LayerX

BROWSER SECURITY ANNUAL REPORT 2023

EXECUTIVE SUMMARY

The browser has become the number one working interface in today's enterprises. As a result it has become the focal point of a wide threat landscape that puts their data, devices, and applications at risk.

These attacks range from using the browser for malicious access to SaaS apps, to theft of sensitive data it stores, or leveraging it to compromise the endpoint it runs on. But security teams have so far regarded them as a combination of dispersed endpoint, identity and SaaS risks. As a result, there wasn't so far an attempt to analyze and understand this cyber attacks' as what they are - an evolving browser-centered threat ecosystem that increases rapidly in volume and sophistication. .

LayerX's team has conducted a wide-scope research to produce the first-ever annual browser security report, that provide comprehensive visibility and granular insights into how the adversaries' browser activities

Insights from the research

1 **Over half of all the browsers in the enterprise environment are misconfigured.** While a configured browser is nearly impossible to compromise, stealing data from misconfigured browsers is like taking candy from a baby. The Leading misconfigurations are improper use of personal browser profiles on work devices (29%), poor patching routine (50%), and the use of corporate browser profiles on unmanaged devices.

2 **3 of every 10 SaaS applications are non-corporate shadow SaaS, and no SaaS discovery/security solution can address its risks.** Shadow SaaS, and more than that, shadow identities, are the number one source for enterprise data loss. No existing data security tool (whether it being a traditional DLP or a DSPM) has access or control to what employees can do on their own personal applications.

3 **Attackers adopt evasive attack techniques that neither email security nor network security tools can detect.** Advanced browser-borne attack techniques, such as the use of SaaS applications to distribute malware or abusing high reputation sites for phishing, have become a threat commodity.

4 Traditional security tools miss over half of those attack vectors at zero hour, making targeted browser attacks into a leading cause for enterprise breaches.

5 **Most browser risks may lead to identity theft.** Weak passwords, misconfigurations and SaaS security issues all circulate around the digital identity. This depressing finding outlines a main pain point - the digital identities are still the corporate achilles heel.

This report's findings clearly show that the browser is the #1 cybersecurity blindspot, and that protection against the risks it exposes the corporate IT environment to are beyond the security teams' capability. The combination of unattended security weaknesses as a common practice in conjunction with extensive adversaries' activity that targets them introduces a challenge that security stakeholders must consider in the plan and execution of their cybersecurity architecture.

TABLE OF CONTENTS

INTRODUCTION:
THE BROWSER HAS CHANGED, SO HAVE BROWSER-RELATED THREATS

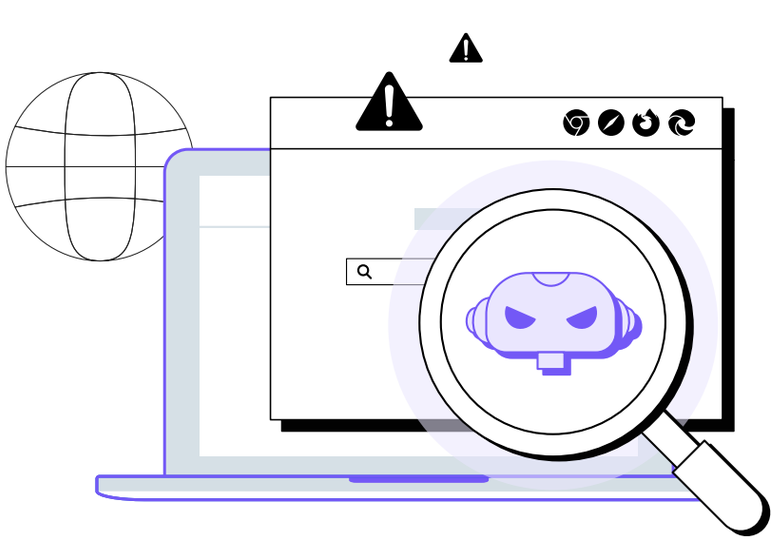
The phrase “nothing endures but change” captures the most important characteristic of cyber security: its volatility. A sound defense strategy starts with the acknowledgment that the threat landscape is ever changing. It is continuously evolving, responding to the improvements in our existing defenses and constantly developing new, and potentially harmful, attack vectors.

The report you’re about to read is the first to shed a light on what is arguably the fastest growing source of threats in today’s corporate environment – the browser. Whether as a standalone attack surface or a vector for malicious access, the browser is at the core of numerous attacks that target enterprises today.

This shouldn’t come as a surprise. It is a well known fact that the browser is now the key working interface in the modern corporate environment. However, we believe that security leaders haven’t yet acknowledged the full implications of this fact when architecting their environments’ defenses. The various stats and figures in this report add up to a disturbing reality. One that compels us to sincerely ask ourselves whether we should reevaluate the architecture of our security stacks and its underlying risk analysis and prioritizations.

Moreover, there is an even more urgent question that arises. Can the security tools employed so far provide our environments with the sufficient mettle to withstand the browser threat landscape? If not, what type of protection should we pursue?

Hence, the true value of this report is not in the numbers it encloses or the stats it cites. Rather, the value lies in its ability to drive us to ask ourselves how our own environments fare against the world it describes. Naturally, answers may vary greatly. Despite this variance, the role browsers play in today’s enterprises is significantly changing, and so is the volume of cyber risks they are exposed to. We should acknowledge this change and adjust to it, so we’re able to maintain secure environments.



BROWSER SECURITY THREATS IN 2022

Note to readers: In this report, LayerX statistics were derived from our analysis of 500 random LayerX users. Any other statistics mentioned in the report are based on a wide variety of publicly available cyber security reports.

Cyber security teams are constantly dealing with a complex array of security threats. These were the nine most prominent browser security threats in 2022:

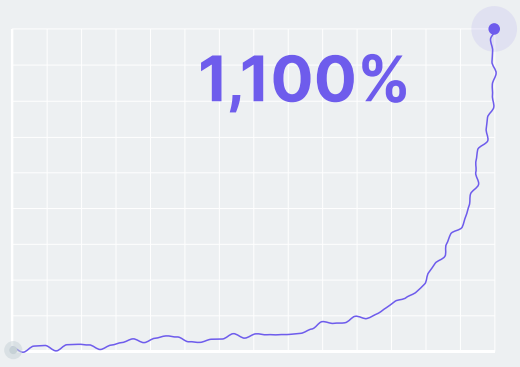
1. Phishing Attacks via High Reputation Domains
2. Malware Distribution via File Sharing Systems
3. Data Leakage Through Personal Browser Profiles
4. Outdated Browsers
5. Vulnerable Passwords
6. Unmanaged Devices
7. High-risk Extensions
8. Shadow SaaS
9. MFA Bypass With AiTM Attacks

1 Phishing Attacks via High Reputation Domains

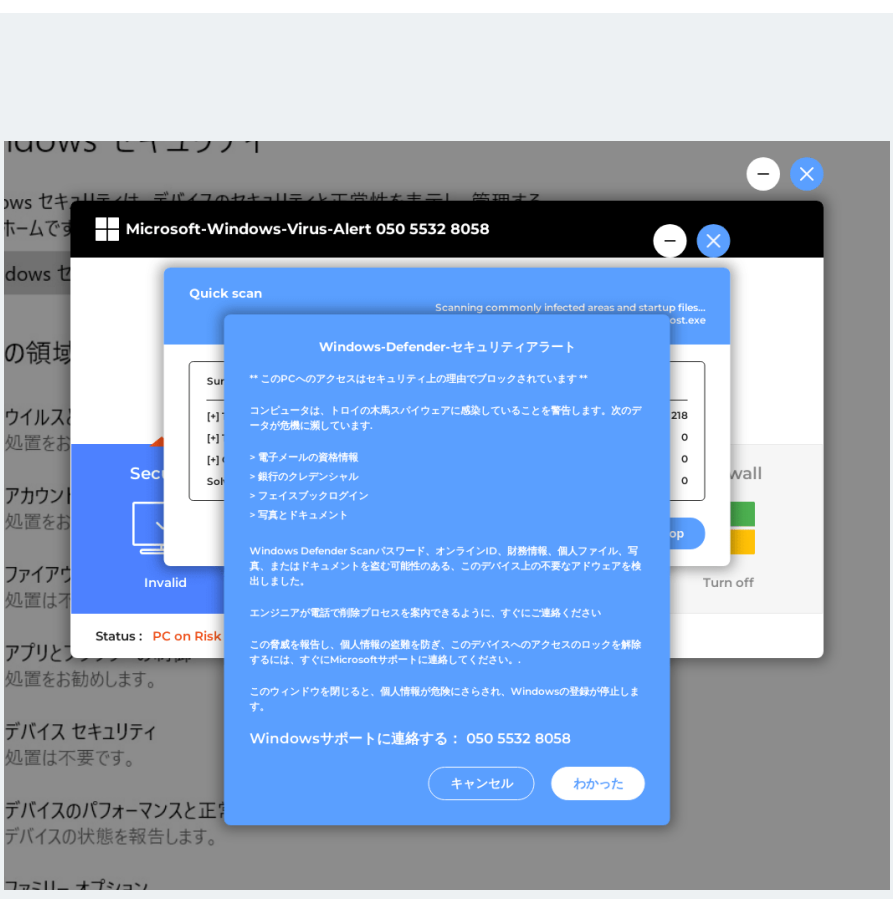
Phishing attacks weaponize websites by disguising them as legitimate assets, while they actually contain malware or other types of malicious code. To mitigate these phishing risks, many security vendors filter websites by determining the security level of the URL. This website security check is based on the domain's reputation, which is calculated by different metrics such as the age, URL history, IP reputation, the website's popularity, and more. If a site has a credible reputation, it passes the check.

Lately, there is increasing evidence of **phishing campaigns bypassing these security mechanisms by reputation jacking**. These are attacks that fool URL filtering vendors by **hosting phishing on legitimate and trusted domains**, such as Google, Microsoft, AWS, GitHub, and more. The credible reputation of these domains allows the attacks to "latch on" and easily bypass the reputation filters.

According to research by Palo Alto Networks' Unit 42, between June of 2021 and June of 2022, **the rate of newly-detected phishing URLs hosted on legitimate SaaS platforms increased by over 1100%**



Here is an example of a phishing website on a Microsoft-owned domain, bmtdfbwddf.blob.core.windows.net:



Source

In an experiment LayerX conducted, we tested the ability of commercial browsers and network security tools to detect 1-day phishing sites (which were already detected by at least one security vendor) hosted on high reputation domains. We found:

The best performing **browser** had a

36% catch rate

missing approximately two thirds of all attacks

The best performing **Network Security** solution had a

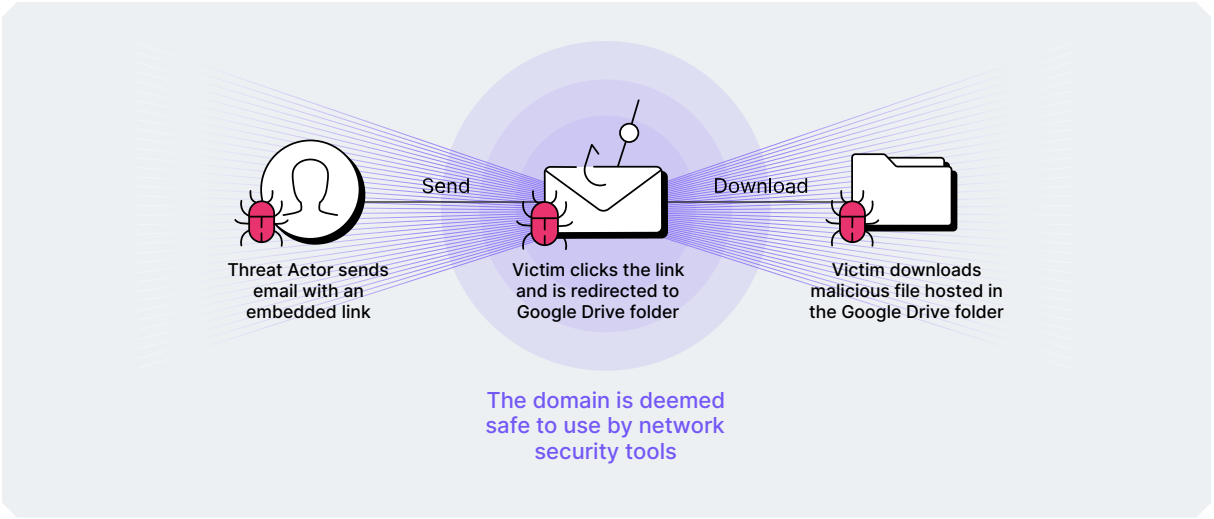
48% catch rate

missing more than 50% of all attacks

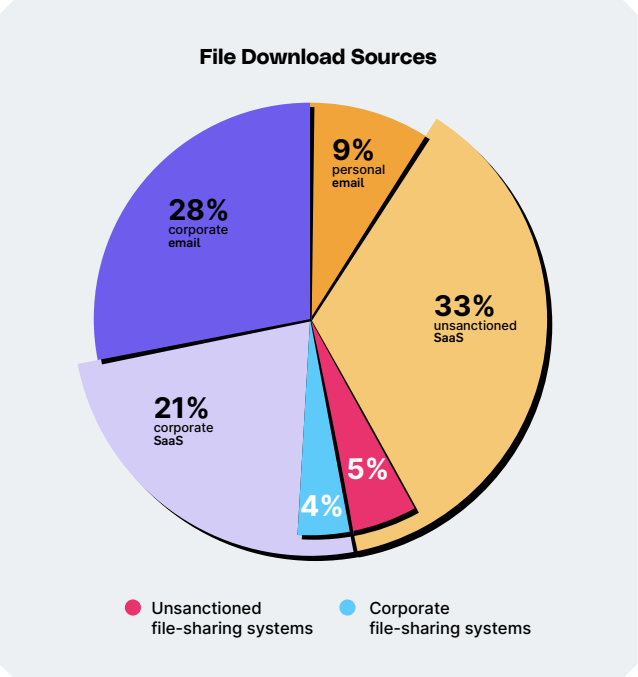
2 Malware Distribution via File Sharing Systems

P2P (Peer-to-peer) file-sharing platforms can be used to distribute malware. In these types of attacks **threat actors place malicious content on trusted file sharing sites** to gain access to users' devices and to spread malware.

For example, in one case Chinese hackers sent embedded links to Google Drive and Dropbox folders which contained malware. These sites have a good reputation, which enabled to capture them to circumvent security mechanisms. This makes it **especially difficult for network security tools,** because they may fail to notice the malicious files as they are stored in legitimate file sharing websites.



In effect, malware files can be distributed both through sanctioned and unsanctioned file sharing systems. This means that malware can be hosted on widely-used, legitimate apps such as Google Drive or Microsoft OneDrive, which are approved by IT. **From analyzing random users' file downloads we found that around 9% of files are downloaded from file sharing systems. These downloads split fairly evenly between corporate (5%) and unsanctioned (4%) file sharing systems.**



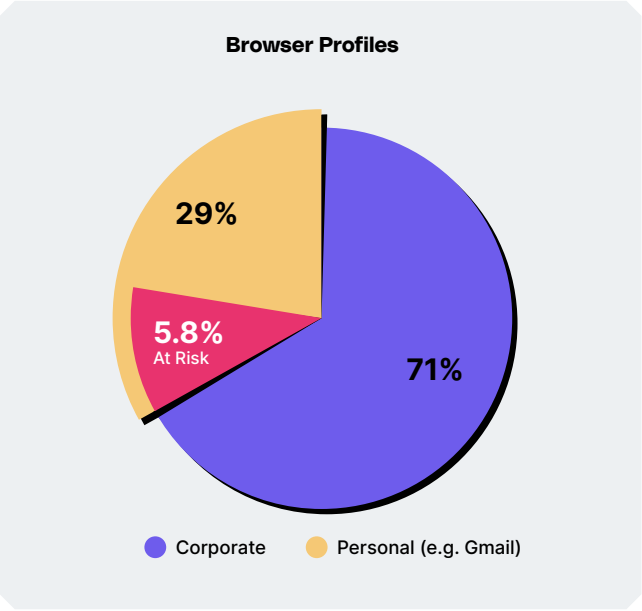
3 Data Leakage Through Personal Browser Profiles

Using personal profiles in a work setting can lead to multiple security risks:

- The Chrome browser syncs passwords from websites and apps, which can accidentally lead to sensitive **corporate passwords being synced to personal devices.**
- File uploads to personal cloud and file sharing systems is a **major data loss risk** because it can expose sensitive company data.
- Usage of corporate apps with personal profiles can lead to **corporate data leakage** because it increases the risk of data being accidentally or intentionally shared outside of the company.

An analysis conducted by LayerX on 500 random browsers found that:

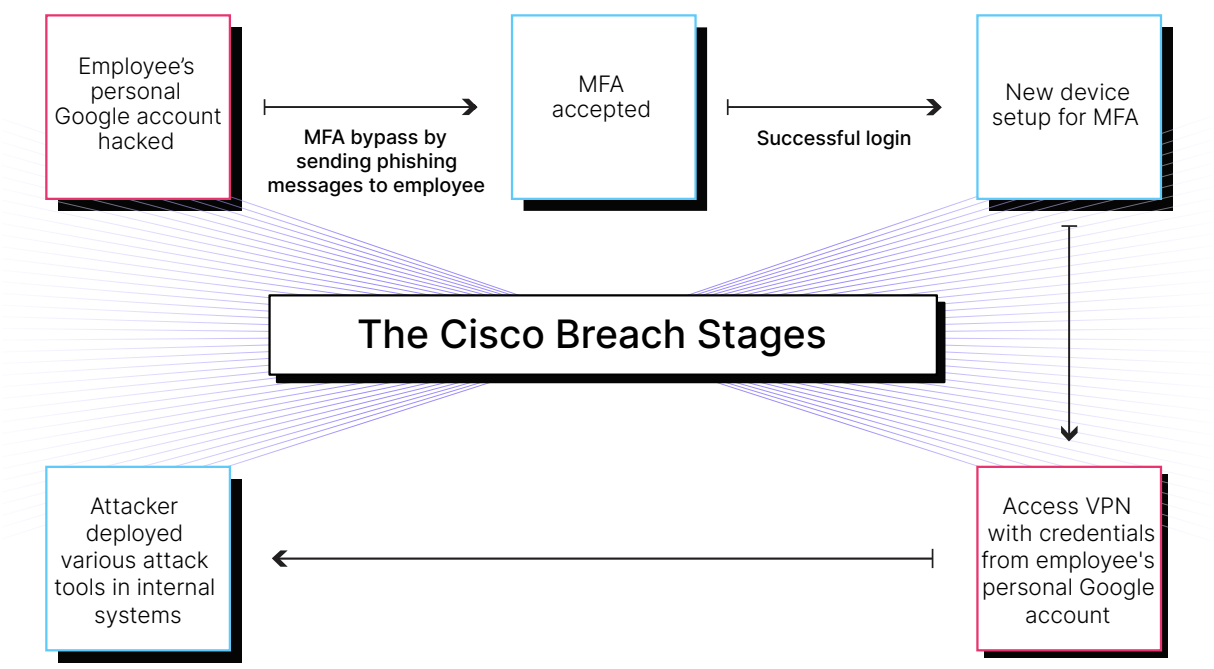
- **29%** of browsers are connected to personal profiles.
- **5.8%** of identities connected to the inspected browser profiles have been exposed in data breaches, which puts credentials involving these identities at risk.



Use Case: Cisco Cyber Attack

- A Cisco employee's credentials were compromised when attackers gained control of his **personal Google account.**
- The employee had enabled **password syncing** and had stored his Cisco credentials on his personal Google Chrome browser.
- The attackers then sent phishing messages to the employee to bypass the MFA security control.
- After evading the MFA mechanism, the attackers **connected to Cisco's VPN with additional credentials they found on the employee's personal browser profile.**
- Finally, they gained access to the company's internal system.

Source

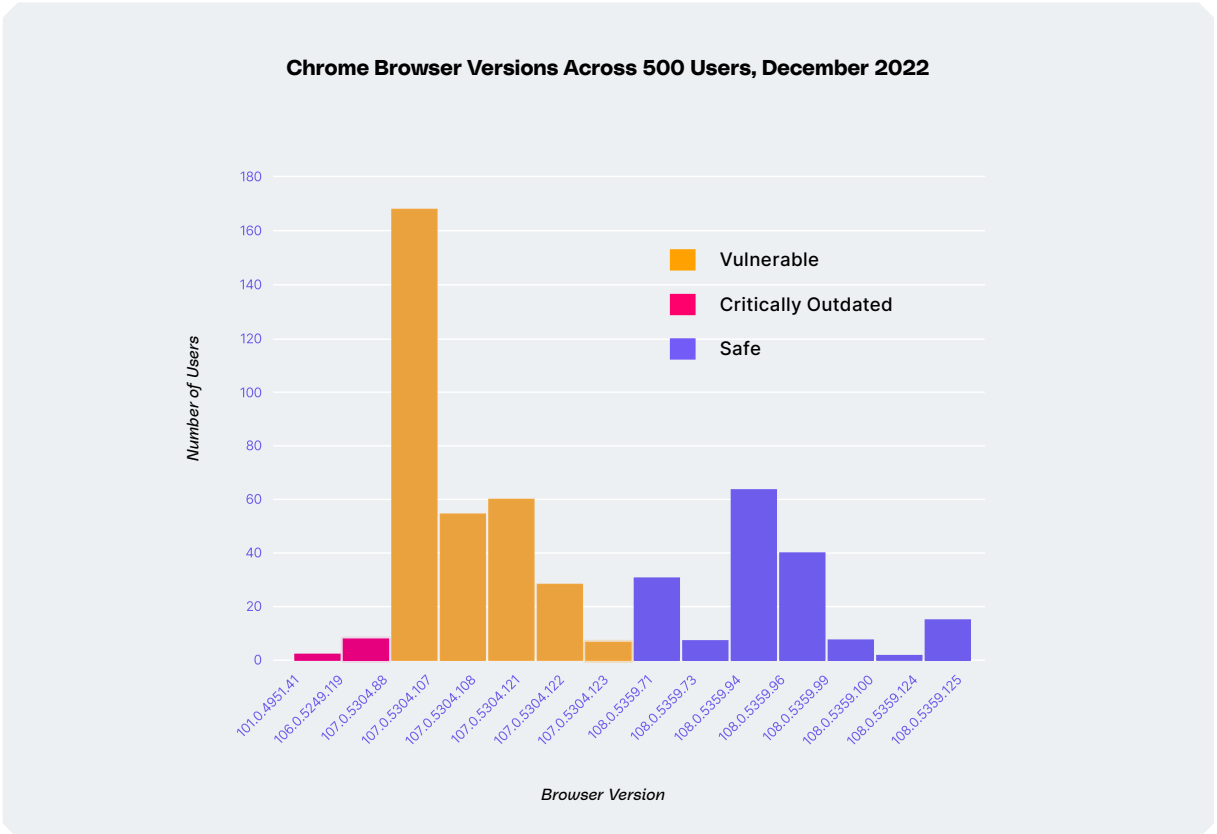


4 Outdated Browsers

New browser updates contain crucial security patches or fixes, usually concerning recently discovered information security vulnerabilities and exposures, also known as CVEs. When a new critical CVE is discovered in the wild, Chrome publishes a new version with the relevant security update.

Patching time is critical. While critical Chromium zero-day vulnerabilities cost attackers up to millions of dollars to produce, when they become 1-days their exploitation cost drops dramatically. After a few months, the technical description of the vulnerability is disclosed and the exploitation becomes a cheap commodity for cyberattackers to use. **Unpatched browsers are vulnerable to these attacks.** Therefore, the faster the browser is updated, the lower the risk.

We analyzed data from 500 browsers and found that **a significant number of users' browsers remained outdated and vulnerable to known CVEs**.



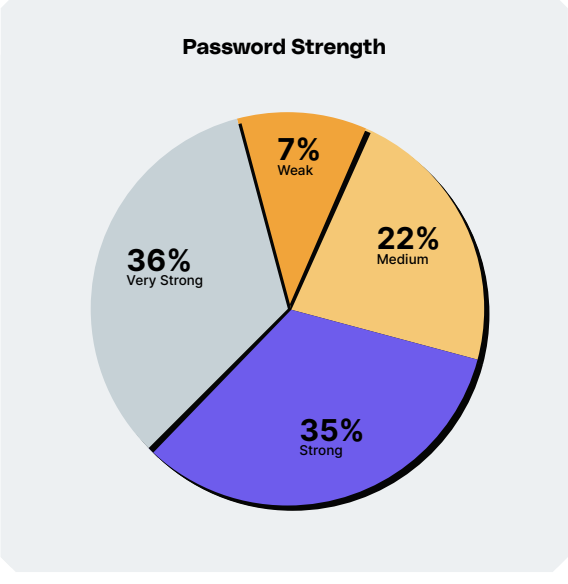
5 Vulnerable Passwords

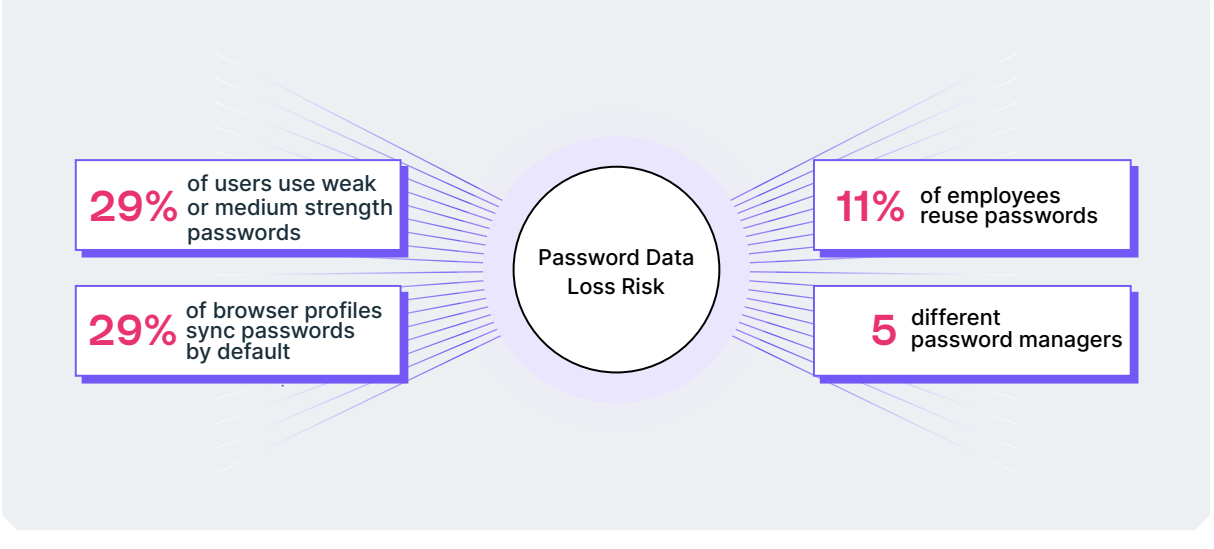
Weak passwords and password reuse continue to be leading factors in data breaches. Approximately **70%** of successful breaches involve the use of lost or stolen credentials, brute force attacks (guessing weak passwords) or exploiting reused passwords on different websites.

Additionally, widespread usage of personal Chrome profiles lead to **password syncing across devices.** This increases the potential attack surface as well as the risk of malicious actors finding passwords. Companies face another significant password hygiene risk from many **unsanctioned password managers,** which control employees' passwords without any IT supervision or approval, and might be breached by hackers. Passwords might then be sold to third parties.

An analysis conducted by LayerX on 500 random browsers found that:

- **29%** of users use weak or medium strength passwords.
- **11%** of users reuse passwords regularly.
- **29%** of browser profiles are personal and sync passwords by default.
- An average of **5** unique password managers were detected.





6 Unmanaged Devices

As remote work is exploding worldwide, employees are using personal desktops, laptops, servers, tablets, and mobile devices for work. These **unauthorized devices connect to sensitive company data** through organizational assets such as internal company networks, SaaS applications, sensitive files, and software.

These unmanaged devices are unsupervised by, or unknown to, the IT department. As a result, they **lack appropriate security protections** that managed devices have. This makes them **an easy gateway for cyberattacks** into the organizational network: a compromised unmanaged device may lead to persistent access to SaaS applications and severe identity theft attacks.

A Forrester survey found that

69%

of respondents claimed half or more of the devices were unmanaged

Due to COVID-19 and the rise of remote work, the number of endpoint devices needed to be managed by the NYC Municipality increased sevenfold.

Source

Unmanaged Devices Pose a Security Risk for Organizations

Criteria	Managed Devices	Unmanaged Devices
Company security tools (EDR, Network Security)	✓	✗
IT visibility and device management	✓	✗
DLP policies	✓	✗
Updated OS and browser	✓	✗
Authorized access to company data	✓	✗
SSO logins	✓	✓

7 High-risk Extensions

Browser extensions are a very attractive attack vector because they can grant excessive permissions once installed on the browser. In a recent study of Chrome extensions with a minimum of 1000 downloads, Incogni researchers found that **nearly half (48.6%) potentially pose a high security or privacy risk.** These extensions receive permissions that enable them to collect personally identifiable information (PII), spread adware and malware, and access passwords and financial data (in a recent study).

Of the many potentially risky extensions **a few are overtly malicious.** Malicious extensions can be installed in various ways and are usually disguised in an attempt to dupe users. Here is an example of one:

Use Case: Vipersoft

- Vipersoft distributes **malware** through cracked games and downloadable.exe files.
- The malware then installs **a malicious extension named Venomsoft** on Chrome-based browsers.
- The extension **steals user passwords and cryptocurrency.**
- The extension tries to disguise itself as well-known and common browser extensions such as Google Sheets.

Risk: Critical

A LayerX analysis conducted on 500 random browsers found multiple instances of problematic extensions.

38%
of extensions grant excessive permissions

3
malicious extensions

8
extensions were removed from the Chrome Store

Extensions removed from the Chrome Store were found to violate Google's privacy or security standards.

66
low reputation extensions

11
non-compliant extensions

Extensions that don't comply with company security and privacy policies.

8 Shadow SaaS

Shadow SaaS refers to the use of unapproved Software as a Service (SaaS) applications within an organization. These applications may be used by employees for work related tasks, but they have **not been formally sanctioned or approved by the company's IT department.**

There are several security risks associated with Shadow SaaS. First, these apps don't meet the security requirements that IT-approved apps are obliged to have. This can increase the **risk of data loss of malware infection.** In addition, Shadow SaaS apps are not integrated with the company's security and management systems, making it more difficult to track and monitor their use. Finally, the use of Shadow SaaS apps decreases the company's ability to comply with Data & Privacy regulations. Uploading sensitive company data to unapproved apps violates regulations, may compromise personal information and can lead to fines and legal procedures.

70%

of organizations run cloud applications that are not officially sanctioned by their IT departments

67%

of users have introduced their own collaboration tools into their organizations

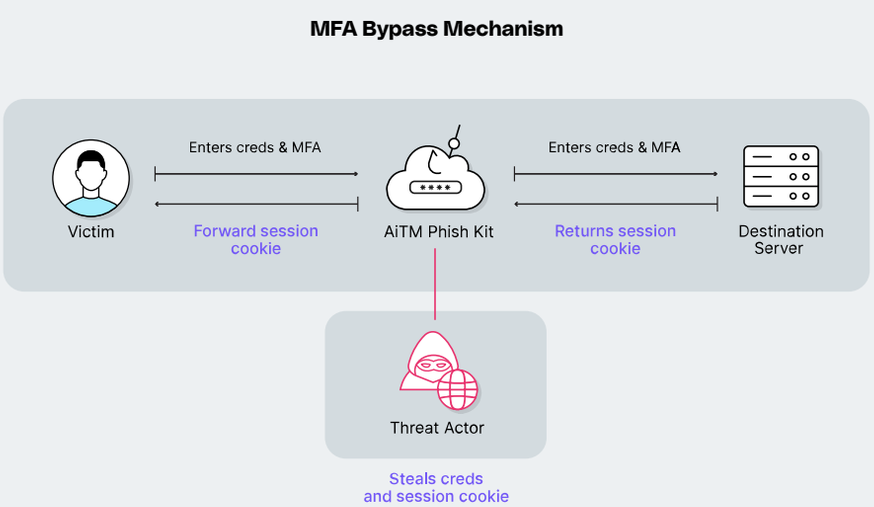
31%

of apps used by employees are connected to non-corporate identities

9 MFA Bypass With AiTM Attacks

Credential phishing, i.e stealing users' logins and passwords or fooling them into providing them, has been practiced for a long time by hackers. With the introduction of MFA (Multi-Factor Authentication) it has become harder for attackers due to the additional verification the user needs to provide for the login.

To counteract this, attackers leverage real-time attacks against MFA protected systems, in the form of "Adversary in the Middle" (AiTM). The AiTM approach, **places an attacker in the middle of the authentication process,** between the client and server to intercept the exchange and steal credentials. Intercepting the MFA authentication information allows the attacker to **bypass the MFA and access the sensitive data.** A recent Okta report found a dramatic rise in MFA bypass attacks over the past two years.



Source

BROWSER SECURITY ANNUAL HIGHLIGHTS

Here are the main news stories that left a mark in the world of browser security in 2022:

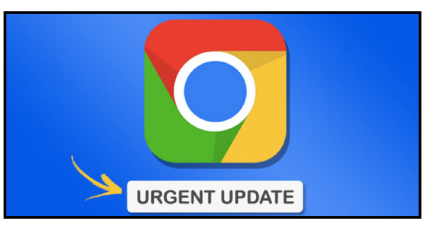
JANUARY

Hackers Use Video Player to Steal Credit Cards From Over 100 Sites

Hackers used a cloud video hosting service that injected malicious scripts to steal information inputted in website forms. The scripts, known as form jackers, steal sensitive payment information entered into forms on the hacked websites (Source).

FEBRUARY

Google Confirms First Chrome Browser Zero-Day Hack of 2022



Google rolled out a version update to address CVE-2022-0609, described as a use-after-free vulnerability, with the ability to run an execution of arbitrary code on affected systems (Source).

MARCH

Browser in the Browser Attack Caught in the Wild

A phishing technique called Browser in the Browser (BITB) has emerged, which consists of simulating a browser window within the browser to spoof a legitimate domain. It has since become a dangerous attack vector preferred by cyber criminals (Source).

APRIL

Chrome Emergency Update Fixes RCE Zero-Day

Google has released a Chrome update to fix a high-severity zero-day vulnerability bug tracked as CVE-2022-1364, which enables remote code execution due to a V8 type confusion weakness (Source).

MAY

Tech Giants Announce Support for Passwordless Logins

Microsoft, Apple, and Google announced plans to support a common passwordless sign-in standard (known as passkeys). This will allow the three tech giants' users to log in to their accounts without using a password (Source).

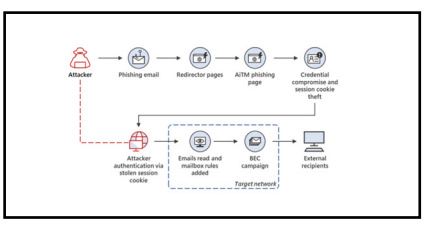
JUNE

Internet Explorer Ends

After finally reaching its end of life, the Internet Explorer desktop application will be disabled. It will be replaced with the new Chromium-based Microsoft Edge (Source).

JULY

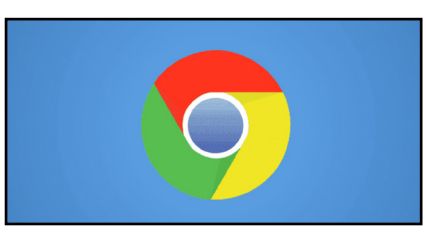
Large-Scale AiTM Phishing Campaign



Microsoft discovered a large-scale phishing campaign targeting over 10,000 organizations. The campaign uses adversary-in-the-middle and can bypass MFA (Source).

AUGUST

5th Zero Day Vulnerability



August marks the fifth zero-day vulnerability in Chrome that Google has resolved since the start of the year (Source).

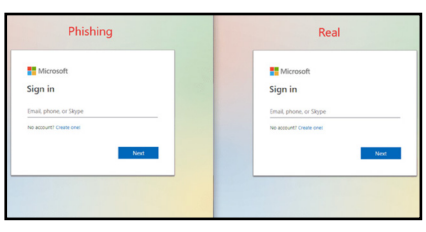
SEPTEMBER

Uber Data Breach

Uber confirmed reports of an organization-wide cybersecurity breach that started with a Social Engineering campaign on employees, where a hacker used stolen credentials found online, and then gained access by an MFA prompt bombing an employee for over an hour until the employee complied (Source).

OCTOBER

New Type of Phishing Attack



Hackers can use 'App Mode' in Chromium browsers for stealth phishing attacks (Source).

NOVEMBER

Cloud9 Malicious Extension

A malicious extension lets attackers control Google Chrome remotely (Source).

DECEMBER

Lastpass Customer Data Breach

LastPass

LastPass has confirmed, for a second time this year, that hackers have gained access to a third-party cloud storage service that contained personal customer data (Source).

2023 PREDICTIONS

What can security professionals expect the upcoming year to bring for browser security? Our experts share their predictions:

1. **SaaS will be a governance and security pain point.** The steady increase in SaaS application adoption will continue. As the SaaS environment grows, it will become harder to manage, creating more and more blind spots, shadow apps, and overall unmanaged identities, employee devices and resources. Maintaining governance over the endlessly piling SaaS applications may be time-consuming and overwhelming for IT departments.

2. **Attacks will be increasingly SaaS-based and less file-based.** The proliferation of SaaS apps usage within the enterprise environment will decrease the portion of traditional files within it respectively. This will be reflected in the threat landscape as well, with more attacks moving from being file execution-oriented to focusing on malicious access to SaaS and web apps. The share of web and cloud based attacks is expected to grow.

3. **The browser will become the main attack surface.** The unique position of the browser as the default tool for both work and private use will drive more adversaries to turn personal browser usage into an attack vector for accessing work resources. Attackers will try to maliciously access enterprise data by going after employees' personal browsers, because of the dual utility of the browser. This, in turn, will compel security teams to treat all browsing activity as a single, consolidated attack surface.

4. **Malicious web pages will become more sophisticated.** The web technology evolution provides users with a browsing experience that is more rich, dynamic and responsive. Yet, it also has a flip side, arming adversaries with the ability to conceal sophisticated attacks within web pages that can avoid the detection of traditional security measures. This growing complexity of web applications will increase security blind spots.

RECOMMENDATIONS FOR SECURITY LEADERS FOR 2023

Forward-thinking security leaders should examine the need for browser security awareness and controls in their organizations. Here are a few recommendations that can be implemented immediately:

1 GET 360⁰ SAAS VISIBILITY AND CONTROL.

The ability to discover and monitor all of your resources and activities is the foundation on which every sound security architecture should be built. It's imperative for security teams to apply this insight to the SaaS environment. In a more actionable manner, the prerequisite from any solution that presumes to secure your SaaS environment is effortless and comprehensive visibility - sanctioned and unsanctioned apps alike.

2 TURN THE BROWSER INTO THE FIRST LINE OF DEFENSE.

The only way to confront the rapidly evolving browser attack surface is to mount real-time visibility and threat protection on the browser itself. Continuous monitoring, risk analysis, and active response can be applied to every browsing event. These actions will not only turn the browser into a managed and controlled attack surface, but they will also transform the browser into a key pillar in the enterprise's security architecture.

3 IMPLEMENT IDENTITY-BASED SECURITY.

Identity-based access to apps can improve security by enforcing strong passwords and multi-factor authentication. Furthermore, Centralized identity management makes it easier for enterprises to manage and track user access to different systems and applications, helping to ensure that only authorized users have access to sensitive data. This can improve efficiency by simplifying the process of granting and revoking access for users and providing a single point of control for managing user identities.

4 DON'T STOP DIGITAL TRANSFORMATION - ACCELERATE IT.

SaaS is here to stay and scale, which is a productivity game changer. Embrace this change while ensuring that you can vouch for its security. Consolidation is the only cybersecurity strategy that makes sense. The one place in which you should consolidate your SaaS-related security controls is the browser, since it is the single access source, by both legitimate users as well as threat actors.

CONCLUSIONS

This report sheds a light on the key role the browser has in today's threat landscape. Put to use as the main worktool and gateway to internet access, naturally the browser has become a widely used attack surface by malicious actors. While every security stakeholder is probably aware of this phenomenon to a certain degree, the purpose of this report is showcasing its true scope, which can no longer be ignored.

Hence, the report's effectiveness is measured by its ability to drive its readers to ask themselves the following constructive questions:

- Which risks and trends described in the report am I familiar with in my environment?
- Do I have the protective measures in place to detect and prevent these threats?
- Are these protective measures effective enough?

Answering these questions will reveal whether there's a need to update your security strategy so it can deliver the protection your environment needs.

Continuing to rely on network-based or proxy-based solutions may fail to prevent your workforce from accessing malicious web pages. As we have shown above, they are simply not sufficient for detecting high-reputation domain phishing attacks. What about malicious extensions and their great potential risks? Unfortunately, various endpoint protection solutions don't cover those. In fact, the common denominator of all the threats described in this research report is that they are not adequately covered by network, endpoint, or cloud protection solutions.

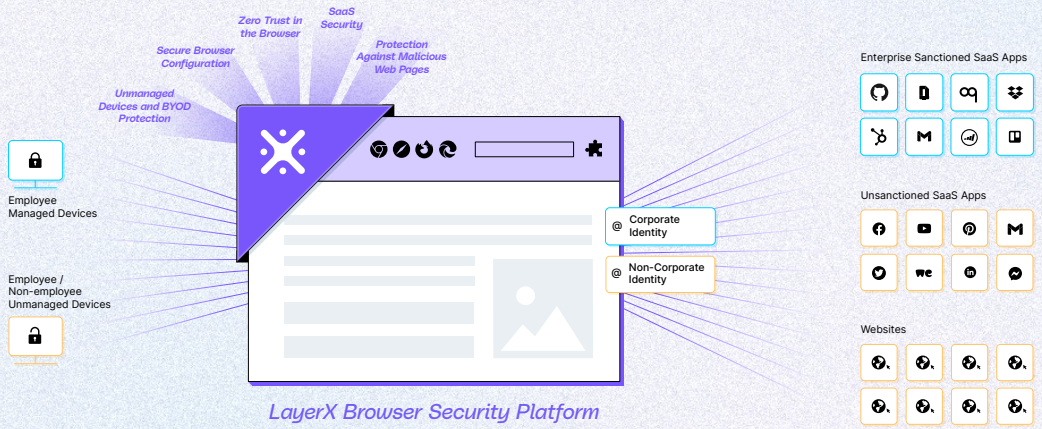
Many security challenges go unanswered because the browser remains a black box that is protected insufficiently. The rapid changes in the threat landscape serve as a wake up call for all who want to be one step ahead in the world of cyber security.

ABOUT LAYERX

LayerX provides a Browser Security Platform that's purpose-built to monitor, analyze, and protect against web-borne cyber threats and data risks. Delivered as a browser extension, LayerX natively integrates with any commercial browser, transforming it into the most secure and manageable workspace. Using LayerX, customers gain comprehensive protection against all threats that either target the browser directly or attempt to utilize it as a bridge to the organization's devices, apps, and data.

LayerX monitors every web-session at its most granular level to detect and disable risky activity at its utmost early stage with near-zero disruption to the user's browsing experience. With LayerX your workforce can securely browse anywhere.

Request Demo



KEY BENEFITS

Eliminate critical blind spots

Gain the most granular visibility into unsanctioned apps, shadow identities, DNS over HTTPS, SaaS apps, and dynamic websites.

Real-time protection

Enforce access & activity policies to restrict browsing activities that expose your apps, devices, and data to compromise.

High-precision risk detection

Multilayered AI analysis of every user activity and web session flags anomalies that can indicate risk in the browser session.

Unified browser management

Manage and configure your workforce's browsers from a single, centralized interface.

Bring your own browser

Enable your users to keep on using their browser of choice for both work and personal use.

Rapid deployment

Deploy across your entire environment and integrate with browser management tools and identity providers in a single click.