



SECURITY

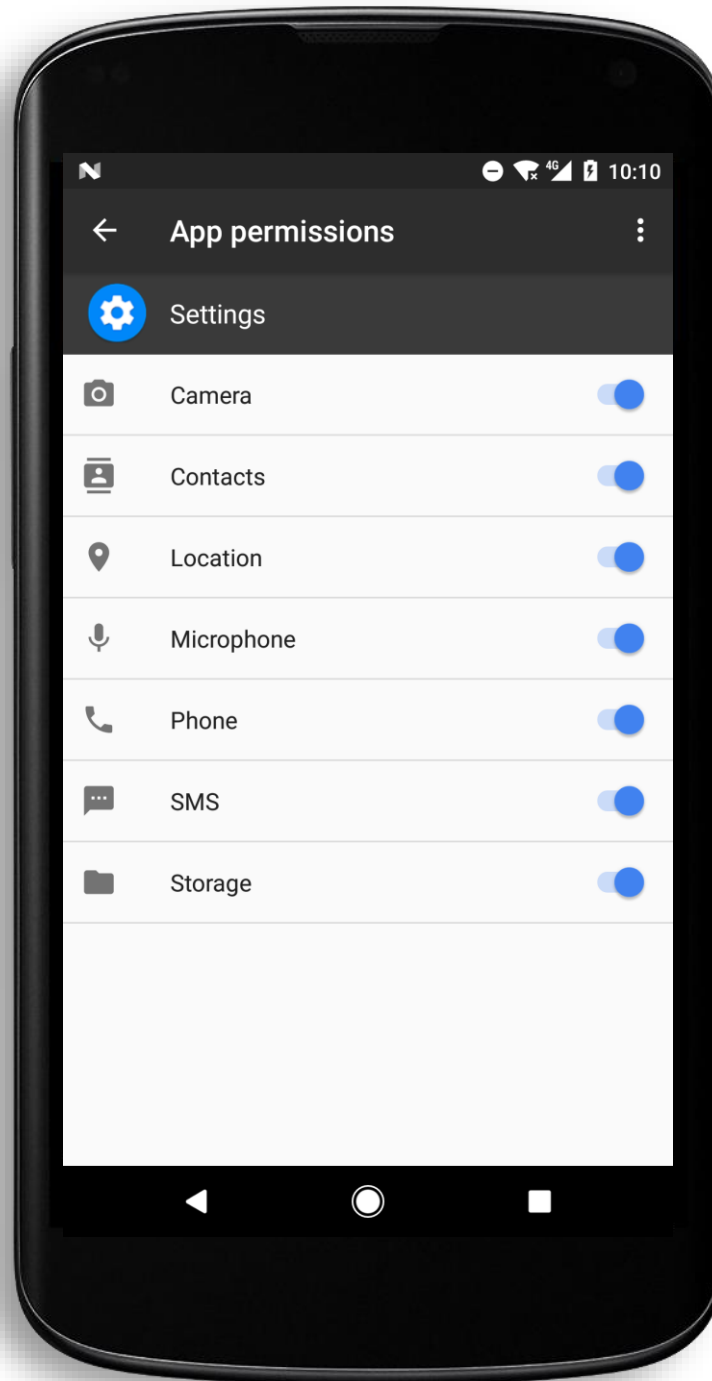
The Hidden Cost of Android Stalkerware

Lukas Štefanko

Malware Researcher

Mobile Stalkerware





Track Employees Check Work Phone Online Spy Free

Outlog Tools

★★★★★ 78

PEGI 3

This app is compatible with your device.

Add to Wishlist Install



Spy Kids Tracker

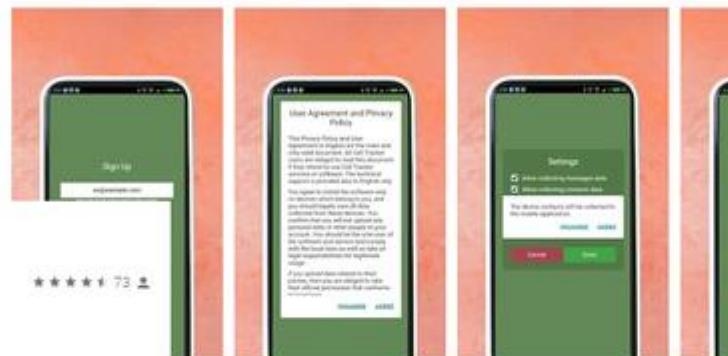
WiDo Personalization

★★★★★ 236

PEGI 3

This app is compatible with your device.

Add to Wishlist Install



Employee Work Spy

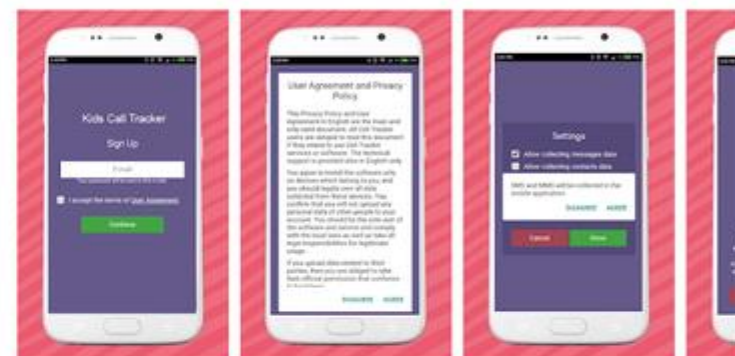
Piter Cline Tools

★★★★★ 1,263

PEGI 3

This app is compatible with your device.

Add to Wishlist Install



Phone Cell Tracker

StaHar Tools

★★★★★ 73

PEGI 3

This app is compatible with your device.

Add to Wishlist



Mobile Tracking

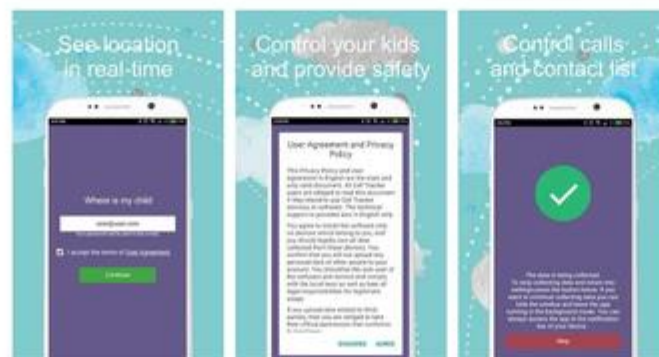
AntWat Tools

★★★★★ 892

PEGI 3

This app is compatible with your device.

Add to Wishlist Install



SMS Tracker

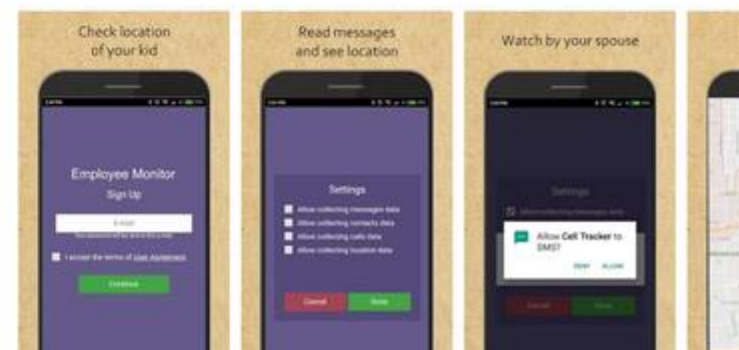
TheHar Tools

★★★★★ 2,865

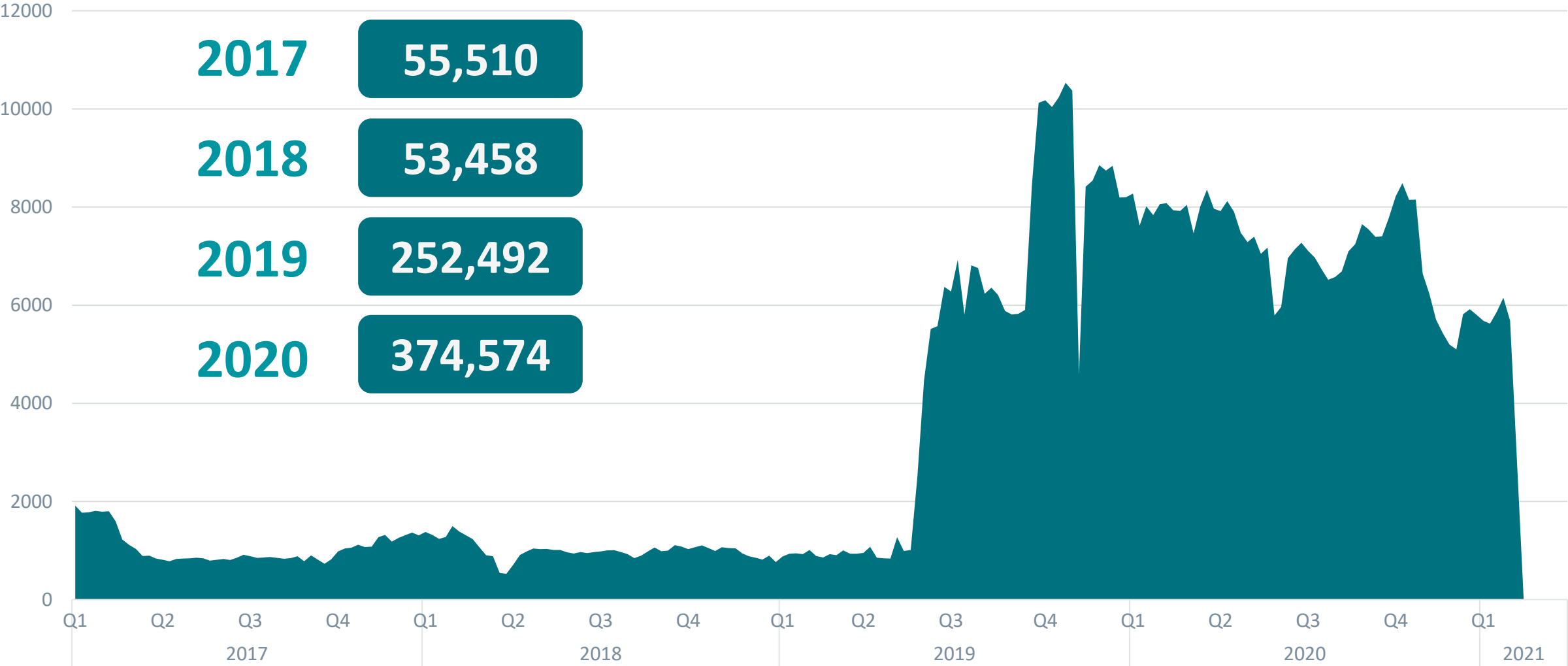
PEGI 3

This app is compatible with your device.

Add to Wishlist Install



Android Stalkerware Detection (2017 - 2020)





DAVID NIELD

SECURITY 07.19.2020 07:00 AM

How to Check Your Devices for Stalkerware

You deserve privacy. Here's how to check your phone, laptop, and online accounts to make sure no one's looking over your shoulder.





Social Media



Facebook



Gmail



Viber



Google+



Instagram



Twitter



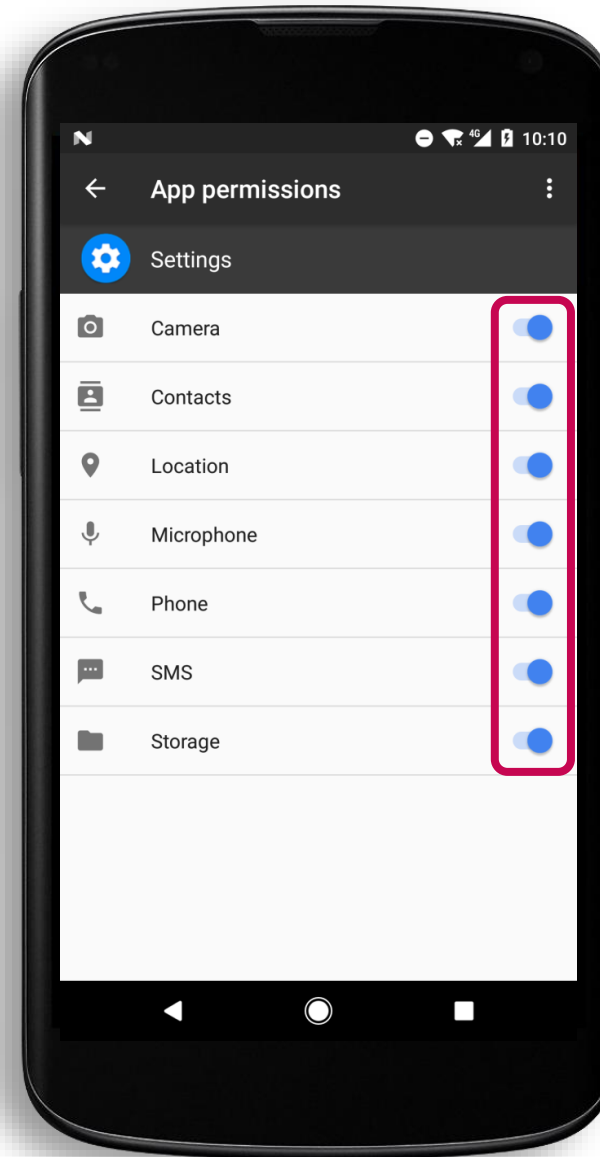
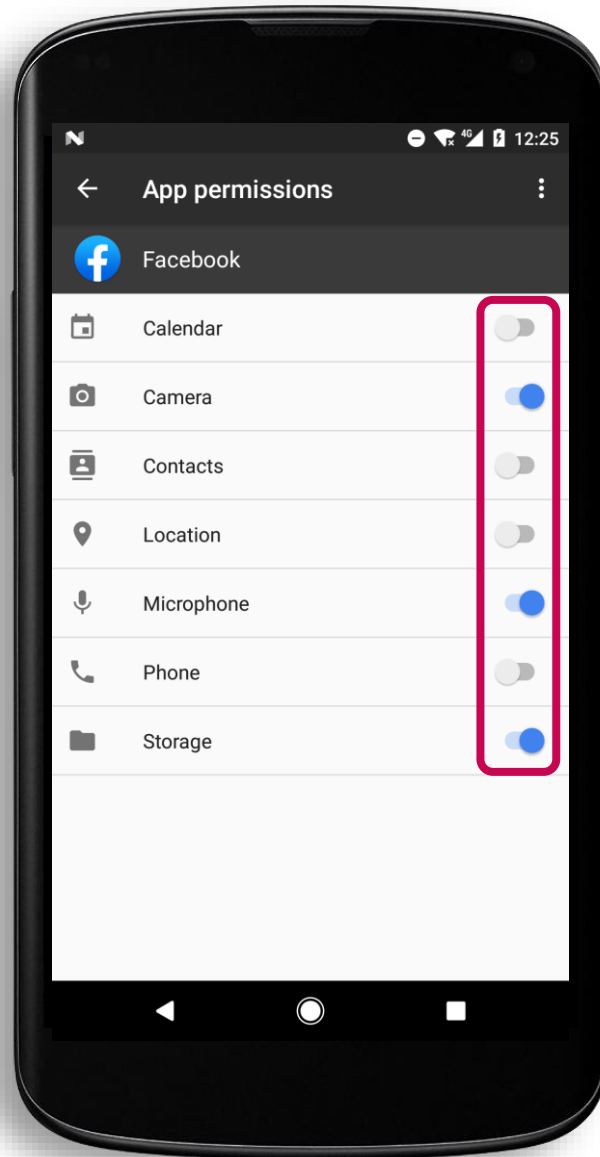
YouTube

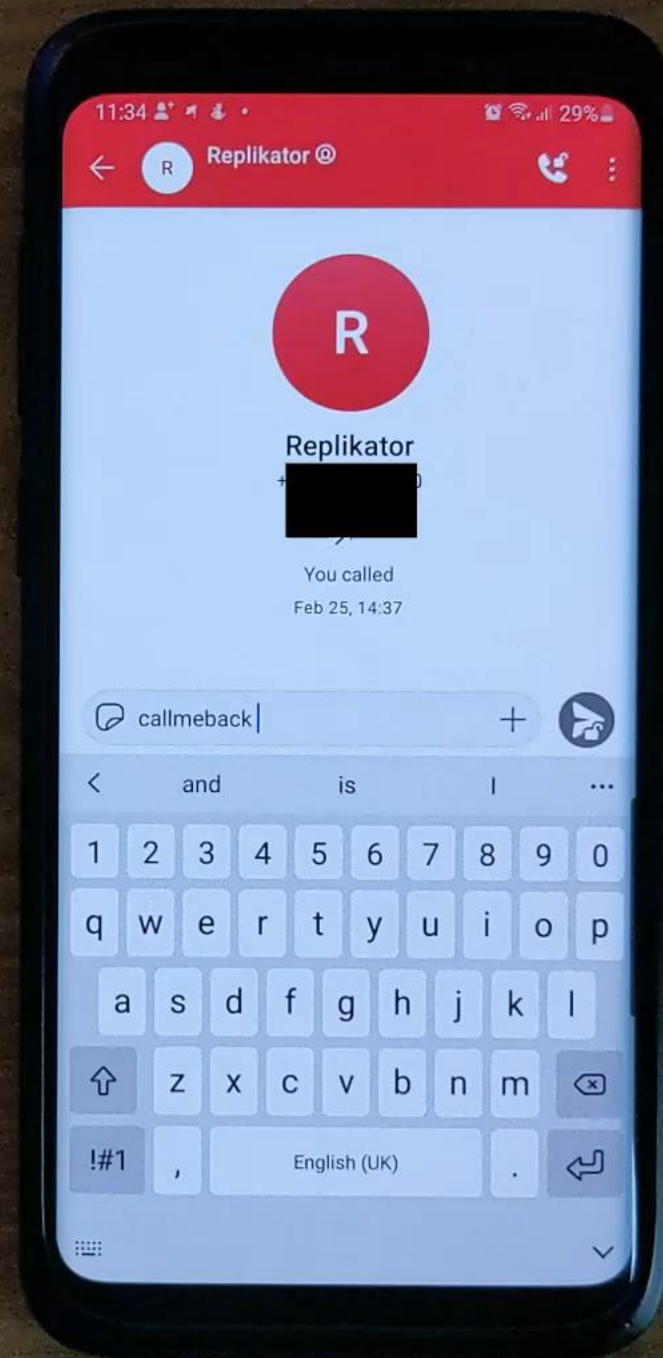


Snapchat



WhatsApp





Stalkerware problems



Security

Vulnerabilities

Data storage

Privacy of paying clients
and their victims



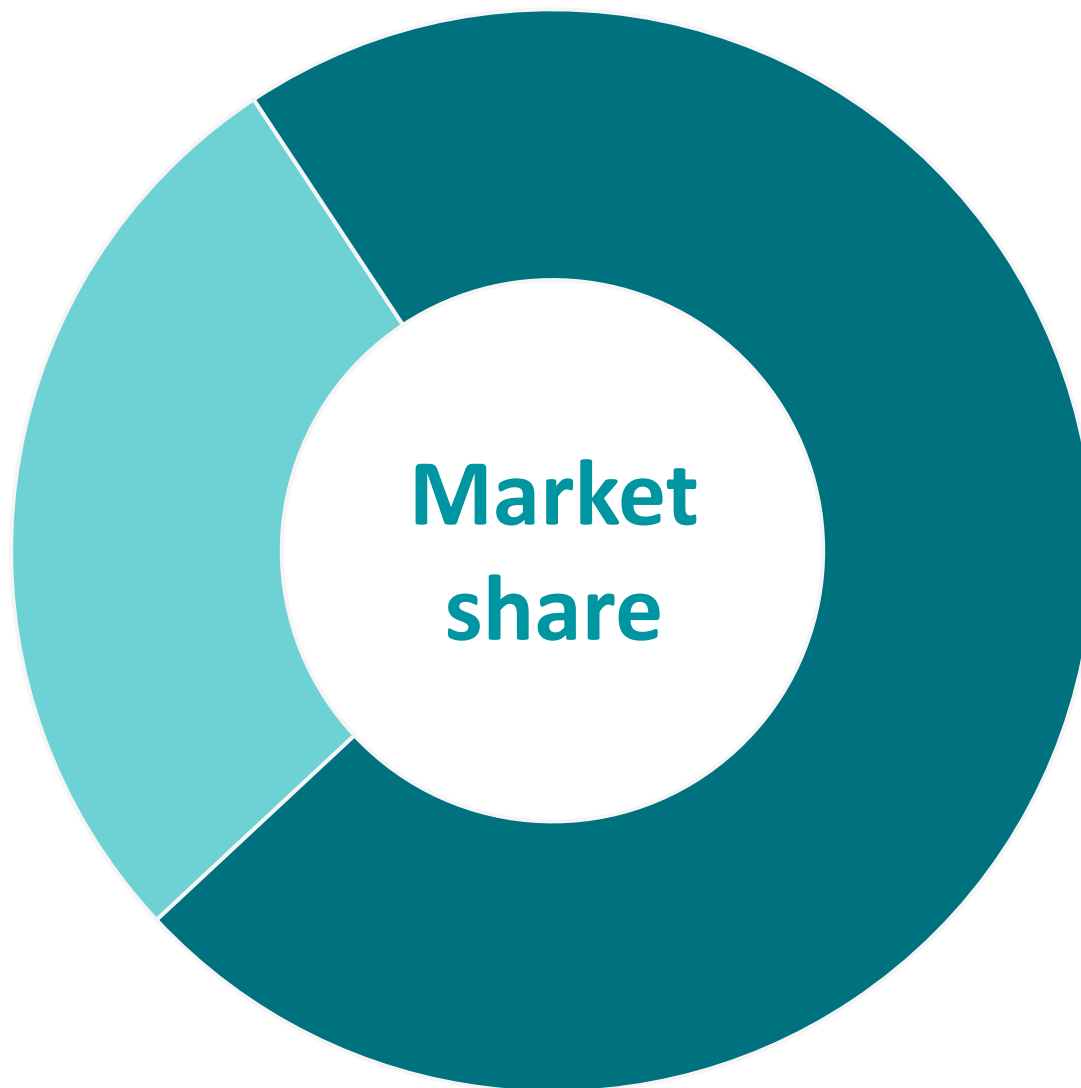
Fixing issues


Source

- Stalkerware Indicators of Compromise
(<https://github.com/Te-k/stalkerware-indicators>)
- Detection from client devices
- Paid advertisement
- Top Google search
- 86 stalkerware vendors

Platform


27,47%
Jailbreak
iCloud credentials

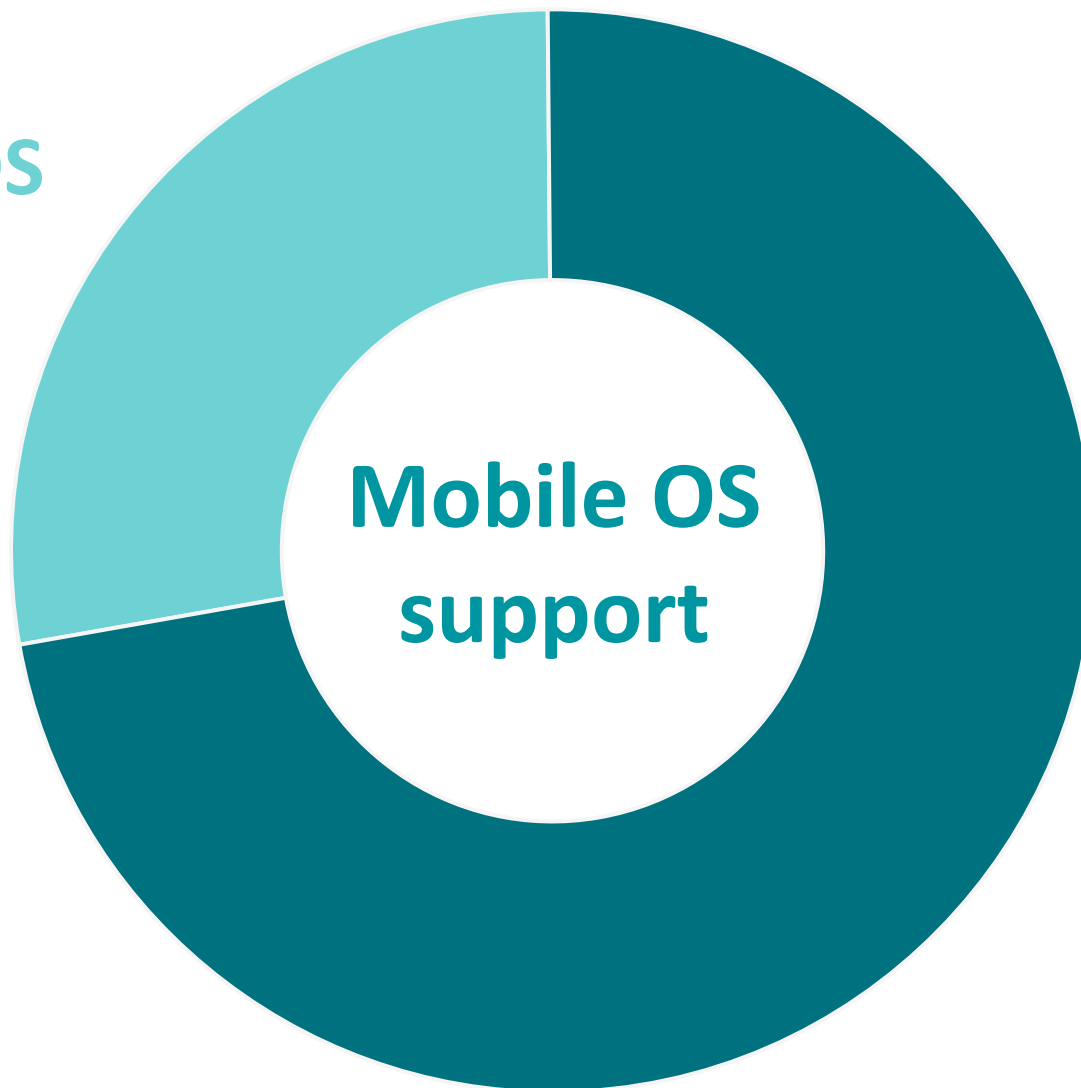



71,93%
Install 3rd
party app

Platform

Android and iOS
37,21%

Android only
62,79%



**Mobile OS
support**

App analysis plan

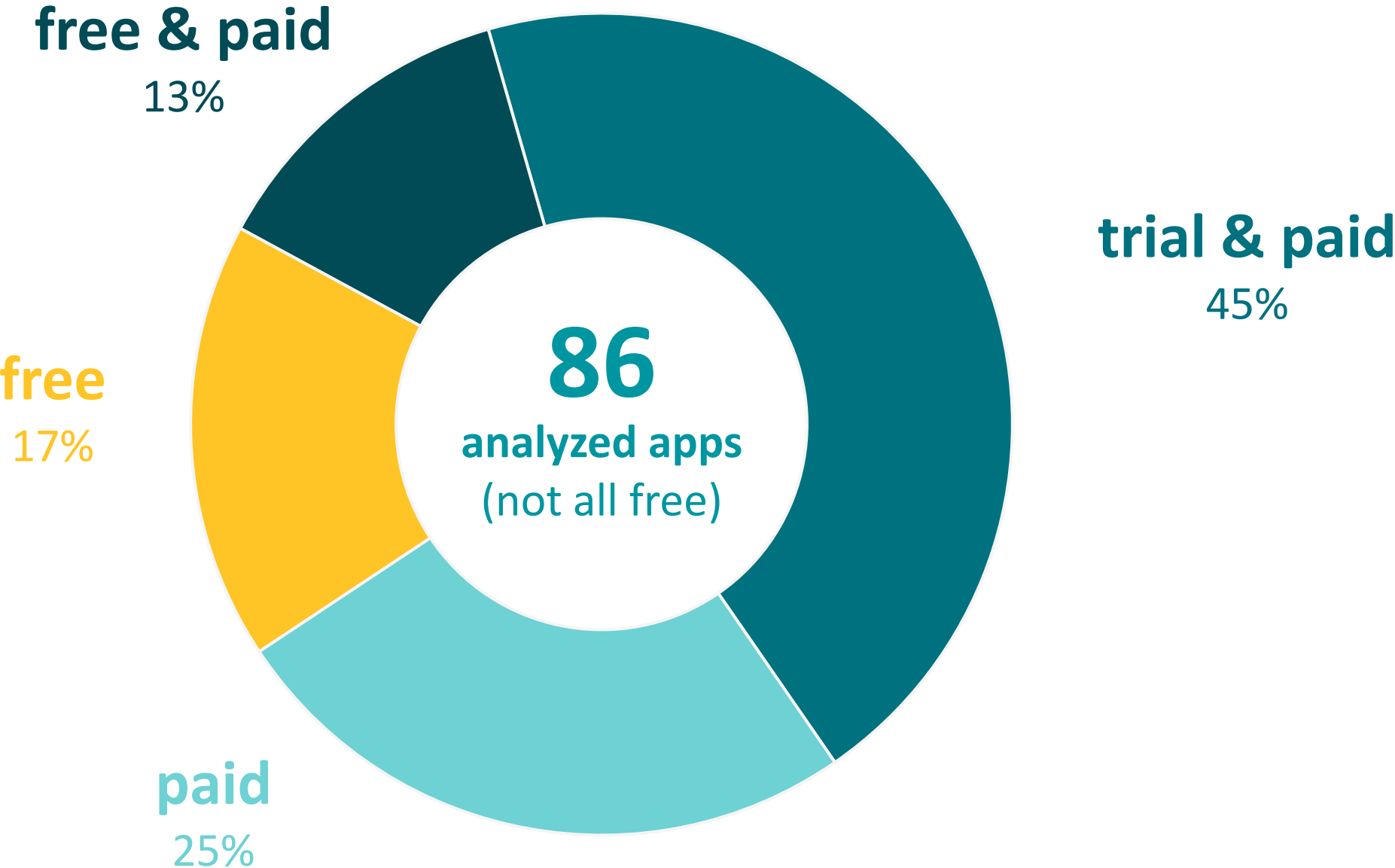
Analyzed 86 stalkerware vendors

Manual static and dynamic analysis

- Security and privacy issues with impact on user or company

Not a full-featured penetration test

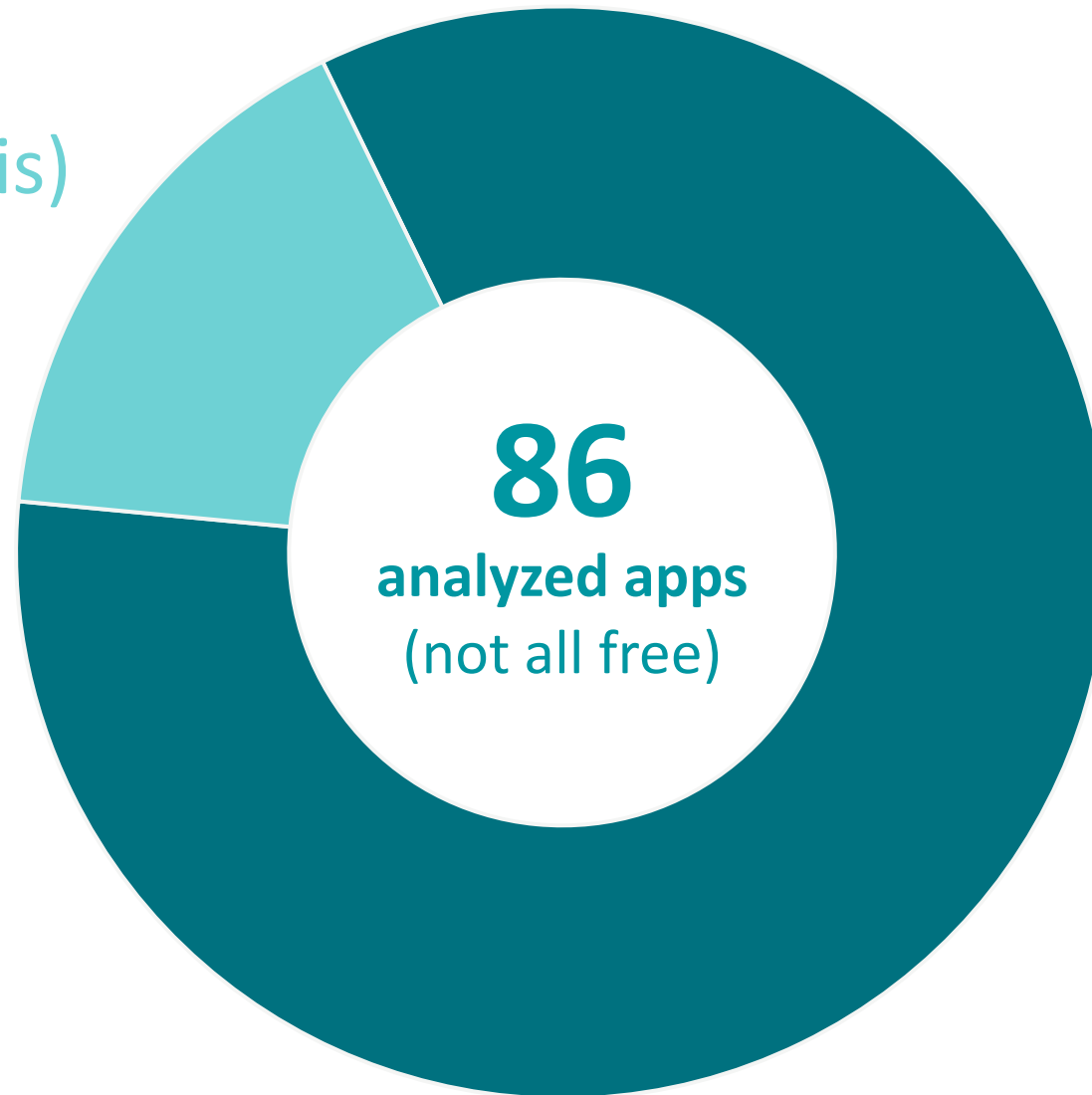
Limitations: Payment model



Limitations: Limited functionality test

limited
(only static analysis)
14

tested
72



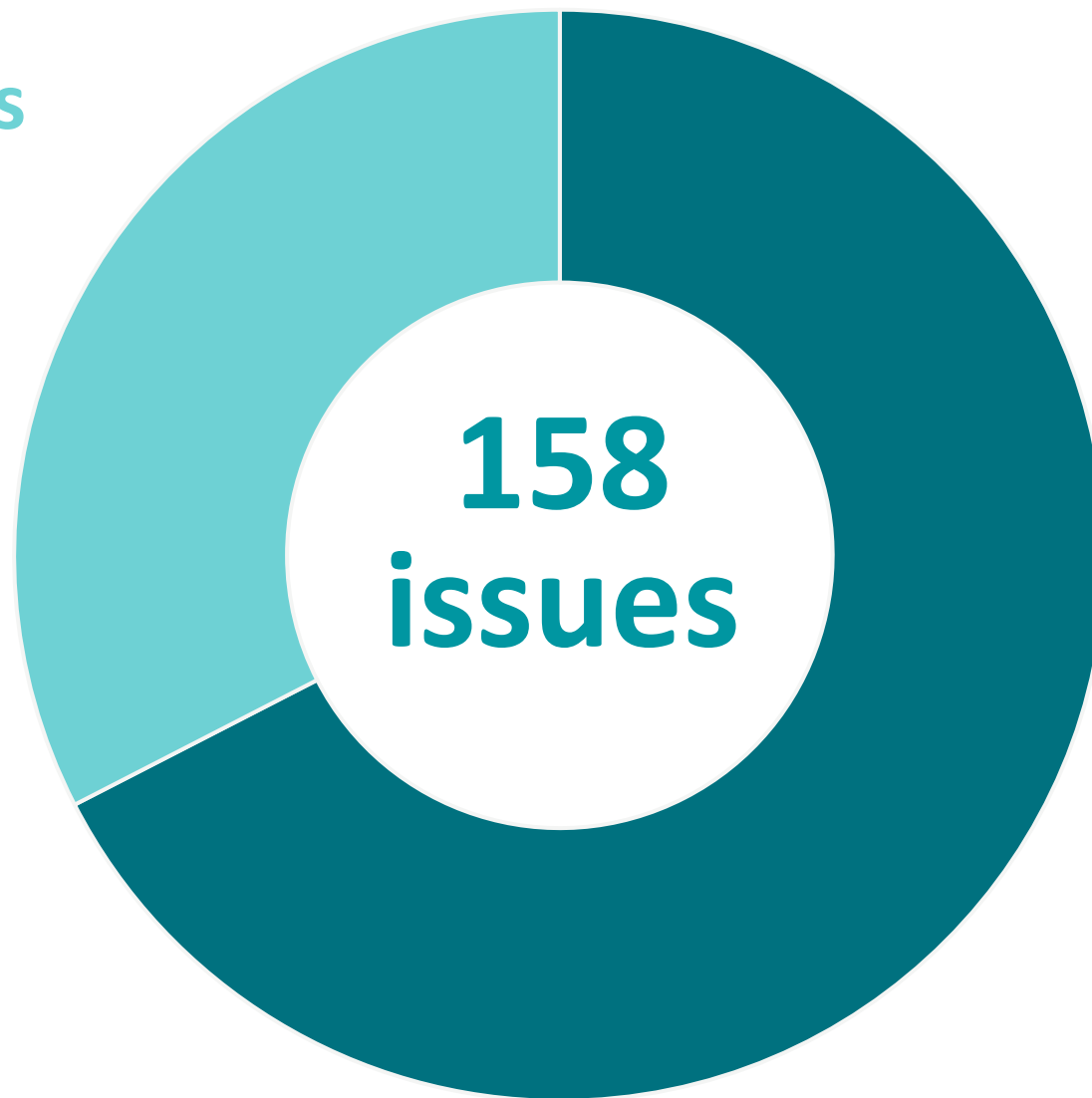
Findings

without issues

33%

with issues

67%

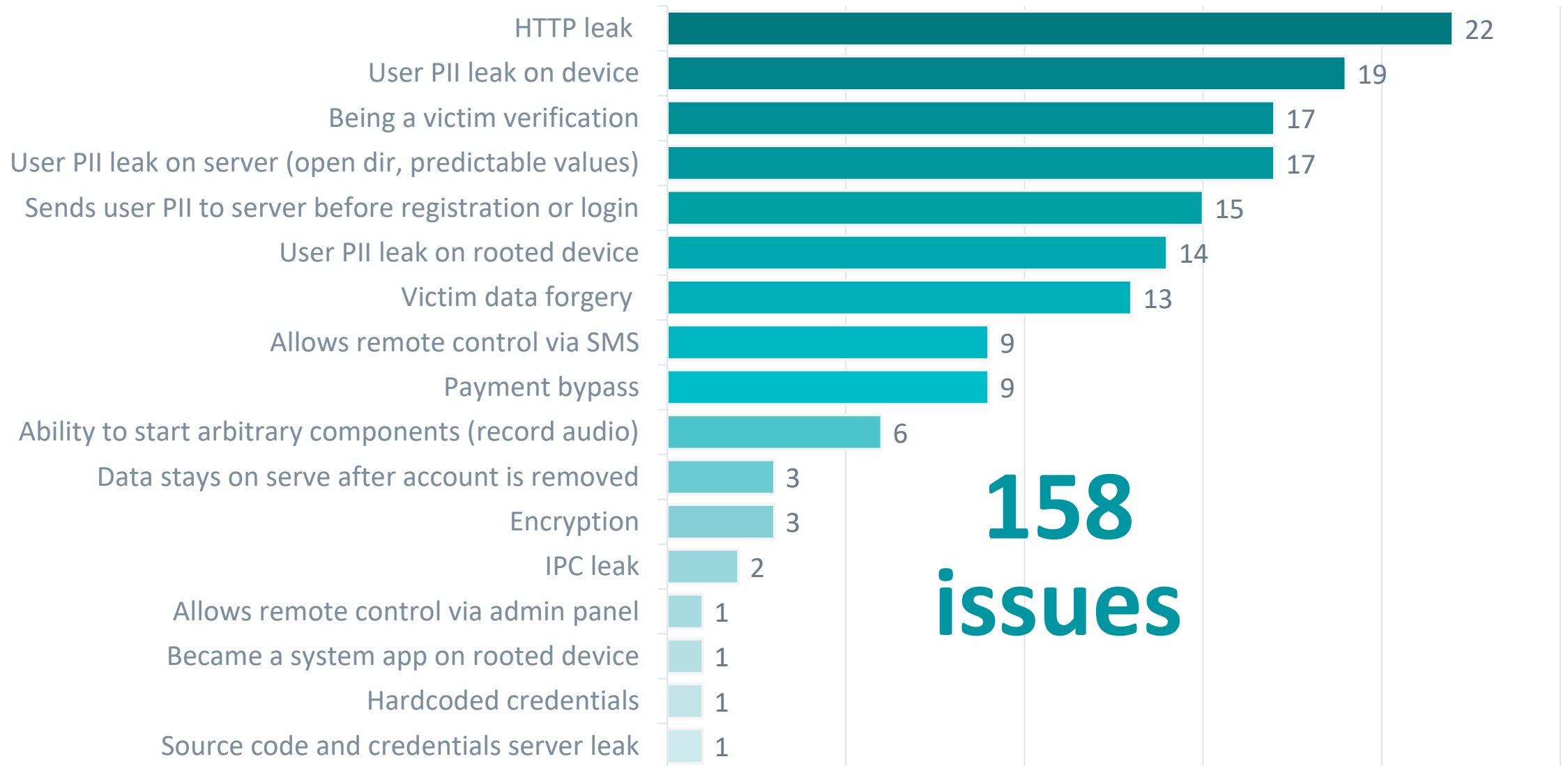


**158
issues**

Security Issues



Security & privacy issues



HTTP leak

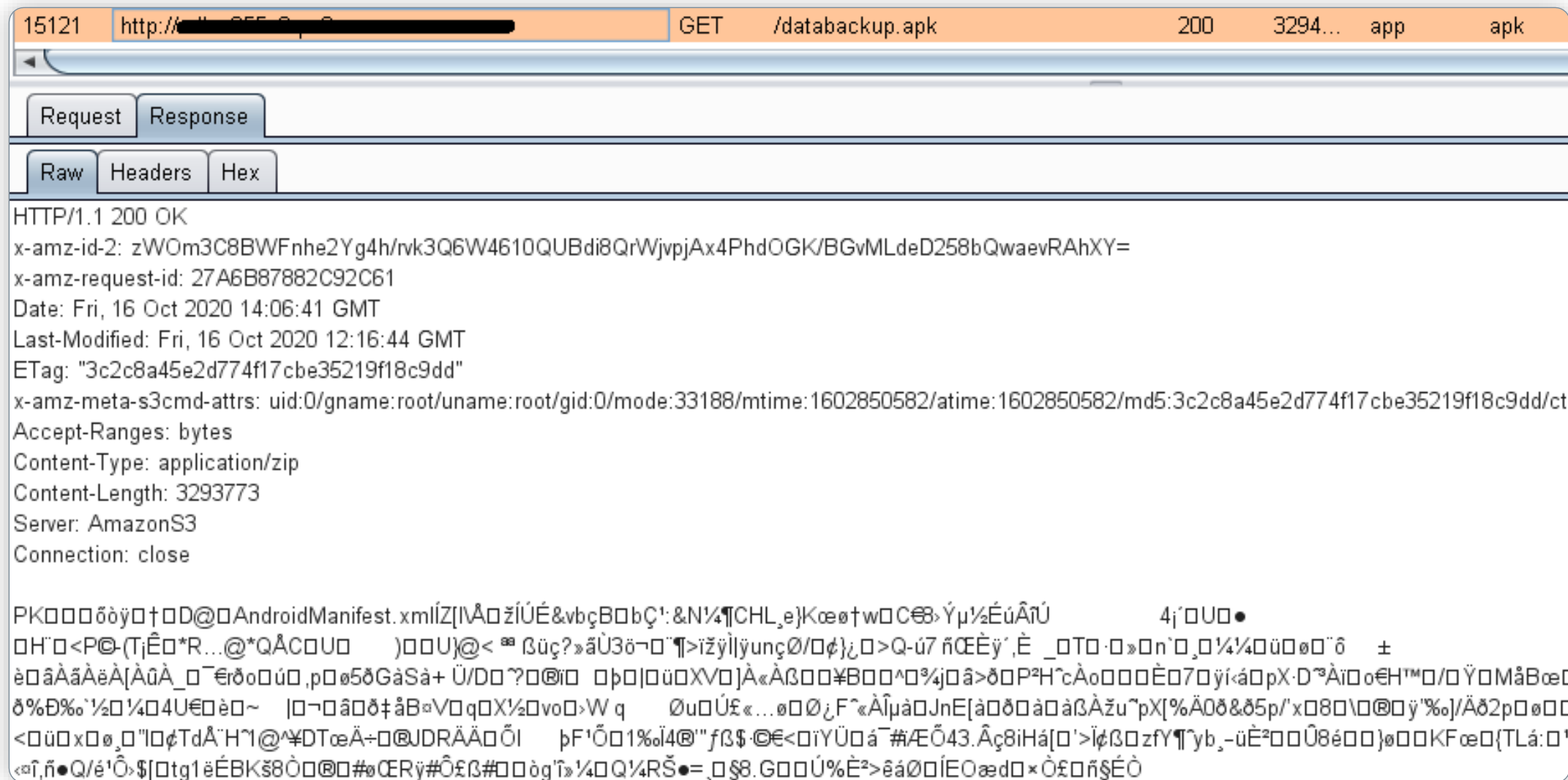
678 http://[redacted] GET /protocols/device_register.aspx?username=lukaste[redacted]@gm... ✓ 200 289

Request Response

Raw Params Headers Hex

GET /protocols/device_register.aspx?username=lukaste[redacted]&password=[redacted]&deviceid=[redacted]&brand_id=2 HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.1.1; Pixel Build/NOF26V)
Host: [redacted]
Connection: close
Accept-Encoding: gzip, deflate

HTTP leak



HTTP leak

39...	http://[REDACTED]	POST	/protocols/log_call_ex.aspx	✓
39...	http://[REDACTED]	POST	/protocols/log_sms_ex.aspx	✓
39...	http://[REDACTED]	POST	/protocols/log_sms_post.aspx	✓
39...	http://[REDACTED]	POST	/protocols/log_sms_post.aspx	✓
39...	http://[REDACTED]	POST	/protocols/log_sms_post.aspx	✓
39...	http://[REDACTED]	POST	/protocols/log_sms_post.aspx	✓
39...	http://[REDACTED]	POST	/protocols/log_sms_post.aspx	✓
39...	http://[REDACTED]	POST	/protocols/log_sms_post.aspx	✓
39...	http://[REDACTED]	POST	/protocols/log_sms_post.aspx	✓
39...	http://[REDACTED]	POST	/protocols/log_sms_post.aspx	✓

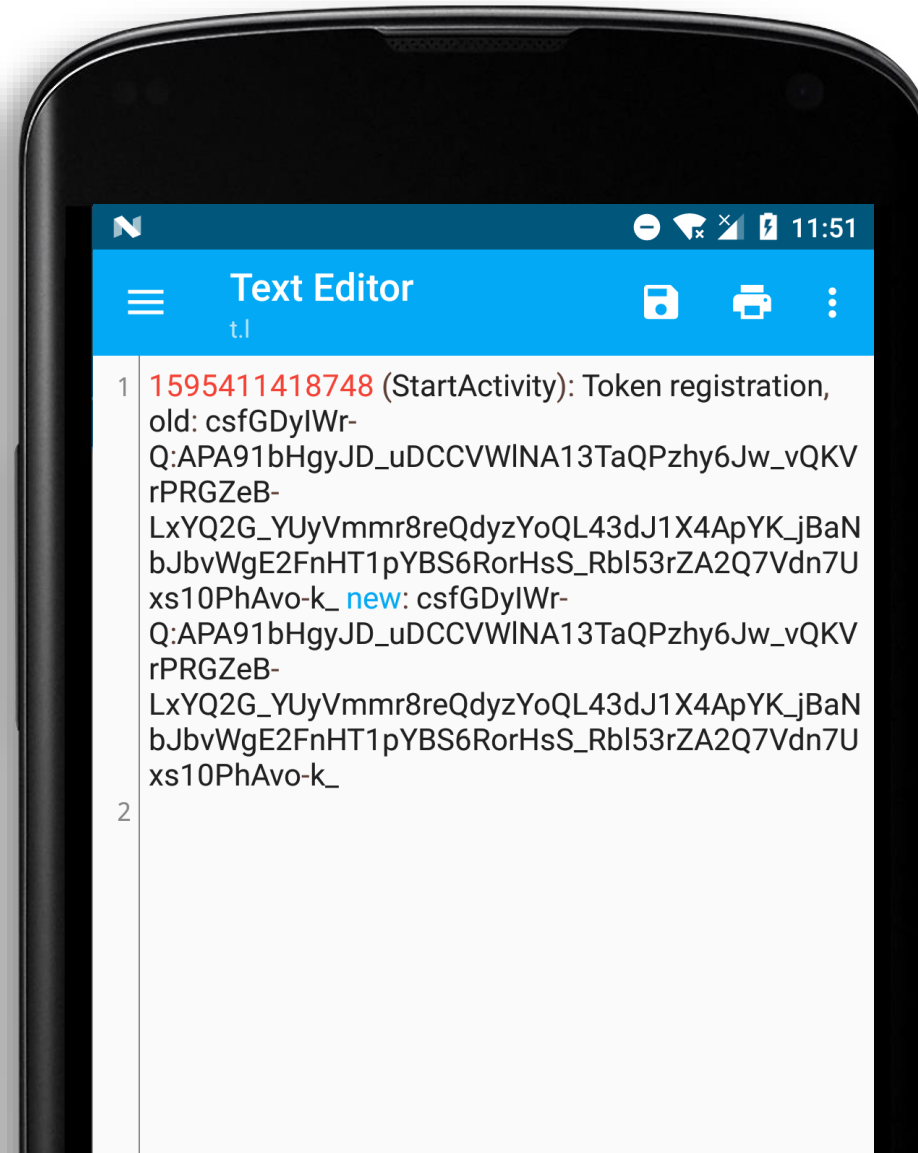
Request Response

Raw Params Headers Hex

POST request to /protocols/log_sms_post.aspx

Type	Name	Value
Body	deviceid	40[REDACTED]6
Body	date	2019-04-07
Body	time	17:38:46
Body	sender	PayPal
Body	receiver	0
Body	direction	1
Body	name	PayPal
Body	message	PayPal: Your security code is: 198419. Your code expires in 5 minutes. Please dont reply.
Body	os	AD
Body	type	0

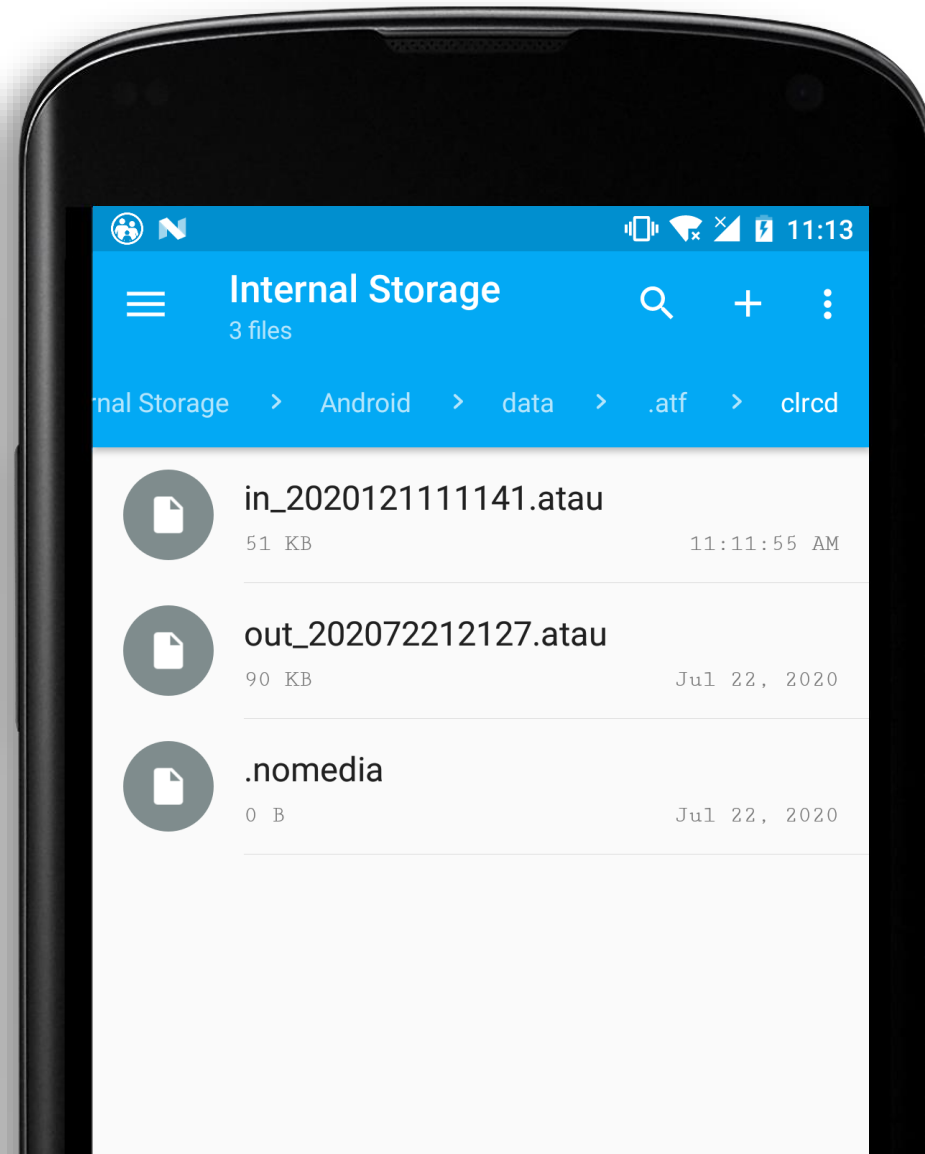
User PII leak on device



User PII leak on device

```
[Password]$com.paypal.android.p2pmobile$1601026221414$1$true  
[.]$com.paypal.android.p2pmobile$1601026222785$1$true  
[p]$com.paypal.android.p2pmobile$1601026222791$1$true  
[p.]$com.paypal.android.p2pmobile$1601026223582$1$true  
[.a]$com.paypal.android.p2pmobile$1601026223589$1$true  
[.a.]$com.paypal.android.p2pmobile$1601026224107$1$true  
[.s]$com.paypal.android.p2pmobile$1601026224132$1$true  
[.s.]$com.paypal.android.p2pmobile$1601026224553$1$true  
[.s.s]$com.paypal.android.p2pmobile$1601026224567$1$true  
[.s.s.]$com.paypal.android.p2pmobile$1601026225292$1$true  
[.w]$com.paypal.android.p2pmobile$1601026225315$1$true  
[.w.]$com.paypal.android.p2pmobile$1601026225526$1$true  
[.o]$com.paypal.android.p2pmobile$1601026225551$1$true  
[.o.]$com.paypal.android.p2pmobile$1601026225744$1$true  
[.r]$com.paypal.android.p2pmobile$1601026225773$1$true  
[.r.]$com.paypal.android.p2pmobile$1601026226167$1$true  
[.d]$com.paypal.android.p2pmobile$1601026226186$1$true  
[.d.]$com.paypal.android.p2pmobile$1601026226669$1$true  
[.1]$com.paypal.android.p2pmobile$1601026226681$1$true  
[.1.]$com.paypal.android.p2pmobile$1601026227142$1$true  
[.2]$com.paypal.android.p2pmobile$1601026227158$1$true  
[.2.]$com.paypal.android.p2pmobile$1601026227605$1$true  
[.3]$com.paypal.android.p2pmobile$1601026227621$1$true
```


User PII leak on device



User PII leak on server

17

apps

11,200

IMEI numbers

3,750+

client emails

182,000

user pictures

1,353,000+

IP logs

167,000+

clients' info

130,000

recorded calls

Victim data forgery

The screenshot displays a network traffic analysis interface. At the top, a list of HTTP requests is shown, all with a status of 39... and a method of POST. The selected request is highlighted in orange. Below the list, the 'Request' tab is active, showing the details of a POST request to /protocols/log_sms_post.aspx. The request body is displayed as a table of key-value pairs.

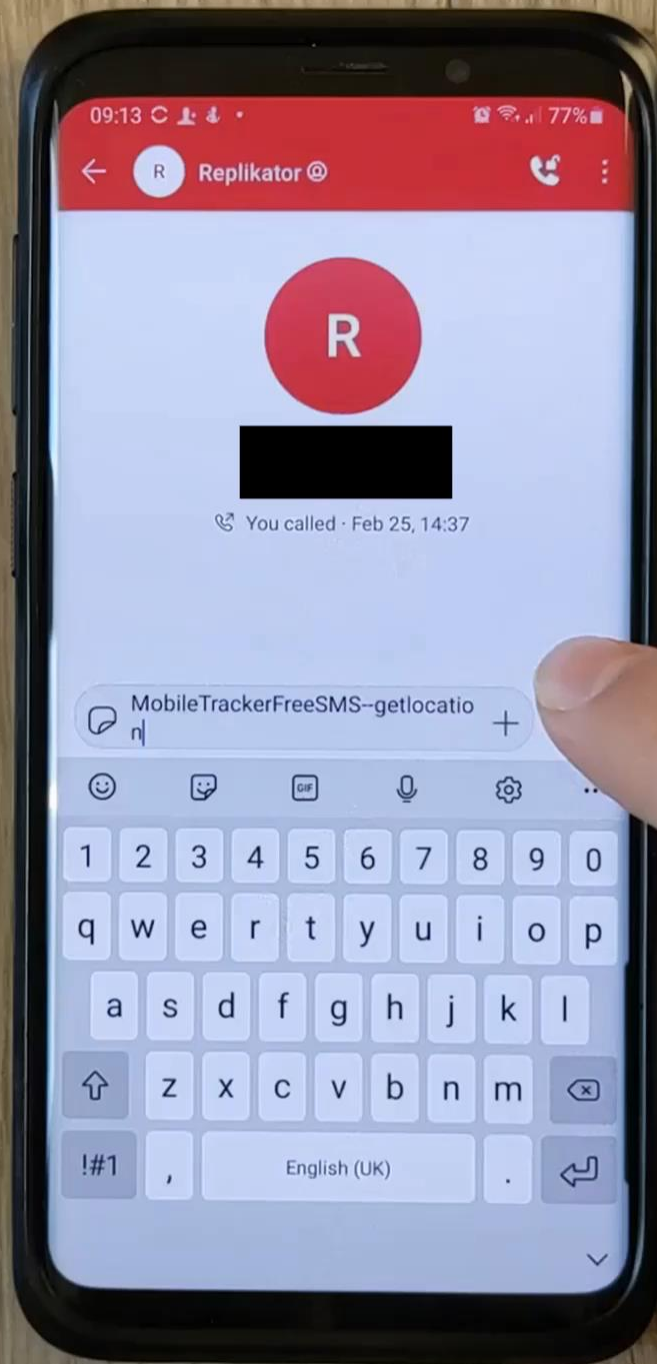
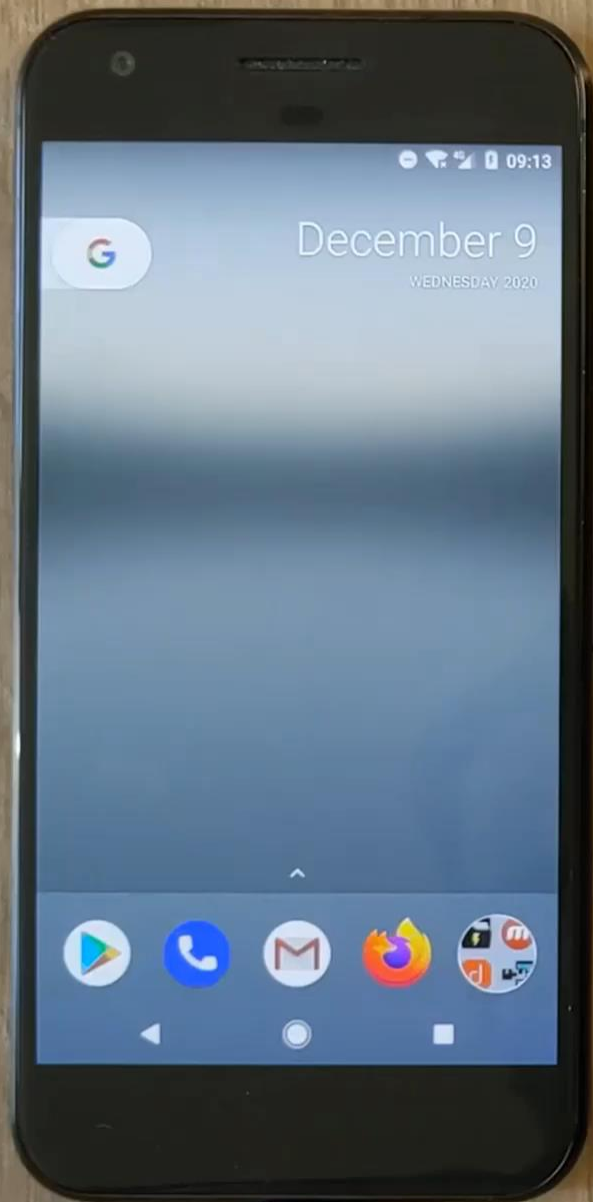
Type	Name	Value
Body	deviceid	40[REDACTED]
Body	date	2019-04-07
Body	time	17:38:46
Body	sender	PayPal
Body	receiver	0
Body	direction	1
Body	name	PayPal
Body	message	PayPal: Your security code is: 198419. Your code expires in 5 minutes. Please dont reply.
Body	os	AD
Body	type	0

Allows remote control via SMS

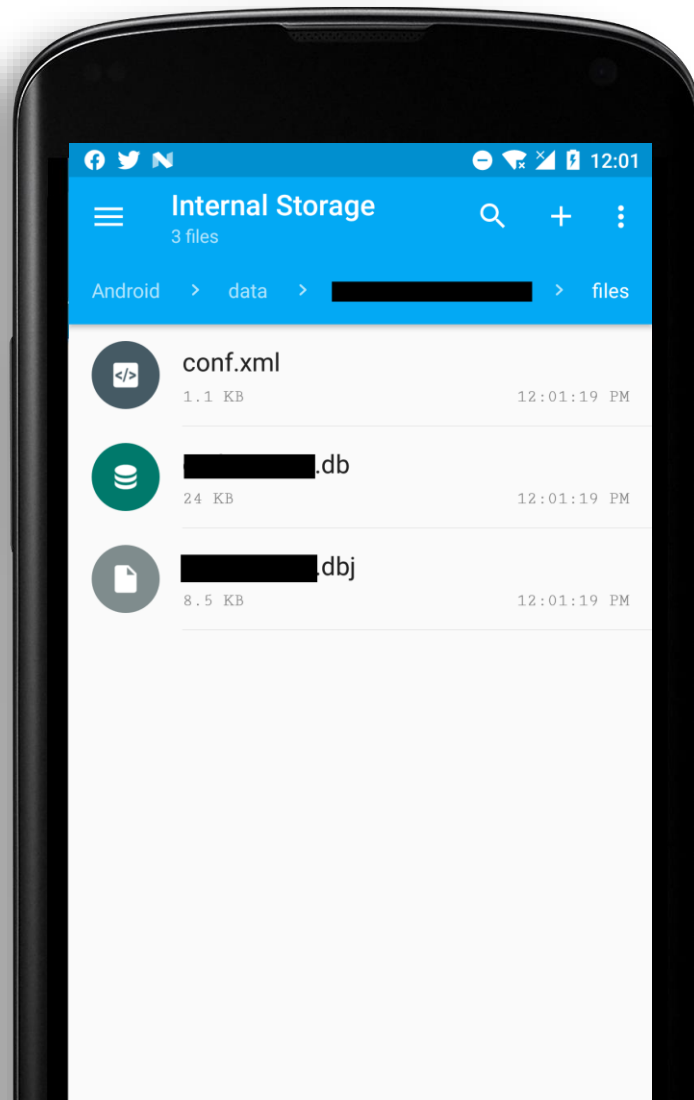


No authorization
without valid license key

Google Pixel	
Restart net command	<input type="text" value="#restartnet"/>
Restart gps command	<input type="text" value="#restartgps"/>
Restart settings command	<input type="text" value="#restartsettings"/>
Take picture	<input type="text" value="#takepic"/>
Record audio	<input type="text" value="#recordaudio"/>
Record audio time	<input type="text" value="10 minutes"/>
Take picture with front camera	<input type="text" value="#takepicfront"/>
List contacts	<input type="text" value="#listcontacts"/>
List apps	<input type="text" value="#listapps"/>
Restart wifi	<input type="text" value="#restartwifi"/>
Start net	<input type="text" value="#startnet"/>
Stop net	<input type="text" value="#stopnet"/>
Stop wifi	<input type="text" value="#stopwifi"/>
Start wifi	<input type="text" value="#startwifi"/>
Start alarm	<input type="text" value="#startalarm"/>
Remote wipe	<input type="text" value="#remotewipe"/>
Lock phone	<input type="text" value="#lockphone"/>
Set silent - ringtone	<input type="text" value="#setsilent"/>
Set vibrate - ringtone	<input type="text" value="#setvibrate"/>
Set normal - ringtone	<input type="text" value="#setnormal"/>
Track location	<input type="text" value="#tracklocation"/>
Last settings change on website	-
Last settings update on the phone	November 19 2020 10:08:24

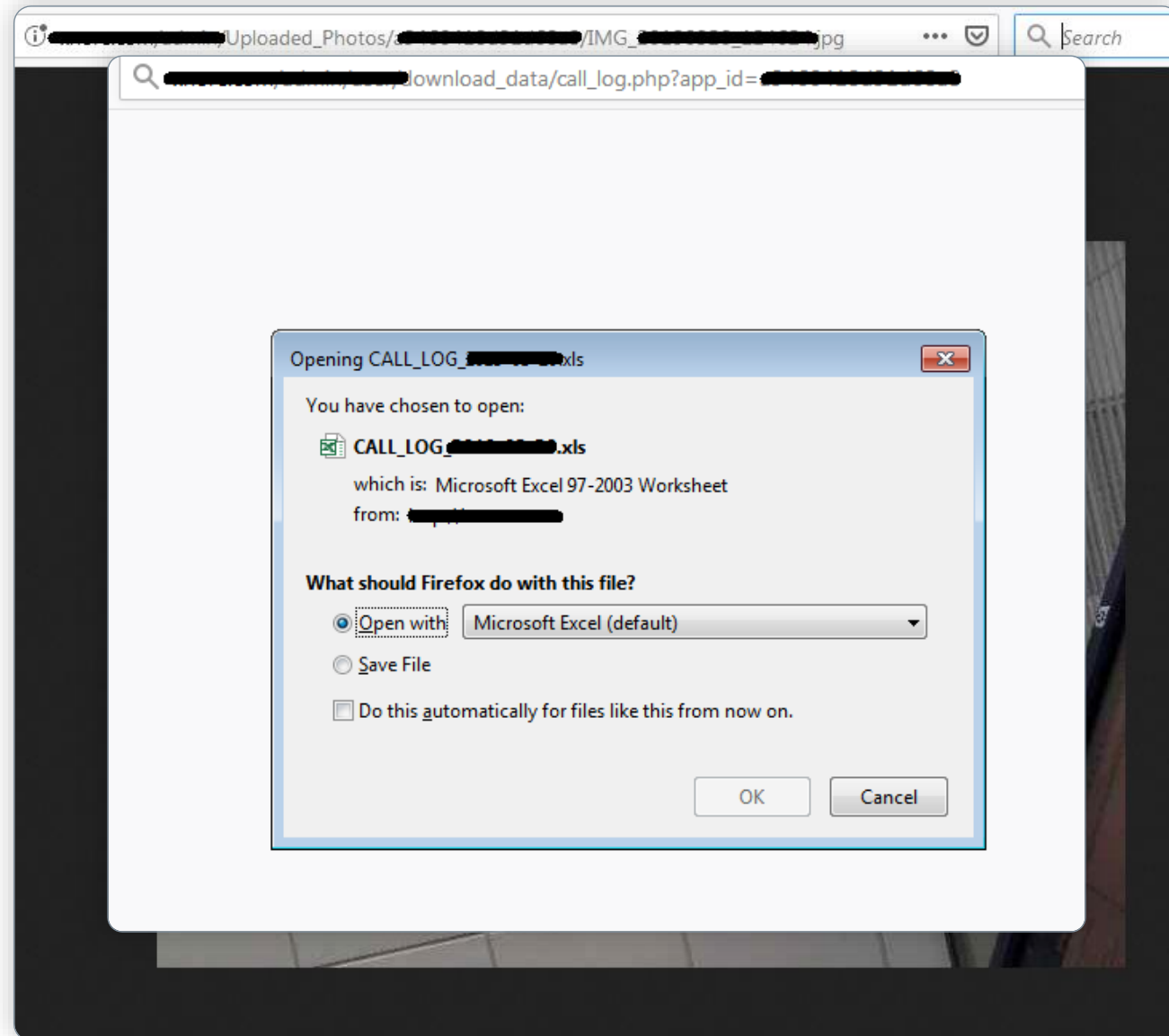


Ability to start arbitrary components



Node	Code
* c.a.a.D.run() void	if (this.f1199c.equals("arecord_settings")) {
● c.a.a.D.run() void	if (this.f1199c.equals("read_calls")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("read_sms")) {
● c.a.a.D.run() void	if (this.f1199c.equals("interval_send")) {
● c.a.a.D.run() void	if (this.f1199c.equals("enable_wifi")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("disable_wifi")) {
● c.a.a.D.run() void	if (this.f1199c.equals("enable_gprs")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("disable_gprs")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("erase_sd_card")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("disable_verify_apps")) {
● c.a.a.D.run() void	if (this.f1199c.equals("check_verify_apps")) {
● c.a.a.D.run() void	if (this.f1199c.equals("hide")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("unhide")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("find")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("app_list")) {
● c.a.a.D.run() void	if (this.f1199c.equals("enable_gps")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("disable_gps")) {
● c.a.a.D.run() void	if (this.f1199c.equals("arecord_start")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("arecord_stop")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("media_send")) {
● c.a.a.D.run() void	if (this.f1199c.equals("content_send")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("command_send")) {
● c.a.a.D.run() void	if (this.f1199c.equals("take_photo2")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("take_photo50")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("take_photo")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("call_password")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("call_record_type")) {
● c.a.a.D.run() void	if (this.f1199c.equals("register_gcm")) {
● c.a.a.D.run() void	} else if (this.f1199c.equals("register_fcm")) {

Data stays on server after account is removed



Hardcoded secrets



Allows stalker to secretly
livestream from device

Report





90

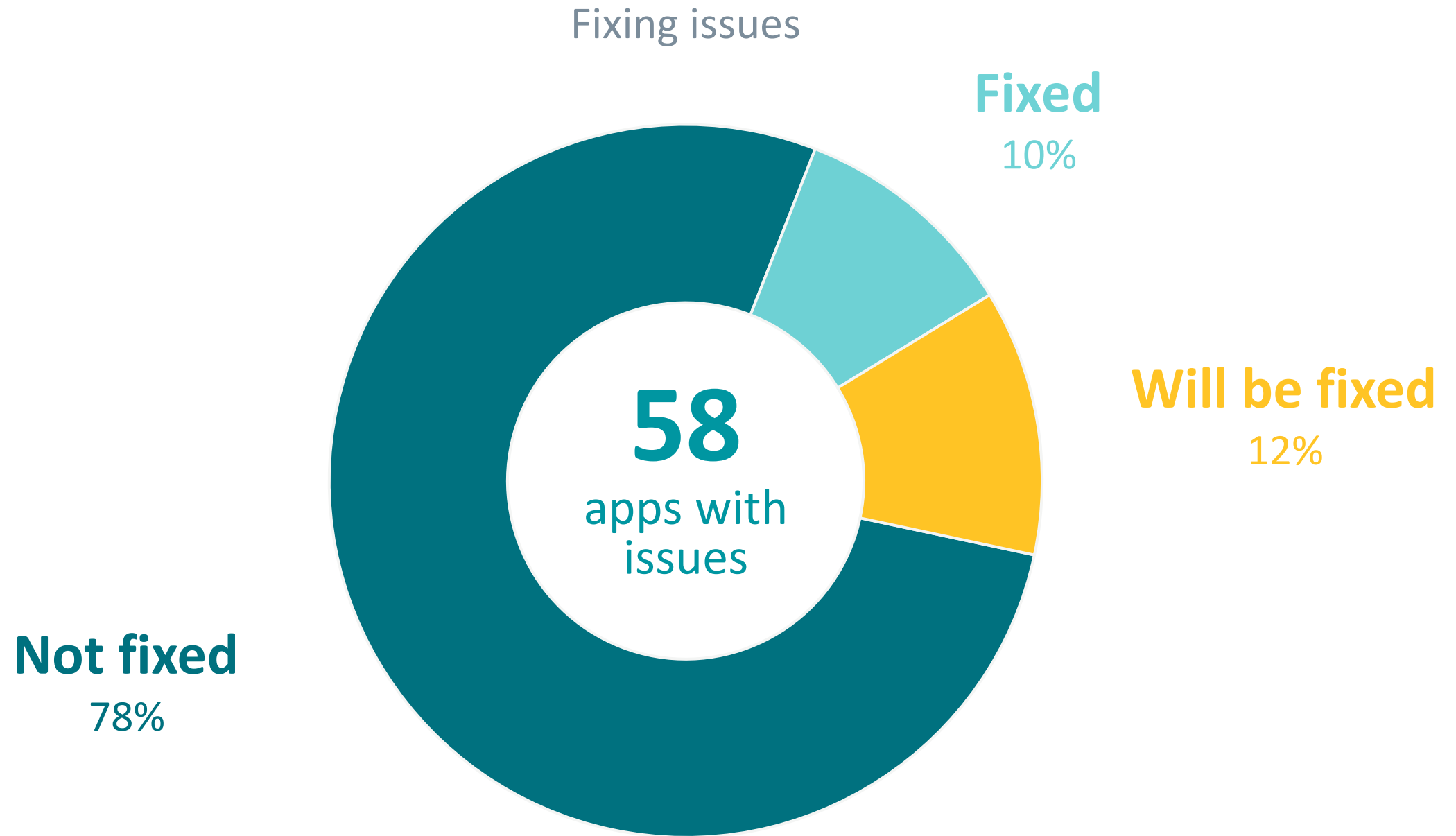
90-day
disclosure
period

3

Up to
three notifications
Email, support ticket

2

In **two cases**
couldn't reach
vendors



Conclusion



Compromise scenario

- ① Physical access to device
- ② Knows lock screen PIN
- ③ Manually side load app

Compromise scenario

- ① Physical access to device
- ② Knows lock screen PIN
- ③ Manually side load app

Prevention tips

- ✓ Don't share PIN
- ✓ Scan device with trustworthy security solution

Compromise signs

- Battery drains faster
- Higher internet consumption
- GPS, Wi-Fi or mobile data enabled by itself
- Suspicious persistent notification in notification bar
- Photos, screenshots or audio recording stored in the smartphone not made by user
- Received questionable text messages

Summary

- Number of used stalkerware apps is increasing (our data)
- They gather and store more data about user than other apps
- Many of them have security issues
- Vendors are not willing to fix them



THANK YOU

