Edition-63

Threatsploit

Adversary Report

BRISK INFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

Introduction :

In an era where technology dominates almost every facet of our lives, cyber threats continue to loom larger, evolving rapidly in their sophistication and impact. At Briskinfosec frequently underscores, understanding these threats is paramount. This month's Threatsploit report delves deep into the cyber landscape, uncovering patterns, exposing vulnerabilities, and providing insights into the most significant cyber incidents affecting various sectors. This report seeks to provide a holistic view of the prevailing trends, potential future developments, and the broader implications for businesses and individuals navigating this digital era.

Advanced Persistent Threats (APTs) : There's a noticeable uptick in sophisticated, long-term campaigns targeting specific entities or technologies. The evolution and persistence of these threats underscore the ever-growing need for advanced security measures.

Rise in Supply Chain Attacks : As businesses become more interconnected and reliant on third-party software, vulnerabilities within the supply chain are expected to become prime targets for adversaries.

Shift in Ransomware Tactics : The focus of ransomware attacks is predicted to shift from solely denying access to data to a more extortion-driven model, wherein stolen data becomes a leverage point for attackers.

Targeted Attacks on Digital Infrastructure : As more sectors digitize, there's an anticipated rise in targeted cyber-attacks on their evolving digital infrastructure,underscoring the need for proactive defense strategies.

The Dual-Faced Nature of Cyber Criminals :

Upside : The term might seem paradoxical, but the evolution in cyber criminality forces industries to innovate and strengthen security. Adversaries inadvertently push industries to adopt best practices, refine incident response strategies, and collaborate globally, making cyberspace safer over time.

Dark Side : On the other hand, cyber criminals are now more advanced, persistent, and unpredictable. Their adaptability to exploit new technologies, combined with the increasing connectivity of devices, presents amplified threats. Their tactics, be it data extortion or zero-day exploits, are becoming more diversified and damaging.

In the fluctuating tides of cyber warfare, knowledge remains our most potent weapon. The events of this month are not isolated incidents but pieces of a larger puzzle, revealing the state and direction of global cyber health. We must remain vigilant, adaptive, and united in our defense against these invisible adversaries.

Best regards,

Briskinfosec Threat Intelligence Team.

Contents :

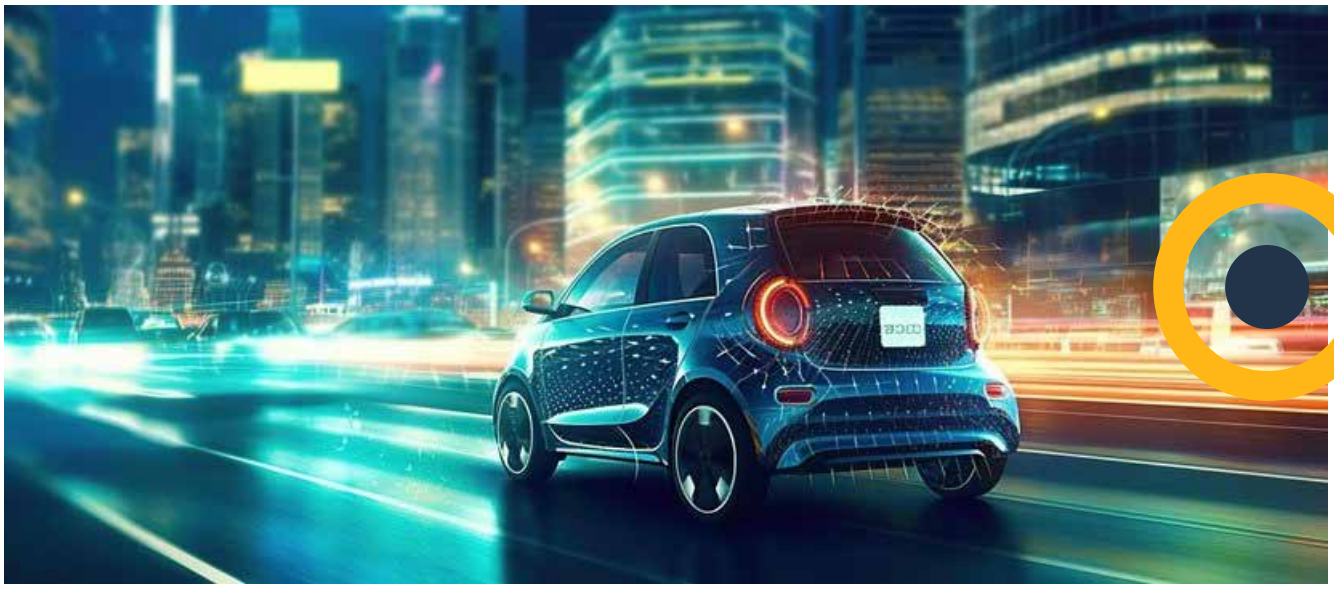
Car companies massively exposed to web vulnerabilities

Security researchers have uncovered a multitude of critical vulnerabilities within the web applications and APIs of major car manufacturers, telematics vendors, and fleet operators. These vulnerabilities span a range of threats, including information theft, account takeover, remote code execution (RCE), and even the ability to commandeer physical functions of vehicles, such as starting and stopping engines. This discovery suggests that the automotive industry, in its rush to introduce digital and online features, has neglected to adequately secure its online ecosystem. Specific instances of these vulnerabilities include poorly configured API endpoints in BMW and Rolls Royce systems, misconfigurations in Mercedes-Benz's single sign-on system, and multiple issues in Kia, Ferrari, Hyundai, Genesis, Honda, Nissan, Infiniti, Acura, and Spireon systems. These findings underscore the urgent need for improved security measures in the digital infrastructure of the automotive industry.

Attack Type : Vulnerabilities in Web Applications and APIs

Cause of Issue : Cyber Risks

Domain Name : Industrial Control Systems (ICS)



Indian transport ministry flaws potentially allowed creation of counterfeit driving licenses

Student and cybersecurity researcher Robin Justin discovered severe vulnerabilities in India's Ministry of Road Transport and Highways' Sarathi Parivahan website, which is used for driver's license applications. Justin found that attackers could access the personal information of potentially 185 million Indian citizens and even create counterfeit driving licenses. The vulnerabilities included broken access controls and missing authorization checks on the portal. By exploiting these issues, an attacker could obtain a person's name, address, date of birth, driving license number, and a photo, often with just an application number and date of birth.

Additionally, Justin discovered a poorly-secured one-time password system for a SYSADMIN account, which allowed him to access critical documents and process applications without verification checks. Despite reporting these vulnerabilities to India's Computer Emergency Response Team (CERT-IN), they received no immediate response. Eventually, the issues were resolved after Justin's reports, but CERT-IN's feedback was limited. The Ministry of Road Transport and Highways has not responded to inquiries about the matter.

Attack Type : Information Disclosure

Cause of Issue : Data Breach

Domain Name : Manufacturing and Industrial Control Systems (ICS)

Act Now : VMware Releases Patch for Critical vCenter Server RCE Vulnerability

VMware has released security updates to address a critical out-of-bounds write vulnerability (CVE-2023-34048) in vCenter Server, potentially leading to remote code execution. No workarounds are available, and updates are provided for various software versions, including vCenter Server 8.0, 7.0, and VMware Cloud Foundation. A patch is also offered for vCenter Server 6.7U3, 6.5U3, and VCF 3.x. Additionally, a partial information disclosure vulnerability (CVE-2023-34056) affecting vCenter Server is addressed, which could allow unauthorized data access by non-administrative users. While no active exploitation is known, VMware advises customers to promptly apply the patches to mitigate potential threats.

Attack Type : Remote Code Execution

Cause of Issue : Remote Code

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

iOS Zero-Day Attacks : Experts Uncover Deeper Insights into Operation Triangulation

Kaspersky has uncovered the TriangleDB implant, a tool used in a campaign called Operation Triangulation, targeting Apple iOS devices. This highly sophisticated attack utilized a zero-click exploit to compromise iOS devices and gather sensitive information. The attack began by exploiting two zero-day security flaws, gaining control over the device and user data through a malicious iMessage attachment. Kaspersky reports that the threat actor remains unidentified. The core of the attack is a backdoor named TriangleDB, deployed after obtaining root privileges through a kernel vulnerability. Before implanting TriangleDB, the attackers used JavaScript and Binary Validators to ensure the target device was not a research environment. These validators gathered device information to avoid detection. The attack leveraged a series of steps to obtain data, erase traces, check for jailbreak, and exfiltrate data to a command-and-control server. The attack affected both iOS and macOS systems, with actions encrypted and sent to the server for TriangleDB implant retrieval.

Attack Type : Zero-Click Exploit

Cause of Issue : iOS Exploits

Domain Name : iOS Industry Sector

1Password discloses security incident linked to Okta breach

1Password suffered a security incident linked to a breach in Okta's support system. Hackers used stolen credentials and gained unauthorized access. While 1Password reported the breach on September 29, Okta's logs indicate access occurred after 1Password's incident report. Both companies are working to address the situation, with 1Password enhancing security measures. The incident underscores the need for robust security practices and collaborative responses in the face of cyber threats.

Attack Type : Session Hijacking

Cause of Issue : Cookie Theft

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

University of Michigan employee, student data stolen in cyberattack

In August, the University of Michigan experienced a data breach where hackers gained unauthorized access to its network. The breach affected a wide range of individuals, including students, applicants, alumni, donors, employees, patients, and research study participants. The unauthorized access occurred from August 23 to 27. The compromised data included personal, financial, and medical information. This data breach prompted the university to isolate its entire campus network from the internet to mitigate the impact. Affected individuals were notified, and the university took steps to reset passwords for impacted accounts. The University of Michigan is a large and prestigious institution in the United States.

Attack Type : Unauthorized Network Access

Cause of Issue : Unauthorized Entry

Domain Name : Media and Entertainment

Signal Debunks Zero-Day Vulnerability Reports, Finds No Evidence

Signal denied reports of a zero-day flaw, finding no evidence to support the claim. The alleged vulnerability could provide complete access to mobile devices. It coincided with revelations that zero-days for messaging apps are being sold for high sums, targeting journalists and politicians. Amnesty International reported attempted spyware attacks using Predator, and commercial surveillance vendors aim to infect mobile devices through digital advertising networks.

Attack Type : Zero-Day Exploitation

Cause of Issue : Signal Exploit

Domain Name : Media and Entertainment

MOVEit vulnerability and data extortion incident

In the 2023 MOVEit hack, the Russian-affiliated ransomware group Clop targeted Progress Software's file-sharing tool. They exploited a previously unknown vulnerability in MOVEit, affecting up to 130 organizations. Unlike typical ransomware attacks, the focus was on data theft, compromising personal information of approximately 16 million individuals. The attackers could use this data for extortion or sell it on the dark web. The incident highlighted software supply chain security risks, as many companies rely on third-party software, making them vulnerable to supply chain vulnerabilities. The exploited vulnerability was a zero-day related to SQL injection, and hackers had known about it since 2021. This hack underscores the widespread impact of advanced cyberattacks on organizations and individuals.

Attack Type : Data Theft and Exploitation

Cause of Issue : SQL Injection Vulnerability

Domain Name : Software Industry

LAPSUS$: AN IN-DEPTH LOOK AT DATA EXTORTION GROUP

In March 2022, Lapsus$ emerged as a new threat actor, targeting prominent organizations, including Okta Inc., an authentication company. The group claimed to have had administrative access to Okta's internal systems for two months, initially leading to denials by Okta but later confirmed. Subsequently, several Lapsus$ members were arrested, revealing the group's substantial size. The group continued its cyberattacks, breaching companies like Globant in March 2022 and T-Mobile in April 2022, resulting in source code theft. This highlights the consequences of delayed disclosure in cybersecurity breaches and the evolving tactics of such threat actors.

Attack Type : Data Extortion

Cause of Issue : Data Breach

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

Critical Flaw in NextGen's Mirth Connect Could Expose Healthcare Data

Users of Mirth Connect, an open-source data integration platform, are advised to update to version 4.4.1 due to an unauthenticated remote code execution vulnerability (CVE-2023-43208). This flaw allows attackers to execute arbitrary commands and poses a significant risk to healthcare data. The vulnerability affects Mirth Connect versions dating back to 2015/2016 and is particularly concerning as it is an easy-to-exploit patch bypass for a previous critical vulnerability (CVE-2023-37679). The update is crucial, especially for publicly accessible instances, to mitigate potential threats to the healthcare industry.

Attack Type : Remote Code Execution

Cause of Issue : Mirth Connect Risk

Domain Name : Healthcare Industry

Nation State Hackers Exploiting Zero-Day in Roundcube Webmail Software

The threat actor Winter Vivern, associated with Belarus and Russia, exploited a zero-day flaw (CVE-2023-5631) in Roundcube webmail software to harvest email messages. This is a change from previously using known vulnerabilities. The attack involves phishing messages with Base64-encoded payloads, weaponizing a stored cross-site scripting flaw to load arbitrary JavaScript code in users' browsers. Despite a relatively unsophisticated toolset, Winter Vivern poses a persistent threat, especially to European governments, due to its regular phishing campaigns and organizations' failure to update vulnerable applications.

Attack Type : Zero-Day Exploitation

Cause of Issue : Winter Vivern Attack

Domain Name : Software Companies

Cisco Zero-Day Exploited to Implant Malicious Lua Backdoor on Thousands of Devices

Cisco has issued a warning about a zero-day flaw (CVE-2023-20273) in IOS XE actively exploited by an unknown threat actor, in combination with CVE-2023-20198, for privilege escalation and implant deployment. A fix will be available from October 22, 2023, but users are advised to disable the HTTP server feature temporarily. Over 36,000 compromised Cisco devices have been reported, making smaller entities and individuals the primary targets, with the vulnerabilities allowing attackers to gain remote access and control over affected systems. Cisco has released software updates for IOS XE software release train 17.9, with fixes for other versions in progress.

Attack Type : Zero-Day Exploitation

Cause of Issue : Cisco Privilege

Domain Name : Industrial Control Systems (ICS)

Google Play Protect Introduces Real-Time Code-Level Scanning for Android Malware

Google has updated its Play Protect service to include real-time code-level scanning, helping to detect new malicious apps before installation on Android devices. This enhancement improves protection against polymorphic apps that use various methods, including AI, to evade detection. The feature is rolling out in select countries, beginning with India. As threat actors find new ways to distribute Android malware, this update aims to bolster security. Additionally, Google has revised the Android Security Paper, offering an overview of the platform's proactive security measures.

Attack Type : Malicious App Detection and Prevention

Cause of Issue : Play Protect Enhancement

Domain Name : Software Development Companies

Google TAG Detects State-Backed Threat Actors Exploiting WinRAR Flaw

State-backed threat actors from Russia and China have exploited a recent security flaw in the WinRAR archiver tool (CVE-2023-38831) to execute arbitrary code when users attempt to view files in ZIP archives. Google TAG attributed these activities to clusters known as FROZENBARENTS (Sandworm), FROZENLAKE (APT28), and ISLANDDREAMS (APT40). These threat actors targeted government organizations in Ukraine, delivered commodity stealer malware, and launched phishing campaigns. The widespread exploitation of this vulnerability underscores the effectiveness of known exploit tactics, even when patches are available.

Attack Type : Zero-Day Exploitation and Phishing

Cause of Issue : WinRAR Exploits

Domain Name : Software Development Companies

Critical Vulnerabilities Uncovered in Open Source CasaOS Cloud Software

Two critical security flaws (CVE-2023-37265 and CVE-2023-37266) in the open-source CasaOS personal cloud software allowed attackers to bypass authentication requirements and gain full access to the CasaOS dashboard. The vulnerabilities also enabled the execution of arbitrary commands, potentially leading to persistent access and network pivoting. Responsible disclosure led to the flaws being addressed in CasaOS version 0.4.4. These vulnerabilities emphasized the risk of relying on IP address identification at the application layer and the need for robust security practice.

Attack Type : Arbitrary Code Execution

Cause of Issue : CasaOS Vulnerabilities

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

Signal Debunks Zero-Day Vulnerability Reports, Finds No Evidence

Signal, the encrypted messaging app, has refuted claims of a zero-day vulnerability, conducting an investigation that found no evidence to support the claim. They also checked with the U.S. government, which did not validate the claim. This comes as zero-days for messaging apps are sold at high prices, with such vulnerabilities being valuable to nation-state actors. Amnesty International reported spyware attacks targeting individuals and institutions, with a focus on deploying Predator, developed by the Intellexa alliance. Commercial surveillance vendors are also exploring the use of digital advertising networks to target and infect mobile devices globally.

Attack Type : Alleged Zero-Day Exploitation

Cause of Issue : Signal Analysis

Domain Name : Software Development Companies

U.K. Electoral Commission Breach Exposes Voter Data of 40 Million Britons

The U.K. Electoral Commission disclosed a significant cyberattack on its systems, revealing that the intrusion, which went undetected for over a year, allowed the threat actors to access extensive voter data for 40 million individuals. The incident, identified in October 2022, actually began in August 2021, with the attackers gaining unauthorized access to the Commission's servers, compromising email, control systems, and electoral registers containing voter data. The exposed information includes names, email addresses, home addresses, contact telephone numbers, and more. The delay in disclosing the breach was aimed at halting the adversary's access, investigating the breach's extent, and implementing security measures to safeguard against future attacks. While this breach does not impact the electoral process, individuals are advised to remain vigilant for unauthorized use of their personal data.

Attack Type : Complex Cyberattack

Cause of Issue : Unauthorized Access by Hostile Actors

Domain Name : Software Development Companies

Russian Hackers Use Zulip Chat App for Covert C&C in Diplomatic Phishing Attacks

The attack type involves phishing campaigns targeting ministries of foreign affairs in NATO-aligned countries, and it's attributed to Russian threat actors, particularly APT29 (aka Cozy Bear). These attacks use PDF documents with diplomatic lures to deliver the Duke malware, employing Zulip, an open-source chat application, for command and control to hide their activities behind legitimate web traffic. The cause is state-sponsored cyber espionage and reconnaissance targeting governments, political organizations, research firms, and critical industries, as well as an unknown adversary employing similar tactics to target Chinese-speaking users with Cobalt Strike. The domain "bahamas.gov[.]bs" is used in both intrusion sets, linking them further. This activity also coincides with recent warnings from the Computer Emergency Response Team of Ukraine about phishing attacks using a Go-based open-source post-exploitation toolkit called Merlin. Ukraine faces continuous cyber assaults from Sandworm, an elite hacking unit affiliated with Russian military intelligence, aimed at disrupting operations and gathering intelligence

Attack Type : Phishing Campaigns

Cause of Issue : Cyber Espionage

Domain Name : Software Development Companies

New QBot Banking Trojan Campaign Hijacks Business Emails to Spread Malware

A QBot malware campaign, active since April 4, 2023, is leveraging hijacked business correspondence to distribute the trojan, primarily targeting users in several countries. QBot, a long-standing banking trojan, steals data, acts as a backdoor, and facilitates further attacks such as Cobalt Strike or ransomware. It spreads through phishing campaigns and utilizes anti-detection techniques. The attackers employ email thread hijacking to trick victims into opening malicious attachments, often disguised as legitimate alerts from Microsoft Office 365 or Azure. When opened, these attachments lead to the download of QBot malware, which has been a prevalent threat in recent months. Elastic Security Labs has also uncovered a separate multi-stage social engineering campaign distributing Agent Tesla and XWorm via weaponized Microsoft Word documents.

Attack Type : Phishing

Cause of Issue : QBot Malware

Domain Name : Finance Sector

New QBot Banking Trojan Campaign Hijacks Business Emails to Spread Malware

A QBot malware campaign, active since April 4, 2023, is leveraging hijacked business correspondence to distribute the trojan, primarily targeting users in several countries. QBot, a long-standing banking trojan, steals data, acts as a backdoor, and facilitates further attacks such as Cobalt Strike or ransomware. It spreads through phishing campaigns and utilizes anti-detection techniques. The attackers employ email thread hijacking to trick victims into opening malicious attachments, often disguised as legitimate alerts from Microsoft Office 365 or Azure. When opened, these attachments lead to the download of QBot malware, which has been a prevalent threat in recent months. Elastic Security Labs has also uncovered a separate multi-stage social engineering campaign distributing Agent Tesla and XWorm via weaponized Microsoft Word documents.

Attack Type : Phishing Attack

Cause of Issue : QBot Malware

Domain Name : Finance Sector

Malvertising Campaign Targets Brazil's PIX Payment System with GoPIX Malware

Brazil's PIX instant payment system has attracted the attention of threat actors using a new malware called GoPIX. This campaign leverages malicious ads, particularly when users search for "WhatsApp web," employing a malvertising technique to serve links that lead to malware landing pages. Users who pass the fraud prevention check will be redirected to a fake WhatsApp download page, where they can download a malicious installer. The malware's primary purpose is to steal PIX payment requests and substitute them with an attacker-controlled PIX string. It also supports substituting Bitcoin and Ethereum wallet addresses. This campaign is one of several targeting users searching for messaging apps on search engines, with similar attacks seen in Hong Kong, Spain, and Mexico. Malware-as-a-Service offerings like Lumar are proliferating, making it easier for cybercriminals to conduct information-stealing attacks.

Attack Type : Malware Distribution

Cause of Issue : GoPIX Deception

Domain Name : Finance and Banking Sector

Over 9,500 Bank of Canton customers may have had personal information exposed due to data breach

A data breach involving Bank of Canton and its vendor Fiserv may have exposed personal information, such as account numbers and social security numbers, of approximately 9,540 customers, with the incident linked to a vulnerability in Fiserv's MOVEit Managed File Transfer software, despite no evidence of customer fraud. The bank is offering affected clients free identity protection services.

Attack Type : Data Breach

Cause of Issue : Fiserv Vulnerability

Domain Name : Banking Sector

Chilean telecom giant GTD hit by the Rorschach ransomware gang

Chile's Grupo GTD suffered a cyberattack, impacting its Infrastructure as a Service (IaaS) platform and disrupting various services, including data centers and internet access. The attack was confirmed to be a ransomware incident by Chile's Computer Security Incident Response Team (CSIRT), involving the Rorschach ransomware variant. The company disconnected its IaaS platform from the internet to prevent the attack's spread, leading to temporary outages. CSIRT is mandating public institutions using GTD's IaaS to report cybersecurity incidents, as per a government decree (No. 273). Some public services in Chile experienced unavailability on their websites due to the attack.

Attack Type : Ransomware Attack

Cause of Issue : GTD Telecom

Domain Name : Telecommunications

F5 Issues Warning: BIG-IP Vulnerability Allows Remote Code Execution

F5 has issued a critical security advisory regarding a vulnerability (CVE-2023-46747) in its BIG-IP system's configuration utility component, which could allow unauthenticated attackers with network access to execute arbitrary system commands, potentially leading to unauthenticated remote code execution. The affected versions of BIG-IP range from 13.1.0 to 17.1.0, and F5 has provided patches for various versions. Praetorian researchers who discovered the vulnerability recommend restricting access to the Traffic Management User Interface (TMUI) from the internet. This vulnerability marks the third unauthenticated remote code execution flaw in TMUI, with prior instances being CVE-2020-5902 and CVE-2022-1388. Mitigation measures have been provided by F5, including a shell script for specific versions of BIG-IP

Attack Type : Unauthenticated Remote Code Execution

Cause of Issue : BIG-IP Vulnerability

Domain Name : Software Companies

European govt email servers hacked using Roundcube zero-day

The Winter Vivern Russian hacking group has been exploiting a zero-day vulnerability in Roundcube Webmail to target European government entities and think tanks since at least October 11. This vulnerability allowed them to remotely inject arbitrary JavaScript code into targeted systems. ESET researchers discovered the attacks and promptly reported them. The cyberespionage group, also known as TA473, used phishing emails to deliver a first-stage payload that took advantage of the Roundcube email server vulnerability. The attacks aimed to harvest and steal emails from compromised webmail servers. Winter Vivern is known for targeting government entities worldwide, with a particular focus on nations like India, Italy, Lithuania, Ukraine, and the Vatican. The group's objectives align with the interests of the governments of Belarus and Russia, and it has been actively targeting Zimbra and Roundcube email servers owned by governmental organizations since at least 2022.

Attack Type : Email Compromise Attack

Cause of Issue : Roundcube Exploit

Domain Name : Software Development Companies

Critical OAuth Flaws Uncovered in Grammarly, Vidio, and Bukalapak Platforms

Critical security flaws have been disclosed in the Open Authorization (OAuth) implementations of online services like Grammarly, Vidio, and Bukalapak, potentially allowing malicious actors to hijack user accounts by exploiting weaknesses in token verification. These flaws could lead to identity theft, financial fraud, and unauthorized access to personal information, posing significant security risks for users of these services. Responsible disclosure has led to fixes by the affected companies.

Attack Type : Authentication Bypass

Cause of Issue : OAuth Weaknesses

Domain Name : Digital Platform

Mozilla Rushes to Patch WebP Critical Zero-Day Exploit in Firefox and Thunderbird

Mozilla released security updates to address a critical zero-day vulnerability (CVE-2023-4863) in Firefox and Thunderbird that was actively exploited in the wild. The flaw was a heap buffer overflow in the WebP image format, allowing arbitrary code execution when processing a specially crafted image. Google had also fixed the issue in its Chrome browser. The vulnerability had the potential to allow remote attackers to execute out-of-bounds memory writes via a crafted HTML page. Apple's Security Engineering and Architecture, along with the Citizen Lab at the University of Toronto, reported the issue. While specific details about the attacks are unknown, they likely targeted high-risk individuals, including activists and journalists. This underscores the importance of promptly updating software to mitigate such threats.

libcue Library Flaw Opens GNOME Linux Systems Vulnerable to RCE Attacks

A security flaw (CVE-2023-43641) in the libcue library on GNOME Linux systems has been revealed, potentially enabling remote code execution with a CVSS score of 8.8. The vulnerability is due to memory corruption in libcue, which parses cue sheet files. The flaw can be triggered by tricking a GNOME user into downloading a malicious .cue file from a malicious webpage. These files are automatically scanned by Tracker Miners, a default tool in GNOME, which employs libcue to parse the file, allowing for code execution. The specific technical details are intentionally withheld to give users time to apply updates. The ease of exploitation from seemingly innocuous libraries highlights the importance of prompt patching.

Attack Type : Remote Code Execution (RCE)

Cause of Issue : Memory corruption in the libcue library

Domain Name : Software Development Companies

Iranian Group Tortoiseshell Launches New Wave of IMAPLoader Malware Attacks

The threat actor known as Tortoiseshell is attributed to a series of watering hole attacks involving the deployment of IMAPLoader malware. This actor, associated with the Iranian regime, has been active since at least 2018 and is known for using compromised legitimate websites to distribute malware. These recent attacks, occurring between 2022 and 2023, primarily targeted the maritime, shipping, and logistics sectors in the Mediterranean. IMAPLoader, a .NET malware, was used in these attacks to download further payloads and communicate through email as a command-and-control channel. Tortoiseshell's activities also extended to phishing sites, particularly targeting the travel and hospitality sectors in Europe for credential harvesting.

Attack Type : Watering Hole Attacks

Cause of Issue : Tortoiseshell Threats

Domain Name : Industrial Control Systems (ICS)

HTTP/2 Rapid Reset Zero-Day Vulnerability Exploited to Launch Record DDoS Attacks

Amazon Web Services (AWS), Cloudflare, and Google have responded to record-breaking distributed denial-of-service (DDoS) attacks employing a novel technique called HTTP/2 Rapid Reset. These layer 7 attacks were discovered in late August 2023, using a zero-day flaw in the HTTP/2 protocol. HTTP/2 Rapid Reset attacks consist of multiple HTTP/2 connections with requests and resets in rapid succession, which can overwhelm a website's capability to respond to new incoming requests, causing it to go offline. While HTTP/2 is widely used, this attack highlights its vulnerability and the need for improved protection measures in web infrastructure

Attack Type : DDOs Attack

Cause of Issue : HTTP/2 Exploit

Domain Name : Cloud-Based (SaaS) Providers

New Attack Alert: Freeze[.]rs Injector Weaponized for XWorm Malware Attacks

Malicious actors are utilizing a legitimate Rust-based injector called Freeze[.]rs to deliver the XWorm malware in a novel attack chain. This attack was discovered by Fortinet FortiGuard Labs and involves a phishing email with a booby-trapped PDF file. The attack leverages the "search-ms" protocol to access a remote LNK file, which, when clicked, executes Freeze[.]rs and the SYK Crypter. Freeze[.]rs is an open-source red teaming tool used for payload creation and evading security solutions. SYK Crypter is a tool employed to distribute various malware families. This attack chain employs multiple layers of obfuscation and polymorphism to avoid detection. The final stage deploys the XWorm remote access trojan to harvest sensitive data and remotely control compromised devices. The attack targets Europe and North America. These findings highlight the rapid adoption of offensive tools by malicious actors. Additionally, another XWorm campaign was discovered, targeting service, transport, and healthcare sectors in multiple countries, using social engineering and heavily obfuscated payloads.

Attack Type : Advanced Persistent Threat (APT)

Cause of Issue : PDF Phishing

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

India's Aadhar breach alert : Millions of digital IDs leaked on dark web

Recent reports have exposed a shocking revelation about the biometric details of millions of Indian citizens linked to the Aadhaar system appearing on the Dark Web. Aadhaar, one of the world's largest biometric ID programs, has raised concerns about the security and reliability of its centralized system. While the Indian government has refuted claims of breaches, findings suggest a different narrative. Aadhaar not only serves as a digital ID but also plays a crucial role in electronic payments, online KYC verifications, and integration with various Indian financial platforms. The Election Commission of India has linked voter registration with Aadhaar for over 945 million Indians. Two threat actors have emerged on Breach Forums, claiming access to a vast database of Indian Aadhaar and passport records, presenting a significant risk of identity theft and financial fraud. The leakage of PII, including Aadhaar details, poses severe digital identity theft risks, making preventive measures crucial.

Attack Type : Data Breach

Cause of Issue : Security Vulnerability

Domain Name : Government Sector

Briskinfosec Technology and Consulting Pvt ltd,
No : 21, 2nd Floor, Krishnama Road,
Nungambakkam, Chennai - 600034, India.

For More Info Contact Us

Mobile : **+91 86086 34123**
Office : **+044 4352 4537**
E-Mail : **contact@briskinfosec.com**
Web : **www.briskinfosec.com**