Threatsploit Adversary Report

Edition-69 May - 2024

BRISKINFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

Introduction :

Dear Readers,

Welcome to the May 2024 edition of the Threatsploit Adversary Report, your comprehensive overview of the most pressing cybersecurity threats and vulnerabilities impacting industries across the globe. As organizations navigate through the complexities of digital transformations, the landscape of cyber threats continues to evolve with increasing sophistication and impact.

This month, we have catalogued a diverse range of security incidents, from the deployment of a Python backdoor exploiting a zero-day flaw in Palo Alto Networks' equipment, to a cunning social engineering attack aimed at gamers. Each entry in our report not only outlines the nature and mechanism of the attack but also delves into the root causes and potential preventative measures.

The cybersecurity community is witnessing a surge in attack vectors targeting various domains, including software development companies, the entertainment sector, and governmental bodies. These attacks highlight critical vulnerabilities such as unauthorized access, social engineering, and cyber extortion, underscoring the urgent need for robust security protocols and awareness.

Our goal with this report is to arm cybersecurity professionals, IT managers, and organizational leaders with the insights needed to fortify their defenses against these relentless threats. For each incident, we provide detailed descriptions, categorize the type of attack, and offer links to further resources for an in-depth understanding.

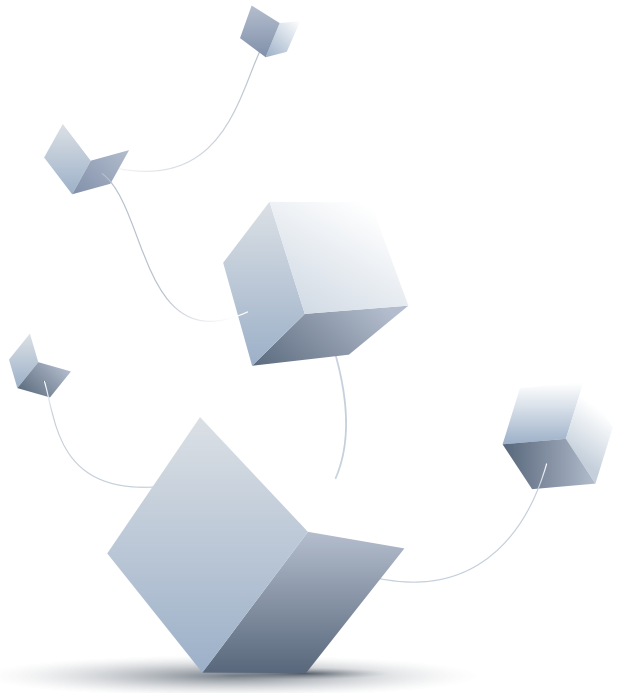
Stay informed and prepared with the Threatsploit Adversary Report as your essential guide to navigating the ever-changing cyber threat environment.

Best regards,

Briskinfosec Threat Intelligence Team.

Report Inside :

- ★ Top Cyberattacks in the Last 30 Days According to Industry
- ★ Top 5 YouTube Channels for Learning Cybersecurity
- ★ Top 5 Cybersecurity Case Studies



Hackers Deploy Python Backdoor in Palo Alto Zero-Day Attack

A zero-day flaw (CVE-2024-3400) in Palo Alto Networks PAN-OS enables remote code execution with root privileges, exploited in Operation Midnight Eclipse. Attackers use a cron job to fetch commands from a server, executing a Python backdoor on affected firewalls. UTA0218 threat actor orchestrates attacks, targeting edge devices to pivot into internal networks for data exfiltration. CISA adds the flaw to its Known Exploited Vulnerabilities catalog, urging patching by April 19.

Attack Type : Command Injection

Cause of Issue : Root Access

Domain Name : Software Development Companies

Fake cheat lures gamers into spreading infostealer malware

A new info-stealing malware linked to Redline masquerades as a game cheat named 'Cheat Lab,' enticing users to download it with promises of a free copy if they convince others to install it. McAfee researchers discovered the malware leveraging Lua bytecode to evade detection and establish persistence on infected systems. While it's associated with Redline, it doesn't exhibit typical Redline behaviors like stealing browser data. Distributed via ZIP files containing an MSI installer, the malware communicates with a command and control server, capturing screenshots and system info while awaiting commands. The infection method remains undetermined, highlighting the risk even from seemingly legitimate sources like Microsoft's GitHub.

Attack Type : Malware Distribution

Cause of Issue : Social Engineering

Domain Name : Media Entertainments

App Managing Student Devices In 127 Singapore Schools Hacked : Names And E-Mail Addresses Leaked

A data breach occurred in Singapore affecting 127 primary and secondary schools, compromising the names and email addresses of parents and teachers. The breach stemmed from unauthorized access to Mobile Guardian's user management portal, used to manage students' personal learning devices. MOE notified affected individuals and advised vigilance against phishing attempts. The breach impacted parents and staff members with access to device management functions.

Attack Type : Data Breach

Cause of Issue : Unauthorized Access

Domain Name : Media and Entertainment

Cyberattack Cripples Solano County Library Computer System

A cyberattack has crippled the Solano County library system, disabling computer services and threatening to release stolen data unless a $100,000 ransom is paid. The attack, possibly ransomware, has left library employees resorting to manual record-keeping. The county is investigating the incident, and there's no estimated timeline for system restoration.

Attack Type : Ransomware Attack

Cause of Issue : Cyber Extortion

Domain Name : Software Development Companies

Dutch Chipmaker Nexperia Falls Victim To Cyberattack

Nexperia, a Dutch chipmaker acquired by China's Wingtech, was targeted in a hacking attack in March 2024. The company disconnected affected servers from the internet and initiated an investigation with third-party specialists. While the extent of damage or losses is unclear, cyber criminals claimed to have stolen confidential data, including trade secrets and information about customers like Apple, Huawei, and SpaceX, demanding ransom on the dark web.

Attack Type : Data Breach

Cause of Issue : Unauthorized Access

Domain Name : Government Sector

German Database Company GBI Genios Hit By Ransomware, Systems And Website Down

GBI Genios, a database company used by media organizations in Germany, suffered a ransomware attack, rendering its servers unavailable. The Munich-based company's databases, widely used by universities and libraries, are inaccessible, causing disruptions to services. Affected organizations, including universities and libraries, await updates on when access will be restored.

Attack Type : Ransomware Attack

Cause of Issue : Server Unavailability

Domain Name : Media and Entertainment

Cyberattack Closes Swinomish Casino And Lodge In Ancortes, Wash

The Swinomish Casino & Lodge temporarily closes due to a cybersecurity incident, pending investigation by law enforcement and experts. Casino and restaurant facilities are shut down indefinitely, while the lodge and RV park remain open only for guests with existing reservations. Visitors are urged to monitor account statements for suspicious activity, with affected individuals to be contacted directly. Updates on system restoration will be provided on the casino's Facebook page.

Attack Type : Data Breach

Cause of Issue : Cyber Intrusion

Domain Name : Media and Entertainment

Panera Bread's Digital Outage Reportedly Blamed On Ransomware Attack

Panera Bread experienced a three-day digital outage in March due to a ransomware attack, which encrypted the company's virtual machines. The attack affected various digital channels, including the website, app, in-store kiosks, and employee access to loyalty programs and schedules. While Panera has not officially confirmed the cyberattack, cybersecurity site BleepingComputer.com reported on internal emails and unnamed sources linking the outage to ransomware. This incident highlights the growing threat of cyberattacks on businesses, especially those reliant on digital technology and customer data.

Attack Type : Ransomware Attack

Cause of Issue : Cyber Compromise

Domain Name : Automobile Industry

Taking a juice break? Your smartphone may be hacked if you're not careful

Juice-jacking is a hardware-based third-party attack where cybercriminals exploit USB charging stations to steal data from users' devices. By infecting the charging station or corrupting connection cables, attackers can extract sensitive information when users connect their devices. This threat emerged in 2011 and primarily targets USB ports and phone charging cables in public places. To protect against juice-jacking, users are advised to switch off devices while charging, avoid using public charging stations, frequently update devices, avoid pairing with unknown devices, and use passwords or PINs for added security.

Attack Type : Hardware Exploitation

Cause of Issue : Data Theft

Domain Name : Automobile Industry

Driving the future : Automotive cybersecurity in the era of connected vehicles

The automotive industry's embrace of cloud applications and software-defined functions promises enhanced convenience but raises cybersecurity concerns. Connectivity facilitates remote control and data management but also exposes vulnerabilities to cyber threats. Addressing these challenges requires a comprehensive approach, including stringent regulations, risk assessment, and implementation of cybersecurity solutions. Stakeholders must prioritize security measures to ensure a smooth and secure transition into the future of connected vehicles.

Attack Type : Remote Hijacking

Cause of Issue : Cyber Vulnerabilities

Domain Name : Automobile Industry

HelloKitty ransomware rebrands, releases CD Projekt and Cisco data

The ransomware operation formerly known as HelloKitty has rebranded itself as HelloGookie, with the threat actor 'Gookee/kapuchinO' claiming to be its original creator. To mark the rebranding, they released stolen data from previous attacks, including CD Projekt source code and Cisco network information. The leaked data includes decryption keys for older attacks and NTLM hashes from the Cisco breach. The move suggests a closer collaboration between HelloKitty and the Yanluowang ransomware group. It remains uncertain if HelloGookie will achieve the same success and notoriety as its predecessor.

Attack Type : Ransomware Rebranding

Cause of Issue : Rebranding Announcement

Domain Name : Software Companies

Russian APT Deploys New 'Kapeka' Backdoor in Eastern European Attacks

Kapeka, a new backdoor linked to the Sandworm APT group, has been detected in cyber attacks across Eastern Europe since mid-2022. It acts as an early-stage toolkit, providing persistent access to compromised systems. The malware disguises itself as a Microsoft Word add-in and communicates with a command-and-control server to execute various malicious functions. Kapeka's sophistication and connections to Sandworm suggest involvement in high-level cyber espionage activities.

Attack Type : Advanced Backdoor

Cause of Issue : APT Activity

Domain Name : Telecommunications Sector

GitHub comments abused to push malware via Microsoft repo URLs

Threat actors are exploiting a flaw in GitHub's file upload feature to distribute malware through URLs associated with Microsoft repositories, making the files appear legitimate. The flaw allows malicious files to be attached to comments on public repositories, creating convincing lures. Despite being alerted, GitHub and Microsoft have not responded, leaving the issue unresolved.

Attack Type : Malware Distribution

Cause of Issue : GitHub Flaw

Domain Name : Software Development Companies

Critical Forminator plugin flaw impacts over 300k WordPress sites

The Forminator WordPress plugin, used on over 500,000 sites, has critical vulnerabilities allowing unrestricted file uploads, SQL injection, and cross-site scripting attacks. Site admins are urged to update to version 1.29.3 immediately to mitigate the risks. Despite a security update, 320,000 sites remain vulnerable, posing a significant threat if left unpatched.

Attack Type : File Upload Vulnerability

Cause of Issue : Insufficient Validation

Domain Name : Software Development Companies

Microsoft : APT28 hackers exploit Windows flaw reported by NSA

"Microsoft warns of Russian APT28 using GooseEgg tool to exploit Windows Print Spooler vulnerability (CVE-2022-38028) for privilege escalation and data theft. The tool, deployed since June 2020, allows attackers to execute commands with SYSTEM-level privileges and drop malicious DLLs. APT28 has targeted government, NGO, education, and transportation sectors in Ukraine, Western Europe, and North America. Known for high-profile cyberattacks, APT28 has been linked to incidents including the DNC hack in 2016 and exploitation of Cisco router zero-days."

Attack Type : Privilege Escalation

Cause of Issue : Print Spooler

Domain Name : Government Sector

Researchers Detail Multistage Attack Hijacking Systems with SSLoad, Cobalt Strike

A cybersecurity research group, Securonix, discovered an ongoing phishing campaign named FROZEN#SHADOW, distributing SSLoad malware to organizations globally, primarily in Asia, Europe, and the Americas. SSLoad stealthily infiltrates systems, deploys backdoors, and gathers sensitive information for attackers. The campaign uses phishing emails containing malicious JavaScript files or macro-enabled Word documents to initiate infections. Once infected, SSLoad fetches and executes additional payloads like Cobalt Strike and ScreenConnect, granting attackers remote access and enabling credential theft. The attackers pivot through networks, potentially compromising domain controllers and establishing persistent access. This discovery coincides with reports of Linux systems being targeted by Pupy RAT.

Attack Type : Phishing Malware

Cause of Issue : Phishing Campaign

Domain Name : Software Development Companies

CoralRaider Malware Campaign Exploits CDN Cache to Spread Info-Stealers

A new malware campaign, linked to the CoralRaider group, has been distributing CryptBot, LummaC2, and Rhadamanthys stealers via CDN cache domains since February 2024. The campaign resembles CoralRaider's Rotbot tactics, using Windows Shortcut files and PowerShell scripts. Targets across various industries globally are likely accessed through phishing emails, leading to booby-trapped links. The campaign employs a CDN cache to store files and a PowerShell loader script to bypass UAC. Stealers gather sensitive data, with CryptBot featuring updated anti-analysis techniques and targeting password and authenticator apps.

Attack Type : Drive-by phishing

Cause of Issue : Malware Campaign

Domain Name : Software Development Companies

Akira Ransomware Gang Extorts $42 Million : Now Targets Linux Servers

Akira ransomware group has amassed $42 million by targeting 250+ victims globally since March 2023. They exploit Cisco flaws and other methods for access, encrypt using Chacha20 and RSA, and delete shadow copies. Similar to Conti, they now target Linux. LockBit gang's disruption prompts leader's efforts to regain credibility. Agenda ransomware evolves to target VMware infrastructure. "Junk-gun ransomware" offers low-cost options for individual profit without group affiliation.

Attack Type : Ransomware Infiltration

Cause of Issue : Ransomware Epidemic

Domain Name : Software Development Companies

ArcaneDoor hackers exploit Cisco zero-days to breach govt networks

Cisco has issued a warning about a state-backed hacking group exploiting zero-day vulnerabilities in Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) firewalls since November 2023. The campaign, dubbed ArcaneDoor, utilized two flaws (CVE-2024-20353 and CVE-2024-20359) to implant malware, including Line Dancer and Line Runner, enabling various malicious actions like reconnaissance and network traffic capture. The attackers manipulated device configurations and authentication settings, prompting a joint advisory from cybersecurity agencies. Cisco urges immediate software updates and vigilant monitoring for signs of compromise. Additionally, recent warnings highlight widespread brute-force attacks and guidance on mitigating VPN-related vulnerabilities.

Attack Type : Cyber-espionage campaign

Cause of Issue : Zero-day Vulnerabilities

Domain Name : Government Sector

WP Automatic WordPress plugin hit by millions of SQL injection attacks

Hackers are exploiting a critical vulnerability (CVE-2024-27956) in the WP Automatic plugin for WordPress, affecting versions before 3.9.2.0. This vulnerability allows them to create admin accounts and plant backdoors on targeted websites through SQL injection attacks. Over 5.5 million attack attempts have been observed since the disclosure. Hackers ensure long-term access by creating backdoors and obfuscating code, often renaming the vulnerable file "csv.php" and installing additional plugins. WPScan suggests checking for indicators of compromise and updating to version 3.92.1 or later to mitigate the risk, alongside regular site backups.

Attack Type : SQL Injection

Cause of Issue : Plugin Vulnerability

Domain Name : Software Development Companies

Health insurance giant Kaiser will notify millions of a data breach after sharing patients' data with advertisers

In a significant breach, U.S. health conglomerate Kaiser Permanente shared patients' data with third-party advertisers like Google and Microsoft. The leaked information includes member names, IP addresses, and browsing activity. Kaiser is notifying 13.4 million affected members and has removed tracking code from its platforms. This breach marks the largest health-related data breach of 2024 so far, triggering mandatory notifications to the U.S. Department of Health and Human Services and California's attorney general.

Attack Type : Data Breach

Cause of Issue : Third-party Sharing

Domain Name : Health Care Sector

India's ICICI Bank exposed thousands of credit cards to 'wrong' users

ICICI Bank, a top private bank in India, inadvertently exposed sensitive data of around 17,000 new credit cards to unintended recipients through its digital channels. The issue, discovered after customers raised concerns on social media, involved the iMobile Pay app revealing full card numbers and CVVs. The bank apologized for the inconvenience and assured compensation for any financial losses. They blocked the affected cards and are issuing replacements. The incident affected 0.1% of the bank's credit card portfolio. ICICI Bank, with over 6,000 branches in India and operations in 17 countries, has more than 28 million users of its iMobile Pay app since its launch in 2008.

Attack Type : Data Exposure

Cause of Issue : Data Mapping

Domain Name : Finance and Banking

UnitedHealth says Change hackers stole health data on 'substantial proportion of people in America'

UnitedHealth Group confirmed a ransomware attack on its subsidiary, Change Healthcare, resulted in the theft of Americans' private healthcare data, potentially affecting a substantial proportion of the population. The attack, carried out by the RansomHub gang, led to the publication of stolen data and a ransom payment by UnitedHealth. Change Healthcare previously paid $22 million to a Russian gang, ALPHV. The attack caused widespread outages in the healthcare system, costing UnitedHealth over $870 million. CEO Andrew Witty is scheduled to testify before House lawmakers on May 1.

Attack Type : Ransomware Attack

Cause of Issue : Data Theft

Domain Name : Health Care Sector

Omni Hotels says customers' personal data stolen in ransomware attack

Last month, Omni Hotels & Resorts experienced a ransomware attack where cybercriminals stole personal information, including names, email addresses, postal addresses, and loyalty program details of customers, but not financial data or Social Security numbers. Omni shut down its systems on March 29 after detecting intruders, causing widespread outages at its properties. Systems were restored on April 8. The ransomware gang responsible, Daixin, claimed to have taken 3.5 million customer records dating back to 2017 and threatened to leak them. The gang previously targeted U.S. healthcare organizations and hospitals.

Attack Type : Ransomware Attack

Cause of Issue : Cybersecurity Breach

Domain Name : Media and Entertainment

US says Russian hackers stole federal government emails during Microsoft cyberattack

"Russian government-backed hackers, known as ""Midnight Blizzard,"" stole emails from U.S. federal agencies through a Microsoft cyberattack.CISA issued an emergency directive for agencies to secure email accounts.Microsoft disclosed the attack in January, targeting corporate email systems.
Microsoft is working to remove hackers from its systems.
Earlier breaches in 2023 linked to China-backed hackers and Microsoft security failures.20,000 individuals' personal information exposed in 2023 due to an unprotected Microsoft cloud server."

Attack Type : Microsoft Email Breach

Cause of Issue : Cybersecurity Lapses

Domain Name : Government Sector

AT&T notifies regulators after customer data breach

AT&T has confirmed a security breach involving millions of customer records posted online. The leaked data includes personal information like names, email addresses, and Social Security numbers, affecting over 51 million people, including around 90,000 in Maine. The breach, dating back to mid-2019, was acknowledged three years after some data first appeared online. AT&T reset encrypted account passcodes after TechCrunch alerted them to the vulnerability. Identity theft and credit monitoring are being offered to affected customers, but the source of the leak remains unidentified.

Attack Type : Data Breach

Cause of Issue : Security Vulnerability

Domain Name : Telecommunications Sector

New Android Trojan 'SoumniBot' Evades Detection with Clever Tricks

A new Android trojan named SoumniBot has been discovered targeting users in South Korea. It employs three techniques to obfuscate its manifest file, making analysis challenging. Despite these tactics, the malware is detected by Google Play Protect. SoumniBot gathers sensitive data and can manipulate device settings, including hiding its own icon. Notably, it searches for digital certificates used in Korean banking services. This highlights a trend of malware creators seeking new methods to evade detection and infect devices.

Attack Type : Manifest Obfuscation

Cause of Issue : Data Theft

Domain Name : Government Sector

North Korea's Lazarus Group Deploys New Kaolin RAT via Fake Job Lures

In summer 2023, the Lazarus Group, associated with North Korea, used fabricated job offers to distribute a new RAT called Kaolin, targeting individuals in Asia. This RAT, besides typical functions, could alter file timestamps and load DLL binaries from a C2 server. It facilitated the deployment of the FudModule rootkit, exploiting CVE-2024-21338. The attack, known as Operation Dream Job, tricked victims into launching a malicious ISO file containing disguised files. These initiated an infection chain, eventually leading to the installation of RollSling malware. RollSling, executed in memory, served as a loader for RollMid, which established contact with C2 servers in a multi-stage process involving steganography. Eventually, Kaolin RAT was retrieved from the C2 server. Avast noted the complexity of the attack, emphasizing Lazarus Group's investment in innovation and resource allocation, posing a significant challenge to cybersecurity.

Attack Type : Advanced Persistent

Cause of Issue : Exploitation of Vulnerabilities

Domain Name : Government Sector

Major Security Flaws Expose Keystrokes of Over 1 Billion Chinese Keyboard App Users

The Citizen Lab uncovered security vulnerabilities in several cloud-based pinyin keyboard apps used by millions of Chinese mobile users. Weaknesses were found in apps from vendors like Baidu, Honor, iFlytek, OPPO, Samsung, Tencent, Vivo, and Xiaomi, potentially exposing users' keystrokes to hackers. These vulnerabilities allowed adversaries to decrypt keystrokes in transit or intercept plaintext data due to encryption flaws. Most developers addressed the issues, but concerns remain about app encryption standards and potential mass surveillance. Users are advised to update their apps and consider using on-device keyboard apps for better security.

Attack Type : Cryptographic Vulnerabilities

Cause of Issue : Encryption Flaws

Domain Name : Cloud-Based Software as a Service (SaaS) Providers

Hackers Exploit Fortinet Flaw, Deploy ScreenConnect, Metasploit in New Campaign

A recent cybersecurity campaign called Connect:fun exploits a critical SQL injection flaw (CVE-2023-48788) in Fortinet FortiClient EMS devices. Attackers target vulnerable systems, aiming to install ScreenConnect and Metasploit Powerfun payloads for post-exploitation activities. Forescout tracked the campaign, which targeted a media company after a proof-of-concept exploit release. The attackers, possibly active since 2022, manually select targets with VPN appliances. Similar incidents have been reported, prompting organizations to apply patches, monitor for suspicious activity, and use web application firewalls for protection.

Attack Type : SQL Injection

Cause of Issue : Vulnerable Devices

Domain Name : Software Development Companies

boAt Data Breach: Name, address, contact number, email ID of 75 lakh boat customers for sale at 2 euro

The boAt data breach exposes personal details of 7.5 million customers, posing serious risks of financial fraud and identity theft. Cybercriminals could exploit this data for phishing attacks and unauthorized transactions. Experts warn of dire consequences, including loss of customer trust and legal ramifications for the company. Security measures must be strengthened immediately to prevent further breaches. boAt, a leading audio products manufacturer, faces scrutiny over security lapses and the urgent need to restore customer confidence.

Attack Type : Data Breach

Cause of Issue : Security Weakness

Domain Name : Media Entertainments

Critical Update : CrushFTP Zero-Day Flaw Exploited in Targeted Attacks

A critical security flaw in CrushFTP versions below 11.1 allows attackers to escape the Virtual File System (VFS) and download system files, potentially leading to unauthorized access and remote code execution. Discovered by Simon Garrelou of Airbus CERT and actively exploited in targeted attacks, the vulnerability (CVE-2024-4040) enables attackers to bypass authentication and gain administrative access. Airbus CERT released exploit scanning tools, while Rapid7 highlights the ease of exploitation and the challenges in detecting malicious payloads. The U.S. CISA has listed the flaw in its Known Exploited Vulnerabilities catalog, mandating federal agencies to apply fixes by May 1, 2024.

Attack Type : File System Escape

Cause of Issue : Security Vulnerability

Domain Name : Software Development Companies

Ransomware Double-Dip : Re-Victimization in Cyber Extortion

A study looked at 11,000 organizations that experienced Cyber Extortion attacks and found that many were targeted more than once. This raised questions about why this happens. It could be because the attackers launch another attack, or they reuse stolen information, or they switch between different extortion schemes. The complexity of the cybercrime world and the desire for money drive these repeat attacks. By studying where victims are listed online, researchers saw that some were targeted multiple times, showing how Cyber Extortion attackers take advantage of opportunities. Understanding this helps organizations protect themselves better against these kinds of attacks.

Attack Type : Cyber Extortion

Cause of Issue : Repeat Victimization

Domain Name : Software Development Companies

Top 5 YouTube Channels for Learning Cybersecurity

www.briskinfosec.com

1. John Hammond

John Hammond is a well-known security researcher who creates informative and engaging videos on a variety of cybersecurity topics. His channel is a great resource for anyone who wants to learn more about the latest threats and vulnerabilities.

https://www.youtube.com/@_JohnHammond

2. David Bombal

David Bombal is a security expert who creates videos that are both informative and entertaining. He covers a variety of topics, including hacking, security tools, and social engineering. Bombal's videos are a great way to learn about the latest cybersecurity trends and how to protect yourself from cyberattacks.

https://www.youtube.com/@davidbombal

3. The Cyber Mentor

The Cyber Mentor is a channel that focuses on ethical hacking and penetration testing. The channel provides viewers with the knowledge and skills they need to identify and exploit vulnerabilities in computer systems. The Cyber Mentor's videos are a valuable resource for anyone who wants to learn more about offensive security.

https://www.youtube.com/@TCMSecurityAcademy

4. Briskinfosec

Briskinfosec has emerged as a valuable resource for anyone seeking to bolster their cybersecurity knowledge. Their channel stands alongside the best in the field, offering effective tips, best practices, and insightful tool tutorials.

https://www.youtube.com/@briskinfosec

5. NetworkChuck (by Ethan Banks)

This channel caters to a broad audience, from cybersecurity novices to experienced professionals. Banks utilizes his engaging personality and clear explanations to break down complex topics like network security, firewalls, and penetration testing. He frequently uses humor and real-world scenarios to make learning cybersecurity both informative and entertaining.

https://www.youtube.com/@NetworkChuck

Top 5 Cybersecurity Case Studies

1. Sony Pictures Entertainment Hack (2014)

The cyber attack on Sony Pictures Entertainment was a high-profile incident that involved the leak of sensitive data including personal information about Sony employees, emails, executive salaries, and unreleased films. The attackers, who called themselves the "Guardians of Peace," allegedly had ties to North Korea and launched the attack in response to the release of the film "The Interview," a comedy about a plot to assassinate North Korean leader Kim Jong-un.

Impact : The hack led to significant financial losses, damaged the company's reputation, and resulted in the resignation of top executives. It also sparked a major international incident involving the U.S. government accusing North Korea of orchestrating the attack.

https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea

2. Equifax Data Breach (2017)

Equifax, one of the largest credit bureaus in the U.S., suffered a massive data breach exposing the personal information of about 147 million consumers. The breach included Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers.

Impact : The breach had far-reaching consequences, leading to numerous lawsuits, the resignation of the CEO, and a complete overhaul of security practices at Equifax. It highlighted the vulnerabilities in the protection of personal data and the need for stricter cybersecurity measures in the financial sector.

https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

3. WannaCry Ransomware Attack (2017)

WannaCry was a global ransomware attack that affected over 200,000 computers across 150 countries. The malware encrypted data on the computers and demanded ransom payments in Bitcoin. It exploited vulnerabilities in older Microsoft Windows operating systems.

Impact : The attack caused significant disruptions in healthcare systems, banks, telecommunications, and other industries. It led to emergency patches from Microsoft and increased awareness of the importance of regular software updates and backups.

https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

4. NotPetya Malware Attack (2017)

Initially believed to be a ransomware attack, NotPetya was later identified as a more malicious cyber weapon aimed at destroying data. It spread through a Ukrainian tax software update and affected many global corporations, including Merck, Maersk, and FedEx.

Impact : NotPetya caused billions of dollars in damages and highlighted the risks of supply chain attacks where vulnerabilities in one vendor can compromise global networks.

Source Link : https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

5. Capital One Data Breach (2019)

A former AWS employee exploited a misconfigured web application firewall to access the personal information of approximately 106 million Capital One credit card holders and applicants. The data included names, addresses, phone numbers, credit scores, and transaction data.

Impact : The breach led to a settlement of $190 million for affected customers and raised concerns over cloud security and the protection of information in large-scale IT environments.

Source Link : https://www.cnet.com/personal-finance/capital-one-190-million-data-breach-settlement-today-is-deadline-to-file-claim/

Briskinfosec Technology and Consulting Pvt ltd,

No : 21, 2nd Floor, Krishnama Road,
Nungambakkam, Chennai - 600034, India.

Office : +044 4352 4537 | Mobile : +91 86086 34123
contact@briskinfosec.com | www.briskinfosec.com