MacOS Malware: Breaking Barriers

By Zoziel

# Whoami ?

# Whoami ?

- Bachelor's degree in Information Systems
- Postgraduate degree in Forensic Computing
- Postgraduate degree Cyber Security
- Forensic Specialist
- Incident Response Specialist
- Passionate about Malware Analysis and Development
- Fan of Music, Chaves, and Chapolin

# Contributions to the community

hackbahia

BHack
SEGURANÇA TI CONHECIMENTO

BSIDES
BSB

BSIDES
VITÓRIA

APPLE RED TEAM VILLAGE
WE HACK APPLES

bxsec
Security Conference

BSIDES
SÃO PAULO

ADINT
• Cyber Intelligence Institute •

NerdZão

BSIDES
RIO DE JANEIRO

RED TEAM VILLAGE

cajusec
SECURITY CONFERENCE

OWASP
LATAM@home

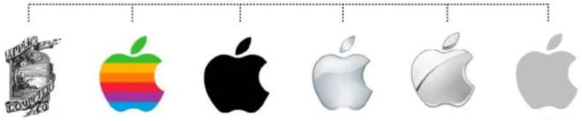
BMW
GROUP

# Topics

- Introduction to macOS and Security
- Malware Development for MacOS
- MacOS Security Barriers
- Evasion Techniques and Adaptations
- Case Study
- Conclusion and Recommendations

Introduction to macOS and Security

Version / Name	**Year**	**Highlight**
System 1.0	1984	First version of the Macintosh. Introduction of the graphical interface with a mouse. Revolution in user experience.
System 7	1991	Milestone of the classic era. Support for multitasking, color, and networking. Foundation of Macs throughout the 1990s.
Mac OS X 10.0 "Cheetah"	2001	Start of the modern era. New Unix-based foundation (NeXTSTEP), Aqua interface, and improved stability.
macOS 10.15 "Catalina"	2019	End of support for 32-bit apps. iTunes split into separate apps. Technical groundwork for the architecture transition.
macOS 11 "Big Sur"	2020	Full interface redesign. Transition from Intel to Apple Silicon (ARM/M1). New era for Macs.
macOS 26 "Tahoe"	2025 (Expected)	Continuation of the ARM era. Deep integration with iPhone, AI, and the Apple ecosystem. Vision for the future of macOS.



Gatekeeper

System Integrity Protection SIP

Sandboxing

XProtect

Firewall

Notarization

TCC
Transparancy, Consent, and Control)

# MacOS Security Features

- **Gatekeeper:** É como um porteiro que verifica apps baixados da internet. Ele só permite abrir aplicativos que sejam da App Store ou assinados por desenvolvedores confiáveis e aprovados (notarizados) pela Apple, bloqueando os suspeitos para evitar malware.

# MacOS Security Features

- **System Integrity Protection (SIP):** Protege os arquivos e partes essenciais do sistema operacional. Mesmo se você tiver privilégios de administrador (root), não pode alterar arquivos críticos do macOS, impedindo que malware modifique o sistema.

# MacOS Security Features

- **Sandboxing:** Coloca cada app em uma "caixa de areia" isolada. O aplicativo só pode acessar recursos permitidos (como seus próprios arquivos), não podendo mexer em dados de outros apps ou no sistema sem permissão, limitando danos se o app for malicioso.

# MacOS Security Features

- **XProtect:** É o antivírus embutido do macOS. Ele verifica automaticamente arquivos baixados e apps em busca de malware conhecido (usando assinaturas atualizadas pela Apple) e bloqueia ou remove ameaças sem você precisar fazer nada.

# MacOS Security Features

- **Firewall:** É uma barreira que controla o tráfego de rede. Ele bloqueia conexões indesejadas de entrada (e pode filtrar saídas), ajudando a prevenir que apps maliciosos se comuniquem com servidores remotos ou que hackers acessem seu Mac.

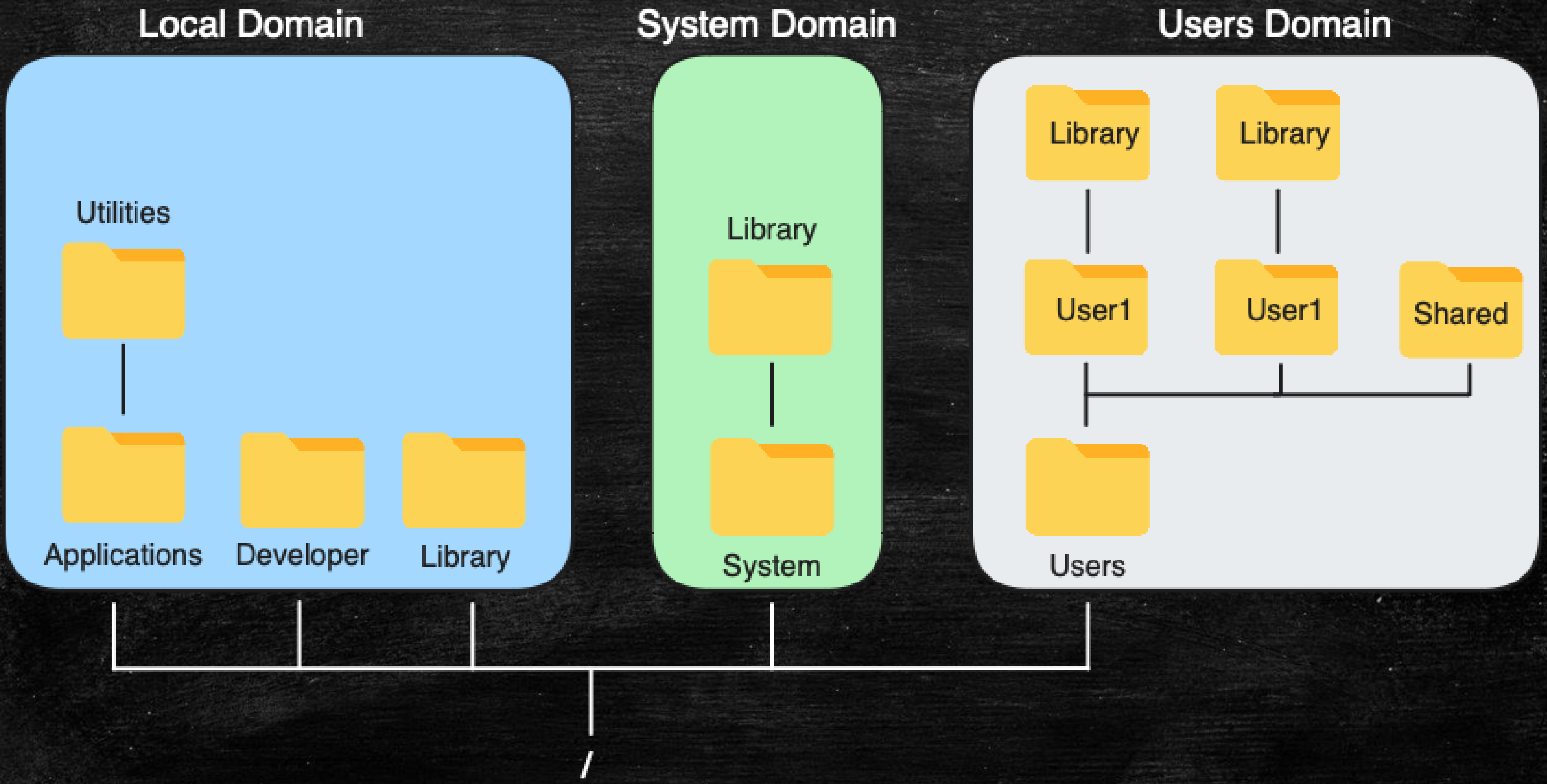
# MacOS Security Features

- **Notarization:** Processo em que desenvolvedores enviam apps para a Apple escanear em busca de malware antes de distribuí-los fora da App Store. Se aprovado, o app recebe um "selo de segurança" que o Gatekeeper verifica, garantindo que não contenha código malicioso conhecido.

# MacOS Security Features

- **TCC (Transparency, Consent, and Control):** Controla permissões de privacidade. Apps precisam pedir sua permissão explícita para acessar câmera, microfone, contatos, localização, fotos etc.

The Local MacOS file system



Malware for macOS

# Types

- Adware
- PUPs (Potentially Unwanted Programs)
- Trojans (Cavalos de Troia)
- Infostealers
- Ransomware
- Scareware/Fake Antivirus

# Types

- Backdoors e RATs
- Cryptominers
- Worms
- Vírus
- Spyware
- Macro Malware
- Downloaders/Droppers

Malware Development for MacOS

# Language choose

- Bash/Shell
- Python
- Ruby
- Perl
- Go

- C/C++
- Java
- JavaScript /Node.js
- Swift

- Rust
- PHP
- Kotlin
- Lua
- Haskell

- Scala
- Elixir
- Clojure
- Dart
- Assembly

# Choosing Python

- Native language in MacOS ✓
- Binary signed by a trusted Certificate ✗
- Run from a trusted location: ✓
  - /usr/bin/python ✓
  - /usr/local/bin/python ✓

# Persistences methods

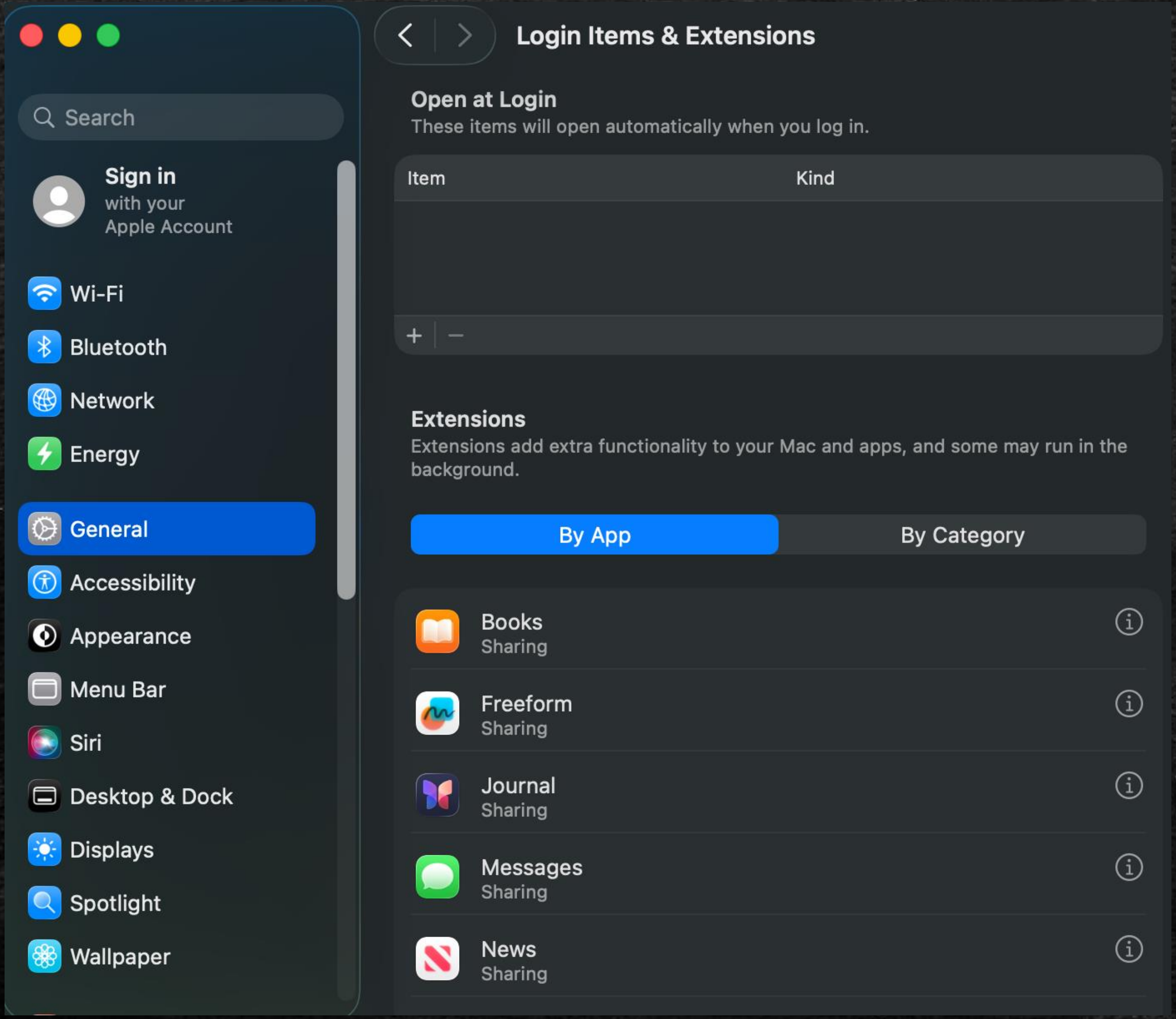
- Login Items (User LaunchD)
- Scheduled Jobs and Tasks
- Login and Logout Hooks
- Scripts
- Applications and Binary Modifications

# MacOS Launchd

Where to Look:

- **~/Library/LaunchAgents/**
- /System/Library/LaunchAgents/
- /Library/LaunchAgents/

# Login Items (User LaunchD)



Login Items & Extensions

Open at Login

These items will open automatically when you log in.

Item	Kind

Extensions

Extensions add extra functionality to your Mac and apps, and some may run in the background.

Books
Sharing

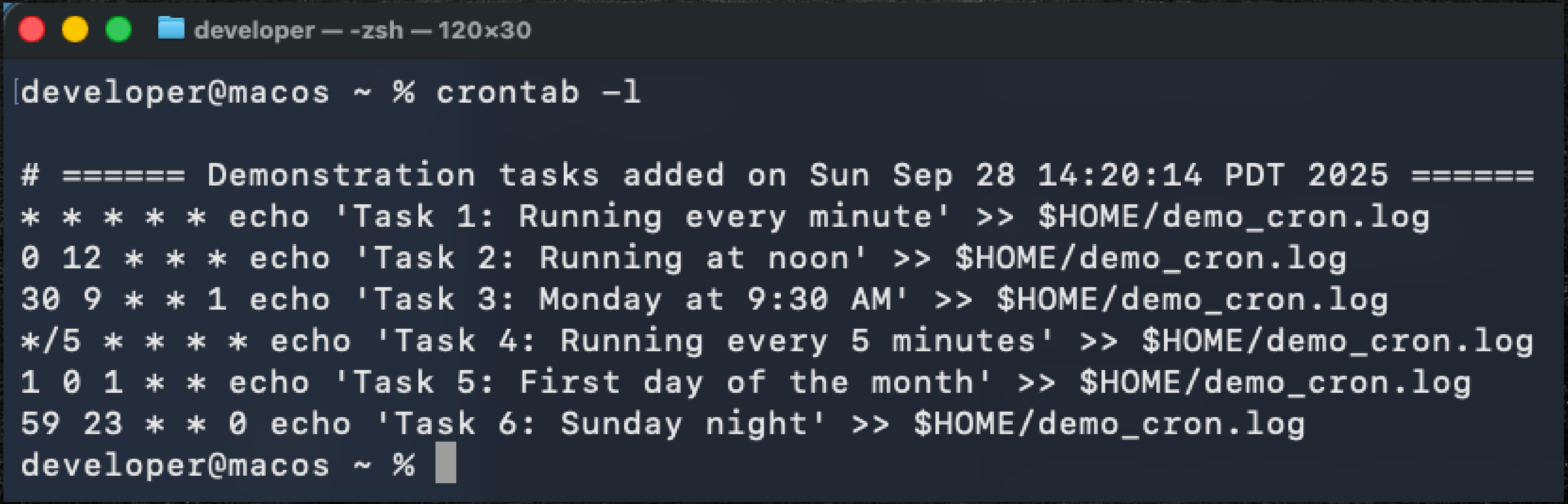
Freeform
Sharing

Journal
Sharing

Messages
Sharing

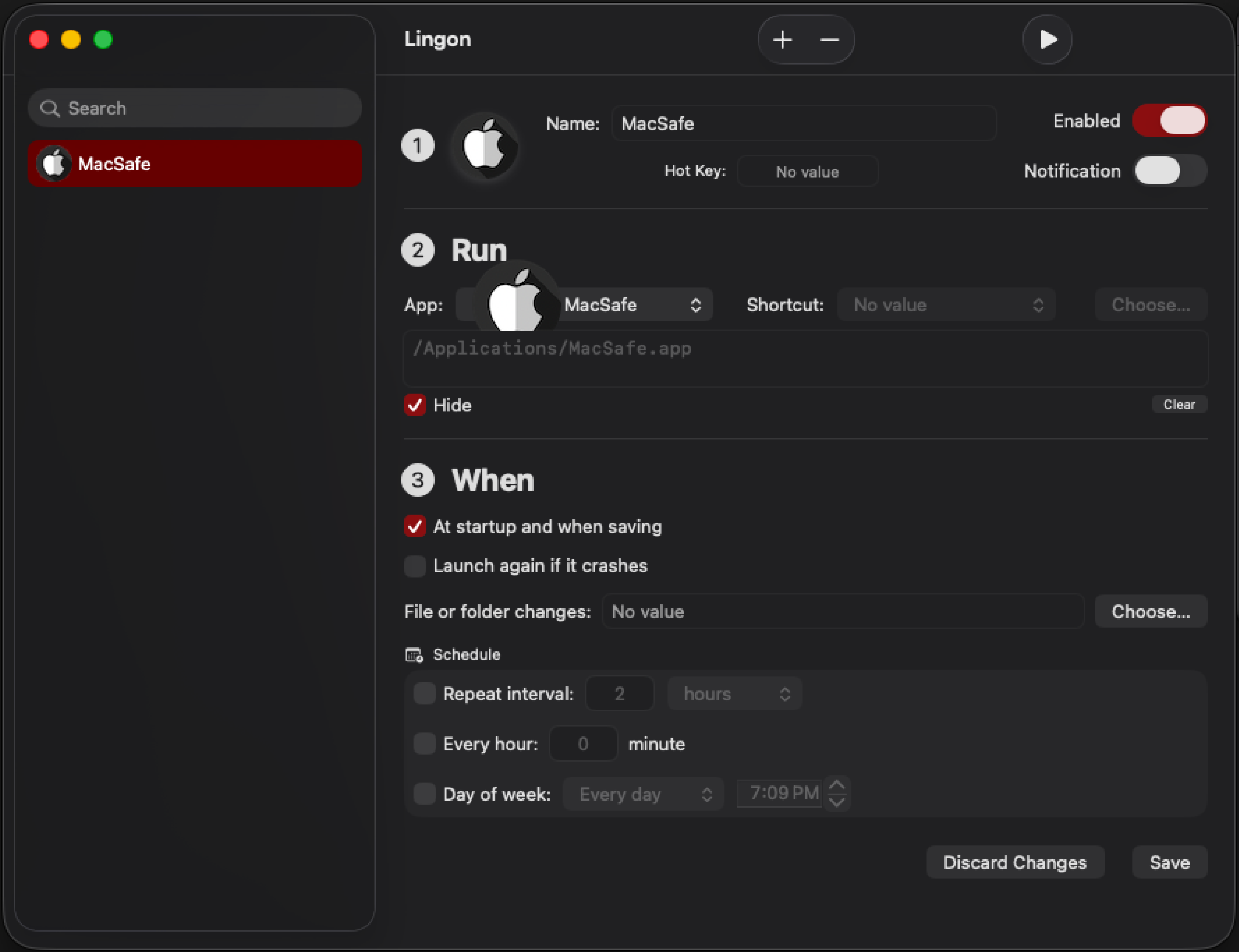
News
Sharing

# Scheduled Jobs and Tasks



```
developer@macos ~ % crontab -l

# ====== Demonstration tasks added on Sun Sep 28 14:20:14 PDT 2025 ======
* * * * * echo 'Task 1: Running every minute' >> $HOME/demo_cron.log
0 12 * * * echo 'Task 2: Running at noon' >> $HOME/demo_cron.log
30 9 * * 1 echo 'Task 3: Monday at 9:30 AM' >> $HOME/demo_cron.log
*/5 * * * * echo 'Task 4: Running every 5 minutes' >> $HOME/demo_cron.log
1 0 1 * * echo 'Task 5: First day of the month' >> $HOME/demo_cron.log
59 23 * * 0 echo 'Task 6: Sunday night' >> $HOME/demo_cron.log
developer@macos ~ %
```

# Login and Logout Hooks



Lingon

Search

MacSafe

1 Name: MacSafe

Hot Key: No value

Enabled ●

Notification ○

2 Run

App: MacSafe

Shortcut: No value

Choose...

/Applications/MacSafe.app

☑ Hide

Clear

3 When

☑ At startup and when saving

□ Launch again if it crashes

File or folder changes: No value

Choose...

Schedule

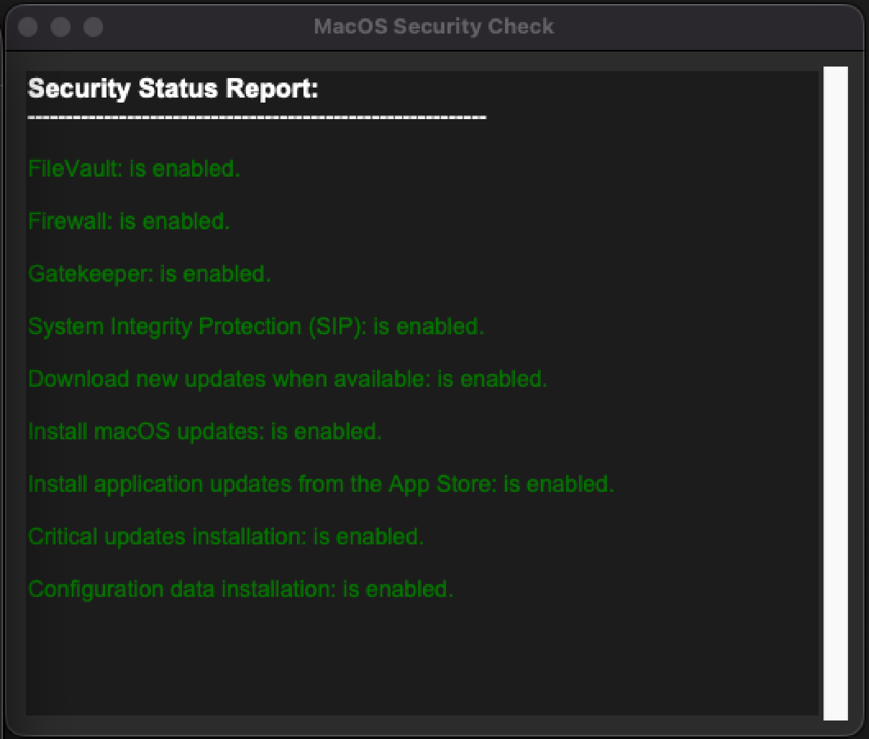
□ Repeat interval: 2 hours

□ Every hour: 0 minute

□ Day of week: Every day 7:09 PM

Discard Changes

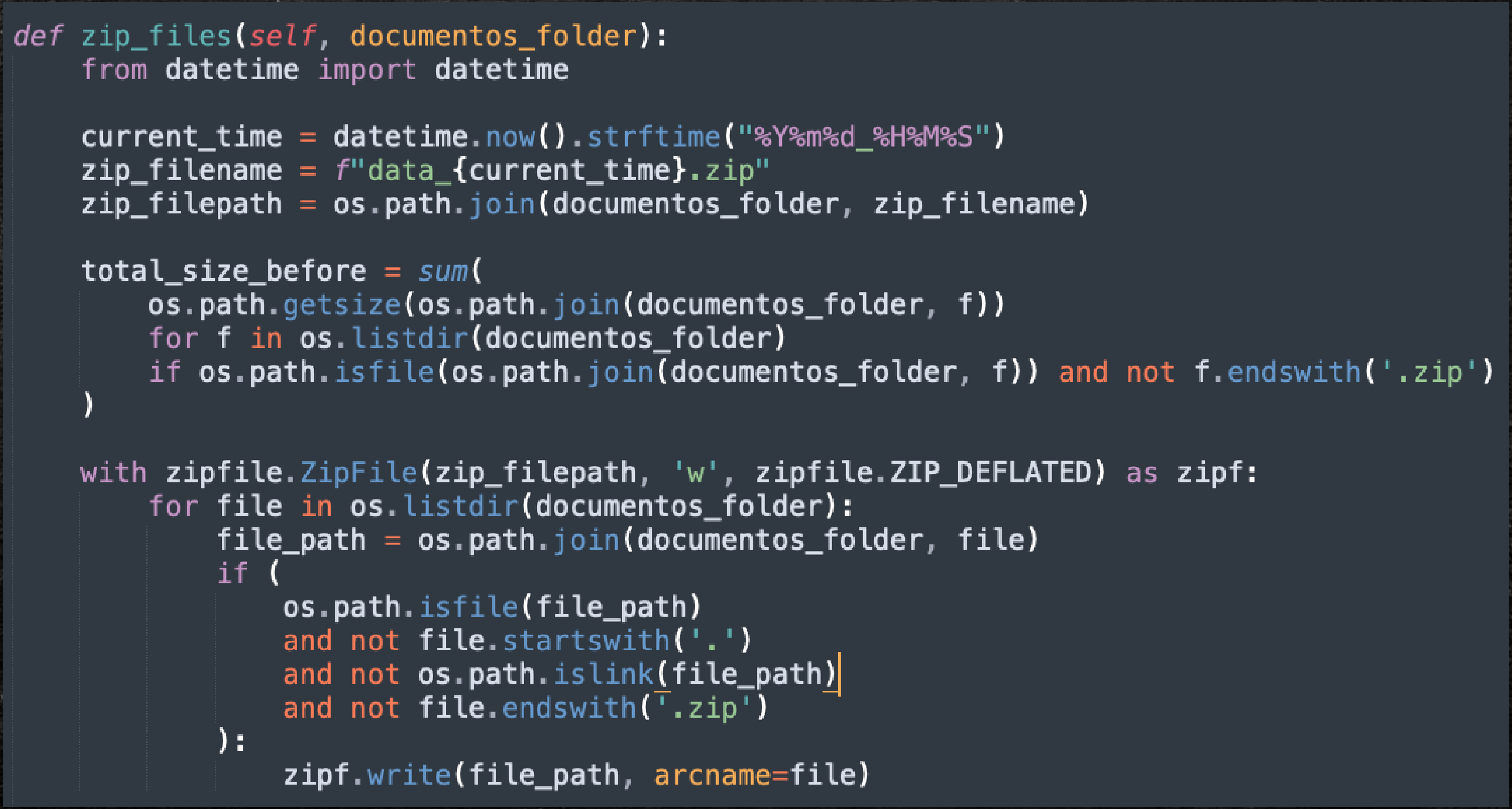
Save



MacOS Security Check

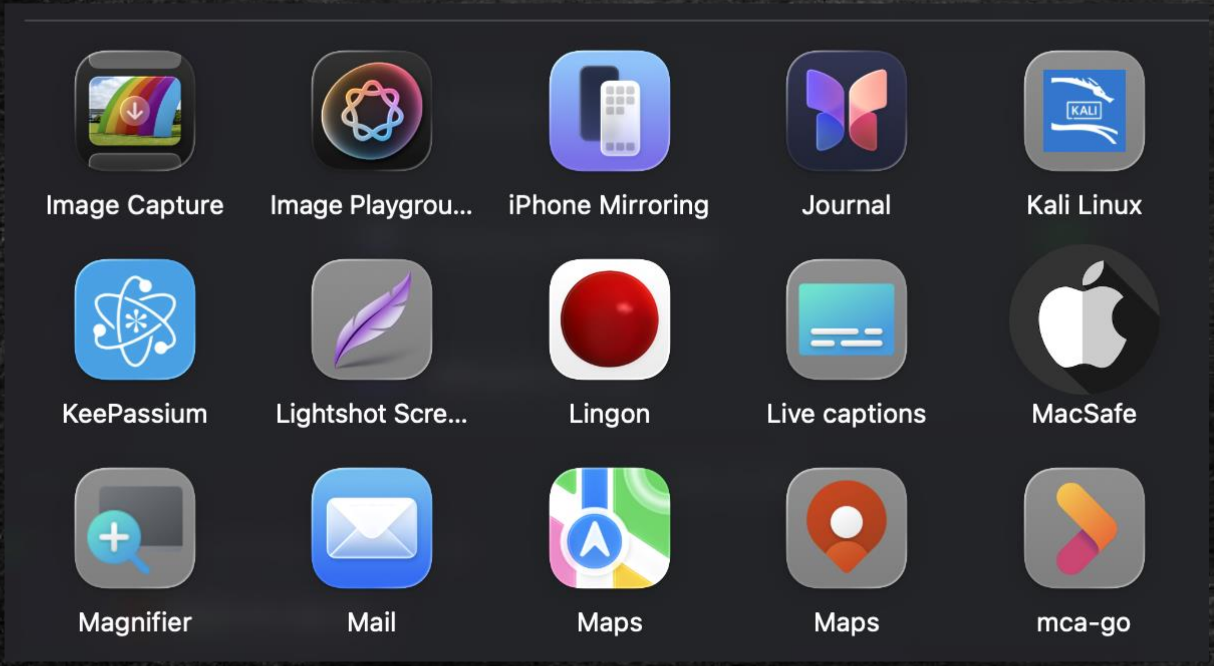
```
Security Status Report:
------------------------------------------------------------
FileVault: is enabled.
Firewall: is enabled.
Gatekeeper: is enabled.
System Integrity Protection (SIP): is enabled.
Download new updates when available: is enabled.
Install macOS updates: is enabled.
Install application updates from the App Store: is enabled.
Critical updates installation: is enabled.
Configuration data installation: is enabled.
```

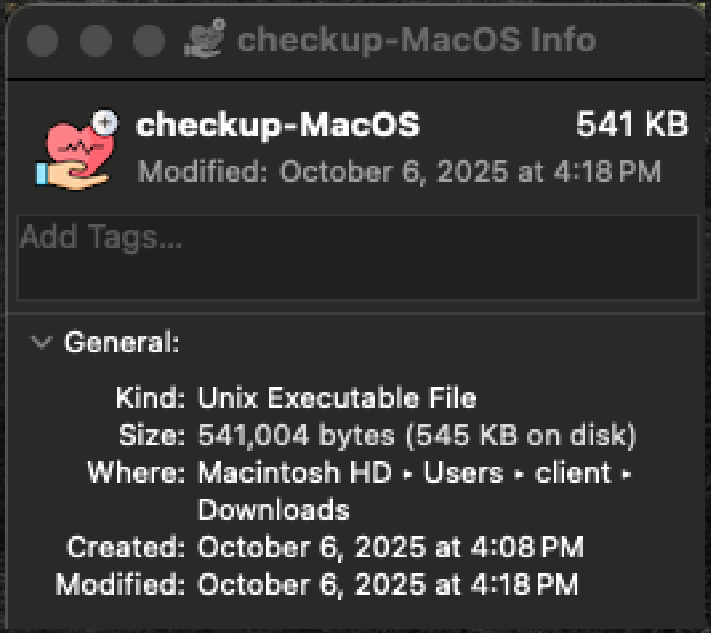
# Scripts



```python
def zip_files(self, documentos_folder):
    from datetime import datetime

    current_time = datetime.now().strftime("%Y%m%d_%H%M%S")
    zip_filename = f"data_{current_time}.zip"
    zip_filepath = os.path.join(documentos_folder, zip_filename)

    total_size_before = sum(
        os.path.getsize(os.path.join(documentos_folder, f))
        for f in os.listdir(documentos_folder)
        if os.path.isfile(os.path.join(documentos_folder, f)) and not f.endswith('.zip')
    )

    with zipfile.ZipFile(zip_filepath, 'w', zipfile.ZIP_DEFLATED) as zipf:
        for file in os.listdir(documentos_folder):
            file_path = os.path.join(documentos_folder, file)
            if (
                os.path.isfile(file_path)
                and not file.startswith('.')
                and not os.path.islink(file_path)
                and not file.endswith('.zip')
            ):
                zipf.write(file_path, arcname=file)
```

# Applications and Binary




checkup-MacOS Info

checkup-MacOS 541 KB
Modified: October 6, 2025 at 4:18 PM

Add Tags...

General:

Kind: Unix Executable File
Size: 541,004 bytes (545 KB on disk)
Where: Macintosh HD ▸ Users ▸ client ▸ Downloads
Created: October 6, 2025 at 4:08 PM
Modified: October 6, 2025 at 4:18 PM

Conclusion and Recommendations

# What do you understand first?

- System Integrity Protection (SIP)
- Gatekeeper
- XProtect
- Firewall (review rules)
- macOS, System, and App Update
- OS Weaknesses

# Material

File System
https://developer.apple.com/library/archive/documentation/FileManagement/Conceptual/FileSystemProgrammingGuide/FileSystemOverview/FileSystemOverview.html

Security
https://developer.apple.com/documentation/security

Apple Platform Security Guide
https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf

# Material

LaunchAgents
https://support.apple.com/pt-br/guide/terminal/apdc6c1077b-5d5d-4d35-9c19-60f2397b2369/mac

The Art Of Infection In MacOS
https://hadess.io/the-art-of-infection-in-macos/

Books Patrick Wardle:

The Art of Mac Malware, Volume 1: The Guide to Analyzing Malicious Software
The Art of Mac Malware, Volume 2: Detecting Malicious Software

# Lab Tools

# Lab Tools

- Parallels
  - MacOS (15 Sequoia)
  - MacOS (26 Tahoe)
- Python3
- Sublime
- PyInstaller
- Create-DMG
- Homebrew
- Xcode-select

# Questions?

Contacts

Telegram: @pun1sh3rx0
linkedin.com/in/zozielfreire

Thank you!