CCRS Bit

July 2023

CONTENTS

Cybercrime

- Cybercriminals Evolve Antidetect Tooling For Mobile OS-Based Fraud. Link
- Criminals, terrorists, and money launderers are ditching Bitcoin. Link
- Deepfake Quantum AI Investment Scam Pops Up on Facebook. Link
- What's up with Emotet? Link
- Neo_Net | The Kingpin of Spanish eCrime. Link
- BreachForums replacement emerges as robust forum for criminal hackers to trade their spoils. Link
- The Saga of Anonymous Sudan. Link
- Anonymous Sudan claims to have stolen 30 million Microsoft's customer accounts. Link
- Cyber Attack on French National Police: VulzSec Hacking Group Claims to Leak Sensitive Data. Link
- Social engineering campaign targeting tech employees spreading through npm malware. Link
- Novel PlugX malware attacks target European diplomats. Link
- Mexico-Based Hacker Targets Global Banks with Android Malware. Link
- New Nitrogen malware pushed via Google Ads for ransomware attacks. Link
- Lazarus hackers hijack Microsoft IIS servers to spread malware. Link
- New Android banking Trojan targets US, UK, and Germany. Link
- Chinese APT41 Hackers Target Mobile Devices with New WyrmSpy and DragonEgg Spyware. Link

- Hackers Use HTML Smuggling Technique to Attack European Government Entities. Link
- Ransomware Criminals Are Dumping Kids' Private Files Online After School Hacks. Link
- UK battles hacking wave as ransomware gang claims 'biggest ever' NHS breach. Link
- FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware. Link
- Ransomware payments on record-breaking trajectory for 2023. Link
- Rhysida Ransomware | RaaS Crawls Out of Crimeware Undergrowth to Attack Chilean Army. Link
- Hacking crew targeting states over transition bans claims cyberattack hitting global satellite systems. Link
- Cybercriminals Exploiting WooCommerce Payments Plugin Flaw to Hijack Websites. Link
- FBI: Tech support scams now use shipping companies to collect cash. Link
- Australia being ravaged by a cybercrime wave. Link
- Norway government ministries hit by cyber attack. Link
- Banking Sector Targeted in Open-Source Software Supply Chain Attacks. Link
- First known open-source software attacks on banking sector could kickstart long-running trend. Link
- Japan's Nagoya Port Suspends Cargo Operations Following Ransomware Attack. Link
- Over 130,000 solar energy monitoring systems exposed online. Link
- AI And Cybercrime Unleash A New Era Of Menacing Threats. Link
- Artificial Intelligence as a Tool for Generating Hybrid-Based Treats. Link

- WormGPT Cybercrime Tool Heralds an Era of AI Malware vs. AI Defenses. Link
- WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks. Link
- "WORMGPT," a project presented as an alternative to ChatGPT for blackhat activities like malware coding and exploits, was found selling in the hackers forum. Link
- WormGPT: Cybercriminals AI Tool Gained Over 5,000 Subscribers in Just a Week. Link
- New AI Tool 'FraudGPT' Emerges, Tailored for Sophisticated Attacks. Link
- Deepfaking it: What to know about deepfake-driven sextortion schemes. Link
- IWF 'sounds alarm' on first confirmed AI-generated child sexual abuse images. Link
- Cybercrime intelligence: blockchain security and anti-money laundering report 2023 mid-year. Link
- The Chainalysis Crypto Myth Busting Report. Link
- Crypto Crime Mid-year Update: Crime Down 65% Overall, But Ransomware Headed for Huge Year Thanks to Return of Big Game Hunting. Link
- These are now the hot cryptocurrencies for crime. Link
- Florida attorney general says complex cybercrime ring led by Orlando teen stole $350K in goods. Link
- California prosecutor Erin West on the massive wealth transfer to Southeast Asia from a crypto scam called 'pig butchering'. Link
- #DoubleFinger on the trigger: a multi-stage malware targeting cryptowallets. Link
- $7.8B lost in crypto Ponzi and pyramid schemes in 2022: Report. Link

- Cryptocurrency Research Firms Vastly Underestimate Illicit Payments, Critics Claim. Link
- North Korean hackers breached a US tech company to steal crypto. Link
- Who Is Hacking the World's Best Online Poker Players? Darknet Diaries Episode. Link
- The Trillion-Dollar Grift: Inside the Greatest Scam of All Time. Link
- Android OS Tools Fuel Cybercrime Spree, Prey on Digital Users. Link
- Why data removal services are vital to maintain privacy amid rising cyber crime. Link
- Inside the Mind of the Hacker: Report Shows Speed and Efficiency of Hackers in Adopting New Technologies. Link
- Hacker Conversations: Inside the Mind of Daniel Kelley, ex-Blackhat. Link
- What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021). Link

Digital Investigation and Digital Evidence

- How the FBI hacked Hive. Link
- How Musk's Twitter is Jeopardizing War Crimes Investigations. Link
- Support and recognition crucial in minimising harmful impacts for CSAM investigators and online moderators. Link
- How to Investigate Infostealer Malware. Link
- The Art of Finding New Darkweb Sources. Link
- ChatGPT and Crime- What Law Enforcement Needs to Know about Large Language Models. Link
- Lili Infante (CAT Labs) on Combating and Preventing Crypto Crime. Link
- Norway investigates cyberattack affecting 12 government ministries. Link
- Blowing Up the Crypto Cartel. Link
- Scareware developer arrested in Spain after a decade on the run. Link
- Police arrest suspect linked to notorius OPERA1ER cybercrime gang. Link
- Former Security Engineer Arrested for Stealing $9 Million from Crypto Exchange. Link
- Defendant Charged With Theft Of Cryptocurrency And NFTs Through Spoofing Of OpenSea Marketplace. Link
- Celsius founder Alex Mashinsky arrested and charged with fraud. Link
- Owner of BreachForums pleads guilty in federal court to three counts, including one involving child pornography. Link

- Couple behind Bitfinex money laundering scheme reach plea deal with US prosecutors. Link
- Silk Road's Second-in-Command Gets 20 Years in Prison. Link
- International Cyber Fraudster Sentenced to More Than 8 Years in Federal Prison. Link
- Russian Cybersecurity Firm Founder Jailed for 14 Years. Link
- U.S. DOJ Has Until October to Process Evidence Against Celsius' Mashinsky. Link
- Cybercrime Convention Committee (T-CY) Guidance Note #13, The scope of procedural powers and of international co-operation provisions of the Budapest Convention. Link
- First Draft of UN Cybercrime Convention Drops Troubling Provisions, But Dangerous And Open-Ended Cross Border Surveillance Powers Are Still on the Table. Link
- Analysis: A new global cybercrime treaty risks becoming yet another legal instrument to punish and muzzle the press. Link
- Analysis: EU's Recently Adopted E-Evidence Regulation. Link
- EU Commission updates payment rules to fight fraud, improve consumer rights. Link
- Commonwealth launches a cybercrime and electronic evidence e-learning course. Link
- New DOJ unit will focus on prosecuting nation-state cybercrime. Link
- DOJ merges cyber, cryptocurrency units to go after ransomware attacks. Link
- Chainalysis Investigations Lead Is 'Unaware' of Scientific Evidence the Surveillance Software Works. Link
- How to determine the admissibility of AI-generated evidence in courts? Link
- Listen: FBI Eyes Evolving Tech to Combat 'Cybercrime as a Service'. Link

Digital Forensics

- Detego Global announced the release of Detego Analyse AI+. Link
- Belkasoft X v.2.0. Link
- Oxygen Analytic Center v.1.1 Is Now Available. Link
- Passware Kit 2023 v3. Link
- Offline Collection With Binalyze AIR. Link
- Bluebear LES and Thorn announced the integration of the Thorn CSAM Classifier with Bluebear LACE Solution, in order to empower investigators to elevate and review CSAM that is unknown to local LACE databases. Link
- Wireshark 4.0.7 Release. Link
- The system architecture of the TRACE tool. Link
- Darkweb OSINT links and new 2023 resources. Link
- Snappy: a tool to detect rogue WiFi access points on open networks. Link
- ADS Locator: a software application that automatically scans the computer for files with Alternate Data Streams (ADS) attached and lets you extract them. Link
- ZEHEF: the OSINT tool for email tracking. Link
- PYOSINT: an open-source Python framework that automates subdomain enumeration, web scraping and usernames search. Link
- PcapXray - A Network Forensics Tool to visualize a Packet Capture offline as a Network Diagram including device identification, highlight important communication and file extraction. Link

- GhostRecon: Scan for Phone, Email & other details. Link
- BadZure: a tool that automates the creation of Azure AD tenants, introducing misconfigurations and attack paths. Link
- New PhoneSploit Pro is available on GitHub PhoneSploit - pentesting tool to remotely exploit Android devices using ADB and Metasploit-Framework to get a Meterpreter session. Link
- Large collection of examples of using ChatGPT for DFIR. Link
- What the rollout of Google Analytics 4 means for website investigations. Link
- Hunting Malware with Velociraptor (YARA & Memory Forensics). Video. Link
- Digital Forensic CTF challenges. Link
- Malware misinformation - a website that tries to collect, document and debunk misinformation related to malware and malware forensics. Link
- Maltego: The Ultimate OSINT & Cyber Investigation Tool. Video. Link
- Brute forcing a mobile's pin over USB with a $3 board. Link
- Automating Web Scraping with ChatGPT Code Interpreter. Link
- Investigating SMS phishing text messages from scratch. Link
- A Comprehensive Guide to Digital Forensics with DJI Drones. Link

Digital Surveillance vs. Privacy

- Code Kept Secret for Years Reveals Its Flaw—a Backdoor. Link
- Even the Government Thinks It Should Stop Buying Corporate Surveillance Data. Link
- Analysis: A new global cybercrime treaty risks becoming yet another legal instrument to punish and muzzle the press. Link
- Data broker loophole threatens journalists and whistleblowers. Link
- "HKLeaks" – The Use of Covert and Overt Online Harassment Tactics to Repress 2019 Hong Kong Protests. Link
- US Spies Are Buying Americans' Private Data. Congress Has a New Chance to Stop It. Link
- Tax Filing Websites Have Been Sending Users' Financial Information to Facebook. Link
- Congressional Report Finds Meta and Tax Prep Companies "Recklessly" Shared Taxpayers' Data. Link
- An email typo has reportedly sent millions of US military messages to Mali. Link
- Revealed: Metropolitan police shared sensitive data about crime victims with Facebook. Link
- Why can't the NHS quit Palantir? Link
- Two years after the Pegasus Project, is the risk of being spied on through your phone higher than before? Link
- Intel leaders, White House argue for keeping digital spy powers. Link
- White House issues warning to US firms interested in acquiring Israeli surveillance tech (NSO). Link

- US government adds two more spyware makers to denylist. Link
- Spain closes probe into Pegasus spyware over Israel's 'complete lack of cooperation'. Link
- Report: Israeli Spyware Firm, Ex-security Boss, Advised on Secret Greek Spy Agency Deal. Link
- North Macedonia endorses human rights initiative, still allows development of Predator spyware. Link
- Spain's High Court shelves Israeli spyware probe on lack of cooperation. Link
- How Your Phone Can Be Hacked Remotely and What You Can Do to Stop It. Link
- Database Mess up Exposed PII and Photos of 2.3M Dating App Users. Link
- Dating app spills 340GB of steamy data and 260,000 user profiles. Link
- Two Spyware Apps on Google Play with 1.5 Million Users Sending Data to China. Link
- 'They want to instil fear': Victorians' files bound for dark web after data breach. Link
- Major banks' privacy policies allow them to monitor customers' social media accounts. Link
- Google hit with lawsuit alleging it stole data from millions of users to train its AI tools. Link
- 3 tax prep firms shared 'extraordinarily sensitive' data about taxpayers with Meta, lawmakers say. Link
- Pornhub Is Being Accused of Illegal Data Collection. Link
- WeChat collects more usage data than they disclose. Link
- Apple security and privacy engineers thwarted Pegasus. It was just one of their successes this year. Link
- Amazon ordered to pay more than $30M for privacy violations related to Alexa, Ring devices. Link

- The FCC aims to stop SIM swappers with new rules. Link
- Threads collects so much sensitive information it’s a ’hacker’s dream,’ experts say. Link
- The FTC is investigating whether ChatGPT harms consumers. Link
- Meta Unveils a More Powerful A.I. and Isn’t Fretting Over Who Uses It. Link
- OpenAI Worries About What Its Chatbot Will Say About People’s Faces. Link
- CJEU declares Meta's GDPR approach illegal. Link
- Spotify gets fine of € 5 Million for GDPR violations. Link
- Norwegian DPA temporarily bans behavioral advertising on Facebook and Instagram. Link
- Data Privacy Framework is just a "copy of Privacy Shield" & must fail. Link
- Google updates its privacy policy to allow data scraping for AI training. Link
- Google forced to postpone Bard chatbot’s EU launch over privacy concerns. Link
- WhatsApp changes legal basis to Legitimate Interest. Link
- Maltego: Check how exposed you are online. Link
- We Asked Researchers About How They Use Blacklight. This Is What They Said. Link
- Digital rights for civil society and civil society for digital rights: how surveillance technologies shrink civic spaces. Link
- Are Many Privacy Violations Also Data Breaches? Link
- Apple slams UK surveillance-bill proposals. Link
- Content Moderation, Encryption, and the Law. Link

- Spies, Lies, and Algorithms: The History and Future of American Intelligence, Book written by Amy Zegart. Link
- Your Face Belongs to Us: A Secretive Startup's Quest to End Privacy as We Know It. Book by Kashmir Hill. Link

Cyber Security

- Designing a Malware Loader detector with Guard Violation Exceptions. Link
- MITRE Unveils Top 25 Most Dangerous Software Weaknesses of 2023. Link
- Aqua Security Study Finds 1,400% Increase in Memory Attacks. Link
- Alert: 330,000 FortiGate Firewalls Still Unpatched to CVE-2023-27997 RCE Flaw. Link
- Automated brain process for smart contract auditing. Link
- Hunting for Nginx Alias Traversals in the wild. Link
- ChatGPT tricked into generating Windows 10 and Windows 11 keys. Link
- DDoS attacks want to make sure you haven't forgotten about them. Link
- Criminal IP Unveils Bug Bounty Program to Boost User Safety, Security. Link
- 'Big Head' malware threat looms, warn researchers. Link
- Microsoft: Hackers turn Exchange servers into malware control centers. Link
- Hackers Actively Exploit Unpatched Office Zero-Day Flaw in the Wild. Link
- Cisco Talos Reports Microsoft Windows Policy Loophole Being Exploited by Threat Actor: Old certificate, new signature: Open-source tools forge signature timestamps on Windows drivers. Link

- Microsoft: Unpatched Office zero-day exploited in NATO summit attacks. Link
- Azure AD Token Forging Technique in Microsoft Attack Extends Beyond Outlook, Wiz Reports. Link
- Andariel's silly mistakes and a new malware family. Link
- Citrix Secure Access Client Flaw Let Attackers Execute Remote Code. Link
- Malware Execution Method Using DNS TXT Record. Link
- Malicious USB Drives Targetinging Global Targets with SOGU and SNOWYDRIVE Malware. Link
- Charming Kitten hackers use new 'NokNok' malware for macOS. Link
- PoC Exploit: Fake Proof of Concept with Backdoor Malware. Link
- Cybercriminals Exploit Microsoft Word Vulnerabilities to Deploy LokiBot Malware. Link
- Cybercriminals Hijacking Vulnerable SSH Servers in New Proxyjacking Campaign. Link
- Who and What is Behind the Malware Proxy Service SocksEscort? Link
- Undocumented driver-based browser hijacker RedDriver targets Chinese speakers and internet cafes. Link
- Newly Surfaced ThirdEye Infostealer Targeting Windows Devices. Link
- Evasive Meduza Stealer Targets 19 Password Managers and 76 Crypto Wallets. Link
- Letscall – New Sophisticated Voice over IP Phishing Attack Steal Banking Details. Link
- DDoSia Attack Tool Evolves with Encryption, Targeting Multiple Sectors. Link
- Following NoName057(16) DDoSia Project's Targets. Link

- Botnets Send Exploits Within Days to Weeks After Published PoC. Link
- CustomerLoader: a new malware distributing a wide variety of payloads. Link
- Move It on Over: Reflecting on the MOVEit Exploitation. Link
- Diplomats Beware: Cloaked Ursa Phishing With a Twist. Link
- Hackers use Cloned pages of Popular Tools to Deliver Blackcat Ransomware. Link
- BlackCat ransomware pushes Cobalt Strike via WinSCP search ads. Link
- Akira Ransomware Expanded its Toolkit to Attack Linux Machines. Link
- New 'Big Head' ransomware displays fake Windows update alert. Link
- PoisonGPT: How we hid a lobotomized LLM on Hugging Face to spread fake news. Link
- Analyzing Attack Opportunities Against Information Security Practitioners. Link
- ESET Threat Report H1 2023. Link
- ENISA Health Threat Landscape. Link
- Microsoft lost its keys, and the government got hacked. Link
- Google exposes intelligence and defense employee names in VirusTotal leak. Link
- Cybersecurity firm Sophos impersonated by new SophosEncrypt ransomware. Link
- Twitter's bot spam keeps getting worse — it's about porn this time. Link
- 17 Million Instagram Accounts, 178 GB of TikTok and Yahoo Databases were Leaked. Link
- EV Charger Hacking Poses a 'Catastrophic' Risk. Link

- The Spies Who Loved You: Infected USB Drives to Steal Secrets. Link
- Apple pushes emergency patch to fix exploited zero-day in iOS and macOS. Link
- ChatGPT can write ransomware, but what about incident response plans? Link
- U.S. National Standards Strategy for Critical and Emerging Technology. Link
- Hackers: We won’t let artificial intelligence get the better of us. Link
- European Interdisciplinary Cybersecurity Conference (EICC) 2023. Recording. Link
- THE D.R. INCIDENT, Darknet Diaries new episode. Link
- Web App Hacking with Caido.io. Link
- Hacker Interview: Ryan Montgomery AKA 0day. Link