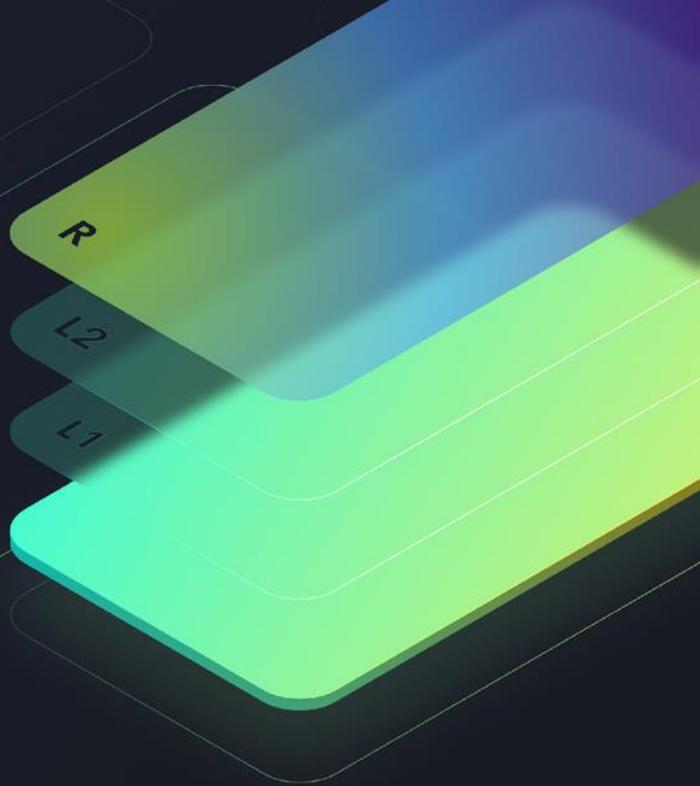




Evidence of App Safety

# App and API security SDK for FinTechs

- Ensure OWASP compliance
- Anti- **fraud, reverse engineering** and **App cloning**
- Anti- **App impersonation** for API

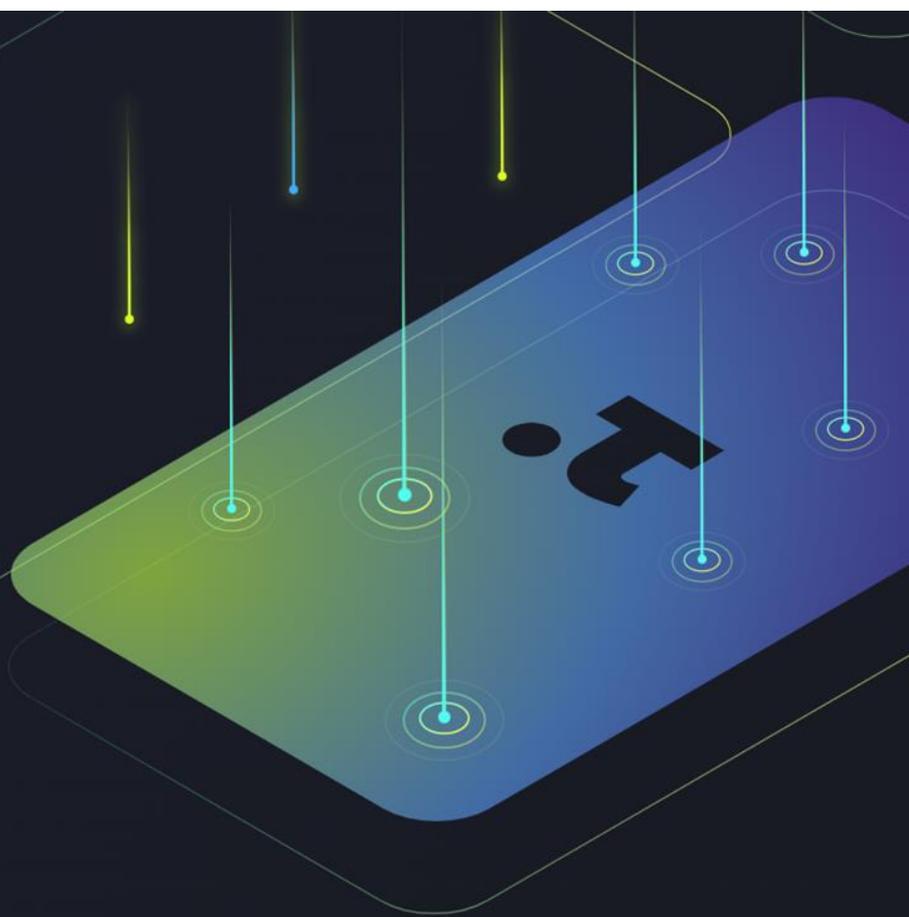


# In-App Protection SDK

Keep your application, business and customers secure with complete in-app and API protection SDK. Using multi-layered approach Talsec SDK combats reverse engineering, app cloning/republishing, rooting, API abuse, Frida hooking, MitM, and much more. Available for iOS, Android and Flutter apps.

[Request Demo](#)

[Learn More](#)



# Trusted by



MINISTRY OF THE INTERIOR  
OF THE CZECH REPUBLIC

ProID



Banco  
ECONOMICO

BancoSol

novü  
card



# Recognized by



Google  
for  
Startups

# SDKs to **WIN TIME**



Tampering



Overlay  
Attacks



Reverse  
Engineering



Root/Jailbreak



Code Injection

- Prepare to Pentesting
- Mitigate mobile cyber fraud
- Comply with Regulations and OWASP

## Supported Platforms



iOS



Flutter

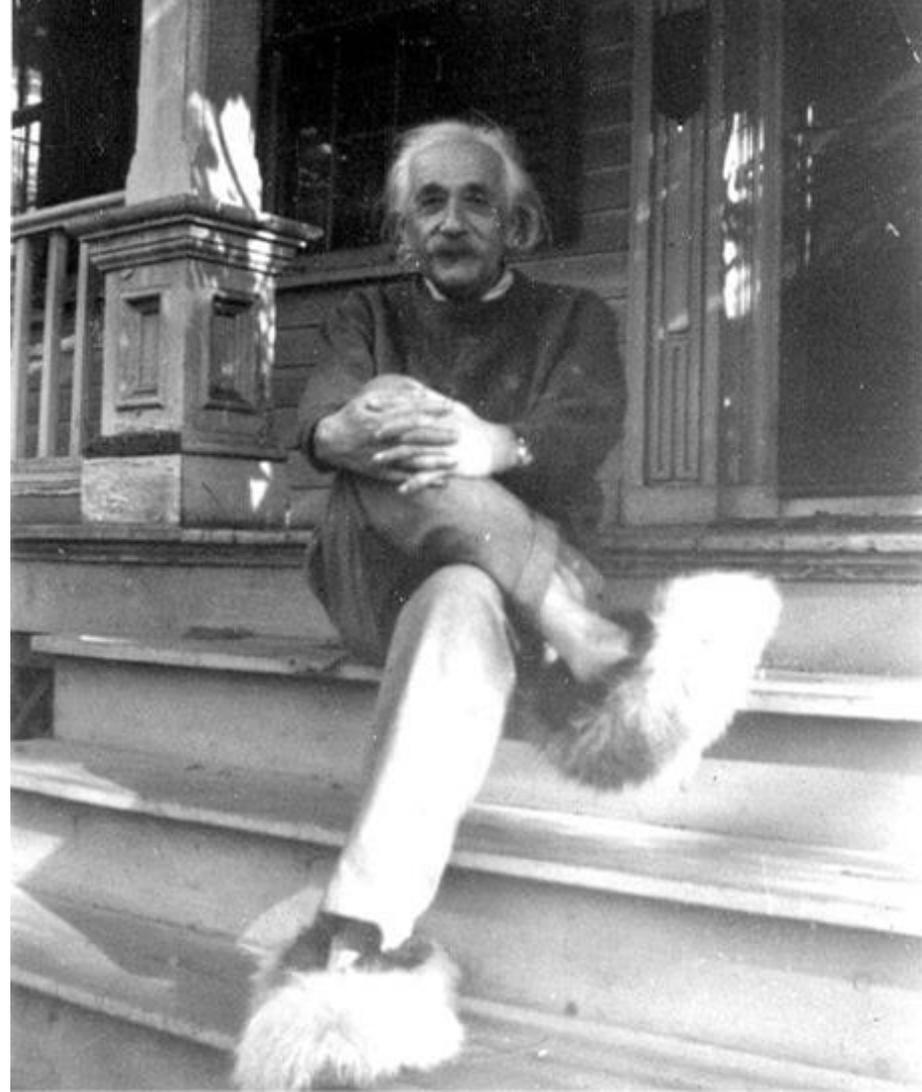


APACHE  
CORDOVA™

“ It is easy to  
complicate

and

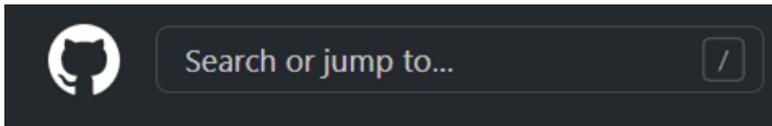
hard to **simplify**



# Talsec is good in not-doing things



# First and only freemium RASP SDK



228  
LIKES

140  
PUB POINTS

93%  
POPULARITY



Repository

github.com/talsec/Free-RASP-ReactNative

Homepage

github.com/talsec/Free-RASP-ReactNati...

Weekly Downloads

24



# OWASP TOP10

Mobile OWASP top 10	Talsec RASP	Talsec AppiCrypt	Talsec App Hardening Suite
M1: Improper Platform Usage	Helps	Helps	
M2: Insecure Data Storage			Soon
M3: Insecure Communication			Solves
M4: Insecure Authentication		Helps	
M5: Insufficient Cryptography			Soon
M6: Insecure Authorization		Helps	
M7: Client Code Quality			
M8: Code Tampering	Solves	Solves	
M9: Reverse Engineering	Solves	Solves	
M10: Extraneous Functionality	Helps	Helps	

# “Hot” attacks

Fraudsters Attack vectors	Talsec RASP	Talsec AppiCrypt	Talsec App Hardening Suite
Session hijacking		Solves	
Man in the middle			Solves
SIM swapping		Helps	
API-abuse		Solves	
JSON injections		Solves	
Fraudulent Apps (malware)	Helps	Helps	
Untrusted install sources		Solves	



# Easy to use SDKs



## RASP App protection & Monitoring

**Comply** with OWASP and Regulations

**Data** Analytics, Audit & Visualization



## AppiCrypt® for API protection

**Zero trust** for Mobile solution. Simple App integrity and device authorization

**Anti-botnet**, anti-API abuse



## App Hardening Suite

**Dynamic** TIS pinning

**App Data Encryption** (Strings Enc, Assets Data Protection, E2EE)

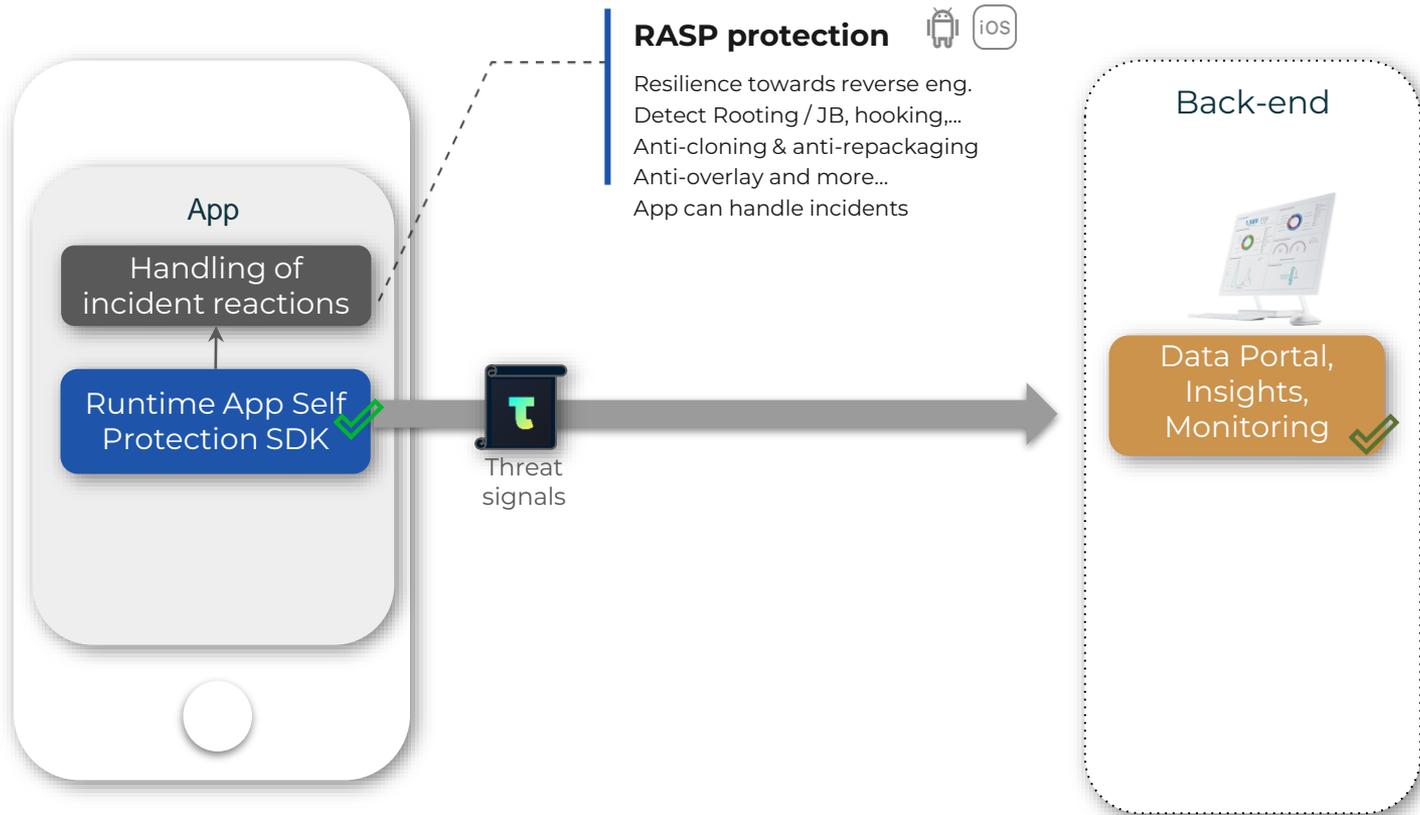
τ.**RASP**: Runtime App Self Protection

anti-

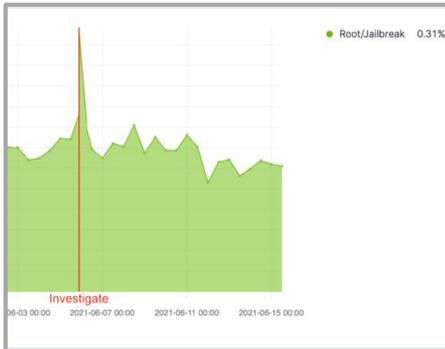
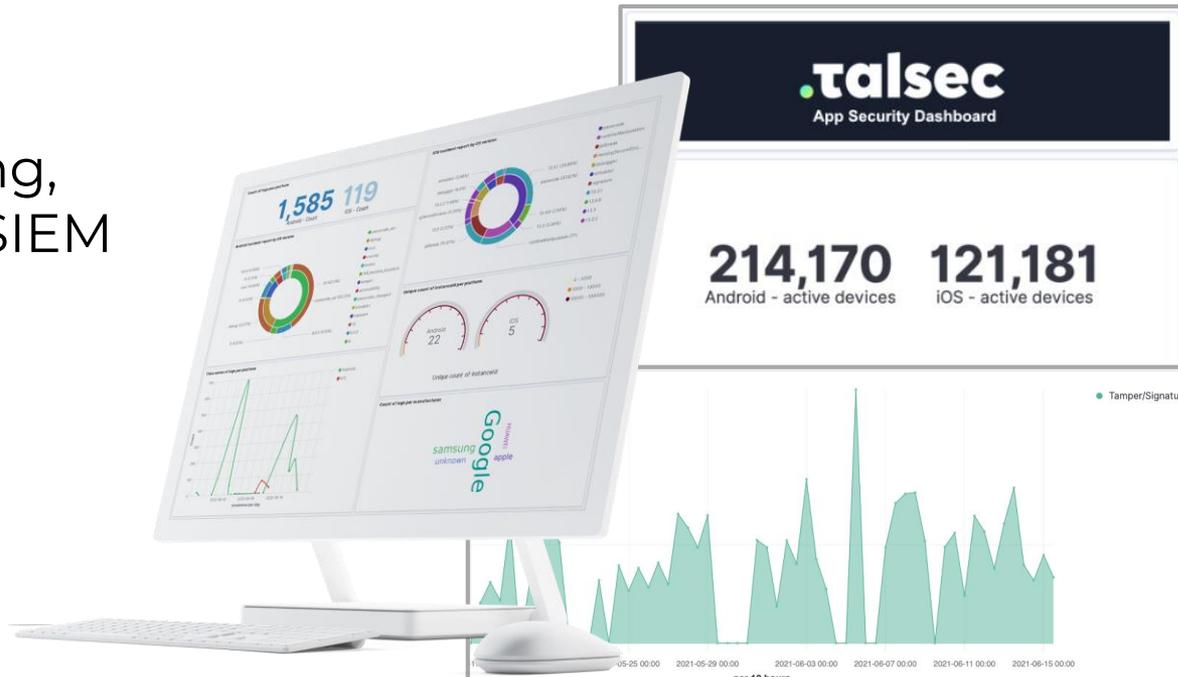
**Reverse Engineering and Malware attacks**

Audit & Monitoring signals to  
database or SIEM

# τ.RASP - Runtime App Self Protection and Monitoring



# Auditing, Monitoring, Data for SIEM

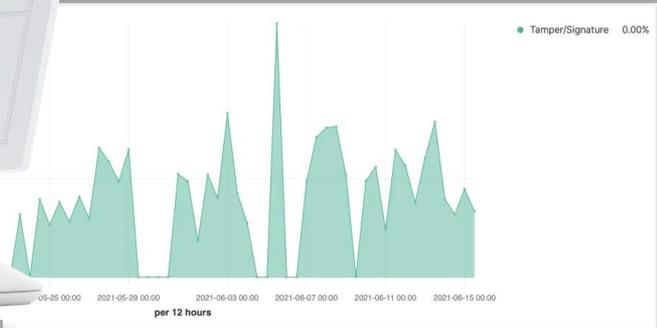


### Root/Jailbreak

Applications are sandboxed by default, which means that the application is executed in its own isolated environment. Rooting/jailbreaking is a technique of acquirement of privileged access, whilst posing a threat to either applications or the operating system.

Average number of compromised devices per time bucket: 108 (0.351%)

Total number of compromised devices: 1314 (0.386%)

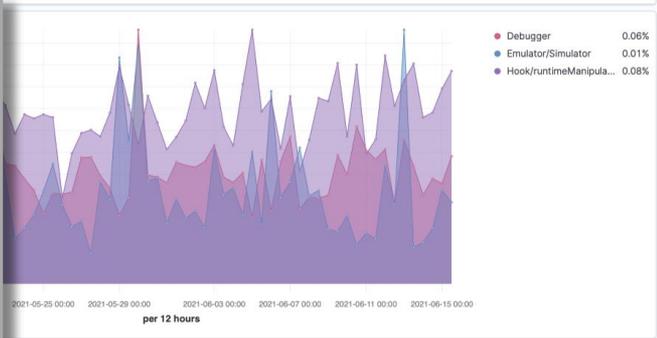


### Tamper/Cloning

Using freely available tools, every application can be modified and then re-signed. This process is known as application repackaging. There are many reasons for modifying an application, for example addition of new code, disabling the application licence or protection.

Average number of compromised devices per time bucket: 2 (0.005%)

Total number of compromised devices: 45 (0.013%)



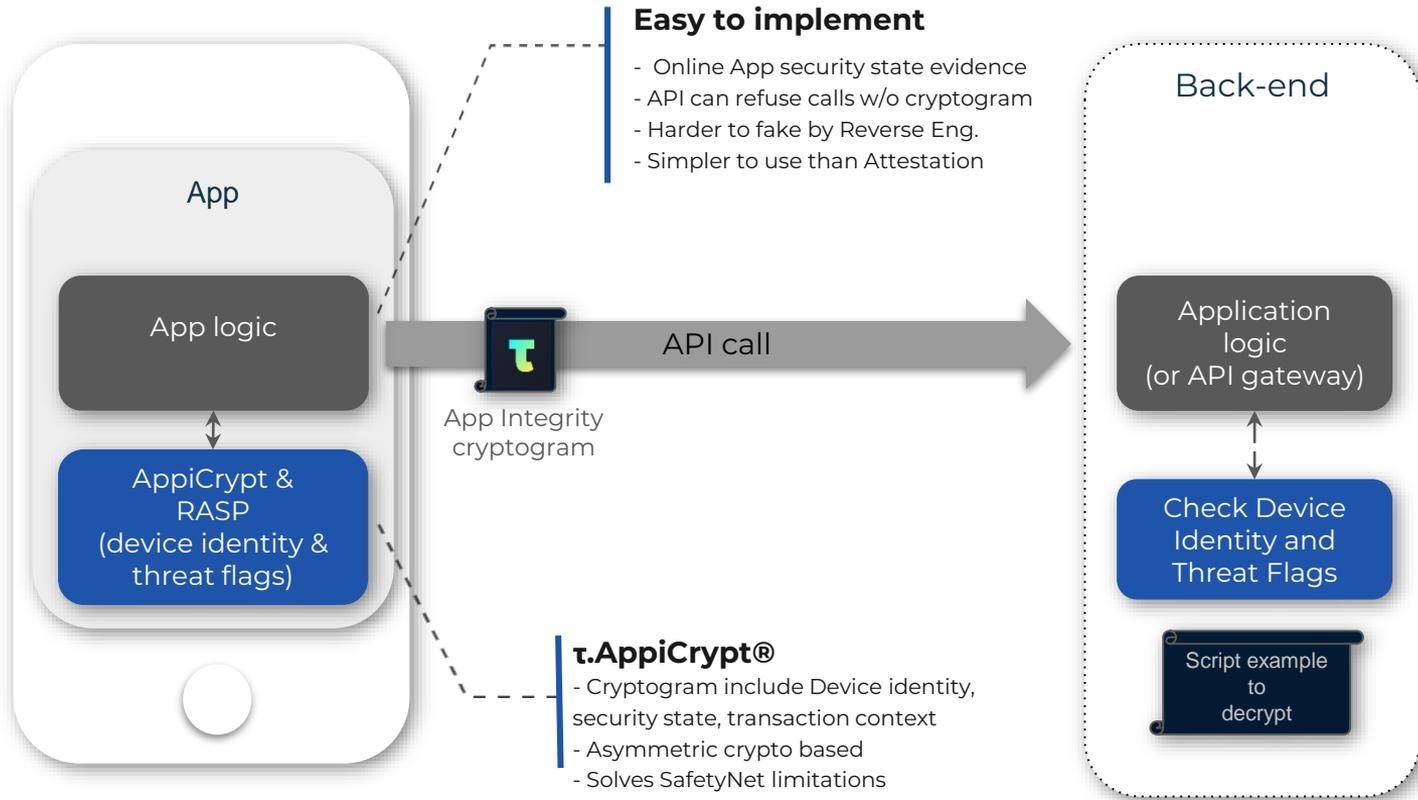
### Reverse engineering attempts

Individual attacker can use various techniques to gain intelligence about the application. Those techniques include attaching a debugger, using emulator with the intention of dynamic behaviour analysis, or hooking the application via well known hooking frameworks like Frida, Substrate, or Xposed.

Average number of compromised devices per time bucket: 39 (0.13%)

Total number of compromised devices: 815 (0.239%)

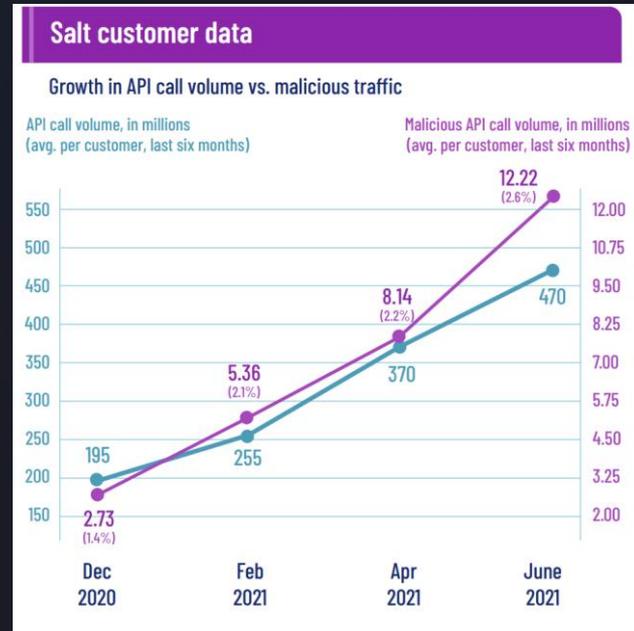
# AppiCrypt® proof of App integrity for back-ends



# API protection challenge

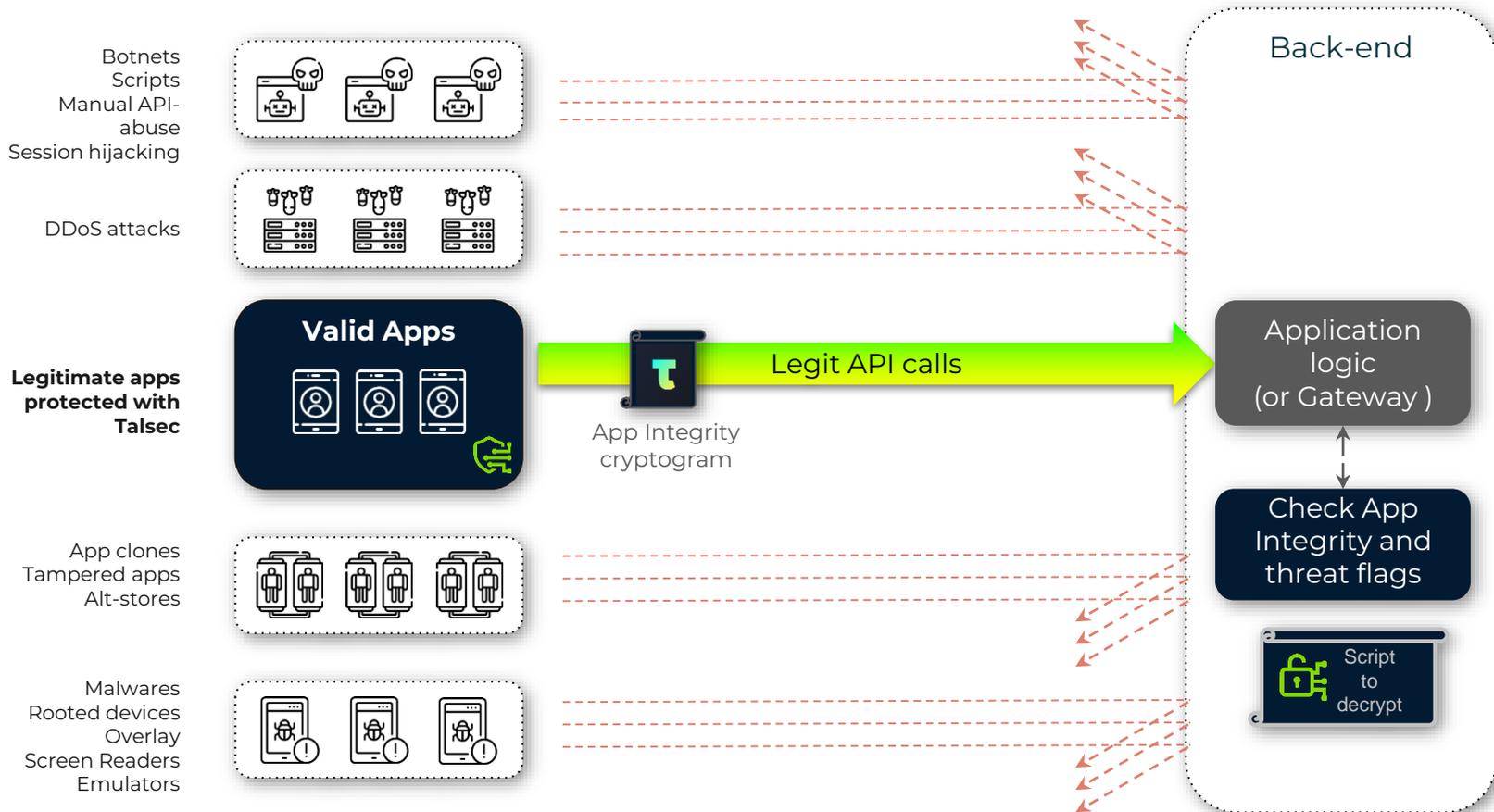
95% of API exploits happened against authenticated APIs\*

WAFs and API Gateways miss majority % of API Attacks\*



\*Salt Security Report (Q3 2021)

# AppiCrypt® proof of App integrity for back-ends



# Talsec Hardening SDK

- **Dynamic TLS Pinning**
- **App Data Encryption**
  - App Strings encryption (e.g. API keys, endpoints )
  - Local data encryption (e.g. shared preferences, App assets )
  - Application layer E2E encryption (light)

## Encryption & Decryption



# App Safety Subscription



## Penetration testing of your App

**Automated** penetration testing with tool like Kryptowire

**Ethical Hacking** exercise with Talsec playbook and OWASP



## App protection by RASP & Monitoring

**Comply** with OWASP and Regulations

**Data** Analytics, Audit & Visualization



## API protection by AppiCrypt®

**Zero trust** for Mobile solution. Simple App integrity and device authorization

**Anti-botnet**, anti-API abuse



## App Hardening Suite

**Dynamic** TIS pinning

**App Data Encryption** (Strings Enc, Assets Data Protection, E2EE)

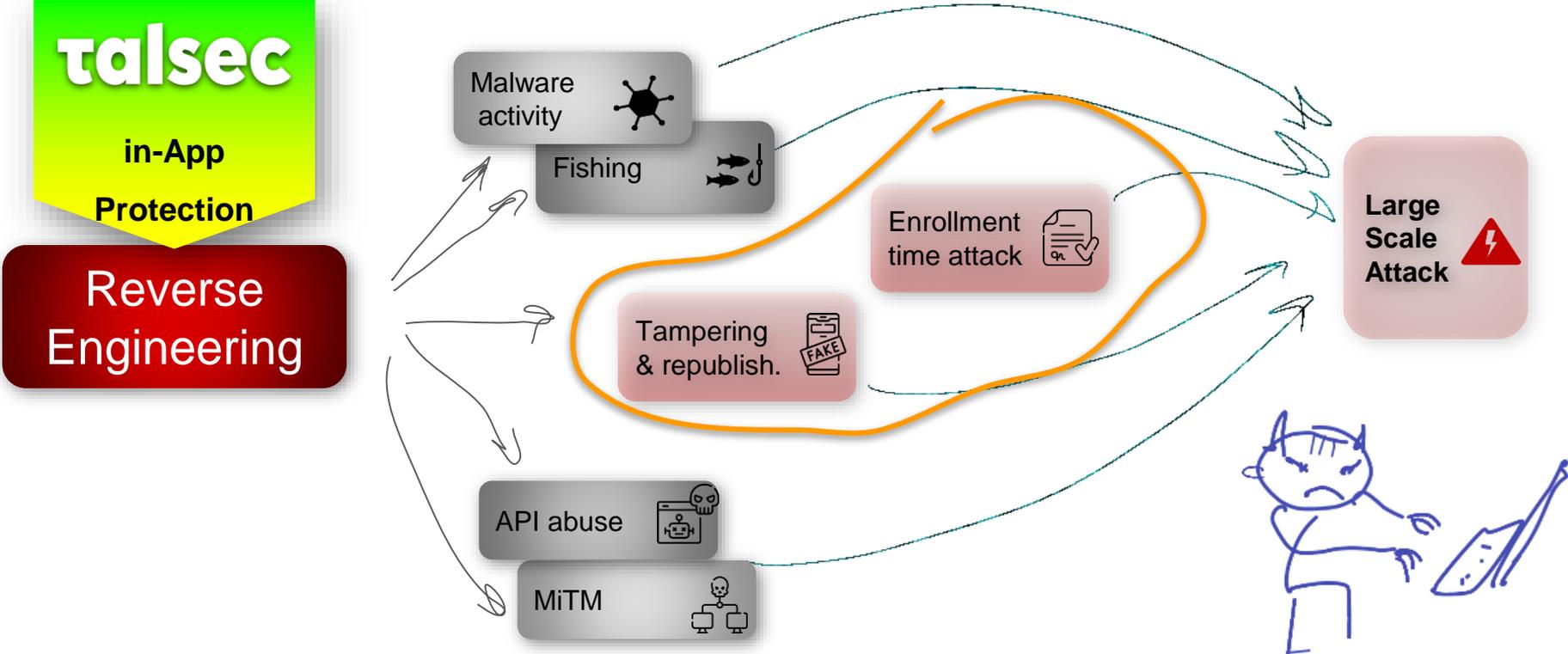
# talsec

Thank you!

**Contact Details**

**<http://talsec.app>**

# Apps are vulnerable by design to Reverse Engineering





# Android OS security Controls

Vulnerabilities detected in FinTech App by RASP SDK

20%



Screen Lock is not activated

38%

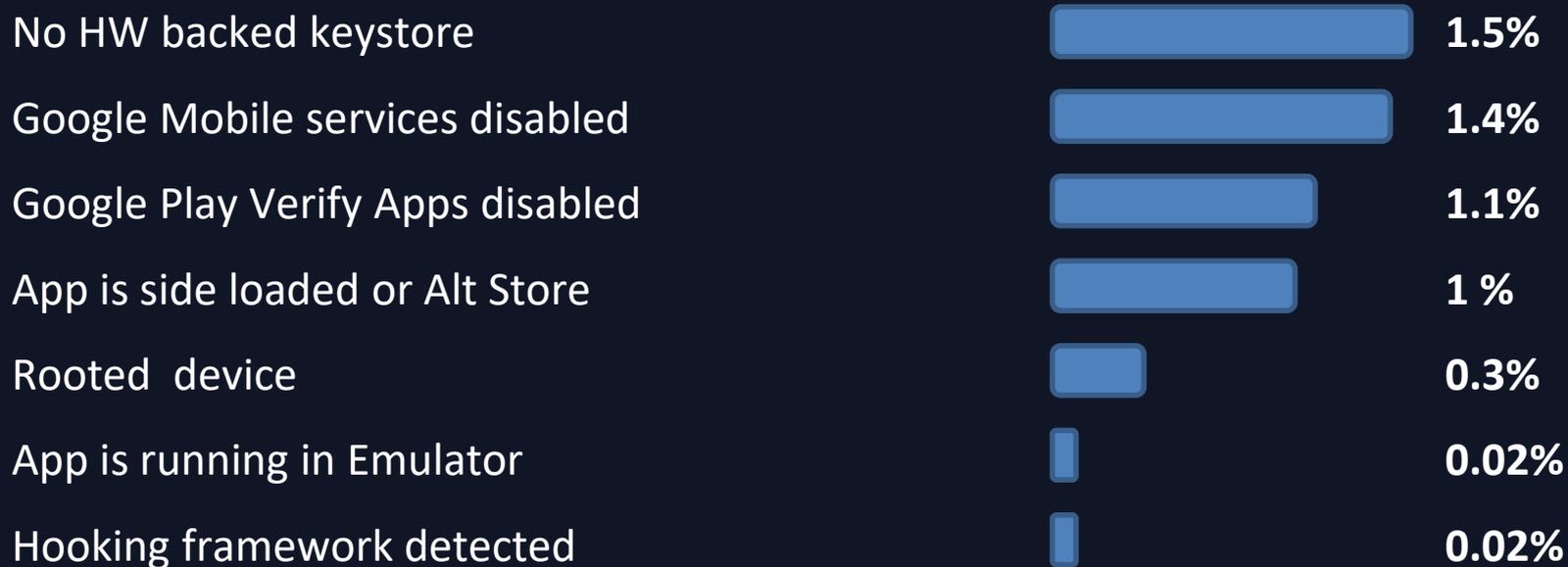


Biometrics is not activated

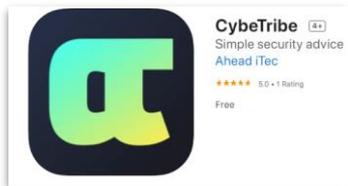


# Android OS security Controls

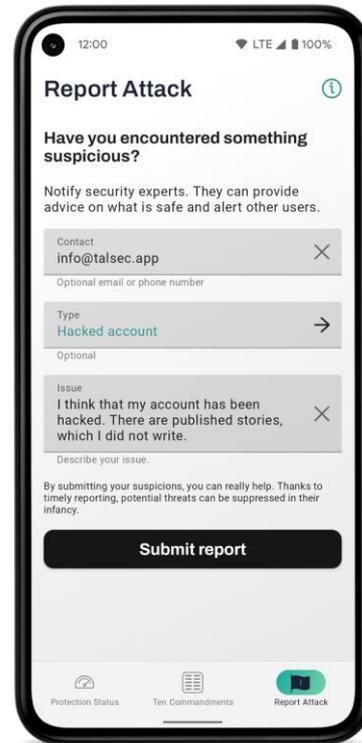
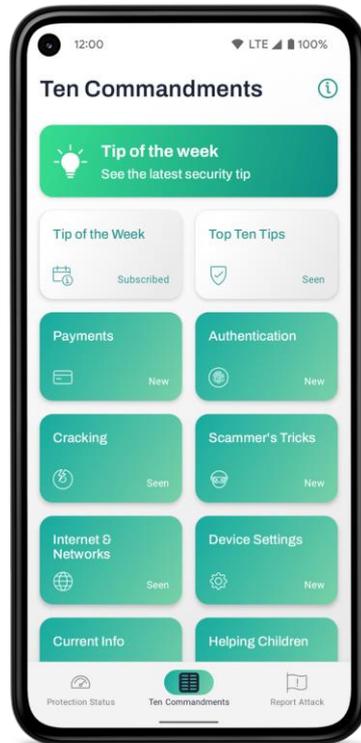
Vulnerabilities detected in FinTech App by RASP SDK



# App Security visualization Widget (CybeTribe App)



**talsec**



# Protection and Monitoring for **Android POS and Kiosk**

