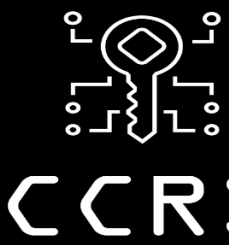

CCRS NEWSLETTER

May 2023

CONTENTS

CYBERCRIME

- Ransomware – Attacks on the Rise: Are We Prepared for the Next Wave of Cybercrime? Link
- LockBit 3.0 Ransomware Case Study: A Huge Cybersecurity Risk. Link
- Cybercrime gang FIN7 returned and was spotted delivering Clop ransomware. Link
- FBI confirms BianLian ransomware switch to extortion only attacks. Link
- Hacker group Anonymous Sudan demands $3 million from Scandinavian Airlines. Link
- Bl00dy Ransomware Gang Strikes Education Sector with Critical PaperCut Vulnerability. Link
- The Lemon Group cybercrime ring has reportedly pre-installed malware known as Guerilla on almost 9 million Android devices. Link
- N. Korean Lazarus Group Targets Microsoft IIS Servers to Deploy Espionage Malware. Link
- Hackers are breaking into AT&T email accounts to steal cryptocurrency. Link
- Hackers infect TP-Link router firmware to attack EU entities. Link
- Dark Pink hackers continue to target govt and military organizations. Link
- Physical and Cyber-Attacks on Energy Infrastructure Expected to Continue. Link
- Iranian hacking groups join Papercut attack spree. Link
- Eurovision 2023: a golden mine for cybercriminals. Link
- Victim conned out of $55K in romance scam on Plenty of Fish speaks out. Link
- QR codes used in fake parking tickets, surveys to steal your money. Link

- Crypto hacks down 70% in Q1 2023. TRM Insights. Link
- Malware disguised as ChatGPT apps are being used to lure victims, Meta says. Link
- When it comes to online scams, 'ChatGPT is the new crypto. Link
- Binance's chief security officer reveals terrifying deepfake AI threat to crypto users. Link
- BreachForums Shutdown: What Happens Now? Link
- New hacking forum leaks data of 478,000 RaidForums members. Link
- INTERPOL and UNICEF sign cooperation agreement to address child sexual exploitation and abuse. Link
- Irish and French parliamentarians sound the alarm about EU's CSA Regulation. Link
- Singapore Introduces New Law to Order Removal, Blocking of Harmful Online Content. Link
- The Underground History of Russia's Most Ingenious Hacker Group. Link
- Knowing how to hack will be vital in a cybercrime-filled future. Link
- Chinese Labs Are Selling Fentanyl Ingredients for Millions in Crypto. Link
- How Volexity Discovered the SolarWinds Hacking Campaign. Link
- How Gamers Eclipsed Spies as an Intelligence Threat. Link
- Redefining "Child Pornography". Link
- The call is coming from inside the internet: AI voice scams on the rise with cloning tech. Link
- How Professional Human Hackers Choose Their Targets. Link
- Ethical hacker scams 60 Minutes staffer to show how easy digital theft is. Link
- Cryptocurrency investment scam victim video interview. Link
- Fancy Bear Goes Phishing: The Dark History of the Information Age, In Five Extraordinary Hacks. Book by Scott J. Shapiro. Link

- Knowledge graphs and the advantage of crowd knowledge in criminal investigations. Link
- Law enforcement crackdowns and new techniques are forcing cybercriminals to pivot. Link
- Cops Just Revealed a Record-Breaking Dark Web Dragnet. Link
- The intelligence cycle incorporating the UK national intelligence model. Link
- Ransomware watchers are finding creative ways to track attacks. Link
- Inside the iSpoof Blockchain Investigation: This Fraud Tool Helped Scammers Steal Over £100 Million. Link
- Chainalysis CEO Says 'Thousands' Of Crypto Investigations Are Now Underway. Link
- Chinese Businesses Fueling the Fentanyl Epidemic Receive Tens of Millions in Crypto Payments. Link
- Crypto and the Opioid Crisis: What Blockchain Analysis Reveals About Global Fentanyl Sales. Link
- Binance helped US authorities freeze $4.4M linked to North Korean cybercrime orgs. Link
- Cybercriminal Network Fueling the Global Stolen Credit Card Trade is Dismantled. Link
- 300 arrested in global crackdown on dark web drug market. Link
- Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service. Link
- FBI seizes 9 crypto exchanges used to launder ransomware payments. Link
- FBI Disrupts Virtual Currency Exchanges Used to Facilitate Criminal Activity. Link

- How the FBI prevented $130 million in crypto ransomware attacks by hacking the hackers behind Hive. Link
- Knocking down Hive: How the FBI ran its own ransomware decryption operation. Link
- Israel Has Seized 190 Binance Accounts With Alleged Terrorist Ties Since 2021. Link
- First ChatGPT arrest in China over fake train crash news. Link
- Man Pleads Guilty to Conspiracy to Sell Stolen Financial Information on Dark Web. Link
- Tornado Cash developer's trial pushed to next year as 'worried' tech contributors seek clarity. Link
- EU Council advances on removal orders, reporting on anti-child abuse law. Link
- Crypto and the Opioid Crisis: What Blockchain Analysis Reveals About Global Fentanyl Sales. Link
- To Catch a Predator with Griffin Glynn. Cloak & Dagger podcast episode. Link

Digital Forensics

- High-tech toolkit to analyze digital evidence made more efficient and budget-friendly for law enforcement agencies. Link
- Kali Linux 2023.2 Release (Hyper-V & PipeWire). Link
- Belkasoft has released a FREE software tool to unlock a number of iOS device models. Link & Link
- Magnet #OUTRIDER is an ultra easy-to-use #triage tool designed to maximize the speed and simplicity of identifying actionable evidence in the field or lab—now with the ability to quickly scan #Android devices to uncover critical data (in beta)! Link
- Oxygen Forensic® Detective v.15.5 Introduces Support For Android Devices with UNISOC Chipsets. Link
- #Wireshark 4.0.6 released. Link
- Avilla Forensics - Open Source tool for Mobile Forensic. Link
- Unlock The Power Of GPU: Passware Kit Mobile 2023 v3 Decrypts 180+ New Mobile Devices. Link
- DetectDee tool. Hunt down social media accounts by username, email or phone across social networks. Link
- PentestGPT – A ChatGPT Powered Automated Penetration Testing Tool. Link
- DorkGPT tool. Describe what you want to find in human language and get a Google query using advanced search operators. Suitable for "juicy info" and vulnerable sites, as well as for any other search tasks. Link
- KernelCallbackTable tool. Could be abused to inject shellcode in a remote process. This method of process injection was used by FinFisher/FinSpy and Lazarus. Link
- Nexfil – OSINT Tool Finding Profiles By Username. Link
- Telegram OSINT VM Part 1. Link
- Telegram OSINT VM Part 2. Link

- Anti-Forensic Tools and packages that are used for countering forensic activities, including encryption, steganography, and anything that modify attributes. Link
- DarkBERT: A Language Model for the Dark Side of the Internet. Link
- Bellingcat OpenStreetMap search – a tool for locating photos and satellite images. Link
- Indicator-Intelligence Tool- finds related domains and IPv4 addresses to do threat intelligence after Indicator-Intelligence collects static files. Link
- Digital Forensics with Kali Linux: Enhance your investigation skills by performing network and memory forensics with Kali Linux 2022.x, 3rd Edition. Link
- Exploring the latest Dark Web onion sites -- showcasing Tor66, a spot to see new and freshly registered v3 onion addresses or search through different Tor hidden services. John Hammond video. Link

- The Prediction Society: Algorithms and the Problems of Forecasting the Future. Link
- Palantir Demos AI to Fight Wars But Says It Will Be Totally Ethical Don't Worry About It. Link
- Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict. Link
- New ICE Privacy Impact Assessment Shows All the Way the Agency Fails to Protect Immigrants' Privacy. Link
- Homeland Security Uses AI Tool to Analyze Social Media of U.S. Citizens and Refugees. Link
- New York State Passes Prohibition on Geofences Around Health Care Facilities. Link
- FTC Issues Warning on Use of Biometric Information. Link
- Computer system used to hunt fugitives is still down 10 weeks after hack. Link
- Paperbug Attack: New Politically-Motivated Surveillance Campaign in Tajikistan. Link
- Cybersurveillance, a Global Impact. Amnesty France Documentary. Link
- Spyware: MEPs sound alarm on threat to democracy and demand reforms. Link
- PEGA Committee does not go all the way on spyware regulation. Link
- Israeli Cyber Company NSO Group Has New Ownership After U.S. Blacklist. Link
- Digital Privacy Legislation is Civil Rights Legislation. Link
- Leaked Government Document Shows Spain Wants to Ban End-to-End Encryption. Link
- First man wrongfully arrested because of facial recognition testifies as California weighs new bills. Link

- Apple, Google Propose Standard to Combat Misuse of Location-Tracking Devices. Link
- Google Beats Class Action over Retention of Video-Viewing Info. Link
- Twitter Abruptly Stops Reporting On Gov't Requests As Data Reveals Elon Obeys Gov't Demands Way More Often Than Old Twitter. Link
- Twitter admits to exposing private tweets, finally. Link
- WhatsApp could disappear from UK over privacy concerns, ministers told. Link
- OpenAI may leave the EU if regulations bite – CEO. Link
- What does your smart fridge know about you? Link
- Brave unveils new "Forgetful Browsing" anti-tracking feature. Link
- Google adds passkey option to replace passwords on Gmail and other account services. Link
- Google Is Rolling Out Password-Killing Tech to All Accounts. Link
- Apple blocked 1.7 million apps for privacy, security issues in 2022. Link
- Microsoft is scanning the inside of password-protected zip files for malware. Link
- European Parliament adopted Resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework. Link
- CJUE Clarifies the Right to Obtain a Copy of Personal Data under the GDPR. Link
- EU General Court Clarifies When Pseudonymized Data is Considered Personal Data. Link
- The CJEU on GDPR: A summary of recent cases. Link
- Tracker gathering key decisions of the Court of Justice of the EU (CJEU) in more than 35 cases related to data protection, following the entry into application of GDPR. Link

- Unlocking Data Protection By Design & By Default: Lessons from the Enforcement of Article 25 GDPR. Future of Privacy Forum Report. Link
- Clearview fined again in France for failing to comply with privacy orders. Link
- Clearview AI data use deemed illegal in Austria, however no fine issued. Link
- CNIL publishes an action plan for the deployment of AI systems that respect the privacy of individuals. Link
- Supreme Court Won't Hold Tech Companies Liable for User Posts. Link
- € 1.2 billion GDPR fine for Meta over US mass surveillance. Link
- RIP World Password Day. Link
- How to hide from the NSA and CIA? Basic anonymity techniques to Black Hat. Link
- How to Delete Your Data From ChatGPT. Link
- How Do Different Encrypted Messaging Apps Treat Deleted Messages? Link
- Spyware is only the tip of the iceberg: we need to protect journalists from all forms of surveillance. Link
- Journalists, Rights Groups Urge Ban on 'Sinister' Spyware Like Pegasus. Link
- Access Now Expert Panel Discussion: Secret surveillance: countering spyware's threats to freedom of the press and expression. The recording. Link
- Re-envisioning Surveillance and Privacy through a Sustainability Lens. The 2023 CRISP Annual Lecture delivered by Professor Julie E. Cohen. The recording. Link
- Biometric Britain: The Expansion of Facial Recognition Surveillance. Big Brother Watch Report. Link
- #Help: Digital Humanitarianism and the Remaking of International Order. Book by Fleur Johns. Link

- Call for briefing papers for the 2024 edition of the ICRC's Symposium on Cybersecurity and Data Protection, to take place in Luxembourg in January 2024. Link

- White House challenges hackers to break top AI models at DEF CON 31. Link
- Why Honeytokens Are the Future of Intrusion Detection. Link
- HackerAI - Artifical Intelligence to detect vulnerabilities in source code. Link

  AceCryptor: Cybercriminals' Powerful Weapon, Detected in 240K+ Attacks. Link
- Critical Siemens RTU Vulnerability Could Allow Hackers to Destabilize Power Grid. Link
- Researchers Uncover New Exploit for PaperCut Vulnerability That Can Bypass Detection. Link
- Working to fix bug which shows WhatsApp accessing phone's mic: Google. Link

  CISA warns of critical Ruckus bug used to infect Wi-Fi access points. Link
- KeePass exploit helps retrieve cleartext master password, fix coming soon. Link
- KeePass 2.X Master Password Dumper – tool allowing attackers to extract the KeePass master password from memory as a proof-of-concept (PoC). Link
- New Wi-Fi MITM Attack That Can Evade WPA3 Security Mechanisms. Link
- How Criminal Enterprises Pre-infect Millions of Mobile Devices. Link
- Legit app in Google Play turns malicious and sends mic recordings every 15 minutes. Link
- This Cybercrime Syndicate Pre-Infected Over 8.9 Million Android Phones Worldwide. Link
- Anatomy of a Malicious Package Attack. Link

- Google's .zip, .mov Domains Give Social Engineers a Shiny New Tool. Link
- Attacks increasingly use malicious HTML email attachments. Link
- New Ransomware Strain 'CACTUS' Exploits VPN Flaws to Infiltrate Networks. Link
- Microsoft: BEC Attackers Evade 'Impossible Travel' Flags With Residential IP Addresses. Link
- New phishing technique poses as a browser-based file archive. Link
- OneNote documents have emerged as a new malware infection vector. Link
- Infecting SSH Public Keys with backdoors. Link
- Microsoft 365 phishing attacks use encrypted RPMSG messages. Link
- Lazarus hackers target Windows IIS web servers for initial access. Link
- New BrutePrint Attack Lets Attackers Unlock Smartphones with Fingerprint Brute-Force. Link
- Critical zero-day flaw (CVE-2023-2868) exploited for 7 months! Backdoor access, data exfiltration, and 3 potent malware strains discovered targeting Barracuda's Email Security Gateways. Link
- Barracuda Email Security Gateway (ESG) hacked via zero-day bug. Link
- Meta Uncovers Massive Social Media Cyber Espionage Operations Across South Asia. Link
- Facebook cracks down on malware actors targeting business accounts. Link
- State of DNS Rebinding in 2023. Link
- New Russia-linked malware, labeled CosmicEnergy, can physically harm power grids, Mandiant reports. Link
- Whistleblower Drops 100 Gigabytes Of Tesla Secrets To German News Site: Report. Link

- Data breaches can happen to anyone: SolarWinds CEO in Exclusive Interview. Link
  Capita warns customers to assume that their data was stolen. Link
- Data Breach in Malta: Company must disclose source within 20 days or face penalties. Link
- Industrial automation giant ABB disclosed data breach after ransomware attack. Link
- MSI Data Breach: Private Code Signing Keys Leaked on the Dark Web. Link
- Toyota: Data on More Than 2 Million Vehicles in Japan Were at Risk in Decade-Long Breach. Link
- HC3 issues fresh sector alert warning of data breaches from Cl0p, Lockbit ransomware groups. Link
- Western Digital Confirms Customer Data Stolen by Hackers in March Breach. Link
- As If Bank Failures Aren't Enough – Hackers Are Exploiting the Chaos to Breach Security. Link
- French data protection authority fined health website doctiddimo.fr for failures in processing of health data and non-compliance with cookie requirements. Link
- AI Spera released a new WordPress plugin called Anti-Brute Force, Login Fraud Detector, also known as Criminal IP FDS (Fraud Detection System). Link
- Best Password Practices to Defend Against Modern Cracking Attacks. Link
- Apple, Google, and Microsoft Just Fixed Zero-Day Security Flaws. Link
- Google launches bug bounty program for its Android applications. Link
- Data Stealing Malware Discovered in Popular Android Screen Recorder App. Link
- New ICANN Project Explores the Drivers of Malicious Domain Name Registrations. Link
- Why Honeytokens Are the Future of Intrusion Detection. Link

- Google Bans Thousands of Play Store Developer Accounts to Block Malware. Link
- Google brings generative AI to cybersecurity. Link
- Google will provide dark web monitoring to all US Gmail users and more. Link
- Researchers show ways to abuse Microsoft Teams accounts for lateral movement. Link
- Meta Is Trying to Push Attackers to the Brink. Link
- FBI Focuses on Cybersecurity With $90M Budget Request. Link
- The Cyber Resilience Act: How to make Europe more digitally resilient? Link
- New EU Cyber Law for the Financial Services Industry with Significant Impact on ICT Service Providers. Link
- New CISA Guidelines Lay Out Unified International Principles on Security-by-Design and Security-by-Default. Link
- ENISA published an assessment of standards for the cybersecurity of AI and issues recommendations to support the implementation of upcoming EU policies on Artificial Intelligence. Link
- The European Cybersecurity Competence Centre opens its doors in Bucharest. Link
- HackerOne: How the economy is impacting cybersecurity teams. Link
- Inside the Mind of the TOP1 Facebook Bug Bounty Hunter. Youssef Sammouda. BBRD podcast. Link
- Evasive Malware: Understanding Deceptive and Self-Defending Threats. Book by Kyle Cucci. Link
- Bluenomicon Book. Link
- BSidesSF 2023 talk by Alethe Denis titled HALT AND CATCH FIRE: Social Engineering CTFs for fun to a job as a Professional Red Team Social Engineer. While the contests were fun and seemingly glamorous, the reality of SE for money was much different. Link