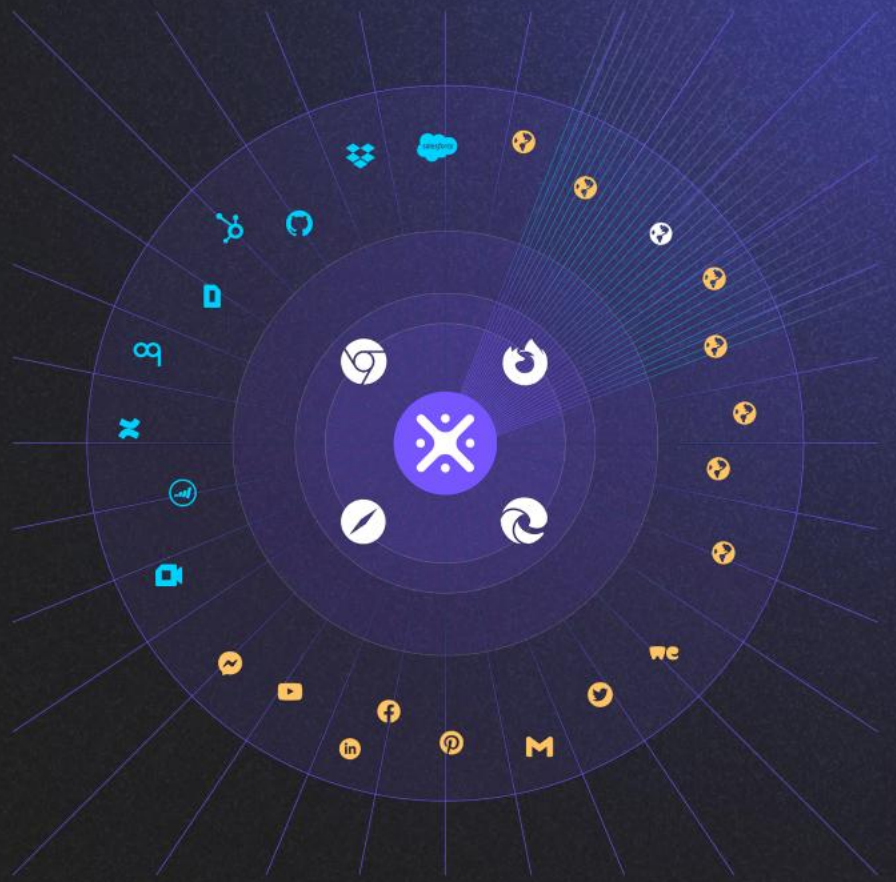
LayerX

Stealing User Credentials and Data With Malicious Browser Extensions



Or Eshed

Or Eshed

- Co-founder and CEO of LayerX Security
- 15+ years of cybersecurity experience as an ML developer, security researcher, and analyst
- Responsible for takedown of one of largest compromised browser campaigns in history (15+ M browsers, 16 bad actors put in jail)

Agenda

Part I: Understanding the Security Threats of Browser Extensions

Part II: How Malicious Browser Extensions Can Compromise Password Data

Part III: A Framework for Mitigating the Risks of Malicious Browser Extensions

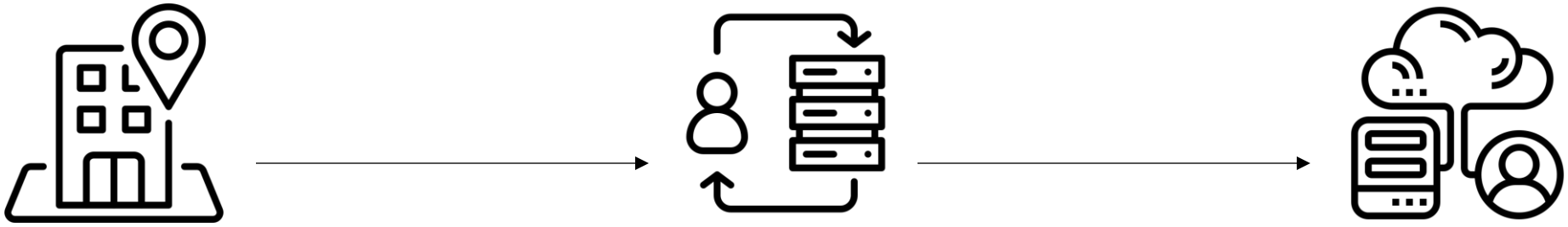
Objective for This Session:

1. Understand the risks posed by malicious browser extensions
2. Understand the key permissions relevant for credential compromise, and their capabilities
3. Understand the key tactics and tools to protect against malicious browser extensions

INTRODUCTION:

Browsers and Identities

The Evolution of Authentication



Physical

- Based on physical location
- IP-based
- Fixed separation of work/personal

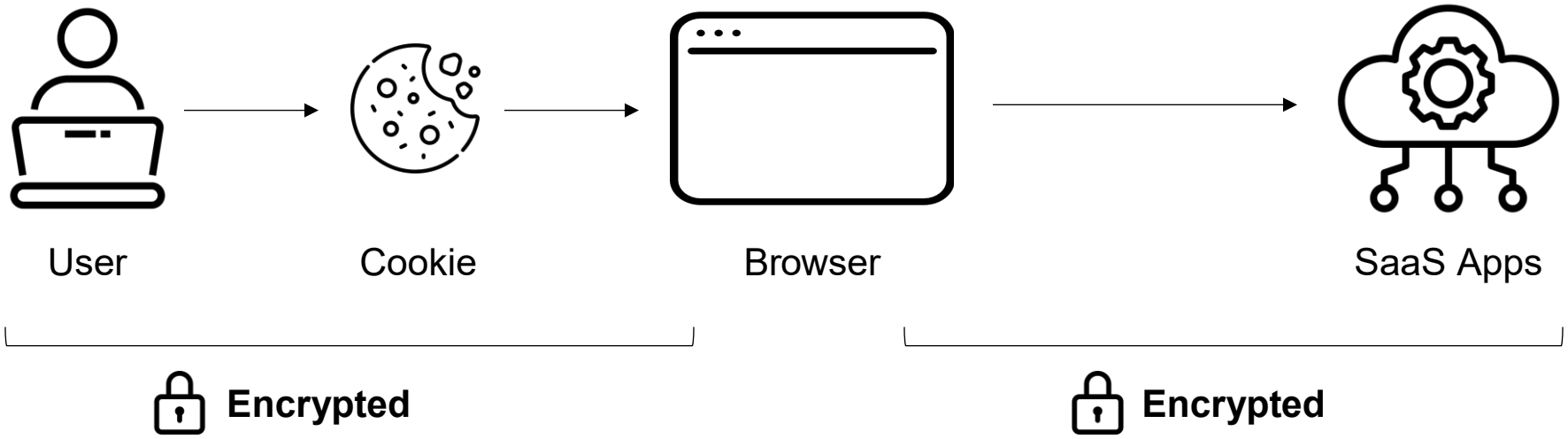
Client/Server

- Based on logical identity
- Password-based
- Distinction between work/personal apps

SaaS

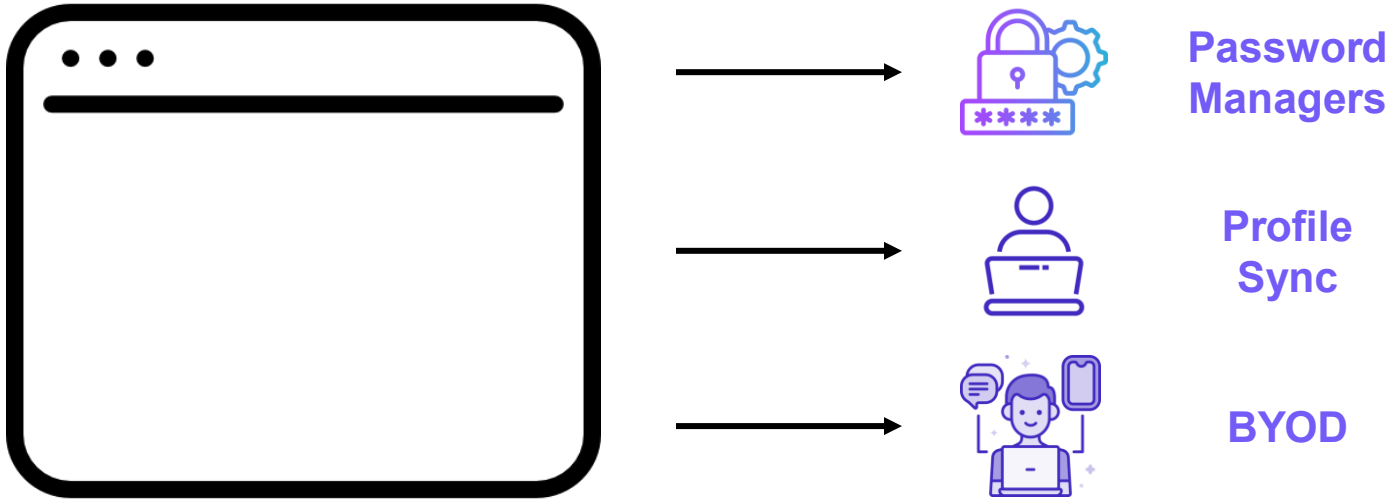
- Many apps, many identities
- Multi-tenant apps used for both work, personal
- Cookie-based persistent authentication

Cookies, Browsers Are Points of Failure



What Happens if You're Inside the Browser Session?

Zero Trust is Dead in the Browser



How Do You Know That Your Users Are *Your* Users?

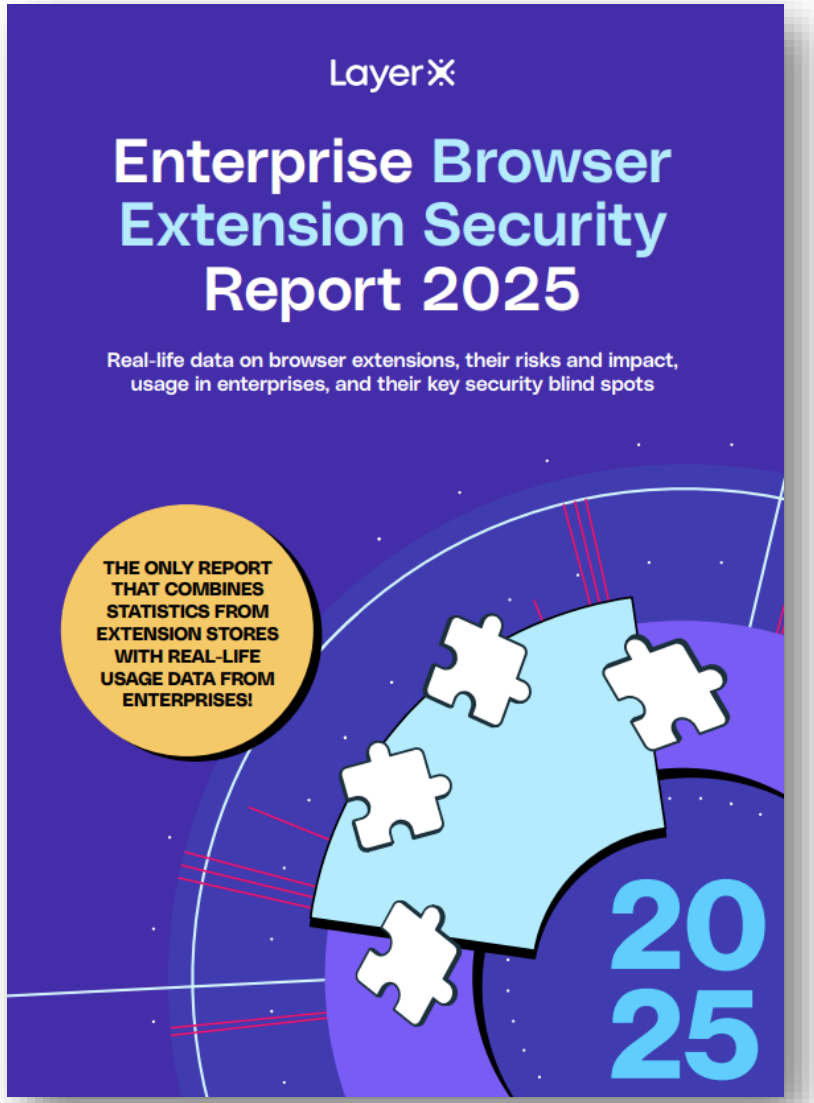
PART I:

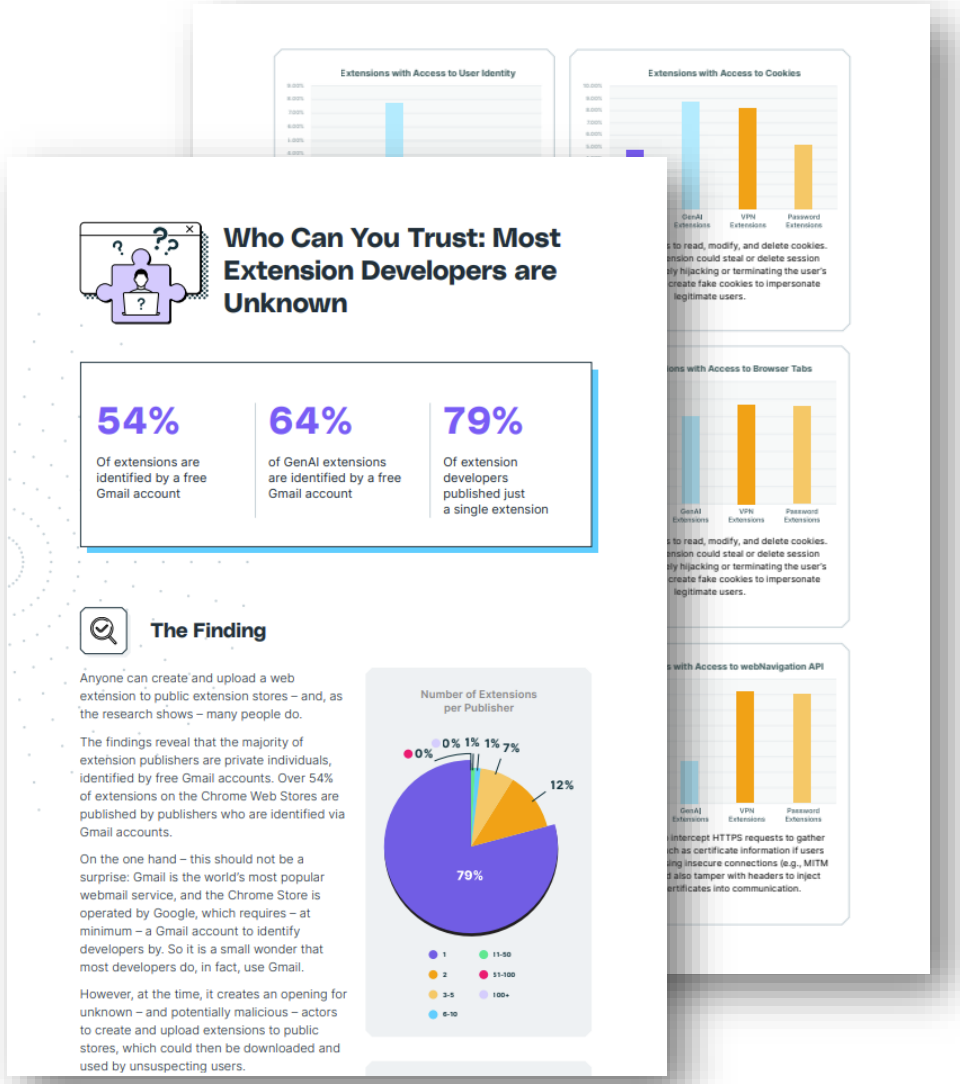
Browser extensions are the biggest security threat surface you don’t know about

What is an extension?

- Running in the browser (agentless)
- Both ‘agent’ and ‘network’ functionalities
- Visibility to unencrypted traffic and data (including network and storage)
- Can use (or abuse) browser access and visibility
- Over time - only the ID and installations of an extension are persistent, and everything else can mutate endlessly
- Using permissions that are here to stay…

2025 LayerX Extension Security Report





Browser Extensions Are Ubiquitous in Enterprise Environments

99%

Of enterprise users have at least *one* browser extension installed on their computer

53%

Of enterprise users have *more than 10* browser extensions installed on their endpoints

The Extension Threat Surface is Everyone

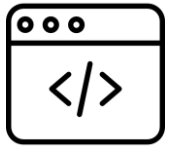
Browser Extensions Have Extensive Access to User Credential Data

53%

Of *enterprise users* have extensions with ‘high’ or ‘critical’ –level permissions

11%

Of *enterprise users* had extensions that had access to cookies



15%

Of extensions on the Chrome Web Store can access scripting permissions

Browser Extension Publisher Reputation is a Black Hole

54%

Of extensions are identified by a free Gmail account

89%

Of extensions in the Chrome Store have fewer than 1,000 installs

79%

Of extension publishers have published just a single extension

Why Malicious Extensions Are Such an Effective Attack Vector?

Ubiquitous	Most users have browser extensions installed in their browsers, they are not perceived as a threat
(Mostly) Harmless	The vast majority of browser extensions are legitimate and offer meaningful productivity benefits
Invisible to Existing Solutions	Existing EDR/XDR and network security solutions don’t have visibility into browser extension activity

How Browser Extensions Become Compromised?

Developed as malicious extension	A browser extension developed from the start as malicious	**Example**: “ChatGPT for Google”
Compromised legit. extension	A legitimate extension that has been compromised with malicious code	**Example**: Cyberhaven
Ownership transfer	A legitimate extension that has been purchased by bad actors	**Example**: YouTube+
Sideloaded by malware	3rd-party malware that ‘sideloads’ an extension to steal browser data	**Example**: Qcom Search Bar

The Hacker News

Dozens of Chrome Extensions Hacked, Exposing Millions of Users to Data Theft

Dec 29, 2025 Ravie Lakshmanan

A new attack campaign has targeted known Chrome browser extensions, leading to at least 35 extensions being compromised and exposing over 2.6 million users to data exposure and credential theft.

The attack targeted publishers of browser extensions on the Chrome Web Store via a phishing campaign and used their access permissions to insert malicious code into legitimate extensions in order to steal cookies and user access tokens.

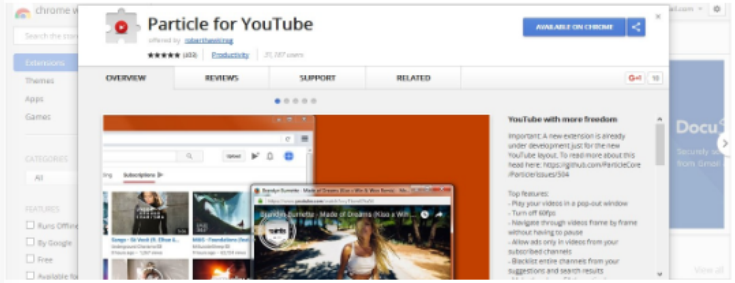
The first company to shed light the campaign was cybersecurity firm Cyberhaven, one of whose employees was targeted by a phishing attack on December 24, allowing the threat actors to publish a malicious version of the extension.

BLEEPINGCOMPUTER

"Particle" Chrome Extension Sold to New Dev Who Immediately Turns It Into Adware

By Catalin Cimpanu

July 13, 2017 11:55 AM 6



A company is going around buying abandoned Chrome extensions from their original developers and converting these add-ons into adware.

This scheme came to light two days ago when the users of a popular Chrome extension began complaining about an update that requested two intrusive permissions that the extension never used, or would have never had a reason to. The two permissions are:

- Read and change data on (all) websites visited
- Manage apps, extensions, and themes

The Chrome extension in question is named Particle (formerly known as YouTube+) and is a simple tool that allows users to change the UI and behavior of some of YouTube's standard features.

The Hacker News

Fake ChatGPT Chrome Browser Extension Caught Hijacking Facebook Accounts

Mar 23, 2023 Ravie Lakshmanan

Google has stepped in to remove a bogus Chrome browser extension from the official Web Store that masqueraded as OpenAI's ChatGPT service to harvest Facebook session cookies and hijack the accounts.

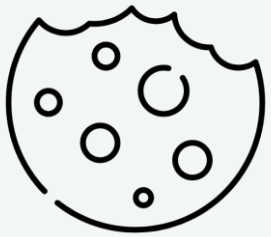
The "ChatGPT For Google" extension, a trojanized version of a legitimate open source browser add-on, attracted over 9,000 installations since March 14, 2023, prior to its removal. It was originally uploaded to the Chrome Web Store on February 14, 2023.

According to Guardio Labs researcher Nati Tal, the extension was propagated through malicious sponsored Google search results that were designed to redirect unsuspecting users searching for "Chat GPT-4" to fraudulent landing pages that point to the fake add-on.

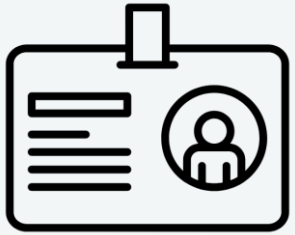
EXPLOITATION:

Browser extensions are the biggest *password security* threat that you don’t know about

How Can Malicious Extensions Steal Credential Data?



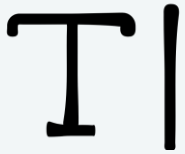
Cookies



Identities

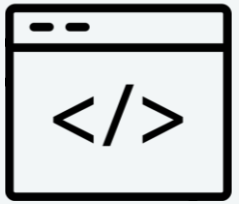
Password Stores

Client Certificates

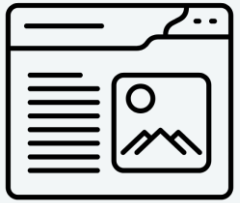


Text Input

Clipboard Data



Browsing Metadata



Page Contents

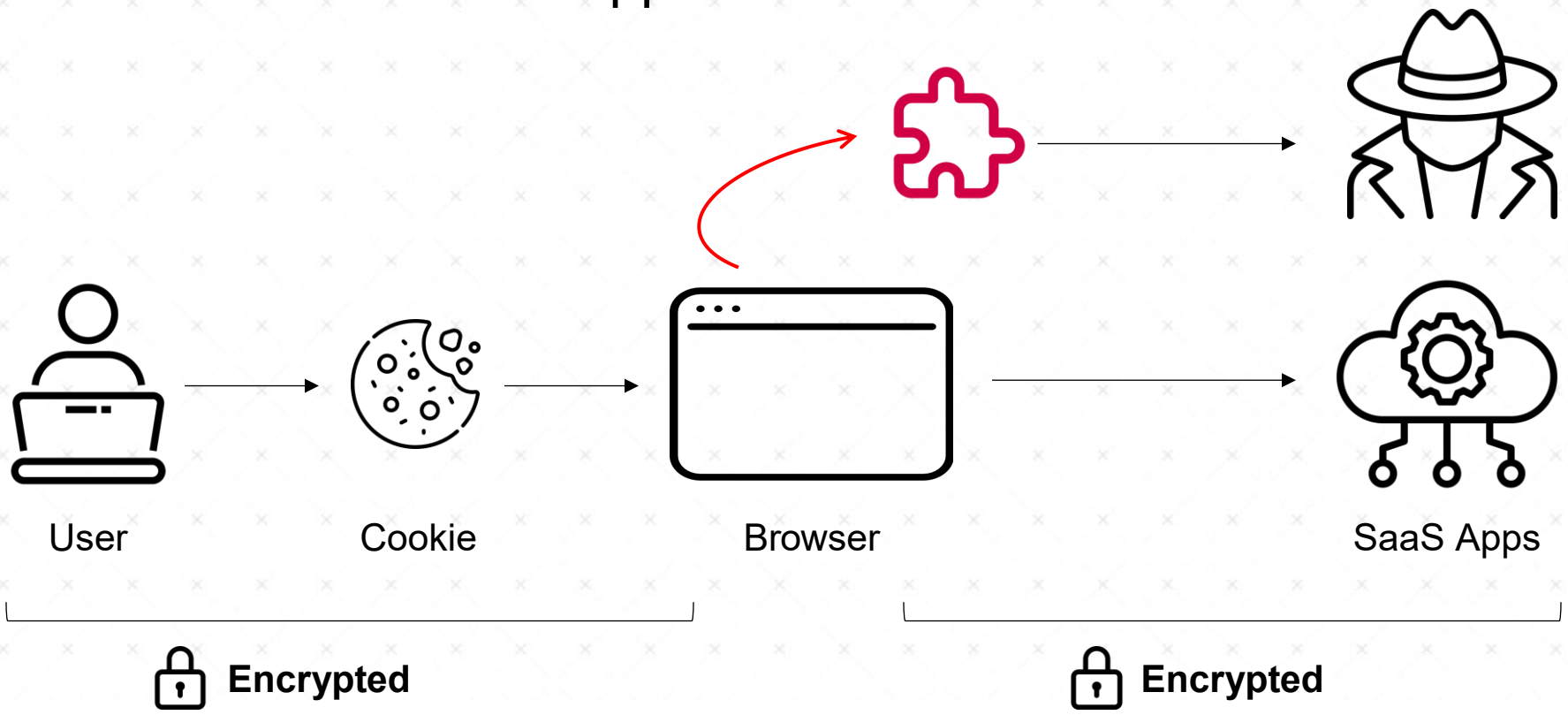
(Sample) Key Permissions That Can Be Used to Steal Password Information

Permission	Key Capabilities	How They Can Be Abused
cookies	Read, modify or delete cookies	Steal, modify or delete session cookies or create fake session cookies to impersonate legitimate users
webRequest	Observe and intercept network requests, and modify request headers	Malicious extensions could intercept session cookies or modify request headers to impersonate users or disrupt active sessions
scripting	Enables injection of JavaScript into web pages	Could be used to forge or manipulate certificate-like data used in web applications (e.g., spoofing clientside validation of certificates).
Content scripts	Run in the context of web pages and interact with the DOM	Could be used to scrape tokens stored in cookies, localStorage, or as hidden form fields on web pages

Sample TTP #1:

T1539 - Steal Web Session Cookies

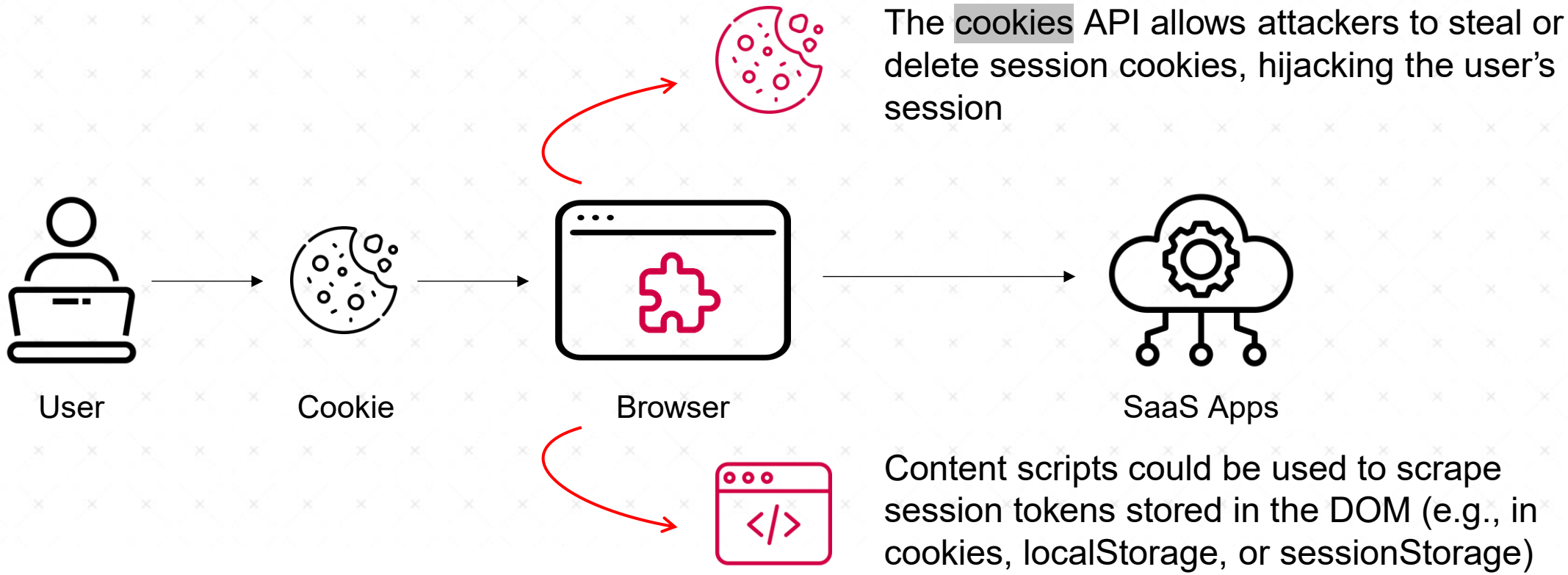
Adversaries steal session cookies to hijack an active user session, bypassing authentication mechanisms and gaining unauthorized access to web apps.



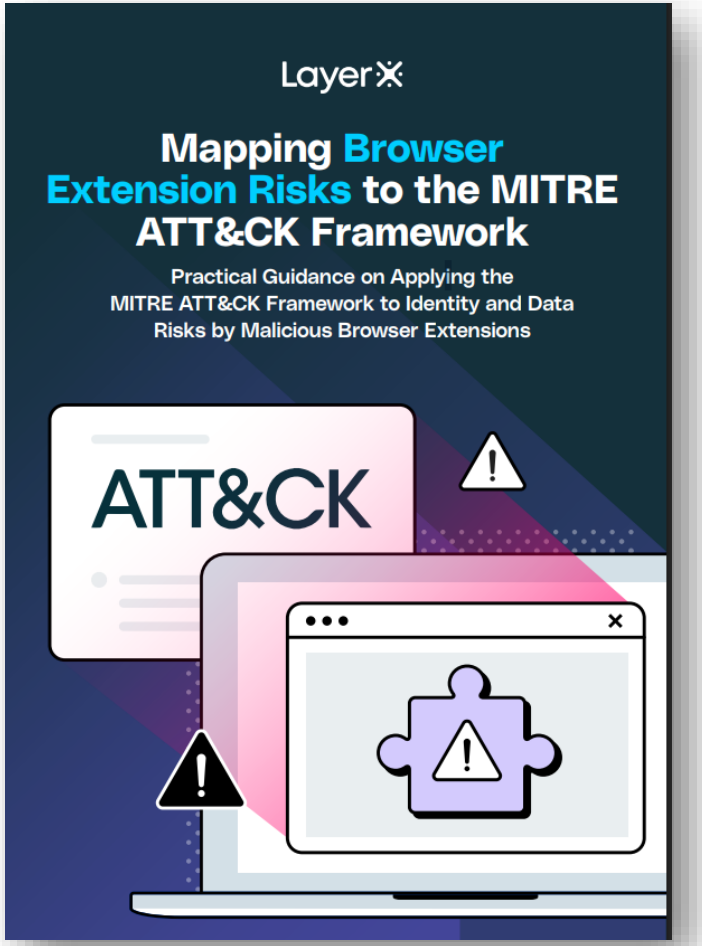
Sample TTP #2:

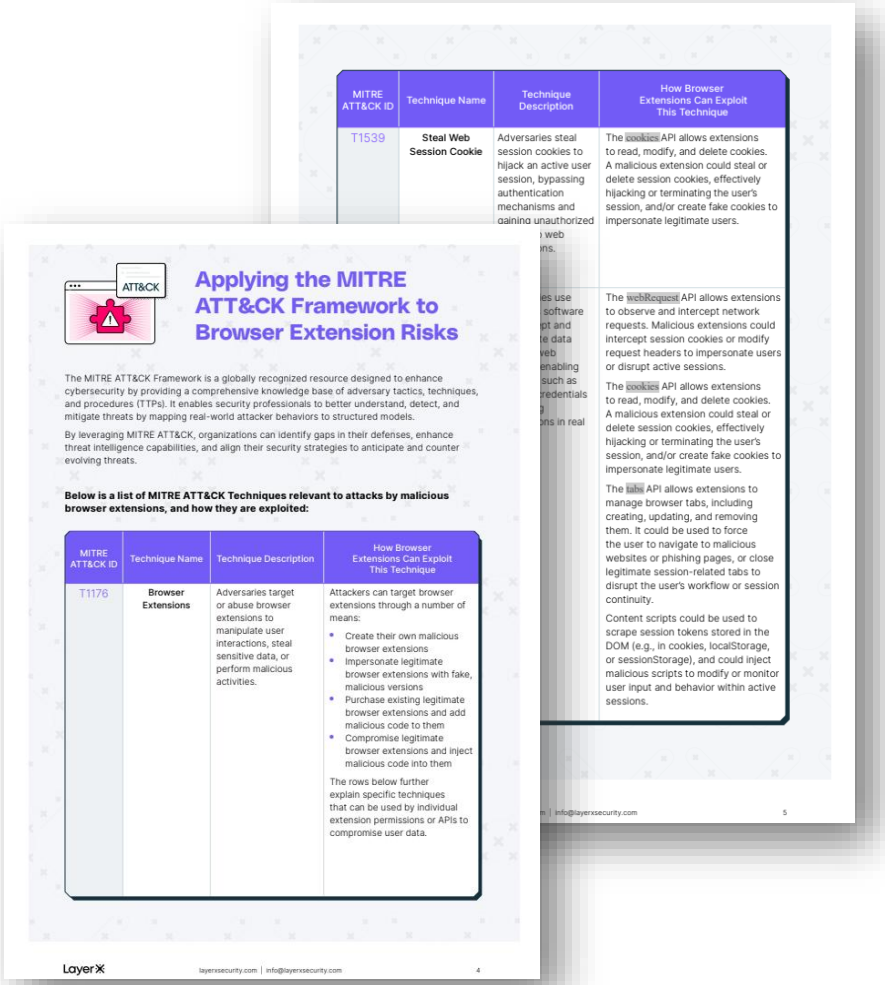
T1185 - Browser Session Hijacking

Adversaries use malicious software to intercept and manipulate data within a web browser, stealing credentials or altering transactions in real time.



Mapping Extension Threats to MITRE ATT&ACK Framework





DEFENSE:

Securing passwords against compromised browser extensions

Potential Security Strategies

Allowlist

- Prevent installation if ID not in the allowlist
- Manual/automated review
- Can still be hit by a compromised/weaponized extension

No Extensions At All

- Good luck fighting with your developers LOL

Blocklist

- Scan periodically and add IDs to blocklist
- Requires robust scanning routine for all approved browsers
- Great way to waste time and still be compromised

Risk based security….

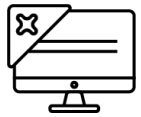
A CISO Framework for Extension Security

1

Audit

Full discovery of all extensions in the organization to understand who's using which extensions

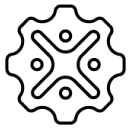
2



Classify

Categorize extensions and assess their level of risk base on their access, usage, and publisher reputation

3



Enforce

Apply risk-adaptive security rules to block the installation of risky extensions and disable already installed ones

Pitfalls to Extension Security:

Phase	Key Challenge	Why This is a Problem	What You Need
Discovery	Do you have all browsers covered?	Many solutions cover only Chrome / Edge, or other major browsers	Cover every browser, not just Chrome / Edge
Risk Classification	How do you know what's in the extension ID?	Extensions are polymorphic, they can change over time	Dynamic sandboxing to detect hidden behaviors and functionality updates
Enforcement	Automatic enforcement	Most extension security solutions offer manual allow/block lists based on extension ID	Risk-adaptive rules based on extension policy conditions (user identity, permissions, website, etc.)

ExtensionPedia:

Password Chameleon

Password Chameleon risk analysis

Risk Score
3.9/10
Low Risk

High
Permission Scope

Low
Reputation Risk

Block Extension

Organizational Risk

Extension Details

Extension ID:	10910	Developer:	https://passwordc...
Store:	Chrome	Developer email:	info@passwordch...
Category:	Workflow and planning	Version:	1.6.1
Last updated:	April 19, 2021	Privacy policy:	-
Number of users:	1,000	Rating:	3.5 (10 ratings)
Website:	-		

Permission Scope

Permission Name	Description	Risk Severity
Tabs	Extensions with the tabs permission can query the url, pendingUrl, title, and favIconUrl of any tab.	High
Clipboard Write	Extensions with the clipboardWrite permission can modify the system's clipboard content.	Medium

Summary

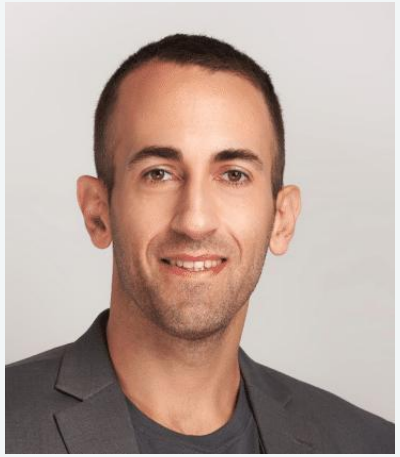
Browser extensions are **everywhere,** the threat surface is **everyone**

Browser extensions have **extensive access permissions** that can be abused for credential / password compromise

Human **identity security = browser security**

Various tools can help, but make sure to **balance cost vs. manual work**

Get In Touch!



https://www.linkedin.com/in/or-eshed/

or@layerxsecurity.com

Thank You!