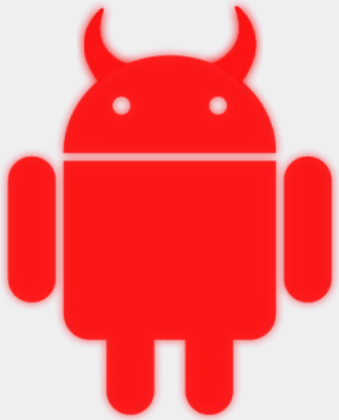
Task Hijacking auf Android-Phones

Patrick Brenner - Spezielle Themen mobiler Kommunikationssysteme - 02.02.2021

Motivation

75%
aller mobilen Geräte weltweit



500
der 500 meist verbreiteten Apps sind durch StrandHogg angreifbar

84%
aller Malware-Attacks auf Android

2015
USENIX Veröffentlichung über Android-Task Hijacking

414
"Schwerwiegende" Schwachstellen in 2019

Bildquelle: [1]
Quellen: [2], [3], [4], [5], [8]

Agenda

01 Security auf Smartphones

02 Task Hijacking bei Android

03 StrandHogg & StrandHogg 2.0

04 Gegenmaßnahmen

05 Fazit und Ausblick

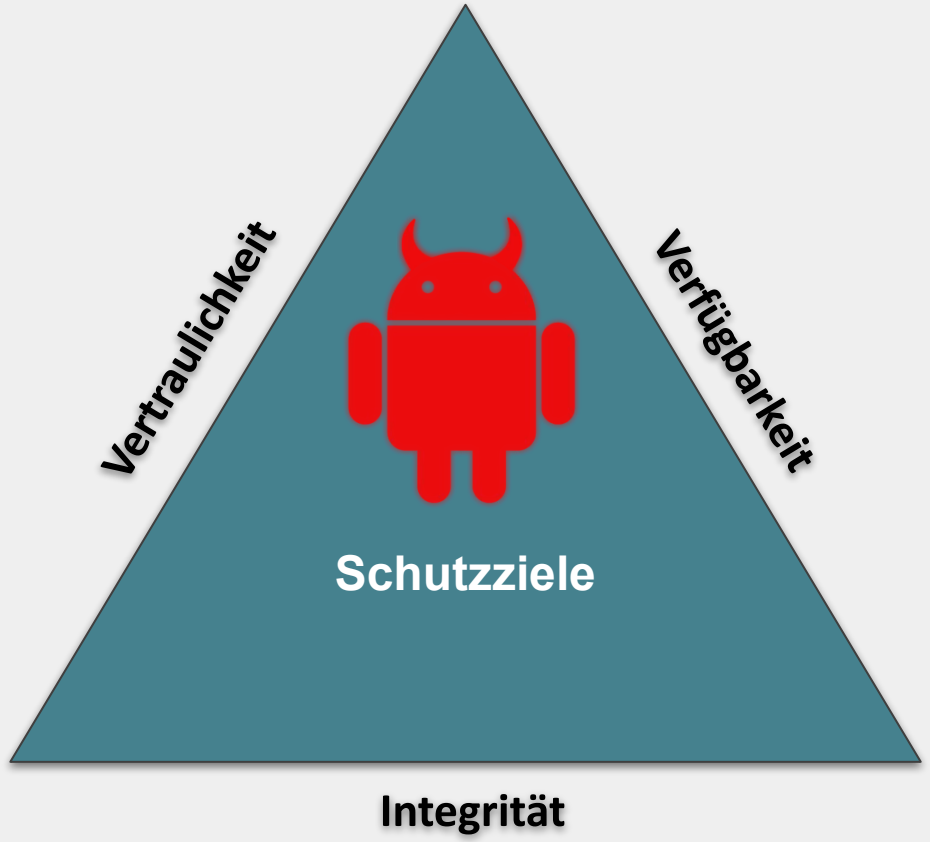
01 Security auf Smartphones

Security auf Smartphones

Schwachstelle
(Common Vulnerabilities and Exposures)

Bösartige Anwendung
(Malware)

Bedrohung
(Phishing, Denial of Service,
Permissions-Escalation)

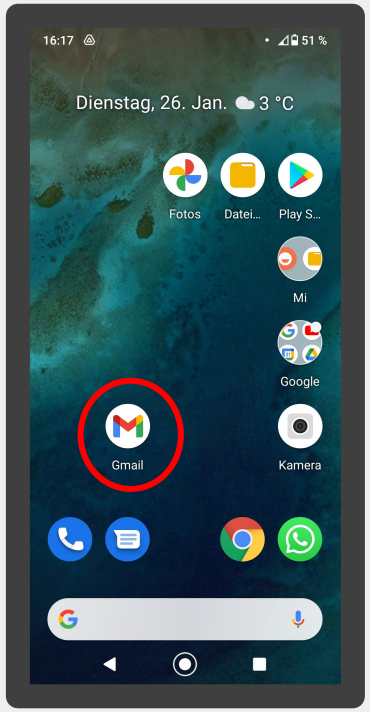


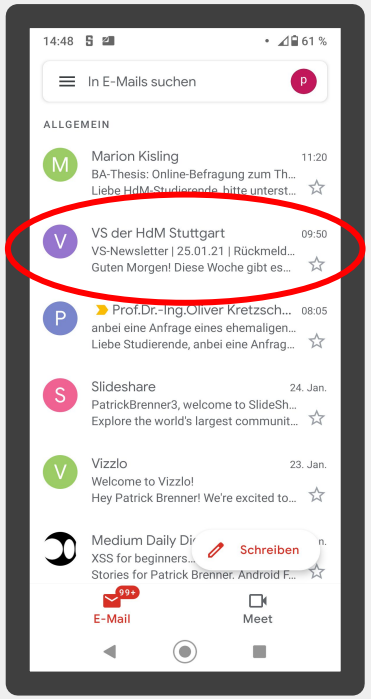
Bildquelle: [1]
Quelle: [3]

02

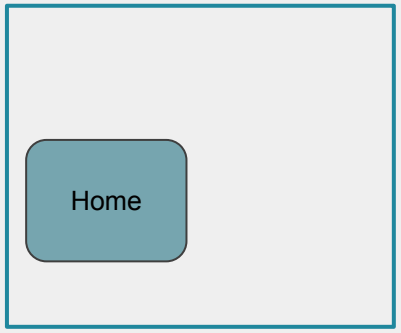
Task Hijacking bei Android

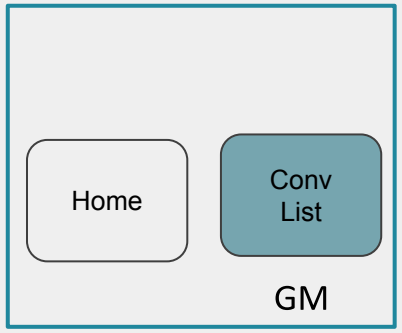
Android Multitasking

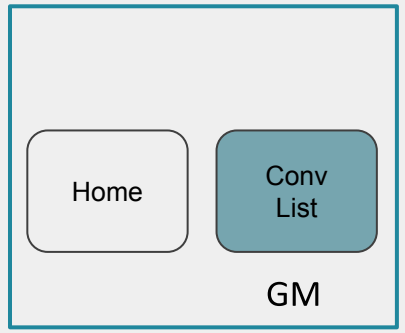


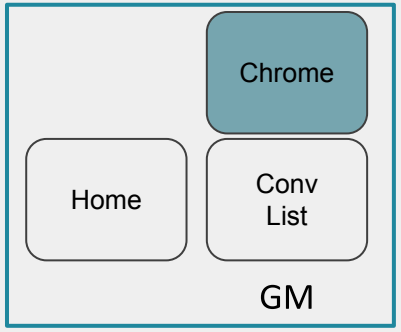


Task State





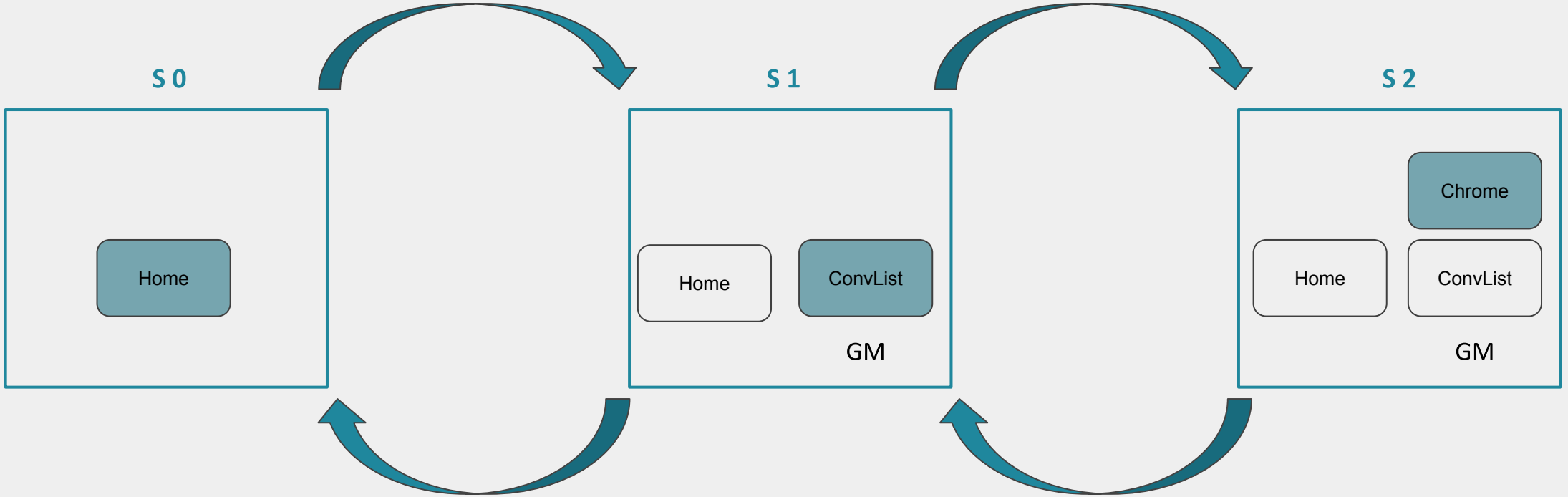




Tasks State Transition Model

$$T1 : (S_0, S_1, e^{Home:startActivity(ConvList)}, \gamma^{default})$$

$$T2 : (S_1, S_2, e^{ConvList:startActivity(CustomTab)}, \gamma^{default})$$



$$T4 : (S_1, S_0, e^{back}, \gamma^{default})$$

$$T3 : (S_2, S_1, e^{back}, \gamma^{default})$$

Quelle: [2]

Manifest.xml

```
<activity
    android:name="CustomTabActivity"
    android:taskAffinity="com.android.chrome"
    android:launchMode="standard">
</activity>
```

```
Running activities (most recent first):
  TaskRecord{4ef09cf #39793 A=com.google.android.gm U=0 StackId=20 sz=2}
    Run #1: ActivityRecord{5485e8b u0 com.android.chrome/org.chromium.chrome.browser.customtabs.CustomTabActivity t39793}
    Run #0: ActivityRecord{8dd3fe4 u0 com.google.android.gm/.ConversationListActivityGmail t39793}
```

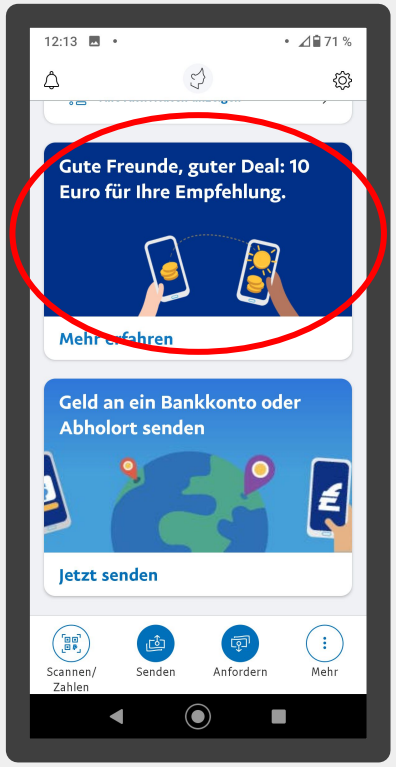
```
<activity
    android:name="ChromeTabbedActivity"
    android:taskAffinity="com.android.chrome"
    android:launchMode="singleTask">
</activity>
```

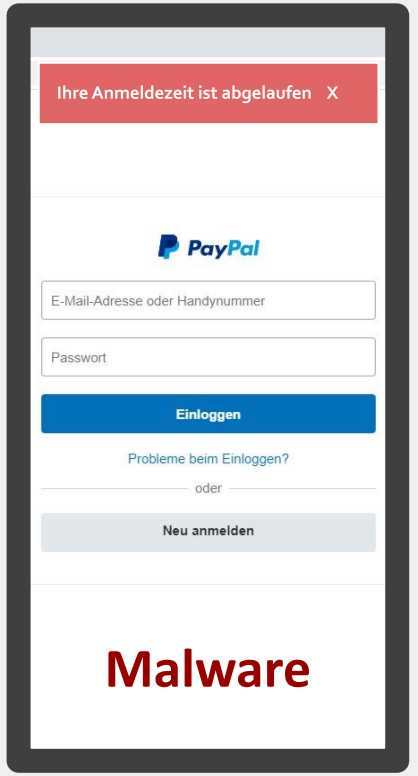
```
Running activities (most recent first):
  TaskRecord{baf0549 #39801 A=com.android.chrome U=0 StackId=28 sz=1}
    Run #0: ActivityRecord{a4467c1 u0 com.android.chrome/org.chromium.chrome.browser.ChromeTabbedActivity t39801}
```

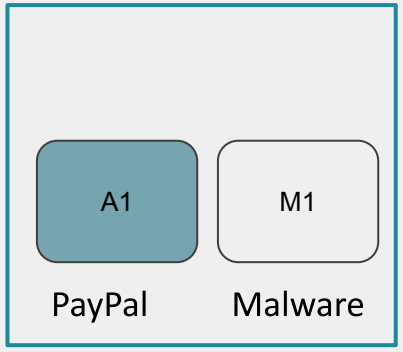
```
Running activities (most recent first):
  TaskRecord{cae0f62 #39795 A=com.paypal.android.p2pmobile U=0 StackId=22 sz=1}
    Run #0: ActivityRecord{2db2a26 u0 com.paypal.android.p2pmobile/o.mfz t39795}
```

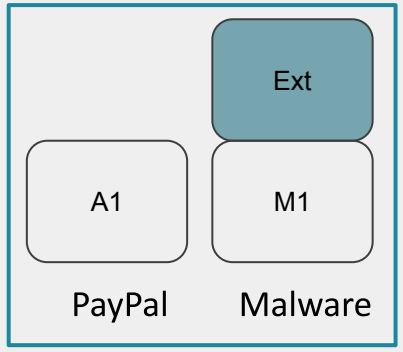
Quellen:
[6],[10]

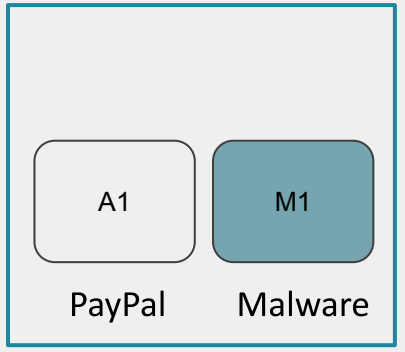
Task Hijacking Beispiel PayPal





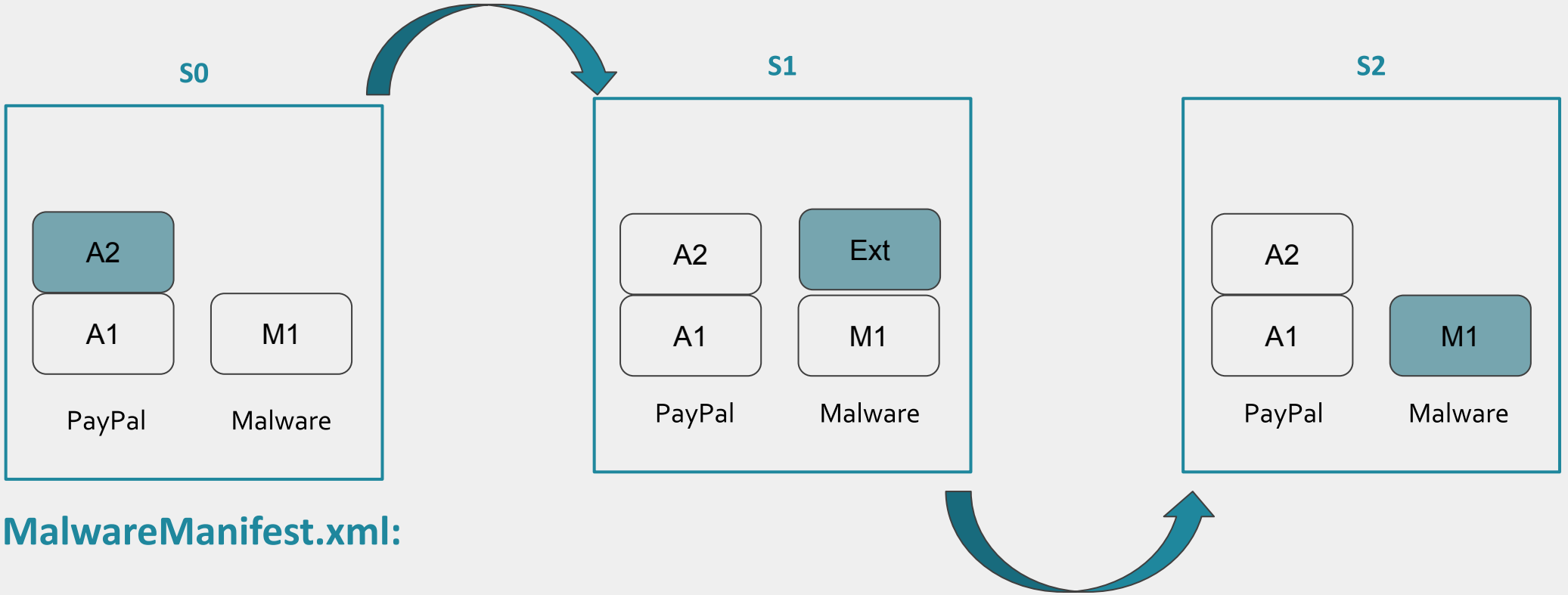






Task Hijacking Beispiel PayPal

$$T1 : (S_0, S_1, e^{A2:startActivity(Ext)}, \gamma^{singleTask})$$



MalwareManifest.xml:

```
<activity
    android:name="M1"
    android:taskAffinity="com.android.chrome">
</activity>
```

$$T2 : (S_1, S_2, e^{Ext:back}, \gamma^{default})$$

03

StrandHogg & StrandHogg 2.0

StrandHogg

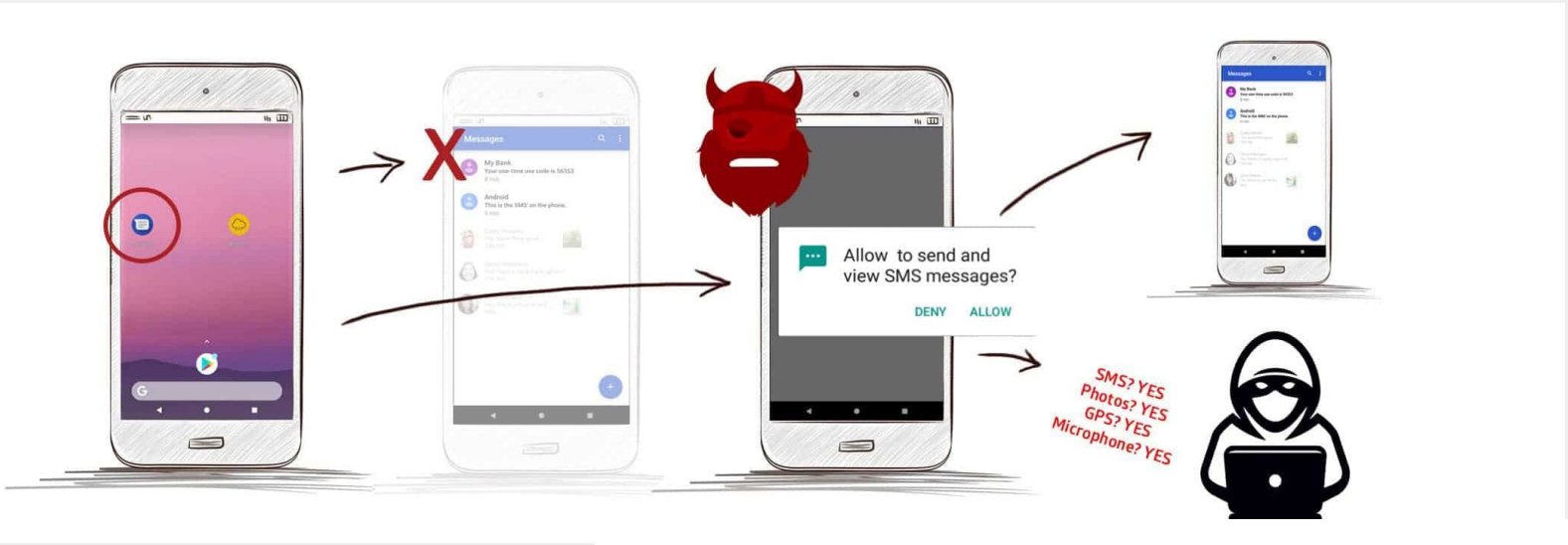
Dezember 2019

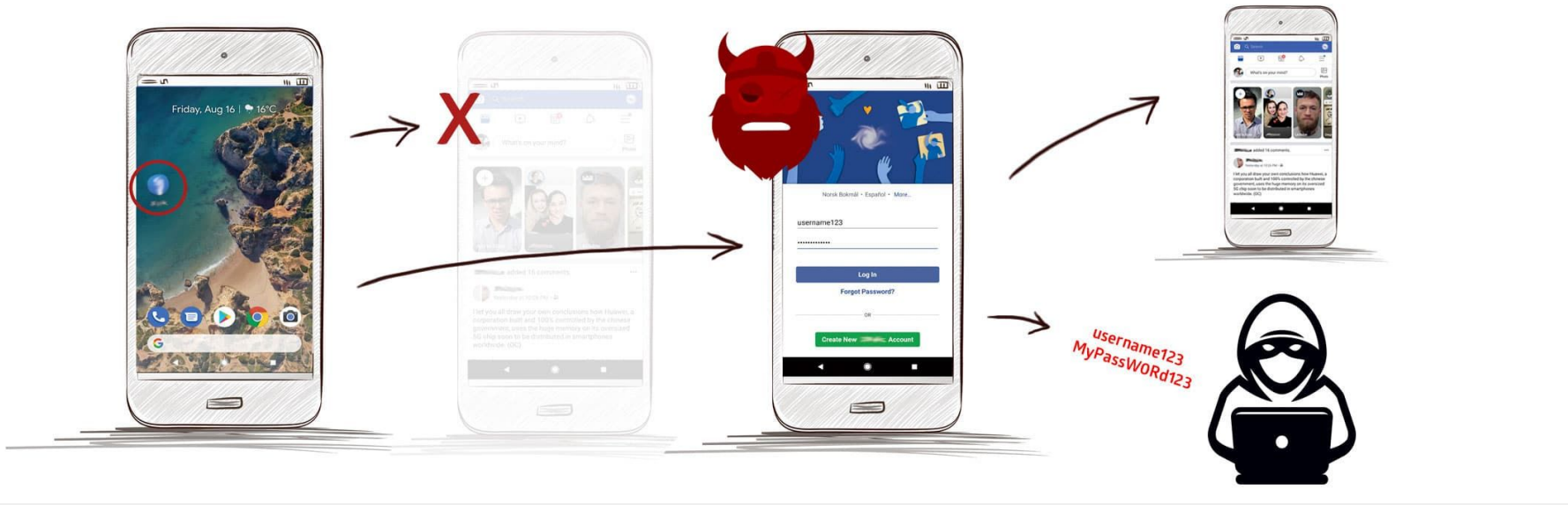
StrandHogg 2.0

Mai 2020

Bildquellen: [7], [8]

StrandHogg





Quelle: [7]

StrandHogg

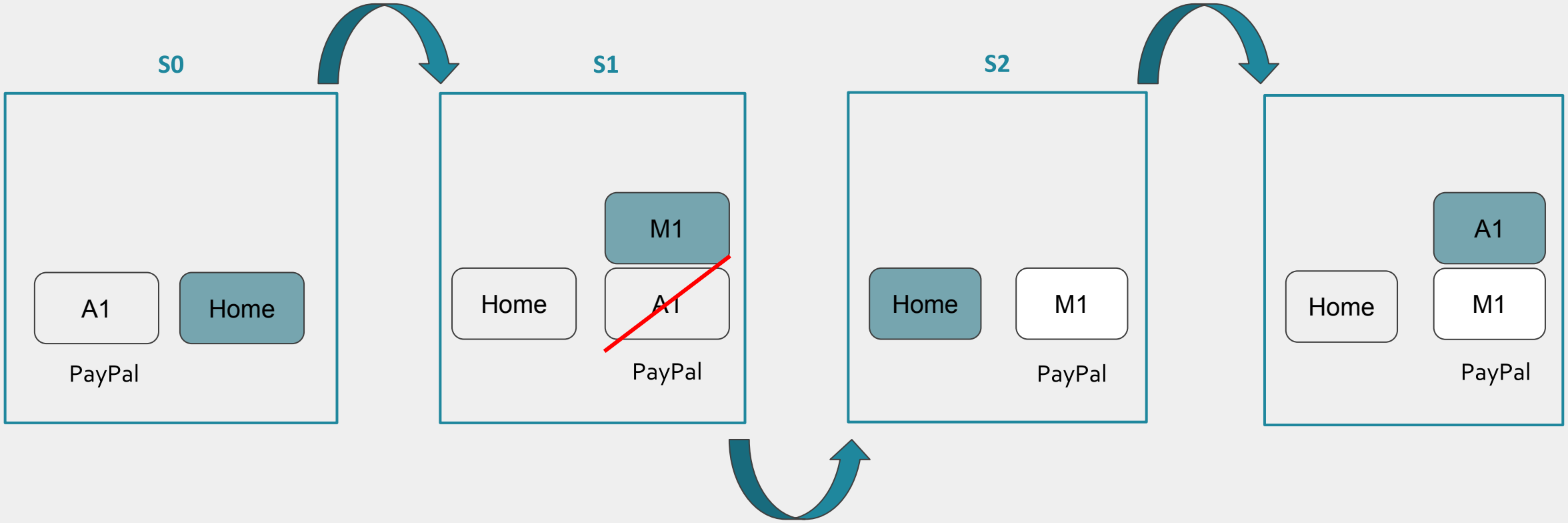
```
<!-- Attacks -->
<activity
    android:name="com.example.malware.attacks.SmsActivity"
    android:allowTaskReparenting="true"
    android:icon="@drawable/icon_[redacted]"
    android:label="Messages"
    android:roundIcon="@drawable/icon_[redacted]"
    android:taskAffinity="com.google.android.apps.messaging"
    android:theme="@style/SmsTheme" />
<activity
    android:name="com.example.malware.attacks.[redacted]Activity"
    android:allowTaskReparenting="true"
    android:icon="@drawable/icon_[redacted]"
    android:label="[redacted]"
    android:roundIcon="@drawable/icon_[redacted]"
    android:taskAffinity="com.[redacted].android.p2pmobile"
    android:theme="@style/[redacted]Theme"
    android:windowSoftInputMode="adjustResize" />
```

Quelle: [7]

StrandHogg

$$T1 : (S_0, S_1, e^{Home:startActivity(M1)}, \gamma^{NewTask+ClearTask})$$

$$T3 : (S_2, S_3, e^{Home:startActivity(A1)}, \gamma^{default})$$



$$T2 : (S_1, S_2, e^{M1:back}, \gamma^{default})$$

Quelle: [7]

StrandHogg 2.0

- 04.12.2019 Report-Issue an Google
- Veröffentlichung nach Google-Patch im Mai 2020
- Keine Konfigurationen mehr in AndroidManifest.xml notwendig
- Simultaner Angriff auf mehrere Apps mit einer Malware
- Betraf alle Android Versionen < Android 10
    - April 2020: 91,8% der Benutzer weltweit mit Android 9 oder darunter

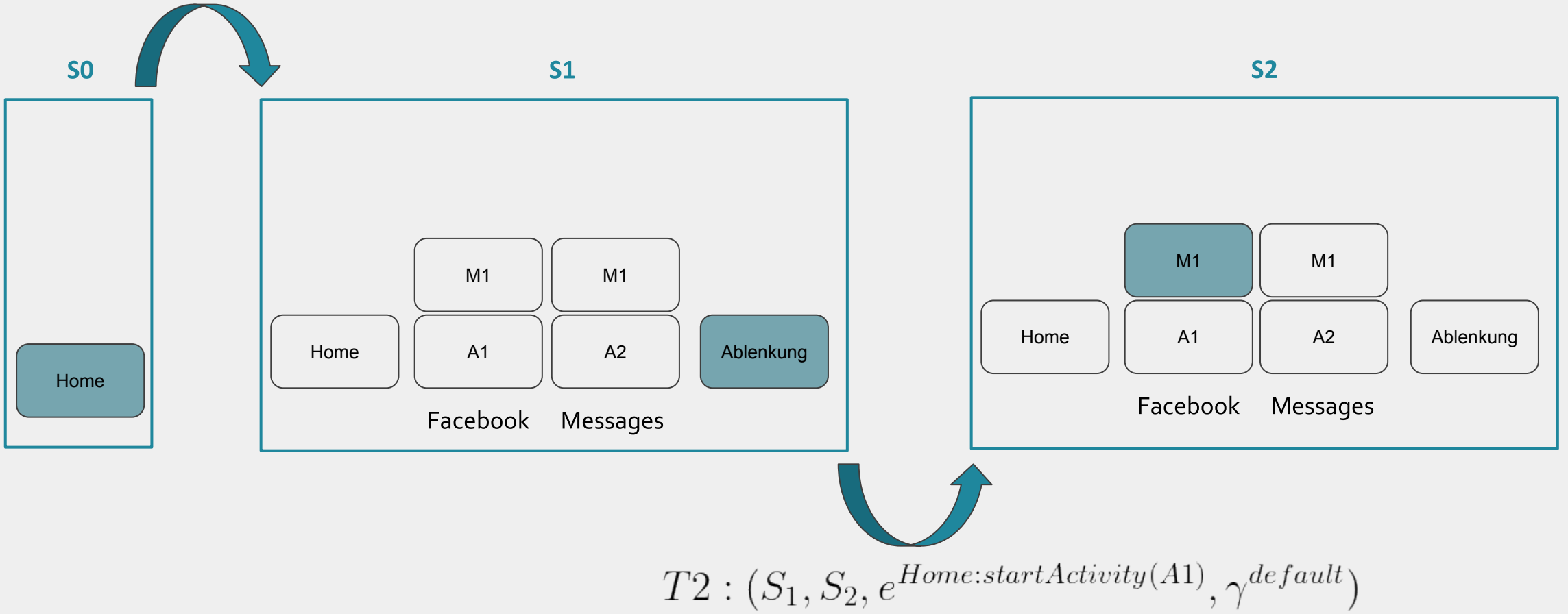
- Proof-of-Concept Beispiel: https://youtu.be/DPsNiQDB7Uw?t=55

Quelle: [8]

StrandHogg 2.0

New_Task

$$T1 : (S_0, S_1, e^{startM1}, \gamma^{startActivities(A1,M1,A2,M1,Ablenkung)})$$



$$T2 : (S_1, S_2, e^{Home:startActivity(A1)}, \gamma^{default})$$

Quelle: [8]

StrandHogg 2.0 - Android Patch

android / platform / frameworks / base / **a952197bd161ac0e03abc6acb5f48e4ec2a56e9d**

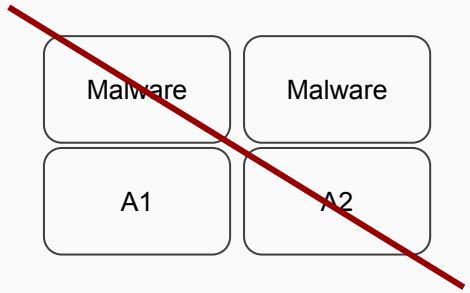
```
commit  a952197bd161ac0e03abc6acb5f48e4ec2a56e9d        [log] [tgz]
author  Riddle Hsu <riddlehsu@google.com>               Sat Feb 22 23:20:41 2020 +0800
committer Anis Assi <anisassi@google.com>               Mon Mar 30 13:56:09 2020 -0700
tree    38634ffb0ab1938bc94bea4df55e06001b66d961
parent  d37eb96212c6fe4819c66bd0a1e0a2f9f7501602 [diff]
```

```
RESTRICT AUTOMERGE Create separated tasks for different apps from startActivities

Assume there are 2 applications A, B with different uids.
There are 4 activities A1, A2, B1, B2 with default task
affinity and launch mode.

After A1 called startActivities(B1, A2, B2):
 Original   : Task(A1, B1, A2, B2)
 This Change: Task(A1, B1), Task(A2, B2)
In other words, the source caller cannot launch its activity
above the activity of other application in the same task, and
it can still launch activity of other application in its task.

Bug: 145669109
Test: run cts --test android.server.cts.StartActivityTests \
      -m CtsServicesHostTestCases
Change-Id: I97bd875146a52f62b8fe82235487ccefb2955e8e
(cherry picked from commit 973ecc619c0bb87a03481774ea9e86d2924601e4)
```



services/core/java/com/android/server/am/ActivityStarter.java [diff]

1 file changed

Quelle: [9]

StrandHogg + StrandHogg 2.0 Analyse

	StrandHogg	StrandHogg 2.0
Betroffene Android-Versionen	Alle Android Versionen (kein Patch veröffentlicht)	Android Version 9 oder geringer (Patch für Version 8, 8.1, 9 im Mai 2020 veröffentlicht)
Betroffene Anwendungen	Alle der 500 meist verbreiteten Apps	Alle der 500 meist verbreiteten Apps
Bedingungen	**Manifest.xml:** TaskAffinity; AllowTaskReparenting **Intents:** NEW_TASK, CLEAR_TASK	**Manifest.xml:** - **Intents:** NEW_TASK in startActivities()
Bedrohungen	Phishing, Denial of Service, Permissions-Escalation	Phishing, Denial of Service, Permissions-Escalation
Gefährdete Schutzziele	Vertraulichkeit, Verfügbarkeit, Integrität	Vertraulichkeit, Verfügbarkeit, Integrität
Malware im Umlauf	36 Malware Apps entdeckt	-

Quellen: [7], [8]

04 Gegenmaßnahmen

Gegenmaßnahmen

	Entwickler	Benutzer
StrandHogg	Intent-Kombination: “FLAG_ACTIVITY_NEW_TASK” + “FLAG_ACTIVITY_CLEAR_TASK” taskAffinity mit leerem String füllen	Mobile-Security Software (inkl Malware-Detection) Permission Pop-Ups prüfen adb verwenden und Tasks überwachen
StrandHogg 2.0	launchMode=”singleInstance” oder “singleTask”	Android Update Mobile-Security Software (inkl Malware-Detection)

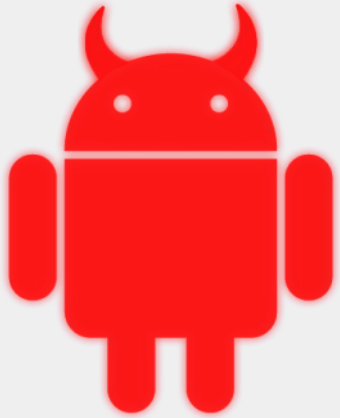
Quellen: [7], [8]

05 Fazit und Ausblick

Fazit und Ausblick

Task Hijacking

Schwachstellen als Möglichkeit mit einzelner Malware alle Schutzziele unterschiedlicher Applikationen zu bedrohen.



Schutzmaßnahmen?

- Zertifizierung zwischen Tasks möglich?
- TaskAffinity einschränkbar?
- Mit Sandboxing Möglichkeiten Tasks zu steuern?

StrandHogg

als gefährliche Task-Hijacking Schwachstelle mit (noch) wenig Auswirkungen auf den Benutzer.

StrandHogg3.0?

- Welche Auswirkungen auf den Benutzer?
- Auf welchen Android-Geräten?

Bildquelle: [1]

Quellen:

Bildquellen:
[1] https://www.onespan.com/de/blog/so-stoppen-sie-die-bedrohung-durch-android-rooting-malware-angriffe-mit-rasp
[7] https://promon.co/security-news/strandhogg/
[8] https://promon.co/strandhogg-2-0/

Inhaltsquellen:
[2] https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-ren-chuangang.pdf
[3] https://arxiv.org/pdf/2001.09406.pdf
[4] https://www.appbrain.com/stats/number-of-android-apps
[5] https://www.cvedetails.com/top-50-products.php?year=2019
[6] https://developer.android.com/docs
[7] https://promon.co/security-news/strandhogg/
[8] https://promon.co/strandhogg-2-0/
[9] https://android.googlesource.com/platform/frameworks/base/+/a952197bd161ac0e03abc6acb5f48e4ec2a56e9d

Verwendete Tools:
[10] https://developer.android.com/studio/releases/platform-tools

Noch Fragen?