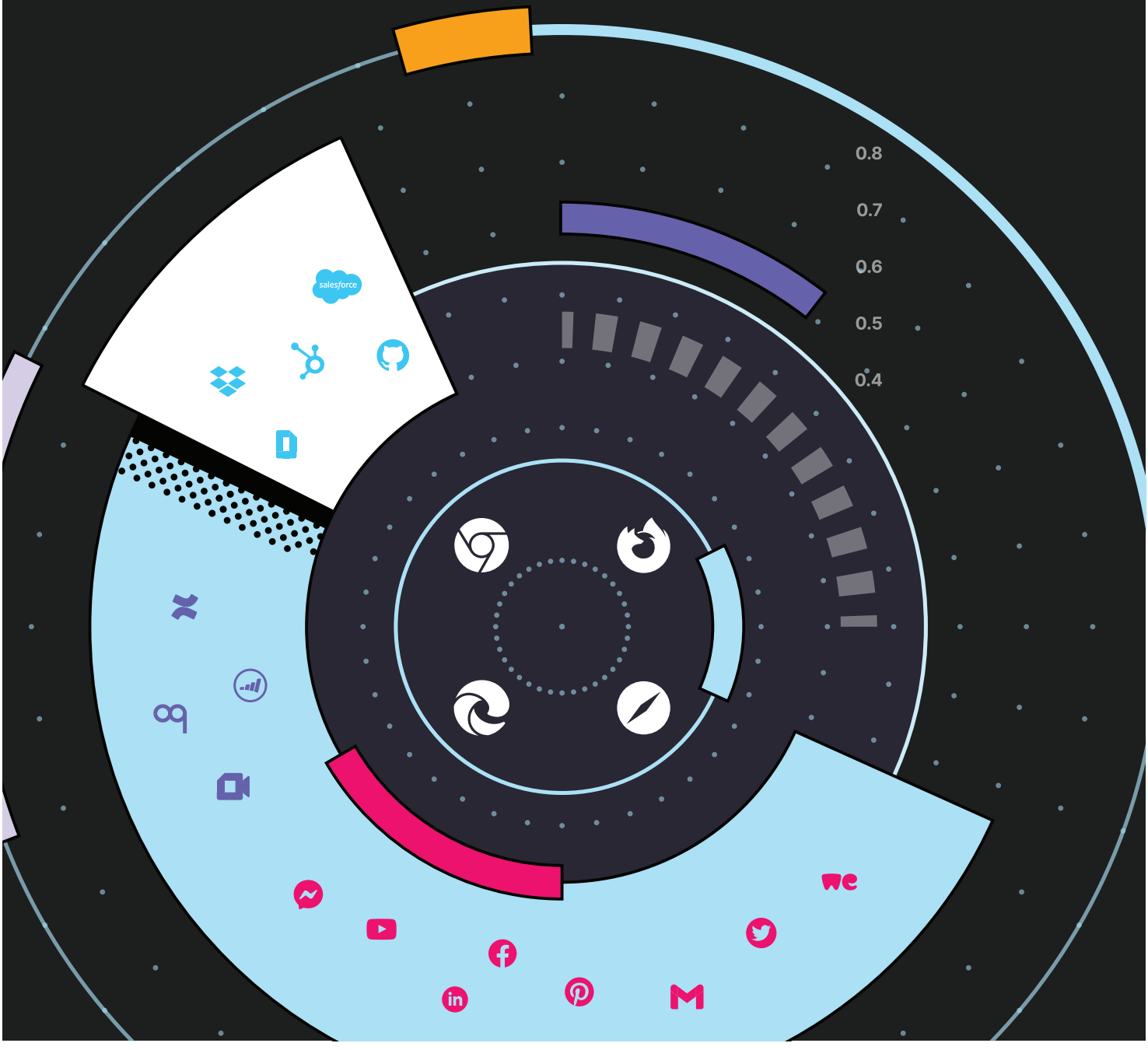
LayerX

BROWSER SECURITY
ANNUAL REPORT
2024



Executive Summary: If the Browser isn't Secure, Nothing is Secure

The browser has become the most prominent workspace in the modern enterprise. As a result, the browser is involved in almost any cyber attack. For account takeover attacks it's a means for malicious access to SaaS apps. For malicious extensions it's a source of sensitive data to steal. For phishing attacks it's the ultimate trap to lure users into disclosing their passwords, and so on and so forth.

Thorough insights into the browser threat landscape are essential for security decision makers. What are the most common browser-related attack vectors? How does data get exposed in web apps and GenAI tools? Clear answers to these questions are a prerequisite to planning and building a resilient security architecture that can keep devices, apps, and data secure from web-borne risks.

The LayerX Annual Browser Security Report provides you with the full picture of browser risks. Covering all key aspects of this space, from identity vulnerabilities to malicious extensions, this report empowers you with the knowledge of what browser risks matter. It includes a wealth of statistics, a zoom-in analysis of notable attacks, and an overview of the browser-related attack evolution across 2023.

Use the report to benchmark the security challenges of your environment. There's no one-size-fits-all – maybe phishing is the greatest risk you need to mitigate first or maybe it's least-privileged SaaS access from unmanaged devices. Compare what you learn from the report with the first-hand knowledge you have on the environment you're accountable for. By doing so, you'll be able to translate the data in the report to actual security actions.

Are you ready?
Let's start the journey now!

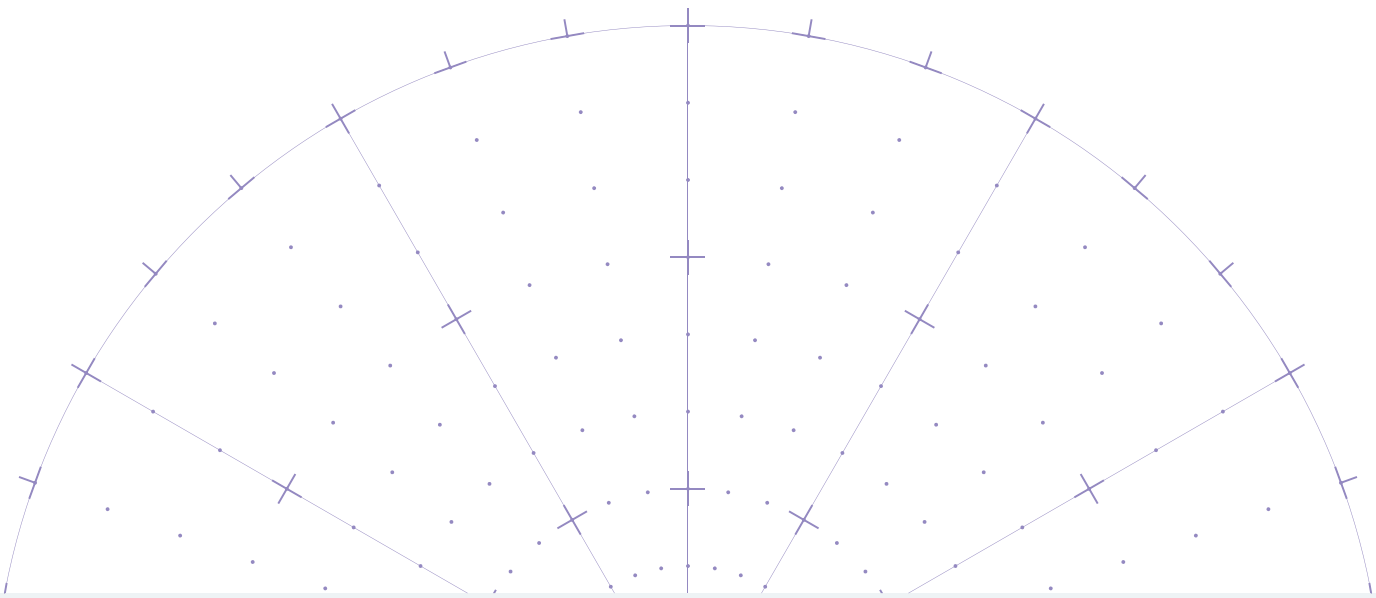


Table of Contents

Browser Security Risks in Hybrid Work Environments

What is the risk?

Hybrid work environments are at risk of employees using their own devices and personal browser profiles. These devices and profiles are not subject to the organization's security controls and are highly targeted by adversaries as a malicious entry point.

What is the root cause?

Flexibility in work arrangements incentivizes employees to use their own devices, as well as explore unvetted tools, creating critical security weaknesses. This is enhanced by the proliferation of shadow IT, wherein employees adopt unauthorized extensions and applications without any security governance.

45%

of All Browsers Within Corporate Devices are Personal Browser Profiles

62%

of the Workforce Uses Unmanaged Devices to Access Corporate Data

Personal Profile Browser Risks

Data leakage

Personal browser profiles are easy prey to insecure extensions, compromised bookmarks, and untrusted personal websites. This risk is well exemplified by incidents like the Okta Breach, where an employee logged into a personal Google account on a company-managed laptop, exposing credentials that led to the theft of data from multiple Okta customers.

Phishing

Personal browsing habits increase susceptibility to targeted attacks, posing risks to login credentials and critical systems. An example of such a phishing campaign was disclosed during August 2023, in which the free hosting service Cloudflare R2 was abused to distribute static phishing pages, mainly of Microsoft login credentials, Adobe, Dropbox, and other cloud apps.

Unmanaged Devices Browser Risks

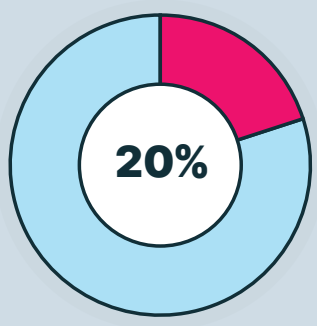
Data exfiltration

An employee that downloads sensitive data to an unmanaged device effectively takes it beyond the organization's data protection control and can easily expose it by uploading to a personal web destination.

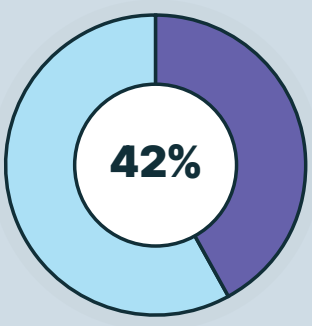
Account takeover

Unmanaged devices are not subject to the corporate's EDR protection. As a result, adversaries can easily compromise them and steal browser data, such as cookies and passwords.

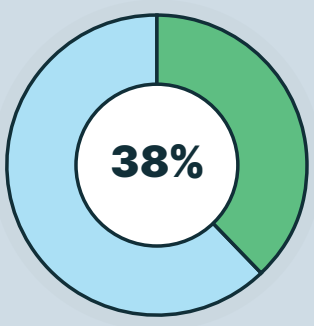
Unmanaged Devices are Key Enablers of Data Exfiltration and Account Takeover



Unmanaged Devices



Both Managed and Unmanaged



Managed Devices

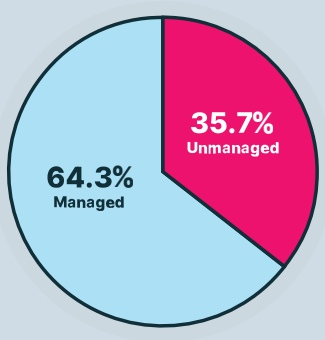
Un/manged Device Distribution in BYOD Organizations

Downloads / Uploads

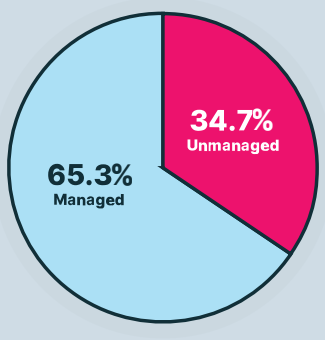
When examining file transfer activity on managed vs. unmanaged devices, we identified that **managed devices, constituting 80% of the enterprise, exhibit a higher volume of downloads and uploads than unmanaged devices.** Managed devices might be performing regular software updates, downloading security patches, or synchronizing enterprise data – all contributing to their higher transfer activity. This pattern likely reflects the stricter administrative controls and security measures in place for managed devices.

65%

Unmanaged Devices are 65% More Likely to Download and Upload Files



Uploads



Downloads

The Unseen Threats in Browser Extensions

What is the risk

Browser extensions harbor grave dangers, threatening data security, privacy, and browsing integrity. They serve as gateways for data theft, phishing, and the betrayal of user trust, through deceptive practices and false assurances.

Malicious Functionality

Malicious browser extensions stealthily harvest sensitive data, employing tactics such as injecting ads, redirecting to phishing sites, and spying on online activity, as seen in the 2023 ChromeLoader Malware incident.

33%

of All Extensions Within an Organization Pose High Risk

1%

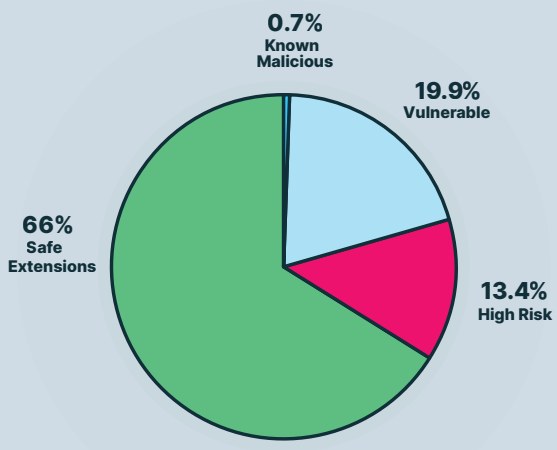
of Installed Extensions are Known as Malicious

Deceptive Dangers of Browser Extensions

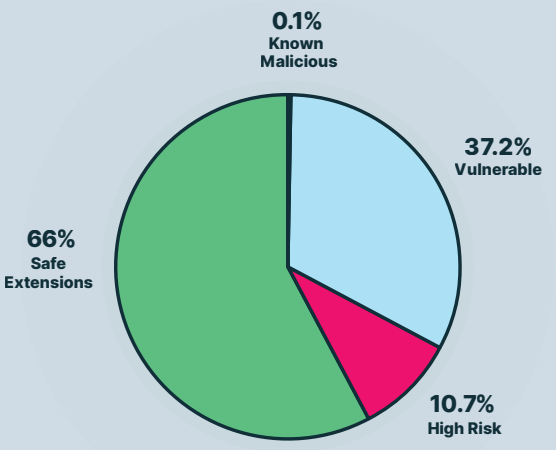
Browser extensions threaten data security and deceive users with false promises. This grants them access to sensitive data and leaves users vulnerable to exploitation.

Vulnerabilities in Browser Extensions

Supply chain compromises and vulnerabilities in popular extensions continue to pose threats, enabling attackers to hijack legitimate extensions and compromise millions of users.



Browser Extension Risk Classification Breakdown by Unique Extension ID



Browser Extension Risk Classification Breakdown by Browser Profile

* Browser Profile - This refers to the employee's email address used to log in to the browser
* Extenson ID - This is a unique alphanumeric code assigned to each browser extension for easy identification and management

The Supply Chain Shadow

The risks associated with browser extensions go beyond just their code, as hackers can exploit vulnerabilities in the supply chain to insert malicious code. This increases the threat posed by AI-powered extensions, which can deceive users and direct them to phishing websites.

Moreover, extensions that require critical permissions such as access to passwords, cookies, etc., pose a high risk to an organization's security.

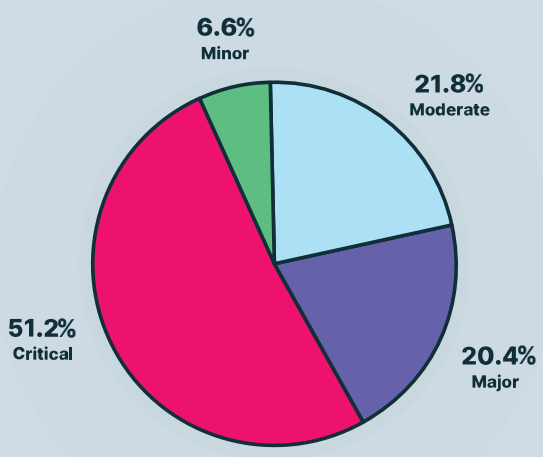
Additionally, incidents involving malicious ChatGPT extensions highlight the potential for AI tools to manipulate user behavior for malicious purposes.

over **50%**

of Extension Installations Within an Organization Require Critical Permissions

Persistent malicious extensions

A concerning trend was observed: despite being labeled as "confirmed malware" and being removed from the Google Chrome store, the extension was still available for sale. This phenomenon exposes users to significant cybersecurity threats, underscoring the urgent need for more proactive measures to detect and block the distribution of malicious extensions across popular browser platforms.



Extension Supply Chain Risk

The Threats of Uncontrolled SaaS

What is the risk?

The clandestine use of Shadow SaaS applications poses a significant threat to organizational security, creating vulnerabilities and unauthorized access to sensitive data.

What is the root cause?

The underlying issue originates from employees adopting SaaS applications without oversight, thereby circumventing stringent security measures and creating vulnerabilities that allow unauthorized access to sensitive data.

> Ignoring Shadow SaaS Leads to Dire Consequences: *Data Breaches, Financial Losses, Legal Issues, and Damaged Reputation*

> Beware the Lurking Blind Spots: *Where Rogue SaaS Apps Flourish, Vulnerabilities Multiply, and Cyber Threats Thrive Unseen*

Identity crisis

Uncontrolled SaaS use exacerbates vulnerabilities in identity management systems, with shared logins and recycled passwords serving as entry points for cybercriminals. This poses a significant risk to organizational security.

Unraveling the Risks of Shadow SaaS

Onboarding anarchy

Employees using unauthorized SaaS apps act as rogue agents, creating data vulnerabilities and exposing the organization to breaches, as seen in incidents like the previously mentioned Okta attack.

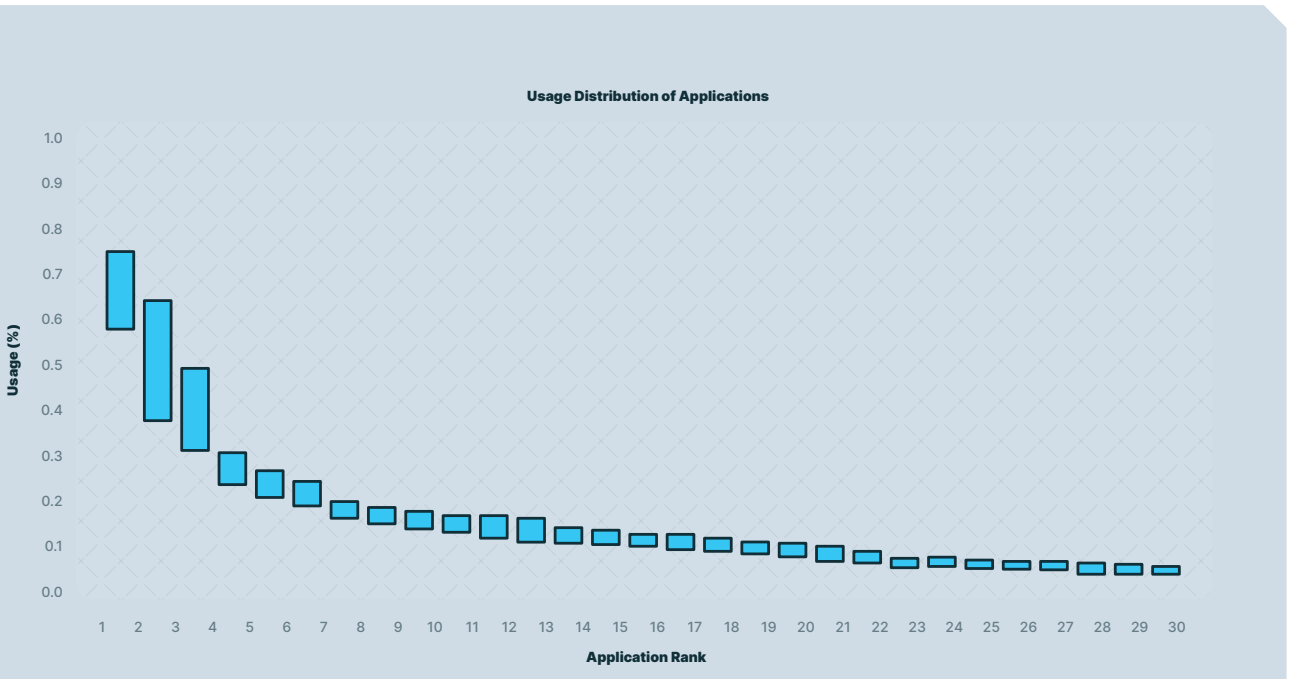
Blind spots blossom

Lack of centralized control over Shadow SaaS leads to operational chaos for IT teams, resulting in unauthorized access to sensitive data and heightened security concerns.

App Usage

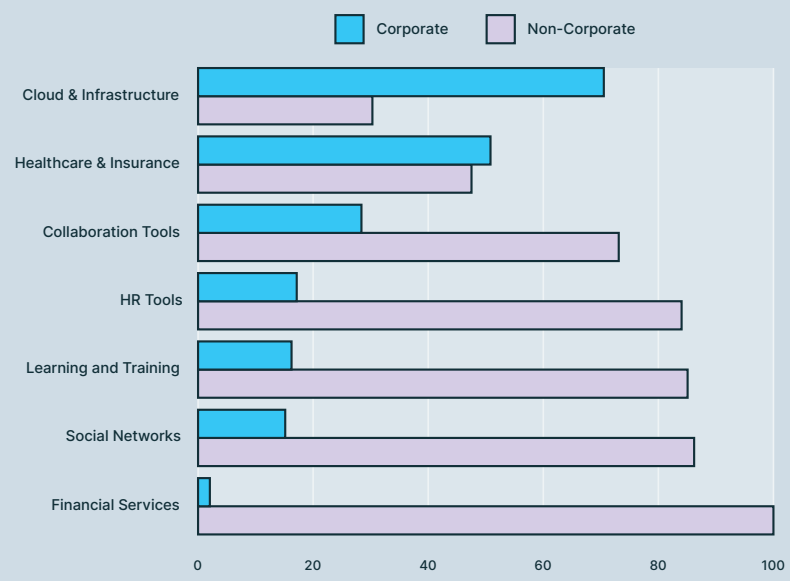
A study on application usage within organizations revealed a noteworthy pattern: while the first app averages a 70% usage rate, engagement sharply declines after that. By the 15th app, only 10% of employees are actively using additional applications, and this figure drops to just 5% by the 30th app. This underscores the significance of streamlining software ecosystems to enhance overall productivity.

> App Engagement Drops to 10% Beyond the 15th App in Use Within an Organization



Corporate and Non-Corporate Identities

Research on application usage in corporate and non-corporate identities within organizations unveils distinct patterns. While work-related apps like cloud and infrastructure are mainly accessed from corporate accounts, financial services are predominantly accessed from non-corporate identities. Interestingly, **sectors such as healthcare and insurance, and collaboration tools show high usage from both corporate and non-corporate identities,** indicating a dual-purpose utilization trend within organizations.



Percentage of Application Usage by Corporate Identities within Organization

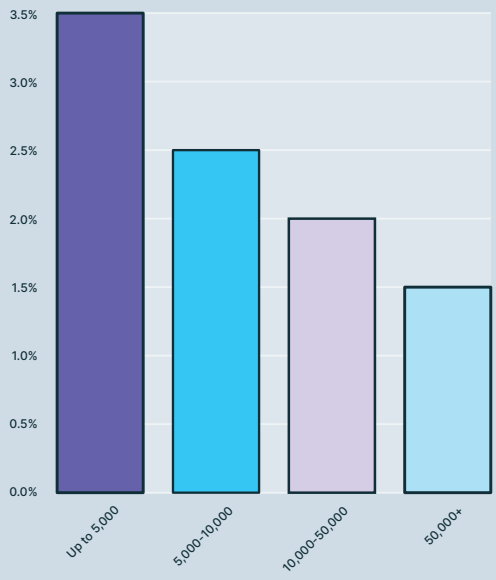
Identity Vulnerabilities

What is the risk?

The vulnerability of digital identities poses a significant threat, leaving sensitive information exposed to cybercriminals.

What is the root cause?

Convenience-driven practices, such as account sharing and widespread adoption of Single Sign-On (SSO), are at the core of identity risks. These practices prioritize convenience over security, leading to the potential compromise of sensitive data and the increased likelihood of unauthorized access.



The Percentage of Shared Accounts in Different Corporates to their Size

Insights on Account Sharing, SSO, and Authentication

Shared accounts are a problem

Account-sharing practices, exemplified by password reuse and incidents like the 23andMe data breach, underscore the dangers of shared identities and the need for robust security measures.

The adoption of SSO is not perfect

While Single Sign-On (SSO) offers convenience, it also concentrates power in one key, potentially becoming a single point of failure and compromising overall security. Insights from our research reveal varying user preferences and adoption rates, highlighting ongoing debates about the effectiveness and security of SSO.

The Number of Accounts Who Use SSO vs. Username and Password in Various Services and Platforms (Classified by Categories)

Gen-AI and Large Language Models

What is the risk?

Pasting data into Generative AI tools like ChatGPT can inadvertently expose it to the entire user community, potentially compromising sensitive information.

Research on ChatGPT and other Generative AI tools' usage patterns among over 10,000 employees revealed a risk: **pasting data into these tools can inadvertently expose it to the entire user community.** Despite widespread adoption, concrete data on volume, trends, and types of exposed data remains scarce, highlighting a significant gap in understanding and mitigating this risk.

40%

of Employees Engage With GenAI

7,5%

of Employees Paste Data into GenAI

8%

of Employees Use GenAI on a Daily Basis

3%

of All Browsers Receive Alerts from GenAI Apps

The Unregulated Upload

AI extensions pose concerns beyond data theft, particularly with unregulated data uploading. These tools can collect vast personal data, like browsing history and email content, and then upload it to remote servers with minimal transparency or user control. The lack of regulatory oversight fosters data misuse and privacy violations.

- Insights reveal varying adoption rates of (Gen AI) apps across sectors, highlighting their evolving landscape.
- High-tech companies show significantly higher adoption, followed by Mid-tech integration companies, while Low/No-tech entities exhibit lower adoption rates.

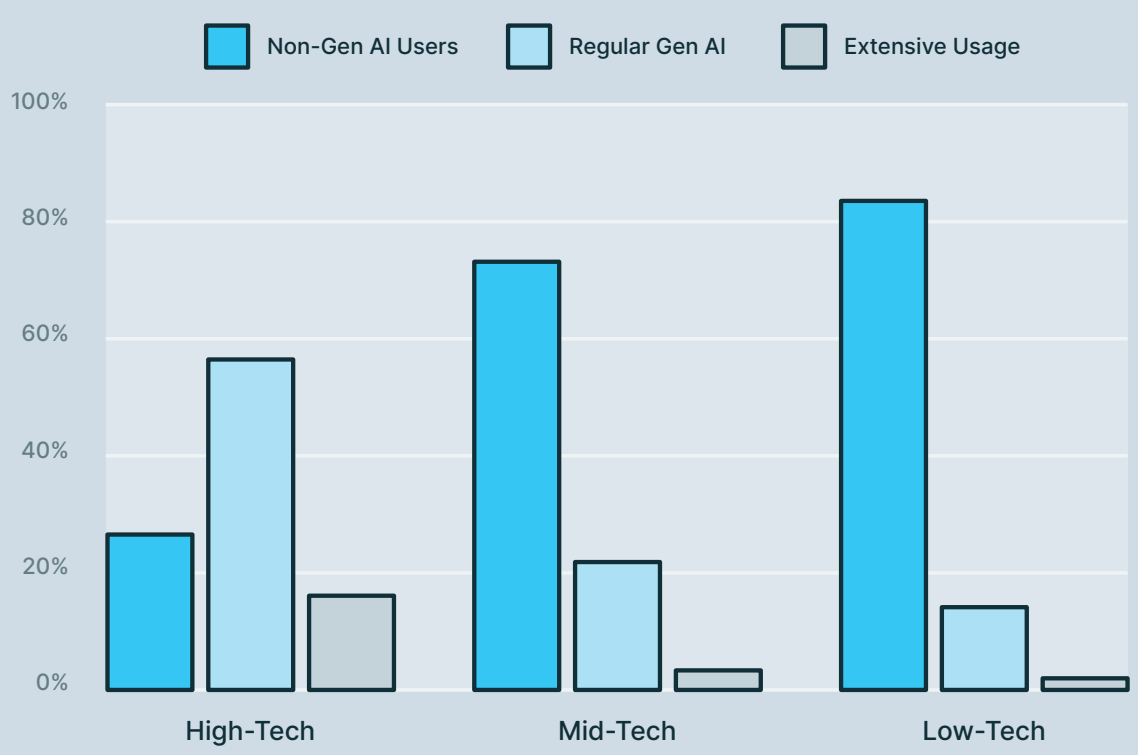
User Engagement

As mentioned before, the trend of extensive usage within companies underscores the evolving landscape of Gen AI applications and their varied adoption across different sectors.

The graph below illustrates the percentage of users utilizing Gen AI applications, distinguishing those with extensive usage, defined as engaging in at least one session per day.

7,5%

Paste with Caution: 7.5% of Employees Risk Data Exposure with GenAI



User Engagement with Gen AI Applications

AI-powered Threats

What is the risk?

The rapidly evolving browser security landscape in 2023 faces significant threats from AI-powered phishing and social engineering attacks. These are exemplified by fake ChatGPT Chrome extensions capable of stealing sensitive information. Such attacks leverage AI-driven personalization, making them more convincing and targeted than ever before, posing serious risks to users' data security.

What is the root cause?

The rise of AI-powered attacks is fueled by the seamless integration of personalized content and high-quality user interfaces, blurring the line between genuine and malicious activities.

> AI-Powered Threats are Evolving Rapidly, Posing Serious Risks to Data Security and Societal Trust

Sophisticated Malware

Cybercriminals utilize AI algorithms to develop advanced malware capable of evading traditional security measures and infecting browsers to steal sensitive information.

Phishing Attacks

AI-driven phishing campaigns employ sophisticated techniques to create convincing and personalized phishing emails or websites, tricking users into revealing login credentials or sensitive data.

Browser Extension Exploitation

Hackers exploit AI algorithms to develop malicious browser extensions that inject code into browsers, leading users to phishing sites or compromising their privacy.

Supply Chain Vulnerabilities

AI-powered threats exploit supply chain vulnerabilities to inject malicious code into legitimate browser extensions or applications, compromising users' browser security.

Unpatched Vulnerabilities: Zero-Days and Outdated Browsers

What is the risk?

Unpatched vulnerabilities in software pose a constant threat to users, exposing them to cyberattacks such as data theft, malware injection, and system compromise. These vulnerabilities, exemplified by recent zero-day exploits in Google Chrome and Microsoft Edge, can lead to widespread chaos and compromise sensitive data.

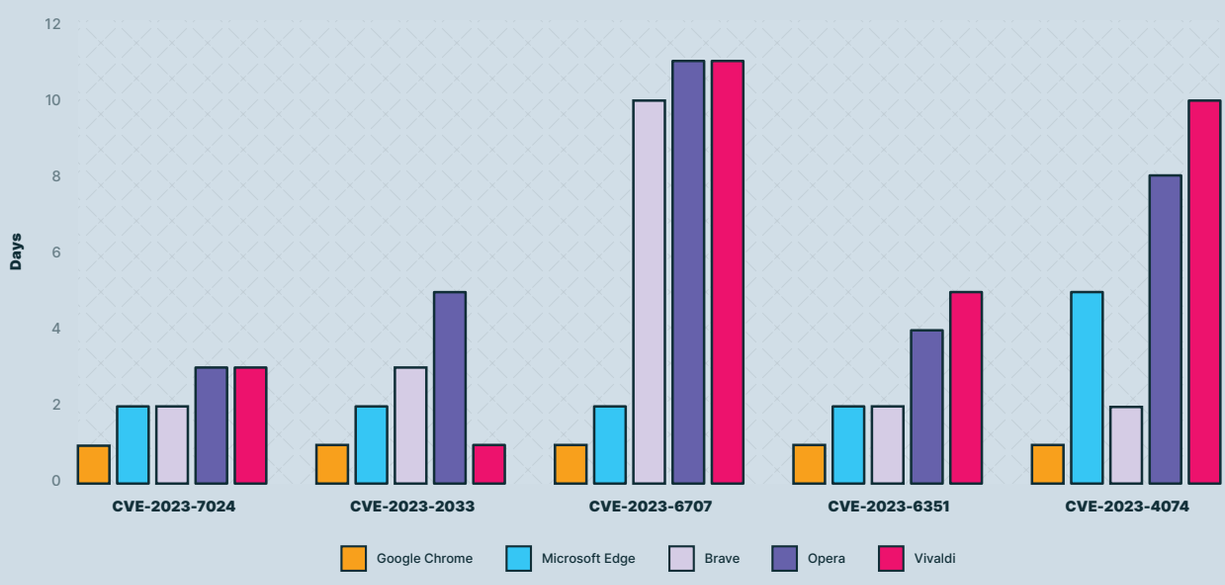
> Chrome Exhibited the Swiftest Response Compared to Chromium-Based Browsers

What is the root cause?

The pervasive impact of unpatched vulnerabilities stems from both technical flaws and human vulnerabilities. Outdated software progressively loses its ability to withstand cyberattacks, providing hackers with backdoors into user systems.

Patching Disparities

Analysis of zero-day vulnerabilities in 2023 browsers reveals notable differences in patching times for zero-day vulnerabilities among different browsers. **Browser size correlates with patching time, revealing differences among Chromium-based browsers,** like Brave, Edge, Opera, and Vivaldi, which exhibit delays in both zero-day and one-day vulnerability patching.



Pathicng Time of Zero-Day Vulnerabilities (Cve-2023-7024 and Cve-2023-2033) vs. One-Day Vulnerablities

The Evolution of Web Attacks in 2023

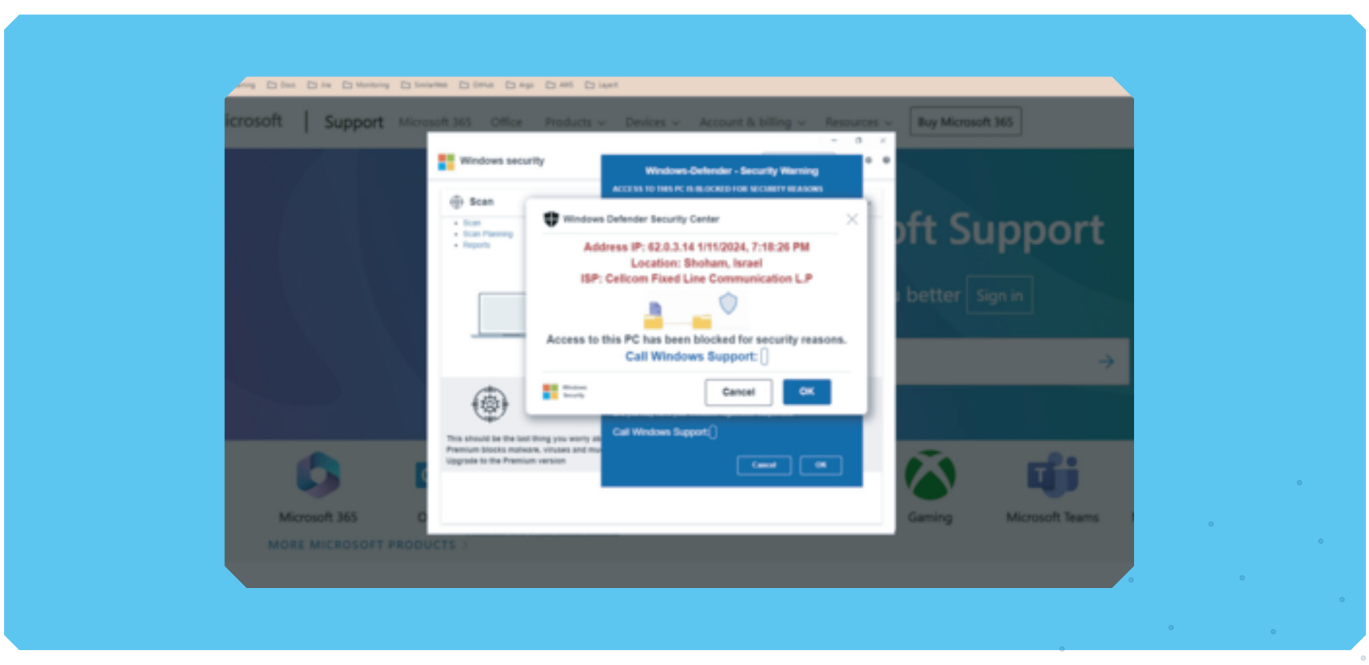
In 2023, browser security advanced with more sophisticated and personalized web attacks, including convincing phishing attempts. The rise of Browser in the Browser (BitB) search relevance emphasized this evolving threat landscape. Attackers focused on creating visually authentic interfaces to deceive users, complicating detection. Two examples highlight the impact of these attacks and data loss.

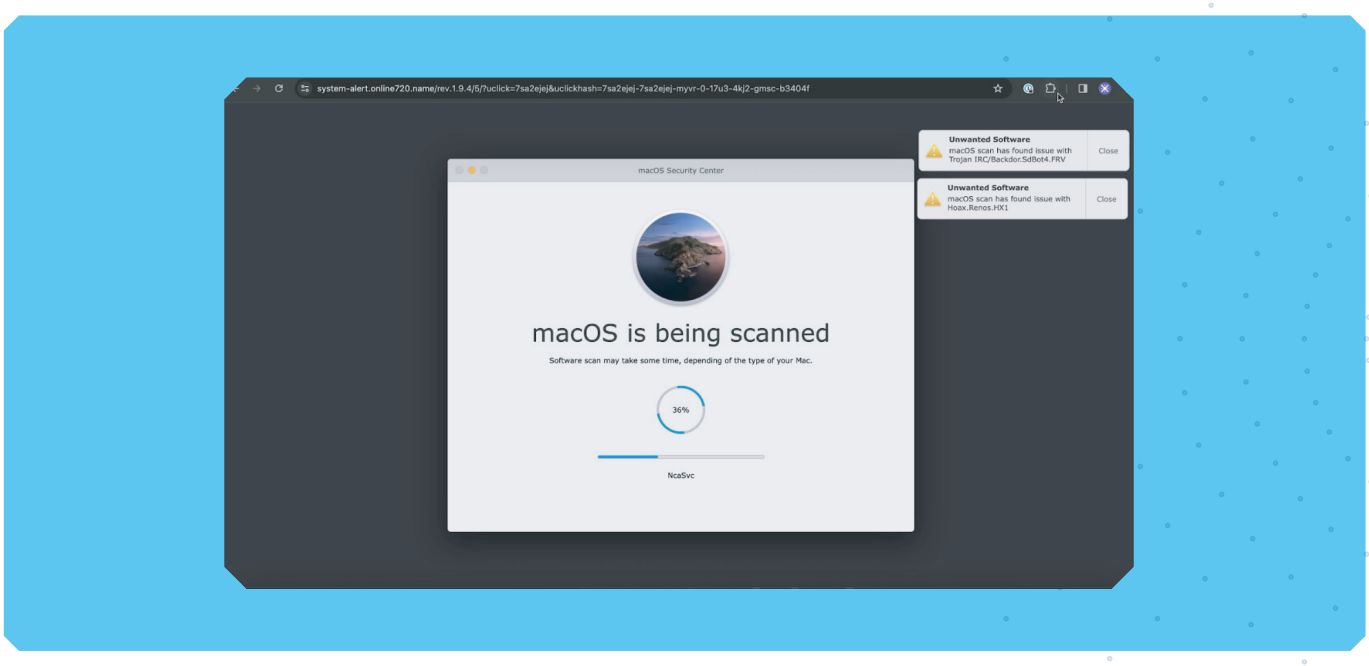
Phishing Attack Utilizing AWS Reputation Hosting

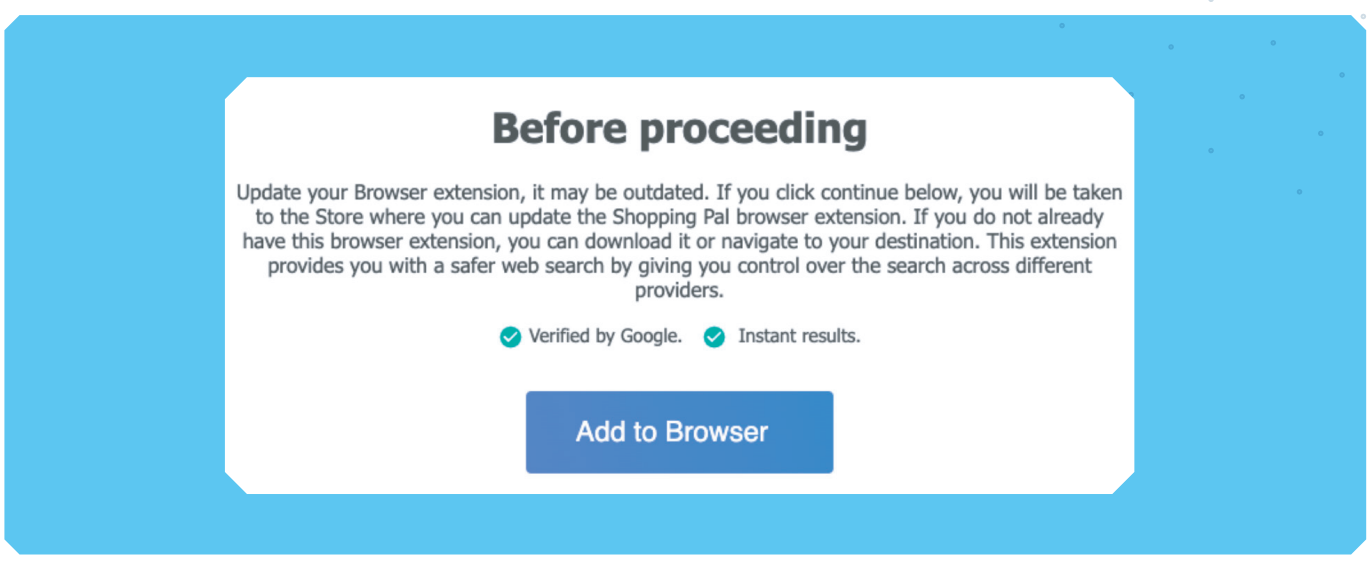
- **Vector:** Deceptive website hosted on AWS disguised as an antivirus tool.
- **Payload:** Automatic file downloads containing malware with functions like password theft and screen recording.
- **Impact:** Risk of internal network spread and further harm as users unwittingly download malware, expecting antivirus assistance.
- **IOCs:**
  ipwho[.]is
  main[.]d8svgaovdhc9s.amplifyapp.com

Deceptive Video Link Phishing Attack

- **Vector:** Deceptive video link urging browser notification enablement.
- **Payload:** Dynamic payload could redirect to phishing sites or inject notifications.
- **Impact:** Disguised as a YouTube converter to lure users. Upon execution, the malware is intercepted by a detection mechanism and traced back to the user's Gmail account, indicating potential compromise.
- **IOCs:**
  R3[.]o.lencr.org
  Rophille[.]com

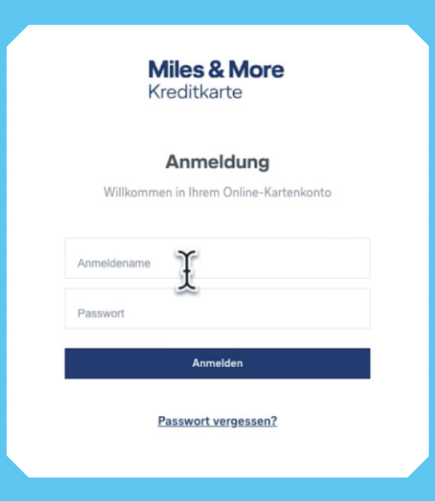


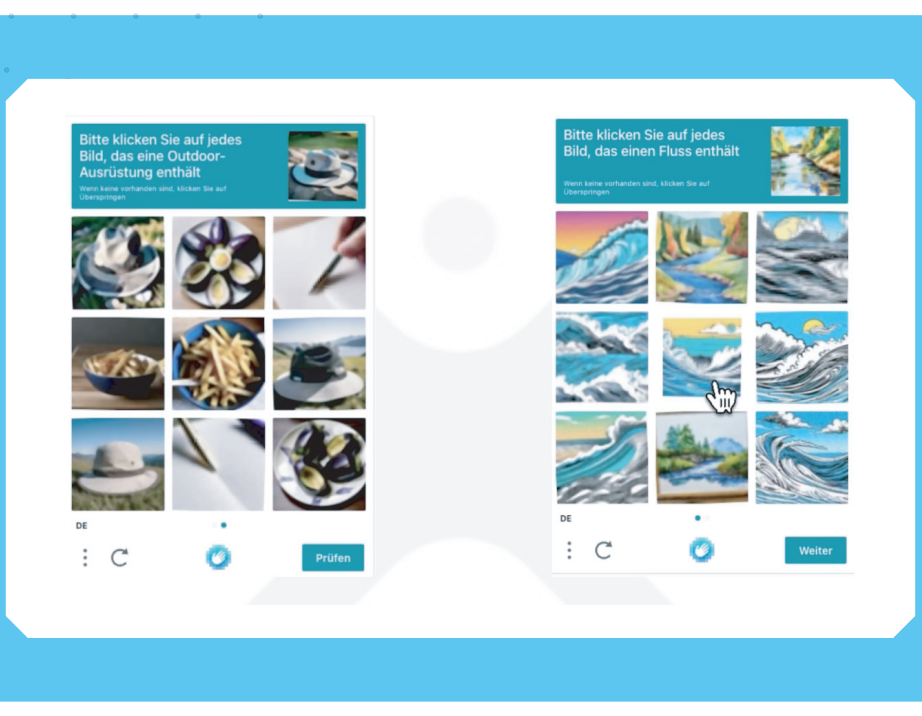




Fake CAPTCHA Phishing Attack

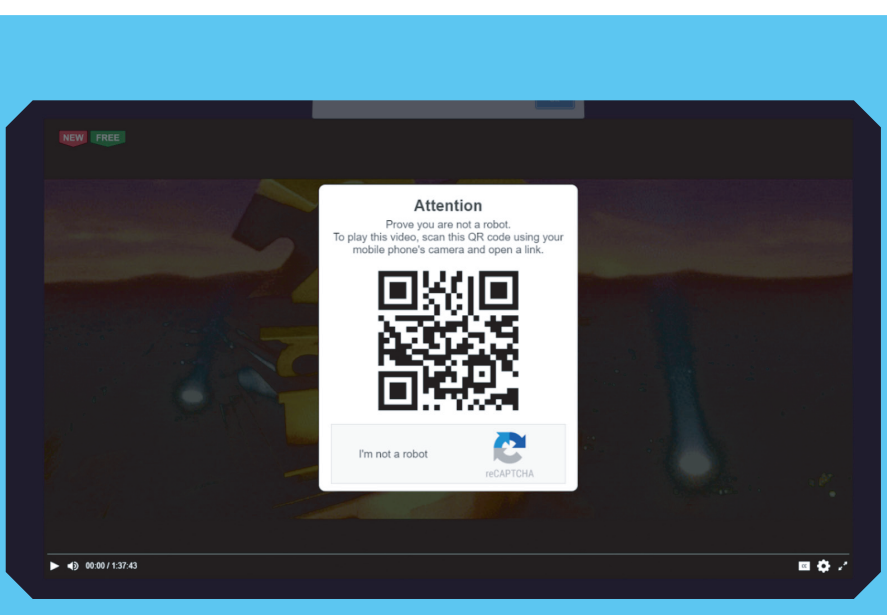
- **Vector:** Deceptive attack disguised as fake CAPTCHA.
- **Payload:** Trick users into divulging sensitive information like login credentials, personal details, or financial information.
- **Impact:** Stolen data used for identity theft, financial fraud, or unauthorized access to accounts or systems. In this case, the victim's Miles & More bonus account.
- **IOCs:** dev-millemordkred[.]pantheonsite.io/de/13161

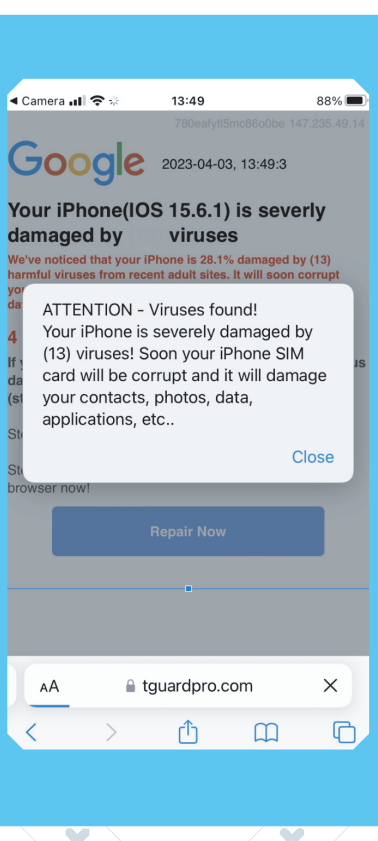




Malicious iPhone App Distributed Through Desktop Malvertising Campaign

- **Vector:** Malvertising campaign distributing fake video through popular streaming sites.
- **Payload:** Users are enticed to scan a QR code displayed in the video, redirecting them to a malicious landing page. Here, a fake security alert induces urgency, claiming device viruses and SIM card corruption.
- **Impact:** Exploits human vulnerabilities, targeting unmanaged mobile devices of employees, posing risks for identity theft and corporate security. This cross-device strategy poses challenges for enterprises, especially when targeting unmanaged mobile devices belonging to employees.
- **IOCs:** hxxps://fmovies[.]to

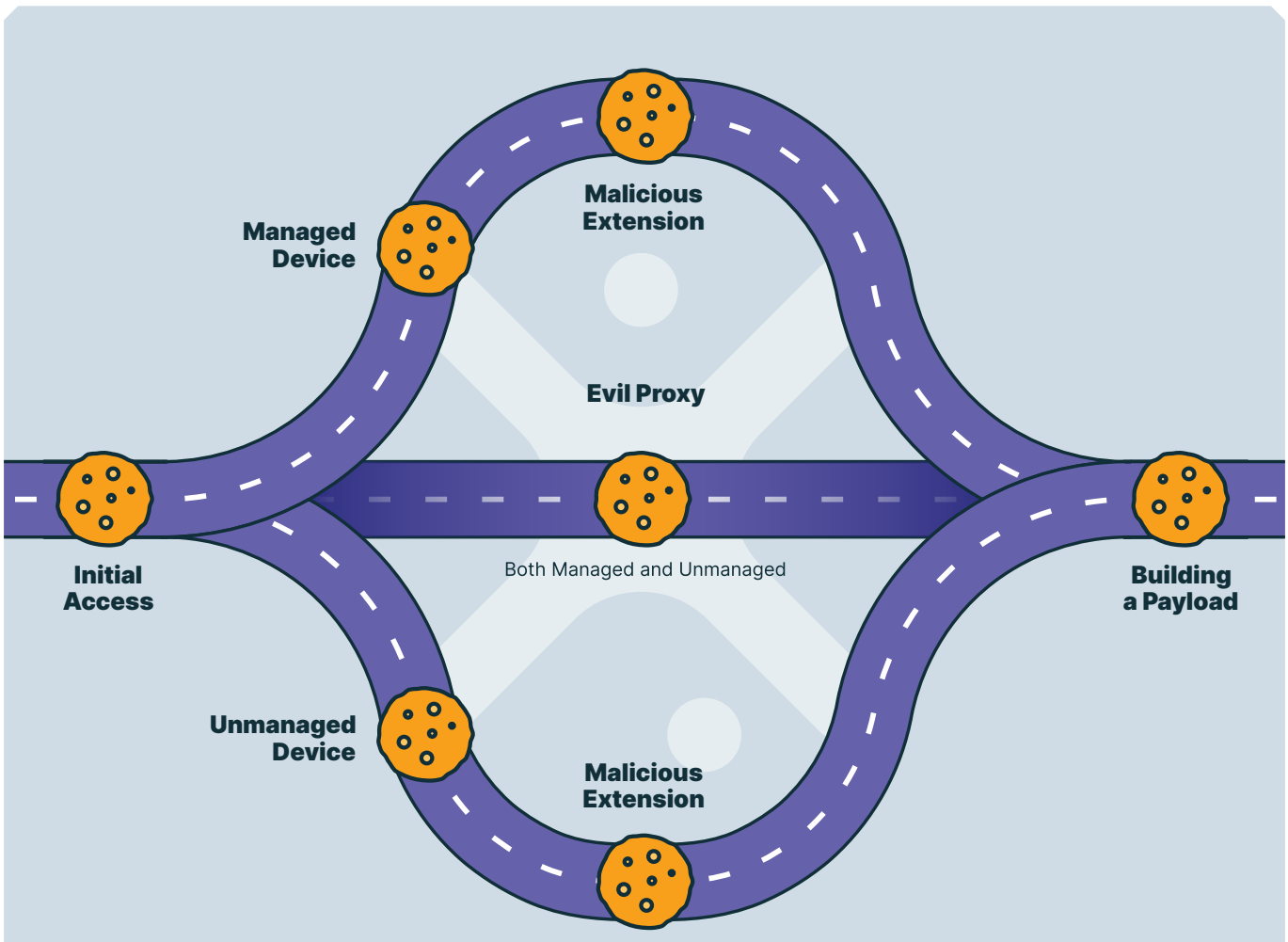




Prevention of Account Takeover

Brute force attacks, phishing scams, and credential leaks are formidable threats to digital security, by breaching defenses and enabling account takeovers. Once attackers possess login credentials, they can manipulate accounts, causing financial harm, data breaches, and reputational loss. For instance, in December 2023, a pass-the-cookie attack emerged, leveraging Google OAuth endpoints to revive cookies and hijack user accounts. This method circumvents authentication, exploiting Google's OAuth functionality for unauthorized access.

How does the Pass-the-Cookie attack work?



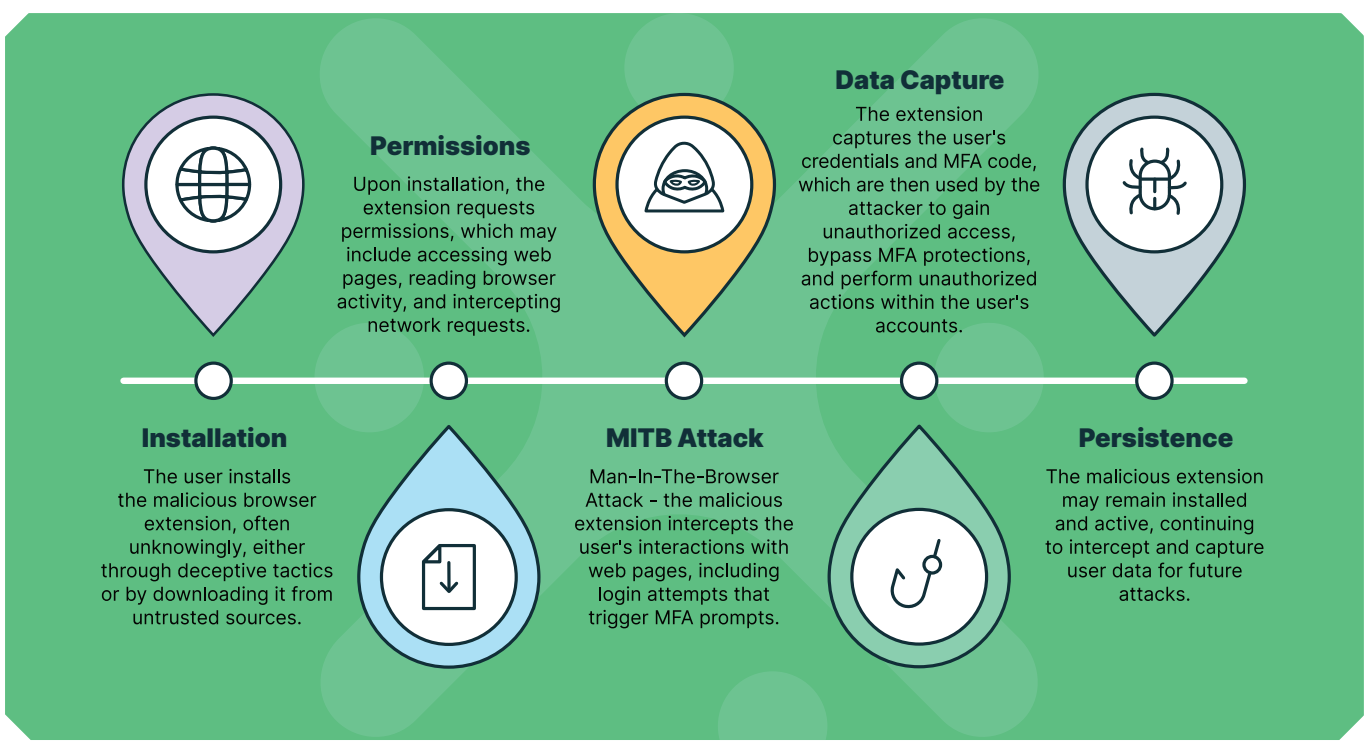
- **Managed Device Scenario:** Malicious extensions stealthily steal session cookies for unauthorized access.
- **Unmanaged Device Scenario:** Vulnerabilities or malware directly obtain session cookies.
- **Evil Proxy Attack:** Intercepted communication prompts users to divulge credentials and MFA codes, leading to cookie theft.

Payload Creation

The attacker assembles a payload by gathering stolen session cookies from various sources, such as malicious extensions, malware, or an evil proxy. With these cookies, they can access the targeted web application without needing the victim's username or password, maintaining persistent access for further exploitation, data theft, or other malicious activities.

Even Multi-Factor Authentication (MFA), once considered a fortress against unauthorized access, isn't invincible. Sophisticated phishing attacks and social engineering tactics can bypass MFA, leaving accounts vulnerable.

One of the hacker's attack methods for an MFA attack is using a malicious browser extension:



To prevent MFA attacks via malicious browser extensions, users should **only install extensions from trusted sources, regularly review permissions** granted to extensions, and **employ security tools** to detect and remove potentially harmful extensions.

Additionally, organizations can implement network-level security measures to detect and block malicious activities originating from browser extensions.

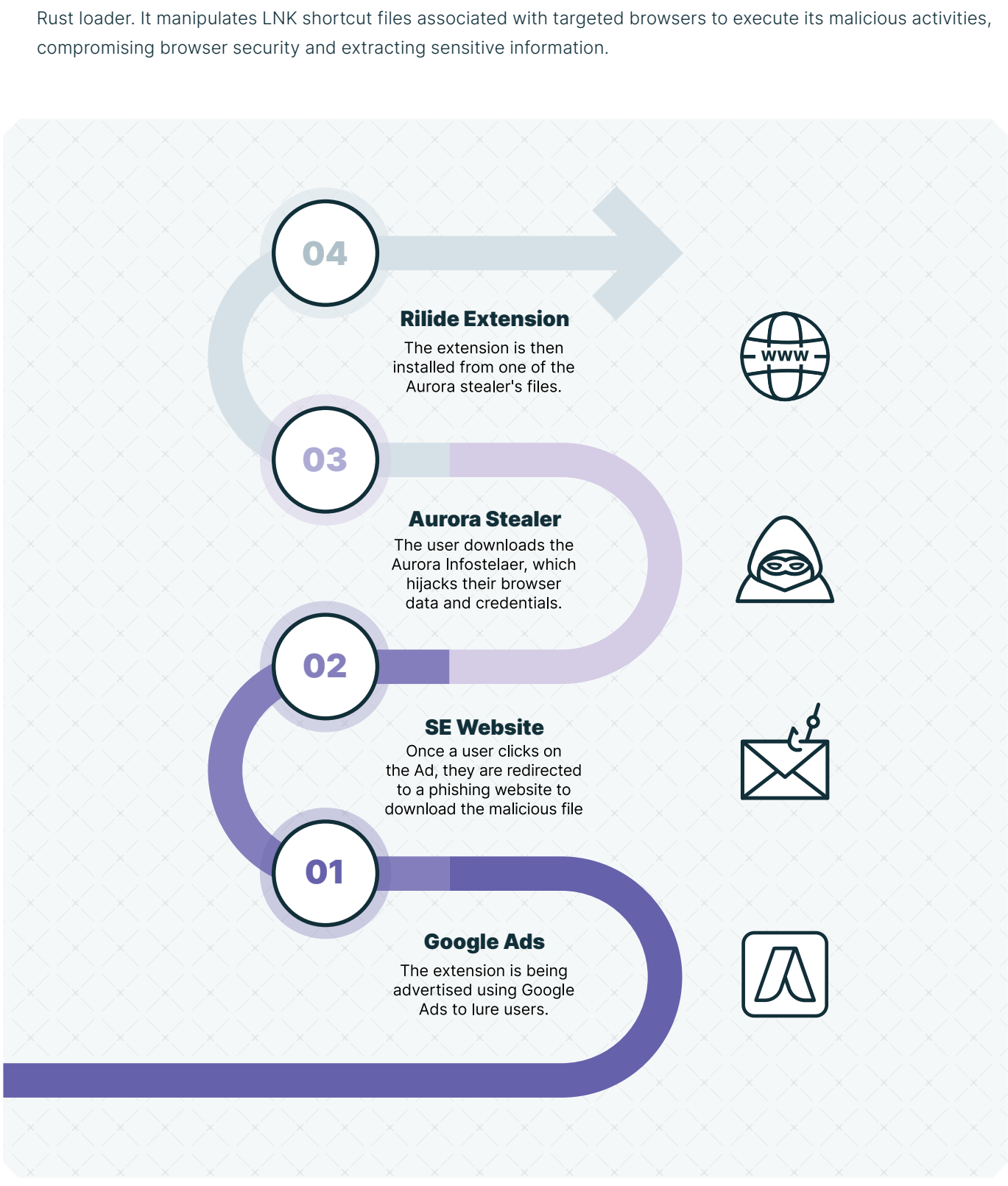
Case Study - Rilide Extension

In April 2023, the malicious Chrome extension Rilide masqueraded as a genuine Google Drive extension, duping users into providing their Multi-Factor Authentication (MFA) codes, which were then sent to attackers. Rilide disabled the Content Security Policy (CSP), enabling data extraction and compromising email and cryptocurrency accounts. Beyond deceiving users, it stole browser credentials and data, resulting in significant privilege escalation within the browser. Rilide has been identified in two separate campaigns, one of which involved the use of malicious Google ads. The attack method follows a specific pattern:

- **Aurora Campaign** – The Aurora stealer campaign uses Google Ads to distribute malware, posing as fake Team Viewer and NVIDIA Drivers installers. Users download the Aurora Stealer from a deceptive site, exploiting the perceived trustworthiness of Google Ads to boost the campaign's impact.

- **Rilide Deployment** – The Aurora Stealer activates the Rilide Locker via its loader, circumventing Content Security Policy (CSP) restrictions for XSS attacks. Rilide monitors browsing history, sends URLs to a designated list, and captures screenshots of active tabs.

- **Impersonation as Legitimate Extension** – Rilide disguises itself as a legitimate Google Drive Extension using a Rust loader. It manipulates LNK shortcut files associated with targeted browsers to execute its malicious activities, compromising browser security and extracting sensitive information.



Browser Security Annual Highlights

January

Hackers Push Malware via Google Search Ads

Hackers used Google Search ads to spread malware disguised as trusted software like VLC, 7-Zip, and CCleaner. The malicious ads redirected users to fake download sites, where unwitting users download and install malware. This sophisticated tactic highlights the importance of cautious online behavior and robust cybersecurity measures to mitigate the risk of such attacks.

February

GoDaddy Security Breach with Hosting Websites Redirecting to Phishing

Web hosting giant GoDaddy reported a security breach after discovering that their hosting sites were redirecting users to phishing campaigns. According to GoDaddy, the attack was supposedly a part of a broader campaign targeting other hosting companies worldwide over the years. Phishing attacks originating from high-reputation domains easily evade traditional network security solutions, as well as email security solutions.

March

Microsoft Warns of Massive Phishing Campaign Sending Millions of Emails

The Microsoft Threat Intelligence team tracked the development of an AiTM phishing kit dubbed DEV-1101. The kit enables cybercriminals to set up phishing landing pages mimicking Microsoft Office and Outlook, and use CAPTCHA checks to evade detection. Microsoft has detected millions of phishing emails utilizing the tool daily.

April

Rilide - A New Malicious Browser Extension for Stealing Cryptocurrencies

In April 2023, a malicious Chrome extension called Rilide tricked users into giving up their MFA codes by posing as a Google Drive extension. Rilide not only stole login information but also bypassed security measures to steal browser data and potentially escalate privileges. Rilide was distributed through deceptive Google Ads campaigns that appeared to offer legitimate software.

May

May 2023 witnessed a surge in disclosed cybersecurity incidents involving AI, raising concerns about vulnerabilities within these powerful technologies. From malicious actors leveraging AI for sophisticated phishing scams to large-scale data breaches, the month highlighted the need for robust security measures as AI integration deepens.

For example:

Samsung Bans the Use of AI Tools After the Internal Leak to ChatGPT

In April, it was disclosed that Samsung employees accidentally shared confidential information while using ChatGPT for help at work, which led to an internal leak. Following this incident, Samsung prohibited the use of generative AI tools like ChatGPT. The ban is aimed at preventing further incidents of data exposure and safeguarding sensitive information.

Malicious Google Search Ads for AI Services like ChatGPT and Midjourney Redirect Users to Malware

A campaign that was trending in May used Google search ads to deliver imposter web pages for ChatGPT and Midjourney. Users were redirected to web pages with fake AI app installers, which contained Redline Stealer malware.

June

Malicious Chrome Extensions with 75M Installs Removed from Web Store

Google removed 32 malicious extensions from the Chrome Web Store that had a collective download count of 75 million. These extensions contained adware that spammed victims with unwanted ads and hijacked search results that redirect users to malicious links.

July

Nitrogen Malware Pushed via Google Ads for Ransomware Attacks

A 'Nitrogen' initial access malware campaign used Google and Bing search ads to promote fake software sites. Users who clicked the links were redirected to compromised pages hosted by WordPress, which contained malicious downloads.

August

August 2023 saw a surge in phishing campaigns, posing significant cyber threats. These sophisticated attacks exploited vulnerabilities in popular platforms, targeting unsuspecting users with alarming frequency. Amidst rising concerns over data security, two notable examples shed light on these alarming trends.

ChromeLoader Campaign Spreads Malicious Browser Extensions

ChromeLoader is a persistent Google Chrome browser hijacker, first discovered in 2022. A new campaign emerged as a notable threat in August, disseminating malicious browser extensions. It stealthily installed malicious Chrome extensions via deceptive online ads, tricking users into running VBScript files.

Phishing-led Cloud Account Takeover Campaign Utilizing EvilProxy

EvilProxy, a phishing-as-a-service platform, was utilized by attackers for covert communication, underscoring the significance of phishing as a strategic component in executing advanced cyber threats. This campaign targeted top-level entities, allowing threat actors to compromise cloud accounts and potentially orchestrate further cyberattacks.

September

Chrome Extensions Steal Plaintext Passwords From Website

University of Wisconsin-Madison researchers uploaded a proof-of-concept extension to the Chrome Web Store that can extract plaintext passwords from website source code. Their findings revealed flaws in Chrome's permission model, violating security principles. Additionally, major websites, including Google and Cloudflare portals, were identified as storing passwords in plaintext within HTML source code, making them vulnerable to extraction by extensions.

October

Massive Cybercrime URL Shortening Service Uncovered via DNS Data

A massive cybercrime URL-shortening service was uncovered. The service facilitated cybercriminal activities by shortening malicious URLs, making it easier for attackers to distribute malware and conduct phishing campaigns. The discovery underscores that threat actors are creatively bypassing traditional protection methods by using high-reputation web platforms.

November

AsyncRAT New Infection Chain

McAfee Labs discovered an AsyncRAT campaign using phishing emails as the infection vector. Recipients received spam emails with malicious links triggering the download of an HTML file (HTML Smuggling). The embedded ISO file concealed a Windows Script File (WSF), initiating a chain of file executions, including PowerShell and VBScript, leading to process injection into RegSvcs.exe. This manipulation allowed attackers to discreetly hide activities within a trusted system application.

December

Malware Abuses Google OAuth Endpoint to 'Revive' Cookies, Hijack Accounts

During December, a pass-the-cookie attack was reported - a malware strain that exploits Google OAuth endpoints to revive cookies and hijack user accounts. The malware can revive cookies associated with user accounts, allowing it to steal those accounts without going through standard authentication procedures. This technique allows the malware to bypass authentication processes and gain unauthorized access to accounts by leveraging Google's OAuth functionality.

Recap on Our 2023 Predictions

As we reflect on the browser-security landscape of 2023, it's evident that the digital realm has experienced significant shifts, bringing both challenges and opportunities. Our predictions for 2023 aimed to anticipate these changes and provide insights into emerging trends. Let's delve into a recap of our 2023 predictions, exploring some examples that illustrate each anticipated development.

- **SaaS - A Governance and Security Pain Point**
  The proliferation of Software as a Service (SaaS) applications presented organizations with a double-edged sword. While these tools enhanced productivity, the growing SaaS environment posed challenges in governance and security. The surge in adoption led to the emergence of blind spots, shadow applications, and unmanaged identities, overwhelming IT departments. For instance, organizations struggled with the management of numerous SaaS applications, emphasizing the need for effective governance strategies to navigate this complex landscape.

- **The Browser Will Become the Main Attack Surface**
  The browser, serving as a central tool for both personal and work-related tasks, emerged as a primary target for cyber adversaries. Exploiting personal browser activity as a vector to access work resources became a prevalent method of attack. Security teams were challenged to view all browsing activities as a unified attack surface, highlighting the importance of securing this gateway to prevent potential breaches and data compromises.

- **Attacks Will be Increasingly SaaS-based and Less File-based**
  A notable transformation in attack vectors occurred as organizations leaned heavily on SaaS applications. The diminishing reliance on traditional files shifted the focus of cyber threats towards SaaS and web applications. This shift influenced the threat landscape, with a surge in attacks targeting the vulnerabilities associated with these platforms. As a result, security measures needed to adapt to the evolving tactics, recognizing the increased prevalence of web and cloud-based attacks.

- **Malicious Web Pages Will Become More Sophisticated**
  In 2023, cybercriminals developed sophisticated strategies, such as "fake bank" websites, to trick users into divulging login credentials and exploiting trusted brands to ensnare unsuspecting victims. These malicious pages don't just steal data; they lead to financial losses, as seen with the rise of pages facilitating investment fraud. Users are deceived into investing in fake schemes or transferring funds to fraudulent accounts, exploiting the trust in online financial services by promising quick returns with minimal risks.

As we revisit our predictions for 2023 in the realm of browser security, one notable and unexpected evolution took center stage — **the surge of AI-powered threats.** While we anticipated the continued sophistication of cyber threats, the extent to which artificial intelligence would be wielded to exploit browser vulnerabilities surpassed our initial foresight.

In particular, **the deployment of Large Language Models (LLMs) for Automated Spear Phishing emerged as a paradigm shift.** The adaptability and personalization capabilities afforded by AI allowed attackers to craft highly targeted phishing campaigns, tailoring their approach to individual users. This marked a departure from traditional phishing techniques, catching both security professionals and users off guard as AI-driven attacks proved to be more convincing and challenging to detect.

Moreover, the integration of AI in the development of malware introduced a new layer of complexity. Malicious actors leveraged AI's dynamic nature to create sophisticated and automated malware that exhibited an uncanny ability to evade traditional security protocols. This unforeseen development forced a reevaluation of defense strategies, emphasizing the need for adaptive and proactive measures to counter the rapidly evolving landscape of AI-powered threats in browser security.

Our predictions not only anticipated most of these changes but also provided valuable insights into the strategies employed by cyber adversaries. As we move forward, staying vigilant and adapting security measures will be crucial to addressing the ever-changing threat landscape.

2024 Predictions by LayerX

Increased Focus on Browser Fingerprinting

Browser fingerprinting, a technique to uniquely identify users based on various browser and device attributes, is gaining prominence among attackers. By utilizing this method, threat actors can meticulously track users across different websites, creating detailed profiles of their online behaviors. This form of tracking poses a significant threat to user privacy and demands enhanced countermeasures to safeguard against intrusive surveillance.

Ransomware Targeting Browser Extensions (Malware Targeting Browser Data)

A rising threat in 2024 involves ransomware attacks that specifically target browser extensions. This type of malware aims to encrypt user data stored within these extensions, posing a substantial risk to users' sensitive information. This indicates a shift in attackers' focus towards exploiting vulnerabilities in browser-related functionalities, requiring increased security measures to prevent data loss and unauthorized access.

Large Language Models (LLM) and AI

Automated Spear Phishing: The integration of AI, particularly LLMs, is expected to facilitate automated spear phishing attacks. This advancement enables attackers to craft highly personalized and targeted phishing campaigns, significantly increasing the chances of success by tailoring deceptive content to individual users.

AI-powered malware: The use of AI in developing malware is foreseen as a growing threat. Attackers will leverage AI to create more sophisticated and automated forms of malware designed to evade traditional security software. This evolution necessitates the enhancement of cybersecurity measures to effectively detect and mitigate AI-powered threats.

Data Leakage

Browsers, in their continuous collection of vast amounts of user data, are becoming a focal point for privacy concerns. The year 2024 anticipates an increased emphasis on regulations addressing the potential risks associated with extensive data collection by browsers. Additionally, misconfigurations and vulnerabilities in browsers and third-party extensions may lead to inadvertent data leakage, exposing sensitive information and highlighting the urgency for robust security practices.

Mobile (Account Takeover)

The mobile landscape faces a rising threat of account takeover incidents. Cybercriminals are likely to target mobile platforms to gain unauthorized access to user accounts, emphasizing the need for strengthened mobile security measures. This prediction underscores the importance of securing mobile browsers and applications to prevent unauthorized access and protect user data.

Recommendations for Security Leaders

The shift to hybrid work has introduced a multitude of challenges to cybersecurity. Blurred lines between personal and professional activities on employee devices, the proliferation of unmanaged devices, and the ever-present threat of phishing attacks all contribute to an evolving threat landscape. To effectively defend their organizations, security leaders must implement a multifaceted approach.

- **Securing Browsers:**
  Enforce strict browser policies: Mandate up-to-date browsers, and push security patches promptly.
  Implement browser extension management: Restrict unauthorized extensions, and review permissions regularly.
  Educate on phishing threats: Train to identify suspicious emails, websites, and prompts. Encourage reporting.

- **Managing Unmanaged Devices:**
  Implement conditional access Controls: Restrict data access based on device type.
  Promote BYOD policies: Establish clear guidelines for personal device usage, and outline security requirements.

- **Implementing Strong Authentication Measures:**
  Enforce Multi-Factor Authentication for all accounts: This adds an extra security layer.
  Educate employees on password hygiene: Promote strong password practices.
  Utilize Single Sign-On cautiously: Evaluate security implications.

- **Policies and Activity Data:**
  Lockdown Browsers: Enforce secure configurations and whitelist extensions.
  Control User Access: Develop a BYOD policy with data encryption and restrict access to sensitive data based on user roles.
  Monitor for Threats: Utilize tools to detect suspicious activity and analyze browser data for threats.

- **Building a Culture of Security Awareness:**
  Implement ongoing security awareness training: Educate employees on best practices.
  Promote open communication: Encourage reporting of suspicious activity.
  Lead by example: Demonstrate a commitment to cybersecurity.

Conclusion

The central role browsers have in today's enterprise is continuously reshaping the cybersecurity landscape. With personal and professional activities converging on devices, a multitude of security concerns have emerged. Browser vulnerabilities, the proliferation of unmanaged devices, and the persistent threat of phishing all pose risks to sensitive data and corporate security.

Acknowledging and addressing the browser risk landscape is an opportunity to redefine the very nature of enterprises' security architecture. By prioritizing a comprehensive approach, security leaders can make browsers the foundational security pillar in their organizations.

For further insights and best practices on securing your hybrid work environment, explore LayerX's comprehensive resources available on our website, including reports on browser security, unmanaged devices, and emerging threats.