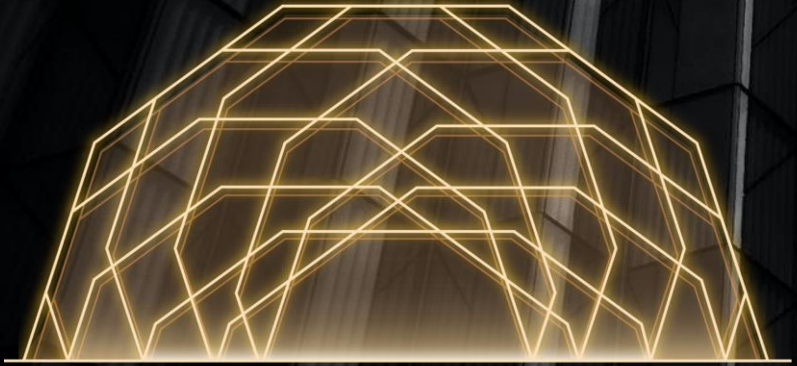
MAIS UM EVENTO Flipside

REALIZAÇÃO Green Helmet



mindthesec

10th edition

17 a 19

DE **SETEMBRO**

TRANSAMÉRICA EXPO CENTER - SP

O MAIOR E **MAIS QUALIFICADO** EVENTO DE SEGURANÇA DA INFORMAÇÃO E CYBER SECURITY DA **AMÉRICA LATINA**

Aviso Legal/ Disclaimer

As apresentações destinam-se apenas a fins educacionais e não substituem o julgamento profissional independente. As declarações de fato e opiniões aqui expressas são de total responsabilidade dos participantes e não representam a opinião ou posição do Mind The Sec ou de quaisquer outros co-patrocinadores. O Mind The Sec não endossa, aprova ou assume responsabilidade pelo conteúdo, precisão ou integridade das informações aqui apresentadas.

Os participantes devem observar que as sessões podem ser gravadas em áudio ou vídeo e podem ser publicadas em diversos meios, incluindo formatos impressos, de áudio e vídeo, sem aviso prévio adicional. O modelo de apresentação e qualquer captura de mídia estão sujeitos à proteção por direitos autorais.

The sessions are intended for educational purposes only and do not substitute for independent professional judgment. The statements of fact and opinions expressed here are the sole responsibility of the participants and do not represent the views or positions of Mind The Sec or any other co-sponsors. Mind The Sec does not endorse, approve, or assume responsibility for the content, accuracy, or integrity of the information presented here.

Participants should note that sessions may be recorded in audio or video and may be published in various media, including printed, audio, and video formats, without further notice. The presentation template and any media capture are subject to copyright protection.

Las presentaciones están destinadas únicamente con fines educativos y no sustituyen el juicio profesional independiente. Las declaraciones de hechos y opiniones expresadas aquí son responsabilidad exclusiva de los participantes y no representan la opinión o posición de Mind The Sec o de cualquier otro copatrocinador. Mind The Sec no respalda, aprueba ni asume responsabilidad por el contenido, precisión o integridad de la información presentada aquí.

Los participantes deben tener en cuenta que las sesiones pueden ser grabadas en audio o video y pueden ser publicadas en diversos medios, incluidos formatos impresos, de audio y video, sin previo aviso adicional. El modelo de presentación y cualquier grabación de medios están sujetos a protección por derechos de autor.

Threats in macOS Systems:Understanding Vulnerabilities and Risks

mindthesec
10th edition

Ricardo LOgan

CARGO: Offensive Security Manager
ricardologanbr@gmail.com

Roberto Soares

CARGO: Co-Founder Thallium Security
roberto@thalliumsecurity.com

mindthesec
10th edition

Agenda

0x01 macOS Security (Default)
0x02 macOS TCC Bypass
0x03 Electron Framework
0x04 Motivation

0x01 macOS Security (Default)

Version	Release Date
Cheetah	2001
Puma	2001
Jaguar	2002
Panther	2003
Tiger	2005
Leopard	2007
Snow Leopard	2009 **The first version of macOS I started using**
Lion	2011
Mountain Lion	2012
Mavericks	2013
Yosemite	2014
El Capitan	2015
Sierra	2016
High Sierra	2017
Mojave	2018
Catalina	2019
Big Sur	2020 **ARM/Intel**
Monterey	2021 **(Supported) + ARM/Intel**
Ventura	2022 **(Supported) + ARM/Intel**
Sonoma	2023 **(Supported) + ARM/Intel**
Sequoia	2024 **Is coming...**

SIP

Secure Boot

Xprotect

TCC

FileVault

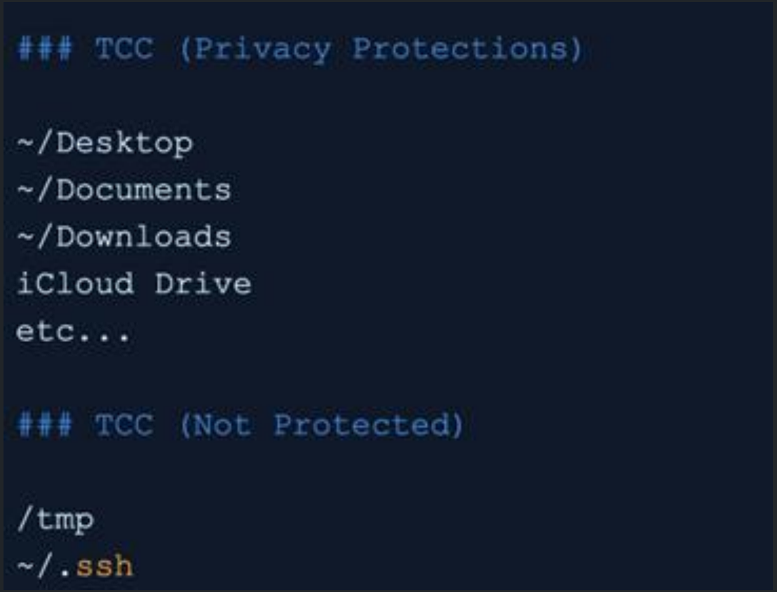
Gatekeeper

SSV

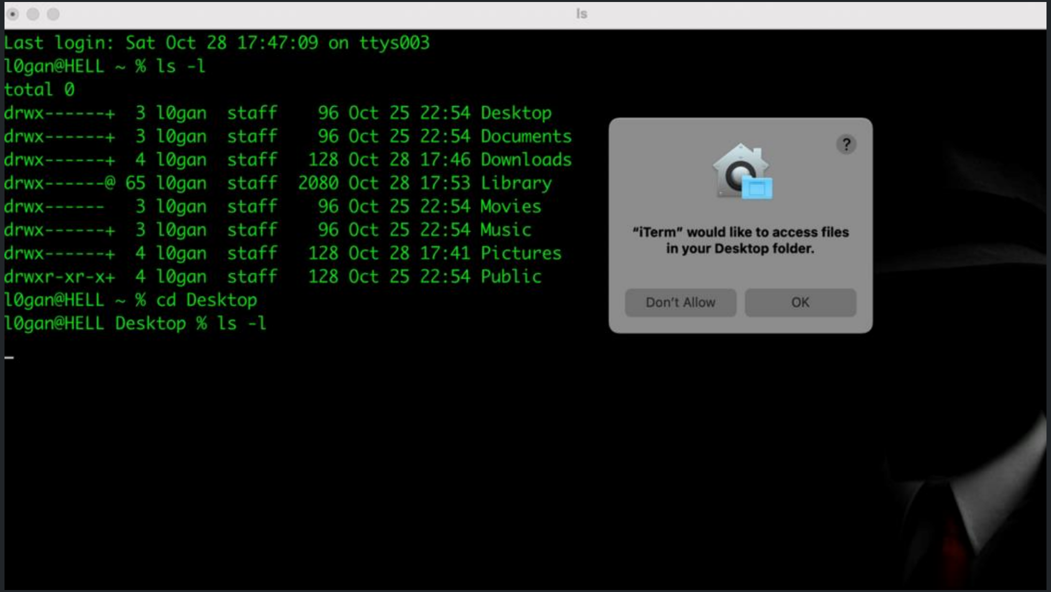
0x02 macOS TCC Bypass

TCC(Transparency, Consent and Control) – Included in macOS since version 10.11 El Capitan

A bypass in macOS TCC is dangerous because it can compromise privacy, security, and system integrity by allowing apps or process to access sensitive resources without consent.



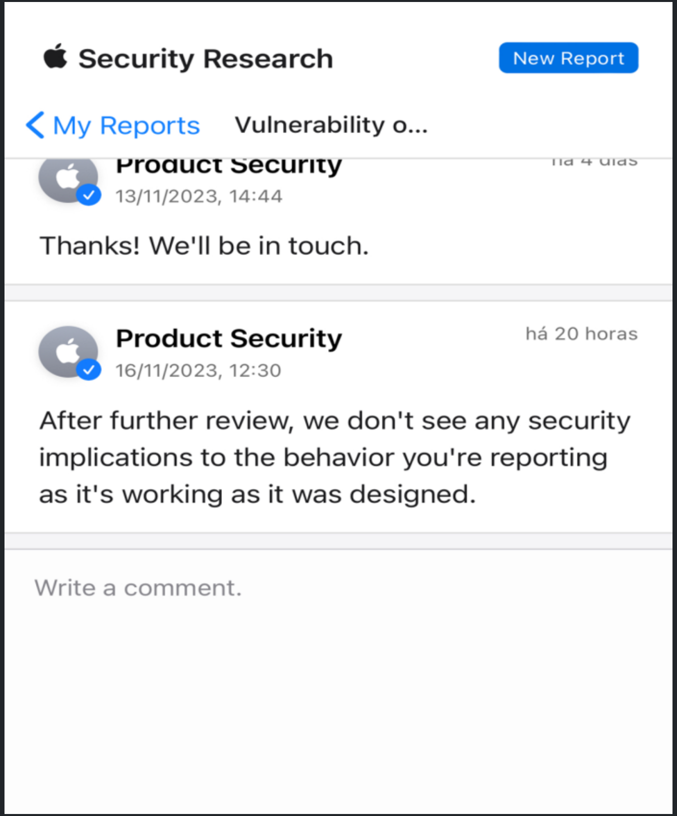
```
### TCC (Privacy Protections)

~/Desktop
~/Documents
~/Downloads
iCloud Drive
etc...

### TCC (Not Protected)

/tmp
~/.ssh
```



```
Last login: Sat Oct 28 17:47:09 on ttys003
l0gan@HELL ~ % ls -l
total 0
drwx------+  3 l0gan  staff    96 Oct 25 22:54 Desktop
drwx------+  3 l0gan  staff    96 Oct 25 22:54 Documents
drwx------+  4 l0gan  staff   128 Oct 28 17:46 Downloads
drwx------@ 65 l0gan  staff  2080 Oct 28 17:53 Library
drwx------   3 l0gan  staff    96 Oct 25 22:54 Movies
drwx------+  3 l0gan  staff    96 Oct 25 22:54 Music
drwx------+  4 l0gan  staff   128 Oct 28 17:41 Pictures
drwxr-xr-x+  4 l0gan  staff   128 Oct 25 22:54 Public
l0gan@HELL ~ % cd Desktop
l0gan@HELL Desktop % ls -l
_
```

"iTerm" would like to access files in your Desktop folder.

0x02 macOS TCC Bypass



Product Security há 4 dias
13/11/2023, 14:44

Thanks! We'll be in touch.

Product Security há 20 horas
16/11/2023, 12:30

After further review, we don't see any security implications to the behavior you're reporting as it's working as it was designed.

Write a comment.

Vulnerability found on TCC (Transparency Consent and Control)

- Access and modify of files protected by the system (TCC+ SSV+SIP).
- Bypass TCC component in macOS does not validate the use of the "open ." the command must block the access to the folder from the terminal to the finder.

Risk:

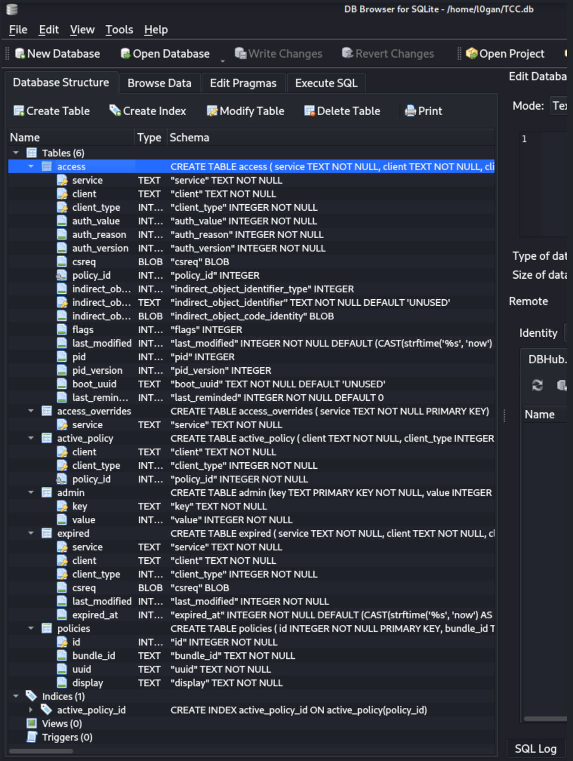
- Drop file with new TCC.db with a malicious entry to disable some security protections that could be explored by another binary (like malware).

Resolution:

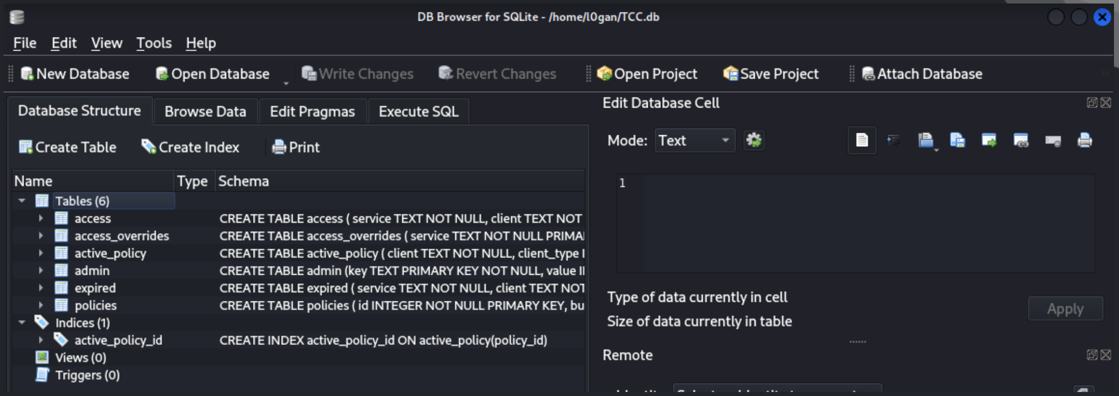
- In my opinion, TCC.db should have a flag created in the operating system based on the hardware and the operating system to ensure that it should not be possible to rewrite TCC.db by an installation generated by another machine.

mindthesec 10th edition

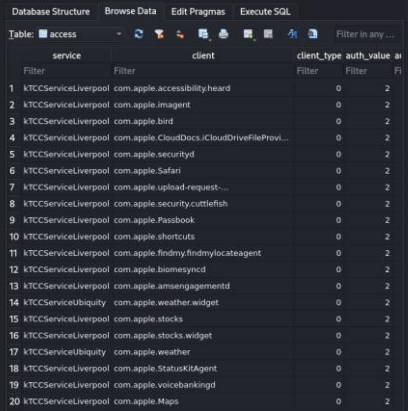
0x02 macOS TCC Bypass



Name	Type	Schema
Tables (6)		
access		CREATE TABLE access (service TEXT NOT NULL, client TEXT NOT NULL, cli
service	TEXT	"service" TEXT NOT NULL
client	TEXT	"client" TEXT NOT NULL
client_type	INT...	"client_type" INTEGER NOT NULL
auth_value	INT...	"auth_value" INTEGER NOT NULL
auth_reason	INT...	"auth_reason" INTEGER NOT NULL
auth_version	INT...	"auth_version" INTEGER NOT NULL
csreq	BLOB	"csreq" BLOB
policy_id	INT...	"policy_id" INTEGER
indirect_ob...	INT...	"indirect_object_identifier_type" INTEGER
indirect_ob...	TEXT	"indirect_object_identifier" TEXT NOT NULL DEFAULT 'UNUSED'
indirect_ob...	BLOB	"indirect_object_code_identity" BLOB
flags	INT...	"flags" INTEGER
last_modified	INT...	"last_modified" INTEGER NOT NULL DEFAULT (CAST(strftime('%s', 'now')
pid	INT...	"pid" INTEGER
pid_version	INT...	"pid_version" INTEGER
boot_uuid	TEXT	"boot_uuid" TEXT NOT NULL DEFAULT 'UNUSED'
last_remin...	INT...	"last_reminded" INTEGER NOT NULL DEFAULT 0
access_overrides		CREATE TABLE access_overrides (service TEXT NOT NULL PRIMARY KEY)
service	TEXT	"service" TEXT NOT NULL
active_policy		CREATE TABLE active_policy (client TEXT NOT NULL, client_type INTEGER
client	TEXT	"client" TEXT NOT NULL
client_type	INT...	"client_type" INTEGER NOT NULL
policy_id	INT...	"policy_id" INTEGER NOT NULL
admin		CREATE TABLE admin (key TEXT PRIMARY KEY NOT NULL, value INTEGER
key	TEXT	"key" TEXT NOT NULL
value	INT...	"value" INTEGER NOT NULL
expired		CREATE TABLE expired (service TEXT NOT NULL, client TEXT NOT NULL, cl
service	TEXT	"service" TEXT NOT NULL
client	TEXT	"client" TEXT NOT NULL
client_type	INT...	"client_type" INTEGER NOT NULL
csreq	BLOB	"csreq" BLOB
last_modified	INT...	"last_modified" INTEGER NOT NULL
expired_at	INT...	"expired_at" INTEGER NOT NULL DEFAULT (CAST(strftime('%s', 'now') AS
policies		CREATE TABLE policies (id INTEGER NOT NULL PRIMARY KEY, bundle_id T
id	INT...	"id" INTEGER NOT NULL
bundle_id	TEXT	"bundle_id" TEXT NOT NULL
uuid	TEXT	"uuid" TEXT NOT NULL
display	TEXT	"display" TEXT NOT NULL
Indices (1)		
active_policy_id		CREATE INDEX active_policy_id ON active_policy(policy_id)
Views (0)		
Triggers (0)		

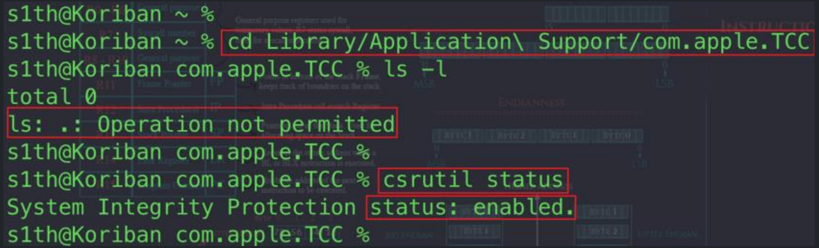


Name	Type	Schema
Tables (6)		
access		CREATE TABLE access (service TEXT NOT NULL, client TEXT NOT
access_overrides		CREATE TABLE access_overrides (service TEXT NOT NULL PRIMA
active_policy		CREATE TABLE active_policy (client TEXT NOT NULL, client_type I
admin		CREATE TABLE admin (key TEXT PRIMARY KEY NOT NULL, value II
expired		CREATE TABLE expired (service TEXT NOT NULL, client TEXT NOT
policies		CREATE TABLE policies (id INTEGER NOT NULL PRIMARY KEY, bu
Indices (1)		
active_policy_id		CREATE INDEX active_policy_id ON active_policy(policy_id)
Views (0)		
Triggers (0)		

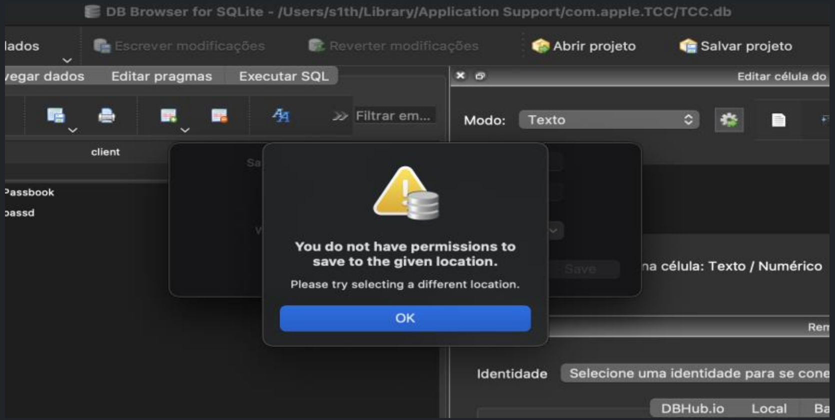


	service	client	client_type	auth_value	a
	Filter	Filter	Filter	Filter	Fi
1	kTCCServiceLiverpool	com.apple.accessibility.heard	0	2	
2	kTCCServiceLiverpool	com.apple.imagent	0	2	
3	kTCCServiceLiverpool	com.apple.bird	0	2	
4	kTCCServiceLiverpool	com.apple.CloudDocs.iCloudDriveFileProvi...	0	2	
5	kTCCServiceLiverpool	com.apple.securityd	0	2	
6	kTCCServiceLiverpool	com.apple.Safari	0	2	
7	kTCCServiceLiverpool	com.apple.upload-request-...	0	2	
8	kTCCServiceLiverpool	com.apple.security.cuttlefish	0	2	
9	kTCCServiceLiverpool	com.apple.Passbook	0	2	
10	kTCCServiceLiverpool	com.apple.shortcuts	0	2	
11	kTCCServiceLiverpool	com.apple.findmy.findmylocateagent	0	2	
12	kTCCServiceLiverpool	com.apple.biomesyncd	0	2	
13	kTCCServiceLiverpool	com.apple.amsengagementd	0	2	
14	kTCCServiceUbiquity	com.apple.weather.widget	0	2	
15	kTCCServiceLiverpool	com.apple.stocks	0	2	
16	kTCCServiceLiverpool	com.apple.stocks.widget	0	2	
17	kTCCServiceUbiquity	com.apple.weather	0	2	
18	kTCCServiceLiverpool	com.apple.StatusKitAgent	0	2	
19	kTCCServiceLiverpool	com.apple.voicebankingd	0	2	
20	kTCCServiceLiverpool	com.apple.Maps	0	2	

0x02 macOS TCC Bypass



```
s1th@Koriban ~ %
s1th@Koriban ~ % cd Library/Application\ Support/com.apple.TCC
s1th@Koriban com.apple.TCC % ls -l
total 0
ls: .: Operation not permitted
s1th@Koriban com.apple.TCC %
s1th@Koriban com.apple.TCC % csrutil status
System Integrity Protection status: enabled.
s1th@Koriban com.apple.TCC %
```



DB Browser for SQLite - /Users/s1th/Library/Application Support/com.apple.TCC/TCC.db

Modo: Texto

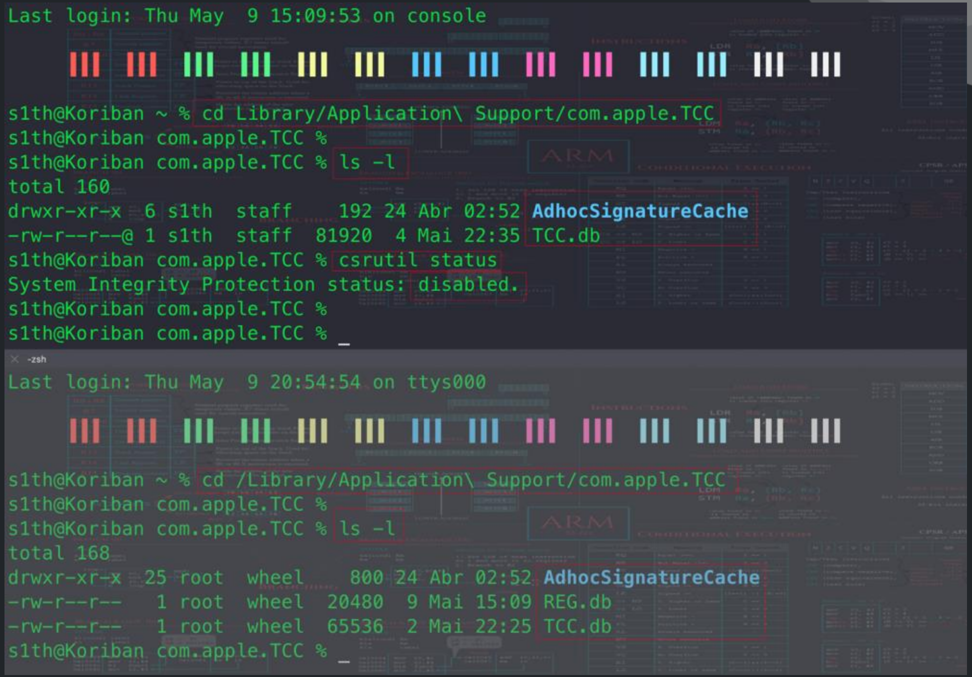
na célula: Texto / Numérico

Identidade: Selecione uma identidade para se cone

You do not have permissions to save to the given location.

Please try selecting a different location.

OK



```
Last login: Thu May  9 15:09:53 on console

s1th@Koriban ~ % cd Library/Application\ Support/com.apple.TCC
s1th@Koriban com.apple.TCC %
s1th@Koriban com.apple.TCC % ls -l
total 160
drwxr-xr-x  6 s1th  staff    192 24 Abr 02:52 AdhocSignatureCache
-rw-r--r--@ 1 s1th  staff  81920  4 Mai 22:35 TCC.db
s1th@Koriban com.apple.TCC % csrutil status
System Integrity Protection status: disabled.
s1th@Koriban com.apple.TCC %
s1th@Koriban com.apple.TCC % _
```

-zsh

```
Last login: Thu May  9 20:54:54 on ttys000

s1th@Koriban ~ % cd /Library/Application\ Support/com.apple.TCC
s1th@Koriban com.apple.TCC %
s1th@Koriban com.apple.TCC % ls -l
total 168
drwxr-xr-x  25 root  wheel    800 24 Abr 02:52 AdhocSignatureCache
-rw-r--r--   1 root  wheel  20480  9 Mai 15:09 REG.db
-rw-r--r--   1 root  wheel  65536  2 Mai 22:25 TCC.db
s1th@Koriban com.apple.TCC % _
```

mindthesec
10th edition

0x02 macOS TCC Bypass

POC ->

Bypass

Replace the TCC.db file located in a protected folder:~/Library/Application Support/com.apple.TCC with a new modified TCC.db.

Automator is an application developed by Apple Inc. for macOS, which can be used to automate repetitive tasks through point-and-click or drag and drop. Automator enables the repetition of tasks across a wide variety of programs, including Finder, Safari, Calendar, Contacts and others.

0x03 Electron Framework

Cross-platform framework used to create desktop applications using web technologies like HTML, CSS, and JavaScript. Allowing developers to build applications for macOS, Windows, and Linux with a single codebase.

?

0x03 Electron Framework

Cross-platform framework used to create desktop applications using web technologies like HTML, CSS, and JavaScript. Allowing developers to build applications for macOS, Windows, and Linux with a single codebase.

slack

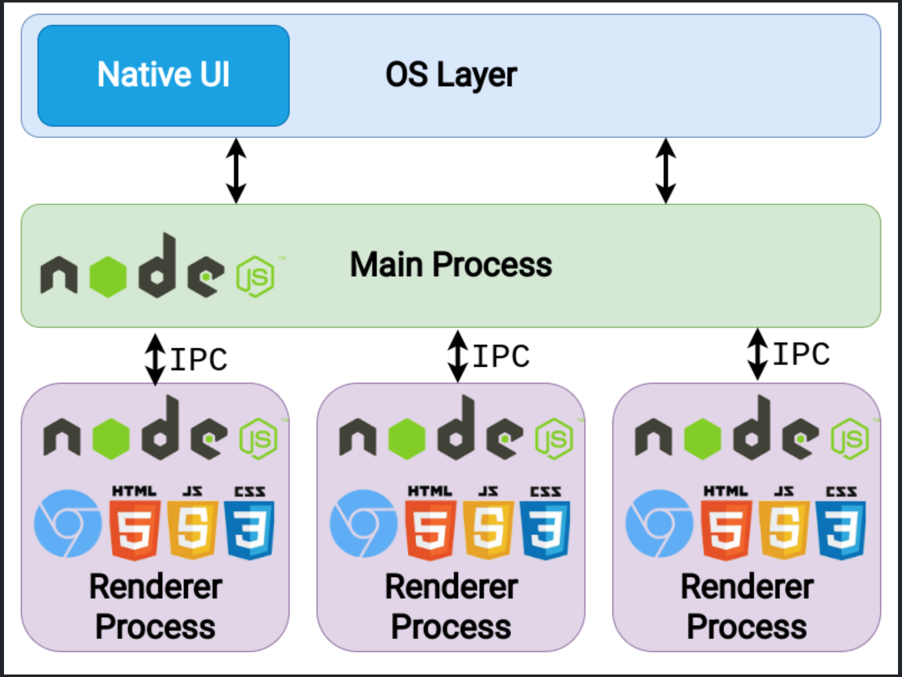
GitHub

Visual Studio

DISCORD

https://www.electronjs.org/apps

0x03 Electron Framework



https://miro.medium.com/v2/resize:fit:1400/1*5G9BFD2ItXo6lv2pinEJrA.png

0x03 Electron Framework

How do I find out if I have an application written in Electron installed?

Take a look at the Frameworks directory if it contains the Electron directory:

```
/Applications/<app name>/Contents/Frameworks/
```

Or, use the npx tool:

```
npx @electron/fuses read --app /Applications/app_name.app
```

0x03 Electron Framework

They are "magic bits" in the Electron binary that can be flipped when packaging your Electron app.

- RunAsNode
- EnableCookieEncryption
- EnableNodeOptionsEnvironmentVariable
- EnableNodeCliInspectArguments
- EnableEmbeddedAsarIntegrityValidation
- OnlyLoadAppFromAsar
- LoadBrowserProcessSpecificV8Snapshot
- GrantFileProtocolsExtraPrivileges

0x03 Electron Framework

Pass the --inspect parameter to the application executable

A debugger will be started on port 9229 (default)

Use websocket to communicate with the application

You can use Chrome to inspect

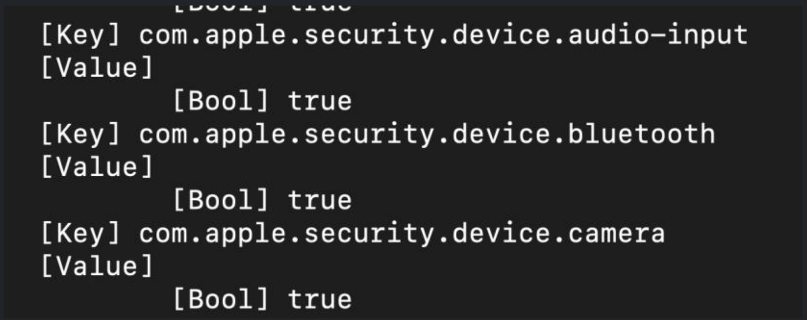
0x03 Electron Framework

Check the Entitlements

An entitlement is a right or privilege that grants an executable particular capabilities

Tool

codesign -dvv --entitlement - /Applications/<app>/Contents/MacOS/executable



```
        [Bool] true
[Key] com.apple.security.device.audio-input
[Value]
        [Bool] true
[Key] com.apple.security.device.bluetooth
[Value]
        [Bool] true
[Key] com.apple.security.device.camera
[Value]
        [Bool] true
```

0x03 Electron Framework

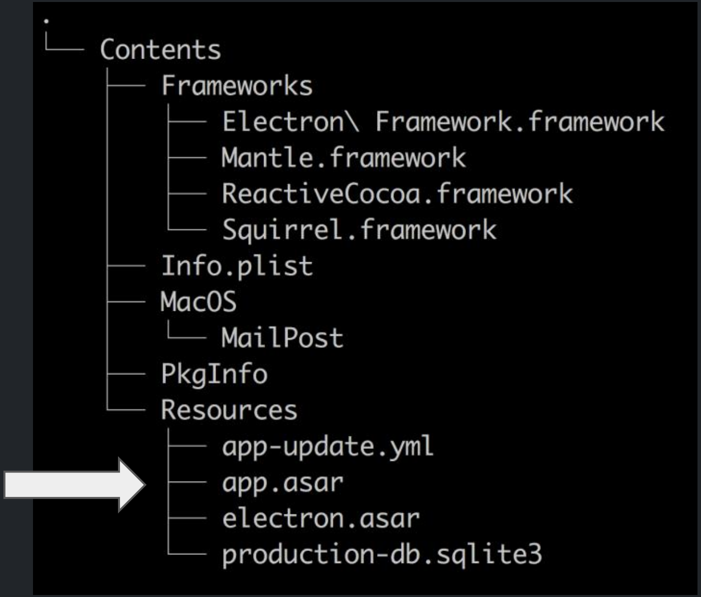
Persistence refers to the technique used by attackers to maintain their access to a system across reboots and other disruptions.

The application's code, including all JavaScript, HTML, and CSS files, is often packaged into an app.asar archive.

The app.asar archive is typically not protected, making it an easy target for modification.

Path:

/Applications/App.app/Contents/Resources/app.asar



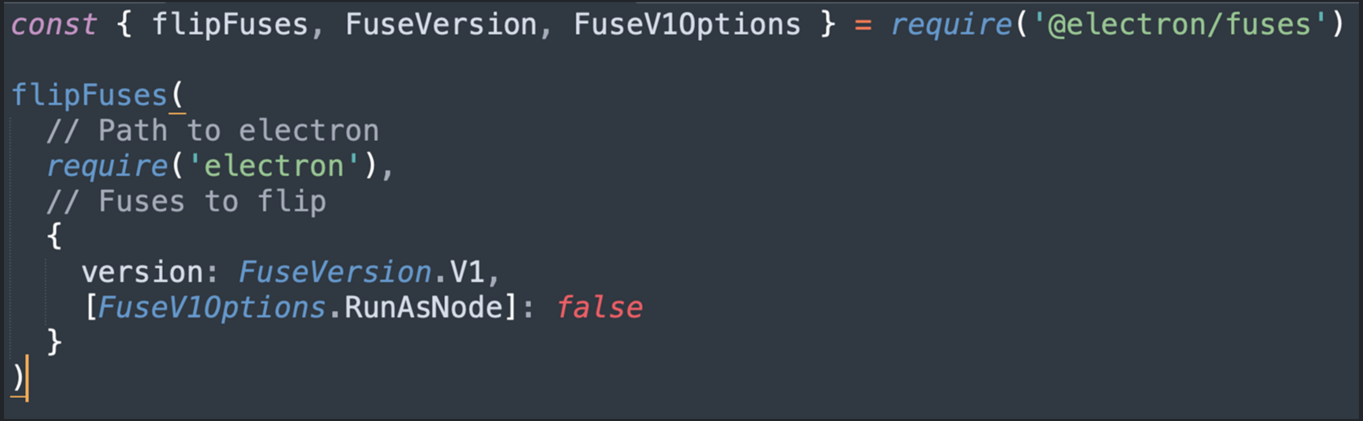
```
.
└── Contents
    ├── Frameworks
    │   ├── Electron\ Framework.framework
    │   ├── Mantle.framework
    │   ├── ReactiveCocoa.framework
    │   └── Squirrel.framework
    ├── Info.plist
    ├── MacOS
    │   └── MailPost
    ├── PkgInfo
    └── Resources
        ├── app-update.yml
        ├── app.asar
        ├── electron.asar
        └── production-db.sqlite3
```

0x03 Electron Framework

6 CVE's (not published yet)
$ 4.800~ in bug bounties

The tools will be released on github: https://github.com/espreto/

0x03 Electron Framework



```
const { flipFuses, FuseVersion, FuseV1Options } = require('@electron/fuses')

flipFuses(
  // Path to electron
  require('electron'),
  // Fuses to flip
  {
    version: FuseVersion.V1,
    [FuseV1Options.RunAsNode]: false
  }
)
```

https://github.com/electron/electron/blob/main/docs/tutorial/security.md

Conclusion

- Are your SOC and Blue Team monitoring and protecting the company from attacks?
- Are the controls really effectives and well implemented?
- Are your systems updated and with last security patches?
- Do you make security tests (Pentest) recurrent in your macOS endpoints?
- Do you have a well oriented team or update service with the last published vulnerabilities?

"A motivated attacker achieves his goal regardless of time"

#Attackium
Research Group Focus on Apple Devices

https://discord.gg/tSpGtcUHVJ

mindthesec

10th edition

obrigado!

mindthesec.com.br

Ricardo Amaral (L0gan)
ricardologanbr@gmail.com
in /l0gan

Roberto Soares (Espreto)
roberto@thalliumsecurity.com
in /espreto

MAIS UM EVENTO Flipside REALIZAÇÃO Green Helmet

mindthesec
10th edition

O MAIOR E **MAIS QUALIFICADO** EVENTO DE SEGURANÇA DA INFORMAÇÃO E CYBER SECURITY DA **AMÉRICA LATINA**