CCRS Bit

September 2023

CONTENTS

Cybercrime

- The Initial Access Broker Economy: A Deep Dive into Dark Web Hacking Forums. Link
- The evolution of command-and-control servers. Link
- What Is Anonymous Sudan About? The Mysterious Group Behind Latest X Outage. Link
- Uncovering DDGroup — A long-time threat actor. Link
- From ScreenConnect to Hive Ransomware in 61 hours. Link
- Unveiling the shadows: the dark alliance between Guloader and Remcos. Link
- Russia-Linked LockBit Gang Attacks an MSP and Two Manufacturers Using the Targets' RMM Tools to Infect Downstream Customers and Employees with Ransomware. Link
- Evolution of USB-Borne Malware, Raspberry Robin. Link
- Mirai variant infects low-cost Android TV boxes for DDoS attacks. Link
- BadBazaar espionage tool targets Android users via trojanized Signal and Telegram apps. Link
- It's a Zero-day? It's Malware? No! It's Username and Password. Link
- Hacker Group Disguised as Marketing Company to Attack Enterprise Targets. Link
- GDPR used by new ransom gang to extort victims. Link
- Inside Akira Ransomware Negotiations. Link
- A Victim of the Akira Ransomware. Link
- MSSQL Databases Under Fire From FreeWorld Ransomware. Link

- The Ransomware Group That Went Too Far. Darknet Diaries episode. Link
- Sekoia.io mid-2023 Ransomware Threat Landscape. Link
- NCSC: Why Cyber Extortion Attacks No Longer Require Ransomware. Link
- Ransomware, extortion and the cyber crime ecosystem. Link
- BadBazaar espionage tool targets Android users via trojanized Signal and Telegram apps. Link
- Dymocks warns customers of data breach after account information leaked on dark web. Link
- Experts link LastPass security breach to a string of crypto heists. Link
- 38TB of data accidentally exposed by Microsoft AI researchers. Link
- Darkbeam leaks billions of email and password combinations. Link
- FBI Identifies Lazarus Group Cyber Actors as Responsible for Theft of $41 Million from Stake.com. Link
- Thousands of dollars stolen from Texas ATMs using Raspberry Pi. Link
- “We don’t ask questions”: Hawala payment system vulnerable to use by organized crime groups, including opiate traffickers and migrant smugglers. Link
- Swedish criminal gangs using fake Spotify streams to launder money. Link
- Hook: New Android Banking Trojan That Expands on ERMAC's Legacy. Link
- Classiscam fraud-as-a-service expands, now targets banks and 251 brands. Link
- Crypto crime displacement: what it is and what you can do about it. Link

- Crypto crimes — ‘Sorry, there’s nothing we can do’ … might not be true. Link
- Can a Vitalik-backed privacy idea stop cyber criminals? One Tornado Cash dev says he’ll test it out. Link
- FBI confirms that North Korea was behind $41 million Stake.com exploit. Link
- Phishing Attack on Cloud Provider With Fortune 500 Clients Led to $15M Crypto Theft From Fortress Trust. Link
- Crypto Whale Suffers $24 Million Loss In Phishing Attack. Link
- FTX Customers Hit by 'Withdrawal' Phishing Mails After SIM Swap Attack. Link
- MetaMask scammers take over government websites to target crypto investors. Link
- Cybercriminals Weaponizing Legitimate Advanced Installer Tool in Crypto-Mining Attacks. Link
- North Korea's Lazarus Group Suspected in $31 Million CoinEx Heist. Link
- How the Lazarus Group is stepping up crypto hacks and changing its tactics. Link
- Asian crime gangs force hundreds of thousands to perpetrate crypto romance scams. Link
- She lost $80,000 in a crypto romance scam. Now she’s fighting back. Link
- ‘Pig butchering’ crypto scams and those who fight back. Link
- The Next Wave of Scams Will Be Deepfake Video Calls From Your Boss. Link
- Gen Z falls for online scams more than their boomer grandparents do. Link

- Deepfake Imposter Scams Are Driving a New Wave of Fraud. Link
- Voice Deepfakes Are Coming for Your Bank Balance. Link
- NSA, U.S. Federal Agencies Advise on Deepfake Threats. Link
- Site for Generating Non-Consensual AI Porn Restricts Content Following 404 Media Investigation. Link
- Spanish teens received deepfake AI nudes of themselves: But is it a crime? Link
- The Transportation sector cyber threat overview. Link
- Unraveling Scattered Spider: A Stealthy and Persistent Threat Actor Targeting Telecom Networks. Link
- Mysterious 'Sandman' Threat Actor Targets Telecom Providers Across Three Continents. Link
- Hackers backdoor telecom providers with new HTTPSnoop malware. Link
- Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies. Link
- Quishing on the rise: How to prevent QR code phishing. Link
- The Comedy of Errors That Let China-Backed Hackers Steal Microsoft’s Signing Key. Link
- Chinese Spies Infected Dozens of Networks With Thumb Drive Malware. Link
- Earth Lusca's New SprySOCKS Linux Backdoor Targets Government Entities. Link
- Google: State hackers attack security researchers with new zero-day. Link
- New Report Uncovers 3 Distinct Clusters of China-Nexus Attacks on Southeast Asian Government. Link
- North Korean Hackers Deploy New Malicious Python Packages in PyPI Repository. Link

- Microsoft: North Korean hackers target Russian govt, defense orgs. Link
- Russia linked hackers hit UK Ministry of Defence as security secrets leaked. Link
- On the frontlines: Decoding Chinese threat actor tactics and techniques. Link
- Iranian hackers breach US aviation org via ManageEngine, Fortinet bugs. Link
- Iranian hackers backdoor 34 orgs with new Sponsor malware. Link
- Iran's Charming Kitten Pounces on Israeli Exchange Servers. Link
- US govt email servers hacked in Barracuda zero-day attacks. Link
- Hong Kong tech hub Cyberport alerts police, privacy watchdog after reports of ransomware attack exposing 400GB of data. Link
- 3 out of 4 cyber attacks in education sector associated with compromised on-premises user or admin account: Report. Link
- Record number of cyberattacks targeting critical IT infrastructure reported to UK gov't this year. Link
- Cybercrime to cost Germany 206 billion euros in 2023, survey finds. Link
- War crimes tribunal ICC says it has been hacked. Link
- One of the FBI's most wanted hackers is trolling the U.S. government. Link

Digital Investigation and Digital Evidence

- Intel agencies just 'scratching the surface' on open source initiatives. Link
- Army to treat OSINT as 'intelligence discipline of first resort' under new strategy. Link
- US and UK Mount Aggressive Crackdown on Trickbot and Conti Ransomware Gangs. Link
- Agile approach to mass cloud credential harvesting and crypto mining sprints ahead. Link
- FBI Identifies Cryptocurrency Funds Stolen by DPRK. Link
- The head of the snake: Israel police bust international crypto fraud ring. Link
- Assets seized in Singapore's money laundering case swell to S$2.4 bln. Link
- US and UK sanction 11 TrickBot and Conti cybercrime gang members. Link
- UK sanctions members of Russian cybercrime gang. Link
- Razzlekhan and husband guilty of $4.5bn Bitcoin launder. Link
- Russian Hacker Sentenced to Nine Years in U.S. Prison. Link
- Russian Malware Developer Pleads Guilty To Conspiracy To Commit Wire And Computer Fraud. Link
- Former Investment Banker and Registered Broker Pleads Guilty to Cryptocurrency Investment Fraud Scheme. Link
- Co-Founder Of Multibillion-Dollar Cryptocurrency Scheme "OneCoin" Sentenced To 20 Years In Prison. Link

- Computer System Administrator and Spouse Plead Guilty in Massive Scheme to Sell Pirated Business Telephone System Software Licenses. Link
- Thodex cryptocurrency boss jailed for 11,196 years in Turkey for fraud. Link
- Experts split on creation of industry-specific rules on illegal online content. Link
- EU lawmakers must regulate the harmful use of tech by law enforcement in the AI Act. Link
- Police AI needs strict limits and controls, warn civil society organisations. Link
- The International Criminal Court Will Now Prosecute Cyberwar Crimes. Link
- How Spamhaus will protect the internet from AI-driven spam and phishing. Link
- Underground Economy Conference 2023 – Commitment to solve global cybercrime challenges needs ongoing collaboration and technical innovation. Link
- Key takeaways from the sixth UN session on cybercrime treaty negotiations. Link
- EU a 'toxic warehouse' of child sexual abuse, as lawmakers urged to 'get a grip' on spiralling problem. Link
- Prosecutors in all 50 states urge Congress to strengthen tools to fight AI child sexual abuse images. Link
- CIA Builds Its Own Artificial Intelligence Tool in Rivalry With China. Link
- U.S. Counterintel Buys Access to the Backbone of the Internet to Hunt Foreign Hackers. Link
- Canadian tech company allegedly implicated in foreign spying received millions from Ontario government. Link

Digital Forensics

- New IDC Report: The State Of Digital Forensics And Incident Response 2023. Link
- The Art of Detection: Digital Forensics and Intellectual Property Theft. Link
- Improving internal investigation through better use and trust-based exchange of forensic information. Link
- Android Now Harder To Crack Than IPhones: Forensics Detectives. Link
- Remote collection of Windows Forensic Artifacts using KAPE and Microsoft Defender for Endpoint. Link
  EDRaser - Tool For Remotely Deleting Access Logs, Windows Event Logs, Databases, And Other Files. Link
- Microsoft Edge Forensics: Screenshot History. Link
- How To Review Mobile Forensics Evidence With Mobile Device Investigator. Link
- Data Validation in Vehicle Systems Forensics. Link
- GrayKey Supports iOS 16.6. Link
- Oxygen Forensic® Detective v.16.0 Introduces Decryption Of VeraCrypt Containers. Link
- Spoof iOS devices with Bluetooth pairing messages using Android. Link
- How to Extract Text From Images With Snipping Tool. Link
- How FBI hackers or Forensics Team identify fake Images. Link
- MD-LIVE 'Chat Scanner'. Link
- Zero to Sherlock: The Ultimate OSINT Adventure. Link

- When you need search by nickname in public IP addresses search engines (Shodan, Netlas, Fofa etc). Link
- Using AI for extracting Usernames, Emails, Phone Numbers, and Personal Names from large datasets. Link
- Analyzing Telegram chats and channels. Regular expressions in OSINT in practice. Link
- The latest version of Nmap, version 7.94, has been released. Link
- OSINT-Practitioners. A list of OSINT Practitioners and learn about OSINT, it includes numerous, blogs and tutorials. Link
- PyPhisher - Easy to use phishing tool with 65 website templates. Link
- Awesome Malware Analysis. A curated list of awesome malware analysis tools and resources. Link
- varc: collects a snapshot of volatile data from a system. Link
- sensity-ai/dot. The Deepfake Offensive Toolkit. Link
- e1abrador/web.Monitor: Fast & user-friendly web change tracking tool. Link
- D4RK-R4BB1T. Archives of the criminal side of the internet. Link
- CyberDefenders New Lab: #REvil. Link
- Executed Anti-Forensic Lab Using Steganography, E-Mail Forensic, and Exif Metadata techniques. Link
- Talks from the @sansforensics @DFIRSummit 2023 in Austin now available. Link

Digital Surveillance vs. Privacy

- Interpol: multi-million dollar "predictive analytics" system under construction. Link
- Human rights groups win European Court of Human Rights claim on UK mass surveillance regime. Link
- Intelligence community to meet with civil liberties groups on controversial surveillance tool. Link
- Customs and Border Protection Says It Will Stop Buying Smartphone Location Data. Link
- Apple and Google Are Introducing New Ways to Defeat Cell Site Simulators, But Is it Enough? Link
- Glukhin and the EU regulation of facial recognition: Lessons to be learned? Link
- Revealed: Home Office secretly lobbied for facial recognition 'spy' company. Link
- What is the live facial recognition the Met is using in London? Link
- Met police data platform deployed with data protection issues. Link
- Wrongly arrested because of facial recognition: Why new police tech risks serious miscarriages of justice. Link
- Czech Police's Facial Recognition Software under scrutiny. Link
- The Twisted Eye in the Sky Over Buenos Aires. Link
- Online child safety law blocked after Calif. argued face scans not that invasive. Link
- EU: Court denies full transparency about emotion recognition. Link

- Op-Ed: “Frontex above the law – a missed opportunity for a landmark judgment on Frontex’s responsibility with regards fundamental rights violations: WS and Others v Frontex (T-600/21)” by Sarah Tas. Link
- Opinion: Here’s how automatic license plate readers make us less safe and expose our personal data. Link
- This AI Watches Millions Of Cars Daily And Tells Cops If You’re Driving Like A Criminal. Link
- New York police will use drones to monitor backyard parties this weekend, spurring privacy concerns. Link
- Why consumer drones represent a special cybersecurity risk. Link
- Is this the most criticised draft EU law of all time? Link
- Europol Sought Unlimited Data Access in Online Child Sexual Abuse Regulation. Link
- Inside Apple’s Impossible War On Child Exploitation. Link
- UK pulls back from clash with Big Tech over private messaging. Link
- Today The UK Parliament Undermined The Privacy, Security, And Freedom Of All Internet Users. Link
- Apple cites privacy concerns to refuse detection of child sexual abuse material. Link
- UK dials up fight with Meta over encryption. Link
- The Protecting Kids on Social Media Act is A Terrible Alternative to KOSA. Link
- U.S. Spying Law Threatens Privacy, Needs Restrictions, Watchdog Says. Link
- Council of Europe report calls use of Pegasus spyware by several countries potentially illegal. Link
- Communications with NSO Group re: Export Controls and Human Rights Initiative. Link

- Revealed: Israeli Cyber Firms Have Developed an 'Insane' New Spyware Tool. No Defense Exists. Link
- Probe reveals previously secret Israeli spyware that infects targets via ads. Link
- U.S. Org Worker Infected With New Pegasus Vector; Apple Releases Security Patch. Link
- Hacking Meduza: Pegasus spyware used to target Putin's critic. Link
- Polish Senate investigation recommends potential criminal charges for politicians implicated in Pegasus scandal. Link
- Polish Senate says use of government spyware is illegal in the country. Link
- Israel investigates potential breach of lawmakers' phones. Link
- Predator in the wires. Link
- Predator. Darknet Diaries episode. Link
- Inside ShadowDragon, The Tool That Lets ICE Monitor Pregnancy Tracking Sites and Fortnite Players. Link
- The Maker of ShotSpotter Is Buying the World's Most Infamous Predictive Policing Tech. Link
- Nowhere to hide: Data harvesters came for your privacy – and found it. Link
- X wants permission to start collecting your biometric data and employment history. Link
- Facebook Trains Its AI on Your Data. Opting Out May Be Futile. Link
- Microsoft admits to massive data leak two years after the event. Link
- TikTok Fined €345m For Children's Data Breaches. Link
- It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy. Link

- Carmakers are failing the privacy test. Owners have little or no control over data collected. Link
- The smart device brands harvesting your data. Link
- Your Wyze webcam might have let other owners peek into your house. Link
- Amazon brings generative AI to Alexa. Link
- Call to shut down Bristol schools' use of app to 'monitor' pupils and families. Link
- Wi-fi signals may soon be used to watch you. Link
- The Man Amazon Erased. Link
- Metaverse poses serious privacy risks for users, report warns. Link
- Meta Platforms must face medical privacy class action. Link
- California Legislature Passes Bill Regulating Data Brokers. Link
- New EU-US data transfer deal also faces criticism in Germany. Link
- French lawmaker challenges transatlantic data deal before EU court. Link
- European Data Protection Supervisor (EDPS) publish audits of Europol. Link

Cyber Security

- CVE-2023-30908: HPE OneView Remote Authentication Bypass Vulnerability. Link
- CVE-2023-4863: Critical Chrome 0-day Bug Under Active Attacks. Link
- Nearly 12,000 Juniper Firewalls Found Vulnerable to Recently Disclosed RCE Vulnerability. Link
- NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild. Link
- Hardcoded secret at the heart of the Dell Compellent VMware vulnerability. Link
- Huobi Was Discovered Leaking Users' Private Keys. Link
- Flipper Zero can be used to launch iOS Bluetooth spam attacks. Link
- Google Looker Studio abused in cryptocurrency phishing attacks. Link
- #NoFilter - Abusing Windows Filtering Platform for Privilege Escalation. Link
- Cisco warns of VPN zero-day exploited by ransomware gangs. Link
- Cybercriminals Using PowerShell to Steal NTLMv2 Hashes from Compromised Windows. Link
- Analyzing a Modern In-the-wild Android Exploit. Link
- Deadglyph: New Advanced Backdoor with Distinctive Malware Tactics. Link
- Akira Ransomware Targeting VPNs without Multi-Factor Authentication. Link

- Telekopye: Hunting Mammoths using Telegram bot. Link
- Cybercriminals Combine Phishing and EV Certificates to Deliver Ransomware Payloads. Link
- Microsoft Teams phishing attack pushes DarkGate malware. Link
- Beware: MetaStealer Malware Targets Apple macOS in Recent Attacks. Link
- Millions Infected by Spyware Hidden in Fake Telegram Apps on Google Play. Link
- Monti Ransomware Returns with New Linux Variant and Enhanced Evasion Tactics. Link
- CISA Warning: Nation-State Hackers Exploit Fortinet and Zoho Vulnerabilities. Link
- NCSC Warns of Chatbot 'Prompt Injection' Attacks. Link
- New WiKI-Eve attack can steal numerical passwords over WiFi. Link
- Steal-It Campaign. Link
- ProxyNation: The dark nexus between proxy apps and malware. Link
- 'From Russia with a 71': Uncovering Gamaredon's fast flux infrastructure. New apex domains and ASN/IP diversity patterns discovered. Link
- Shining some light on the DarkGate loader. Link
- Stealthy Android Malware MMRat Carries Out Bank Fraud Via Fake App Stores. Link
- Technical Analysis of HijackLoader. Link
- Pegasus spyware and how it exploited a WebP vulnerability. Link
- Guarding against the unseen: investigating a stealthy Remcos malware attack on Colombian firms. Link
- Moveit bug's ripple effect still unfolding. Link

- Millions of files with potentially sensitive information exposed online, researchers say. Link
- Guardians of the data galaxy: Navigating the universe of data leaks. Link
- Unwanted Guests: Mitigating Remote Access Trojan Infection Risk. Link
- SEC cyber disclosure rules are taking effect: Here’s what to expect. Link
- How China Demands Tech Firms Reveal Hackable Flaws in Their Products. Link
- Sleight of hand: How China weaponizes software vulnerabilities. Link
- The proposal on security of EU information: transforming the “bubble” into a “fortress”? Link