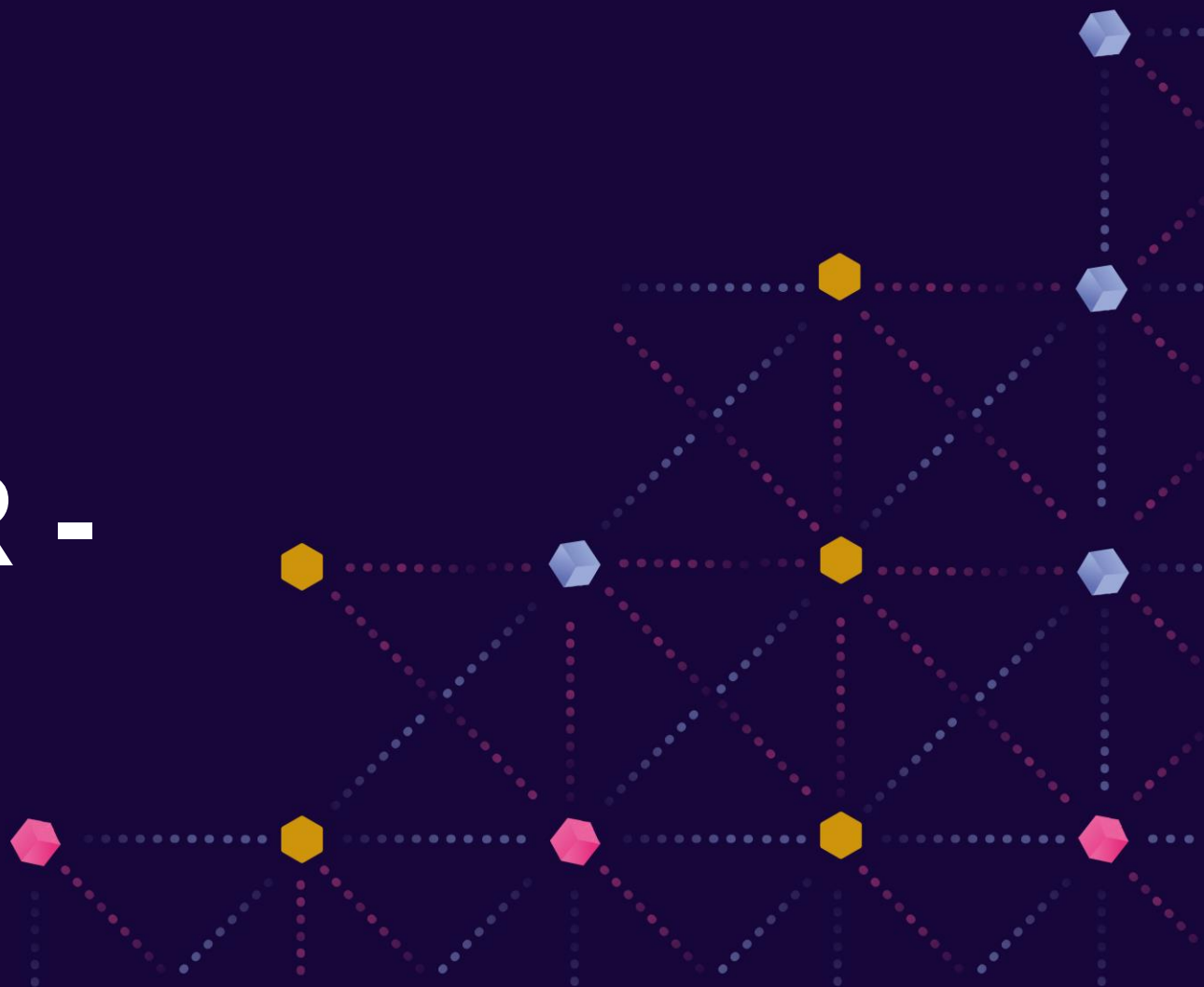
PurpleBox

A Mutant Mobile Banking Botnet

- TODDLER -



www.prplbx.com

$whoami

Ömer Faruk Çulha

PurpleBox -> Cyber Security Engineer

Sakarya Üniversitesi -> Makine Müh.

https://twitter.com/0x1337root

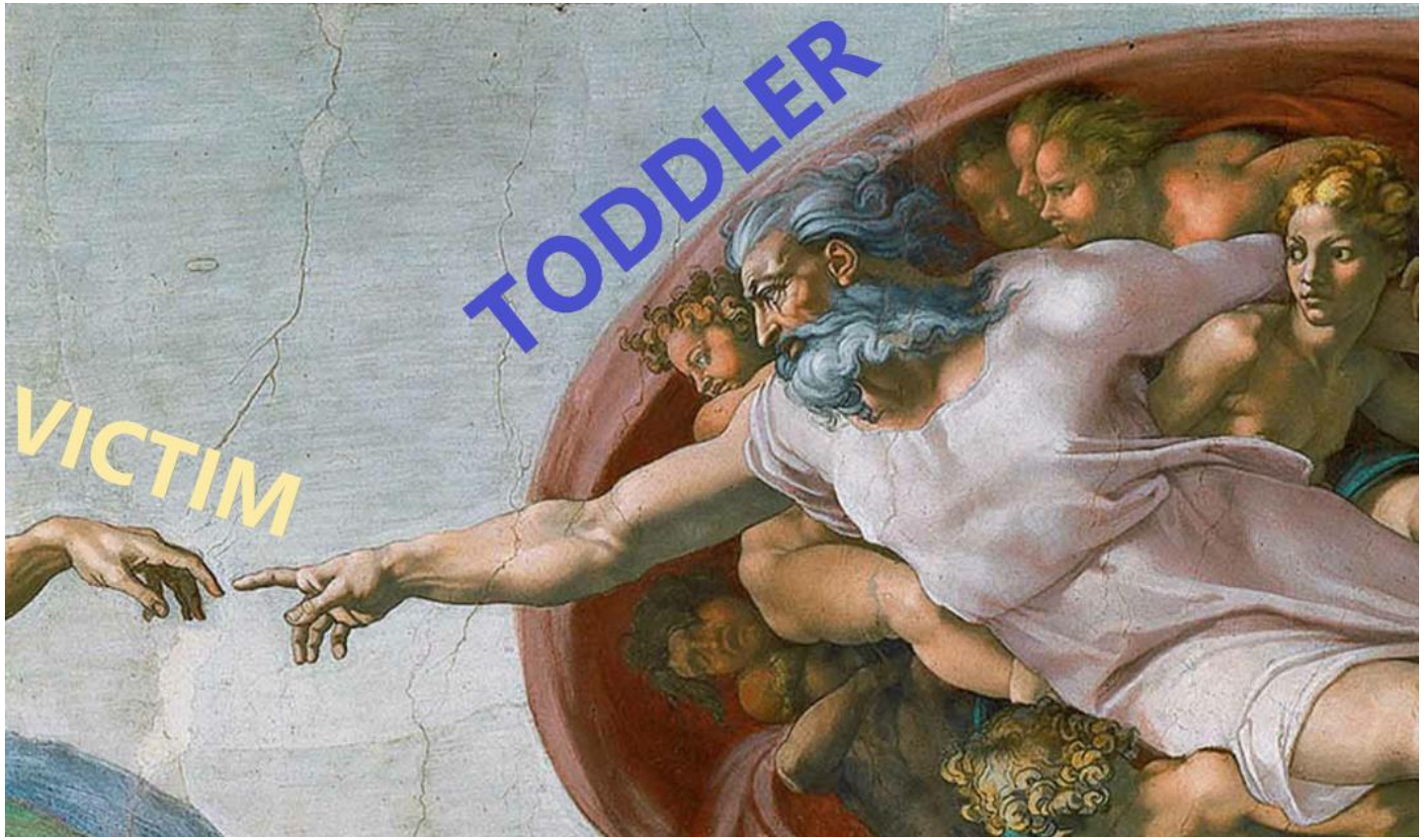
https://tryhackme.com/p/0x1337root

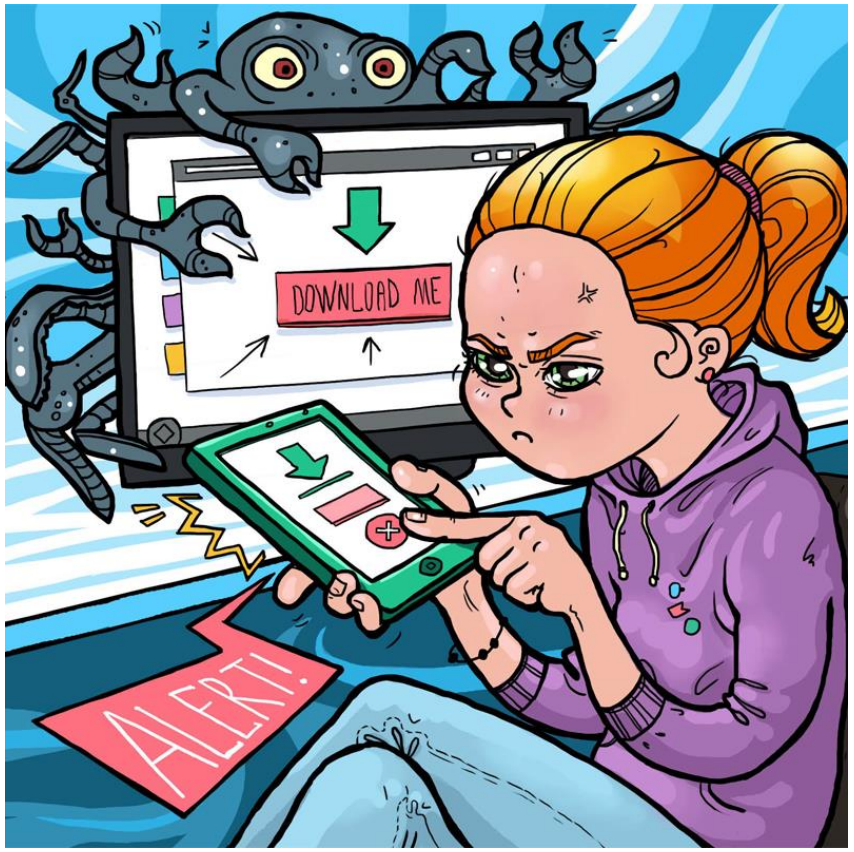
https://www.linkedin.com/in/ömer-faruk-çulha-b95880195

TODDLER Nedir ?

Hedef ?

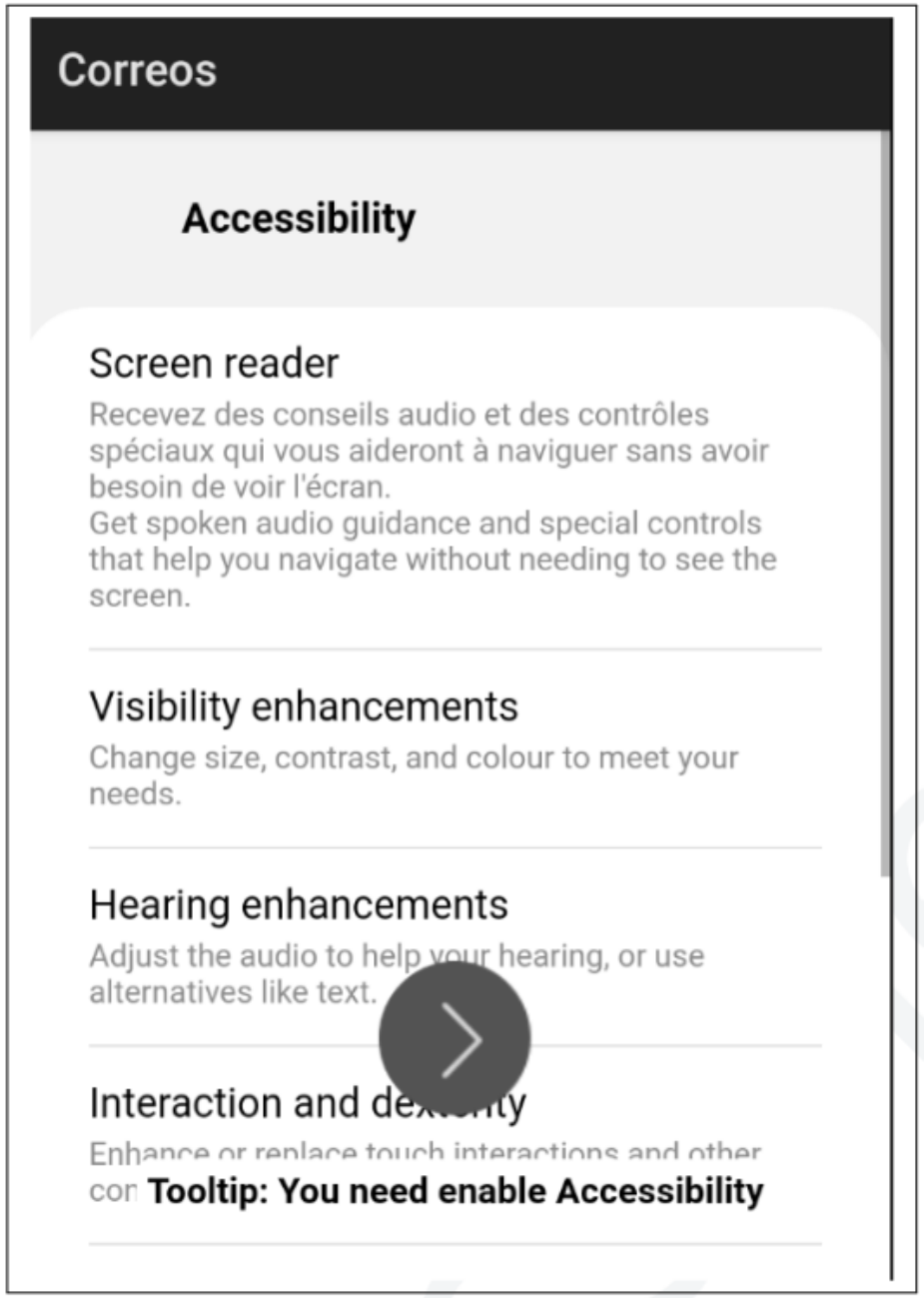
İlk Temas ?

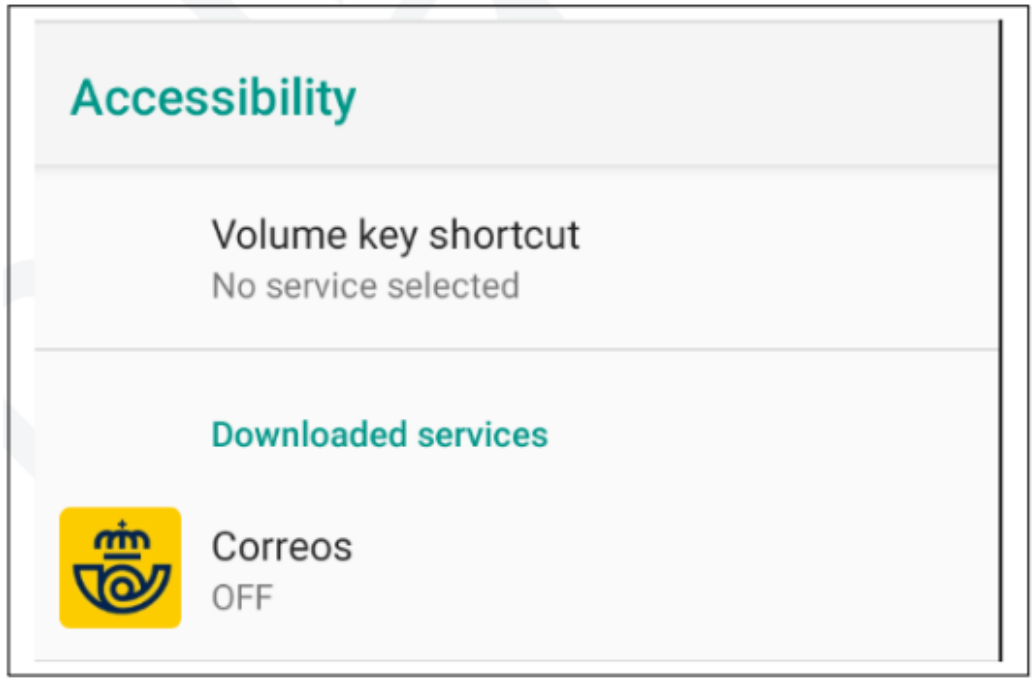




Potansiyel ?

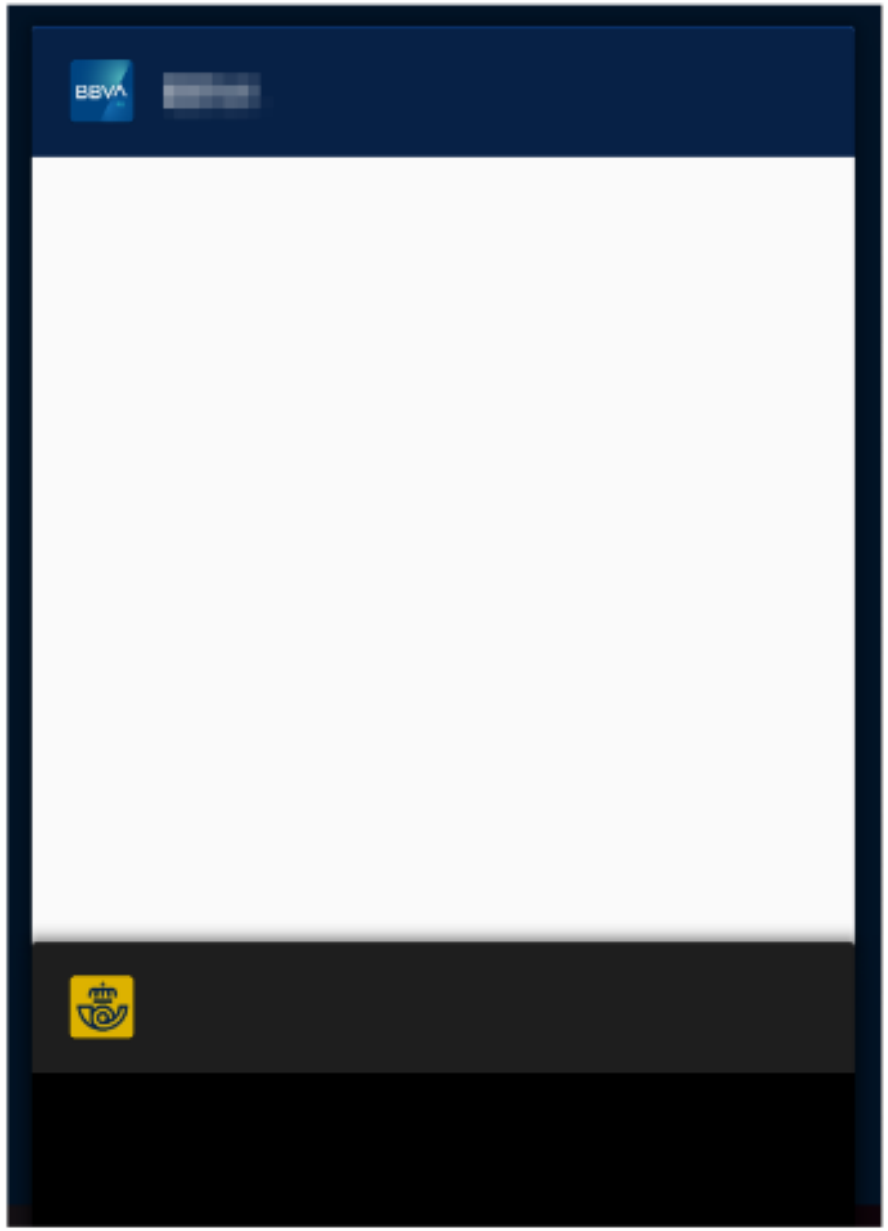

Delete application
Package name
EXECUTE
Open inject
Package name
EXECUTE
Activate screen
EXECUTE
Show grab system pass
EXECUTE
Ask permissions
EXECUTE
Grab google authenticator
EXECUTE
Hide sms
Hide sms
EXECUTE
Google auth push confirmer
Auto confirm
EXECUTE
KILL BOT
EXECUTE
Enable exntensive logging
Logging
EXECUTE
Lock device
Lock device
EXECUTE
Reset password
EXECUTE
Grab user emails
EXECUTE
Mute phone
EXECUTE
Add reserve domain
Ip
Port
EXECUTE
Open activity
Package
EXECUTE
Change pass
EXECUTE
Stop Protection (30 sec)
EXECUTE
Swipe down
EXECUTE
BOT DETAILS: REFRESH
HWID: 402e343e9647c729
Keep alive: 0 hours 0 mins 24 secs
Total alive: 96 hours 2 mins 10 secs
Device name: Samsung SM-N770F
Phone: no permission
Battery: 45
Locale: en_gb
Android version: 30
Screen active: false
Screen secure: true
Country: de
Hide sms : false
Google auth push confirmer : false
Lock device: false
Accessibility enabled: true
Doze enabled: true
Sms manager: com.samsung.android.messaging
Knock domain:
Logged password:
Installed apps
com.amazon.mShop.android.shopping
com.google.android.youtube
com.samsung.android.app.galaxyfinder
com.aminullahdev.btshdwallpaper
com.sec.location.nfwlocationprivacy
com.ebay.kleinanzeigen
PENDING COMMANDS: REFRESH

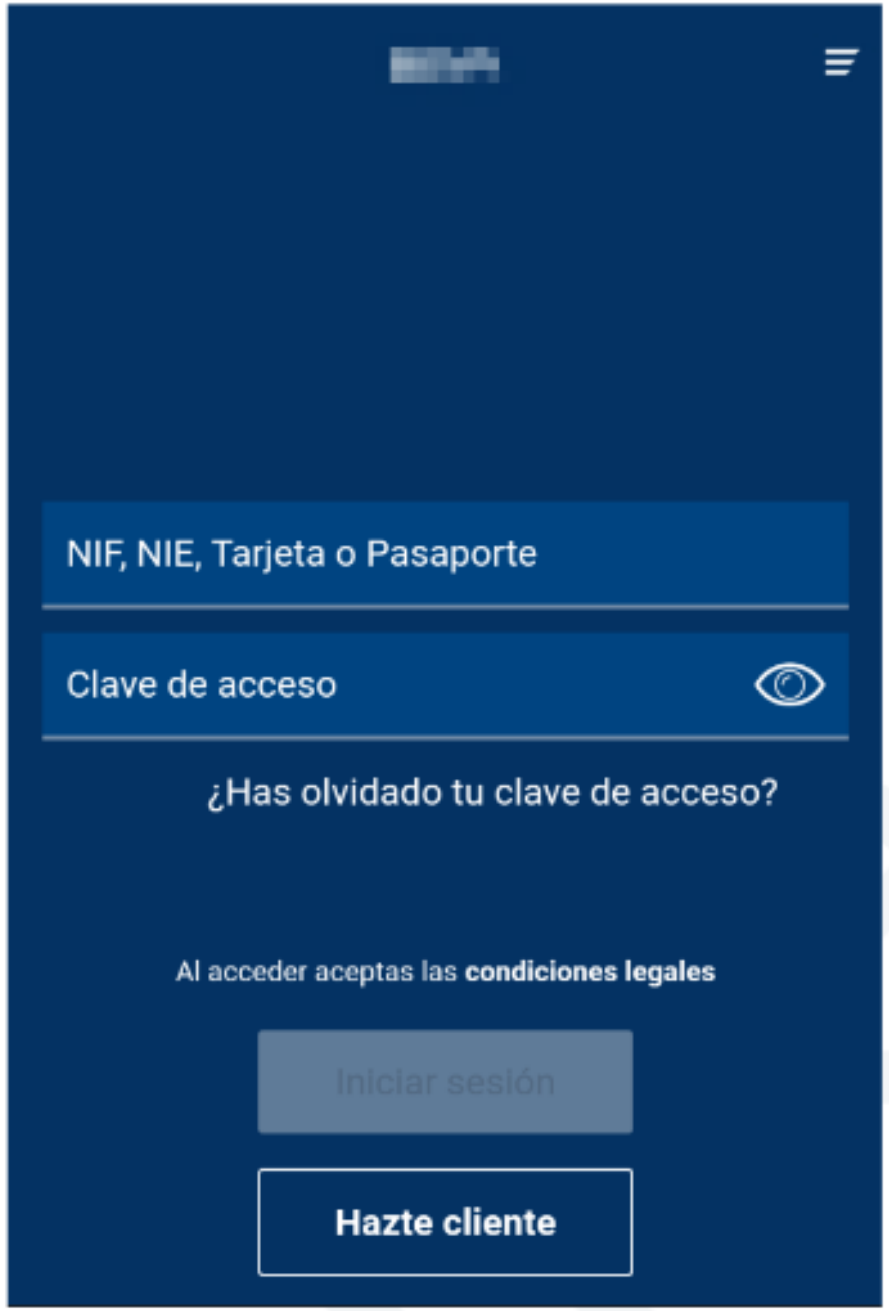

Correos
Accessibility
Screen reader
Recevez des conseils audio et des contrôles spéciaux qui vous aideront à naviguer sans avoir besoin de voir l'écran.
Get spoken audio guidance and special controls that help you navigate without needing to see the screen.
Visibility enhancements
Change size, contrast, and colour to meet your needs.
Hearing enhancements
Adjust the audio to help your hearing, or use alternatives like text.
Interaction and dexterity
Enhance or replace touch interactions and other
cor
Tooltip: You need enable Accessibility


Accessibility
Volume key shortcut
No service selected
Downloaded services
Correos
OFF

Post Exploitation ?

- Overlay Attack
- Webview-based application phishing

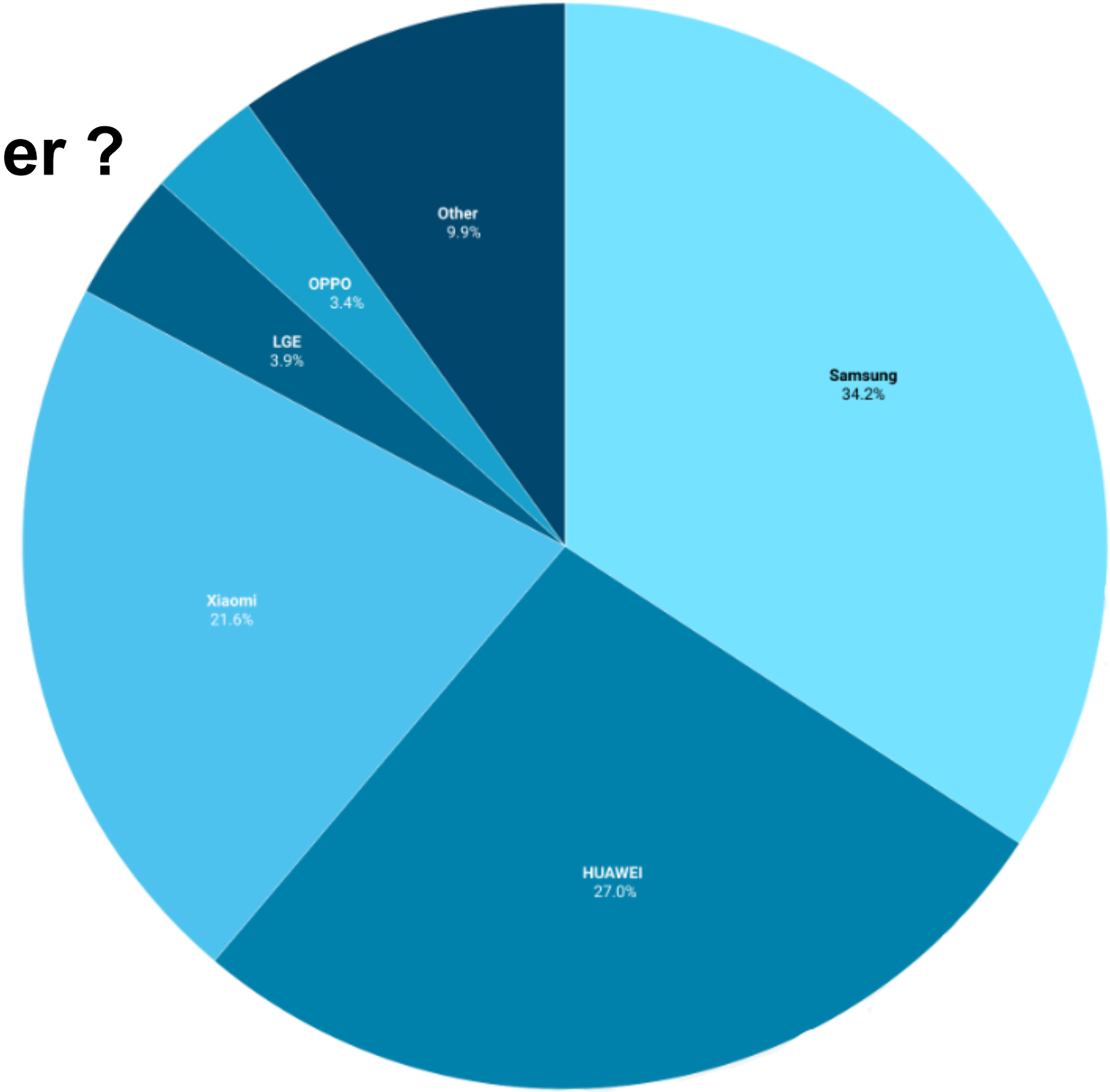


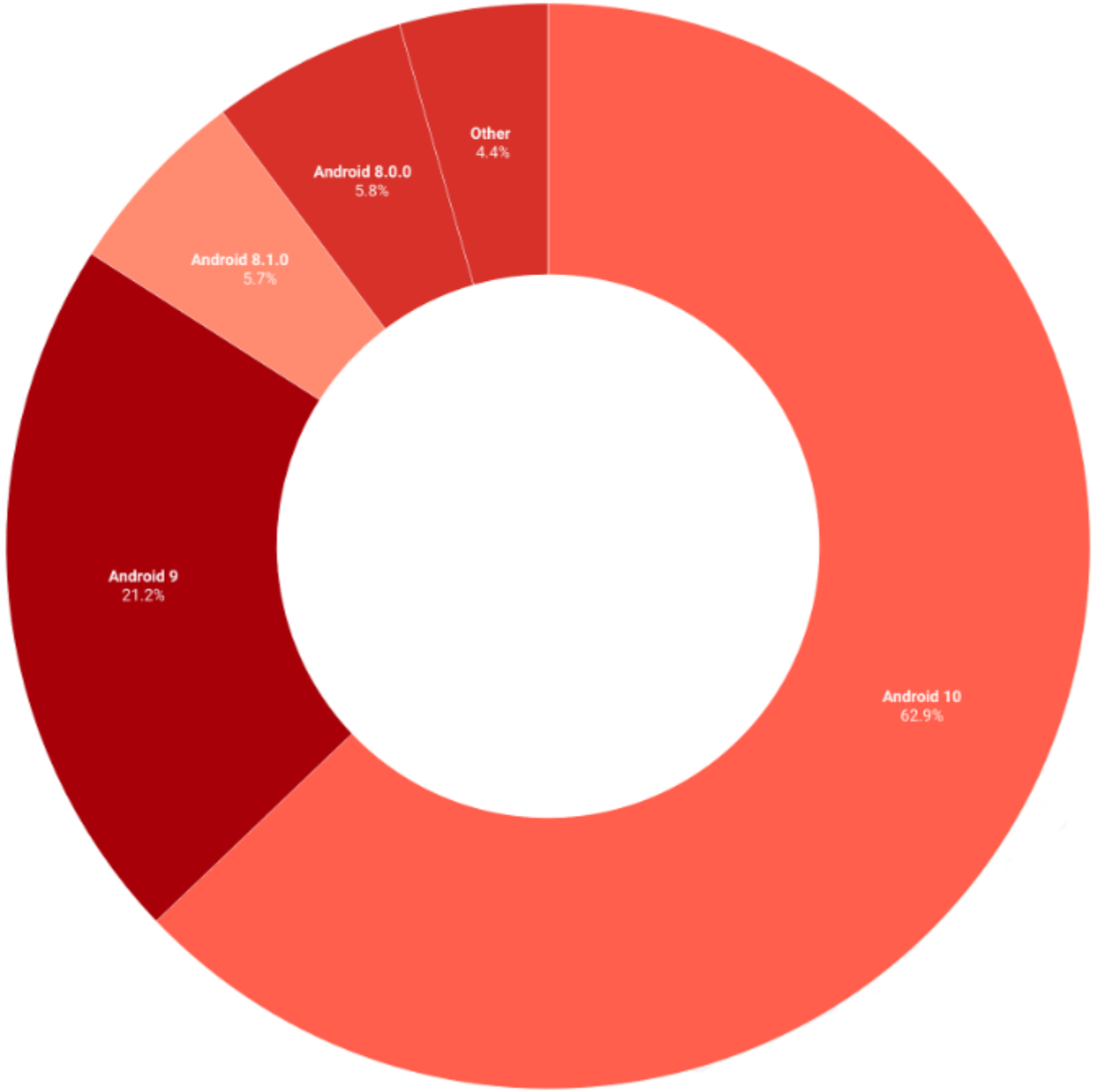

NIF, NIE, Tarjeta o Pasaporte
Clave de acceso
¿Has olvidado tu clave de acceso?
Al acceder aceptas las condiciones legales
Iniciar sesión
Hazte cliente

Kalıcılık ?

Mutant köpek tarafından ziyaret edildin.

İstatistikler ?




Other
4.4%
Android 8.0.0
5.8%
Android 8.1.0
5.7%
Android 9
21.2%
Android 10
62.9%

Referanslar

- https://www.prodaft.com/tr/kaynak/detay/toddler-mobile-banking-botnet-analysis-report

Thank you!
Any Questions?

PurpleBox

www.prplbx.com