CCRS Bit

December 2023

CONTENTS

Cybercrime

- Top 10 cyber crime stories of 2023. Link
- New cybercrime market 'OLVX' gains popularity among hackers. Link
- How Telegram Messenger Turned Into a Cybercrime Ecosystem. Link
- BidenCash darkweb market gives 1.9 million credit cards for free. Link
- Ransomware Gangs Use PR Charm Offensive to Pressure Victims. Link
- Why extortion is the new ransomware threat. Link
- More than $100 million in ransom paid to Black Basta gang over nearly 2 years. Link
- Seattle cancer center confirms cyberattack after ransomware gang threats. Link
- FBI: Play ransomware gang has attacked 300 orgs since 2022. Link
- 8220 Gang Targets Telecom and Healthcare in Global Cryptojacking Attack. Link
- Russian APT29 Hacked US Biomedical Giant in TeamCity-Linked Breach. Link
- Press and pressure: Ransomware gangs and the media. Link
- Cybercriminals Launched “Leaksmas” Event In The Dark Web Exposing Massive Volumes Of Leaked PII And Compromised Data. Link
- Fortune-telling website exposes 13M+ user records. Link

- Kroll reveals FTX customer info exposed in August data breach. Link
- October cyberattack leaked data of 14.7 million people, mortgage giant Mr. Cooper says. Link
- FBI: Play ransomware breached 300 victims, including critical orgs. Link
- 23andMe says hackers accessed ‘significant number’ of files about users’ ancestry. Link
- Data of over a million crypto exchange users exposed. Link
- Integris Health patients get extortion emails after cyberattack. Link
- Hackers steal customer data from Europe’s largest parking app operator. Link
- Fidelity National Financial subsidiary says 1.3 million affected by November cyberattack. Link
- Ukraine mobile network Kyivstar hit by 'cyber-attack'. Link
- Ukraine’s intelligence claims cyberattack on Russia’s state tax service. Link
- Russian APT28 Hackers Targeting 13 Nations in Ongoing Cyber Espionage Campaign. Link
- Volt Typhoon-Linked SOHO Botnet Infects Multiple US Gov't Entities. Link
- New Threat Actor 'AeroBlade' Emerges in Espionage Attack on U.S. Aerospace. Link
- How cybercriminals are using Wyoming shell companies for global hacks. Link
- Sellafield nuclear site hacked by groups linked to Russia and China. Link
- North Korean hackers stole anti-aircraft system data from South Korean firm. Link

- Curse of the Krasue: New Linux Remote Access Trojan targets Thailand. Link
- $10 million up for grabs in fight against North Korean hackers. Link
- Feds: Iran-linked hacking campaign a ‘clarion call’ for digital defenses. Link
- Israel-linked hacking group claims attack on Iranian gas pumps. Link
- When Predatory Sparrow Strikes: Israel-Iran Shadow War Awakens. Link
- UK and allies expose Russian intelligence services for cyber campaign of attempted political interference. Link
- 'Disrupt or destroy’: China-linked hackers have targeted U.S. infrastructure ‘to cause societal chaos,’ officials say — are your finances also vulnerable? Link
- Regulating transnational dissident cyber espionage. Link
- Navigating the Nuances of Intelligence: Balancing Between Security and Privacy. Link
- Civilian hackers blur the lines of modern conflict. Link
- Trafficking for cyberfraud an increasingly globalized crime, Interpol says. Link
- 7 Months Inside an Online Scam Labor Camp. Link
- Cybercrime Orgs Increasingly Use Human Trafficking to Staff Scam Mills. Link
- Examining emerging fraud facilitated by the internet through crime scripts. Link
- Annual Payment Fraud Intelligence Report: 2023. Link
- Europol identifies hundreds of e-commerce platforms used in digital skimming attacks. Link
- ChatGPT tool could be abused by scammers and hackers. Link

- How a mysterious crypto exchange used an insider trading scam to swipe $3m from wealthy victims. Link
- Beware: Scam-as-a-Service Aiding Cybercriminals in Crypto Wallet-Draining Attacks. Link
- Why there's no such thing as 'crypto crime'. Link
- Hackers stole $2 billion in crypto in 2023, data shows. Link
- Bitcoin ATM company Coin Cloud got hacked. Even its new owners don't know how. Link
- Crypto Hardware Wallet Ledger's Supply Chain Breach Results in $600,000 Theft. Link
- Crypto Country: North Korea's Targeting of Cryptocurrency. Link
- In Cambodia's 'underground' crypto economy, Tether becomes coin of choice for Chinese-linked activities. Link
- Ten new Android banking trojans targeted 985 bank apps in 2023. Link
- They Cracked the Code to a Locked USB Drive Worth $235 Million in Bitcoin. Then It Got Weird. Link
- Generative Artificial Intelligence: the impact on intellectual property crimes. Link
- A high school's deepfake porn scandal is pushing US lawmakers into action. Link
- a16z Funded AI Platform Generated Images That "Could Be Categorized as Child Pornography," Leaked Documents Show. Link
- Child Sex Abuse Material Was Found In a Major AI Dataset. Researchers Aren't Surprised. Link. Link
- How AI Is Shaping the Future of Cybercrime. Link
- Child Sex Abuse Material Was Found In a Major AI Dataset. Researchers Aren't Surprised. Link. Link

- How AI Is Shaping the Future of Cybercrime. Link
- Hacktivism and its impacts on mental health. Link
- Unlocking Digital Doors: On the Hacker Group That Told Congress They Could Take Down the Internet. Link
- Ace in the Hole: exposing GambleForce, an SQL injection gang. Link
- Leader of Russian hacktivist group Killnet 'retires,' appoints new head. Link
- Polish Hackers Repaired Trains the Manufacturer Artificially Bricked. Now The Train Company Is Threatening Them. Link
- Approaching stealers devs: Summary & refused talks. Link
- The Man Behind the Dark Web. Link
- On the Trail of the Fentanyl King. Link
- Meet Joe Biden's Favorite Hacker. Link
- What to expect when hackers get busted. Link
- What Happens to Hackers in Prison? Ghost Exodus. Link
- The psychology of internet trolls. Link
- Cybercrimeology EP 99. Hack Righter: Working together to make good things better. Dr. Rutger Leukfeldt from NSCR and Leiden University joins us to discuss the Hack_Right program reforming young criminals and the role of academics in analyzing the program. Link
- Darknet Diaries EP 140. Revenge Bytes. Link
- Smashing Security podcast EP351. Nuclear cybersecurity, Marketplace scams, and face up to porn. Link
- The Cybersecurity Defender's podcast EP82. Decrypting Darknet Diaries: A conversation with Jack Rhysider. Link
- Cybercrime and freedom of expression: discussion paper. Link

- Book. Hacks, Leaks, and Revelations: the Art of Analyzing Hacked and Leaked Data. Link
- Book. The Crypto Launderers: Crime and Cryptocurrencies from the Dark Web to DeFi and Beyond. Link

Digital Investigation and Digital Evidence

- Negotiating with LockBit: Uncovering the Evolution of Operations and Newly Established Rules. Link
- Cyber Robin Hoods and the wars on pirated software. Link
- The crypto use case of 2023: Law enforcement. Link
- ALPHV ransomware site outage rumored to be caused by law enforcement. Link
- Verizon Gave Phone Data to Armed Stalker Who Posed as Cop Over Email. Link
- Interpol's Operation HAECHI IV: Global Crackdown Nets 3,500 Cybercriminals and $300 Million in Seized Assets. Link
- Disrupting the gateway services to cybercrime. Link
- FBI disrupts Blackcat ransomware operation, creates decryption tool. Link
- FBI posts takedown notice on AlphV ransomware group's website. Link
- FBI warrant reveals 'confidential source' helped AlphV/Blackcat ransomware takedown. Link
- AlphV claims to have 'unseized' its darkweb domain from the FBI. What's happening? Link
- A Major Ransomware Takedown Suffers a Strange Setback. Link
- German police takes down Kingdom Market cybercrime marketplace. Link
- The Binance Crackdown Will Be an 'Unprecedented' Bonanza for Crypto Surveillance. Link
- Crypto Firms Help Take Down International 'Pig Butchering' Scam. Link

- U.S. and Allies Sanction Kimsuky Actors. Link
- UK sanctions nine linked to cyber trafficking in Southeast Asia. Link
- Treasury Targets DPRK’s International Agents and Illicit Cyber Intrusion Group. Link
- 39 suspects identified in major online child sexual abuse swoop in the Western Balkan region. Link
- 'This was a success': Local police catch scammers who showed up to victims' homes to collect cash. Link
- 3,500 arrested, $300M seized in global cybercrime crackdown. Link
- French authorities arrested a Russian national for his role in the Hive ransomware operation. Link
- US detains suspects behind $80 million 'pig butchering' scheme. Link
- Alleged LockBit operator to face new cybercrime charges in Canada. Link
- Alleged leader of Kelvin Security hacker gang arrested in Spain. Link
- 2 Russian intel officers charged with hacking into U.S. and British government agencies. Link
- US indicts alleged Russian hackers for years-long cyber espionage campaign against Western countries. Link
- Four U.S. Nationals Charged in $80 Million Pig Butchering Crypto Scam. Link
- A Spanish man accused of teaching North Korea how to evade US sanctions using cryptocurrencies faces 20 years in prison. Link
- Founder of Bitzlato Cryptocurrency Exchange Pleads Guilty in Money-Laundering Scheme. Link

- Smart Contract Breach: Hacker Cracks Code, Faces Justice. Link
- Ex-Amazon Engineer Pleads Guilty to $12.3 Million Hack. Link
- Russian Hacker Vladimir Dunaev Convicted for Creating TrickBot Malware. Link
- Prison for man who wiped bank's data after being fired for accessing porn in the office. Link
- Meet the cybercriminals of 2023: indicted, but not forgotten. Link
- Amazon sues REKK fraud gang that stole millions in illicit refunds. Link
- Silk Road’s 69,370 BTC Forfeiture Wins U.S. Court Approval. Link
- Read more on DailyCoin: https://dailycoin.com/silk-roads-69370-btc-forfeiture-wins-u-s-court-approval/
- Smartphones ‘game-changer’ in criminal cases – DPP. Link
- Utah’s Top Court Says Government Can’t Portray Refusals To Unlock Phones As Incriminatory. Link
- ICANN Launches Global Service to Simplify Requests for Nonpublic Domain Name Registration Data. Link
- A Devastating Blow to Child Protection: Meta Expands Encryption. Link
- The Government Shouldn’t Prosecute People With Unreliable “Black Box” Technology. Link
- Latest UN Cybercrime Treaty draft a ‘significant step in the wrong direction,’ experts warn. Link
- UN Cybercrime Convention calls EU values into question, civil society warns. Link

- Implementing the First Protocol to the Convention on Cybercrime on Xenophobia and Racism: Good practice study. Link
- Dissecting EU electronic evidence. 37th Chaos Communication Congress. Link
- Cyber Mercenaries: The Failures of Current Responses and the Imperative of International Collaboration. Link
- Establishing New Rules for Cyber Warfare. Link
- New guidance will help smaller hosting service providers to tackle terrorist content online. Link
- Darknet Diaries Ep. 103: Cloud Hopper: The Secret Message Hackers Left Deep Inside Their Malware. Link

Digital Forensics

- Validation of image stream hashing: A forensic method for content verification. Link
- Fast Flux 101: How Cybercriminals Improve the Resilience of Their Infrastructure to Evade Detection and Law Enforcement Takedowns. Link
- How Cyber Criminals Use Domain Generation Algorithms to Evade Detection. Link
- SMTP Smuggling Allows Spoofed Emails to Bypass Authentication Protocols. Link
- SMTP Smuggling – Spoofing E-Mails Worldwide. 37th Chaos Communication Congress. Link
- How to Analyze Malware's Network Traffic in a Sandbox. Link
- Apple's iPhone 15: Under the C. Hardware hacking tooling for the new iPhone generation. 37th Chaos Communication Congress. Link
- Einführung in Smartphone Malware Forensik: Wie man Stalkerware und Staatstrojaner auf Smartphones finden kann. 37th Chaos Communication Congress. Link
- Unlocking the Road Ahead: Automotive Digital Forensics. 37th Chaos Communication Congress. Link
- Back in the Driver's Seat: Recovering Critical Data from Tesla Autopilot Using Voltage Glitching. 37th Chaos Communication Congress. Link
- Combating the Rising Criminal Use of AI with Digital Intelligence. Link

- Leveraging AI and ML in OSINT: The Significance, Limitations, and Unique Advantages to Human Investigators. Link
- MediaTek Device Extraction With Boot ROM Interface Disabled. Link
- Picture Perfect: Using Screenshots And Screen Recording In Mobile Device Investigations. Link
- Has the user ever used the XYZ application? aka traces of application execution on mobile devices. Link
- iOS 17 Initial Access Support For Magnet GRAYKEY And Magnet VERAKEY. Link
- BFU Extraction Support From MSAB – Seeing Is Believing. Link
- Acquisition And Extraction With Cellebrite's New Endpoint Mobile Now And Mobile Ultra. Link
- Investigating A Malware Attack Using Binalyze AIR's Investigation Hub. Link
- Introducing Oxygen Forensic® KeyDiver – A Decryption Tool For Enhanced Digital Investigations. Link
- Digital Forensic Challenge Images (Datasets). Link
- Collection of forensic tools. Link
- ForensicMiner: PowerShell-based DFIR automation tool. Link
- goHackTools. Hacker tools on Go (Golang). Link
- Hacker Roadmap. A collection of hacking tools, resources and references to practice ethical hacking. Link
- Linpmem. A Physical Memory Acquisition Tool For Linux. Link
- Tamarin-C. iPhone 15 USB-C exploration tool. Link
- New Sources of Microsoft Office Metadata – Tool Release MetadataPlus. Link
- Darkus. An Onion websites searcher. Link

- Internet-OSINT. Link
- PacketSpy. Powerful Network Packet Sniffing Tool Designed To Capture And Analyze Network Traffic. Link
- IP Address Analysis in OSINT Investigations. Link
- CloakQuest3r. Tool for Uncovering the true IP address of websites safeguarded by Cloudflare & Others. Link
- HackBrowserData. Decrypt passwords/cookies/history/bookmarks from the browser. Link
- Automate email extraction with the Harvester. Link
- SOWEL (SOcmint Weaknesses Enumeration List). A collection SOCMINT techniques (password: osinterdam). Link
- Social-Media-OSINT-Tools-Collection. Link
- META Osint. Link
- ScrapedIn. Tool to scrape LinkedIn. Link
- Email2WhatsApp is a GoLang project aimed at OSINT. Link
- Whatsapp Spoofing impersonate of reply message. Link. Link
- Telegram Explorer V0.3.0. Link
- Pegasus Spyware easy scanner. Link
- Darknet Diaries Ep. 105 Secret Cells. Even If Your Phone's Encrypted, the Cops Found a Way In. Link

Digital Surveillance vs. Privacy

- Surveillance Self-Defense: 2023 Year in Review. Link
- State of Surveillance in 2023. Big Brother Watch Report. Link
- The Internet Enabled Mass Surveillance. A.I. Will Enable Mass Spying. Link
- Personal Data in the Cloud is Under Siege. End-to-end Encryption Is Our Most Powerful Defense. Link
- Expanding the Reverse Targeting Prohibition: A Back Door Repeal of 702? Link
- Civil society calls for an end to the expansion of EU's EURODAC database. Link
- House Judiciary easily clears bill to renew surveillance tools with warrant mandate. Link
- Atlanta police use Signal to discuss 'Cop City' amid outcry over transparency. Link
- New legislation gives government permission to snoop on your bank account. Link
- Emmanuel Macron Is Using the 2024 Olympics to Make France a Surveillance State. Link
- A year of surveillance in France: a short satirical tale by La Quadrature du Net: From the so-called Country of human rights to a surveillance State. 37th Chaos Communication Congress. Link
- UN travel surveillance system needs "pause and urgent review", says Special Rapporteur. Link
- The Navy Bought 'Global' Surveillance Data Through Adtech Company Owned by Military Contractor. Link

- Here's a Warrant Showing the U.S. Government is Monitoring Push Notifications. Link
- US senator: Govts spy on Apple, Google users via mobile notifications. Link
- Google will update Maps to prevent authorities from accessing location history data. Link
- Google Disrupts Geofence Warrants, Says (Most) Location Data Will Be Stored Locally. Link
- Google Just Denied Cops a Key Surveillance Tool. Link
- Did Google Just Defeat Every Geofence Warrant? Link
- Apple admits to secretly giving governments push notification data. Link
- Apple will no longer give police users' push notification data without a warrant. Link
- Meta defies FBI opposition to encryption, brings E2EE to Facebook, Messenger. Link
- Proton Mail founder vows to fight Australia's eSafety regulator in court rather than spy on users. Link
- When You Roam, You're Not Alone. Link
- The Autocrat in Your iPhone. Link
- Predator Files: How European spyware threatens civil society around the world. 37th Chaos Communication Congress. Link
- Intellexa and Cytrox: From fixer-upper to Intel Agency-grade spyware. Link
- Reining in Pegasus: The Oversight of the Spanish Intelligence Service in the Catalangate. Link
- Pegasus spyware trial implicating former president kicks off in Mexico. Link

- India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists. Link
- MEP Sophie in ‘t Veld stresses keeping spyware discussions in EU Parliament. Link
- Hardline EU governments in late push to legitimise surveillance of journalists. Link
- Bundesverwaltung setzt auf iPhone und iPad. Link
- Face Recognition Software Led to His Arrest. It Was Dead Wrong. Link
- A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations. Link
- Police across UK equipped with live facial recognition bodycams. Link
- Live facial recognition labelled ‘Orwellian’ as Met police push ahead with use. Link
- Clearview AI tops 40 billion reference images in facial recognition database. Link
- Clearview AI Settles Privacy Case Over Facial Recognition Data. Link
- Big Tech Is Exploiting the Mental Health Crisis to Monetize Your Data. Link
- Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework. Link
- UK Commissioner Who Pushed Controversial Facewatch Tech Leaves Post To… Work For Facewatch. Link
- Facial recognition surveillance in São Paulo could worsen racism. Link
- Problems in Argentina’s justice system exacerbated by public facial recognition: report. Link

- Judge declares Buenos Aires' fugitive facial recognition system unconstitutional. Link
- Book: Intelligence Oversight in Times of Transnational Impunity: Who Will Watch the Watchers? Link
- Surveillance technology and Artificial Intelligence. Link
- Responsible development can help harness AI advancements. Link
- Generative AI, Legitimate Interest and Reasonable Expectations of Privacy. Link
- ChatGPT Is Apparently a Great Surveillance Tool. Link
- Euroviews. EU governments' hypocrisy is on full display over dangerous police AI. Link
- EU: Lawmakers reluctant to stop EU companies profiting from surveillance and abuse through the AI Act. Link
- AI Act stumbles over provisional deal with biometrics among main culprits. Link
- A rights-free zone? Blanket national security exemption in AI legislation. Link
- Human rights protections…with exceptions: what's (not) in the EU's AI Act deal. Link
- The end of street anonymity — is Europe ready for that? Link
- CCTVs and the Criminal City. Link
- San Francisco to install 400 more license plate reading cameras. Link
- Creeping Road Traffic Surveillance in Latvia: Social and Legal Implications of Digital Policing Tools. Link
- This Week in Gear News: The NYPD Brings Robot Dogs Back. Link
- Fremont enlists drones as first responders. Link

- Polizeibefugnis: CDU und SPD in Hessen wollen digitale Wanzen im Wohnzimmer. Link
- Do You Want Mark Zuckerberg Snooping in Your Closet? Link
- Facebook and the fight for #opchildsafety. Link
- Cartels Are Using a Police Database to Track and Target Their Enemies. Link
- Hidden Cameras, GPS Data, and License Plate Readers: How the USPIS Tracks Down Mail Thieves. Link
- Major US pharmacies release customer prescription data to police without warrant. Link
- Cars have become computers on wheels — and police have easy access to their data. Link
- How Your New Car Tracks You. Link
- 'This should be illegal': Driver warns how new car owners can read your lips with 'super high tech' new rearview mirrors. Link
- Marketing Company Claims That It Actually Is Listening to Your Phone and Smart Speakers to Target Ads. Link
- Controversial clothes hook spy cameras for sale on Amazon. Link
- A Powerful Tool US Spies Misused to Stalk Women Faces Its Potential Demise. Link
- How Congress can rein in data brokers. Link
- The Information Commissioner's Office (ICO) has introduced a toolkit called "Data Sharing and the Law: Explained". Link
- Dutch Watchdog Sues Adobe Over Mass Collection of Citizen Data. Link

CYBER SECURITY

- CVE-Collector. Simple Latest CVE Collector. Link
- The rising tide of vulnerabilities…might be more predictable than you think. Link
- The sound of you typing on your keyboard could reveal your password. Link
- Researchers figure out how to bypass the fingerprint readers in most Windows PCs. Link
- Researchers discovered a lock screen bypass bug in Android 14 and 13 that could expose sensitive data in users' Google accounts. Link
- Hacking Android, macOS, iOS, and Linux through a Bluetooth vulnerability. Link
- New JaskaGO Malware Targets Mac and Windows for Crypto, Browser Data. Link
- BlueNoroff: new Trojan attacking macOS users. Link
- Warning for iPhone Users: Experts Warn of Sneaky Fake Lockdown Mode Attack. Link
- Russian Hackers' Lawsuit Reveals Weaknesses In Apple's iOS 16. Link
- Microsoft Warns of Kremlin-Backed APT28 Exploiting Critical Outlook Vulnerability. Link
- 15,000 Go Module Repositories on GitHub Vulnerable to Repojacking Attack. Link
- Fake WordPress security advisory pushes backdoor plugin. Link

- SpyLoan Android malware on Google Play downloaded 12 million times. Link
- Anti-Israel hacking campaign highlights danger of internet-connected devices. Link
- IDEMIA's Big Glitch: Critical Vulnerabilities Expose Biometric Terminals. Link
- Hackers Exploited ColdFusion Vulnerability to Breach Federal Agency Servers. Link
- Scalable Extraction of Training Data from (Production) Language Models. Link
- AI Chatbot Jailbreaks Reveal Private Data from OpenAI and Amazon. Link
- CVE-2023-50428: Bitcoin Core Client Vulnerability. Link
- The magic of sophisticated cyber attacks. Link
- In a first, cryptographic keys protecting SSH connections stolen in new attack. Link
- Infecting SSH Public Keys with backdoors. Link
- New 'NKAbuse' Linux Malware Uses Blockchain Technology to Spread. Link
- New Hacker Group 'GambleForce' Tageting APAC Firms Using SQL Injection Attacks. Link
- Agent Racoon Backdoor Targets Organizations in Middle East, Africa, and U.S. Link
- 'BattleRoyal' Hackers Deliver DarkGate RAT Using Every Trick. Link
- AD CS - New Ways to Abuse ManageCA Permissions. Link
- Hackers breach US govt agencies using Adobe ColdFusion exploit. Link
- Microsoft Warns of Malvertising Scheme Spreading CACTUS Ransomware. Link

- Obfuscation and AI Content in the Russian Influence Network "Doppelgänger" Signals Evolving Tactics. Link
- Iranian State-Sponsored OilRig Group Deploys 3 New Malware Downloaders. Link
- Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally. Link
- Microsoft: OAuth apps used to automate BEC and cryptomining attacks. Link
- Cybercriminals Exploit Travel Season with MrAnon Stealer Email Phishing. Link
- Operation Blacksmith: Lazarus targets organizations worldwide using novel Telegram-based malware written in DLang. Link
- CISA and Partners Release Advisory on Russian SVR-affiliated Cyber Actors Exploiting CVE-2023-42793. Link
- Attackers Exploit 6-Year-Old Microsoft Office Bug to Spread Spyware. Link
- Microsoft Warns of Storm-0539: The Rising Threat Behind Holiday Gift Card Frauds. Link
- Supply chain attack targeting Ledger crypto wallet leaves users hacked. Link
- New KV-Botnet Targeting Cisco, DrayTek, and Fortinet Devices for Stealthy Attacks. Link
- Chinese APT Volt Typhoon Linked to Unkillable SOHO Router Botnet. Link
- kbandla/APTnotes. Various public documents, whitepapers and articles about APT campaigns. Link
- Exposing The Cyber-Extortion Trinity - BianLian, White Rabbit, And Mario Ransomware Gangs Spotted In A Joint Campaign. Link

- USBSamurai — A Remotely Controlled Malicious USB HID Injecting Cable for less than 10$. Link
- Fighting Ursa Aka APT28: Illuminating a Covert Campaign. Link
- IBM. Hiding in the Clouds: Abusing Azure DevOps Services to Bypass Microsoft Sentinel Analytic Rules. Link
- Chameleon Android Trojan Offers Biometric Bypass. Link
- Researchers Unveal GuLoader Malware's Latest Anti-Analysis Techniques. Link
- Lazarus group log4j attacks spread new malware families. Link
- Blockchain dev's wallet emptied in "job interview" using npm package. Link
- Careless oversight of Linux SSH servers draws cryptominers, DDoS bots. Link
- Operation Triangulation: The last (hardware) mystery. Link
- Operation Triangulation: What You Get When Attack iPhones of Researchers. Link
- Unmasking the Tactics of a Stealthy Banking Malware Impacting Over 50K Users. Link
- gozi malware threat actor. Link
- Pivoting through a Sea of indicators to spot Turtles. Link
- SQL Brute Force leads to Bluesky Ransomware. Link
- Akira Ransomware. Link
- Trigona. Link
- Uncovering the “Serpent”. Link
- Analysis of North Korean Hackers’ Targeted Phishing Scams on Telegram. Link
- FakeSG campaign, Akira ransomware and AMOS macOS stealer. Link

- What it means — CitrixBleed ransomware group woes grow as over 60 credit unions, hospitals, financial services and more breached in US. Link
- Cyberattacks on UK Critical Infrastructure - A collection of reports and case studies to understand the threat landscape for UK critical infrastructure. Link
- Protect your organizations against QR code phishing with Defender for Office 365. Link
- Incident Response Playbook: Dark Web Breaches. Link
- CISA says US government agency was hacked thanks to ‘end of life’ software. Link
- The US Needs to Follow Germany's Attack-Detection Mandate. Link
- Accounting software provider Tipalti investigating alleged ransomware attack. Link
- Ransomware gang files SEC complaint over victim’s undisclosed breach. Link
- UK government risking ‘catastrophic ransomware attack,' parliamentary report warns. Link
- BushidoUK/Breach-Report-Collection. A collection of companies that disclose adversary TTPs after they have been breached. Link
- Conference slides. Link