From Offensive to Defensive Security

Through Three Practical Case Studies

Les Assises 2022

Guillaume VALADON - @guedou

Quarkslab

Bonjour Les Assises!

- Head Of QLab R&D
  previously at ANSSI & Legrand/Netatmo
- First time at Les Assises
  a regular at technical conferences
- Scapy co-maintainer
  Python-based packet manipulation tool

scapy

https://github.com/secdev/scapy

Quarkslab

https://www.quarkslab.com

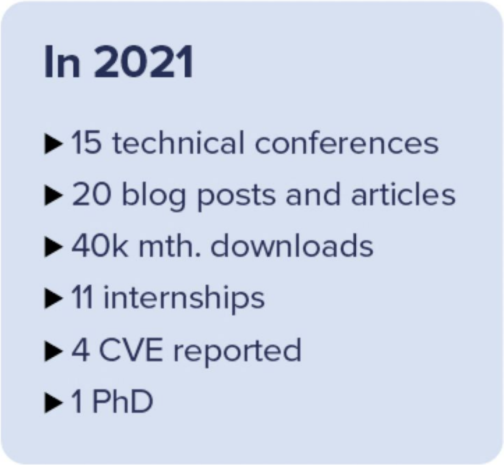
- *“be a leader in vulnerability research”*

  by relying on a high level of expertise

- motto declined according to two axes

  improve security systems

  develop new tools



In 2021

- ▶ 15 technical conferences
- ▶ 20 blog posts and articles
- ▶ 40k mth. downloads
- ▶ 11 internships
- ▶ 4 CVE reported
- ▶ 1 PhD

#1 - Improve Security Systems

...... investigate facts

1. study systems
2. report vulnerabilities
3. publish results

#2 - Develop New Tools

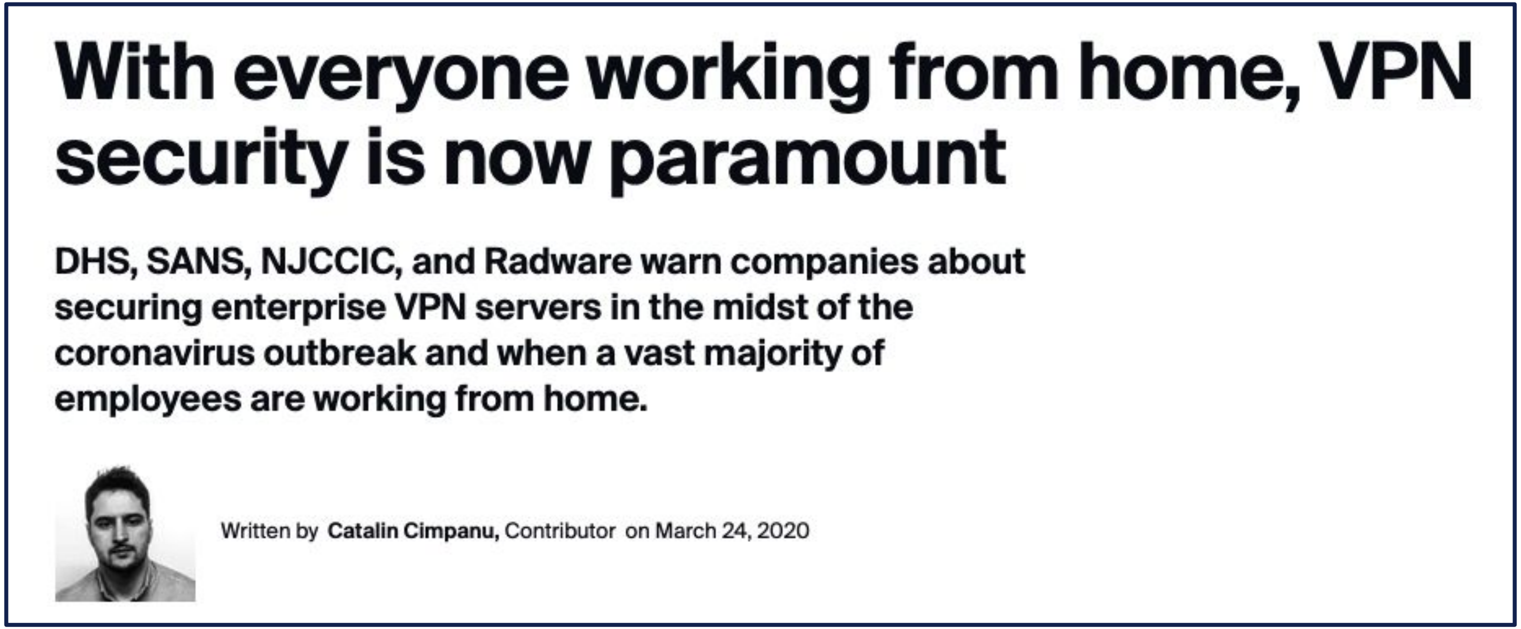
What is a Vulnerability?

- weakness not anticipated by designers

  any complex system is potentially vulnerable

- discovered it can be exploited

  crash, data theft, privilege escalation…

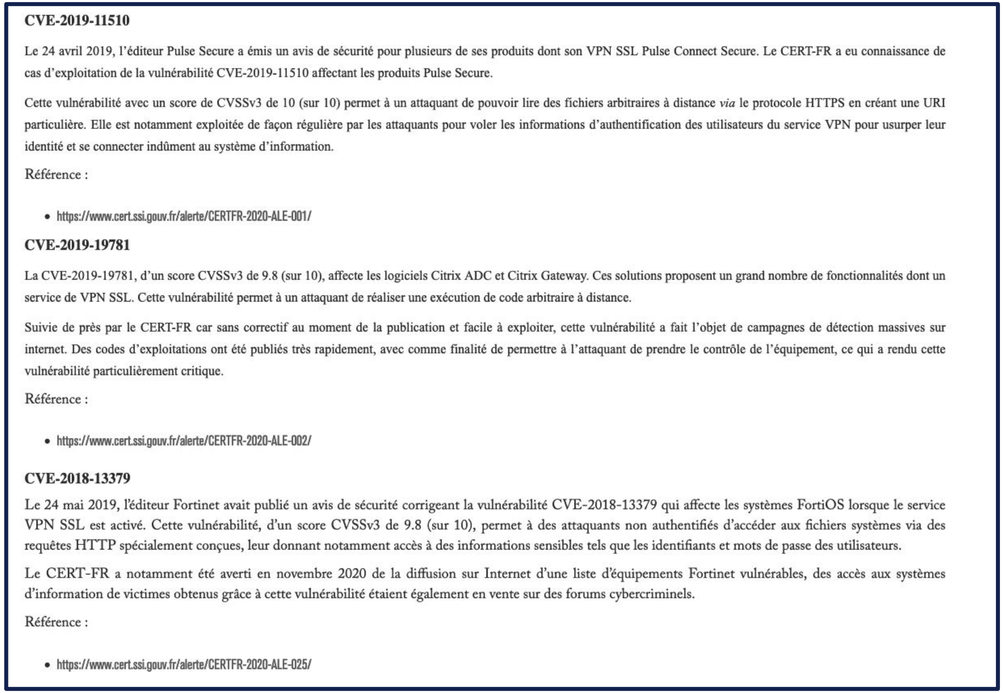


With everyone working from home, VPN security is now paramount

DHS, SANS, NJCCIC, and Radware warn companies about securing enterprise VPN servers in the midst of the coronavirus outbreak and when a vast majority of employees are working from home.

Written by **Catalin Cimpanu,** Contributor on March 24, 2020

https://www.zdnet.com/article/covid-19-with-everyone-working-from-home-vpn-security-has-now-become-paramount/



CVE-2019-11510

Le 24 avril 2019, l'éditeur Pulse Secure a émis un avis de sécurité pour plusieurs de ses produits dont son VPN SSL Pulse Connect Secure. Le CERT-FR a eu connaissance de cas d'exploitation de la vulnérabilité CVE-2019-11510 affectant les produits Pulse Secure.

Cette vulnérabilité avec un score de CVSSv3 de 10 (sur 10) permet à un attaquant de pouvoir lire des fichiers arbitraires à distance *via* le protocole HTTPS en créant une URI particulière. Elle est notamment exploitée de façon régulière par les attaquants pour voler les informations d'authentification des utilisateurs du service VPN pour usurper leur identité et se connecter indûment au système d'information.

Référence :

- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-001/

CVE-2019-19781

La CVE-2019-19781, d'un score CVSSv3 de 9.8 (sur 10), affecte les logiciels Citrix ADC et Citrix Gateway. Ces solutions proposent un grand nombre de fonctionnalités dont un service de VPN SSL. Cette vulnérabilité permet à un attaquant de réaliser une exécution de code arbitraire à distance.

Suivie de près par le CERT-FR car sans correctif au moment de la publication et facile à exploiter, cette vulnérabilité a fait l'objet de campagnes de détection massives sur internet. Des codes d'exploitations ont été publiés très rapidement, avec comme finalité de permettre à l'attaquant de prendre le contrôle de l'équipement, ce qui a rendu cette vulnérabilité particulièrement critique.

Référence :

- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-002/

CVE-2018-13379

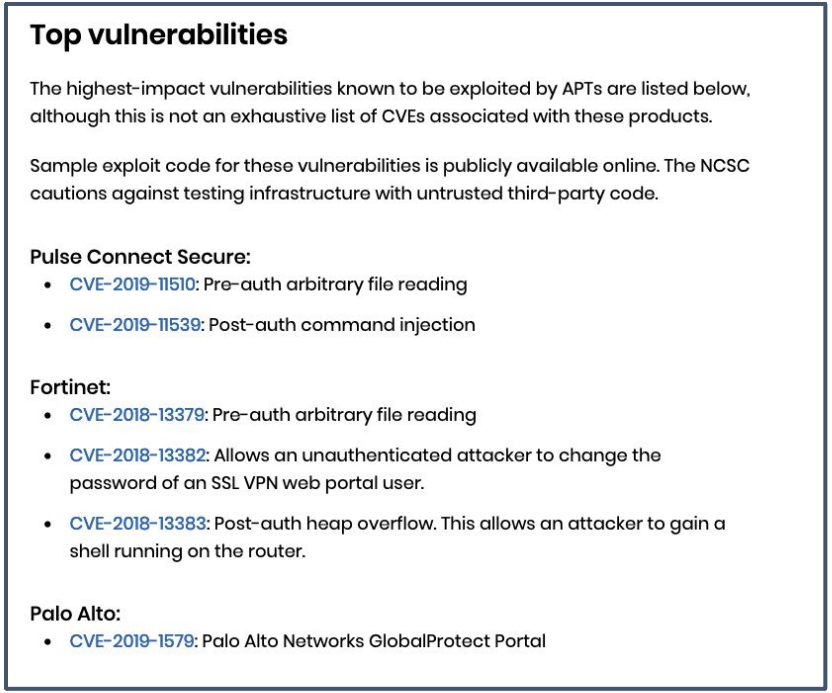
Le 24 mai 2019, l'éditeur Fortinet avait publié un avis de sécurité corrigeant la vulnérabilité CVE-2018-13379 qui affecte les systèmes FortiOS lorsque le service VPN SSL est activé. Cette vulnérabilité, d'un score CVSSv3 de 9.8 (sur 10), permet à des attaquants non authentifiés d'accéder aux fichiers systèmes via des requêtes HTTP spécialement conçues, leur donnant notamment accès à des informations sensibles tels que les identifiants et mots de passe des utilisateurs.

Le CERT-FR a notamment été averti en novembre 2020 de la diffusion sur Internet d'une liste d'équipements Fortinet vulnérables, des accès aux systèmes d'information de victimes obtenus grâce à cette vulnérabilité étaient également en vente sur des forums cybercriminels.

Référence :

- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-025/

https://www.cert.ssi.gouv.fr/actualite/CERTFR-2021-ACT-008/



Top vulnerabilities

The highest-impact vulnerabilities known to be exploited by APTs are listed below, although this is not an exhaustive list of CVEs associated with these products.

Sample exploit code for these vulnerabilities is publicly available online. The NCSC cautions against testing infrastructure with untrusted third-party code.

Pulse Connect Secure:

- CVE-2019-11510: Pre-auth arbitrary file reading
- CVE-2019-11539: Post-auth command injection

Fortinet:

- CVE-2018-13379: Pre-auth arbitrary file reading
- CVE-2018-13382: Allows an unauthenticated attacker to change the password of an SSL VPN web portal user.
- CVE-2018-13383: Post-auth heap overflow. This allows an attacker to gain a shell running on the router.

Palo Alto:

- CVE-2019-1579: Palo Alto Networks GlobalProtect Portal

https://www.cisa.gov/uscert/ncas/alerts/aa22-117a

Offensive Security?

Quarkslab

- a tool among many

  BCP, network architectures, redteam, risk analysis…

- behave as an attacker

  time, budget and scope constraints
  business knowledge
  greybox

Quarkslab Mindset

- disassembly

  take ownership of a system

- reassembly

  exploit weaknesses

- improvement

  share findings

Quarkslab + Lego = <3

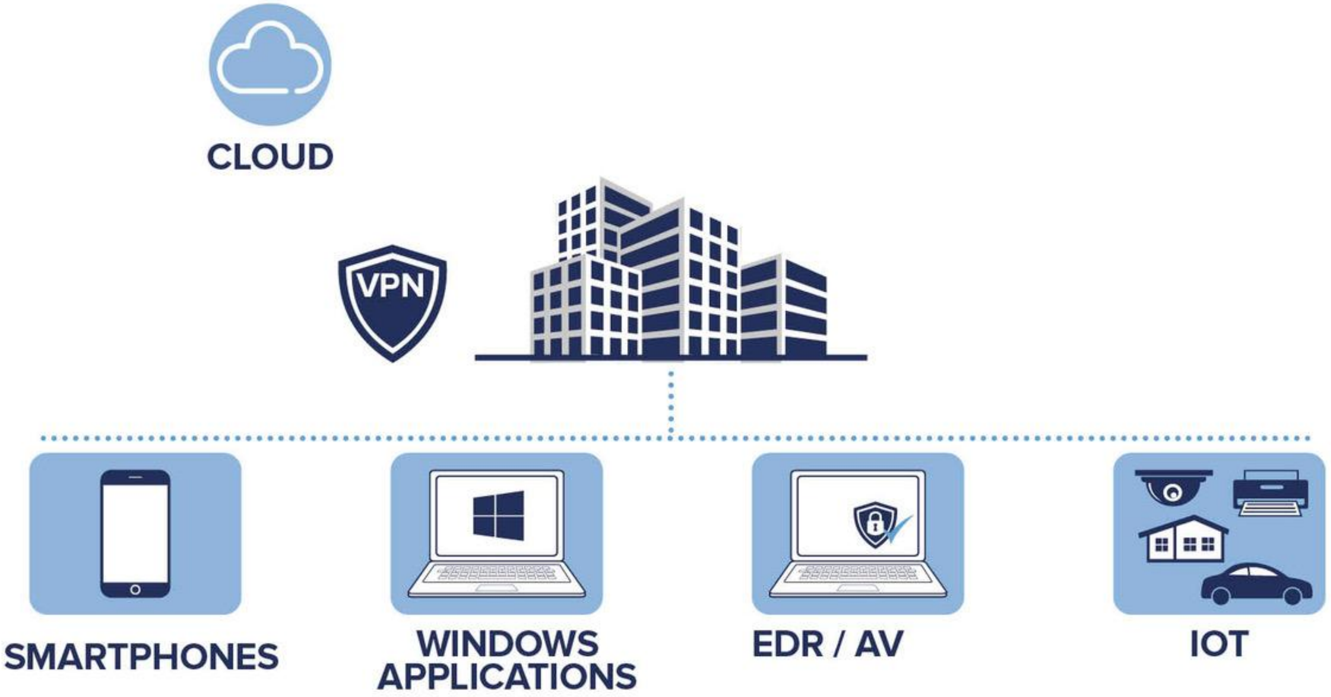
reassemble

disassemble

improve

From https://rebrickable.com/sets/75125-1/resistance-x-wing-fighter/

Focus on a typical corporate network


CLOUD
VPN
SMARTPHONES
WINDOWS APPLICATIONS
EDR / AV
IOT

Can an attacker bypass my EDR/AV solution?

Added Attack Surface

- more code == more vulnerabilities
  - privileged services
  - format parsers
  - efficiency compromises

Worst-Case Scenarios

- detection bypass

  legitimate ways to execute code

- vulnerable component

  in privileged application

QLab Methodology

Quarkslab

- focus on the most privileged components

  filesystem, network, virtual drivers

- look for vulnerabilities

  integer, stack & buffer overflows

- identify driver stacks

  the lower, the more critical

Some Discovered Vulnerabilities

- vendor #1

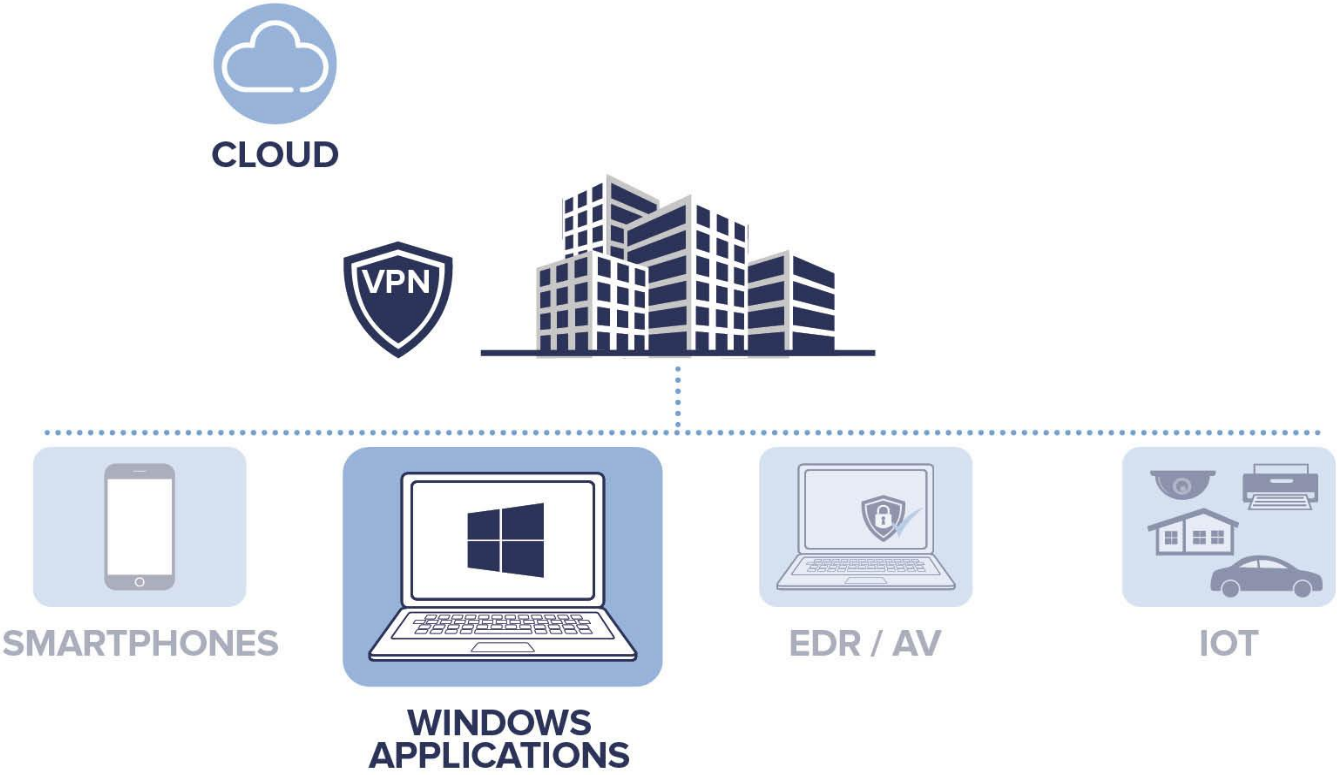
  executable received via email
  emulation in a privileged application
  arbitrary read and write memory access

- vendor #2

  backdoored driver? feature?
  allowing any application to run in kernel mode

- vendor #3

  Microsoft tools whitelisted (aka LOLBins)
  executing code, copying files, persisting...



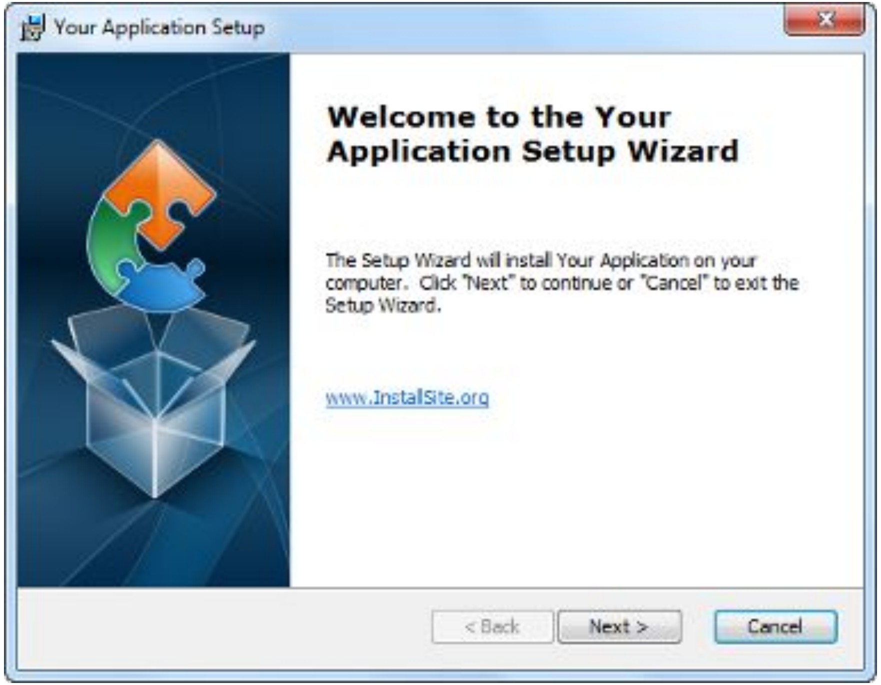
CLOUD

SMARTPHONES

WINDOWS APPLICATIONS

EDR / AV

IOT



Welcome to the Your Application Setup Wizard

The Setup Wizard will install Your Application on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

www.InstallSite.org

binaries

drivers

config files

registry keys

...

Does this Windows *application* contains a vulnerability?

Backups & VPN Clients

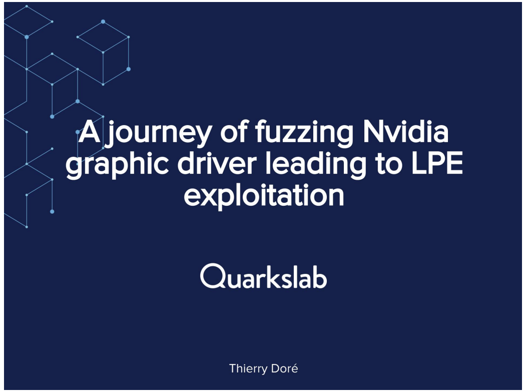
Quarkslab

- CVE-2020-10143 - Macrium Reflect
  1. privileged service uses OpenSSL
  2. anyone can modify openssl.cnf

- CVE-2020-3153 - Cisco AnyConnect
  1. an executable can be moved
  2. vulnerable to DLL hijacking

NVIDIA Graphic Driver

- a simple kernel entrypoint
  - manipulating complex data structures
- methodology
  - reverse the buffer format
  - automatic fuzzing corpus generation
- QLab Public Tools
  - Rewind - snapshot-based fuzzer
  - Triton - dynamic symbolic execution



A journey of fuzzing Nvidia graphic driver leading to LPE exploitation

Quarkslab

Thierry Doré

https://www.hexacon.fr/conference/speakers/#a_journey

Customers Typology

- software development companies

  source code available
  access to the knowhow

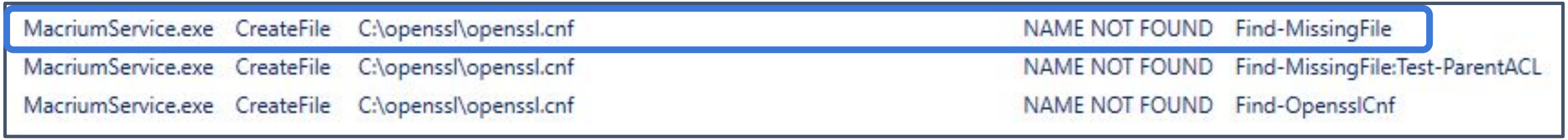
  ➪ **QLab helps secure business opportunities**

- CIO, CISO…

  blackbox audit
  reverse engineering & dynamic analysis

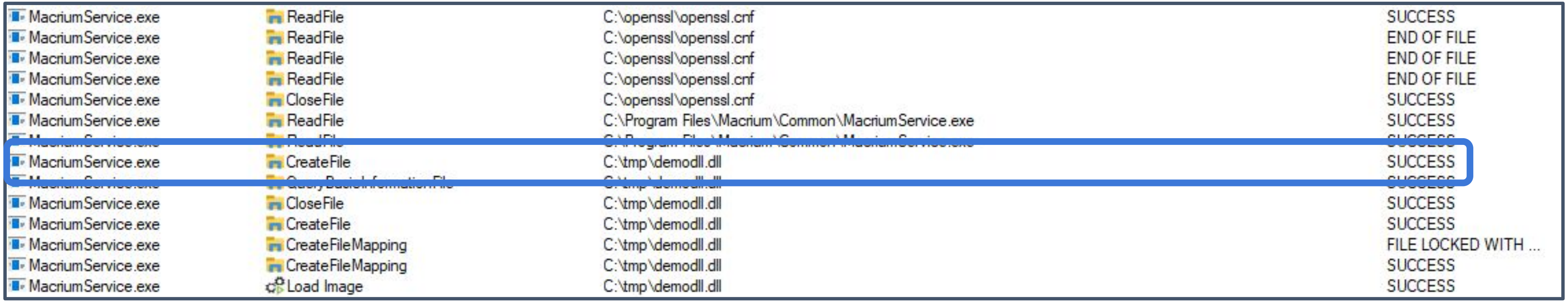
  ➪ **QLab helps assessing risks**

QLab Tools & Automated Detection



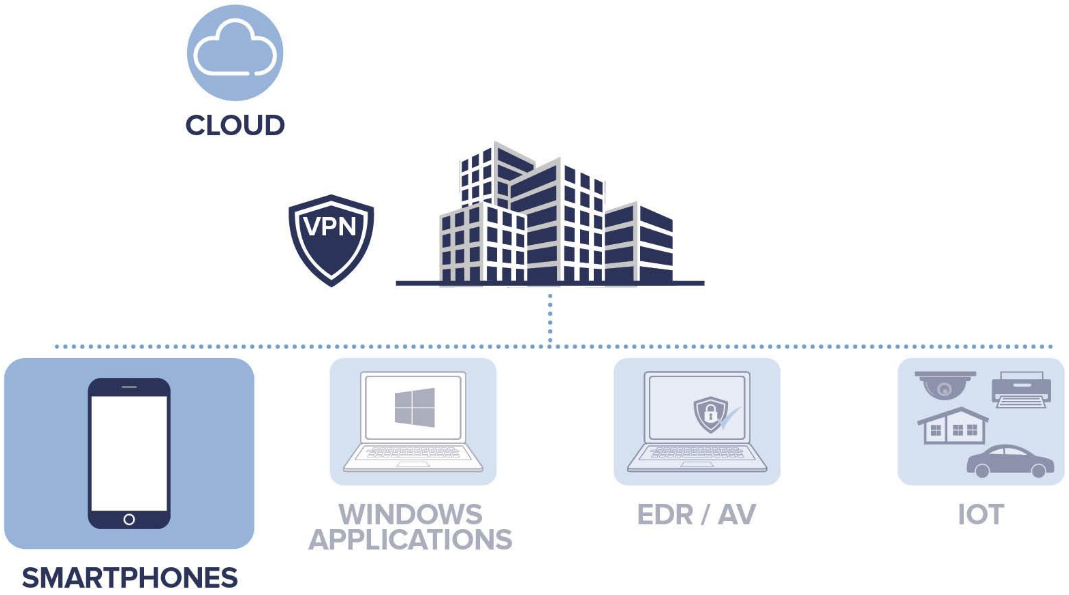
```
MacriumService.exe   CreateFile   C:\openssl\openssl.cnf        NAME NOT FOUND   Find-MissingFile
MacriumService.exe   CreateFile   C:\openssl\openssl.cnf        NAME NOT FOUND   Find-MissingFile:Test-ParentACL
MacriumService.exe   CreateFile   C:\openssl\openssl.cnf        NAME NOT FOUND   Find-OpensslCnf
```

Missing file detection



```
MacriumService.exe   ReadFile                   C:\openssl\openssl.cnf                                   SUCCESS
MacriumService.exe   ReadFile                   C:\openssl\openssl.cnf                                   END OF FILE
MacriumService.exe   ReadFile                   C:\openssl\openssl.cnf                                   END OF FILE
MacriumService.exe   ReadFile                   C:\openssl\openssl.cnf                                   END OF FILE
MacriumService.exe   CloseFile                  C:\openssl\openssl.cnf                                   SUCCESS
MacriumService.exe   ReadFile                   C:\Program Files\Macrium\Common\MacriumService.exe       SUCCESS
MacriumService.exe   ReadFile                   C:\Program Files\Macrium\Common\MacriumService.exe       SUCCESS
MacriumService.exe   CreateFile                 C:\tmp\demodll.dll                                       SUCCESS
MacriumService.exe   QueryBasicInformationFile  C:\tmp\demodll.dll                                       SUCCESS
MacriumService.exe   CloseFile                  C:\tmp\demodll.dll                                       SUCCESS
MacriumService.exe   CreateFile                 C:\tmp\demodll.dll                                       SUCCESS
MacriumService.exe   CreateFileMapping          C:\tmp\demodll.dll                                       FILE LOCKED WITH ...
MacriumService.exe   CreateFileMapping          C:\tmp\demodll.dll                                       SUCCESS
MacriumService.exe   Load Image                 C:\tmp\demodll.dll                                       SUCCESS
```

Verification with Procmon



CLOUD

SMARTPHONES

WINDOWS APPLICATIONS

EDR / AV

IOT

A Smartphone from Above

- hardware

  baseband, Trust Zone, security elements…

- Operating System & configuration

  MDM bypasses, roots, jailbreaks..

- Applications

  permissions, cryptographic protocols….

Can a mobile application attack the hardware?

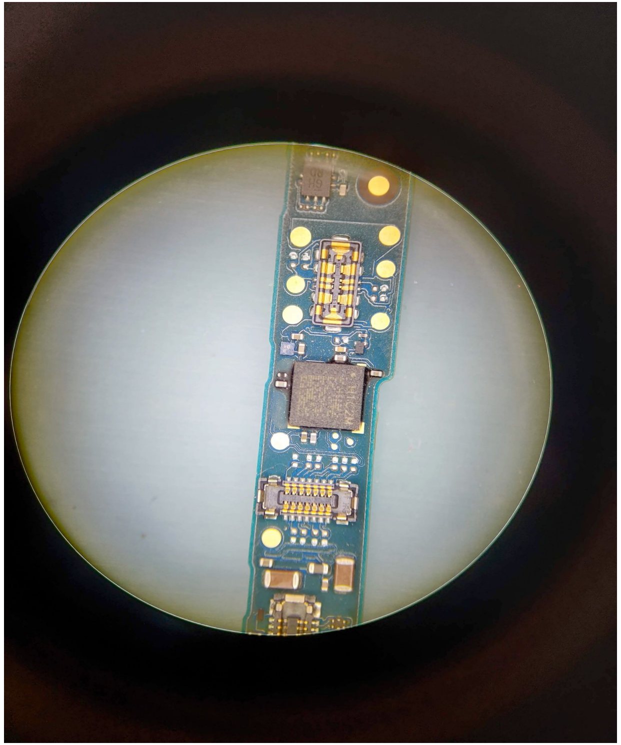
Google TITAN-M on Pixel Phones

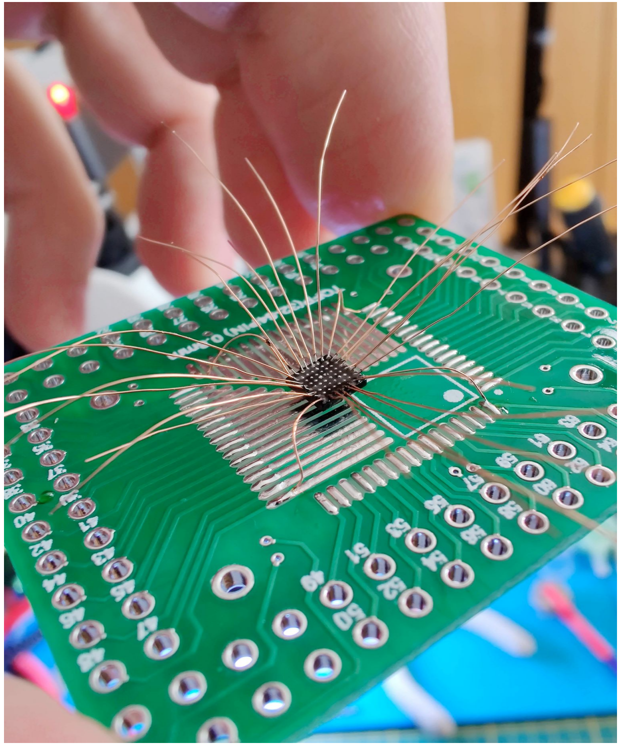
Quarkslab

- **security chip**
  - made by Google, closed-source…
  - hardware-based Android KeyStore

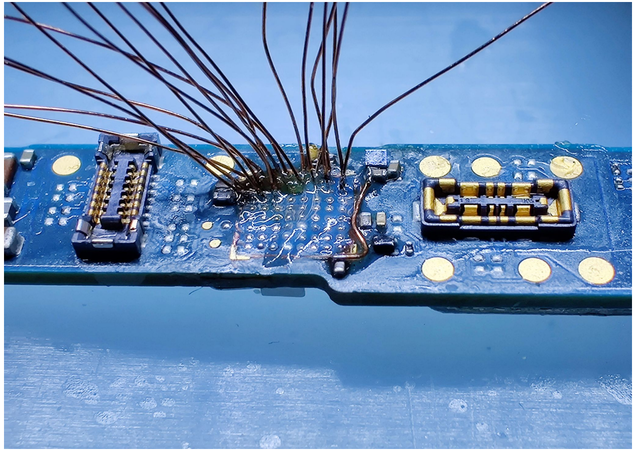
- **methodology**
  - reverse the firmware
  - desolder the chip and reverse the pinout
  - emulate & fuzz parsing functions

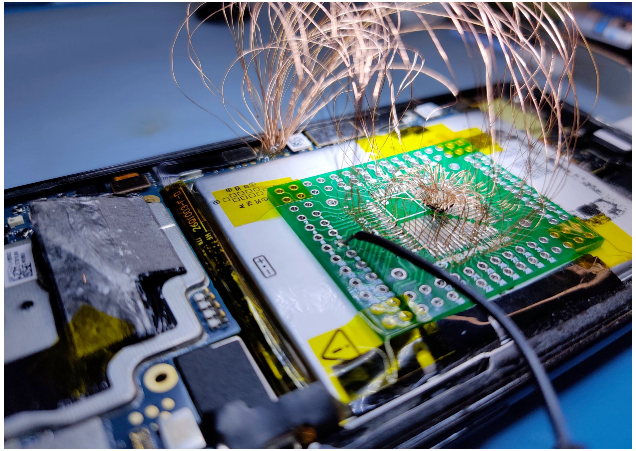
Preparing the TITAN-M

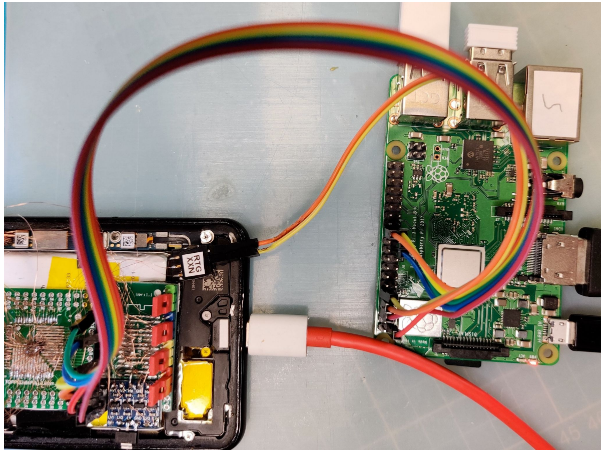




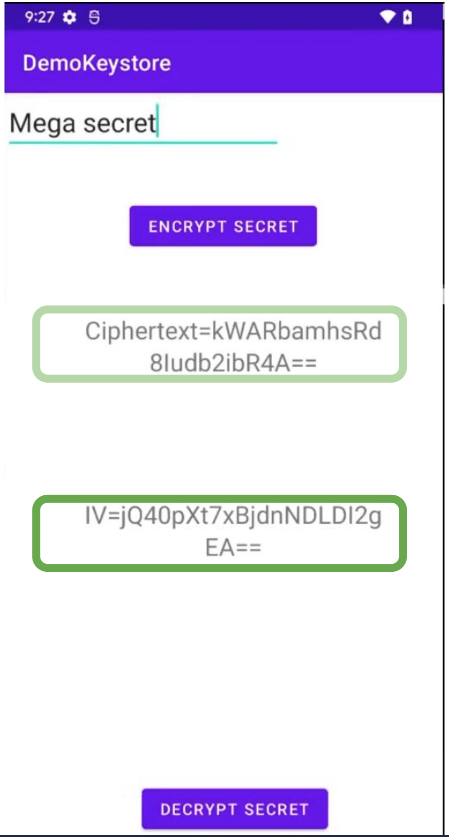
Solder it Back







Focus on CVE-2022-20233 [redacted]



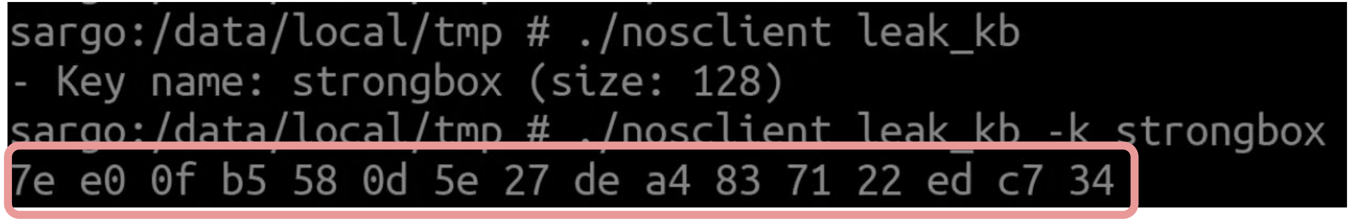
9:27

DemoKeystore

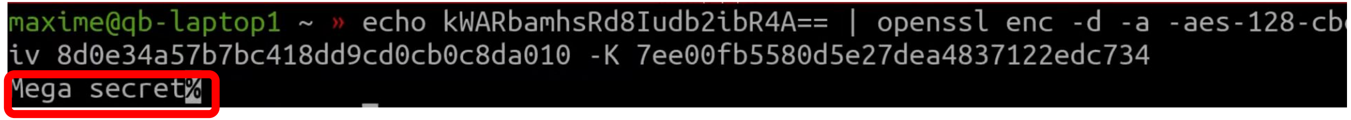
Mega secret

Ciphertext=kWARbamhsRd8Iudb2ibR4A==

IV=jQ40pXt7xBjdnNDLDI2gEA==



```
sargo:/data/local/tmp # ./nosclient leak_kb
- Key name: strongbox (size: 128)
sargo:/data/local/tmp # ./nosclient leak_kb -k strongbox
7e e0 0f b5 58 0d 5e 27 de a4 83 71 22 ed c7 34
```



```
maxime@qb-laptop1 ~ » echo kWARbamhsRd8Iudb2ibR4A== | openssl enc -d -a -aes-128-cb
iv 8d0e34a57b7bc418dd9cd0cb0c8da010 -K 7ee00fb5580d5e27dea4837122edc734
Mega secret%
```

Questions?

Stand #225

Quarkslab