

# Haben Androiden Alpträume?

Wie Malware Mobilgeräte  
kompromittiert



# Unsere Themen



Formen von  
Android Malware



Einblicke in  
Hydra



Einblicke in  
Octo

# Formen von Android Malware





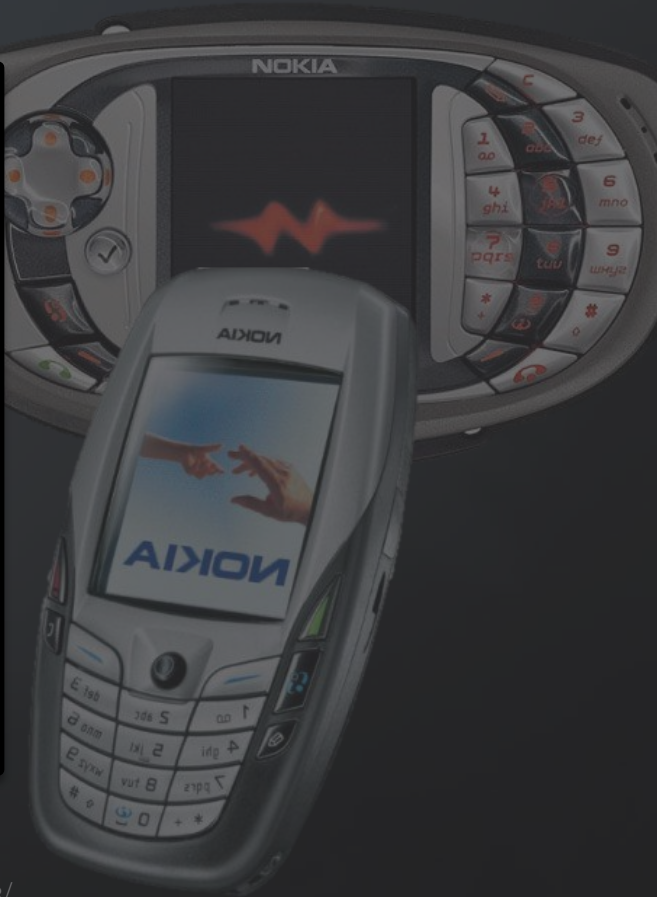
<https://www.kaspersky.co.uk/blog/cabir-10/4168/>



12:00  
W9 01/01/2006

**Coribe-V2/29a** !

OK



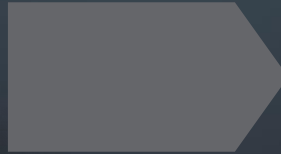
# Cabir – 2004





<https://apkpure.com/>

<https://github.com/Zimperium/DarkHerring>



Laki is a subscription service that will be automatically renewed daily. By completing the subscription flow, you will agree on the below terms and conditions:

- 2 EGP per day for Vodafone , Etisalat and Orange subscribers (auto renewal)
- You will start the paid subscription after the free period automatically

- No commitment, you can cancel your subscription at any time by sending STOP 2301 to 7785 for Vodafone , STOP 3293 to 7786 for Etisalat and for Orange to unsubscribe click [here](#)

- To get support, please contact [vasshelpdesk@gmail.com](mailto:vasshelpdesk@gmail.com)

- To make use of this service, you must be older than 18 years old or have received permission from your parents or person who is authorized to pay your bill

[Terms & Conditions](#)  
[Privacy Policy](#)



# Slimy - ASMR Schleim Spiele

WHOOSH VIDEO CONFERENCING LIMITED

Enthält Werbung · In-App-Käufe

3,2★  
19.700 Rezensionen

1 Mio.+  
Downloads

USK ab 0 Jahren



Installieren



Über diese App →

Stresst Sie das Leben? Slimy ist die perfekte App für Sie, um Ihre Sinne zu erfreuen. Genießen Sie über hundert ASMR-Antistressgeräusche und Schleimspiele, die Sie beruhigen sollen. Tauchen Sie mit uns in ein Sinnesparadies ein, um Körper und Geist zu erfrischen.

Slimy ist der beste Schleimsimulator mit vielen ASMR-Auslösern. Verwenden Sie die App, wenn Sie sich auf Prüfungen vorbereiten, sich gestresst fühlen oder etwas Neues lernen möchten. Diese A...

Aktualisiert am  
08.02.2022

Version  
2.5.10

Aktualisiert am  
08.02.2022

Erforderliche Android-Version  
5.0 oder höher

Downloads  
1.000.000+ Downloads

**In-App-Käufe**  
0,79 € bis 74,99 € pro Artikel

Freigabe  
ab 0 Jahren [Weitere Informationen](#)

[Details ansehen](#)

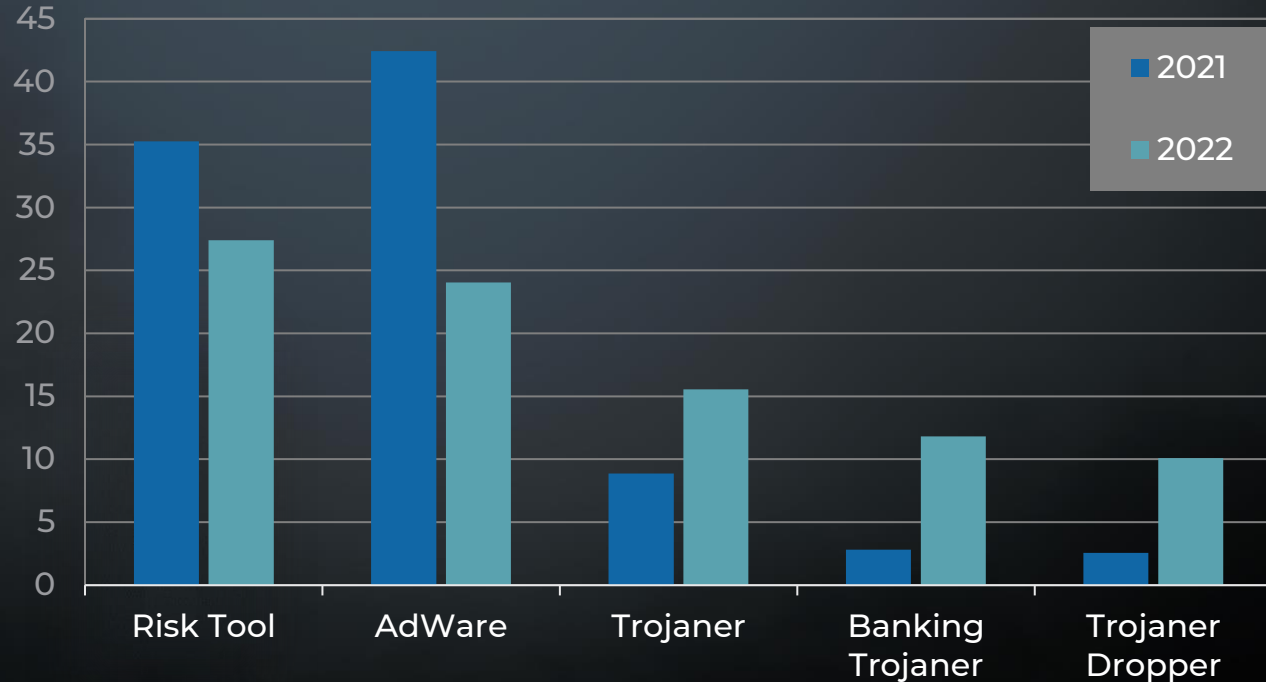
Aktive Elemente  
In-App-Einkäufe

Veröffentlichungsdatum  
05.03.2019

Angeboten von  
Google Commerce Ltd

# Formen mobiler Malware

% der analysierten  
Malware-Samples



# Einblicke in Hydra







eBayMob...



YouTube



Photos



Clock



Gmail



Android ...



Calculator



Calendar



Camera



Chrome



Clock



Contacts



Drive



eBayMob...



Files



Firefox



Gmail



Google



Google TV



Maps



Messages



Phone



Photos



Play Music



Play Store



Privacy O...



ProxyDroid



Safety



Settings




Settings





← Accessibility  

DOWNLOADED APPS

 eBayMobile  
Off

SCREEN READERS

 Select to Speak  
Off / Hear selected text

 TalkBack  
Off / Speak items on screen



Text-to-speech output

DISPLAY

Font size  
Default

Display size  
Default

Dark theme

 Magnification  
Off

# Einblicke in Octo





User ID

Password

Login





User ID

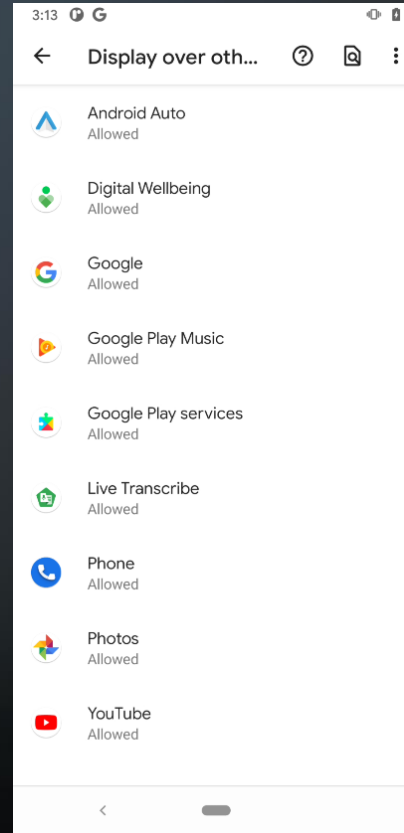
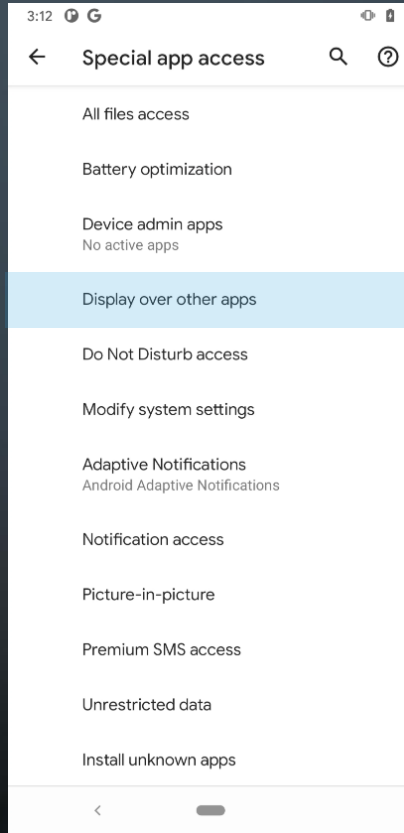
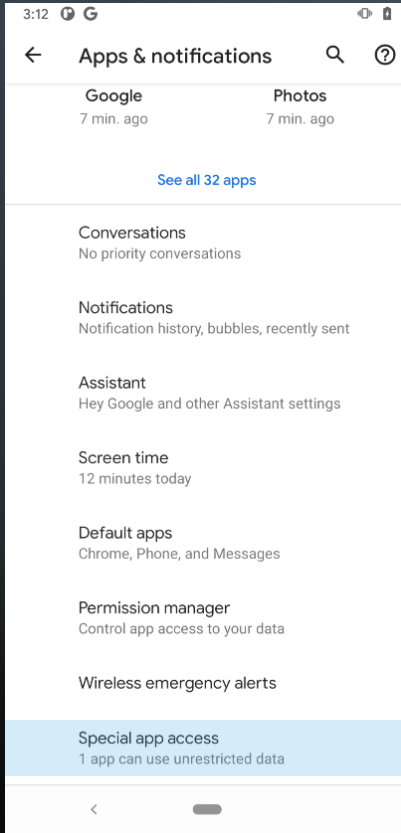
Password

Login

User ID

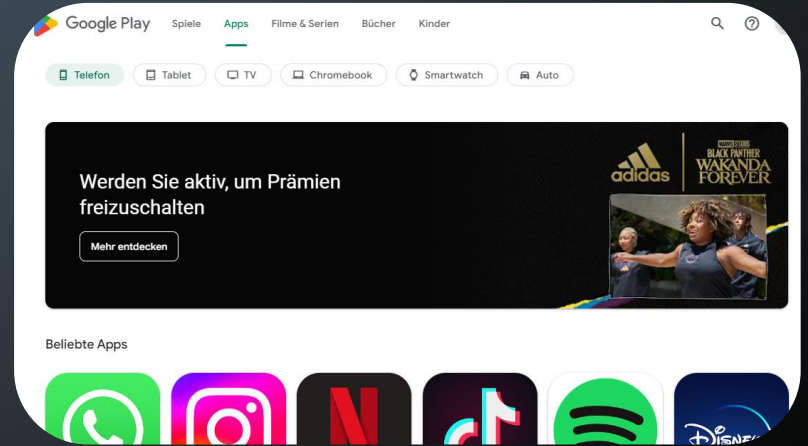
Password

Login



# Wie infizieren sich Geräte?

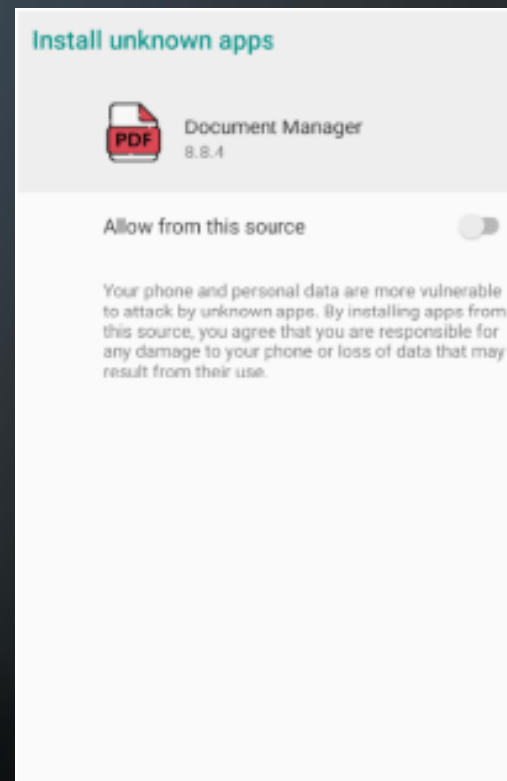
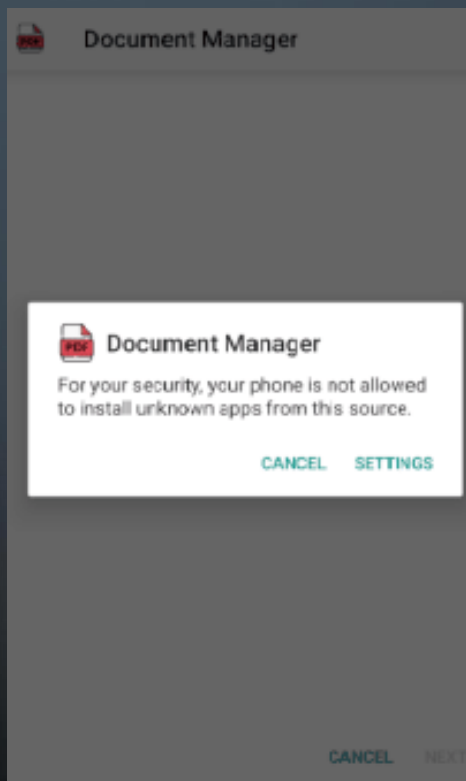
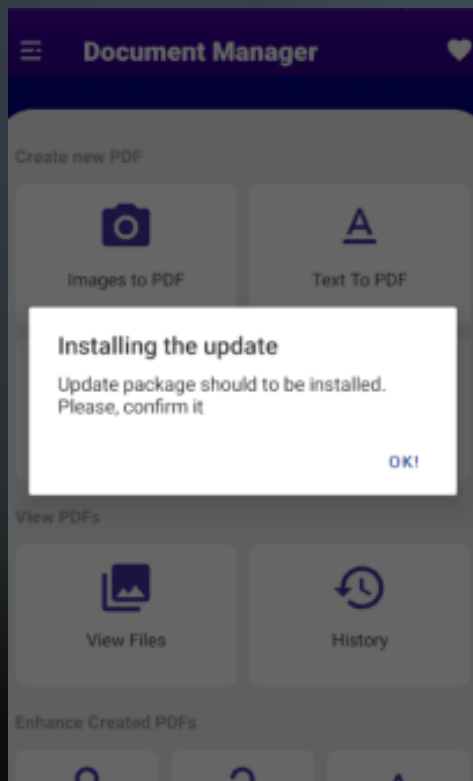
https://www.rnd.de/





AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
2 <manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="111"
7   <uses-sdk android:minSdkVersion="26" android:targetSdkVersion="30" />
11  <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
12  <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
13  <uses-permission android:name="android.permission.INTERNET" />
14  <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
15  <uses-permission android:name="android.permission.REQUEST_INSTALL_PACKAGES" />
```



Das Kleingedruckte lesen

In-App-Kosten prüfen

Android-Geräte updaten

Accessibility Services meiden

App-Berechtigungen prüfen

Installation von unbekanntem  
Quellen nicht erlauben



# Fragen?



Kommen Sie gerne auf mich zu!  
[claudia.ully@nviso.eu](mailto:claudia.ully@nviso.eu)