macOS Red Teaming on Corporate Scenarios

SPEAKER:

Ricardo L0gan

Agenda

About Me:

Security Specialist with extensive experience in enterprise networks and enthusiastic on malware research, pentest and reverse engineering. I have been focused in the last years in research for vulnerability and malware for macOS environment.

I am part of the staff for some security conferences organizations such as H2HC (Hackers to Hackers Conference), BsidesSP and SlackShow/Slackzine Community.

Brazil

Agenda

0x00 Motivation of Research
0x01 macOS Security (Default / Corp)
0x02 macOS TCC Bypass
0x03 Conclusion
0x04 Reference

0x00 Motivation of Research

Empire Transfer 2024

RustDoor 2024

MetaStealer 2024

Lockbit 2023

CriptoMiner 2023

Silver Sparrow 2021

OSX/Linker 2019

Mac Auto Fixer 2018

LoundMiner 2019

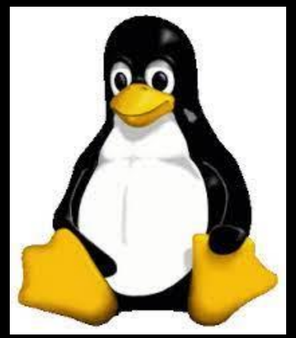
Crossrider (OSX/Shalyer) 2018

OSX/MaMi 2018

Others….

0x00 Motivation of Research

Is one of them safer?



Windows

macOS®

?

0x01 macOS Security (Default / Corp)

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

FileVault

Xprotect

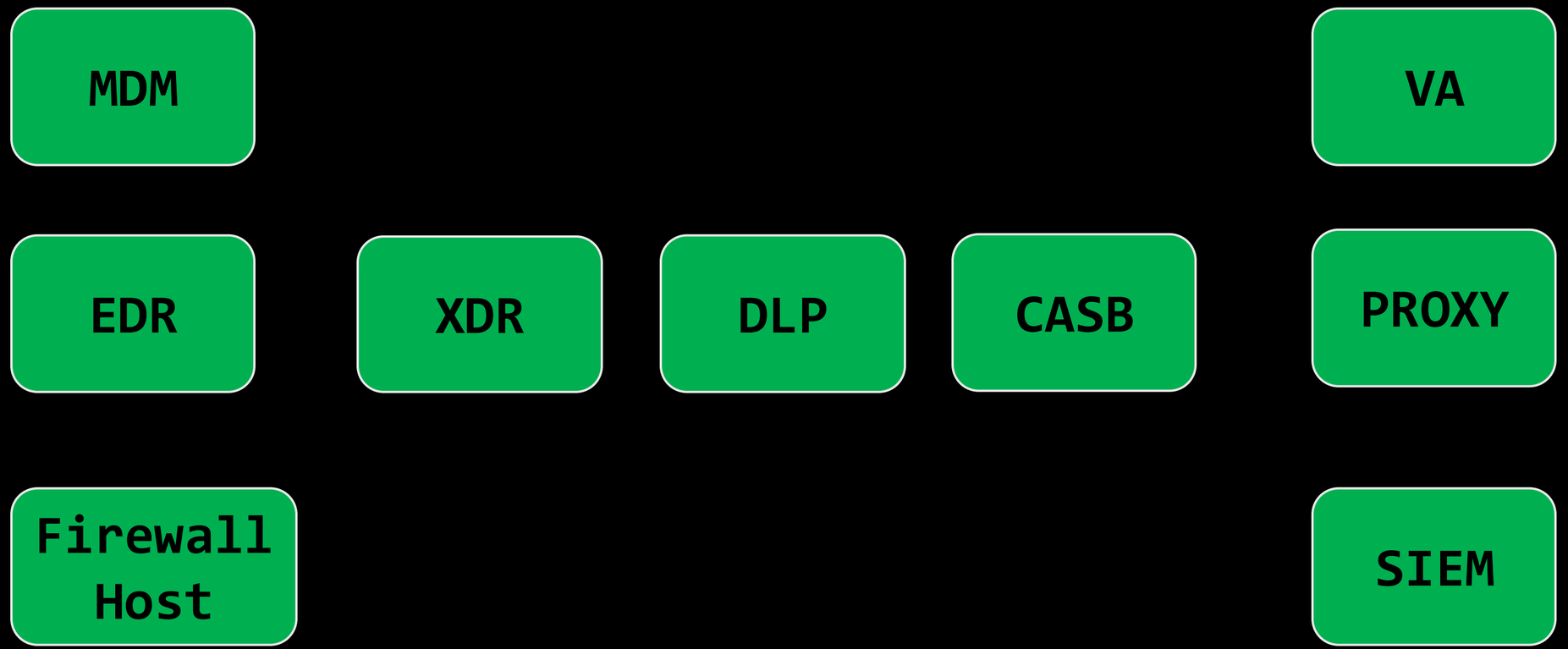
Secure Boot

Gatekeeper

TCC

SSV

0x01 macOS Security (Default / Corp)



And now?

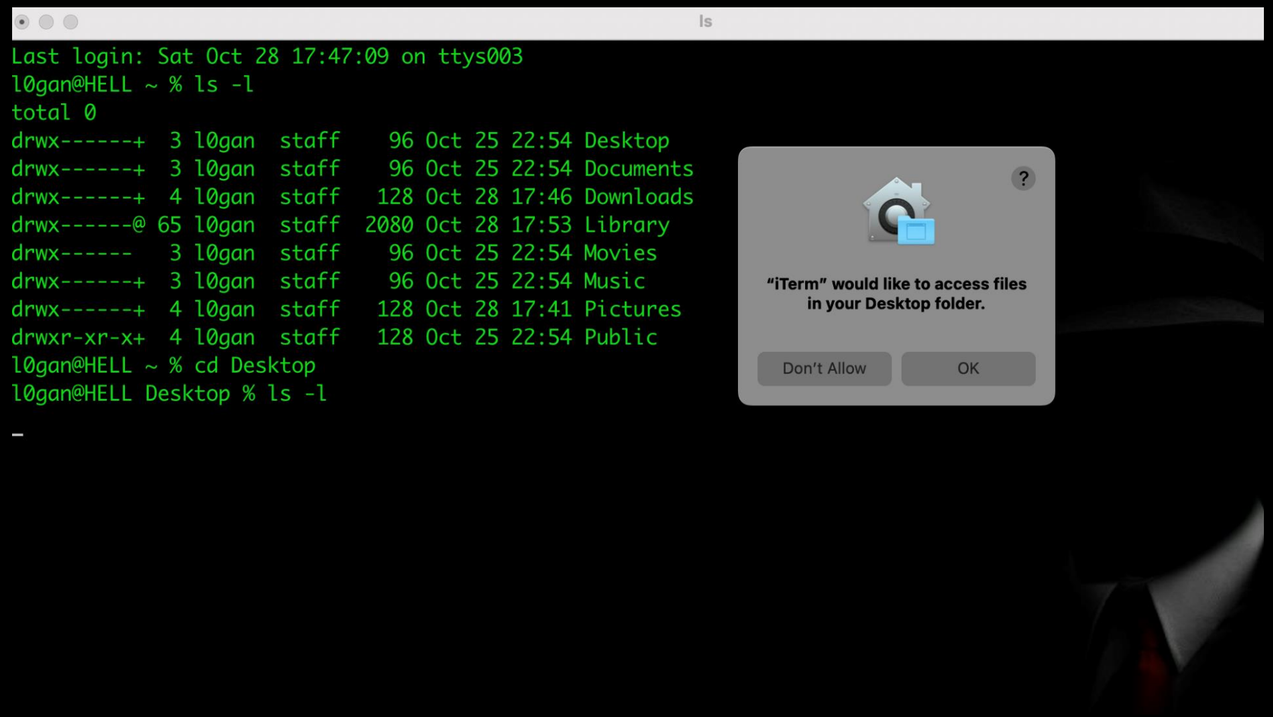
Where should I go?

0x02 macOS TCC Bypass

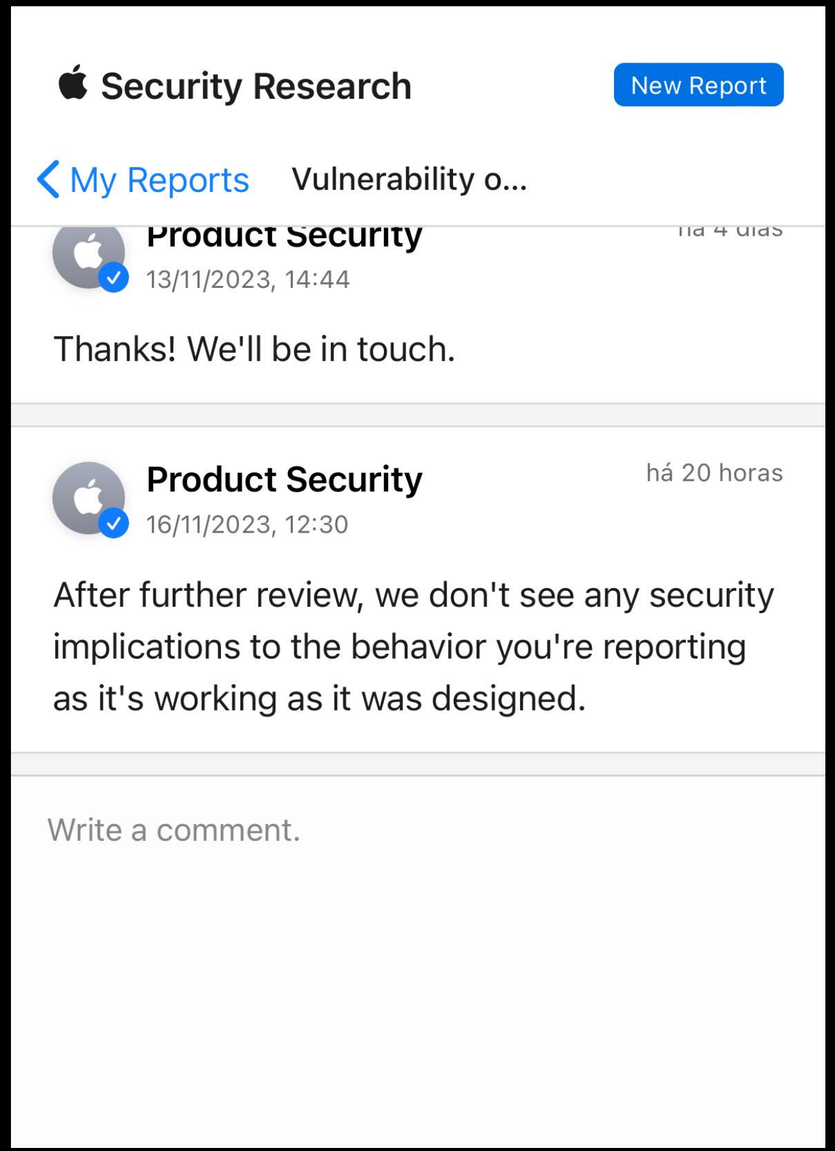
TCC(Transparency, Consent and Control) – Included in macOS since version 10.11 El Capitan

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
```



0x02 macOS TCC Bypass



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.

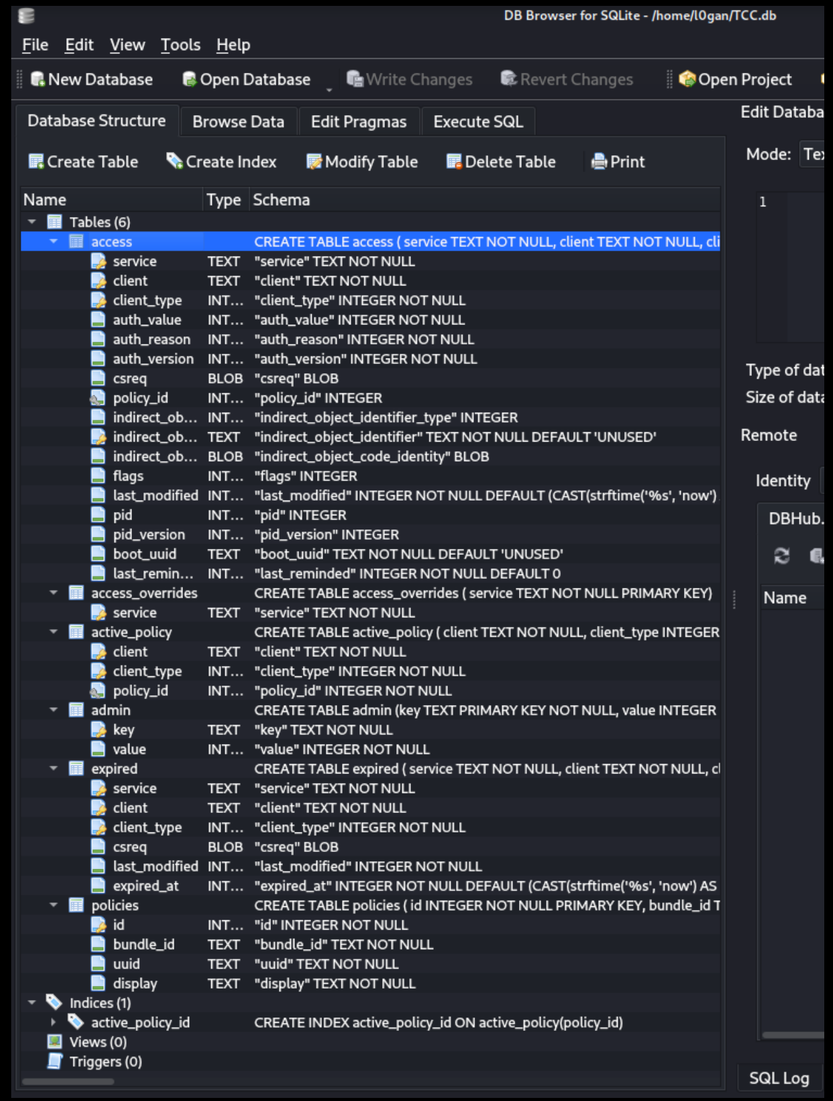
Risk:

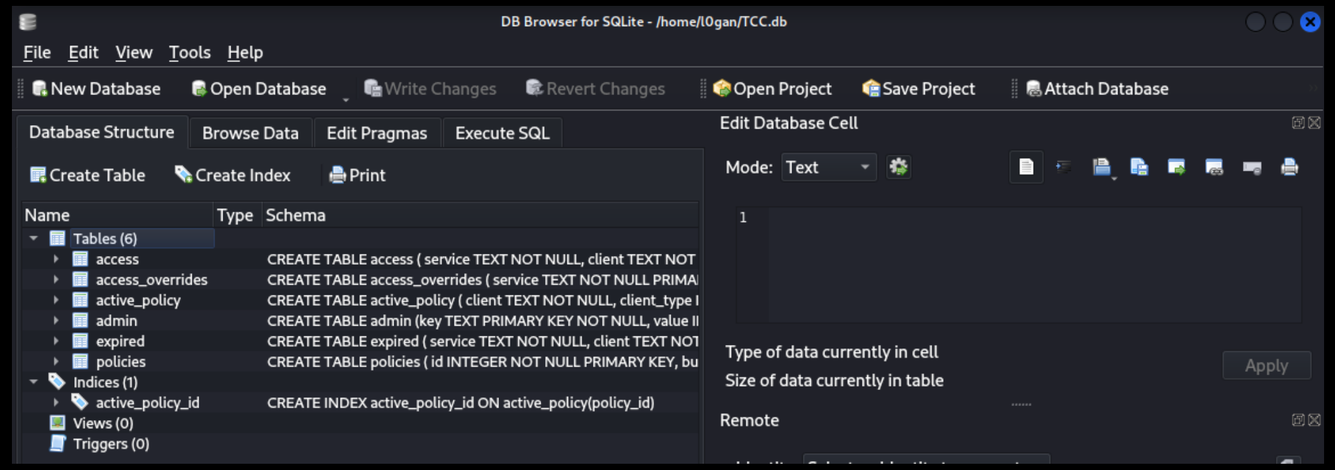
Drop file with new TCC.db with a malicious entry to disable some security protections that could be explored by another binary (like malware).

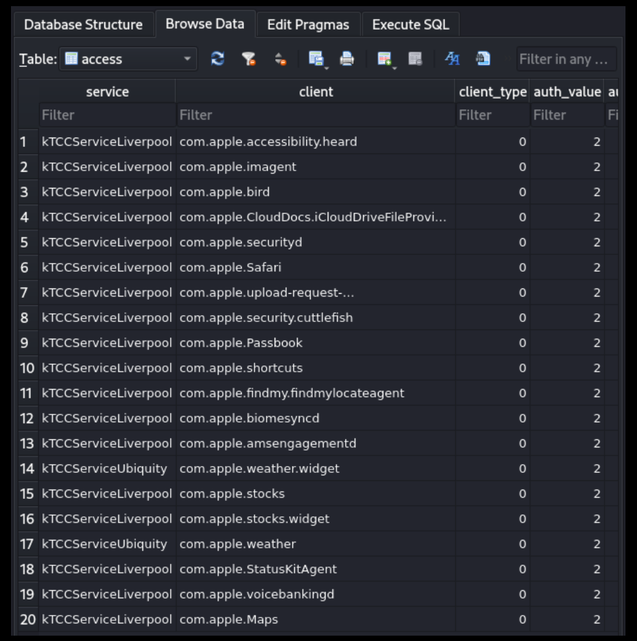
Resolution:

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.

0x02 macOS TCC Bypass

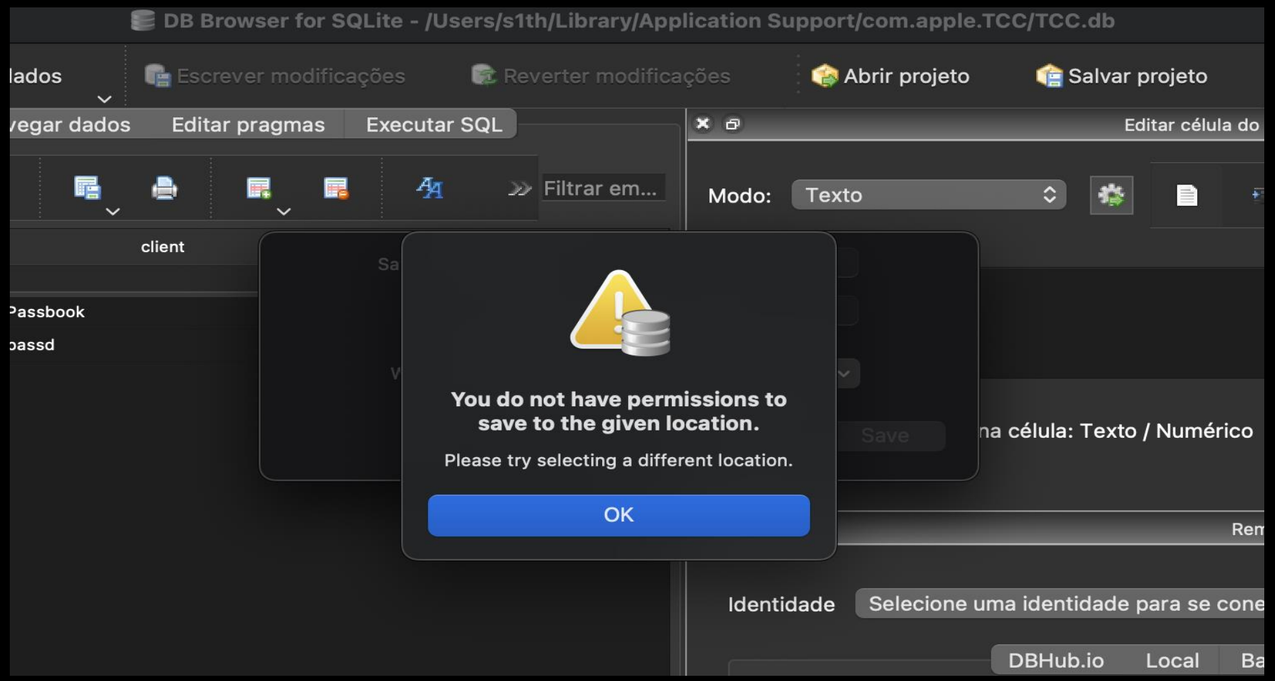






0x02 macOS TCC Bypass

```
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 %
```




```
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 % _
```

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 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/her goals regardless of time"

0x04 Reference

Hacking is a way of life

macOS Red Teaming on Corporate Scenarios (Defcon 2024)
https://github.com/loganbr/Presentations/blob/main/2024%20-%20Defcon%20Red%20Team%20Village.pdf

My First Publication of this research (Nullbyte 2019)
https://github.com/loganbr/Presentations/blob/main/2019%20-%20Nullbyte%20-%20macOS%20Hacking%20Tricks.pdf

Research about malwares (mach-o files) for macOS(H2HC 2016)
https://github.com/loganbr/Presentations/blob/main/2016%20-%20H2HC%20-%20R3v3rs1ng%20on%20Mach-O%20File%20%20Version%200.pdf

Cedric Owens - Gone Apple Pickin: Red Teaming MacOS Environments in 2021
https://www.youtube.com/watch?v=IiMladUbL6E&t=93s

Objective-See / Objective ByTheSea
https://objective-see.org
https://objectivebythesea.org

Research Group Focus on Apple Devices #Attackium

https://discord.gg/tSpGtcUHVJ

Thanks a Lot

Any Questions ?

ricardologanbr@gmail.com
Twitter: @l0ganbr