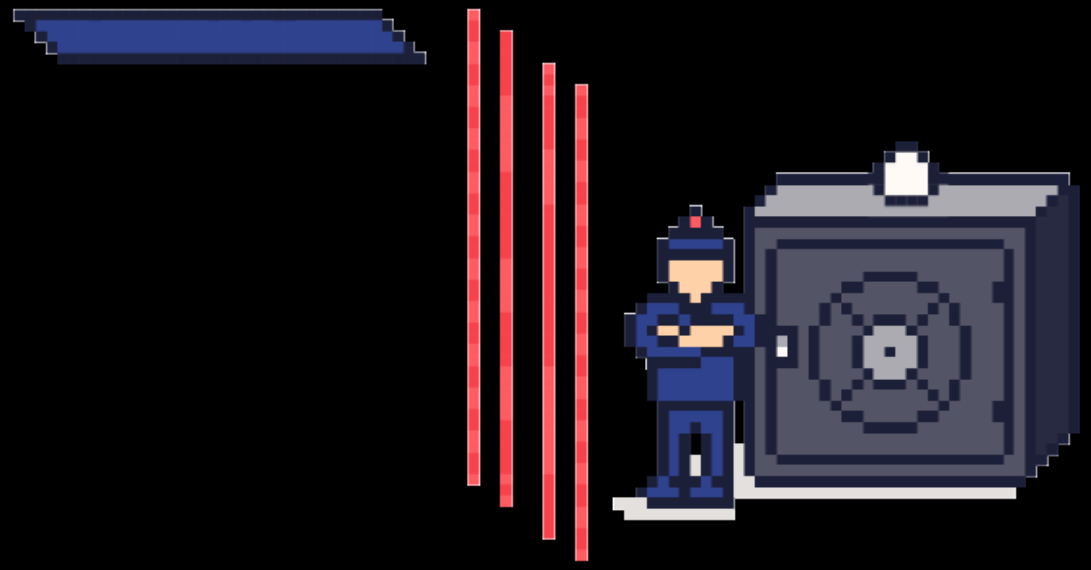
# ВРЕДОНОСНЫЕ РАСШИРЕНИЯ

## КАК ВАШ БРАУЗЕР РАБОТАЕТ НА АТАКУЮЩЕГО

Артемий Цецерский

# WHOAMI

- Работаю в **Angara Security**
- **5+** лет практической кибербезопасности
- Security Research -> Adversary Simulation -> Pentest -> RedTeam
- CVEs, BDUs
- OSCP, OSEP, OSWP



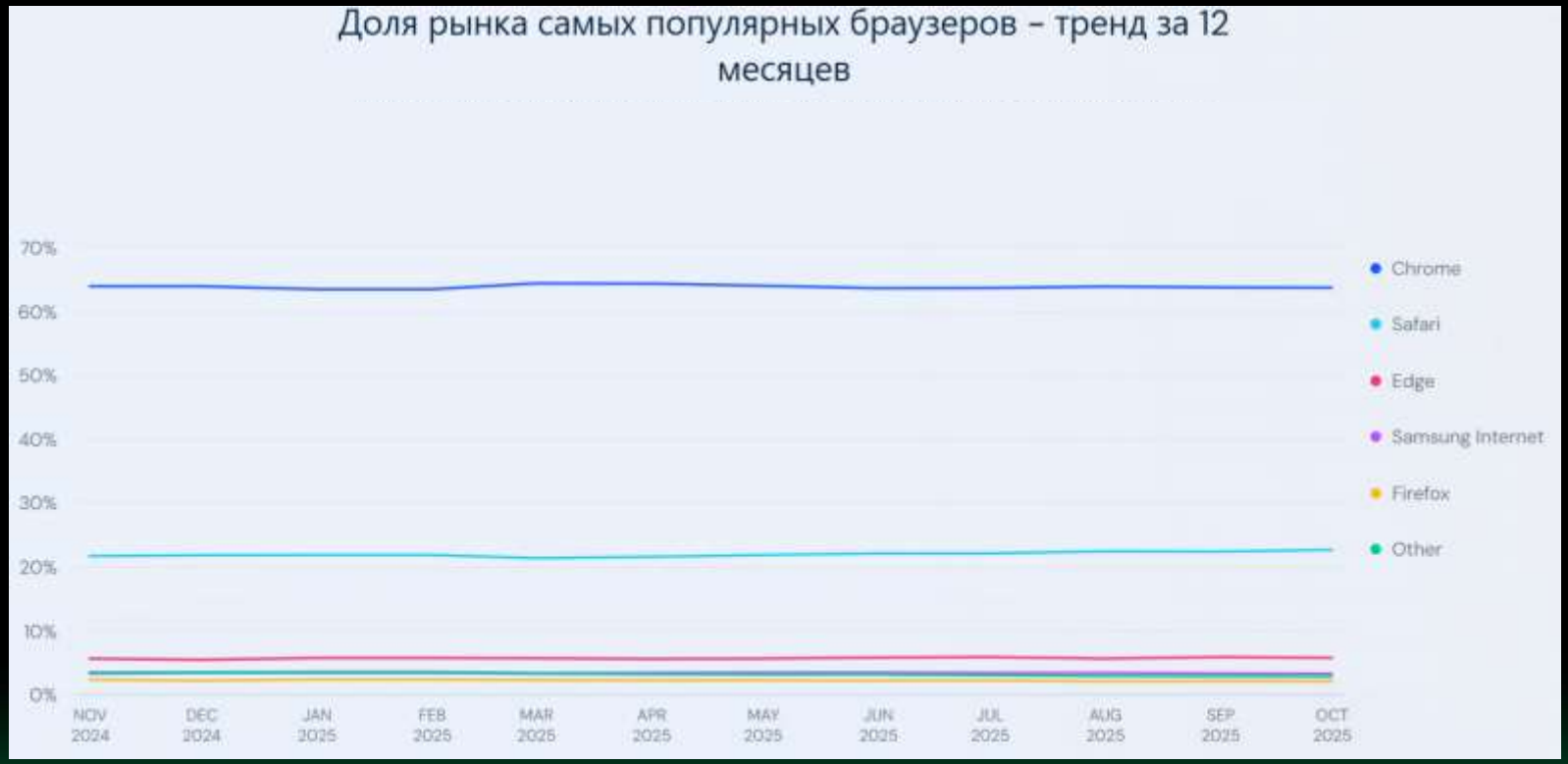
# Agenda

- Почему мне стоит дальше слушать этот доклад?
- Анатомия и устройство Chrome Extensions
- Доставка Chrome Extensions жертве
- Пост-эксплуатация с помощью Extensions-Fu
- Как защищаться и мониторить?

# Почему эта тема интересна и актуальна?

# Google Chrome – самый популярный браузер

Браузер – главное окно в цифровой мир, современный рабочий стол
Согласно аналитике* доля Google Chrome – **66 %**




**90%**

Всех пользовательских действий в интернете – через **браузер**

** https://www.similarweb.com/ru/browsers/*

# Chrome == Chromium

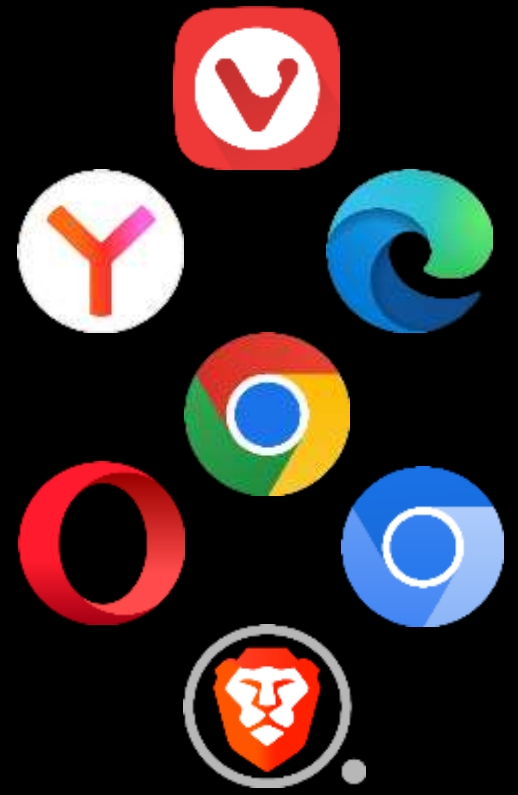
**Chrome** расширения работают в других **Chromium-**браузерах (**80%** рынка браузеров на базе этого движка)

support.microsoft.com/ru-ru/microsoft-edge/добавление-отключение-и-удаление-расширений-в-microsoft-e...

## Добавление расширения в Microsoft Edge из интернет-магазина Chrome

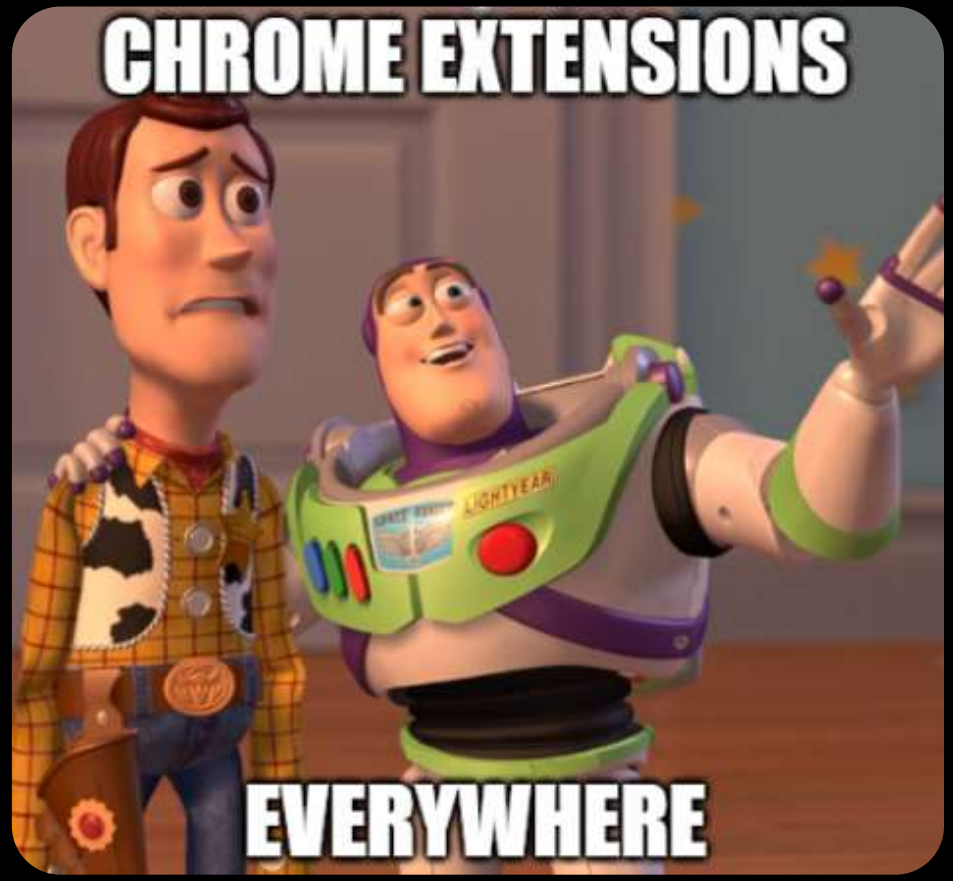
Расширения, предназначенные для Google Chrome, также можно использовать в Microsoft Edge.

1. В Microsoft Edge перейдите в интернет-магазин Chrome.
2. Выберите **Разрешить расширения из других магазинов** в заголовке в верхней части страницы, а затем выберите **Разрешить**, чтобы подтвердить.
3. Выберите расширение, которое требуется добавить, и нажмите **Добавить в Chrome**.
4. При отображении запроса со списком разрешений, необходимых расширению, внимательно изучите их и, чтобы продолжить, нажмите кнопку **Добавить расширение**.
5. Появится последний запрос, подтверждающий добавление расширения.



# Расширения – везде и всюду

- **190 000+** расширений в Chrome Web Store
- Из редкости в норму
- Активно в **корпоративных средах** (Парольные менеджеры, конференц-связь, Dev-утилиты, Productivity-утилиты)
- Многие имеют выше **10 млн.** установок
- Всё больше прав и доступов



# Интерес для атакующих

## Chrome API

Обширная документация управления браузером

## Cross-platform

Расширение устанавливается на любую ОС (Windows, macOS, UNIX)

## JavaScript

Просто и мощно для написания вредоносного ПО

## chrome.exe

Вредоносный трафик легко прячется в легитимном процессе

## Persistence

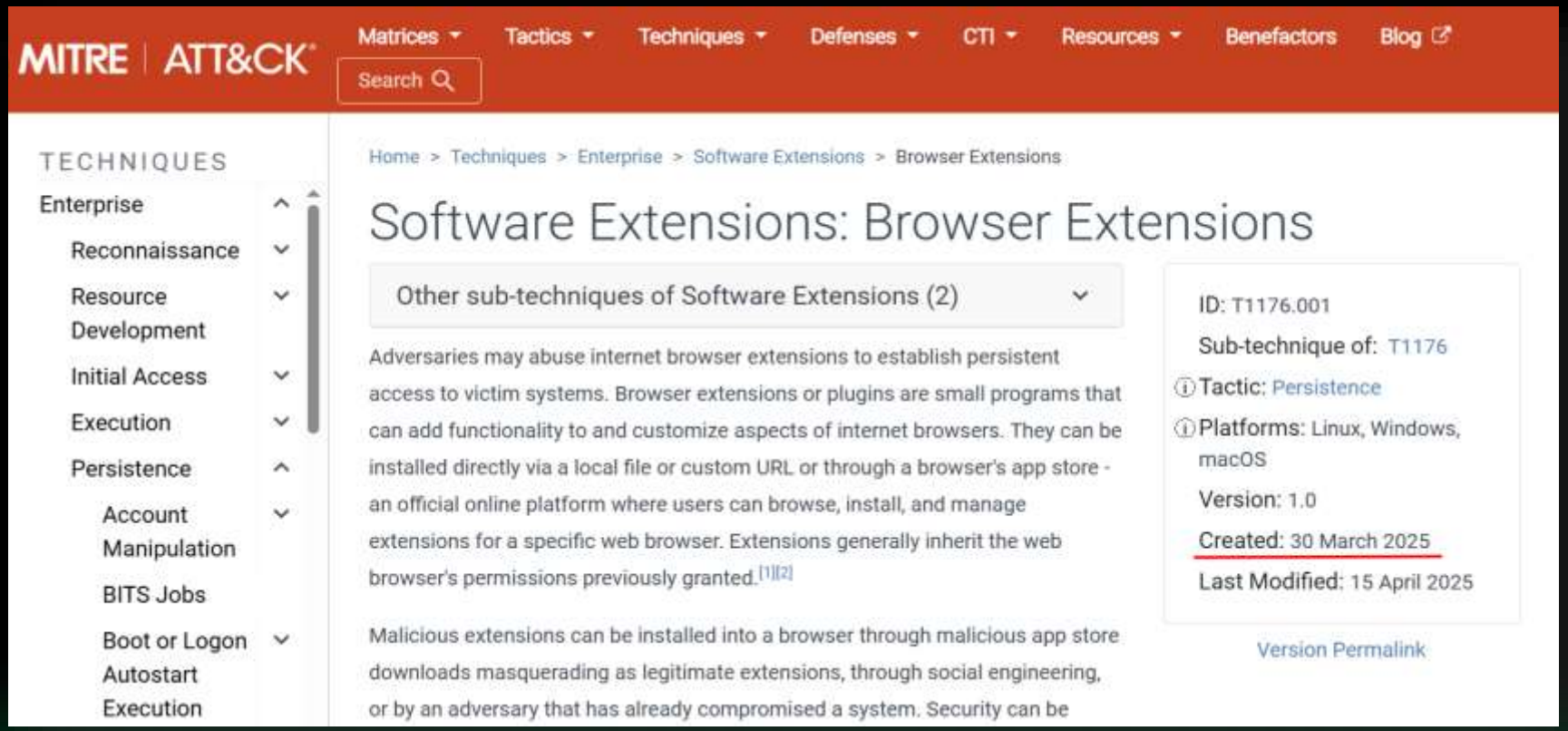
Установленное расширение живёт после перезагрузки ПК

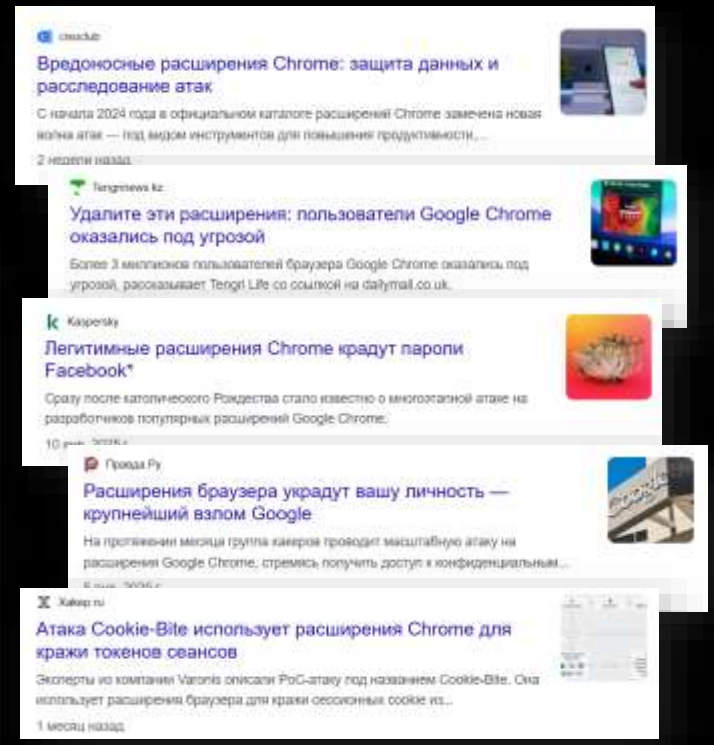
## AV/EDR

Слабо детектируют вредоносные расширения

# Киберинциденты

- Стабильный рост атак, новостные заголовки
- Техники все более опасные и изощрённые
- MITRE ATT&CK – Browser Extensions Technique

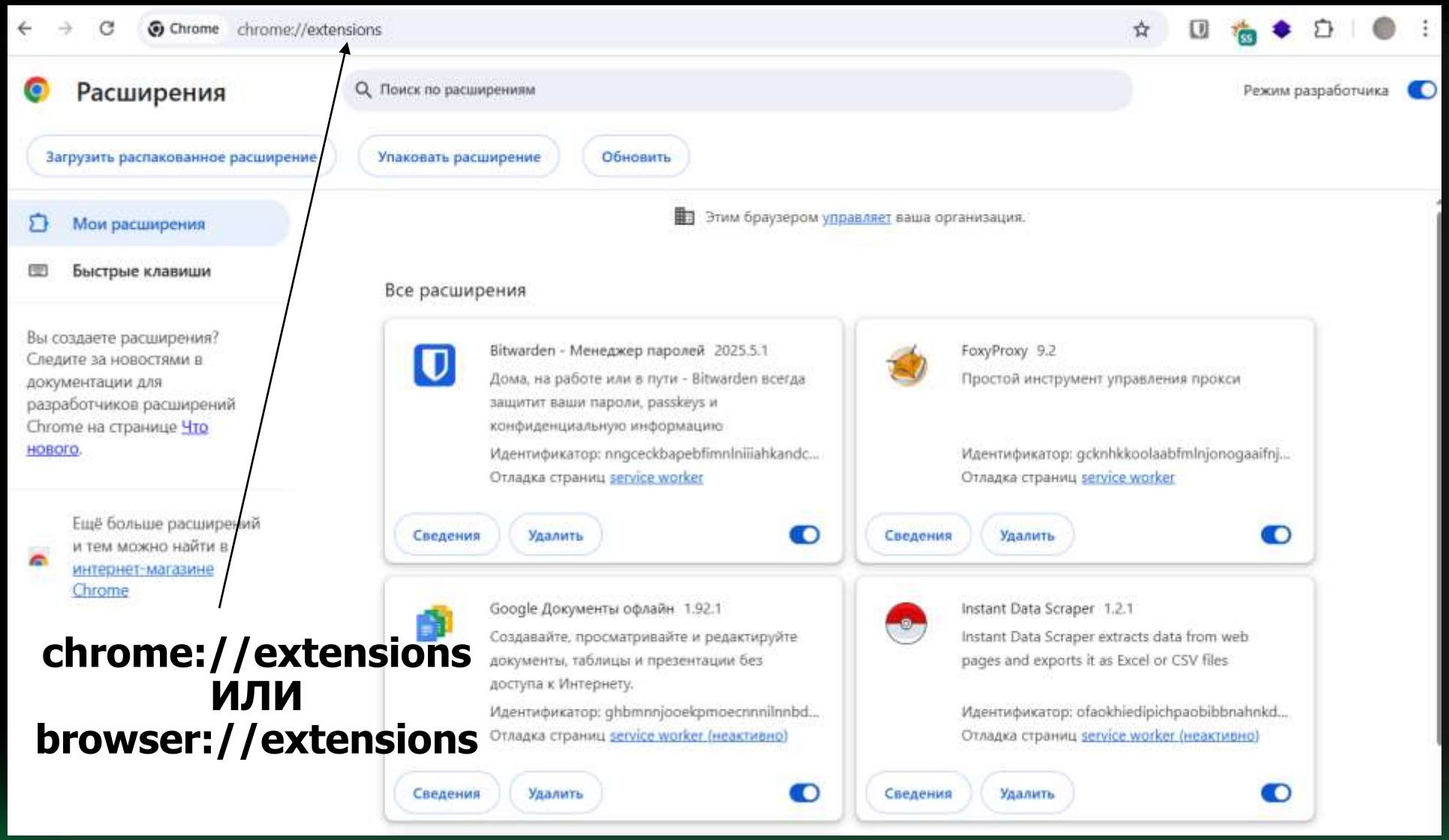


# АНАТОМИЯ CHROME EXTENSION

Как устроены расширения под капотом?

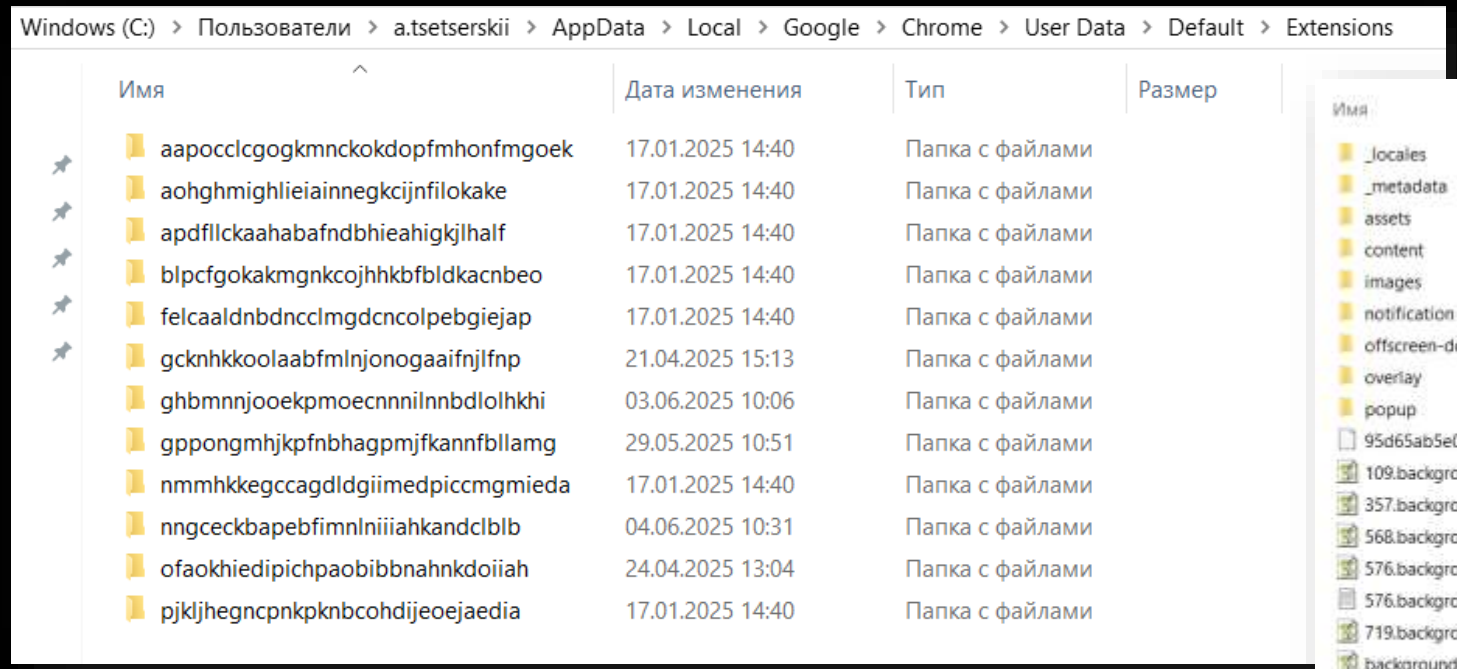
# Где эти ваши расширения в браузере?!




**chrome://extensions**
**ИЛИ**
**browser://extensions**

# Расширение на файловой системе

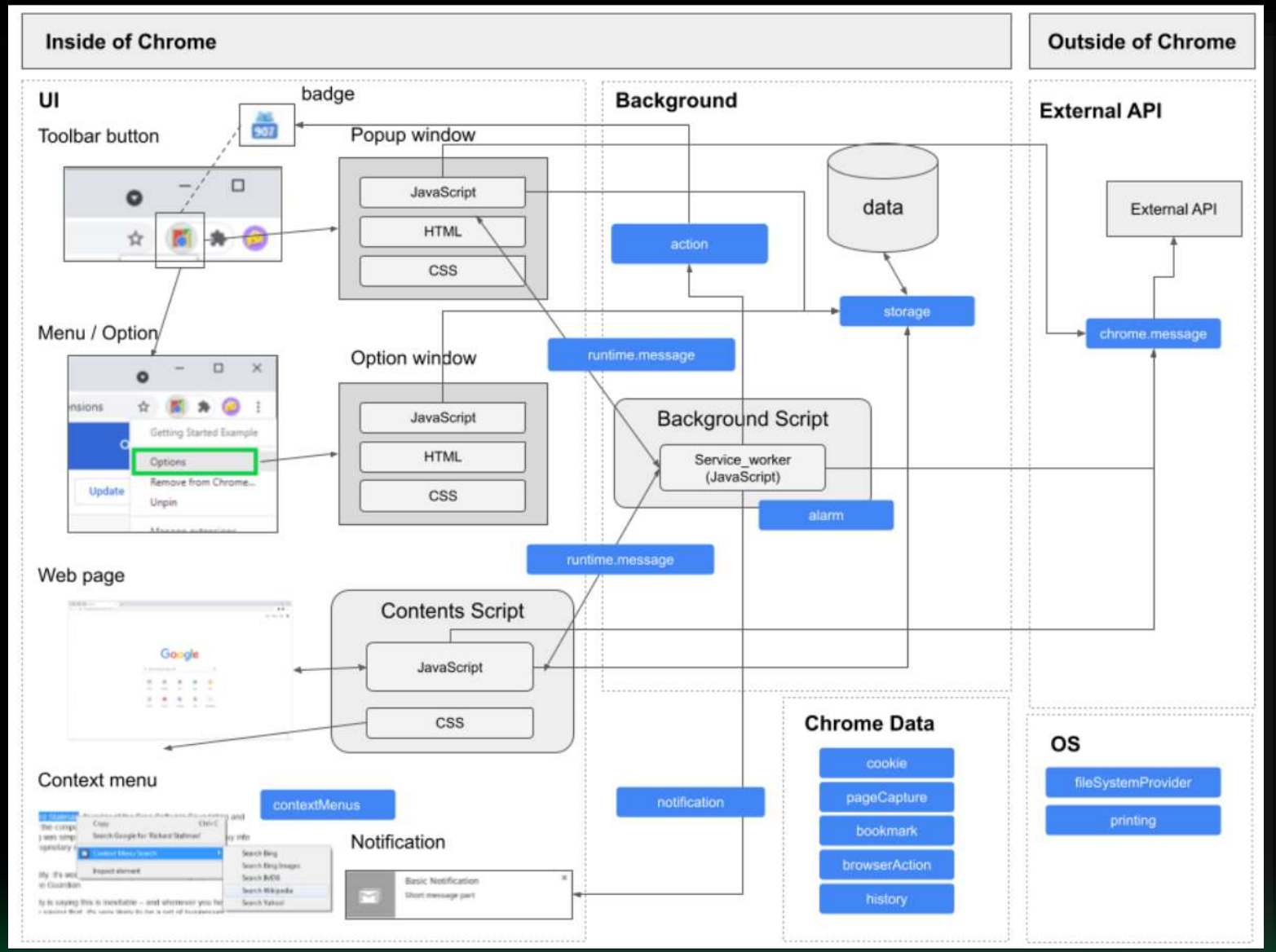
**На диске:**
`%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions`



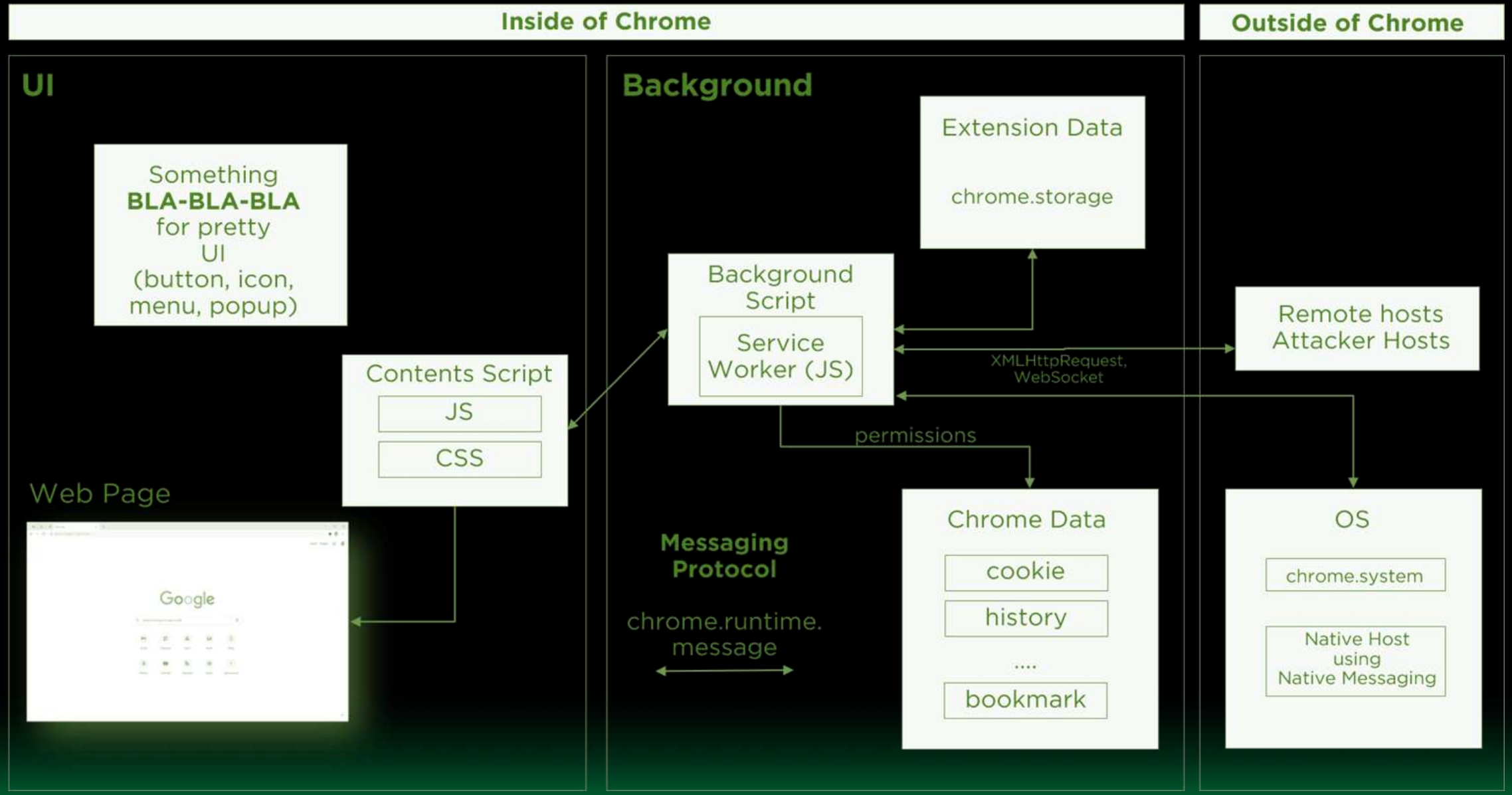


Структура Bitwarden расширения
(парольный менеджер)

# Из чего состоит расширение?

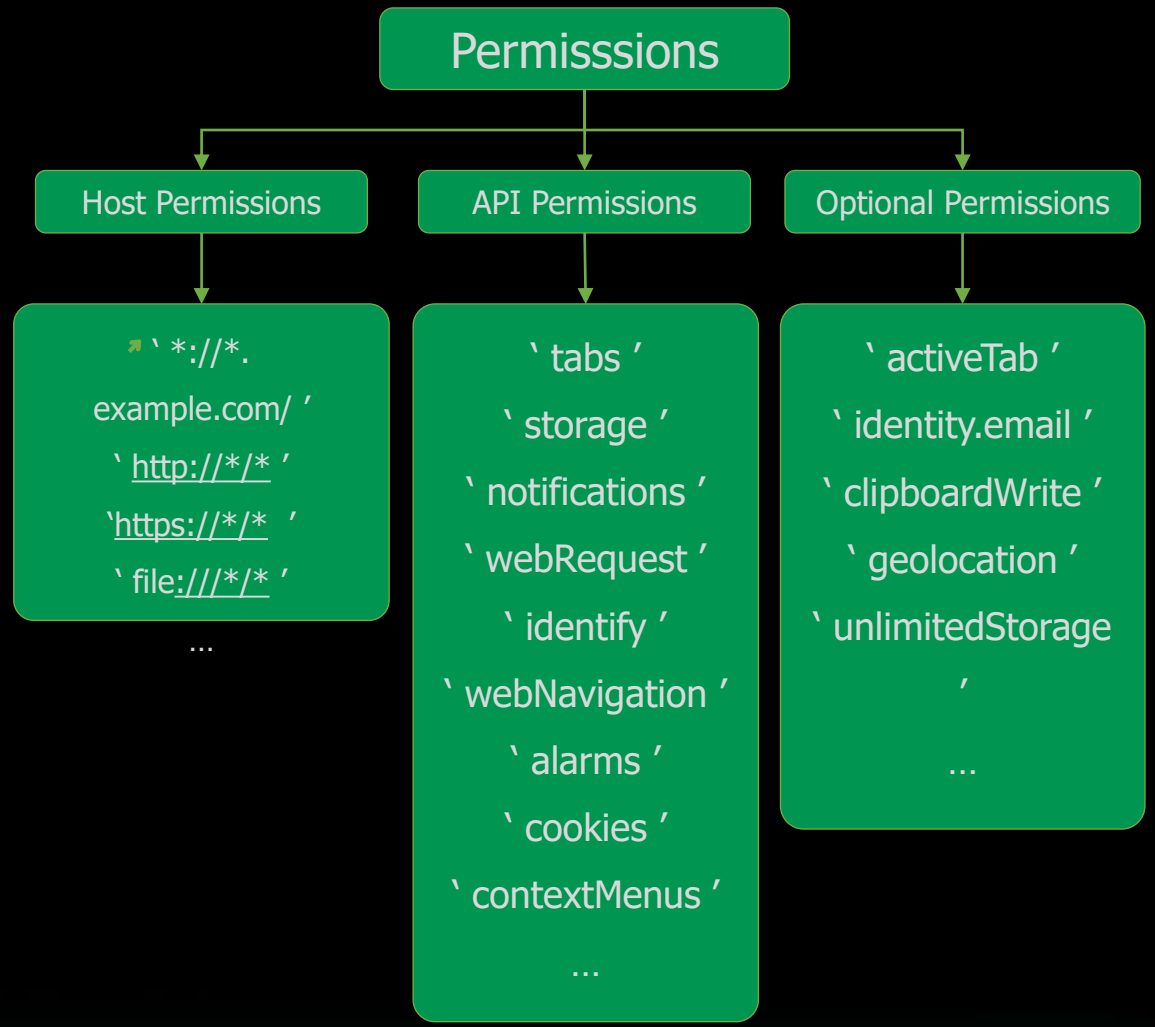


# Из чего состоит расширение? Основное!



# Offensive-like Permissions

| Permission | Action |
|---|---|
| tabs | Доступ к активным вкладкам |
| history | Доступ к истории браузера |
| cookies | Запрос и изменение куки |
| storage | Хранение и изменение пользовательских данных |
| clipboard | Доступ к данным буфера обмена (чтение, запись) |
| scripting | Внедрение JS,CSS в страницу |
| alarms | Периодический запуск кода |
| webRequest | Динамический перехват/подмена сетевого запроса |
| declarativeNetRequest | Блокировка/Редирект сетевого запроса без перехвата |
| proxy | Конфигурация прокси браузера |



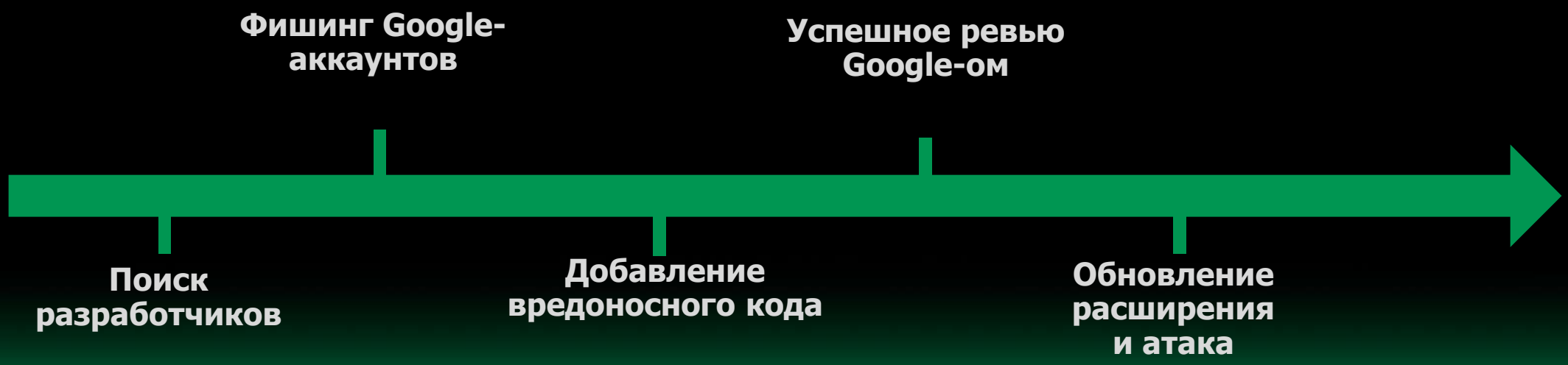
# Механизм обновления расширений

Раньше можно было обновлять через **произвольный** URL.
Теперь только через **Chrome Web Store**

Обновления происходят автоматически при наличии:

- `update_url` в `manifest.json`
- При публикации новой версии в **Chrome Web Store**

**Как следствие**, этот механизм порождает вариант атаки

# EXTENSIONS DELIVERY

Доставка вредоносных расширений жертве

# Варианты доставки

## ★ Working:

- Ручная установка в GUI браузера
- Supply Chain: компрометация разработчика и внедрение кода
- Публикация в Chrome Web Store (собственное расширение)
- GPO-развёртывание (на этапе Post-Compromise)
- Подмена LNK Chrome и размещение расширения на диске
- Extension Side-loading (Stealth-способ)

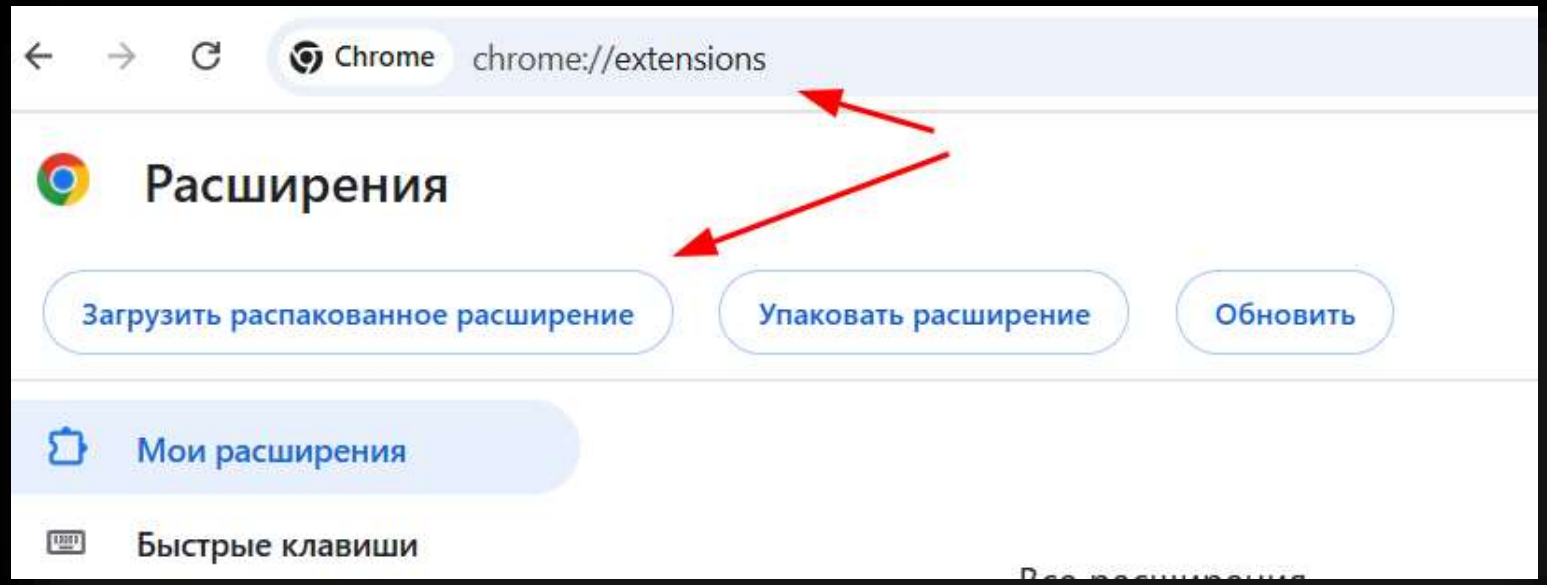

## Not working:

- Установка запакованного расширения CRX

# Ручная установка & Social Engineering

Установка вручную в GUI браузера (chrome://extensions -> Load Unpacked Extension)

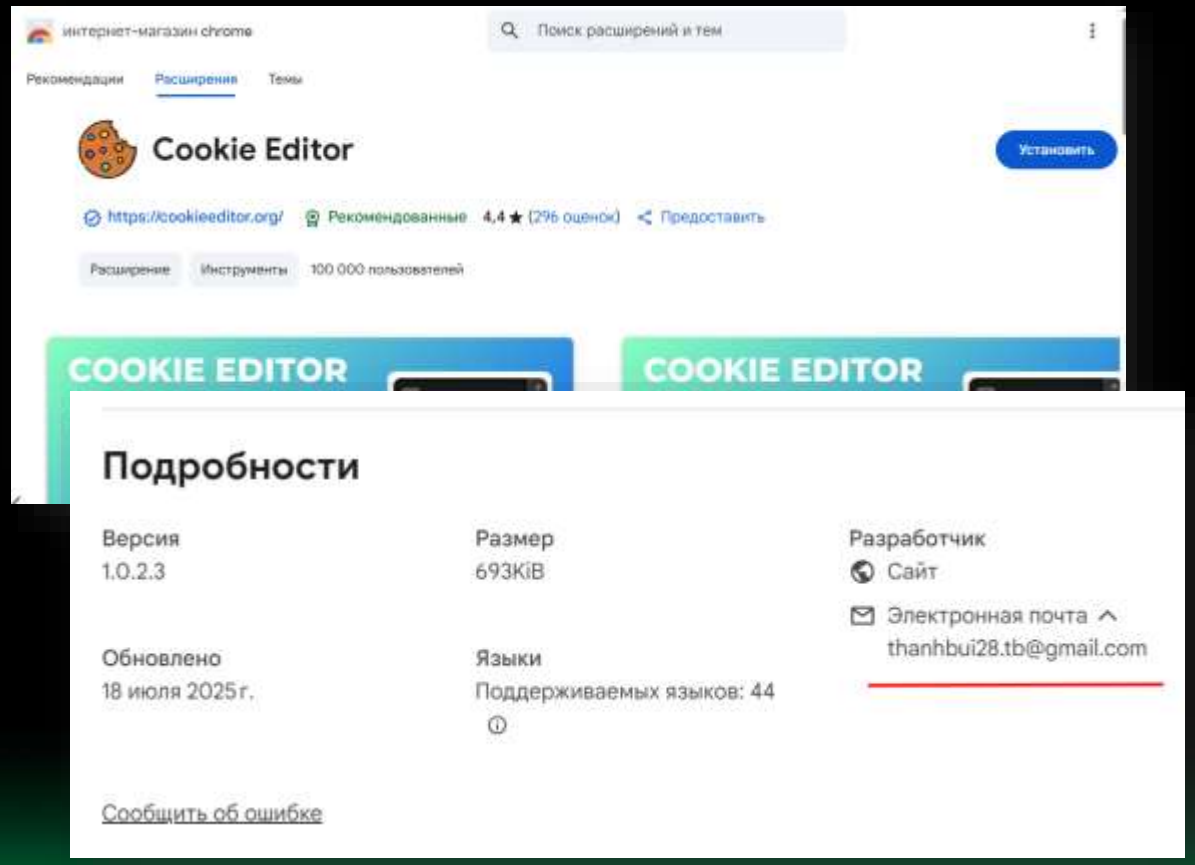
**Жертва**

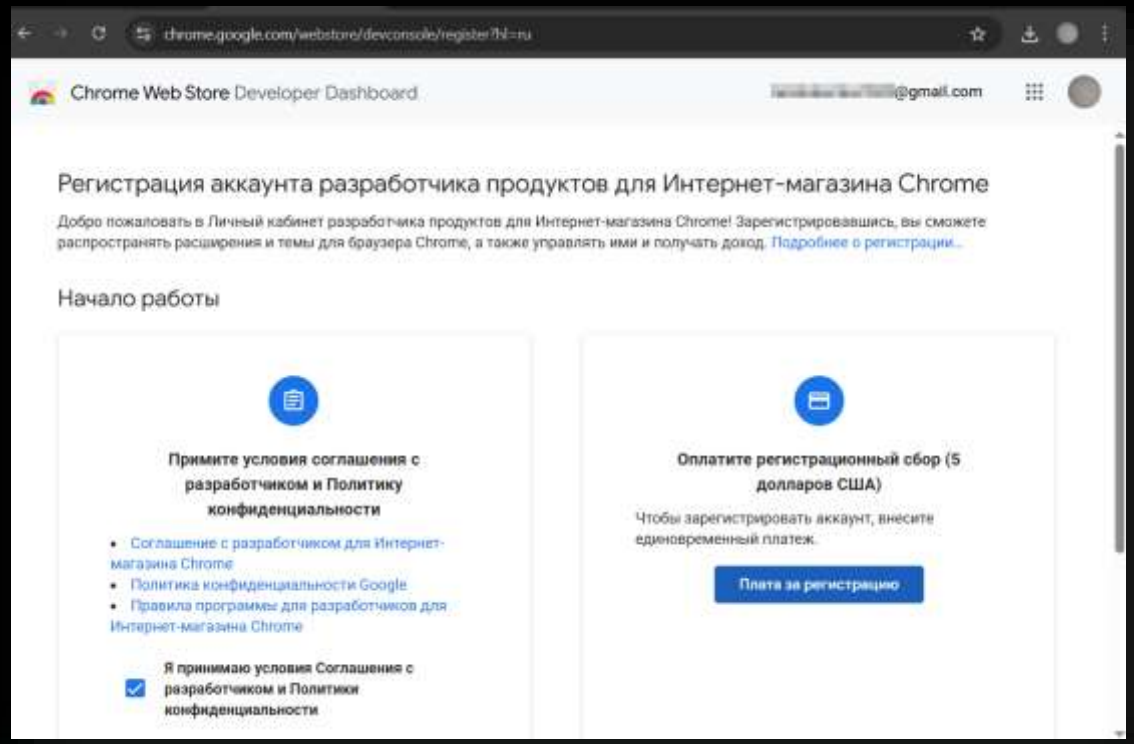


# «Supply Chain»

Загрузка в **Chrome Web Store** и постепенное обновление вредоносным функционалом

- Либо компрометируем разработчика
- Либо сами регистрируемся как разработчик (**но платим $5**)



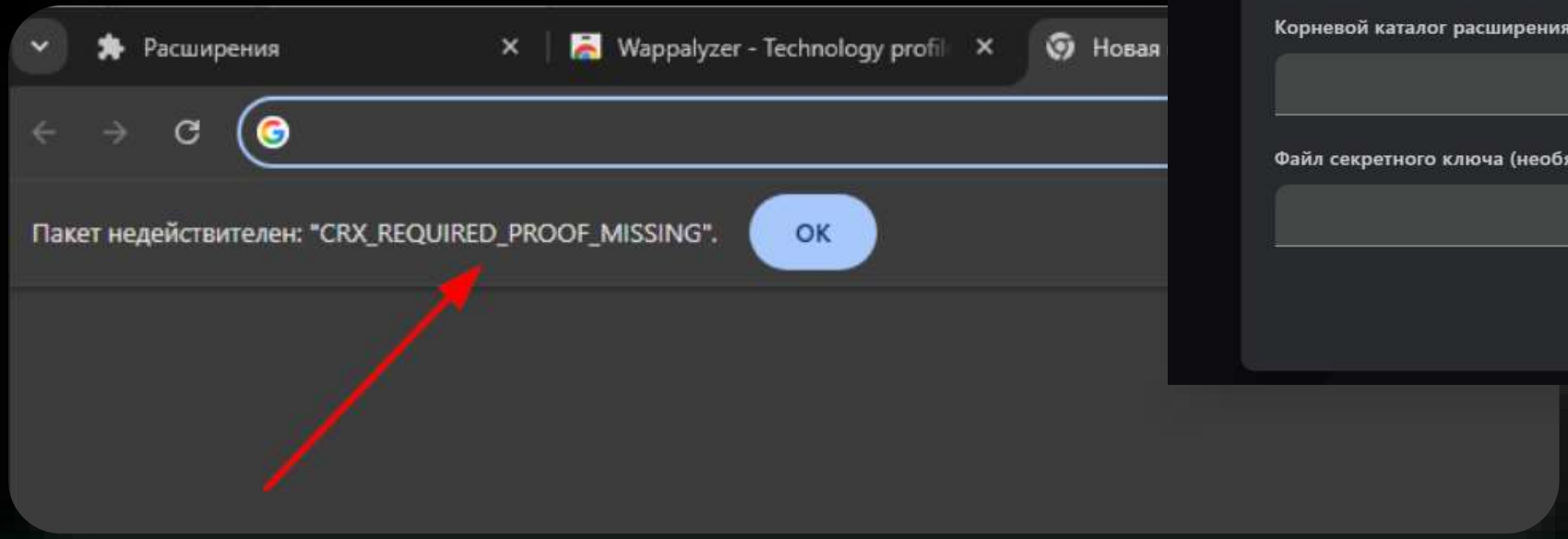



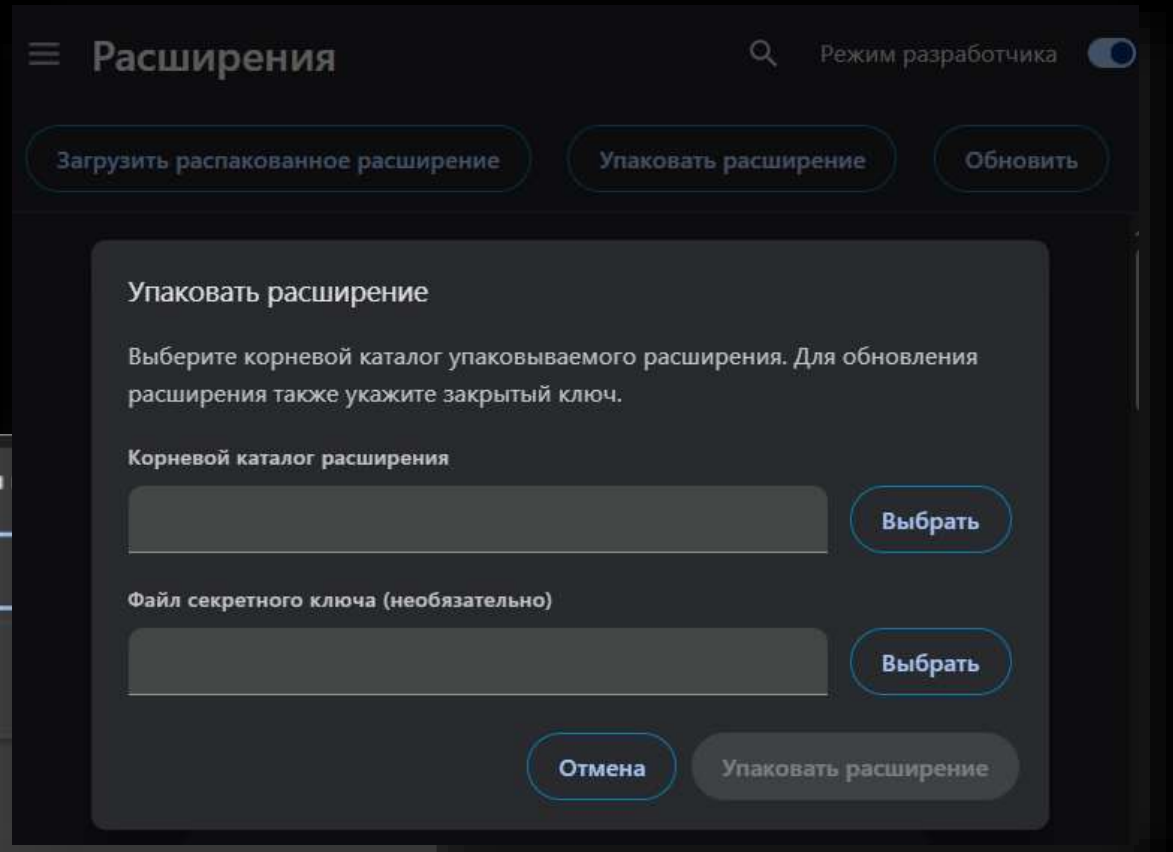
# Установка из CRX

**CRX** – запакованное/сжатое расширение.

Могут возникать ошибки из-за отсутствия цифровой подписи **Chrome Web Store**:

- `CRX_REQUIRED_PROOF_MISSING`
- `CRX_HEADER_INVALID`



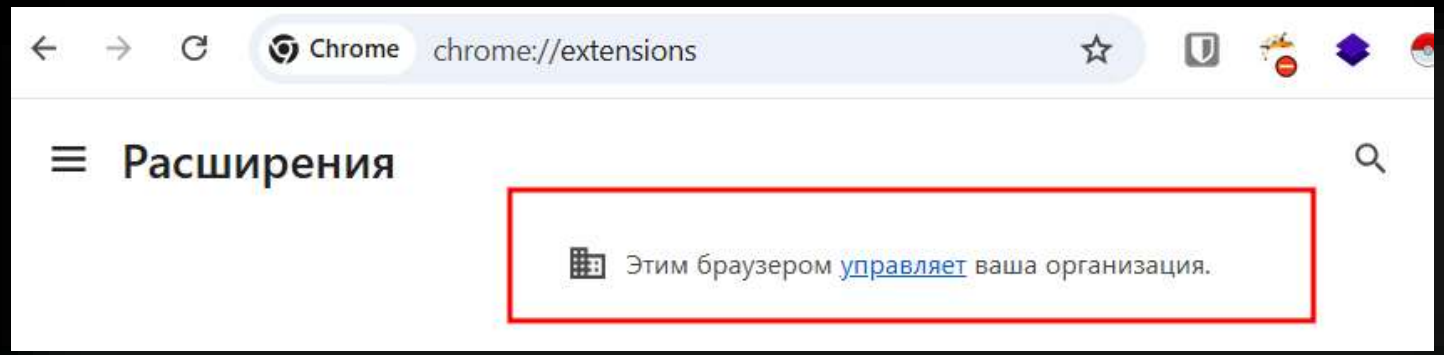
# GPO Installation

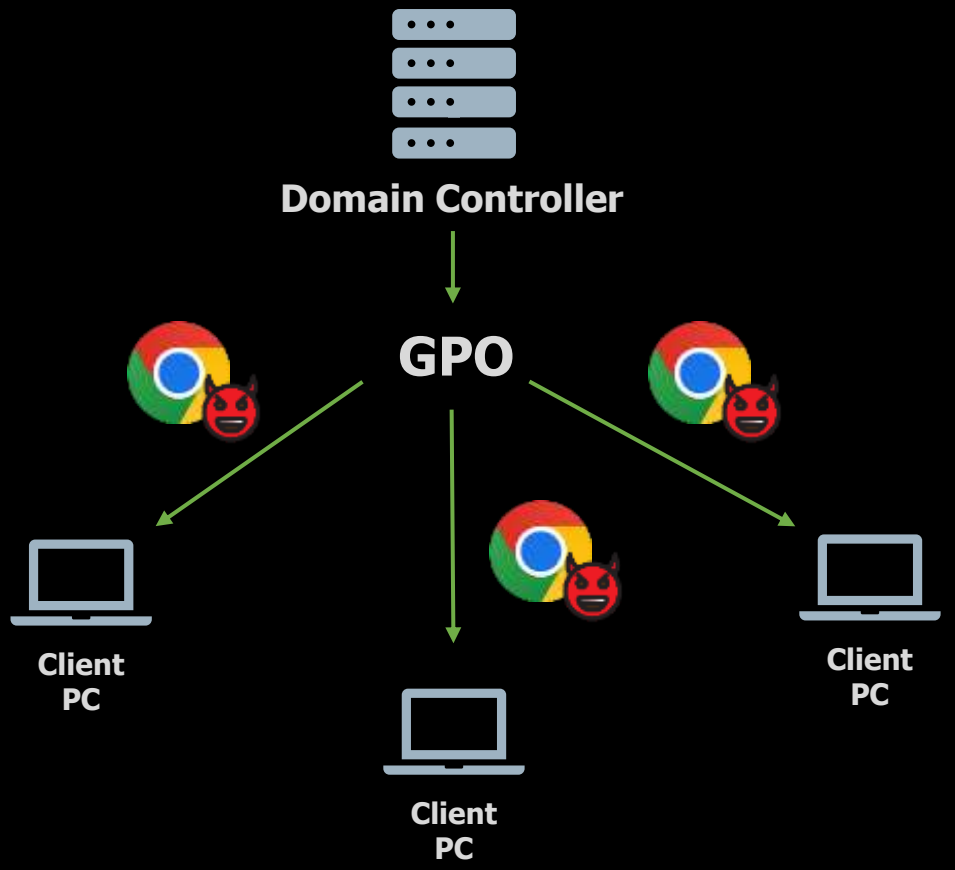
**GPO** (групповые политики) — установка расширения для всех пользователей в домене:

**Ключ реестра:**
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist`

- Нельзя распакованное расширение

+ Работает CRX не из Chrome WebStore



# LNK-файл

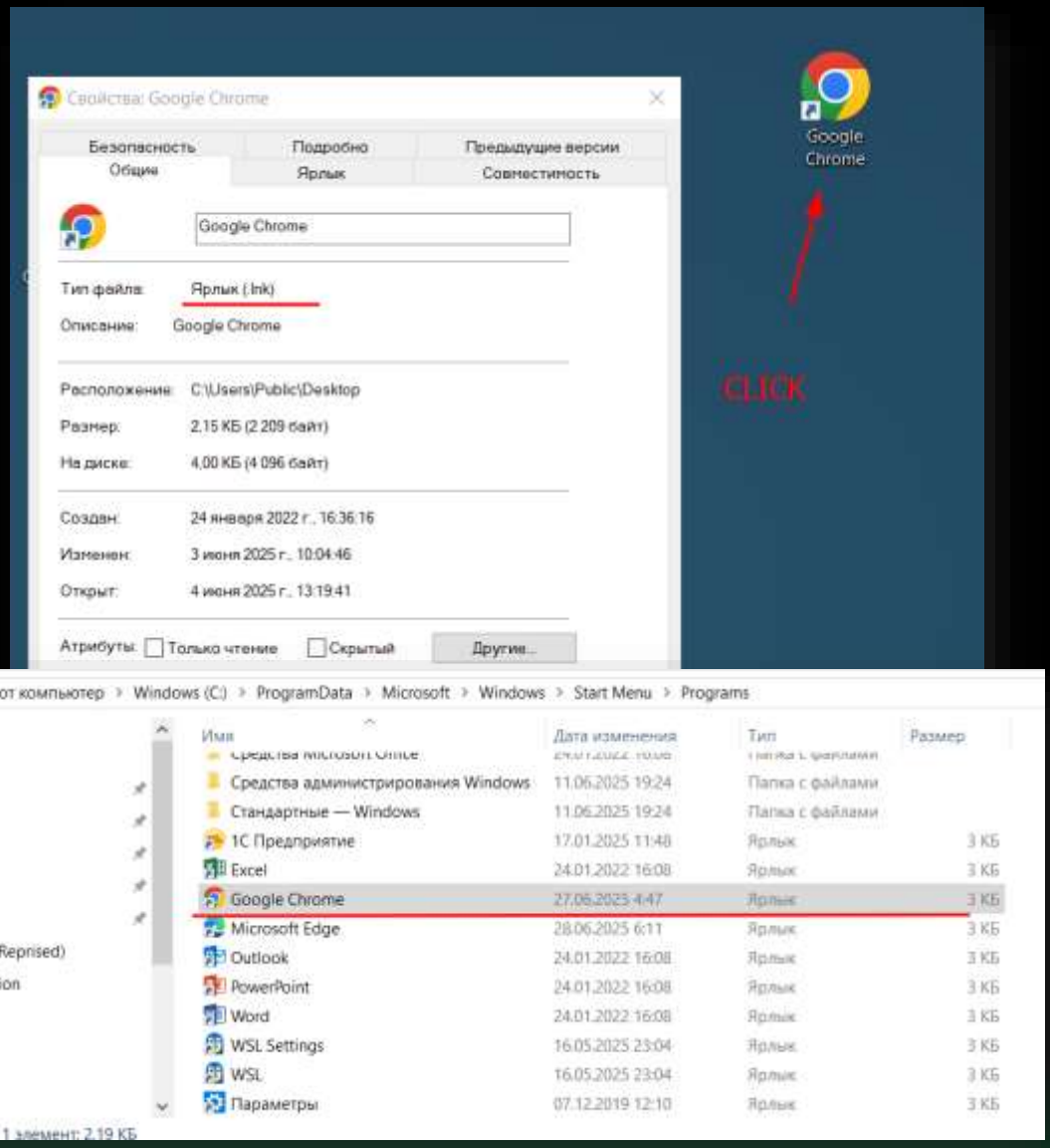
Подмена ярлыка (**.LNK**) для авто-запуска с «подсунутым» вредоносным расширением

**Командная строка:**

```
> chrome.exe --load-extension=/path/to/extension
```

**Шаги воспроизведения:**

- Разместить файлы расширения на файловую систему
- Подменяем ярлык Google Chrome на ярлык с внедрённым параметром `--load-extension`
- Ждём запуска браузера от жертвы



# BAN LNK-метода?!

```
[8060:12444:0617/162655.846:WARNING:chrome\browser\extensions\extension_service.cc:403] --load-extension is not allowed
in Google Chrome, ignoring.
```

Google Git

chromium / chromium / src / 290ed8046692651ce76088914750cb659b65fb17^! / . / chrome / browser / extensions /

**extension_service.cc**

| | |
|---|---|
| **commit** | 290ed8046692651ce76088914750cb659b65fb17 [log] [tgz] |
| **author** | Richard Chen <richche@chromium.org> Sat Apr 05 00:58:56 2025 |
| **committer** | Chromium LUCI CQ <chromium-scoped@luci-project-accounts.iam.gserviceaccount.com> Sat Apr 05 00:58:56 2025 |
| **tree** | 0412f83aafc88dddb7349086665b5ec45059a576 |
| **parent** | f2d7f979c3d97f1883db1f05272e4d91336c575c [diff] [blame] |

Remove `--load-extension` switch on Chrome builds

Part of an on-going effort to reduce harm from the malicious
command-line extensions, this CL removes the exploited switch
only on Chrome builds.

Bug: 401529219
Change-Id: I989dc9b3d50bbeb349b9e0a534945dd64d8c55cf
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/6335815
Reviewed-by: Devlin Cronin <rdevlin.cronin@chromium.org>
Reviewed-by: Justin Lulejian <jlulejian@chromium.org>
Commit-Queue: Richard Chen <richche@google.com>
Reviewed-by: Anunoy Ghosh <anunoy@chromium.org>
Cr-Commit-Position: refs/heads/main@{#1443013}

# А нет, показалось!

**Отключаем** эту же фичу с помощью параметра:

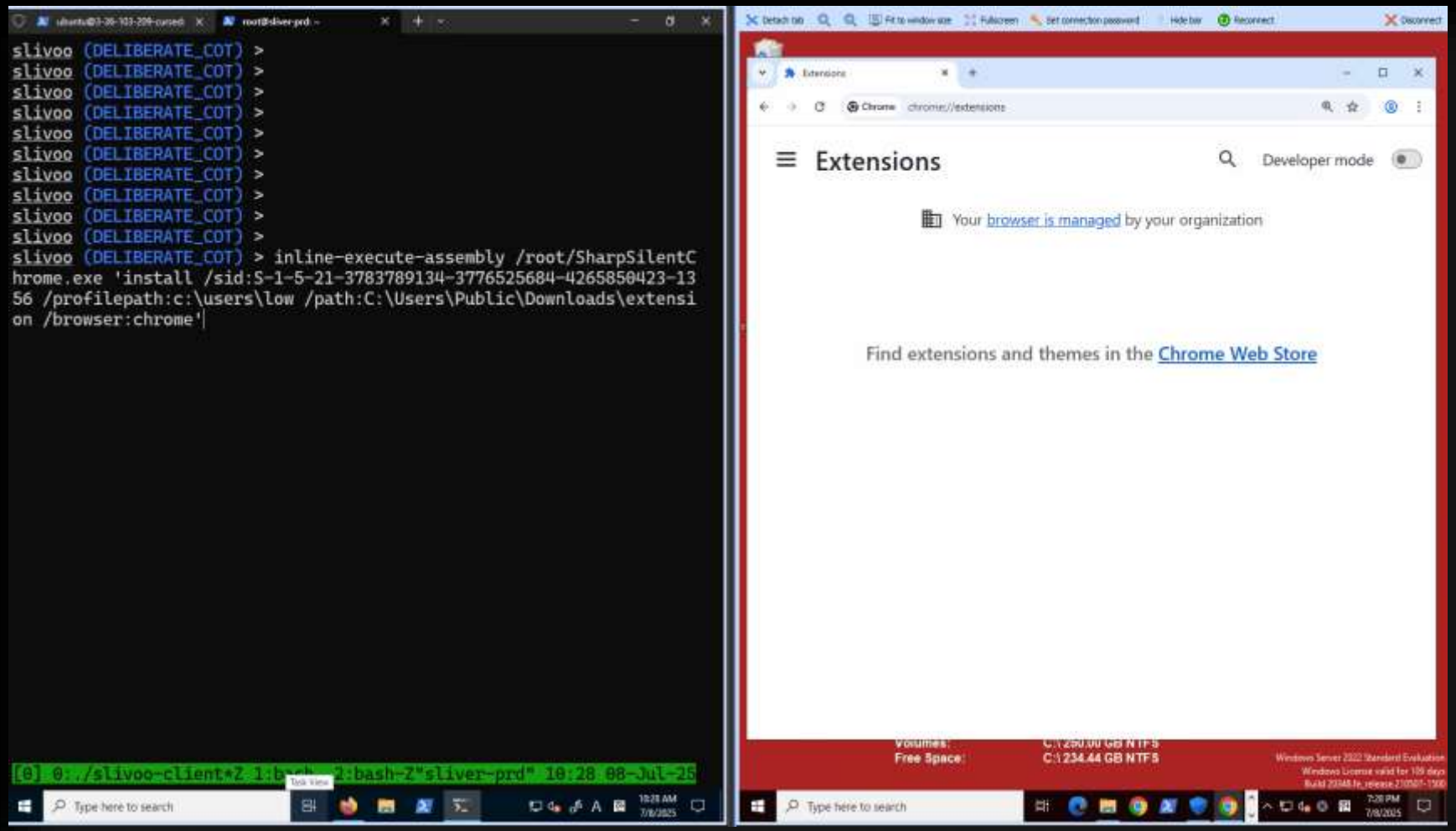
```
"chrome.exe" --disable-features=DisableLoadExtensionCommandLineSwitch
--load-extension="C:\Temp\my-extension"
```

# Proof-Of-Concept

# Extension Side-Loading

**SharpSilentChrome –** утилита

- Модифицируем файлы браузера (Secure Preferences, Preferences)
- Подсчитываем HMAC
- Не используем LNK с --load-extension
- Не требуется участие пользователя



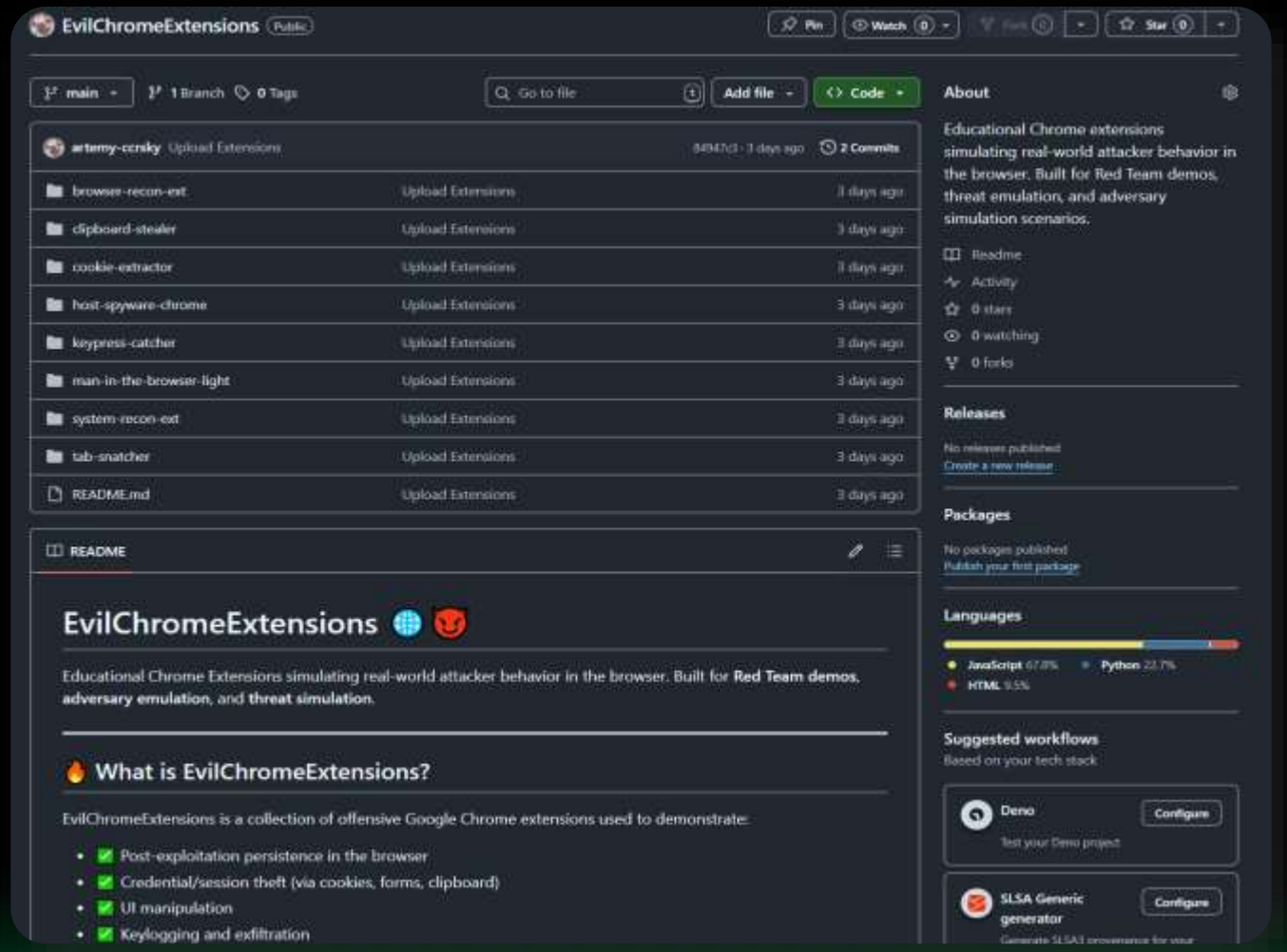

*https://github.com/ChoiSG/SharpSilentChrome*

# POST-EXPLOITATION

Что же всё-таки может делать атакующий?

# Offensive Chrome Extensions Workshop

https://github.com/artemy-ccrsky/EvilChromeExtensions




SCAN ME

# System Recon Extension

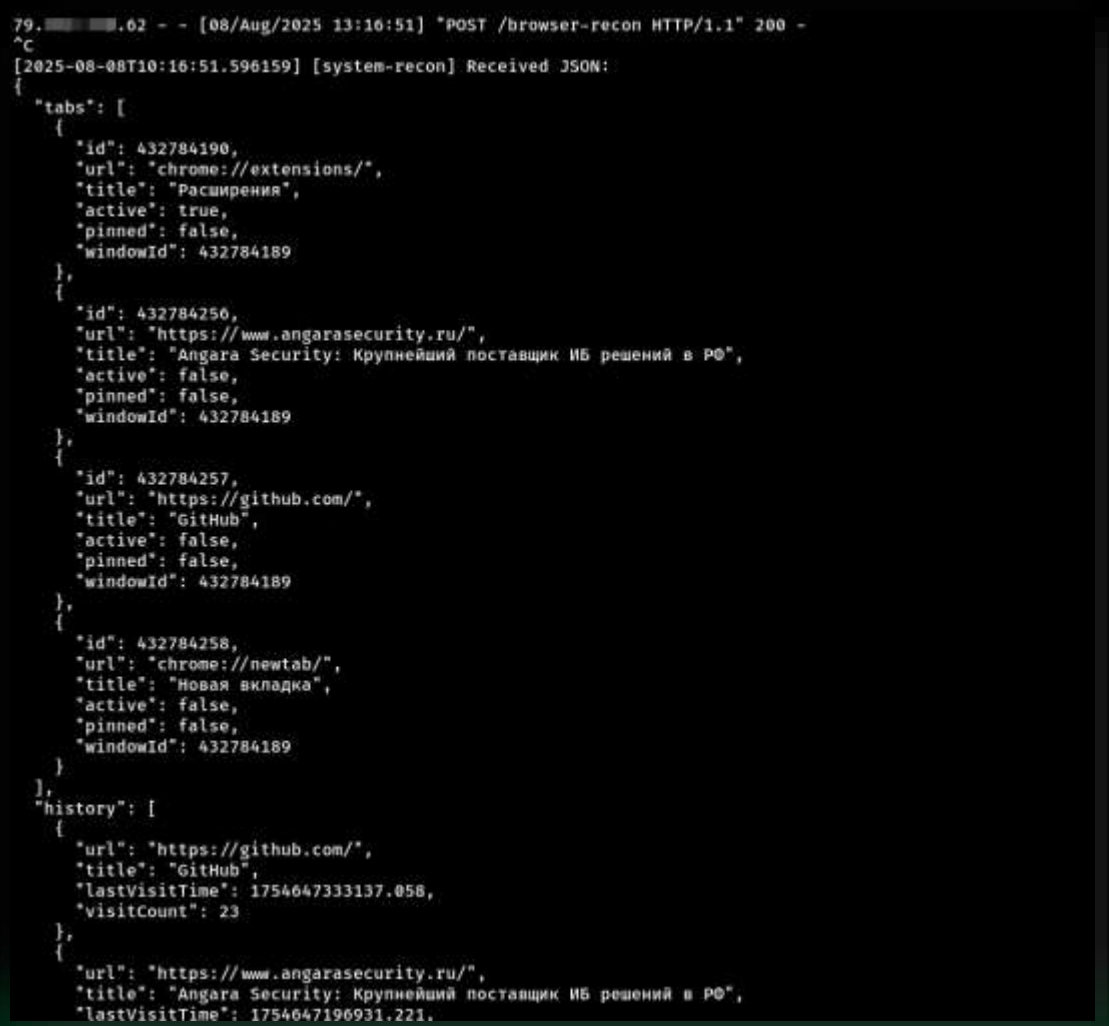
Сбор информации о системе и комплектующих

| Данные | API / Метод |
|---|---|
| ОС и архитектура | `chrome.runtime.getPlatformInfo()` |
| Инфо о процессоре | `chrome.system.cpu.getInfo()` |
| Инфо о видеокарте | `WebGL (WebGraphics Library)` |
| Дисковые устройства | `chrome.system.memory.getInfo()` |
| Дисплей | `chrome.system.display.getInfo()` |
| Браузерная платформа | `navigator.platform` |
| Часовой пояс | `Intl.DateTimeFormat().resolvedOptions().timeZone` |
| Ноутбук ли?<br>Проверка батареи | `Navigator.getBattery` |

# Browser Recon Extension

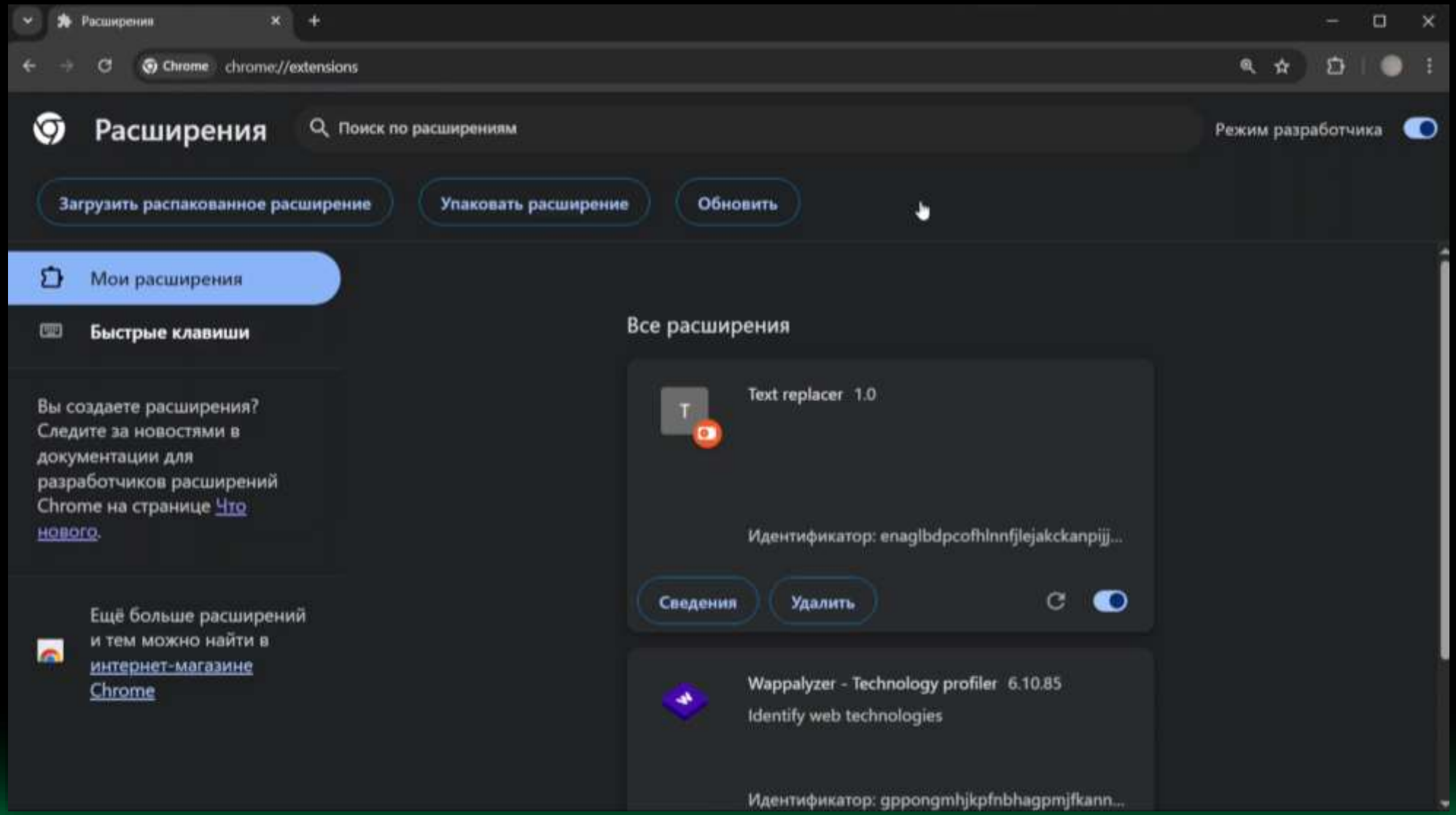
Сбор информации о браузере и окружении

| Данные | API / Метод |
|---|---|
| Активные вкладки | `chrome.tabs.query()` |
| История браузера | `chrome.history.search()` |
| Закладки | `chrome.bookmarks` |
| User-Agent | `navigator.userAgent` |
| Storage (пользовательские данные) | `chrome.storage` |
| Браузерная платформа и версия | `navigator.platform` |
| Инфо о прокси | `chrome.proxy.settings` |
| Буфер обмена | `navigator.clipboard` |
| Установленные расширения | `chrome.management` |



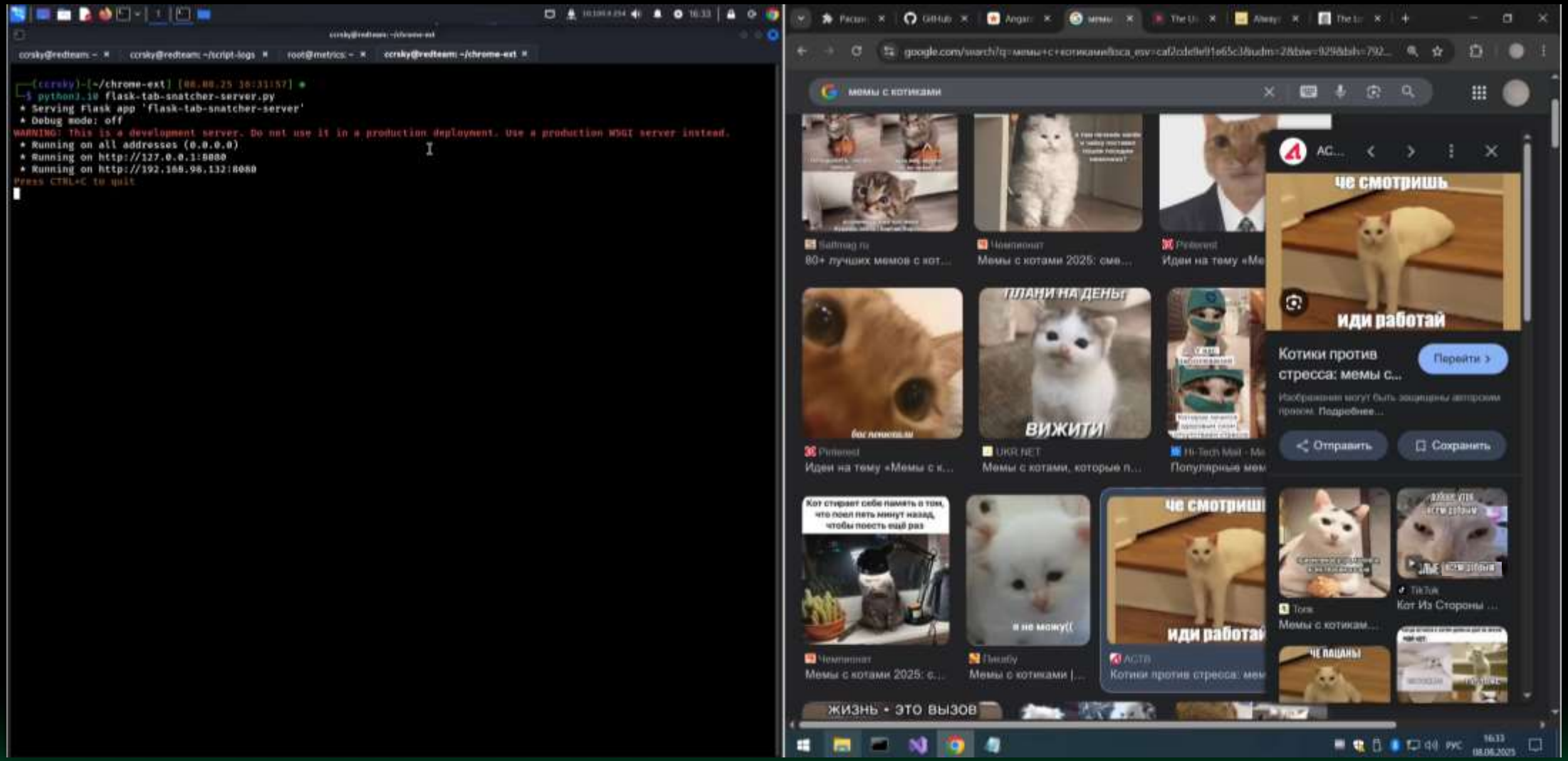
# Man-In-The-Browser Light

**Подменяем** содержимое в HTML с помощью `content.js`



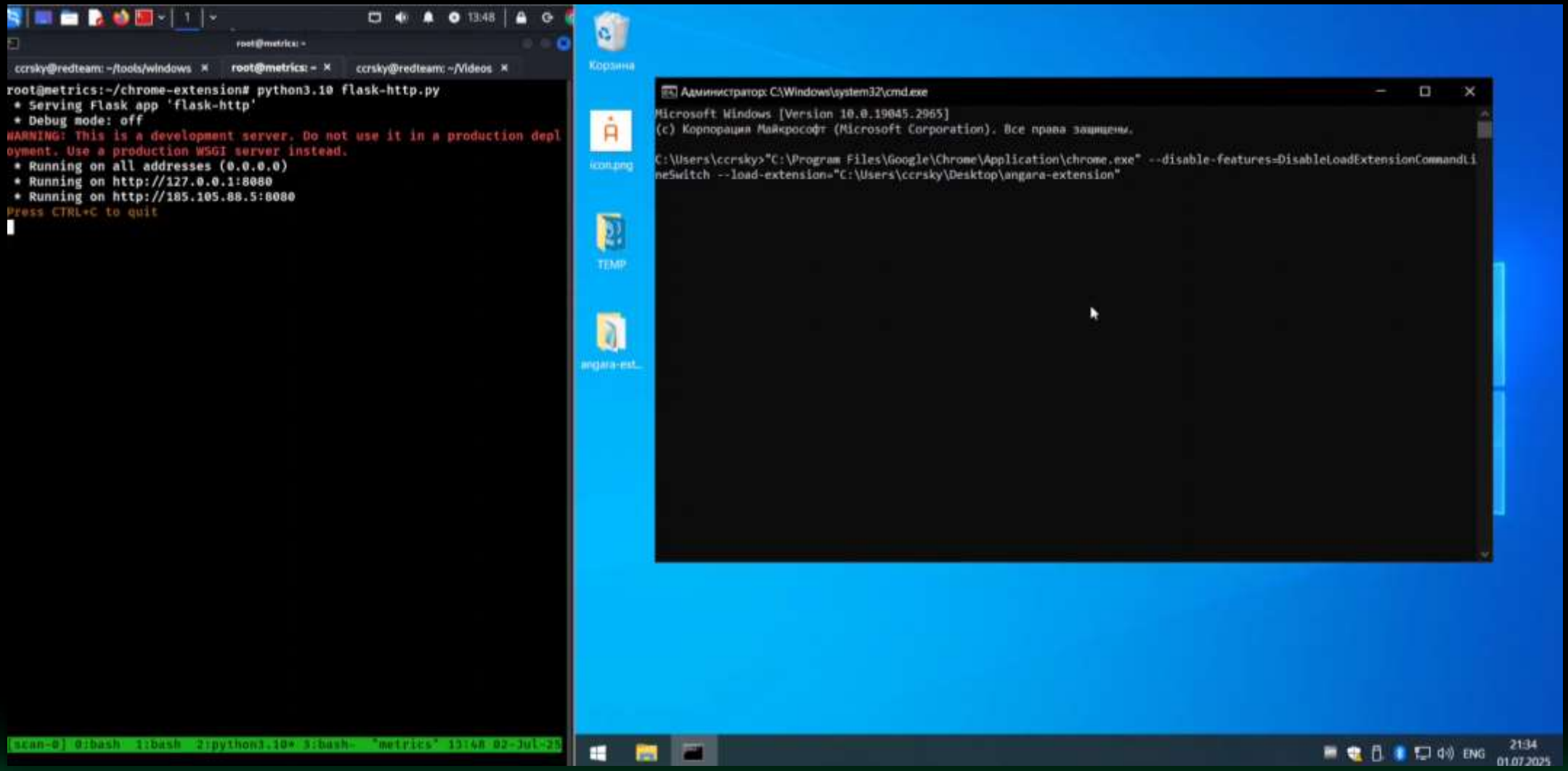
# Tab Snatcher

**Скриншотим** вкладки пользователя и забираем **DOM-**страницы



# Cookie Extraction

Авторизация на ресурс без логина и пароля. Периодический запрос актуальных Cookie

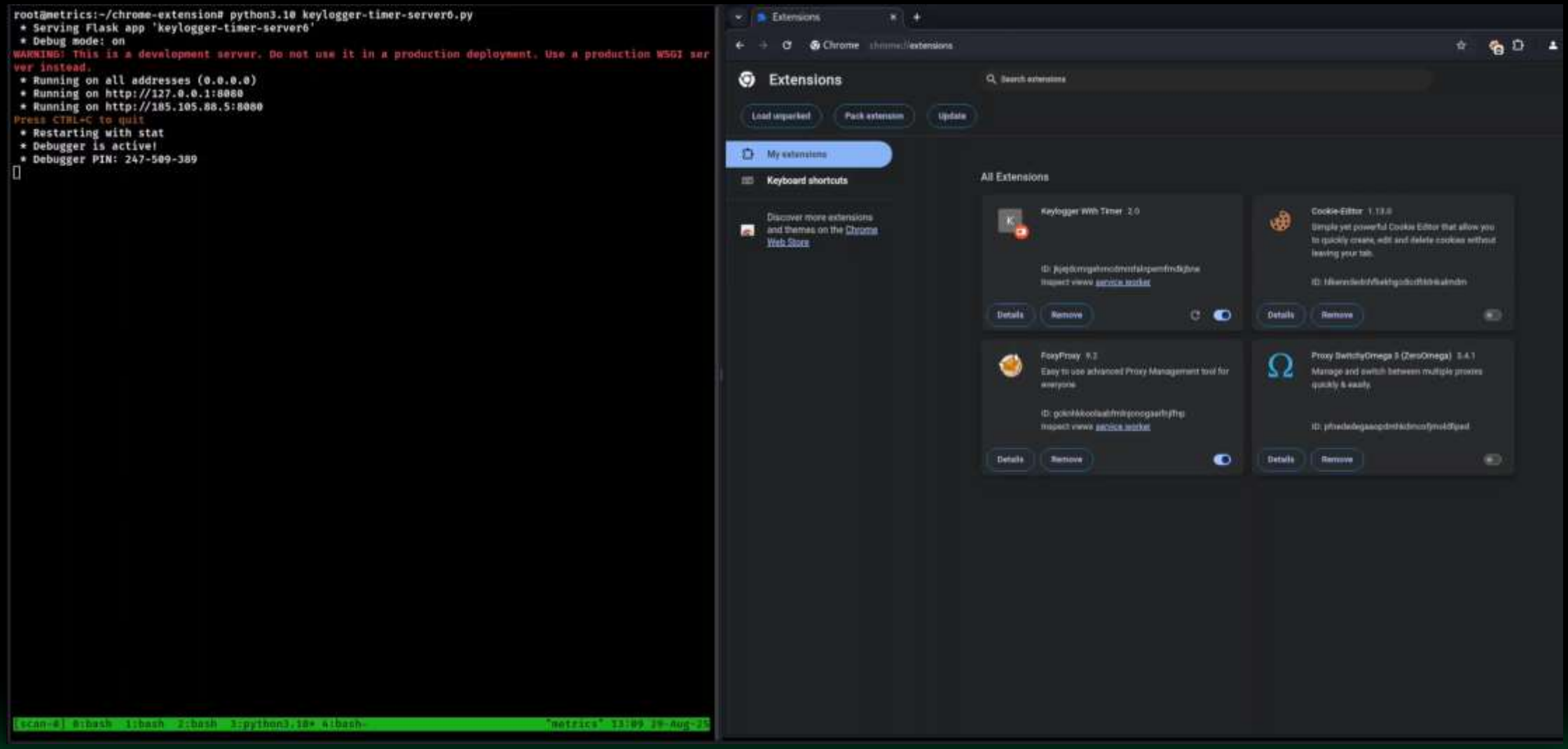


# Dump DPAPI vs Chrome Extension

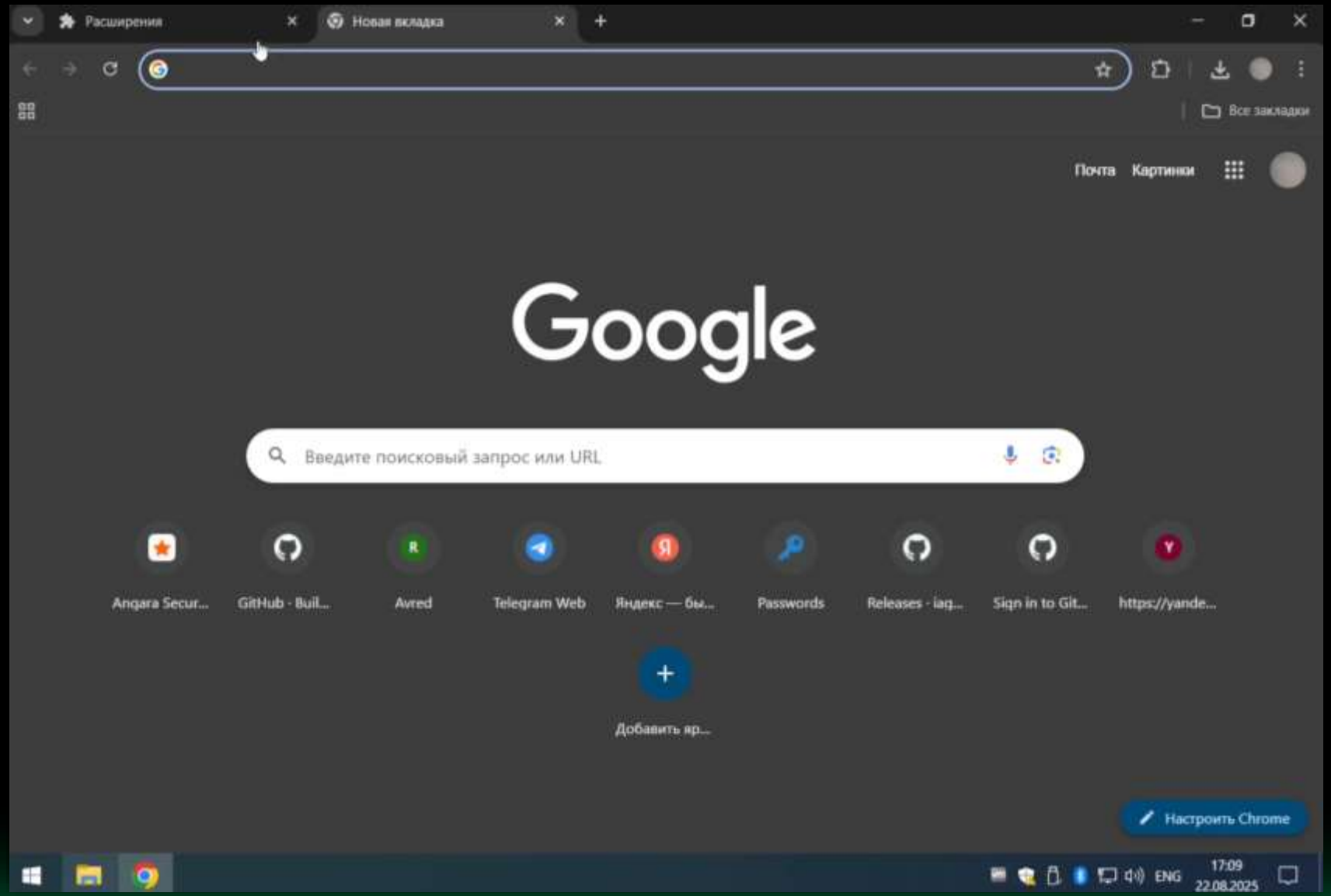

VS

# Simple Keylogger

Внедрение JS в браузере и отправка нажатий на удалённый сервер



# Clipboard Stealer

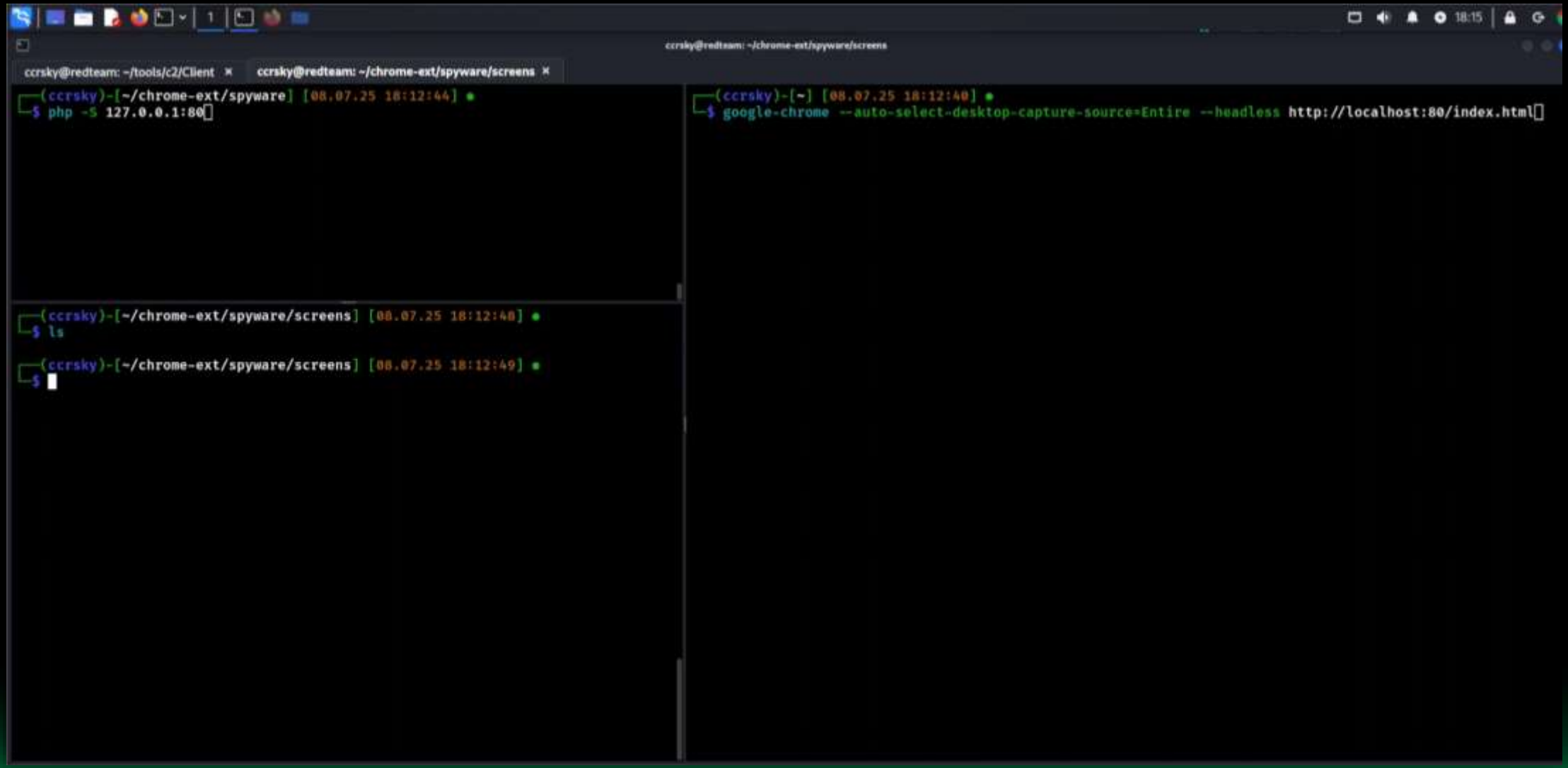



Ждём срабатывания **COPY** события и отправляем буфер обмена на удалённый сервер.

Интересно в случаях **парольных менеджерей**: Bitwarden, ПассВорк, 1Password, Google Password Manager и т.д.

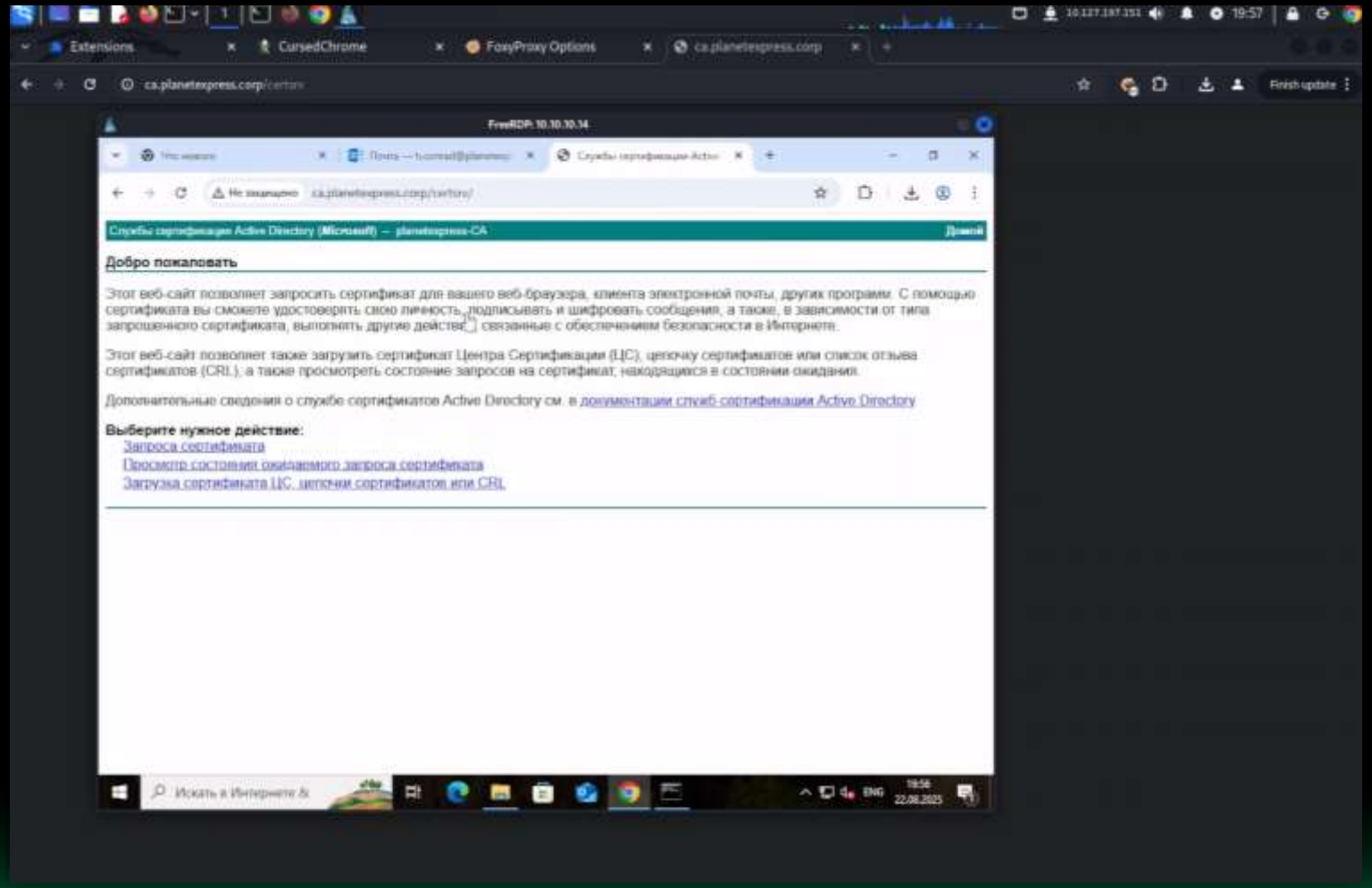
# Host Spyware by Chromium

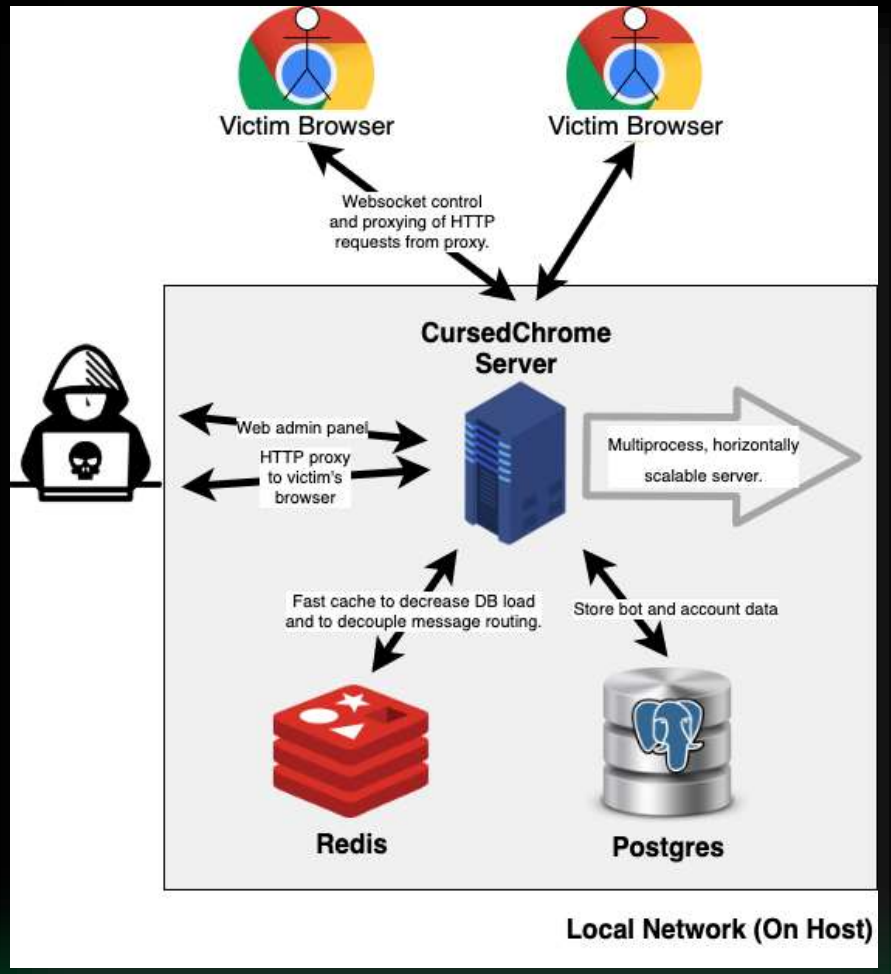
Запуск с флагом `--auto-select-desktop-capture-source=Entire`
Открывается ресурс с предложением Sharing Screen -> Авто-применение -> Отправка скриншотов на сервер



# Proxy-over-Chrome. CursedChrome

**Удалённый доступ** по WebSocket к браузеру жертвы в режиме **HTTP Proxy**
(Доступ к внутренним сайтам из-за NAT/корпоративной сети без VPN).



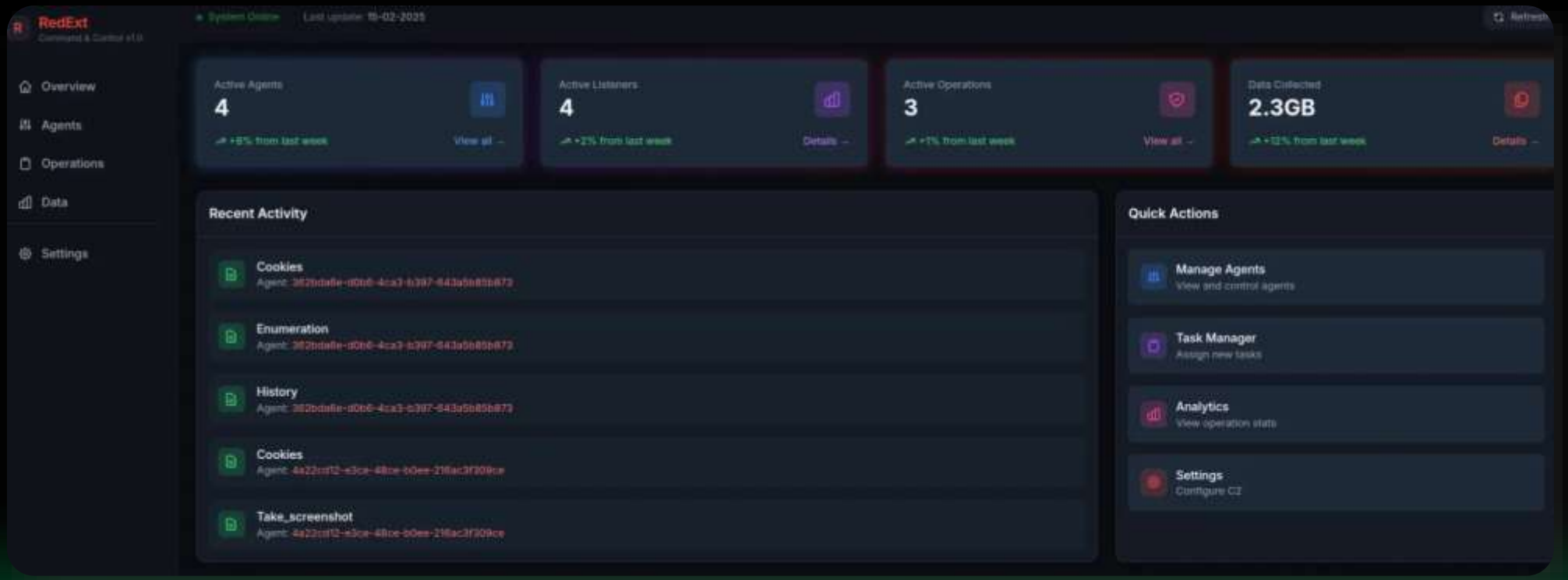



# C&C Extension. RedExt

Управление браузером через удаленный командный сервер

**Функции**:

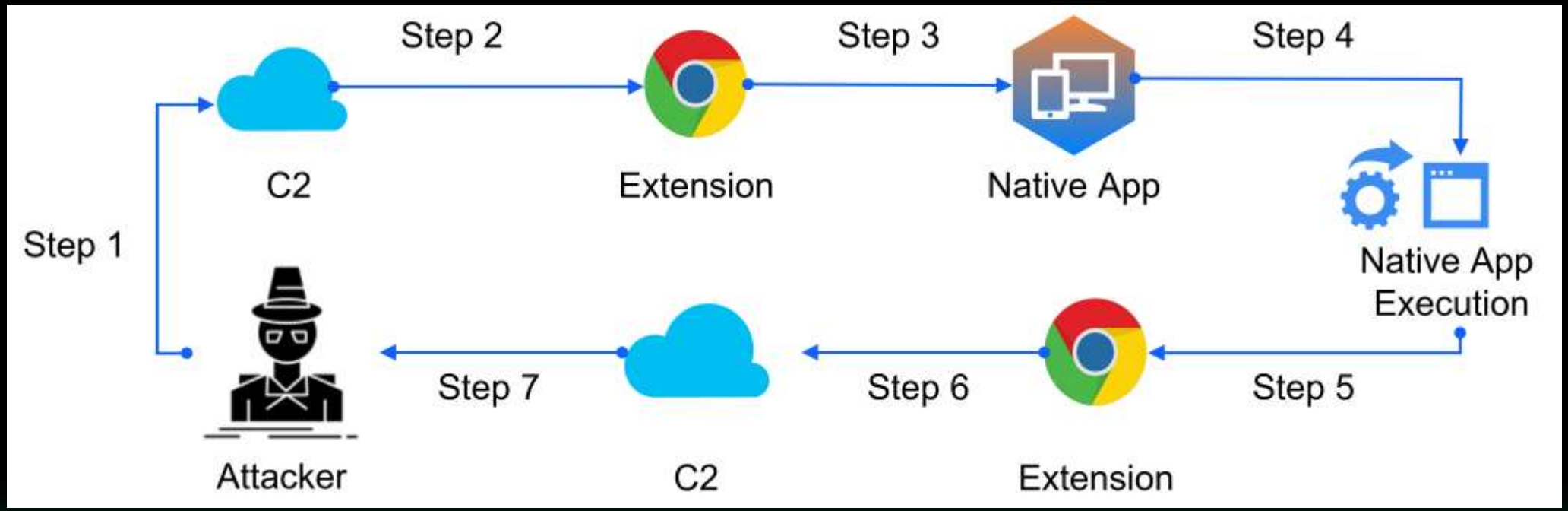
- Извлечение истории браузера, DOM активных вкладок
- Скриншоттинг страниц, System-разведка
- Перехват Cookie



# C&C Extension. Native App

Управление ОС с использованием **Native Messaging Host**

- **Native Host** общается с расширением, используя JSON
- В расширении метод – `chrome.runtime.connectNative("com.example.nativehost")`
- Регистрация в реестре `HKEY_CURRENT_USER\Software\Google\Chrome\NativeMessagingHosts\<имя>.json`



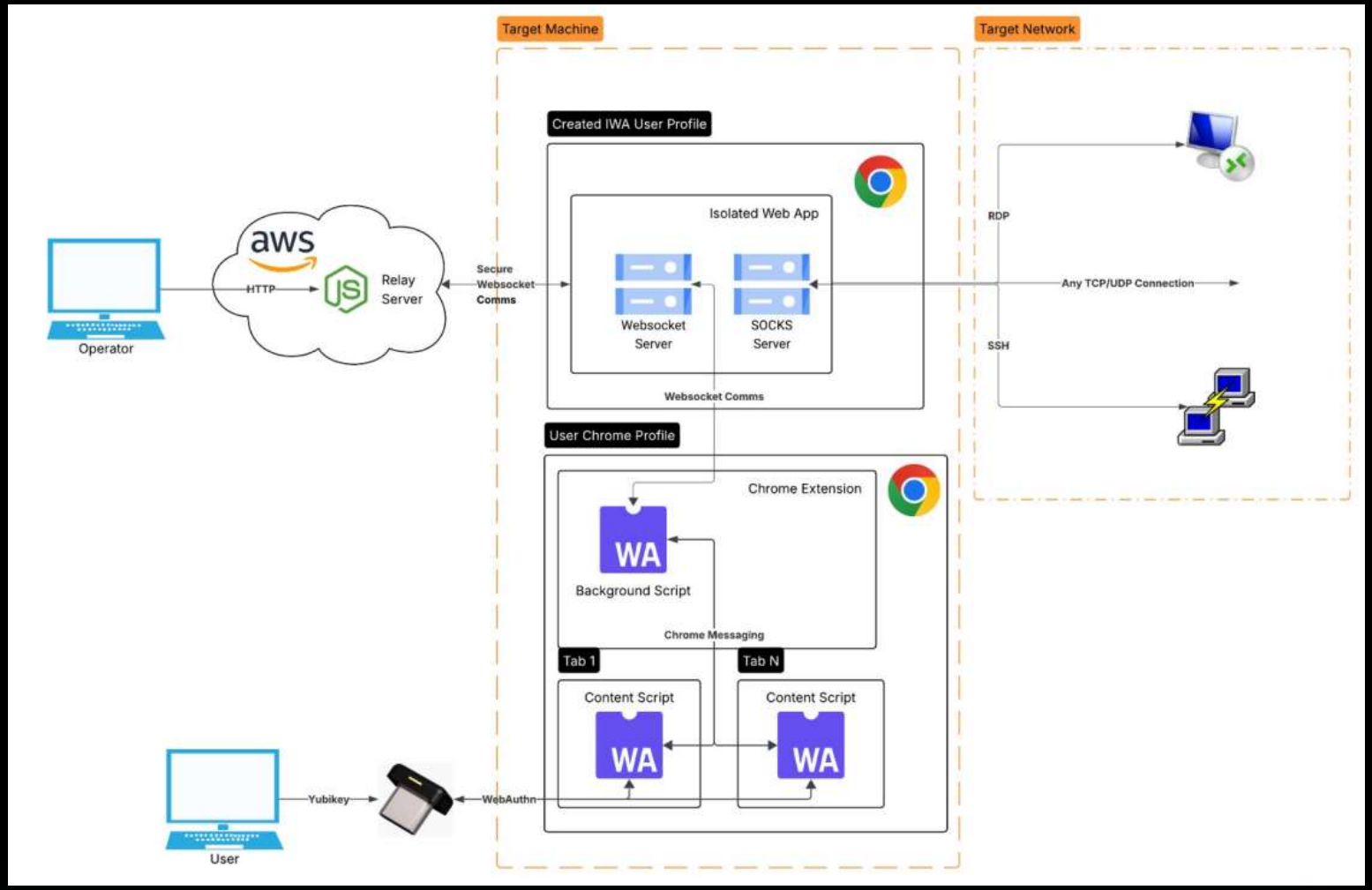

** https://github.com/efchatz/Covert-C2*

# C&C Extension. ChromeAlone

Агент на базе **Chrome Extension** + **Isolated Web App** представлен на DEF CON в 2025** Пока завязан на **AWS**

**Функции**:

- SOCKS TCP Proxy
- Кража Cookie + паролей
- Запуск EXE на хосте (native messaging)
- Достает до физических токенов
- Устойчиво к EDR (пока что)




* - https://github.com/praetorian-inc/ChromeAlone
** - Michael Weber - ChromeAlone - Transforming a Browser into a C2

# DEFENSE

Как защищаться от всего этого?

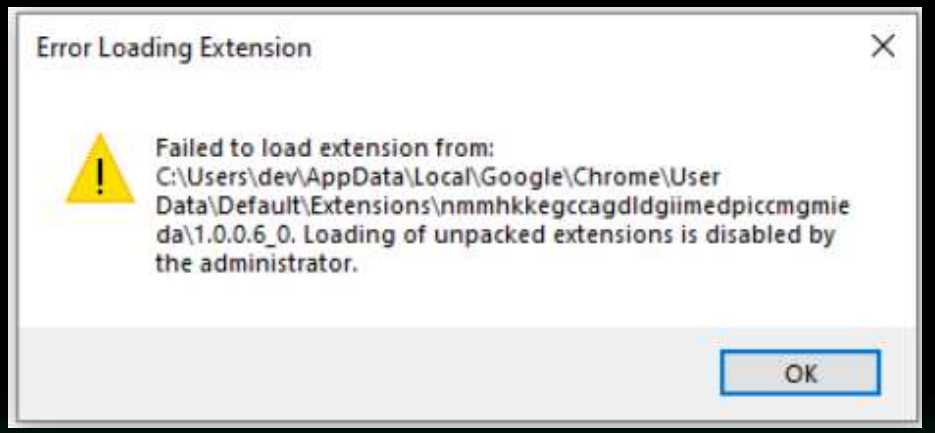
# Рекомендации по защите

- Избыточные привилегии у расширения **(ALERT!)**
- Обфусцированный код у расширения **(ALERT!)**
- Мониторить модификации (Secure Preferences, Preferences), сделанные **не** chrome.exe
- Мониторить реестр: `HKCU\HKLM\SOFTWARE\Google\Chrome\NativeMessaging Hosts\com.my_company.my_application`

**Ужесточаем настройки GPO:**

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome`

- Запрет установки расширений – `ExtensionInstallBlockList=<something>`
- «Белый список» расширений – `ExtensionInstallAllowList=<something>`
- Запретить установку распакованных расширений



# Борьба Google с расширениями

Активные коммиты в исходный код в разделе chrome/browser/extensions/*.c
**Google Dork:** `malicious extensions chrome site:googlesource.com`

Google Open Source
https://chromium.googlesource.com › ... · Перевести эту страницу

e156ccff5dc879607ca48817e63...

Remove `--extensions-on-chrome-urls` switch from Chrome builds Part of an on-going effort to **reduce harm from the malicious extensions** command-line switches ...

Google Open Source
https://chromium.googlesource.com › ... · Перевести эту страни

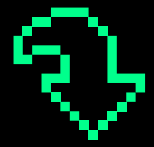
06bd8d4d66c477de2801b60044...

Remove `--disable-extensions-except` switch on Chrome b
harm from the malicious command-line extensions, this CL ...

Google Open Source
https://chromium.googlesource.com › ... · Перевести эту страни

290ed8046692651ce760889147...

Remove `--load-extension` switch on Chrome builds Part of an
**malicious command-line extensions**, this CL removes the ...



chromium / chromium / src / 290ed8046692651ce76088914750cb659b65fb17^! / . / chrome / browser / extensions /
**extension_service.cc**

```
commit 290ed8046692651ce76088914750cb659b65fb17                    [log] [tgz]
author Richard Chen <richche@chromium.org>                         Sat Apr 05 00:58:56 2025
committer Chromium LUCI CQ <chromium-scoped@luci-project-accounts.iam.gserviceaccount.com> Sat Apr 05 00:58:56 2025
tree 0412f83aafc88dddb7349086665b5ec45059a576
parent f2d7f979c3d97f1883db1f05272e4d91336c575c [diff] [blame]

Remove `--load-extension` switch on Chrome builds

Part of an on-going effort to reduce harm from the malicious
command-line extensions, this CL removes the exploited switch
only on Chrome builds.
```

# SIEM Rules

Имеются публично доступные SIEM-правила. Например, детект аргумента `--load-extension`

```
18    logsource:
19        category: process_creation
20        product: windows
21    detection:
22        selection:
23            Image|endswith:
24                - '\brave.exe'
25                - '\chrome.exe'
26                - '\msedge.exe'
27                - '\opera.exe'
28                - '\vivaldi.exe'
29            CommandLine|contains: '--load-extension='
30        condition: selection
```

sigma / rules / windows / process_creation / proc_creation_win_browsers_chromium_load_extension.yml

github-actions[bot] and nasbench Merge PR #5027 from @nasbench - Promote older rules status from 'expe...

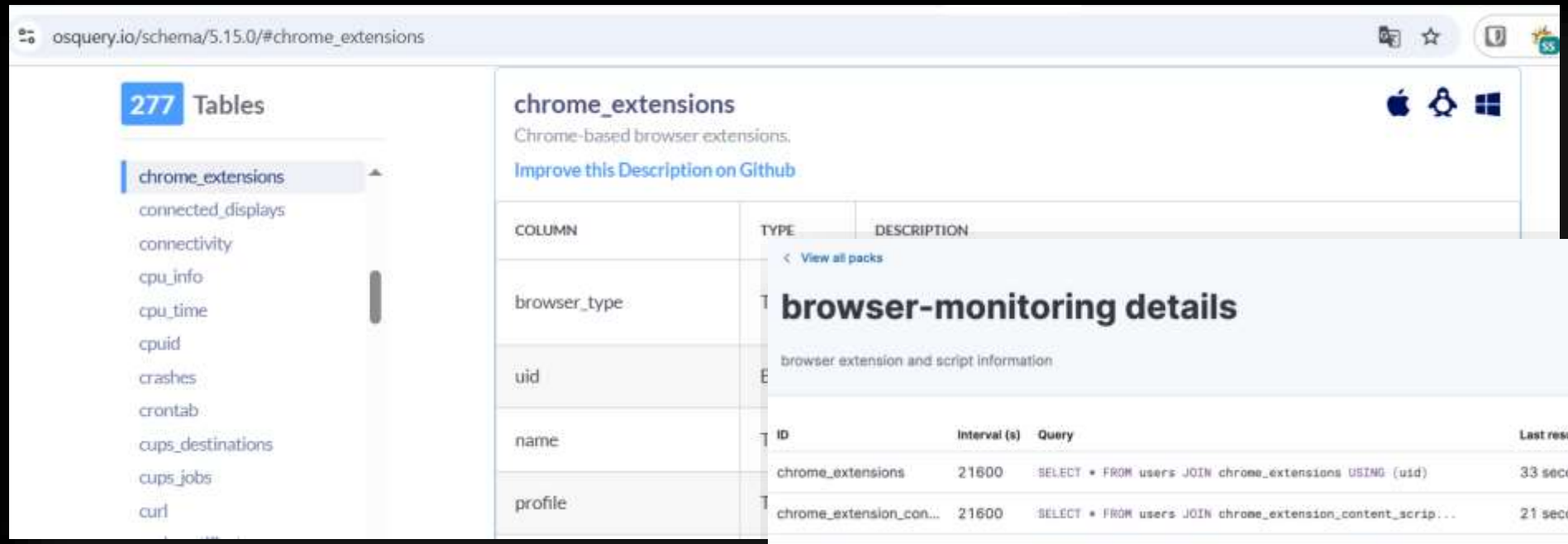
Code Blame 33 lines (33 loc) · 1.05 KB

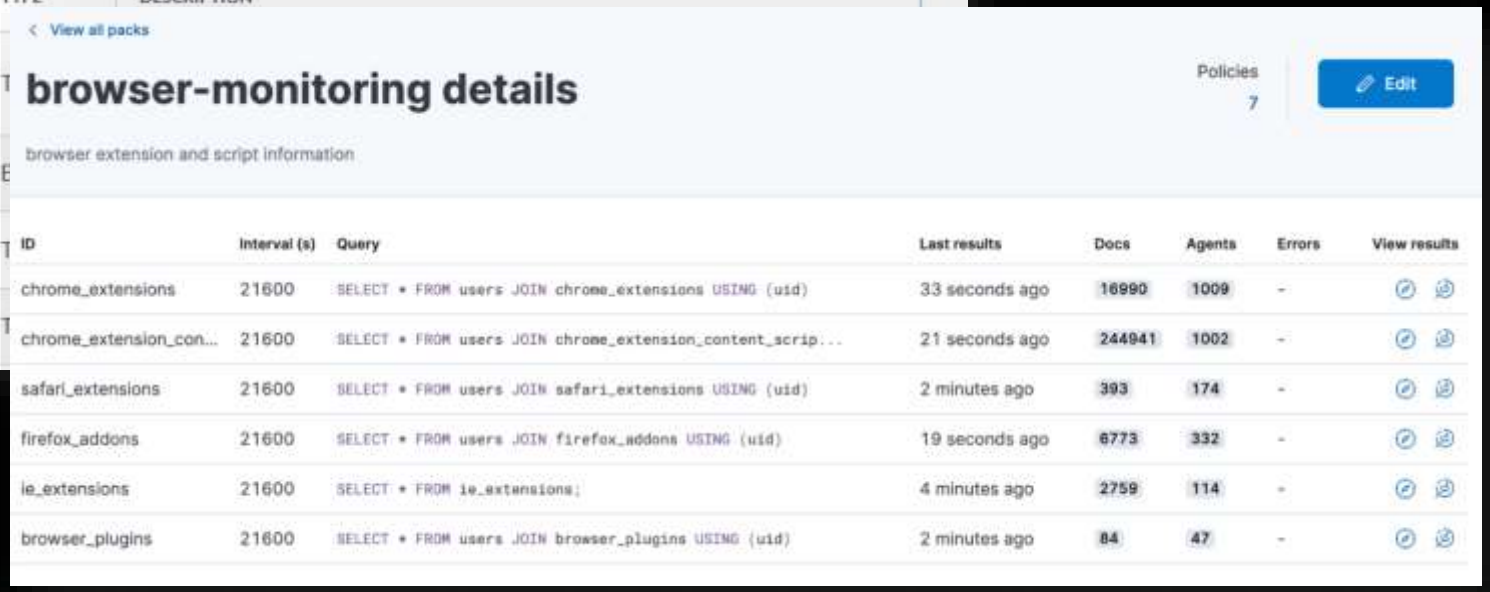
```
1   title: Chromium Browser Instance Executed With Custom Extension
2   id: 88d6e60c-759d-4ac1-a447-c0f1466c2d21
3   related:
4       - id: 27ba3207-dd30-4812-abbf-5d20c57d474e
5         type: similar
6   status: test
7   description: Detects a Chromium based browser process with the '--load-extension' flag to start a instance with a custom extension
8   references:
9       - https://redcanary.com/blog/chromeloader/
10      - https://emkc.org/s/RJjuLa
11      - https://www.mandiant.com/resources/blog/lnk-between-browsers
12  author: Aedan Russell, frack113, X__Junior (Nextron Systems)
13  date: 2022-06-19
14  modified: 2023-11-28
15  tags:
16      - attack.persistence
17      - attack.t1176
18  logsource:
19      category: process_creation
20      product: windows
21  detection:
22      selection:
23          Image|endswith:
24              - '\brave.exe'
25              - '\chrome.exe'
26              - '\msedge.exe'
27              - '\opera.exe'
28              - '\vivaldi.exe'
29          CommandLine|contains: '--load-extension='
30      condition: selection
31  falsepositives:
32      - Usage of Chrome Extensions in testing tools such as BurpSuite will trigger this alert
33  level: medium
```

# OS Query

**OS Query** for Chrome Extensions для анализа и мониторинга

**OS Query Pack** для мониторинга браузеров




https://www.elastic.co/blog/how-to-detect-malicious-browser-extensions-using-elastic
https://github.com/aarju/osquery-packs-and-dashboards/blob/main/osquery%20packs/browser_monitoring.conf

# Conclusion

Выводы  и перспективы направления

# Выводы и перспективы

- **Расширения Chrome** – удобный, но опасный инструмент. Всё упирается в фантазию атакующего!
- По сей день случаются **киберинциденты** – защищайте себя!
- Пользуйтесь **Offensive Chrome Extension Workshop** и расширяйте Pentest-арсенал

**Перспективные направления:**

- **Chrome V8 Exploitation** – захватываем ОС из расширения браузера!
- Откат к **старой версии** Google Chrome и эксплуатация 1-day CVEs
- Исследование Isolated Web App
- Больше Yandex Browser!

# Спасибо за **внимание** и попытку **понимания!**

TG: @artemy_ccrsky

ZERONIGHTS