sensitive data. Link
- Hackers Deliver Magniber Ransomware Disguised as Windows Security Update. Link
- New 'Deep Learning Attack' Deciphers Laptop Keystrokes with 95% Accuracy. Link
- No More Speculation: Exploiting CPU Side-Channels for Real. Link
- A Practical Deep Learning-Based Acoustic Side Channel Attack on Keyboards. Link
- New acoustic attack steals data from keystrokes with 95% accuracy. Link
- Lazarus Group Launches First Open Source Supply Chain Attacks Targeting Crypto Sector. Link
- Backdoor in Barracuda Email Security Gateway Attacks. Link

- QwixxRAT: New Remote Access Trojan Emerges via Telegram and Discord. Link
- Massive 400,000 proxy botnet built with stealthy malware infections. Link
- AI Incident Database. Link
- IBM launches open-source detection and response framework for MFT attacks. Link
- The MOVEit mass hacks hold a valuable lesson for the software industry. Link
- Generative AI and Cybersecurity: Bright Future or Business Battleground? Link
- Google Introduces Chrome Quantum Attack Protection. Link
- Apple issues third mobile OS update after zero-click spyware campaign. Link
- Hacking group plans system to encrypt social media and other apps. Link
- ImmuniWeb releases Mobile Neuron to scan for OWASP Mobile Top 10 vulnerabilities, iOS/Android weaknesses. Link
- Trulioo enhances identity verification with “person match” intelligent routing. Link
- DARPA launches two-year competition to build AI-powered cyber defenses. Link
- How international cybersecurity frameworks can help CISOs. Link
- NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers. Link
- The U.S. Is Falling Behind on Encryption Standards – And That’s a Global Problem. Link
- ATHI — An AI Threat Modeling Framework for Policymakers. Link

- Cybersecurity: How Can Companies Benefit From FBI and Homeland Security Collaboration? Link
- BSides Las Vegas roundup: Passwordless misconfigurations and hidden app vulnerabilities. Link
- Black Hat USA 2023 slides. Link
- Guarding The Digital Frontier. AI As A Cyber Weapon. Link