



# CCRS Bit

January 2024

## CONTENTS

Cybercrime.....	2
Digital Investigation and Digital Evidence .....	7
Digital Forensics .....	11
Digital Surveillance vs. Privacy .....	14
Cyber Security.....	20

# CYBERCRIME

- Global Cybercrime Report: Which Countries Are Most at Risk in 2023? [Link](#)
- The Worst Hacks of 2023. [Link](#)
- The biggest cyber attacks of 2023. [Link](#)
- List of Data Breaches and Cyber Attacks in 2023 - 8,214,886,660 records breached. [Link](#)
- ITRC 2023 Annual Data Breach Report. [Link](#)
- UNODC: Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat. [Link](#)
- Europol: the Spotlight Report 'Online fraud schemes: a web of deceit'. [Link](#)
- Annual Payment Fraud Intelligence Report: 2023. [Link](#)
- Burnout: Inferno Drainer's multimillion-dollar scam scheme detailed. [Link](#)
- Key Highlights from the 2023 UK Cyber Crime Landscape. [Link](#)
- Looking back at 2023 with the NSA's Rob Joyce and Morgan Adamski. [Link](#)
- Grooming, radicalization and cyber-attacks: INTERPOL warns of 'Metacrime'. [Link](#)
- Port scanning and legality. [Link](#)
- Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system. [Link](#)
- How a Group of Israel-Linked Hackers Has Pushed the Limits of Cyberwar. [Link](#)

- Leaks and Revelations: A Web of IRGC Networks and Cyber Companies. [Link](#)
- Move Over, APTs: Cybercriminals Now Target Critical Infrastructure Too. [Link](#)
- Russia's strategic culture drives its foreign hacking. [Link](#)
- Another US government agency account hacked - this time on Facebook. [Link](#)
- Georgia's largest county confirms cyberattack causing widespread issues. [Link](#)
- Bucks County Computer-Aided Dispatch System Crippled By Cyberattack. [Link](#)
- December cyberattack on Chicago community hospital claimed by LockBit gang. [Link](#)
- Energy giant Schneider Electric hit by Cactus ransomware attack. [Link](#)
- Italian Businesses Hit by Weaponized USBs Spreading Cryptojacking Malware. [Link](#)
- Ransomware gang demands €10 million after attacking Spanish council. [Link](#)
- Ransomware attack on US Navy shipbuilder leaked information of nearly 17,000 people. [Link](#)
- Ransomware gang targets nonprofit providing clean water to world's poorest. [Link](#)
- Energy giant Schneider Electric hit by Cactus ransomware attack. [Link](#)
- Ransomware attacks hospitalizing security [pros](#), as one admits suicidal feelings. [Link](#)
- NCSC Warns That AI is Already Being Used by Ransomware Gangs. [Link](#)
- Who pays, and why: A researcher examines the ransomware victim's mindset. [Link](#)

- Ransomware payments drop to record low as victims refuse to pay. [Link](#)
- Mother of all breaches reveals 26 billion records: what we know so far. [Link](#)
- Hackers breached Microsoft to find out what Microsoft knows about them. [Link](#)
- 23andMe data breach: Hackers stole raw genotype data, health reports. [Link](#)
- Texas-based care provider HMG Healthcare says hackers stole unencrypted patient data. [Link](#)
- Theft of Vancouver rape crisis centre server containing sensitive data raises privacy concerns. [Link](#)
- LoanDepot says 16.6M customers had 'sensitive personal' information stolen in cyberattack. [Link](#)
- Vans, Supreme owner VF Corp says hackers stole 35 million customers' personal data. [Link](#)
- Law firm that handles data breaches was hit by data breach. [Link](#)
- Documents belonging to the Swiss Air Force were leaked on the dark web as a result of cyberattack on a US security provider. [Link](#)
- List Containing Millions of Credentials Distributed on Hacking Forum, but Passwords Old. [Link](#)
- Binance Code and Internal Passwords Exposed on GitHub for Months. [Link](#)
- 750 million Indian mobile subscribers' data offered for sale on dark web. [Link](#)
- Cybercriminals stole \$1.7 billion from crypto funds in 2023 as attacks proliferated. [Link](#)
- 'Stablecoins' Enabled \$40 Billion in Crypto Crime Since 2022. [Link](#)

- North Korea's Cyber Heist: DPRK Hackers Stole \$600 Million in Cryptocurrency in 2023. [Link](#)
- Hundreds of Thousands of Dollars Worth of Solana Cryptocurrency Assets Stolen in Recent CLINKSINK Drainer Campaigns. [Link](#)
- Hackers steal \$112 million of XRP Ripple cryptocurrency. [Link](#)
- Burnout: Inferno Drainer's multimillion-dollar scam scheme detailed. [Link](#)
- How a Single 'Pig Butchering' Scam Netted \$40 Million. [Link](#)
- A Huge Scam Targeting Kids
- Feds say anti-robocall efforts appear to be working against foreign sources. [Link](#)
- "Scammers Paradise" –Exploring Telegram's Dark Markets, Breeding Ground for Modern Phishing Operations. [Link](#)
- FBI: Tech support scams now use couriers to collect victims' money. [Link](#)
- With Roblox and Fortnite 'Offers' Has Been Hiding in Plain Sight. [Link](#)
- The young people sifting through the internet's worst horrors. [Link](#)
- It's not just Taylor Swift: AI-generated porn is targeting women and kids all over the world. [Link](#)
- Three ways we can fight deepfake porn. [Link](#)
- Child Abusers Are Getting Better at Using Crypto to Cover Their Tracks. [Link](#)
- Hacker lassen fremde Facebook- und Instagram-Konten sperren. [Link](#)
- Sextortion training materials found on TikTok, Instagram, Snapchat and YouTube, according to new report. [Link](#)

- Nigerian 'Yahoo Boys' Behind Social Media Sextortion Surge in the US. [Link](#)
- Frantech Solutions and its relationship with pedophile networks. [Link](#)
- Search engines can act as one-click gateways to self-harm and suicide content. [Link](#)
- U.K. Regulator Calls Out Search Engines Over Access To Self-Harm Content. [Link](#)
- Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking. [Link](#)
- Anonymous Russia and 62IX groups have announced that they are now part of KillNet 2.0. [Link](#)
- The BlackForums project has stopped all its operations. The upcoming forum, utilizing the BlackForums database, will be named "SecretForums. [Link](#)
- Who is Alleged Medibank Hacker Aleksandr Ermakov? [Link](#)
- The Dark Web Secrets Uncovered by Elite Online Investigators. [Link](#)
- How The Dark Web Was Allowed To Thrive. [Link](#)
- "The Bank Robber Lurking Inside Your Web Browser. Darknet Diaries Ep. 111: Zeus". [Link](#)
- Hacker Conversations: HD Moore and the Line Between Black and White. [Link](#)
- Ransomware Diaries Volume 4: Ransomed and Exposed - The Story of RansomedVC. [Link](#)
- Cybernews podcast: "We break the law but for good reasons" - with hacker GhostExodus. [Link](#)

## DIGITAL INVESTIGATION AND DIGITAL EVIDENCE

- How a 27-Year-Old Codebreaker Busted the Myth of Bitcoin's Anonymity. [Link](#)
- The law enforcement operations targeting cybercrime in 2023. [Link](#)
- DOJ to up tempo of cybercrime operations in 2024, senior official says. [Link](#)
- International Collaboration Exposes Underage Cyber Fraudster in Morocco. [Link](#)
- Pentagon investigating theft of sensitive files by ransomware group. [Link](#)
- Fla. Man Charged in SIM-Swapping Spree is Key Suspect in Hacker Groups Oktapus, Scattered Spider. [Link](#)
- U.S. Officials Detained A 19-Year-Old SIM-Swap Hacker. [Link](#)
- U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure. [Link](#)
- FBI disrupts Chinese botnet by wiping malware from infected routers. [Link](#)
- Police Arrest Teen Said to Be Linked to Hundreds of Swatting Attacks. [Link](#)
- Ukrainian arrested for infecting US cloud provider with cryptomining malware. [Link](#)
- 'Asia's best hacker' caught. [Link](#)
- Brazilian police make arrests in Grandoreiro banking malware case. [Link](#)
- Nigerian hacker arrested for stealing \$7.5M from charities. [Link](#)

- International Collaboration Exposes Underage Cyber Fraudster in Morocco. [Link](#)
- ChatGPT-aided ransomware in China results in four arrests as AI raises cybersecurity concerns. [Link](#)
- DOJ charged 19 individuals in a transnational cybercrime investigation xDedic Marketplace. [Link](#)
- Feds Charge Alleged 'TLO' Underground Data Broker. [Link](#)
- Court charges dev with hacking after cybersecurity issue disclosure. [Link](#)
- French hacker from 'ShinyHunters' group sentenced to three years in US prison. [Link](#)
- Jailed BreachForums creator, admin sentenced to 20 years of supervised release. [Link](#)
- Russian National Sentenced for Involvement in Development and Deployment of Trickbot Malware. [Link](#)
- Canada's 'most prolific hacker' jailed for two years. [Link](#)
- DraftKings Hacker Sentenced to 18 Months Over \$600,000 Theft. [Link](#)
- Member of notorious international hacking crew sentenced to prison. [Link](#)
- Man Sentenced to Life in Prison for Running Child Sexual Abuse Material Website. [Link](#)
- CEO Sentenced for Transnational "Cherry-Picking" Scheme Involving Foreign Exchange and Cryptocurrency Futures Contracts. [Link](#)
- Lawyer gets 10-year sentence for laundering OneCoin scam proceeds. [Link](#)
- Nigerian national who laundered funds from romance and BEC scams gets 10-year sentence. [Link](#)
- Former Federal Employees Sentenced for Conspiracy to Steal Proprietary U.S. Government Software and Databases. [Link](#)



- DHS employees jailed for stealing data of 200K U.S. govt workers. [Link](#)
- United States, Australia, and the United Kingdom Sanction Russian Cyber Actor Responsible for the Medibank Hack. [Link](#)
- United States Settles Suit Against Lead Generator for Assisting and Facilitating Illegal Robocalls. [Link](#)
- Police Scotland welcome their latest recruit: SIM-card sniffer dogs. [Link](#)
- Countries tighten screws on biometric SIM registration amid rise in mobile phone fraud. [Link](#)
- Police must return phones after 175 million passcode guesses, judge says. [Link](#)
- Constitutionality of police using keyword warrants challenged in Pa. case. [Link](#)
- Maxwell's Lawyers Fought To Hide Search Terms. [Link](#)
- Cell tower data police say linked ex-CT cop to series of burglaries a concern for rights advocates. [Link](#)
- Post Office scandal furore is moment to change digital evidence rules. [Link](#)
- Celebrite donates AI investigative tools to nonprofits to help find missing children faster. [Link](#)
- Police 'investigate sexual abuse of young girl's avatar in the metaverse' - prompting NSPCC warning. [Link](#)
- Inside the Met Police's investigation into EncroChat crime gangs. [Link](#)
- Encrochat: The hacker with a warrant and fair trials? [Link](#)
- The Mystery of the \$400 Million FTX Heist May Have Been Solved. [Link](#)
- Vastaamo hacker traced via 'untraceable' Monero transactions, police says. [Link](#)
- Cartographic representation of the investigation. [Link](#)

- Deepfake voice attacks are here to put detection to the real-world test. [Link](#)
- Using Artificial Intelligence and Machine Learning to Identify Terrorist Content Online. [Link](#)
- Enforcement of EU law in the Area of Freedom, Security and Justice Policy. [Link](#)
- Must-Know Crypto Investigations of 2023: North America. [Link](#)
- Encrochat: The hacker with a warrant and fair trials? [Link](#)
- Encrypted Phone 'Sky' Linked to Murder-for-Hire Plot in Maryland. [Link](#)
- Fujitsu Bugs That Sent Innocent People to Prison Were Known 'From the Start'. [Link](#)
- EU countries share case studies on fighting child sexual abuse material. [Link](#)
- Amend or reject: joint statement on the UN Cybercrime Treaty. [Link](#)

# DIGITAL FORENSICS

- Forensic Technology: Algorithms Offer Benefits for Criminal Investigations, but a Range of Factors Can Affect Outcomes. [Link](#)
- OSAC And Standards In The Digital Evidence World. [Link](#)
- Memory Forensics - Practical Example, Detect Classic Remote Process Injection. [Link](#)
- Deep Dive into the Technical & Legal Complexities of Forensic Data Acquisition from Remote Cloud Storage. [Link](#)
- A first look at Android 14 forensics. [Link](#)
- Analysis of Android settings during a forensic investigation. [Link](#)
- Busting up Monopoly: Methods for modern darknet marketplace forensics. [Link](#)
- DFIR Next Steps: What To Do When You Find Mimikatz Was Run. [Link](#)
- New iShutdown Method Exposes Hidden Spyware Like Pegasus on Your iPhone. [Link](#)
- ChatGPT for digital forensic investigation: The good, the bad, and the unknown. [Link](#)
- Acquisition And Extraction With Cellebrite's New Endpoint Mobile Now And Mobile Ultra. [Link](#)
- Magnet GRAYKEY Supports Full Access For Google Pixel Series 6 And 8. [Link](#)
- Hacktivists Leak 1.7TB of Cellebrite, 103GB of MSAB Data. [Link](#)
- A comprehensive set of forensic resources for Android devices. [Link](#)

- DarkCool All Tools For Hacking Activity! List:~ Exploiter, Checker, Webshell Finder, Grabber, Searching, Bruteforce, Random, And Others Tools. [Link](#)
- YouVBeenHacked. A tool for searching and collection information. [Link](#)
- Ultimate-RAT-Collection. [Link](#)
- OSINVGPT - A Tool For Open-Source Investigations. [Link](#)
- N0rz3/Phunter: an OSINT Tool allowing you to find various information via a phone number. [Link](#)
- Uscraper - Powerful OSINT Webscraper For Personal Data Collection. [Link](#)
- Taranis AI - an advanced Open-Source Intelligence (OSINT) tool, leveraging Artificial Intelligence to revolutionize information gathering and situational analysis. [Link](#)
- Antisquat - Leverages AI Techniques Such As NLP, ChatGPT And More To Empower Detection Of Typosquatting And Phishing Domains. [Link](#)
- DomainTrail is a fast subdomain enumeration tool that uses effective passive and active techniques. [Link](#)
- Airgorah - A WiFi Auditing Software That Can Perform Deauth Attacks And Passwords Cracking. [Link](#)
- AutomatedEmulation - An automated Breach and Attack Simulation lab with terraform. Built for IaC stability, consistency, and speed. [Link](#)
- Malware and cryptography 24: encrypt/decrypt file via Madryga. Simple C/C++ example. [Link](#)
- Pmkidcracker - A Tool To Crack WPA2 Passphrase With PMKID Value Without Clients Or De-Authentication. [Link](#)
- learn-evm-attacks - Learn & Contribute on previously exploited vulnerabilities across several EVM projects. [Link](#)

- AI Exploits: A collection of real world AI/ML exploits for responsibly disclosed vulnerabilities. [Link](#)

## DIGITAL SURVEILLANCE VS. PRIVACY

- There's So Much Data Even Spies Are Struggling to Find Secrets. [Link](#)
- Der Bund überwacht uns alle. [Link](#)
- LEAK: EU Commission mulls options for boosting R&D in dual-use technologies. [Link](#)
- EU Commission launches bid to expand funding of dual-use research in Horizon Europe's successor. [Link](#)
- Germany demonstrates passive radar system using Starlink satellite radiation. [Link](#)
- Satellites: Our invisible infrastructure. [Link](#)
- Drone incidents and misuse: legal considerations. [Link](#)
- Police Drone Footage is Not Categorically Exempt From California's Public Records Law. [Link](#)
- Identifying Small Drones from Screenshots and Displays. [Link](#)
- EFF Unveils Its New Street Level Surveillance Hub. [Link](#)
- A geofence warrant typo cast a location dragnet spanning two miles over San Francisco. [Link](#)
- Police struggle to justify use of Fusus, a community surveillance tool they foisted on citizens. [Link](#)
- Is Your Local Police Department Using Fusus AI-Enabled Cameras? Find Out Here. [Link](#)
- Che intenzioni ha il governo per vigilare sull'intelligenza artificiale. [Link](#)
- Is Your Local Police Department Using Fusus AI-Enabled Cameras? Find Out Here. [Link](#)

- Il Garante sanziona Trento, telecamere e microfoni sparsi per la città allenavano il sistema di intelligenza artificiale. [Link](#)
- The Italian DPA announced it imposed a fine on a municipality for failing to comply the GDPR in the way it used AI in street surveillance projects. [Link](#)
- We Tested Europe's New Lie Detector For Travelers – And Immediately Triggered A False Positive. [Link](#)
- Predictive Policing In France: Against Opacity And Discrimination, The Need For A Ban. [Link](#)
- Cops Used DNA to Predict a Suspect's Face—and Tried to Run Facial Recognition on It. [Link](#)
- FBI Agents Are Using Face Recognition Without Proper Training. [Link](#)
- Miami Police Used Clearview AI Facial Recognition in Arrest of Homeless Man. [Link](#)
- Lords question legality of police facial recognition. [Link](#)
- Facial recognition used after Sunglass Hut robbery led to man's wrongful jailing, says suit. [Link](#)
- Police draw up report on offences when evicting Lützerath: "Mud Wizard" allegedly also uncovered. [Link](#)
- Clearview AI founder Hoan Ton-That on weathering a global regulatory storm, and the road ahead. [Link](#)
- NIST in the spotlight for facial recognition standards; some say it's too much. [Link](#)
- Racial profiling, policing and immigration control. [Link](#)
- Exclusive: Thermo Fisher halts DNA collection kit sales in Tibet. [Link](#)
- US migration data demands are "challenging", say Norwegian authorities. [Link](#)
- Belgium defends tax data sharing with US. [Link](#)

- Nederlandse telefoons online stiekem te volgen: 'Extreem veiligheidsrisico'. [Link](#)
- Digitale Rasterfahndungen durch die US-Polizei. [Link](#)
- N.S.A. Buys Americans' Internet Data Without Warrants, Letter Says. [Link](#)
- NSA purchase of Americans' personal data from brokers is illegal, senator says. [Link](#)
- FTC Order Will Ban InMarket from Selling Precise Consumer Location Data. [Link](#)
- FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data. [Link](#)
- The Sad Truth of the FTC's 'Historic' Privacy Win. [Link](#)
- Biden Prepping Order to Stop Foreign Countries From Accessing Americans' Private Data: Report. [Link](#)
- Inside Biden's Secret Surveillance Court. [Link](#)
- Palantir's Momentum Hurt by Slowing Growth in Government Deals. [Link](#)
- Palantir Cofounder Joe Lonsdale Defends The Newly Public Data Mining Company Amid Ongoing Criticism. [Link](#)
- Palantir-Software: Bayerisches LKA soll Testbetrieb stoppen. [Link](#)
- German police categorise people with "phenotypes": Study sees "racist glasses". [Link](#)
- Portugal: New data retention law fails at the Constitutional court; Parliament will try for a third time. [Link](#)
- Inside a Global Phone Spy Tool Monitoring Billions. [Link](#)
- New ways that law enforcement spies: push notifications. [Link](#)
- Alert: iPhone Push Notifications Exploited Users Data - Security Research. [Link](#)



- Attack of the week: Airdrop tracing. [Link](#)
- China hat wohl Apples Airdrop-Protokoll "geknackt". [Link](#)
- iPhone, Android Ambient Light Sensors Allow Stealthy Spying. [Link](#)
- Court of Appeal strikes out Saudi Government case in Pegasus spyware claim brought by UK based dissident Ghanem Al-Masarir. [Link](#)
- Federal judge rejects NSO's effort to dismiss Apple's Pegasus lawsuit. [Link](#)
- Poland to probe previous government's spyware use. [Link](#)
- Judge Confirms Surveillance With Pegasus Against Journalist Carmen Aristegui; FGR Must Continue With Investigations. [Link](#)
- US judge rejects spyware slinger NSO's attempt to bin Apple lawsuit. [Link](#)
- In first for Togo, RSF identifies spyware on phones of two Togolese journalists. [Link](#)
- Encryption discussion during the 8 December trial: from myth to reality. [Link](#)
- Spain to declassify secret documents in 'Catalan Gate' scandal. [Link](#)
- Citizen Lab details ongoing battle against spyware vendors. [Link](#)
- Notorious Spyware Maker NSO Group Is Quietly Plotting a Comeback. [Link](#)
- EDPS Opinion 8/2024 on the Proposal for a Regulation amending Regulation (EU) 2021/1232 on a temporary derogation from certain ePrivacy provisions for combating CSAM. [Link](#)
- EU Ombudsman launches probe into Europol officials' alleged conflict of interest. [Link](#)

- Thorn brachte Chatkontrolle auch für andere Themen ins Spiel. [Link](#)
- EU-backed surveillance software for detecting child abuse has serious flaws, manufacturer admits. [Link](#)
- FBI recruits Amazon Rekognition AI to hunt down 'nudity, weapons, explosives'. [Link](#)
- Biometric surveillance options increase for US police. [Link](#)
- More Police Are Using Your Cameras for Video Evidence. [Link](#)
- Amazon of 2 minds with law enforcement deals - fleeing locally, selling federally. [Link](#)
- FBI recruits Amazon Rekognition AI to hunt down 'nudity, weapons, explosives'. [Link](#)
- Amazon Scraps Deal to Buy Maker of Roomba Amid Regulatory Scrutiny. [Link](#)
- Victory! Ring Announces It Will No Longer Facilitate Police Requests for Footage from Users. [Link](#)
- Amazon Under Fire for Selling Hidden Spy Cameras. [Link](#)
- Each Facebook User is Monitored by Thousands of Companies. [Link](#)
- Mark Zuckerberg apologizes to parents at Senate child safety hearing. [Link](#)
- Hi Meta, WhatsApp with privacy? [Link](#)
- Google Update Shows How Bard AI May Work With Your Messages App. [Link](#)
- Sharing is Not Always Caring: Delving Into Personal Data Transfer Compliance in Android Apps. [Link](#)
- Film Companies' Third Attempt to Obtain Reddit User Information Faces Opposition. [Link](#)
- EU AI Act will fail commitment to ban biometric mass surveillance. [Link](#)

- EU set to allow draconian use of facial recognition tech, say lawmakers. [Link](#)
- EDRi, Challenges ahead: European Media Freedom Act falls short in safeguarding journalists and EU fundamental values. [Link](#)
- Right to erasure: the general and indiscriminate storage of biometric and genetic data of persons convicted of criminal offences, until their death, is contrary to EU law, Judgment of the Court of Justice in Case C-118/22. [Link](#)
- Book. Digital Technologies and Public Procurement. [Link](#)

## CYBER SECURITY

- Statista Cyber Threat Report 2023. [Link](#)
- ThreatMon "2023 Global Threat Report". [Link](#)
- 2023 Adversary Infrastructure Report. [Link](#)
- The Mac Malware of 2023. [Link](#)
- A Victim of the Akira Ransomware. [Link](#)
- Akira Ransomware and exploitation of Cisco Anyconnect vulnerability CVE-2020-3259. [Link](#)
- Evolution of UNC4990: Uncovering USB Malware's Hidden Depths. [Link](#)
- Unmasking a Financial Services Intrusion: REF0657. [Link](#)
- Buzzing on Christmas Eve: Trigona Ransomware in 3 Hours. [Link](#)
- Older Leaks Re-Surfaces: LOCKBIT Imitator on Surface Web. [Link](#)
- Newly ID'ed Chinese APT Hides Backdoor in Software Updates. [Link](#)
- NSPX30: A sophisticated AitM-enabled implant evolving since 2005. [Link](#)
- Security Brief: TA866 Returns with a Large Email Campaign. [Link](#)
- New Python-based FBot Hacking Toolkit Aims at Cloud and SaaS Platforms. [Link](#)
- Compromised Routers Are Still Leveraged As Malicious Infrastructure To Target Government Organizations In Europe And Caucasus. [Link](#)
- Blackwood APT Group Has a New DLL Loader. [Link](#)

- 'Yet another Mirai-based botnet' is spreading an illicit cryptominer. [Link](#)
- Kasseika Ransomware Deploys BYOVD Attacks, Abuses PsExec and Exploits Martini Driver. [Link](#)
- Exploiting 0-click Android Bluetooth vulnerability to inject keystrokes without pairing. [Link](#)
- New TTPs observed in Mint Sandstorm campaign targeting high-profile individuals at universities and research orgs. [Link](#)
- New Docker Malware Steals CPU for Crypto & Drives Fake Website Traffic. [Link](#)
- The Underestimated Scourge Of Spoofing Attacks. [Link](#)
- This AI Chatbot is Trained to Jailbreak Other Chatbots. [Link](#)
- Virtual attack boxes meet hacktivism. [Link](#)
- Bugcrowd sees surge in vulnerability submissions, led by public sector. [Link](#)
- Zero-day, supply-chain attacks drove data breach high for 2023. [Link](#)
- CVE-2023-36025 Exploited for Defense Evasion in Phemedrone Stealer Campaign. [Link](#)
- Cutting Edge: Suspected APT Targets Ivanti Connect Secure VPN in New Zero-Day Exploitation. [Link](#)
- Cutting Edge, Part 2: Investigating Ivanti Connect Secure VPN Zero-Day Exploitation. [Link](#)
- Flying Under the Radar: Abusing GitHub for Malicious Infrastructure. [Link](#)
- Cryptocurrency Malware: The Hidden Threat Lurking on YouTube. [Link](#)
- How anti-fraud systems use explainable AI to protect the betting and gaming industry. [Link](#)

- Hackers discover way to access Google accounts without a password. [Link](#)
- NIST: No Silver Bullet Against Adversarial Machine Learning Attacks. [Link](#)
- AI is helping US spies catch stealthy Chinese hacking ops, NSA official says. [Link](#)
- Paraguay military warns of 'significant impact' of ransomware after attack on internet provider. [Link](#)
- CISA, FBI warns of Chinese-manufactured drones. [Link](#)
- The European Union Cybersecurity Certification (EUCC) explained. [Link](#)
- Age-old problems to sharing cyber threat info remain, IG report finds. [Link](#)
- For Ai Risk, 'The Real Answer Has To Be Regulation'. [Link](#)
- NWO publishes preliminary guidelines for the use of AI. [Link](#)
- The Necessity of Explainable AI (XAI) for Causal Explanations of AI-related harm - Deconstructing the 'Refuge of Ignorance' in the EU's AI Liability Regulation. [Link](#)
- Generative A.I. Regulation and cybersecurity. [Link](#)
- White House implements AI safety reporting mandate. [Link](#)
- CISA's Road Map: Charting a Course for Trustworthy AI Development. [Link](#)
- Federal agencies release cyber guidance for water sector after watchdog criticism. [Link](#)
- An EU Prime! EU adopts first Cybersecurity Certification Scheme. [Link](#)
- Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity. [Link](#)