



CCRS Bit

October 2023

CONTENTS

Cybercrime.....	2
Digital Investigation and Digital Evidence	8
Digital Forensics	11
Digital Surveillance vs. Privacy	14
Cyber Security.....	19

CYBERCRIME

- Living in a World of Cyber Threats and God Bots. [Link](#)
- From High Life Hackers to National Menace: The Rise and Fall of Digital Bandits 'ACG'. [Link](#)
- Hack, Leaks, and Revelations. [Link](#)
- Hacks and leaks, then and now. [Link](#)
- Nigerian Killer Bee Cybercrime Syndicate - Organized Criminal Enterprise Profile. [Link](#)
- FBI: Crippling 'Dual Ransomware Attacks' on the Rise. [Link](#)
- Lockbit ransomware gang demanded an 80 million ransom to CDW. [Link](#)
- Reichsadler Cybercrime Group unsuccessfully targets unpatched WS_FTP Server with ransomware. [Link](#)
- MGM Resorts Refused to Pay Ransom in Cyberattack on Casinos. [Link](#)
- Ransomware victims continue to pay up, while also bracing for AI-enhanced attacks. [Link](#)
- Void Rabisu Targets Female Political Leaders with New Slimmed-Down ROMCOM Variant. [Link](#)
- How Keyloggers Have Evolved From the Cold War to Today. [Link](#)
- LightSpy iPhone Spyware Linked to Chinese APT41 Group. [Link](#)
- SpyNote: Beware of This Android Trojan that Records Audio and Phone Calls. [Link](#)
- Hackers modify online stores' 404 pages to steal credit cards. [Link](#)

- New TetrisPhantom hackers steal data from secure USB drives on govt systems. [Link](#)
- Hundreds of malicious Python packages found stealing sensitive data. [Link](#)
- Plastic surgeries warned by the FBI that they are being targeted by cybercriminals. [Link](#)
- Hackers steal user database from European telecommunications standards body. [Link](#)
- Casio discloses data breach impacting customers in 149 countries. [Link](#)
- DNA testing service 23andMe investigating theft of user data. [Link](#)
- Hacker leaks millions more 23andMe user records on cybercrime forum. [Link](#)
- 23andMe scraping incident leaked data on 1.3 million users of Ashkenazi and Chinese descent. [Link](#)
- Database Mess Up: 7TB of Healthcare Data Leak Affects 12 Million Patients. [Link](#)
- A threat actor is selling access to Facebook and Instagram's police portal. [Link](#)
- Leaky platform at Chinese adult platform exposed sensitive info of 14 million users. [Link](#)
- Shadow PC warns of data breach affecting over 500,000 customers. [Link](#)
- Lazarus Group Targeting Defense Experts with Fake Interviews via Trojanized VNC Apps. [Link](#)
- Hackers that breached Las Vegas casinos rely on violent threats, research shows. [Link](#)
- Inside the deadly instant loan app scam that blackmails with nudes. [Link](#)

- Fraudsters target Booking.com customers claiming hotel stay could be cancelled. [Link](#)
- Hackers Target Robinhood Accounts in Cash Out Schemes. [Link](#)
- Chinese Scammers Use Fake Loan Apps for Money Laundering. [Link](#)
- “Darknet Dangers: How Scammers Leverage Stolen Info for Carding and Credit Card Fraud”. [Link](#)
- Amazon, Microsoft, and India crack down on tech support scams. [Link](#)
- Latest evolution of ‘pig butchering’ scam lures victim into fake mining scheme. [Link](#)
- Palestine crypto donation scams emerge amid Israel-Hamas war. [Link](#)
- The state of Cross-chain Crime. [Link](#)
- A cryptor, a stealer and a banking Trojan. [Link](#)
- Fantom Foundation hot wallet hacked for \$550K. [Link](#)
- Unveiling Lazarus: Bridging the Web2 to Web 3 with Access Control Breach. [Link](#)
- EtherHiding: Hackers create novel way to hide malicious code in blockchains. [Link](#)
- Hackers use Binance Smart Chain contracts to store malicious scripts. [Link](#)
- LastPass breach linked to theft of \$4.4 million in crypto. [Link](#)
- Tales from the crypto: how the Baltic states became the hub of money laundering and fraud. [Link](#)
- Record \$7 billion in crypto laundered through cross-chain services. [Link](#)
- North Korea's Lazarus Group Lauanders \$900 Million in Cryptocurrency. [Link](#)

- New Clues Suggest Stolen FTX Funds Went to Russia-Linked Money Launderers. [Link](#)
- Inside a \$30 Million Cash-for-Bitcoin Laundering Ring in the Heart of New York. [Link](#)
- Correcting the Record: Inaccurate Methodologies for Estimating Cryptocurrency's Role in Terrorism Financing. [Link](#)
- Exploring the Realm of Malicious Generative AI: A New Digital Security Challenge. [Link](#)
- What to know about new generative AI tools for criminals. [Link](#)
- Will Generative AI Kill the Nigerian Prince Scam? [Link](#)
- How generative AI is boosting the spread of disinformation and propaganda. [Link](#)
- A Chatbot Encouraged Him to Kill the Queen. It's Just the Beginning. [Link](#)
- Deepfake Porn Is Out of Control. [Link](#)
- How it feels to be a victim of deepfake pornography. [Link](#)
- The Peril of Child Identity Theft and How to Mitigate It. [Link](#)
- New Report: Child Sexual Abuse Content and Online Risks to Children on the Rise. [Link](#)
- Global Threat Assessment 2023: Assessing the scale and scope of child sexual abuse online. [Link](#)
- Paedophiles using AI to turn singers and film stars into kids. [Link](#)
- The AI-Generated Child Abuse Nightmare Is Here. [Link](#)
- An Analysis on Online Self-Harm & CSAM Cults: Part 1. [Link](#)
- An Analysis on Online Self-Harm & CSAM Cults: Part 2. [Link](#)
- People Use Find My iPhone For Long Distance Stalking—And There's Not Much Apple Can Do. [Link](#)

- Pro-Ukraine group says it took down Trigona ransomware website. [Link](#)
- Stayin' Alive - Targeted Attacks Against Telecoms And Government Ministries In Asia. [Link](#)
- Sophisticated MATA Framework Strikes Eastern European Oil and Gas Companies. [Link](#)
- Iran-backed hackers dwelled for 8 months in Mideast government's system, report says. [Link](#)
- Twitter glitch allows CIA informant channel to be hijacked. [Link](#)
- CIA exposed to potential intelligence interception due to X's URL bug. [Link](#)
- Hackers Target Company That Vets Police Data Requests for Tech Giants. [Link](#)
- Cyber Espionage, Winter Vivern attacks European government entities-Think Tank. [Link](#)
- Russia and China-linked hackers exploit WinRAR bug. [Link](#)
- Vietnamese Hackers Target U.K., U.S., and India with DarkGate Malware. [Link](#)
- Bangladeshi Hackers Paralyze Italian Airports: The Rise of Mysterious Team and Its Geopolitical Implications. [Link](#)
- Kazakhstan-associated YoroTrooper disguises origin of attacks as Azerbaijan. [Link](#)
- Why it is time to stop mocking - and underestimating - North Korea. [Link](#)
- China Threat Landscape: Meet the Typhoon. [Link](#)
- Navigating the Digital Frontier: Cyber Threats in the Israeli-Palestinian War. [Link](#)
- Israelis told to secure their home security cameras against hackers. [Link](#)

- 'Don't play with fire': Israeli hackers claim to have disabled Tehran electrical grid. [Link](#)
- Rules of engagement issued to hacktivists after chaos. [Link](#)
- Bringing Humanitarian Law to Cyber War. [Link](#)
- The Dark Roulette: A Timeline of Cyberattacks on Casinos. [Link](#)
- How North Korean Workers Tricked U.S. Companies into Hiring Them and Secretly Funneled Their Earnings into Weapons Programs. [Link](#)
- Kubikle. Episodes about cybercrime. [Link](#)

DIGITAL INVESTIGATION AND DIGITAL EVIDENCE

- Borders have always been artificial: Migration, data and AI. [Link](#)
- NSO, Israeli Cyber Firms Help Track Missing Israelis and Hostages. [Link](#)
- India disconnects 6.4 million 'fraudulent' phone connections with the help of facial recognition. [Link](#)
- El Cajon Police recovers 50 stolen cars in 3 months using license plate readers. [Link](#)
- La polizia italiana vuole utilizzare finti profili social per monitorare la rete. [Link](#)
- FinCEN Seeks to Impose Strict Surveillance Requirements onto Broadly Defined Class of 'Bitcoin Mixers'. [Link](#)
- The Week in Ransomware - October 20th 2023 - Fighting Back. [Link](#)
- One of the most destructive ransomware gangs is being taken down by law enforcement. [Link](#)
- Feds seize 17 web domains used by North Korean tech workers in fraud scheme. [Link](#)
- Westport Police Recover 3 Million Dollars' worth of Bitcoin. [Link](#)
- Binance Aids Royal Thai Police in Crackdown on Criminal Networks. [Link](#)
- Nigerian National Extradited to Nebraska to Face Fraud Scheme Charge. [Link](#)

- A joint international law enforcement investigation led to the arrest of a malware developer who was involved in the Ragnar Locker ransomware operation. [Link](#)
- Ex-Navy IT manager jailed for selling people's data on the dark web. [Link](#)
- Spanish police arrest 34 alleged cybercriminals for scamming operation. [Link](#)
- Hacker accused of breaching Finnish psychotherapy center facing 30,000 counts. [Link](#)
- Crypto Groups Gemini, Genesis, and DCG Sued for \$1.1 Billion 'Fraud'. [Link](#)
- Moldovan accused of running cybercrime marketplace to face charges in US. [Link](#)
- Boston Man Sentenced for Defrauding Victims of More Than \$1 Million Using Various Online Scams. [Link](#)
- NJ Man Hired Online to Firebomb, Shoot at Homes Gets 13 Years in Prison. [Link](#)
- 'Article 7' shockwaves, ByLock and beyond: unpacking the Grand Chamber's Yalçinkaya Judgment. [Link](#)
- Un juez investiga a la exdirectora del CNI por el espionaje a Aragón con Pegasus. [Link](#)
- Spanish court investigates ex-spy chief over alleged snooping on Catalans. [Link](#)
- The beginning of the "8 december" trial is also the judgement of the right to privacy and encryption. [Link](#)
- Rules On Seizures Of Laptops, Phones A 'Grey Zone', Experts Say Amid NewsClick Raids. Know What The Law Says. [Link](#)
- Colorado Supreme Court upholds search warrant in 2020 arson case that led to teenage suspects. [Link](#)
- Colorado Court OKs Use of Google Search Data in Murder Case. [Link](#)

- Town Repeatedly Surveilled Man's Yard With Drone Without a Warrant. [Link](#)
- Does the Rapid Deployment of Information to Police Improve Crime Solvability? A Quasi-Experimental Impact Evaluation of Real-Time Crime Center (RTCC) Technologies on Violent Crime Incident Outcomes. [Link](#)
- Neuberger: New global initiatives will include information sharing, ransomware payment tracking. [Link](#)
- Hackers in the Hague? The Prospects of Prosecuting International Cyber Crimes Before the ICC. [Link](#)
- +Δ: CyberEngineer & CyberDetective & CyberAdvisor, Cybercrimeology Podcast Episode. [Link](#)
- Practitioners' gaps and requirements, The [CYCLOPES - Cybercrime Law Enforcement Practitioners' Network](#) project, 2nd public available annual report for industry and academia. [Link](#)
- CYBERCRIME@COE UPDATE July - September 2023. [Link](#)
- Cybercrime Digest by C-PROC: 1 - 15 October 2023. [Link](#)
- CYCLOPES Project Newsletter: Autumn 2023. [Link](#)

DIGITAL FORENSICS

- The Registry Hives you may be MSIX-ING: Registry Redirection with MS MSIX. [Link](#)
- Forensics: Active Directory ACL investigation. [Link](#)
- Hunting for Leaked Cobalt Strike v4.9 servers. [Link](#)
- Investigating a Compromised Web Server. [Link](#)
- Hunting for Leaked Cobalt Strike v4.9 servers. [Link](#)
- Forensic Timeline of an IcedID Infection. [Link](#)
- From ScreenConnect to Hive Ransomware in 61 hours. [Link](#)
- Reflective call stack detections and evasions. [Link](#)
- .NET Assembly Obfuscation for Memory Scanner Evasion. [Link](#)
- Raze to the Ground: Query-Efficient Adversarial HTML Attacks on Machine-Learning Phishing Webpage Detectors. [Link](#)
- Delving into the Depths of NoSQL Injection: A Research Odyssey. [Link](#)
- Researchers Unveil ToddyCat's New Set of Tools for Data Exfiltration. [Link](#)
- FBI shares AvosLocker ransomware technical details, defense tips. [Link](#)
- Good Day Ransomware. [Link](#)
- The Final Curtain for Process Doppelganging: Unmasking the Defender. [Link](#)
- The Alarming Rise of Illegal Hidden Cameras: Uncovering Illegal Hidden Cameras With Criminal IP. [Link](#)
- Active Lycantrox infrastructure illumination. [Link](#)
- The outstanding stealth of Operation Triangulation. [Link](#)

- AI algorithm detects MitM attacks on unmanned military vehicles. [Link](#)
- An emulator for the Flipper Zero. [Link](#)
- "Unmasking the Godfather - Reverse Engineering the Latest Android Banking Trojan". [Link](#)
- ClearFake: a newcomer to the "fake updates" threats landscape. [Link](#)
- AI-Driven Code Adaptation: Revolutionizing Ransomware Trackers in the Darkweb. [Link](#)
- IoT forensics: Exploiting log records from the DAHUA technology CCTV systems. [Link](#)
- # Wireshark 4.0.9 has been released. [Link](#)
- Oxygen Forensic® Detective v.16.0.1 Is Out. [Link](#)
- GMDSOFT New Product Release Announcement 'MD-PLUG'. [Link](#)
- Passware introduced Device Decryption Add-on. [Link](#)
- Chainsaw - provides a powerful 'first-response' capability to quickly identify threats within Windows forensic artefacts such as Event Logs and the MFT file. [Link](#)
- Invictus-AWS - a Python script that will help automatically enumerate and acquire relevant data from an AWS environment. [Link](#)
- synacktiv/nord-stream - a tool that allows you to extract secrets stored inside CI/CD environments by deploying malicious pipelines. It currently supports Azure DevOps, GitHub and GitLab.
- Apepe - a Python tool developed to help pentesters and red teamers to easily get information from the target app. This tool will extract basic informations as the package name, if the app is signed and the development language. [Link](#)

- VTScanner - A Comprehensive Python-based Security Tool For File Scanning, Malware Detection, And Analysis In An Ever-Evolving Cyber Landscape. [Link](#)
- TEx - a Telegram Explorer tool. [Link](#)
- CovenantDecryptor - designed to decrypt the communication data of Covenant traffic. [Link](#)
- Obfuscation Detection -a Binary Ninja plugin to detect obfuscated code. [Link](#)
- AVET - an AntiVirus Evasion Tool. [Link](#)
- GreyNoise captures data on IPs that scan the internet and saturate security tools with internet noise. [Link](#)
- Detect Wi-Fi deauthentication attack using ESP8266 and receive notification on smartphone. [Link](#)
- Spoofy - Program That Checks If A List Of Domains Can Be Spoofed Based On SPF And DMARC Records. [Link](#)
- BlackHat MEA - All Forensic Challenge Writeup. [Link](#)
- Digital forensic vans a 'game-changer' for policing, says PDS. [Link](#)
- Unraveling Digital Mysteries: How AI Copilots can Revolutionize Digital Forensic Investigations. [Link](#)
- Mass. forensic firm finds planted documents on jailed Indian activists' computers. [Link](#)

DIGITAL SURVEILLANCE VS. PRIVACY

- Some new snippets from the Snowden documents. [Link](#)
- Don't Fall for the Intelligence Community's Monster of the Week Justifications. [Link](#)
- Why your data might already be on a Europol list. [Link](#)
- On thin ICE: Santa Clara County offered haven to undocumented while selling access to feds. [Link](#)
- Revealed: UK government keeping files on education critics' social media activity. [Link](#)
- The State of Chihuahua Is Building a 20-Story Tower in Ciudad Juarez to Surveil 13 Cities—and Texas Will Also Be Watching. [Link](#)
- EDPS finishes audit of Europol. [Link](#)
- TechScape: How police use location and search data to find suspects – and not always the right ones. [Link](#)
- ICE, CBP, Secret Service All Illegally Used Smartphone Location Data. [Link](#)
- Spies on wheels: how carmakers collect and then resell information. [Link](#)
- Drones and Data Protection by Agencia Española de Protección de Datos - AEPD. [Link](#)
- Cops Can Now Fly Drones From Anywhere In The World Using Just A Web Browser. [Link](#)
- Michigan junkyard case could change how government uses drones. [Link](#)
- Police in Canada look into tech that accesses your home security cameras. [Link](#)

- The Network Effect of Telecommunications Vulnerabilities for Location Disclosure. [Link](#)
- iLeakage Hackers Can Read Gmail On All 2020 Or Later iPhones And Macs. [Link](#)
- HTTPS Interception by a state actor in Germany. [Link](#)
- Sandvine Scraps Plan to Market Tool in US That Tracks Encrypted Messages. [Link](#)
- DDoS-ing client-side scanning. [Link](#)
- Undermining Democracy: The European Commission's Controversial Push for Digital Surveillance. [Link](#)
- Five member states must investigate spyware abuse, says PACE committee. [Link](#)
- How Europe became the Wild West of spyware. [Link](#)
- Global: 'Predator Files' spyware scandal reveals brazen targeting of civil society, politicians and officials. [Link](#)
- Operation Behind Predator Mobile Spyware Is 'Industrial Scale'. [Link](#)
- Spyware Companies Flourishing in Europe due to Ineffective Regulation. [Link](#)
- Mehr Spionage aus dem Homeoffice. [Link](#)
- Madagascar Drops Predator Spyware on Citizens in Watering Hole Attack. [Link](#)
- Amnesty International calls for investigation into spyware firm's Dublin office. [Link](#)
- Mercenary spyware: Defending against what's next. [Link](#)
- Chinese surveillance firm recommits to UK after new guidance. [Link](#)
- Face Scanning and the Freedom To "Be Stupid In Public": A Conversation with Kashmir Hill. [Link](#)

- UK government accused of 'vandalism' over abolishing biometrics safeguards. [Link](#)
- GAO Report Shows the Government Uses Face Recognition with No Accountability, Transparency, or Training. [Link](#)
- Discover the stupidity of AI emotion recognition with this little browser game. [Link](#)
- Hikvision Violates Pledge, Ethnic Minority Analytics In Latest Platform. [Link](#)
- Britain is 'omni-surveillance' society, watchdog warns. [Link](#)
- Major UK retailers urged to quit 'authoritarian' police facial recognition strategy. [Link](#)
- Predictive Policing Software Terrible At Predicting Crimes. [Link](#)
- The Repressive Power of Artificial Intelligence. [Link](#)
- Unchecked AI will lead us to a police state. [Link](#)
- AI Chatbots Can Guess Your Personal Information From What You Type. [Link](#)
- How the "Surveillance AI Pipeline" Literally Objectifies Human Beings. [Link](#)
- Large Language Models and Data Privacy. [Link](#)
- Inside Ohio's Controversial AI Crime Fighting Experiment. [Link](#)
- Outsourced & Automated: How AI Companies Have Taken Over Government Decision-Making. [Link](#)
- CIPL Publishes White Paper & Recommendations on Data Sharing Between Public & Private Sectors. [Link](#)
- Adtech Surveillance and Government Surveillance are Often the Same Surveillance. [Link](#)
- Why Big Tech, Cops, and Spies Were Made for One Another. [Link](#)

- Amazon's 'Neighborhood Watch' Might Be Turning Police Officers Into 'Reddit Moderators'. [Link](#)
- Accidental Spies: Amazon Ring Owners May Be Unknowingly Emailing Police. [Link](#)
- Amazon will use real user conversations to train Alexa's AI model. [Link](#)
- Yepic fail: This startup promised not to make deepfakes without consent, but did anyway. [Link](#)
- Face search company Clearview AI overturns UK privacy fine. [Link](#)
- An AI firm harvested billions of photos without consent. Britain is powerless to act. [Link](#)
- The Mimics of Punjab. Darknet Diaries Podcast Episode. [Link](#)
- Event summary: Encryption in the age of surveillance. [Link](#)
- Sovereign Immunity Is Alive and Well, Even After a Cyberattack. [Link](#)
- 23andMe hit with lawsuits after hacker leaks stolen genetics data. [Link](#)
- "Did I just riot when I was there with my camera?": Social media, riot tourism, and the participatory visuality of riots – A review of [I'm Just Here for the Riot](#) (2023), an ESPN documentary. [Link](#)
- The Growing Threat of Cybercrime Law Abuse: LGBTQ+ Rights in MENA and the UN Cybercrime Draft Convention. [Link](#)
- Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations. [Link](#)
- TorBrowser 12.5.6 no longer flagged by Windows Defender. [Link](#)
- Hacker Advocates Turning Tracking Tables on Law Enforcement. [Link](#)

CYBER SECURITY

- New Quantum Factoring Algorithm Notably Reduces RSA Cryptography Breach Times. [Link](#)
- New Marvin attack revives 25-year-old decryption flaw in RSA. [Link](#)
- Mathematician warns US spies may be weakening next-gen encryption. [Link](#)
- NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations. [Link](#)
- Mature Organisations Still a Security Horror Show. [Link](#)
- FortiGuard Labs Uncovers Series of Malicious NPM Packages Stealing Data. [Link](#)
- Lighting the Exfiltration Infrastructure of a LockBit Affiliate (and more). [Link](#)
- Sophisticated StripedFly Spy Platform Masqueraded for Years as Crypto Miner. [Link](#)
- NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations. [Link](#)
- Zero-days for hacking WhatsApp are now worth millions of dollars. [Link](#)
- A look at CVE-2023-29360, a beautiful logical LPE vuln. [Link](#)
- MacOS "DirtyNIB" Vulnerability. [Link](#)
- Thousands of Android devices come with unkillable backdoor preinstalled. [Link](#)
- Android TV Boxes Infected with Backdoors, Compromising Home Networks. [Link](#)

- Researchers warn of 100,000 industrial control systems exposed online. [Link](#)
- Critically close to zero(day): Exploiting Microsoft Kernel. [Link](#) streaming service
- Chromecookiestealer - Steal/Inject Chrome Cookies Over The DevTools Protocol. [Link](#)
- Critical 'ShellTorch' Flaws Light Up Open Source AI Users, Like Google. [Link](#)
- Supply Chain Attack Targeting Telegram, AWS and Alibaba Cloud Users. [Link](#)
- Over 10,000 Cisco devices hacked in IOS XE zero-day attacks. [Link](#)
- DarkGate malware spreads through compromised Skype accounts. [Link](#)
- Phishing for Primary Refresh Tokens and Windows Hello keys. [Link](#)
- QR Codes Used in 22% of Phishing Attacks. [Link](#)
- Hackers Exploit QR Codes with QRLJacking for Malware Distribution. [Link](#)
- The Fake Browser Update Scam Gets a Makeover. [Link](#)
- Researcher Reveals New Techniques to Bypass Cloudflare's Firewall and DDoS Protection. [Link](#)
- ClearFake: a newcomer to the "fake updates" threats landscape. [Link](#)
- Encrypted traffic interception on Hetzner and Linode targeting the largest Russian XMPP (Jabber) messaging service. [Link](#)
- Skype message threads hijacked to spread DarkGate malware. [Link](#)
- Abusing Active Directory Certificate Services - Part One. [Link](#)

- BlackCat Climbs the Summit With a New Tactic. [Link](#)
- CVE-2022-4908: SOP bypass in Chrome using Navigation API. [Link](#)
- "I Had a Dream" and Generative AI Jailbreaks. [Link](#)
- Sophisticated StripedFly Spy Platform Masqueraded for Years as Crypto Miner. [Link](#)
- Another InfoStealer Enters the Field, ExelaStealer. [Link](#)
- New iLeakage attack steals emails, passwords from Apple Safari. [Link](#)
- IZ1H9 Mirai campaign launches DDoS attacks on Linux-based routers. [Link](#)
- IZ1H9 Campaign Enhances Its Arsenal with Scores of Exploit. [Link](#)
- The Art of Concealment: A New Magecart Campaign That's Abusing 404 Pages. [Link](#)
- X-Force uncovers global NetScaler Gateway credential harvesting campaign. [Link](#)
- Largest-ever DDoS leverages zero-day vulnerability. [Link](#)
- Concerns grow as LockBit knockoffs increasingly target popular vulnerabilities. [Link](#)
- Breaking Fortinet Firmware Encryption. [Link](#)
- How I stole my colleague's OneDrive content and WiFi passwords using a fake iPhone cable and PowerShell. [Link](#)
- From Copacabana to Barcelona: The Cross-Continental Threat of Brazilian Banking Malware. [Link](#)
- ENISA Threat Landscape 2023. [Link](#)
- Google mitigated the largest DDoS attack to date, peaking above 398 million rps. [Link](#)
- How Cloudflare mitigated yet another Okta compromise. [Link](#)

- Signal debunks online rumours of zero-day security vulnerability. [Link](#)
- HTTP/2 Rapid Reset: deconstructing the record-breaking attack. [Link](#)
- Measures taken following the unprecedented cyber-attack on the ICC. [Link](#)
- The European Union and NATO intensify cooperation on addressing cyber threats. [Link](#)
- It's Time to Establish the NATO of Cybersecurity. [Link](#)
- EFF And Other Experts Join in Pointing Out Pitfalls of Proposed EU Cyber-Resilience Act. [Link](#)