CCRS Bit

March 2023

CONTENTS

Cybercrime

- FBI Internet Crime Report said that reported losses jumped from $6.9 billion in 2021 to $10.2 billion in 2022 — a nearly 48 percent leap. Link
- The World's Real 'Cybercrime' Problem. From US state laws to the international stage, definitions of "cybercrime" remain vague, broad, and increasingly entrenched in our legal systems. Link
- Stolen credentials increasingly empower the cybercrime underground. Link
- Clop ransomware gang begins extorting GoAnywhere zero-day victims. Link
- Mirai Hackers Use Golang to Create a Bigger, Badder DDoS Botnet. With HinataBot, malware authors have created a beast many times more efficient than even the scariest botnets of old, packing more than 3Tbit/s DDoS speeds. Link
- Hackers mostly targeted Microsoft, Google, Apple zero-days in 2022. Link
- FTX Says $415 Million In Crypto Was Hacked. Link
- Coinbase wallet and other decentralized crypto apps (dapps) were found to be vulnerable to "red pill attacks," a method that can be used to hide malicious smart contract behavior from security features. Link
- Zero-Day Bug Allows Crypto Hackers to Drain $1.6M from Bitcoin ATMs. Link
- Cybercriminals Targeting Law Firms with GootLoader and FakeUpdates Malware. Link
- Trezor warns of massive crypto wallet phishing campaign. Link

- General Bytes Bitcoin ATMs hacked using zero-day, $1.5M stolen. Link
- Record Breaking DDoS Attack – 158.2 Million Packets Per Second. Link
- The LockBit ransomware group claims to have stolen confidential data belonging to SpaceX from the systems of Maximum Industries. Link
- Royal Ransomware Made Upto $11 Million USD Using Custom-Made Encryption Malware. Link
- Emotet malware attacks return after three-month break. Link
- Security researchers targeted with new malware via job offers on LinkedIn. Link
- This Is the New Leader of Russia's Infamous Sandworm Hacking Unit. Evgenii Serebriakov now runs the most aggressive hacking team of Russia's GRU military spy agency. To Western intelligence, he's a familiar face. Link
- State of Cyber Threat Intelligence: 2023. A deep dive into the perpetual cycles of cybercrime—and how to fight back. Link
- Nine in 10 enterprises fell victim to successful phishing in 2022. Link
- A New Crypto Mixer Promises to Be Tornado Cash Without the Crime. Privacy Pool founder says he can preserve users' privacy while keeping money launderers and regulators at bay. Link
- FBI Warns of Crypto-Stealing Play-to-Earn Games. Link
- Thousands scammed by AI voices mimicking loved ones in emergencies. Link
- Cybercriminals, APT Exploited Telerik Vulnerability in Attacks on US Government Agency. Link
- Blockchain Forensics and Crypto-Related Cybercrimes. Free handbook. Link

- A Hacker's Mind. New Book. Bruce Schneier, Security Technologist and Cryptographer. Cybercrime Magazine podcast episode. Link
- Ageless Security: Cybercrime prevention across the generation gap. Cybercrimeology podcast. Link
- Evolution of criminal scams (especially BEC). Law enforcement honeypots. ChatGPT data leak. Hybrid war updates. CyberWire Daily podcast episode. Link
- Interview with one of the world's most famous hackers #OccupyTheWeb. Link

Digital Investigation and Digital Evidence

- How Open Source Evidence was Upheld in a Human Rights Court. Link
- First forensic sprint at Europol to speed up human trafficking investigations. Link
- The U.S. government announced today it seized a website used to sell NetWire, software widely considered to be malware. In an affidavit, an FBI agent explained how the feds determined that NetWire was indeed malicious. Link
- How the Dutch National Police Tricked Prolific Ransomware Strain Deadbolt into Giving Up Victim Decryption Keys. Link
- European police, FBI bust international cybercrime gang. Link
- One of the darkweb's largest cryptocurrency laundromats washed out. Link
- Police Arrest Suspected Members of Prolific DoppelPaymer Ransomware Gang. Link
- Do Kwon: Fugitive 'cryptocrash' boss arrested in Montenegro. Link
- Chinese hackers use new custom backdoor to evade detection. Link
- Breached hacking forum shuts down, fears it's not 'safe' from FBI. Link
- New Cyber Platform Lab 1 Decodes Dark Web Data to Uncover Hidden Supply Chain Breaches. Link
- Hacker Group Arrested for Targeting High-Profile Business Leaders. Link

- ChatGPT - the impact of Large Language Models on Law Enforcement. Tech Watch Flash reports, Europol's Innovation Lab. Link
- Tips for Investigating Cybercrime Infrastructure. Link
- A US Congressman Says the FBI Unlawfully Targeted Him. Link
- UK police reveal they are running fake DDoS-for-hire sites to collect details on cybercriminals. Link
- Cyber Police of Ukraine Busted Phishing Gang Responsible for $4.33 Million Scam. Link
- SIRIUS annual Advisory Board meeting: celebrating past achievements and preparing for a promising future of cross-border access to electronic evidence. Link
- Dan Golden and Renee Dudley, reporters at ProPublica and authors of "The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World from Cybercrime," discuss their book. Hacking Humans podcast episode. Link

Digital Forensics

- A Comparative Analysis of Digital Forensic Investigation Tools on Facebook Messenger Applications. Journal of Cyber Security and Mobility. Link
- CYCLOPES Project shared the first Annual Standardisation Recommendations in the field of Digital Forensics with a special focus on Mobile Devices and Wearable Technologies. Link
- Digital forensics and incident response: The most common DFIR incidents. Link
- Research Lab AI4forensics is opened, in a collaboration between the University of Amsterdam (UvA) and the Netherlands Forensic Institute (NFI), and is located in the ICAI - Innovation Center for Artificial Intelligence in Amsterdam. The research lab focuses on the application of artificial intelligence (AI) in forensic evidence. Link
- AI and OSINT: New Breakthroughs Meet Next Gen Solutions. Link
- Wireshark 4.0.4 Release. Link
- Free Phishing E-Mail Analysis Tools. Link
- Oxygen Forensics Launches a browser-based Real-Time Data Collaboration Solution, Oxygen Analytic Center. Link
- Magnet RESPONSE: New Free Tool For IR Investigations. Link
- Training, Digital Strategies, and … Onions? Unveiling the World of Digital Forensics with Jason Cullum. Link
- Free E-book: 5 Things you're Doing Wrong in your Digital Forensics Lab. Link
- Magnet Forensics. 2023 State of Enterprise Digital Forensics and Incident Response. Link

- Why hardware needs to be validated and you will be shown how to validate the proper operation of writeblockers. Webinar, on demand. Link
- Mistakes to Avoid in Your Digital Forensics Lab. Webinar, April 12, 2023. Link
- Dark Web Search. Practical OSINT and SOCMINT Techniques. Tutorial. Link
- Online workshop. Conducting Open-Source Investigations tradecraft: key skills and best practice for investigators and analysts, April 26-27, 2023. Link

Digital Surveillance vs. Privacy

- Can a quantum algorithm crack RSA cryptography? Not yet. Link
- Google One subscribers to gain access to a free VPN and dark web monitoring service. Link
- GitHub to require 2FA for all contributors starting from March 13. Link
- The privacy loophole in your doorbell. Police were investigating his neighbor. A judge gave officers access to all his security-camera footage, including inside his home. Link
- Why You Should Opt Out of Sharing Data With Your Mobile Provider. Link
- Data for Sale: The Commoditization of Personal Information in a Controlled Society. Link
- Cerebral, the therapy telehealth startup, shared millions of patients' personal and health information with advertisers, like Google, Facebook and TikTok, for at least three years. More than 3.1 million individuals affected. Link
- Electronic Frontier Foundation (EFF) added 400 new points to the Atlas of Surveillance. Link
- Europe's borders are a surveillance testing ground. The AI Act could change that. Link
- Predictive Policing Makes Everyone a Suspect, Even EU Officials. Link
- EFF. How We Fought For and Won Access to Records about Predictive Policing. Link

- Clearview AI used nearly 1m times by US police, it tells the BBC. Link
- BKA und Zitis suchen Zero-Day-Exploits – Bundesregierung weiß nichts davon. Seit anderthalb Jahren arbeiten BKA und die Hackerbehörde Zitis im Rahmen eines EU-geförderten Projekts an einem "Live-Zugang" zu verschlüsselten Smartphones. Link
- Israeli Firm Suspected of Illegally Selling Classified Spy Tech. Haaretz reveals NFV Systems' surveillance tools; firm under investigation by secretive Israeli body for skirting arms export controls, in case that may 'damage national security'. Link
- The Department of Homeland Security's Inspector General has released a troubling new report detailing how federal agencies like Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and the Secret Service have conducted surveillance using cell-site simulators (CSS) without proper authorization and in violation of the law. Specifically, the office of the Inspector General found that these agencies did not adhere to federal privacy policy governing the use of CSS and failed to obtain special orders required before using these types of surveillance devices. Link
- The FBI Just Admitted It Bought US Location Data. Link
- Secret Service and ICE conducted warrantless stingray surveillance, says watchdog. Link
- FBI, Pentagon helped research facial recognition for street cameras, drones. Internal documents released in response to a lawsuit show the government was deeply involved in pushing for face-scanning technology that could be used for mass surveillance. Link
- President Biden Signs Executive Order Restricting Use of Commercial Spyware. Link

- New Chinese regulatory body will reportedly bring all data-related issues under a single entity, which is expected to streamline and clarify data regulations for multinational companies. Link
- EU – US adequacy decision: Update. Link
- EDPB Issues Opinion on the EU-US Data Privacy Framework: Key Takeaways. Link
- Use of Meta tracking tools found to breach EU rules on data transfers. A groundbreaking decision in one of NOYB 101 complaints, the Austrian Data Protection Authority (DSB) has decided that the use of Facebook's tracking pixel directly violates the GDPR and the so-called "Schrems II" decision on transatlantic data flows. Link
- The EDPB has just published "Guidelines 9/2022 on personal data breach notification under GDPR Version 2.0", adopted on 28 March 2023. Link
- Court rules Facebook violated Dutch law when processing personal data. Link
- EU watchdog: Online child abuse draft law creates 'illusion of legality'. Link
- German Parliament Rejects EU Commission Call For Client-Side Scanning. Link
- WhatsApp and UK government on collision course, as app vows not to remove end-to-end encryption. Link
- Russia's Rostec allegedly can de-anonymize Telegram users. Link
- How to "Access the Dark Web Safely", tools to stay "Anonymous, Dark Web Monitoring for Blue Team Operations" and much more. Dark Web & Anonymity Home-Lab. Link
- Enemy of the state (part 1): Mexico, spyware, and a secret military intelligence unit. Enemy of the state (part 2) :

¿Quién es Guacamaya? (who is Guacamaya?). Click here Podcast episodes: Link

- The digital Euro: the end of privacy in payments? Brussels Privacy Hub, April 20, 2023, online event. Link

Cyber Security

- Security's 2023 Top Cybersecurity Leaders. Link
- Fake Friends: Leak Reveals Israeli Firms Turning Social Media into Spy Tech. Link
- Akamai releases new threat hunting tool to detect and eliminate evasive threats most evasive threats and risks. Link
- New malware variant has "radio silence" mode to evade detection. Link
- Planting Undetectable Backdoors in Machine Learning Models. Link
- Trojanized TOR Browser Installers Spreading Crypto-Stealing Clipper Malware. Link
- WiFi protocol flaw allows attackers to hijack network traffic. Link
- Ransomware crooks are exploiting IBM file-exchange bug with a 9.8 severity. Link
- CISA orders agencies to patch bugs exploited to drop spyware. Link
- Emotet attempts to sell access after infiltrating high-value networks. Link
- GoBruteforcer: Golang-Based Botnet Actively Harvests Web Servers. Link
- Flaw spotted in the US government's quantum-safe encryption algorithm. Link
- Google warns users to take action to protect against remotely exploitable flaws in popular Android phones. Link

- Microsoft Rolls Out Patches for 80 New Security Flaws — Two Under Active Attack. Link
- ChatGPT Gut Check: Cybersecurity Threats Overhyped or Not? Link
- Twitter's Source Code Leak on GitHub a Potential Cyber Nightmare. Link
- Android app from China executed 0-day exploit on millions of devices. Link
- Amazon-owned Ring reportedly suffers ransomware attack. Russia-linked ALPHV ransomware gang has threatened to leak the stolen data if the company refuses to pay the ransom. Link
- North Korea-linked Lazarus APT group exploits a zero-day vulnerability in attacks aimed at a South Korean financial entity. Link
- Kaspersky releases decryptor for ransomware based on Conti source code. Link
- White House Releases National Cybersecurity Strategy. Link
- Australia: Cyber security round-up – new Cyber Security Strategy, data breach stats and more. Link
- Security vendors report economic hit as they struggle to lure newer customers. Link
- New Book "Women Know Cyber" by Steve Morgan & Di Freeze, published by Cybersecurity Ventures. Link
- APWG.EU and Meta Host Webinar on Techniques for Protecting Enterprises and Customers against Phishing Today. Webinar, April 5, 2023. Link