Cybersecurity Coordinator Forum

April 2024

Todd Pauley, CISSP, CISM

Deputy CISO/Cybersecurity Coordinator

Texas Education Agency

todd.pauley@tea.texas.gov

Cybersecurity Coordinator Forum

The **TEA Cybersecurity** team hosts a **monthly** meeting for Texas Local Education Agency (LEA) **Cybersecurity Coordinators,** Education Service Center (ESC) **Cybersecurity personnel**, and other members of the community that support K12 Cybersecurity efforts. It provides content designed to assist LEAs and ESCs towards maturity in an information security program.

Cybersecurity Coordinator Forum

We are transitioning to Zoom from GoTo Webinar

Please re-register:

https://t.ly/Hmimy

Emails will be sent out to all current registered attendees with the registration link.

Please register with your LEA email account.

Agenda

- Cybersecurity Announcements
  - TxISAO (Texas Information Sharing & Analysis Organization)
  - State-Local Cybersecurity Grant Program (SLCGP) Update
  - Cybersecurity Advisory
  - Local Incident Reporting Update
  - Legislative Update
- Texas K12 Cybersecurity Initiative Update
- Browser Security Informational Session
  - Josh Olson – TEA's Cybersecurity Operations Team Lead

TxISAO

ACTION: Please sign up for mailing list at the link below.

https://dir.texas.gov/txisao

The Texas Information Sharing & Analysis Organization (TxISAO) is open to all organizations in Texas to include K-12.

State and Local Cybersecurity Grant Program (SLCGP)

CISA Cybersecurity Grant

Currently in the review process.

Reviews due by 6/22/2024.

CISA is seeking feedback on the SLCGP Program here:

https://answer.rand.org/StateandLocalCybersecurityGrantProgramSurvey

Palo Alto Networks PAN-OS (CVE-2024-3400)

This issue is applicable only to PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 firewalls configured with GlobalProtect gateway or GlobalProtect portal (or both). Device telemetry does not need to be enabled for PAN-OS firewalls to be exposed to attacks related to this vulnerability.

https://unit42.paloaltonetworks.com/cve-2024-3400/

Malware Next-Generation Analysis

The US Cybersecurity and Infrastructure Security Agency (CISA) has released a version of its Malware Next-Gen malware analysis system for public use. Until now, Malware Next-Gen was available only to federal agencies. Organizations and individuals may now submit “malware samples and other suspicious artifacts for analysis” after registering with a login.gov account.

https://www.cisa.gov/resources-tools/services/malware-next-generation-analysis

Cybersecurity Advisories

https://get.gov/

CISA has released a guidance document for help with transitioning you to the .gov domain.

(Available in the 'Handouts' section)

Is it required? **No**

Why switch?

- It's free
- Only available to governmental entities in the US (school districts included)
- Helps the public better recognize official sites and emails while avoiding phishing attempts.

Local Government Incident Reporting (SB 271)

This replaces the previous School District Incident Report, required by Section 11.175 of the Texas Education Code.

Updates

- The form now contains a new field to indicate if you are submitting an incident on behalf of another organization. If you answer yes, you will be required to input contact information for both the submitter and the affected organization. Upon submission of the form, both the submitter and the affected organization will receive an incident confirmation email. Please note that the affected organization will be required to submit the closure report once the incident is resolved.

- The form now contains a new field to indicate if you would like a consultation with DIR's Cybersecurity Incident Response Team (CIRT). If you answer yes, a member of the CIRT will contact the affected organization to discuss the incident and review available resources.

https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting/sb-271-security-incident

Legislative Update

HB 18 (SCOPE)

TEA released a TAA late last year that included ‘Standards for Electronic Devices and Software Applications’

https://tea.texas.gov/about-tea/news-and-multimedia/correspondence/taa-letters/standards-for-permissible-electronic-devices-and-software-applications

HB 18 Protection of minors on digital services and devices:

- Requires users to register with their age for a digital services and social media.
- Minors will need parental consent.
- Reduce marketing content to minors
- TEA shall adopt standards for permissible electronic devices and software used by a school district.
- When issuing a device, LEAs must “install an Internet filter that blocks and prohibits pornographic or obscene materials or applications, including from unsolicited pop-ups, installations, and downloads.”
- Establishes a joint committee of the legislature to study the effects of media on minors.

Texas Education Agency

Texas K12 Cybersecurity Initiative

April 2024

Texas K12 Cybersecurity Initiative

- **Fully funded services currently available for request :**
  - To start request please *register*: New customer form
  - **Managed Endpoint Detection and Response (EDR)**
    - Requirement: student enrollment 15,000 or less, licenses up to 20% enrollment, 30 license min.
    - Once registered, request service via Managed Security Service (MSS): MSS Portal Log In Process (texas.gov).
    - LEAs may choose between EDR vendors CrowdStrike or SentinelOne.
    - Standard option should be most common for LEAs.

K-12 Cybersecurity Initiative | Texas Education Agency

Texas K12 Cybersecurity Initiative

- **Fully funded services currently available for request :**
  - **School District Cybersecurity Assessment**
    - Requirement: First come, first served for any LEA.
    - Once registered, request service via MSS : TX K-12 Cybersecurity Assessment Quick Start Guide
    - LEAs may choose between Basic, Intermediate, or Advanced Cybersecurity Assessments.

Assessment Level	# Controls	# Questions
Basic	26	100
Intermediate	33	109
Advanced	42	123

- Output of the assessment is a formal report provided to the LEA with a security maturity designation level ranging from 0-5.

K-12 Cybersecurity Initiative | Texas Education Agency

Upcoming Funded Services

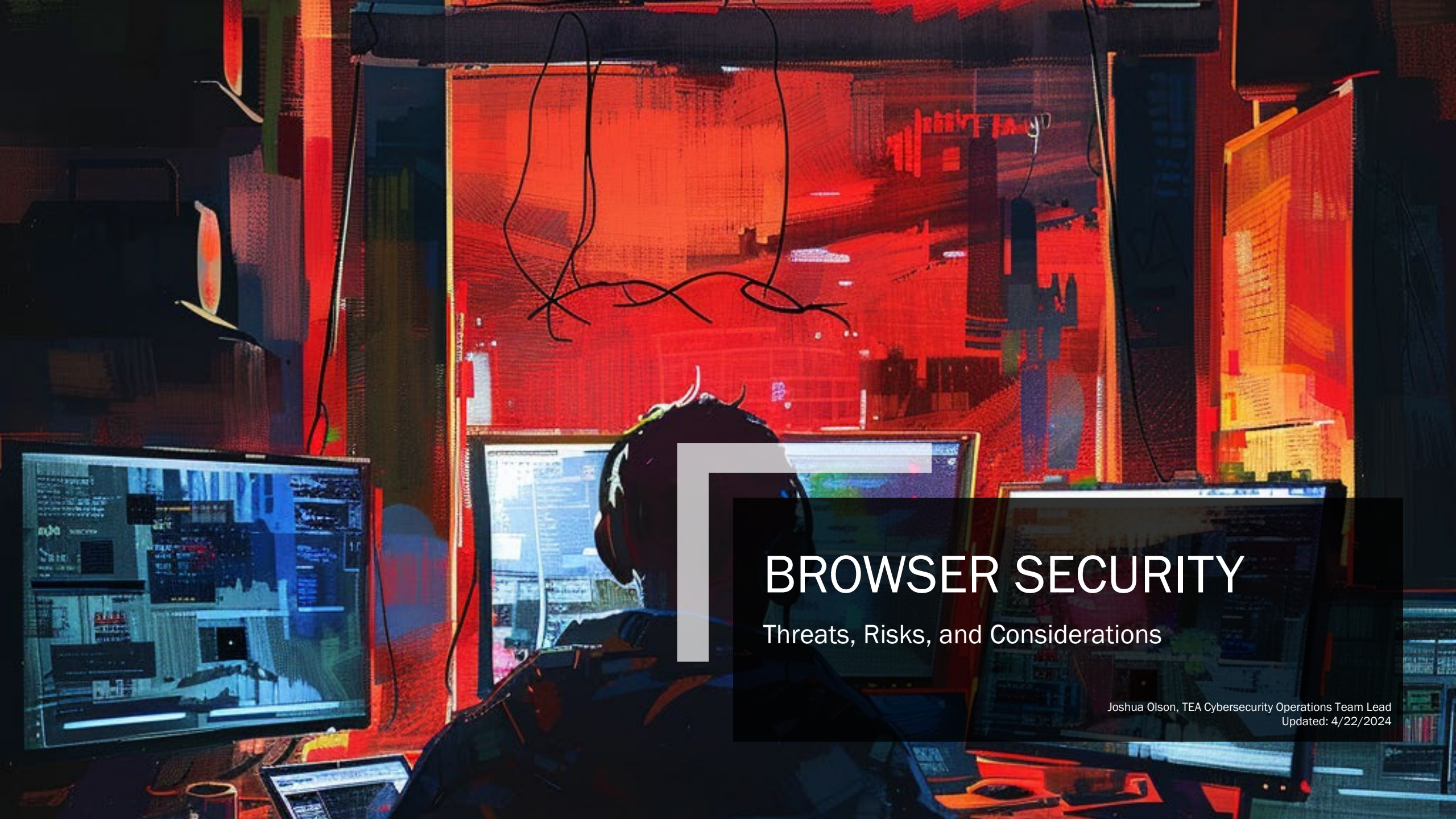
- Upcoming Services via your Education Service Center:
  - Technical assistance to implement the following critical controls
    - **EDR**
    - **Multifactor Authentication** for staff email
    - **Email security protocol** (SPF, DKIM, and DMARC)
    - **Restrict local admin access**
- Upcoming Services
  - Network Detection and Response (NDR)

K-12 Cybersecurity Initiative | Texas Education Agency

Texas Education Agency

Browser Security

Josh Olson, TEA



BROWSER SECURITY

Threats, Risks, and Considerations

Joshua Olson, TEA Cybersecurity Operations Team Lead
Updated: 4/22/2024

Agenda

INTRODUCTION

BROWSER SECURITY CONSIDERATIONS

PROPOSE MITIGATIONS

QUESTIONS

Introduction: Speaker

Josh Olson

- TEA's Cybersecurity Operations Team Lead
- Master of Science in Cybersecurity and Information Assurance
- CISSP, CHFI, Pentest+, CySA+ certifications
- A few vulnerability credits:
  - CVE-2020-28096 (Foscam)
  - CVE-2022-34567 (Imaging Software)
  - Synology (Bug bounty)
- Contact

josh.olson@tea.texas.gov

/joshua-olson-cissp

Introduction: Browsers

Web browsers present an attractive attack surface.
The vary nature of web browsers require…

Interaction with remote, untrusted systems

Browsers exchange data with remote and unknown systems

The ability to execute unknown code

JavaScript, web assembly, extensions, etc.

Interaction with system resources

Camera, microphone, speaker, file system, etc.

Interaction with authentication and identity

Form data, cookies and sessions storage, etc.

Security Considerations: High Level

Stored Passwords

Browsers, by default, allow users to store credentials. Threat actors are known to target these vaults.

Patch management

Though modern browsers allow for automatic updates, legacy versions still exist, and enforcement of automated patching varies.

Extensions

Unmanaged user access to extensions increases risk malicious extensions will be loaded

Enterprise Management

Lack of enterprise enforced standards increase risk controls will not be uniformly applied.

Security Considerations: Stored Passwords

T1555.003

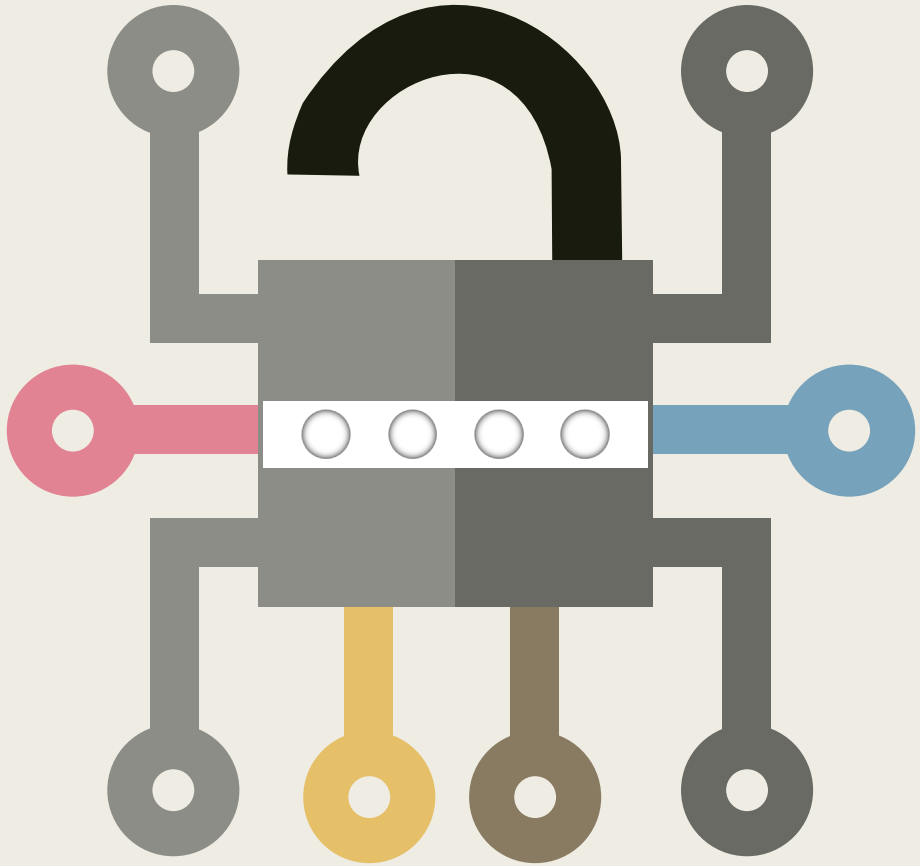
Adversaries may acquire credentials from web browsers by reading files specific to the target browser.*

71

The number of threat actors MITRE ATT&CK lists that are known to use T1555.003*

Insistent

Most of the common browsers, by default are insistent on wanting to store credentials



Autofill

Opens risk malicious extensions or sites could steal credentials

Visibility

Lack of enterprise tooling to monitor access and retrieval of stored browser credentials

Syncing

Do you enable browser syncing? Do you allow users to sign in to home devices? Where are those credentials going?

* Source: MITRE ATT&CK

Security Considerations: Stored Passwords

Wait, what?... Syncing? Yes, Browser Syncing....

Home / Tech / Security

Google Chrome sync feature can be abused for C&C and data exfiltration

A security researcher has found a malicious Chrome extension in the wild abusing the Chrome Sync process.

Written by **Catalin Cimpanu,** Contributor

Feb. 5, 2021 at 7:38 a.m. PT

Source: Google Chrome sync feature can be abused for C&C and data exfiltration | ZDNET

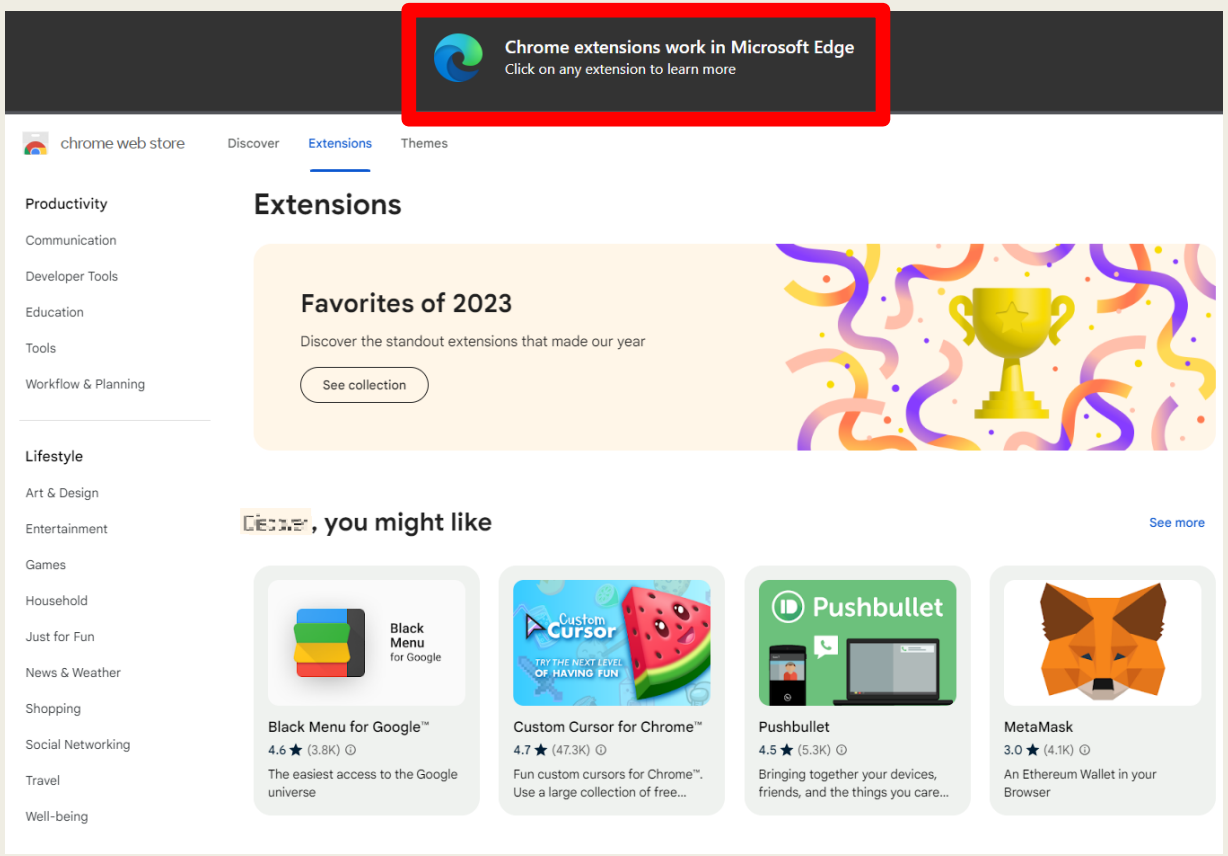
Security Considerations: Stored Passwords

- By leveraging a malicious extension, a threat actor could set up various text-based fields to store data.
- To set, read or delete these keys, all the attacker must do is log in with the same account to Google, in another Chrome browser (and this can be a throwaway account), and they can communicate with the Chrome browser in the victim's network by abusing Google's infrastructure…
- The data can be anything… it could be data the malicious extension gathered about the infected browser (such as usernames, passwords, cryptographic keys, or more) or commands the attacker wanted the extension to execute on the infected workstation. Remember sync is bi-directional.
- Since the stolen content or subsequent commands are sent via Chrome's infrastructure, none of these operations would be inspected or blocked in most corporate networks, where the Chrome browser is usually allowed to operate and transmit data unhindered.
  - Looking at network logs all you would see is traffic going out to Google’s infrastructure (e.g., clients4.google.com), which really cannot be blocked as Chrome uses this domain for a lot of things.
- Speaking of Extensions….

Source: Google Chrome sync feature can be abused for C&C and data exfiltration | ZDNET

Security Considerations: Extensions

- What are browser extensions?
  - Browser extensions are small software programs that add functionality to web browsers, enhancing the user experience by customizing and extending their capabilities, often through integration with third-party services or by modifying web content and behavior.



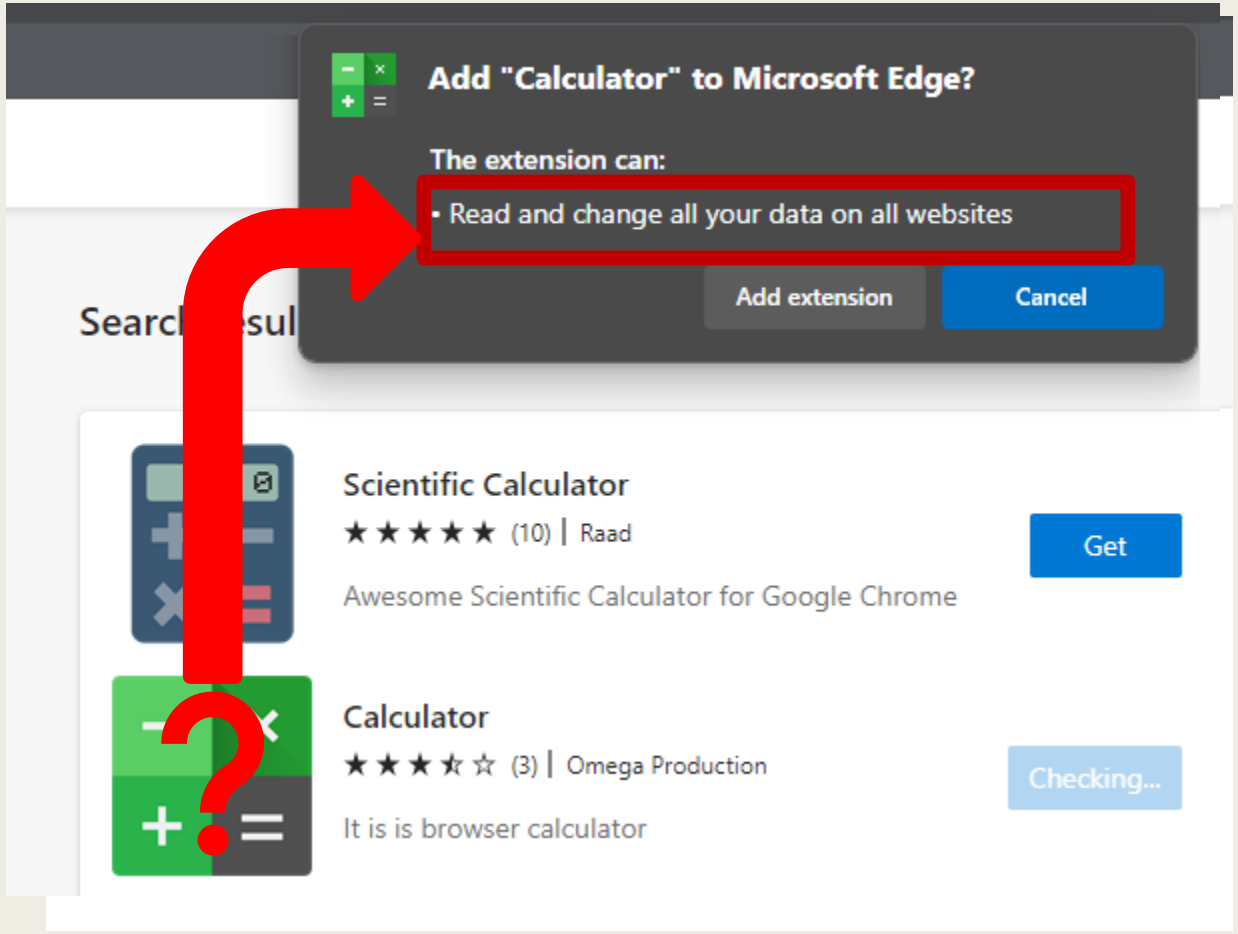
Chrome Extension Store

Security Considerations: Extensions

- Some headlines regarding extensions shenanigans
  - 3/24/2023: Malicious ChatGPT Extensions Add to Google Chrome Woes
    - Account stealer
    - darkreading.com
  - 6/2/2023: Malicious Chrome extensions with 75M installs removed from Web Store
    - bleepingcomputer.com
  - 12/26/2023: Three malicious VPN extensions on the Chrome Web Store infected 1.5 million devices before being removed by Google
    - TechSpot

Security Considerations: Extensions

- Extensions with permissions to read and change website data pose significant risks, including:
  - Potential for unauthorized access to sensitive information entered on websites, such as login credentials or financial data.
  - Introducing security vulnerabilities by modifying website content in unintended ways, potentially leading to phishing attacks or injection of malicious code.
  - Can compromise user privacy by monitoring and manipulating browsing behavior without consent.



Security Considerations: Extensions

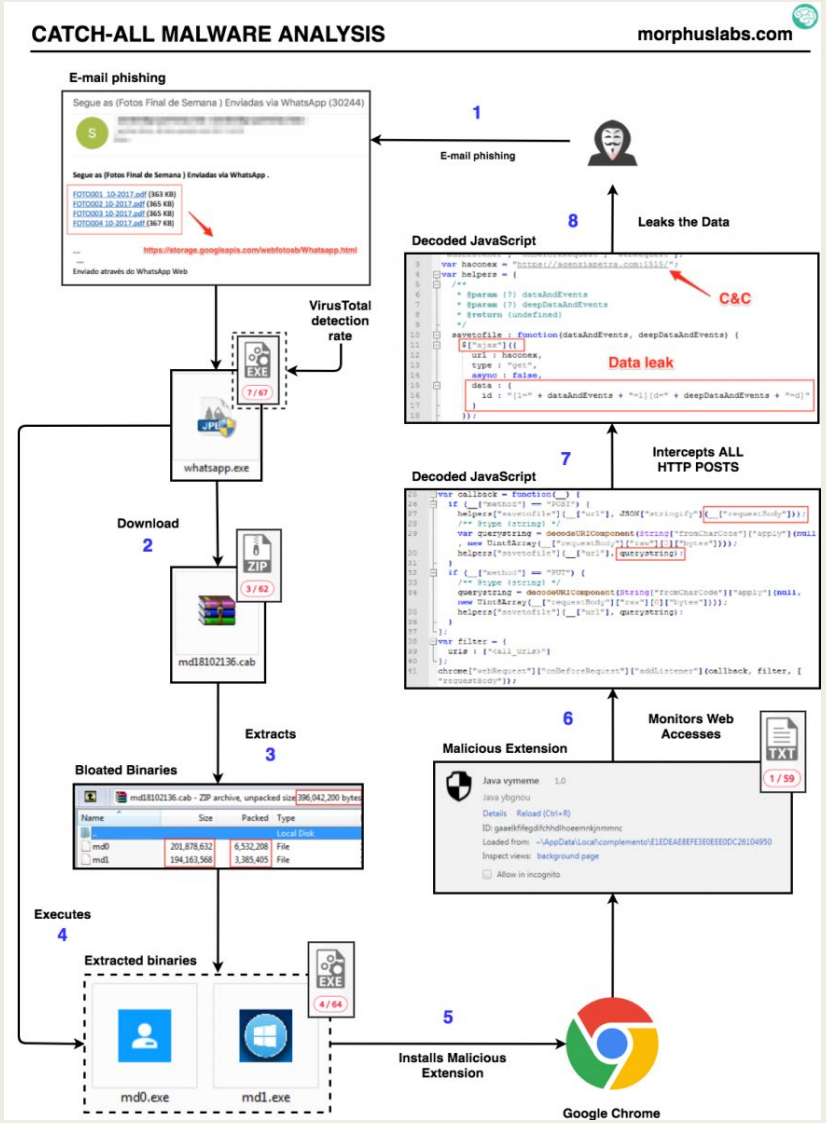
- Here are just some of the permissions Extensions can have:

Permission Name	Description
2-factor devices	Allows app or extension to communicate with devices with 2-Factor Authentication that support U2F.
Audio capture	Allows app or extension to capture audio directly from the microphone.
Clipboard read	Allows app or extension to **read the contents of the clipboard at any time.**
Desktop capture	Allows app or extension to capture screen, window, or tab content.
File system	Allows app or extension to create, read, navigate, and write to the user's local file system at a user-selected location.
Identity	Allows app or extension to get OAuth 2.0 access tokens.
Web requests	Allows app or extension to observe and analyze web traffic. **It also intercepts or *modifies* in-progress requests.**

Source: Chrome app and extension permissions - Chrome Enterprise and Education Help (google.com)

Security Considerations: Extensions

- Malicious extensions do not have to be installed via the store. They can be dropped in by gray market browsers (Wave), or …
  - *They can be dropped by other malicious files as this malware analysis details*
    - Phishing email (1) > Download (2) > Execution (4) > Extensions installation (5)
  - *Once installed malicious extension:*
    - Monitors web access
    - Intercepts all POST requests and
    - Sends data back to threat actors



Source: "Catch-All" Google Chrome Malicious Extension Steals All Posted Data - SANS Internet Storm Center

Security Considerations: Extensions

- The extensions is installed with the following command:
  - *C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-extensions-file-access-check --always-authorize-plugins --disable-improved-download-protection --load-extension = "C:\Users\<USER>\AppData\Local\complemento \E1EDEAE8EFE3E0EEE0DC2610495*

    - **--disable-extensions-file-access-check**: disable checking for user opt-in for extensions that want to inject script into file URLs (ie, always allow it). This is used during automated testing.
    - **--always-authorize-plugins**: prevents Chrome from requiring authorization to run certain widely installed but less commonly used plug-ins.
    - **--disable-improved-download-protection**: disables improved SafeBrowsing download protection (do not verify files with built-in protection)

- There are many switches, this site has a good catalog of them which links to the Chromium source code: List of Chromium Command Line Switches « Peter Beverloo

Source: "Catch-All" Google Chrome Malicious Extension Steals All Posted Data - SANS Internet Storm Center

Security Considerations: Patch Management

- 7/5/22: [Browser vulnerabilities are] not just serious but growing: In the first quarter of 2022 alone, Chrome fixed 113 vulnerabilities, 13% more than in the same period in 2021, while Firefox fixed 88 vulnerabilities, a 12% jump from the first quarter of 2021. These increases make browsers a top target for hackers.
  - Why Browser Vulnerabilities Are a Serious Threat — and How to Minimize Your Risk (darkreading.com)
- 12/22/23: [A] vulnerability in Chrome that has been under active exploitation in the wild, ***marking the eighth zero-day vulnerability*** identified for the browser in 2023. … "The exploitation of Chrome is tied to its ubiquity — even Microsoft Edge uses Chromium," he says. "So, exploiting Chrome could also potentially target Edge users and allow bad actors a wider reach.“
  - Google Releases Eighth Zero-Day Patch of 2023 for Chrome (darkreading.com)
- 4/3/24: “In total, Google patched four Chrome zero-days this year…”
  - Google fixes one more Chrome zero-day exploited at Pwn2Own (bleepingcomputer.com)

Security Considerations: Patch Management

- Modern web browsers support automatic updates
  - Does your enterprise enforce them?
  - Keep in mind older versions may not support automatic updates and may require manual upgrade.

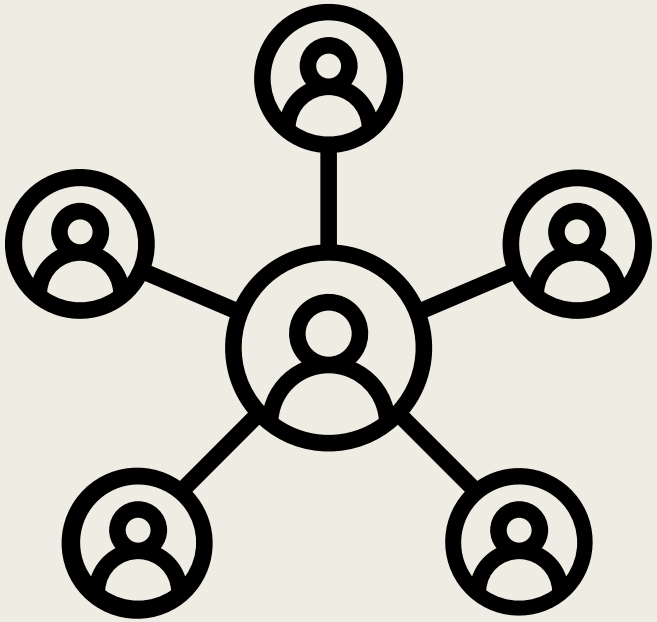
- Automatic updates does not mean “right away.”
  - Does your enterprise allow users to invoke a manual update?
  - Do your users know how to check for browser updates?

Security Considerations: Enterprise Management

- Do you centrally manage browser configurations and settings?
  - Example: do you have Intune/GPO rules which prevent password manager use? Automatic updates? Limit extensions?
- Do you allow users to install “other” browsers?
  - Brave, Opera, DuckDuckGo, etc.
  - If so, how are you managing them to ensure these “other” browsers conform to your security baseline?

Security Considerations: Enterprise Management

- Intune can manage Chrome and Edge natively.
  - Manage Chrome browser with Intune Settings Catalog (Windows) - Chrome Enterprise and Education Help (google.com)
  - Configure Microsoft Edge policy settings for Windows using Microsoft Intune | Microsoft Learn
- Firefox requires adding an ADMX package to Intune
  - Managing Firefox with Microsoft Endpoint Manager (Intune) | Firefox for Enterprise Help (mozilla.org)



Purposed Mitigators

Approved Browsers

Establish and enforce a list of approved browsers

Disable Password Managers

Consider disabling browser-based password managers

Manage Browsers

Ensure approved browsers are managed and security controls are enforced

Monitor

Monitor for endpoints executing commands which could weaken browser security (command line switches, others?).

Auto Update

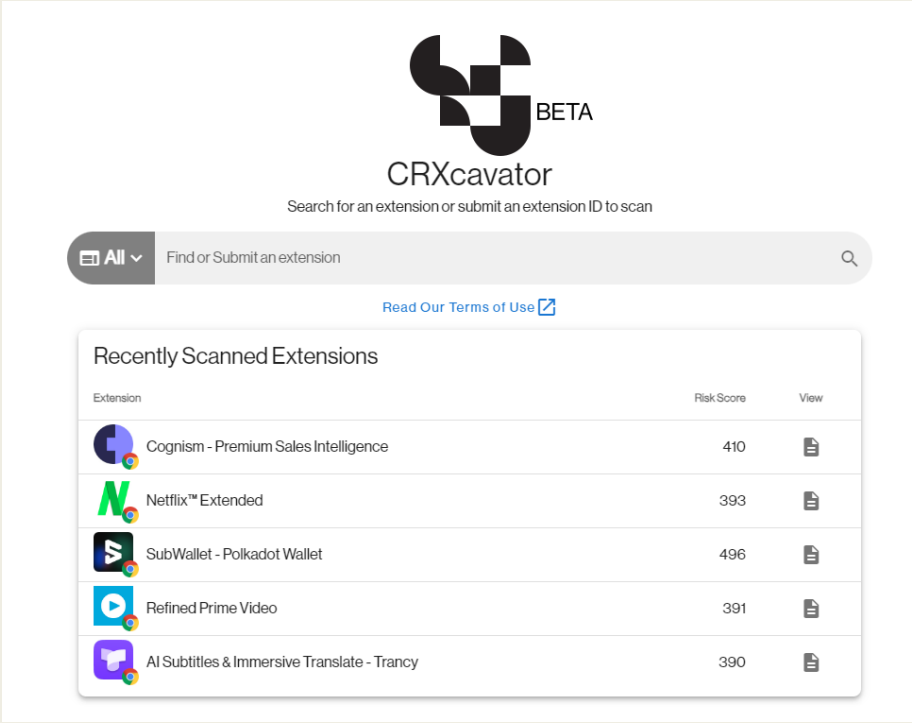
Ensure browsers are configured to auto update and users cannot opt out. Allow users to manually update as well.

Extensions

If allowed, consider denying extensions by default and allowing extensions by exceptions.

Security Considerations: Purposed Mitigators (cont.)

- Validate and research extensions
- https://crxcavator.io
  - It's like Virus Total for extensions!
- First find the extension ID.



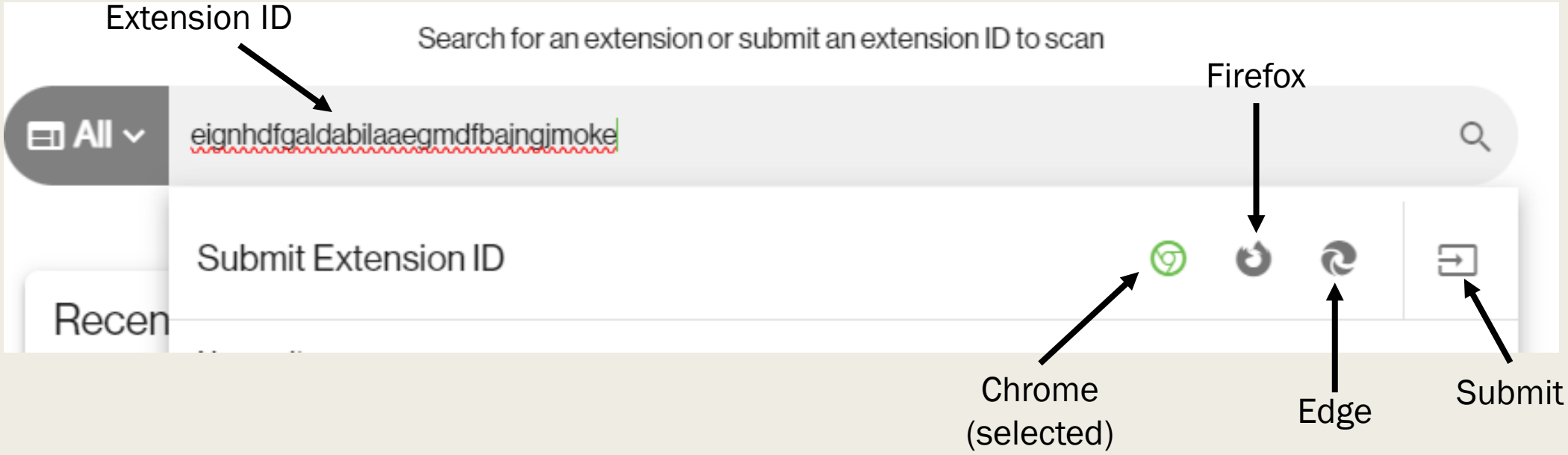
Edge:
https://microsoftedge.microsoft.com/addons/detail/dark-reader/**ifoakfbpdcdoeenechcleahebpibofpc**

Chrome:
https://chromewebstore.google.com/detail/black-menu-for-google/**eignhdfgaldabilaaegmdfbajngjmoke**

Firefox:
https://addons.mozilla.org/en-US/firefox/addon/**black-menu-google**

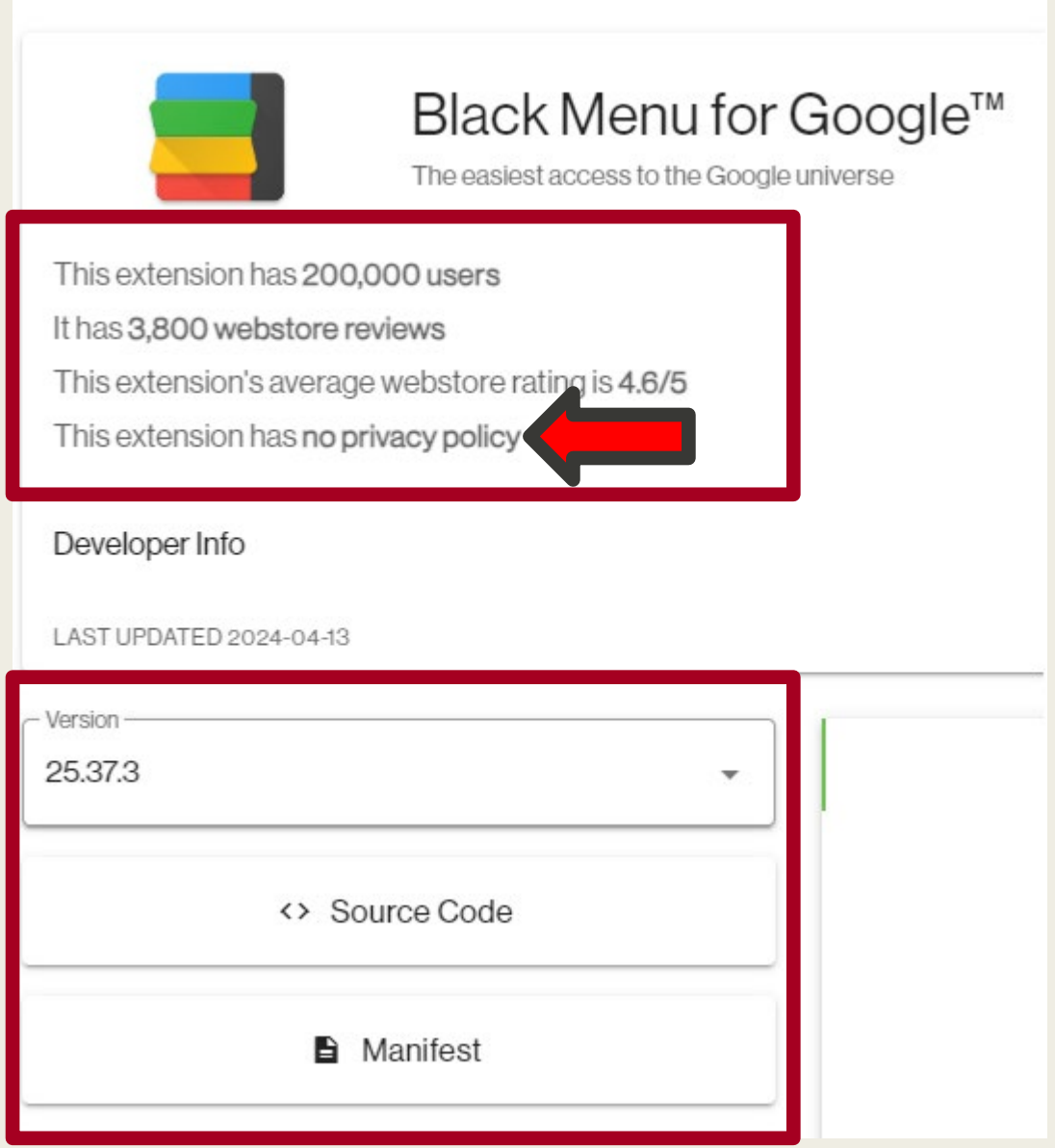
Security Considerations: Purposed Mitigators (cont.)

- Once you have the extension ID, enter it in the search box, and select the browser for the ID.



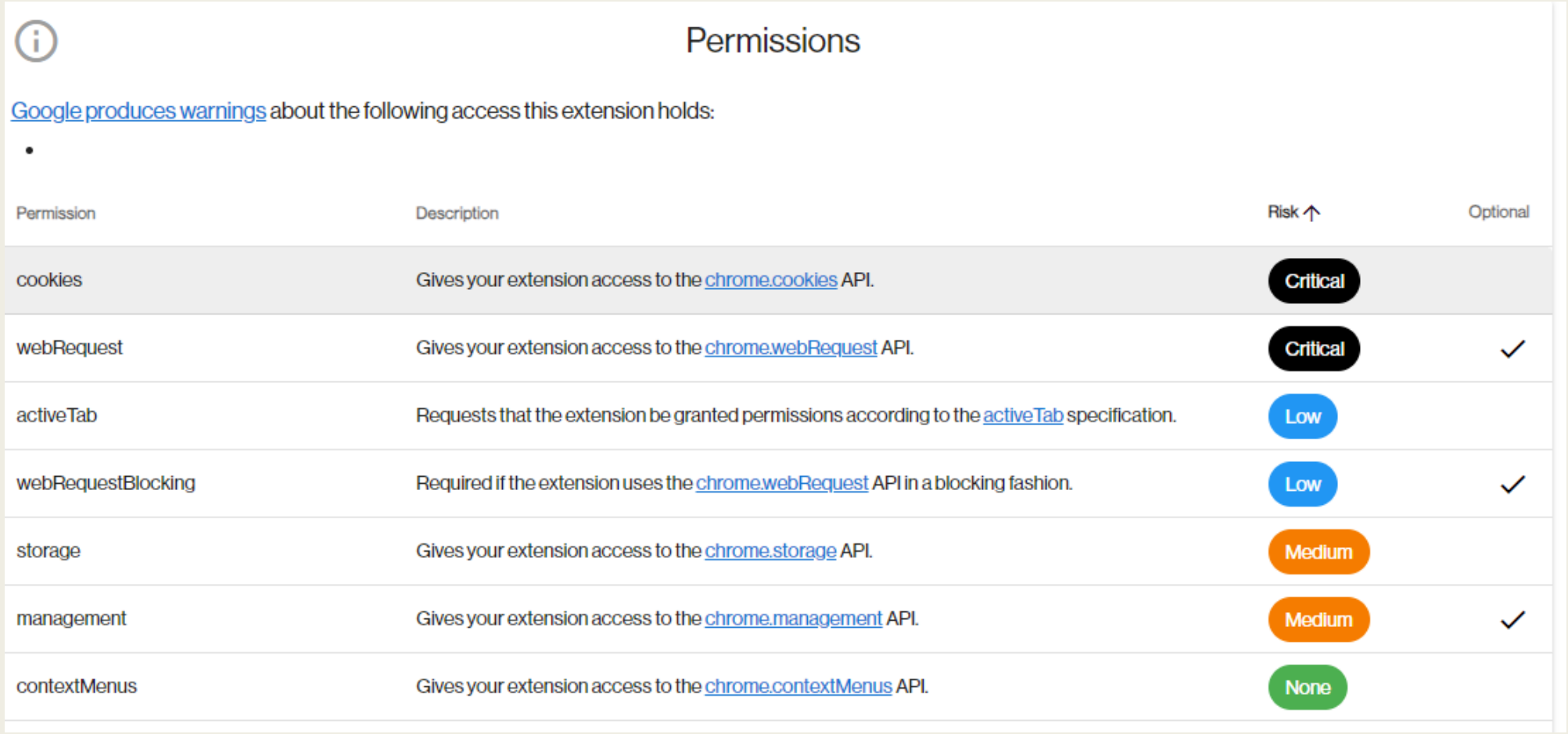
Security Considerations: Purposed Mitigators (cont.)

- Once the extensions is found/loaded, you will be able to see and access a lot of details about this extension.



Security Considerations: Purposed Mitigators (cont.)

- ...but wait, there's more. Get an overview of permissions



Permissions

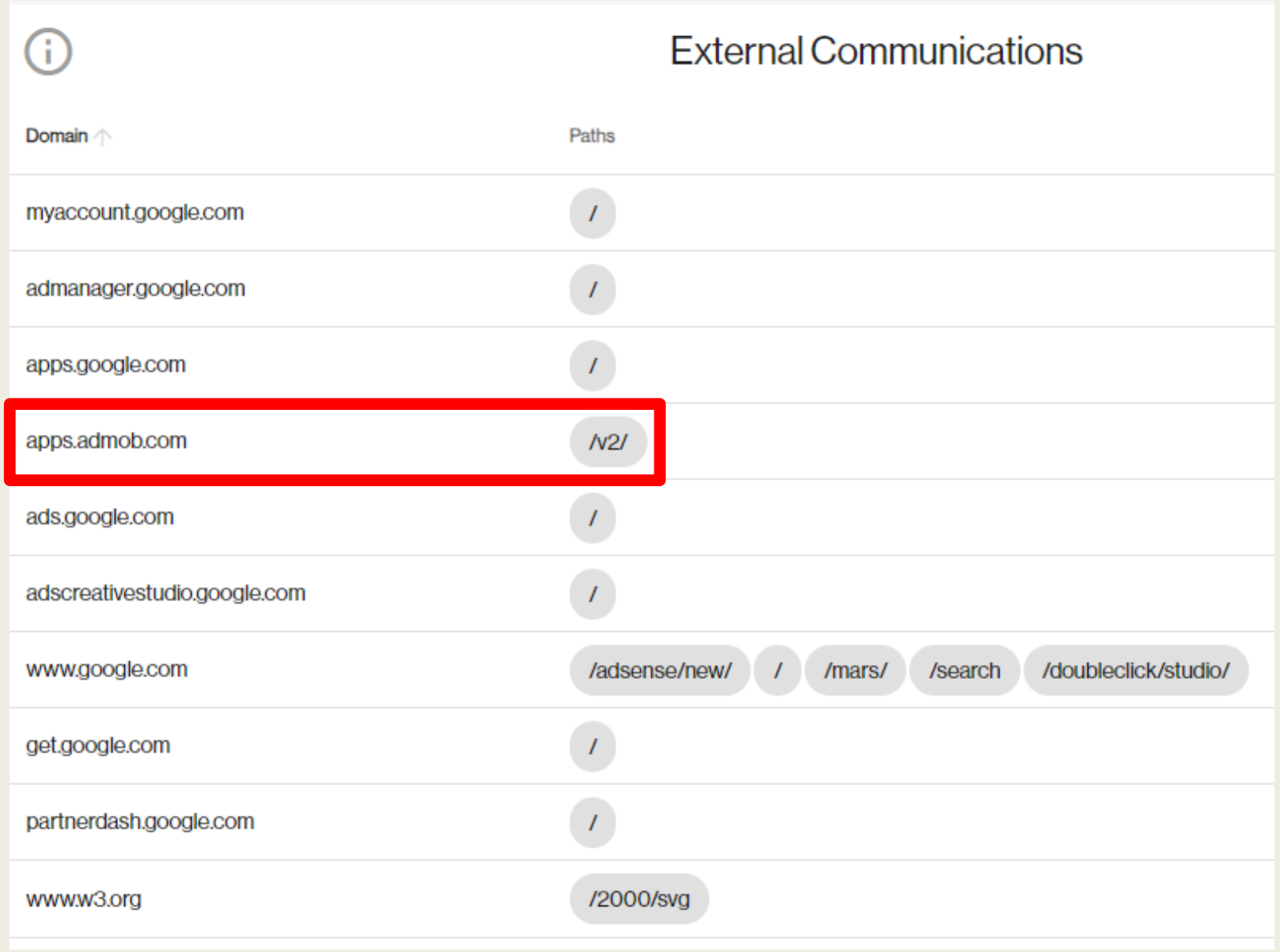
Google produces warnings about the following access this extension holds:

-

Permission	Description	Risk ↑	Optional
cookies	Gives your extension access to the chrome.cookies API.	Critical	
webRequest	Gives your extension access to the chrome.webRequest API.	Critical	✓
activeTab	Requests that the extension be granted permissions according to the activeTab specification.	Low	
webRequestBlocking	Required if the extension uses the chrome.webRequest API in a blocking fashion.	Low	✓
storage	Gives your extension access to the chrome.storage API.	Medium	
management	Gives your extension access to the chrome.management API.	Medium	✓
contextMenus	Gives your extension access to the chrome.contextMenus API.	None	

Security Considerations: Purposed Mitigators (cont.)

- ...See what the app communicates with...
- Perhaps some potential here to add to domain block lists ????



Security Considerations: Purposed Mitigators (cont.)

- Consider prohibiting users from clearing history.
  - *Not cache, cookies, sessions, stored data, users should still be allowed to clear those things, but merely disabling the ability to clear history.*
- Consider disabling web development tools for those users who have no business need to use.
- Regardless of what browsers your enterprise approves, the security team needs to understands all the various features and how they can impact security. Then tune security baselines accordingly.
- Do not think of browser security controls/mitigators as “the end,” but rather as another layer of your defense in depth strategy.

Questions?

josh.olson@tea.texas.gov

/joshua-olson-cissp

Thank you!

Questions?

Email :

cybersecurity@tea.texas.gov