CCRS Bit

April 2023

CONTENTS

Cybercrime 2
Digital Investigation and Digital Evidence 4
Digital Forensics 6
Digital Surveillance vs. Privacy 7
Cyber Security 10

Cybercrime

- Ransomware – Attacks on the Rise: Are We Prepared for the Next Wave of Cybercrime? Link
- New victims come forward after mass-ransomware attack. Link
- Cybercrime group exploits Windows zero-day in ransomware attacks. Link
- The developers of the Typhon info-stealing malware announced on a dark web forum that they have updated the malware to a major version they advertise as 'Typhon Reborn V2'. Link
- Microsoft has observed phishing attacks targeting accounting and tax return preparation firms to deliver the Remcos remote access trojan, among threats that take advantage of current events and major news headlines like Tax Day. Link
- Mercenary spyware hacked iPhone victims with rogue calendar invites, researchers say. Link
- Lazarus Hacker Group Evolves Tactics, Tools, and Targets in DeathNote Campaign. Link
- 'Proxyjacking' Cybercriminals Exploit Log4j in Emerging, Lucrative Cloud Attacks. Link
- CryptoClippy: New Clipper Malware Targeting Portuguese Cryptocurrency Users. Link
- Hackers claim vast access to Western Digital systems. Link
- The Massive 3CX Supply-Chain Hack Targeted Cryptocurrency Firms. Link
- 3CX's supply chain attack was caused by… another supply chain attack. Link
- North Korean hackers turn to 'cloud mining' for crypto to avoid law enforcement scrutiny. Link

- The New Face of Fraud: FTC Sheds Light on AI-Enhanced Family Emergency Scams. Link
- DDoS attacks shifting to VPS infrastructure for increased power. Link
- A cyber attack hit the water controllers for irrigating fields in the Jordan Valley. Link
- Hackers used spyware made in Spain to target users in the UAE, Google says. Link
- New dark web market STYX focuses on financial fraud services. Link
- Thieves Use CAN Injection Hack to Steal Cars. Link
- Cybercriminals 'CAN' Steal Your Car, Using Novel IoT Hack. Link
- The Hacker. Runa Sandvik. Link
- My phone, my credit card, my hacker, and me. Verizon, Chase, the police — they were all useless when my identity got hacked. Then Psycho Bunny came to the rescue. Link
- Hacker Group Names Are Now Absurdly Out of Control. Link
- Looking Back On Cybercrime, CISO Show. Link
- Hacker's Movie Guide: The Complete List of Hacker and Cybersecurity Movies (2022-23 Edition). Book. Link
- Click Here episode: about cryptocurrency tracing industry and financial cyberwarfare. Link

Digital Investigation and Digital Evidence

- Takedown of Genesis Market listed for sale the identities of over 2 million people when it was shut down. Link
- Genesis Market seizure a warning that cybercrime no longer anonymous. Link
- Spain's most dangerous and elusive hacker now in police custody. Link
- NetWire Remote Access Trojan Maker Arrested. Link
- The U.S. Cracked a $3.4 Billion Crypto Heist—and Bitcoin's Anonymity. Link
- Justice Department Seizes Over $112M from Scammers who allegedly used the seized accounts to launder funds acquired via cryptocurrency confidence scams, known as "CryptoRom" or "pig butchering." Link
- Israel confiscates dozens of digital accounts dealing with Hamas. Link
- Do Kwon associate Han bought $2.2m flat in Belgrade during manhunt. Link
- Police seize $2.2m Belgrade apartment where Do Kwon hid during six-month manhunt. Link
- Inside the international sting operation to catch North Korean crypto hackers. Link
- Benefits of sharing financial cybercrime information. Link
- The IRS is sending four investigators across the world to fight cybercrime. Link
- Ransomware Investigation: The New Challenges. Link

- Dutch Police mails RaidForums members to warn they’re being watched. Link
- UK Sets Up Fake Booter Sites To Muddy DDoS Market. Link
- The DEA Has Added Apple’s AirTags to Its Surveillance Arsenal. Link
- ‘Predictive Policing’, ‘Predictive Justice’, and the Use of ‘Artificial Intelligence’ in the Administration of Criminal Justice on Germany, by Johanna Sprenger and Dominik Brodowski. Link
- AI and the Administration of Criminal Justice in Italy, by Mitja Gialuz and Serena Quattrocolo. Link
- AI and Administration of Criminal Justice. Report on The Netherlands. By Maša Galič, Abhijit Das and Marc Schuilenburg. Link
- Microsoft Takes Legal Action to Disrupt Cybercriminals' Illegal Use of Cobalt Strike Tool. Link
- @ROXANNE project published the final newsletters. Link
- Dutch Police Releases Documentary on Operation CookieMonster. Link

Digital Forensics

- Dusting for Fingerprints: How New Anti-Detect Browsers Spoof Real Users with Stolen Digital Fingerprints. Link
- Tackling Time In Digital Investigations – Succeeding When Seconds Matter. Link
- Volatility New Release. Link
- Wireshark New Release. Link
- DFIR via XDR: How to expedite your investigations with a DFIRent approach. Link
- Lnkbomb - Malicious shortcut generator for collecting NTLM hashes from insecure file shares. Link
- lsassy Python tool to remotely extract credentials on a set of hosts. This blog post explains how it works. Link
- Blackbird - An OSINT tool to search for accounts by username in social networks. Link
- Cellebrite webinar "Deep Dive into SQLite" in the rdv4n6s series, which will give you a deeper understanding of the internal structure of SQLite, and how to optimize our search on deleted information. May 16th, 2023, online
- Book. Deep Dive: Exploring the Real-world Value of Open Source Intelligence. Link

DIGITAL SURVEILLANCE VS. PRIVACY

- The DEA Bought Customer Data from Rogue Employees Instead of Getting a Warrant. Link
- NSO Group Used 3 Zero-Click iPhone Exploits against Human Rights Defenders. Link
- Apple's high security mode blocked NSO spyware, researchers say. Link
- Israeli's iPhone Hacked With NSO's Pegasus Spyware Twice in Two Years. Link
- Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers. Link
- New Spyware Firm Said to Have Helped Hack iPhones Around the Globe. Link
- Greek Government Used Predator Spyware To Spend A Year Surveilling A US Citizen. Link
- The Predator spyware was developed in North Macedonia. Link
- How Mexico Became the Biggest User of the World's Most Notorious Spy Tool. Link
- Clearview AI scraped 30 billion images from Facebook and other social media sites and gave them to cops: it puts everyone into a 'perpetual police line-up'. Link
- What Happens When your Social Media Photos End Up in the Hands of Police. Link
- A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations. Link
- Tor Teamed up with Mullvad VPN to Launch the Mullvad Browser: a Tor Browser without the Tor Network. Link

- A review of some encryption methodologies and an introduction to a new methodology that may challenge the National Security Agency. Link
- WhatsApp and other messaging apps oppose 'surveillance'. Link
- Mozilla and Internet Freedom Foundation Join Global Encryption Coalition Steering Committee. Link
- 3 Fronts in the Battle for Digital Identity. Link
- Biometric Authentication Isn't Bulletproof —Here's How to Secure It. Link
- Unpacking the Privacy Implications of Extended Reality. Link
- ChatGPT Has a Big Privacy Problem. Italy's recent ban of Open AI's generative text tool may just be the beginning of ChatGPT's regulatory woes. Link
- ChatGPT and the future of digital identity: bot, until proven otherwise. Link
- The 'Manhattan Project' Theory of Generative AI. Link
- Generative AI: Privacy and tech perspectives. Link
- Telegram: an App finds anonymous users. According to some rumors circulating on the Net in the past few hours, the Russian government could use an application called Okhotnik ("hunter") with which it would be possible to discover the identity of anonymous users on Telegram. Link
- TikTok fined $16m for 'misusing children's data' in the UK. Link
- An Introduction to Washington's My Health My Data Act. Link
- 'Shut it off immediately': The health industry responds to data privacy crackdown. Link
- Arkansas Enacts Legislation Restricting Social Media Accounts for Minors. Link
- Big Tech Should Embrace California's Age Appropriate Design Code. Link
- Why age-verification bills for porn sites won't work. Link

- EU Parliament study slams online child abuse material proposal. Link
- EFF and Partners Call Out Threats to Free Expression in Draft Text as UN Cybersecurity Treaty Negotiations Resume. Link
- CISA Publishes International Guidance on Implementing Security-by-Design and Security-by-Default Principles for Software Manufacturers and Customers. Link
- EDPB adopts final version of Guidelines on data subject rights - right of access. Link
- EDPB resolves dispute on transfers by Meta and creates task force on Chat GPT. Link
- Data Protection Commission Ireland issues Guidance for Drivers on use of "Dash Cams". Link
- A Tiny Blog Took on Big Surveillance in China—and Won. Link
- The Air Force Loves War Gamers Like Teixeira. Link
- Assume the humans are human and bad things will happen. Link
- Book. The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology. Link

Cyber Security

- Malware is proliferating, but defenses are stronger: Mandiant. Link
- Hackers Use Google Ads to Deliver Bumblebee Malware. Link
- Lazarus Group Adds Linux Malware to Arsenal in Operation Dream Job. Link
- Rorschach Ransomware Emerges: Experts Warn of Advanced Evasion Strategies. Link
- Crypto-Stealing OpcJacker Malware Targets Users with Fake VPN Service. Link
- Cryptocurrency Companies Targeted in Sophisticated 3CX Supply Chain Attack. Link
- First-Ever Ransomware Found to be Attacking MacOS. Link
- First-Ever Cyber Attack Via Kubernetes RBAC to Create Backdoor on Clusters. Link
- New DDoS attacks on Israel's enterprises, infrastructure should be a wake-up call. Link
- Hackers Using Self-Extracting Archives Exploit for Stealthy Backdoor Attacks. Link
- Blind Eagle Cyber Espionage Group Strikes Again: New Attack Chain Uncovered. Link
- Newly Discovered "By-Design" Flaw in Microsoft Azure Could Expose Storage Accounts to Hackers. Link
- Credential harvesting malware appears on deep web. Link
- Google Play threats on the dark web are big business. Link
- OpenAI launched its Bug Bounty Program with BugCrowd, inviting hackers to help identify and address vulnerabilities in their AI systems. Link

- Google Issues First 2023 Zero Day Warning To 3 Billion Chrome Users. Link
- Google Chrome Hit by Second Zero-Day Attack - Urgent Patch Update Released. Link
- Apple Zero-Days Exploited to Hack iPhones and MacOS. Link
- Hackers Exploiting WordPress Elementor Pro Vulnerability: Millions of Sites at Risk! Link
- Printers Pose Persistent Yet Overlooked Threat. Link
- Apple released emergency updates to fix recently disclosed zero-day bugs on older devices. Link
- Urgent: Microsoft Issues Patches for 97 Flaws, Including Active Ransomware Exploit. Link
- Experts warn patching won't protect critical infrastructure against 'new-age malware'. Link
- BBB Scam Tracker (https://bbb.org/scamtracker/us/) is an online tool that enables consumers and businesses to report scams in an effort to prevent others from falling prey to similar cons
- Siemens Metaverse exposes sensitive corporate data. Link
- Multinational bank leaks passports and credit card numbers. Link
- French video games leak user passwords. Link
- Peugeot leaks access to user information in South America. Link
- Kodi discloses data breach after forum database for sale online. Link
- MSI confirms security breach after Money Message ransomware attack. Link
- NATO’s 2023 Locked Shields Cyber Exercise: 38 Countries Take Part. Link
- Microsoft: Iranian hackers behind retaliatory cyberattacks on US orgs. Link

- Iranian Hackers Using SimpleHelp Remote Support Software for Persistent Access. Link
- Google TAG Warns of Russian Hackers Conducting Phishing Attacks in Ukraine. Link
- US and UK agencies warn of Russia-linked APT28 exploiting Cisco router flaws. Link
- Pakistani APT-36 Hackers Using a Linux Malware to Attack Indian Government. Link
- The Military Counterintelligence Service and the CERT Polska team (CERT.PL) observed a widespread espionage campaign linked to Russian intelligence services. Link
- EU proposes $1.2 billion plan to counter growing cybersecurity threats. Link
- On the 18 April 2023, the Commission has adopted a proposal for the EU Cyber Solidarity Act to strengthen cybersecurity capacities in the EU and has presented a Cybersecurity Skills Academy, to ensure a more coordinated approach towards closing the cybersecurity talent gap, a pre-requisite to boosting Europe’s resilience
- Hacker Interviews: ArchAngelDDay. Link