

הסתרת רוט מאפליקציות

March 02, 2021 • דוד לב



אם צרבתם או חשבתם לצרוב רוט במכשירכם, בוודאי שמעתם על מספר חסרונות מזעריים בתהליך. החיסרון העיקרי בביצוע רוט הוא כביכול 'בעיות האבטחה' שנוצרות מכך לאפליקציות מסוימות שמסרבות לפעול על מכשירים מושרשים. במדריך הבא נרחיב כיצד ניתן להסתיר מהאפליקציות האלו את העובדה שהמכשיר שלכם עבר רוט.

למי שלא יודע כיצד רוט פועל, הרשאת הרוט מספקת גישה לשורש המערכת ובכך גם למסדי הנתונים של האפליקציות השונות. עכשיו נסו לדמיין את אפליקציית הבנק שלכם ששומרת מידע מקומי מסוים בתיקיית האחסון המאובטחת שלה, בעצם לכל אפליקציה שתתנו הרשאת רוט - תהיה גישה לנתונים האלו! זו הסיבה שהרבה מאוד אפליקציות פיננסיות או כאלו שמאחסנות, מקבלות ושולחות נתונים רגישים, מפעילות מנגנוני אבטחה שונים שמטרתם לקבל אינדיקציה האם המכשיר שלכם עם רוט או לא, ובמידה וכן, לסגור את השימוש באפליקציה בפני המשתמש.

זה המקום לעצור ולומר - מפתחי האפליקציות פועלים בצדק כשהם סוגרים את הגישה ממכשירים מושרשים כיוון שלמעשה, אם אינכם זהירים ומחלקים הרשאות רוט 'כאילו אין מחר', אתם אכן חשופים לבעיות אבטחה רציניות ביותר.

אז כמובן, לתת הרשאות רוט רק כשצריך ורק לאפליקציות קוד פתוח! | [להרחבה](#).

בשנה האחרונה הצטרף ג'ון וו (Jon Wu), המפתח של מג'יסק, לצוות האבטחה של אנדרואיד בחברת גוגל, מה שגרם להרבה שמועות שהפרוייקט הולך להיסגר (ניגוד אינטרסים.. בכל זאת). אך באוגוסט 2021 פרסם ג'ון פוסט

שבו הוא מסביר כי הוא קיבל אישור להמשיך לעבוד על מג'יסק אך הוא יאלץ להסיר את התמיכה ב-MagiskHide, כלי הסתרת הרוט המובנה של מג'יסק.

החל מגרסה 23.0 ואילך תרד התמיכה במג'יסקהייד ולכן לא מומלץ בשלב זה לעדכן את מג'יסק עד להודעה חדשה.

למידע נוסף על ההחלטה ולכיוון שאליו מג'יסק צועד - קראו את הכתבה ב-XDA.

לעוד מדריכים מעולים הצטרפו לערוץ אנדרוטיפס בטלגרם!

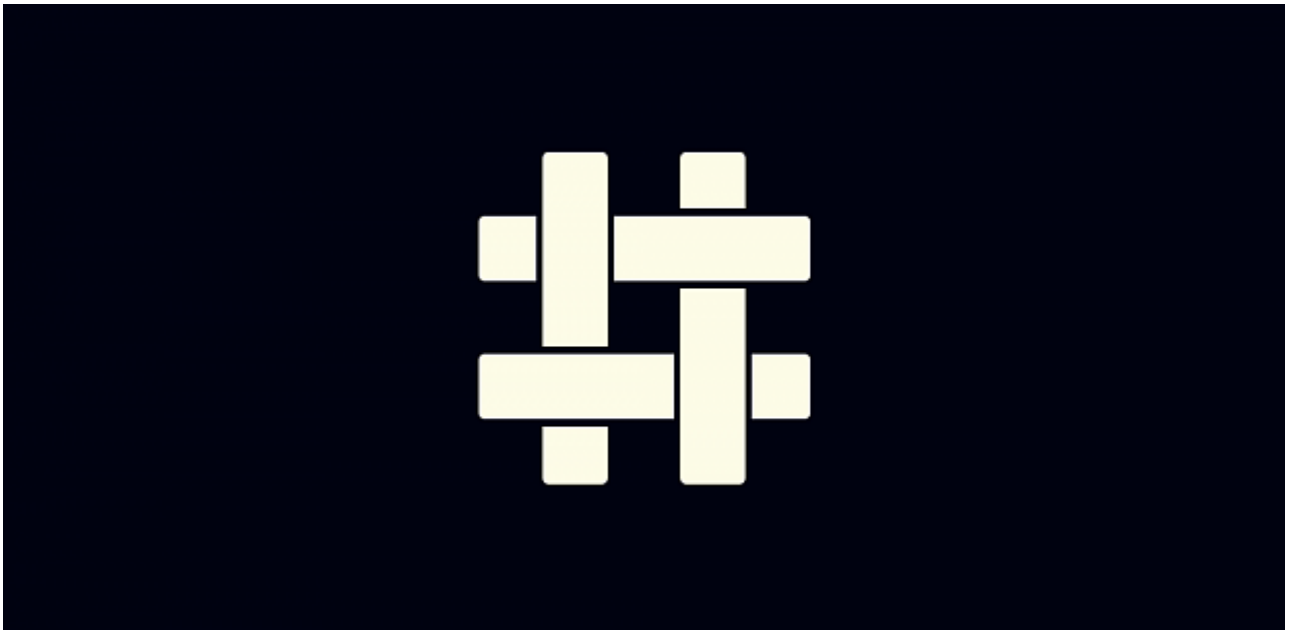
הנה סוגי אפליקציות נפוצות שלא יפעלו על מכשיר שצורב בו רוט: נטפליקס, סנאפצ'אט, אנדרואיד פיי, אפליקציות בנקים (שמכבדים את עצמם), אפליקציות תשלומים (או חלקים מסוימים מהן כגון תשלום ב-NFC), אפליקציות ארגוניות כמו Citrix, Mobileiron, Intelligent Hub, אפליקציות שליחים ונהגים, משחקים כגון פוקימון, מריו גו, גוגל פליי שלא יאפשר הורדה של אפליקציות מסוימות, ועוד אלפי אפליקציות שהמשתמש לכולם הוא שמפתחי האפליקציה אינם מעוניינים לחשוף את הנתונים או את צורת העבודה שלהם או פשוט למנוע עקיפות מסוימות מצד המשתמש (הרשאות, רכישות, רישיונות) ולכן הן אינם מאפשרים פעולה של האפליקציות על מכשירים מושרשים.

האפליקציות שמסרבות לפעול על מכשירים שצורב בהם רוט מבצעות בדרך כלל מספר בדיקות אבטחה שמספקות להם את המידע האם המכשיר מושרש או לא -

בדיקות האבטחה מתחלקות לשני חלקים:

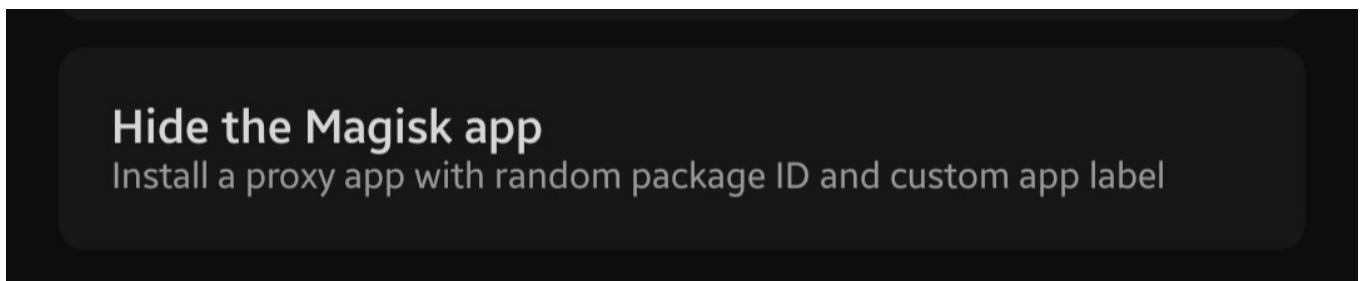
- בדיקה בסיסית של קבצים ואפליקציות (su, magisk, busybox ועוד)
- בדיקת SafetyNet (מורכבת משני חלקים, פירוט בהמשך)

הבדיקה הבסיסית

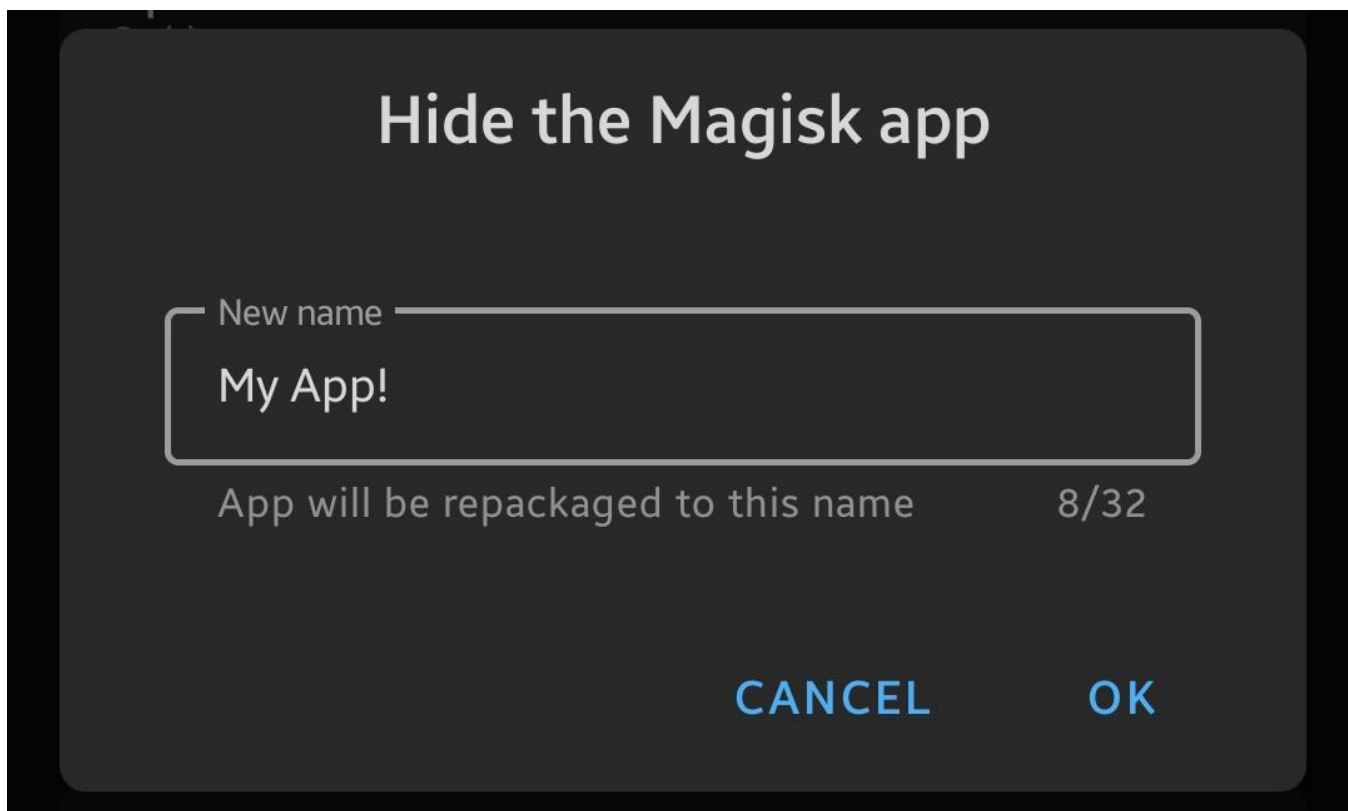


הבדיקה הפשוטה ביותר שבה משתמשות הרבה מאוד אפליקציות בשל הנוחות והאמינות היחסית שהיא מספקת, היא בדיקה מקיפה שמחפשת אפליקציות שמותקנות כשבמכשיר צרוב רוט, דוגמת **Magisk Manager**, **EdXposed**, **Super SU**, כמו כן היא בודקת רשימה של אפליקציות זדוניות פוטנציאליות כמו לאקי פאצ'ר (זו הסיבה שמחליפים לה את החתימה) ואפליקציות שפועלות רק עם הרשאות רוט כמו **Titanium Backup** ועוד, עוברת על props חשודים בקובץ ה-**build.prop**, מנסה לגשת להרשאות הרוט, מחפשת את קבצי **su** ו-**busybox** במחיצת המערכת, מחפשת מחיצות מערכת עם הרשאות כתיבה ועריכה (**rw**) ועוד. קיימת ספריית קוד פתוח שמשמשת אפליקציות רבות הנקראת **RootBeer**, הספרייה מבצעת את הבדיקות הנ"ל ומספקת לאפליקציה אינדיקציה האם המכשיר מושרש או לא. ראשית כל נאמר שאת הבדיקות האלו ניתן לעבור בקלות על ידי כלים ש-**Magisk** מספקת באופן מובנה. הכלי הראשון הוא **Hide Manager** שיוצר לאנצ'ר נפרד שמריץ את **Manager** מתוך שם הבילה רנדומלי כך שלא יוכלו לזהות אותו.

כדי להפעיל את ההסתרה יש להיכנס להגדרות ב-**Magisk** ולבחור באופציה **Hide the Magisk app**:



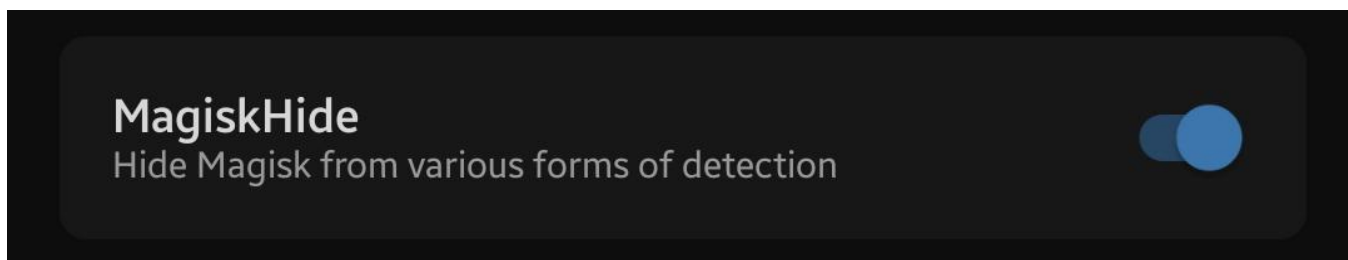
הקלידו את שם האפליקציה (ניתן להשאיר על **Manager**) ולחצו על **Ok**:



לאחר מספר שניות ה-Manager יוסר ואתם תועברו לאפליקציה הרנדומלית.

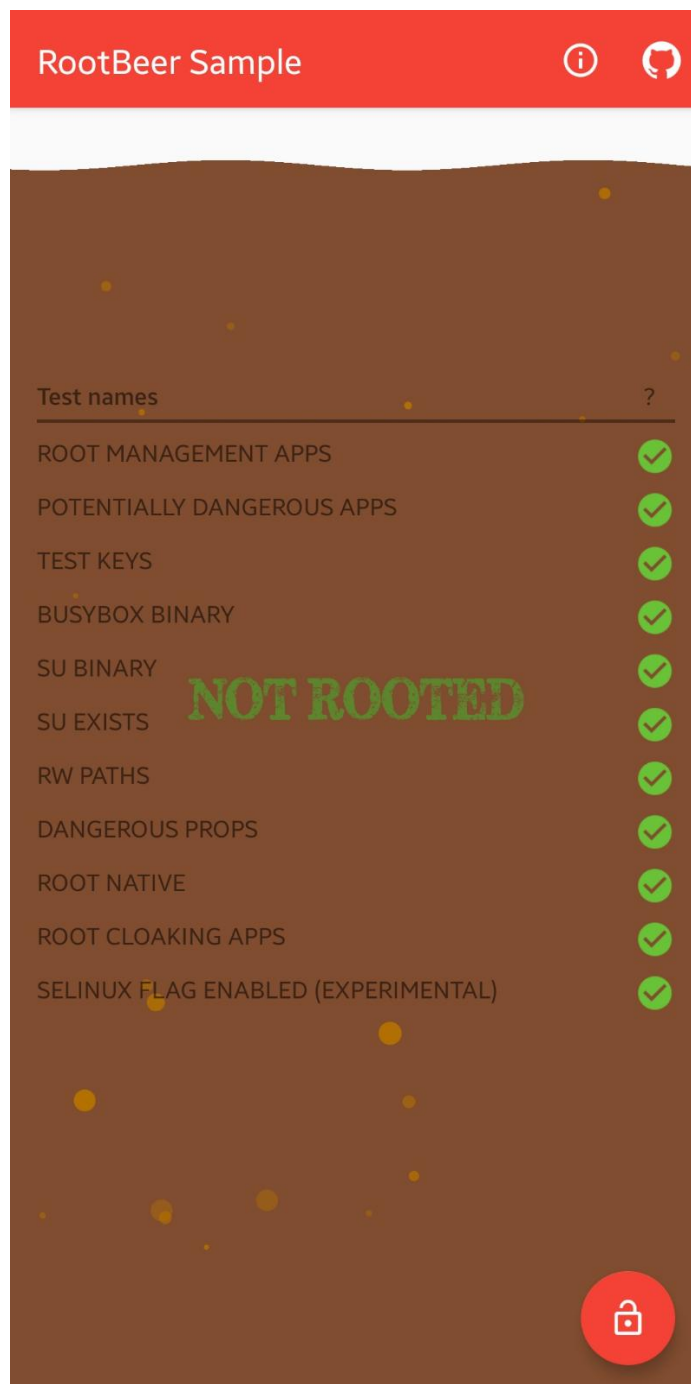
הכלי השני שעליו כבר דיברנו בעבר הוא **MagiskHide** שמגיע כבוי כברירת מחדל (בגרסאות החדשות של מג'יסק) ומאפשר מעבר של רוב הבדיקות הקיימות על ידי בידוד תהליך הריצה של האפליקציה ובכך מציג לה נתונים שגויים מסוימים שמונעים ממנה לזהות האם המכשיר עבר רוט. (אם תרצו לקרוא על הנושא בהרחבה, כיצד MagiskHide עושה את הפעולה המדהימה הזו - מצאתי כתבה מעולה במדיום, באנגלית, לחצו כאן).

כדי להפעיל את תכונת ההסתרה היכנסו להגדרות ה-Magisk והעבירו את MagiskHide למצב פעיל.



כעת הפעילו את המכשיר מחדש ולאחר מכן היכנסו למנהל הרשאות הרוט (סימון של מגן), לחצו למעלה על MagiskHide וסמנו את האפליקציה שברצונכם להסתיר ממנה את הרוט. שימו לב לא לסמן אפליקציות שכן צריכות גישה לרוט.

כדי לבצע בדיקה ולראות האם כלי ההסתרה עובד, הורידו את אפליקציית RootBeer מכאן או מגוגל פליי, הכניסו אותה לרשימה ב-MagiskHide וגלו האם אתם עוברים את הבדיקה. במכשיר שלי למשל אני מקבל את התוצאה הבאה למרות שיש לי גם Magisk וגם EdXposed. ניתן לראות שהמכשיר עבר את כל הבדיקות (NOT ROOTED).



אגב, כלי ההסתרה MagiskHide ניתן גם לשימוש מהטרמינל. לאחר שנכנסתם עם `adb shell` או דרך Termux הקלידו `su` כדי להיכנס למצב רוט ואז וודאו ש-MagiskHide מופעל על ידי הקלדת הפקודה:

```
magiskhide --status
```

אם קיבלתם תשובה של Disabled (מושבת), הפעילו עם הפקודה:

```
magiskhide --enable
```

ואז התחילו להוסיף אפליקציות עם הפקודה:

```
magiskhide --add package-name
```

במקום `<package-name>` הכניסו את שם החבילה של האפליקציה שממנה אתם מעוניינים להסתיר את הרוט.

להסרת אפליקציה מרשימת ההסתרה הריצו:

```
magiskhide --rm package-name
```

ולצפייה ברשימה המלאה:

```
magiskhide --ls
```

בדיקת SafetyNet



בדיקת סייפטינט היא בדיקה יחסית חדשה שגוגל מספקת כחלק מ-Google Play Services שמאפשרת למפתח האפליקציה לקבל אינדקציה האם המכשיר עבר רוט או לא.

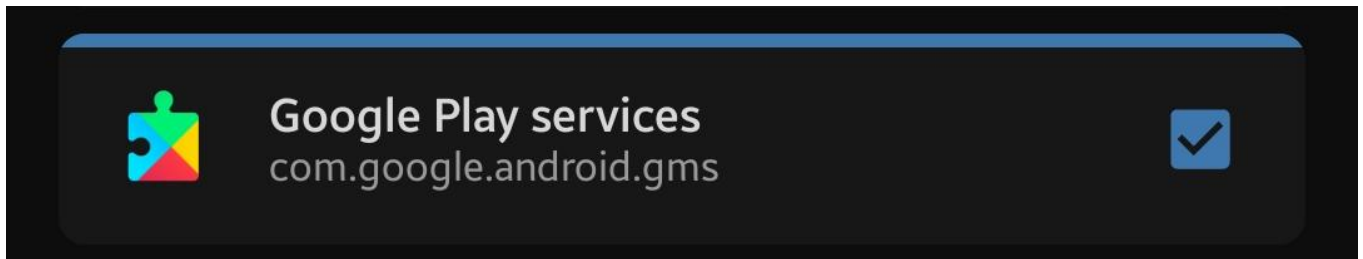
בסייפטינט קיימות שני בדיקות: הראשונה נקראת basicIntegrity והיא בודקת את הדברים הבסיסיים שפירטנו למעלה, אותה ניתן לעבור בקלות עם MagiskHide.

הבדיקה השנייה נקראת CTS Profile והיא בודקת בין השאר את נעילת הבוטלואדר (שתפקידו לחסום צריבה של קושחות שעברו שינויים). בדיקה זו עושה שימוש בhardware backed key attestation (עדות מגובה חומרה), מה שאומר שלא ניתן לזייף את הנתונים המתקבלים מהבדיקה ונכון להיום, לא קיימת דרך לעבור אותה.

למזלנו הרב, גוגל כרגע אינה כופה את הבדיקה השנייה ברוב המכשירים ולכן קיימת דרך 'לחייב' את SafetyNet להשתמש רק בבדיקה הראשונה (basicIntegrity) ובכך אם הצלחתם לעבור את basic, תוכלו לקבל אימות שהמכשיר שלכם עבר את שני הבדיקות.

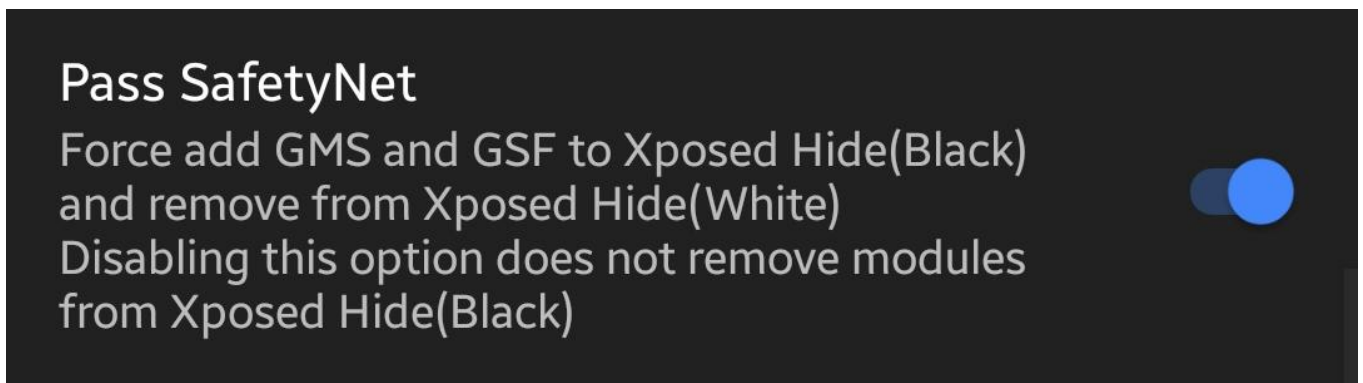
שימו לב, יתכנו מכשירים שבהם מספיק להפעיל את MagiskHide והם יעברו גם את SafetyNet. אין כללים בתחום הזה, כל מכשיר ומצבו הוא.

הבה נבצע בדיקת SafetyNet: ראשית וודאו MagiskHide מופעל ושאפליקציית Google Play Services נמצאת ברשימת האפליקציות המוסתרות.



לא תוכלו לעבור SafetyNet עם EdXposed! נסו לעבור ל-LSposed או לחילופין למצוא אלטרנטיבה אחרת במדריך הבא.

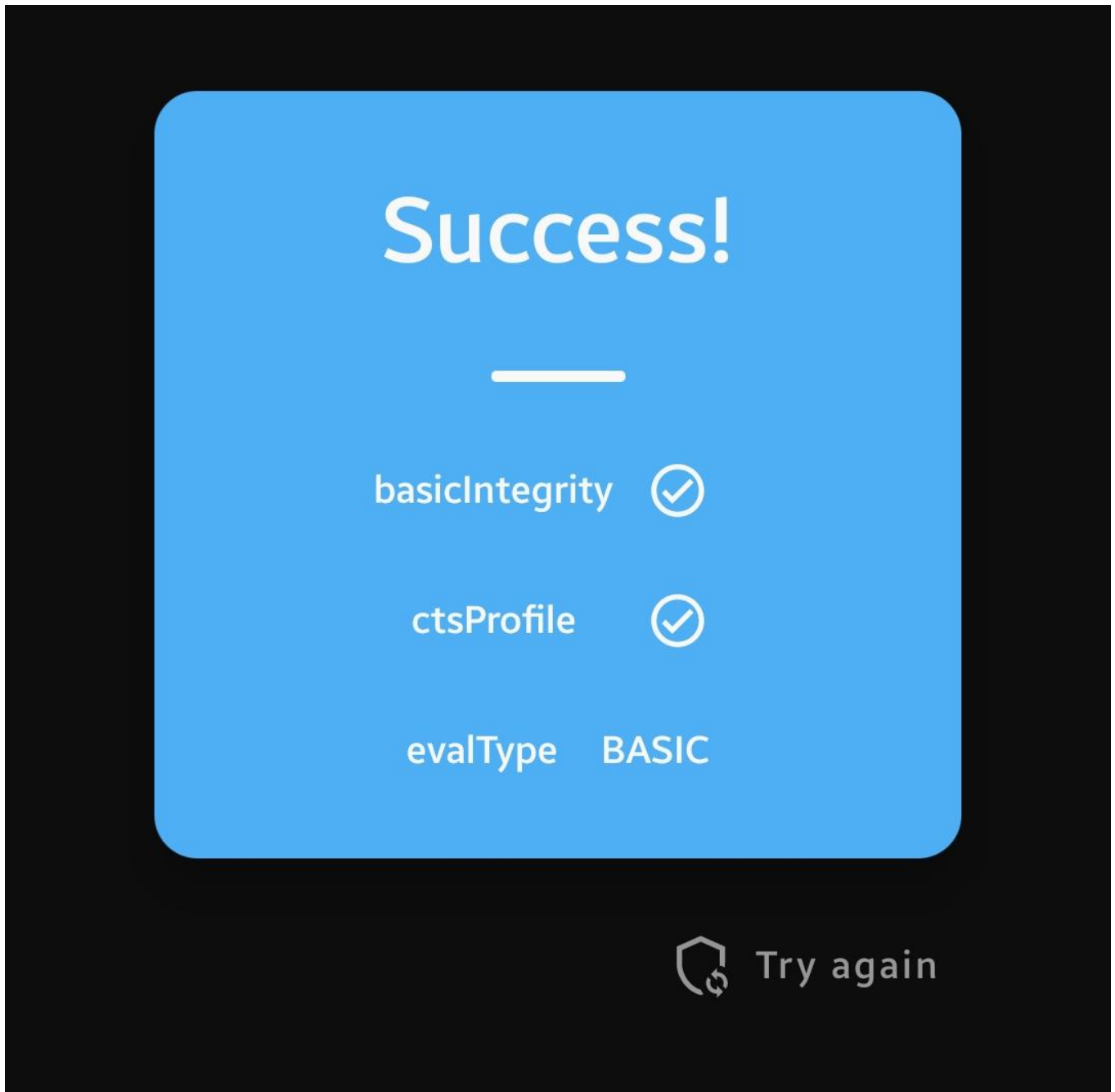
~~אם אתם משתמשים בנוסף ב-EdXposed, היכנסו ל-EdXposed Manager < הגדרות < גללו למטה והפעילו את האופציה Pass SafetyNet:~~



הפעילו מחדש את המכשיר ולאחר מכן היכנסו לאפליקציית Magisk ולחצו על Check SafetyNet:



אם קיבלתם את המסך הבא, עברתם את הבדיקה! אם לא, המשיכו במדריך.



שימו לב כי בצילום המסך שמעליכם, קיימת שורה הנקראת evalType. זו הבדיקה **שבוצעה ועברה** בפועל. המכשיר שלי לא הצליח לעבור את בדיקת ה-CTS ולכן כפיתי עליו שיבצע רק את בדיקת ה-basic שאותה עברתי בעזרת MagiskHide.

אז בואו נעשה סדר: את בדיקת ה-CTS אף אחד לא עובר. הדרך לעבור היא או שגוגל עוד לא כופים אצלכם את בדיקת ה-CTS Profile או שאתם כופים על גוגל לבצע את בדיקת ה-basicIntegrity בלבד. אם לאחר שהפעלתם MagiskHide הבדיקה נכשלה וקיבלתם evalType של HARDWARE (בעצם CTS), עליכם לכפות על גוגל לבצע רק את בדיקת ה-BASIC.

הורידו את המודול SafetyNet-Fix מערון העזר שלנו או מגיטהאב והתקינו אותו דרך Magisk, הפעילו מחדש את המכשיר והריצו שוב את הבדיקה (Try again). כעת אתם אמורים לראות שה-evalType השתנה

ל-BASIC ואתם אמורים לעבור את הבדיקה בהצלחה.

- באם החלטתם להוריד מגיטהאב ואתם עדיין על Magisk v23.0 שימו לב שאתם מורידים את הגרסה הרגילה (לא של Riru או Zygisk). אחרת זה פשוט לא יעבוד..

אם עדיין הבדיקה נכשלה על BASIC קיים מודול נוסף שמכיל מאגר טביעות אצבע (ro.build.fingerprint) של מכשירים רשמיים שעברו את האישור של גוגל. המודול יוצר סקריפט אתחול שמחליף את המפתח שלכם במפתח רשמי.

הורידו את המודול מכאן או מגיטהאב והתקינו דרך Magisk.

פתחו טרמינל עם adb shell או דרך Termux הקלידו su כדי להיכנס למצב רוט. הקלידו את הפקודה הבאה על מנת להריץ את המודול:

```
props
```

לאחר שהמודול יפתח וירענן את מאגרי טביעות האצבע, לחצו על 1 כדי לערוך את טביעת האצבע ואז על f כדי לבחור טביעת אצבע חדשה. בחרו את יצרן המכשיר שלכם (המספר שלצידו) וחפשו את הדגם שלכם. (טביעת האצבע של המכשיר מייצגת אתכם מול אפליקציות כגון Google Play ועוד ולכן חשוב לא לקחת טביעת אצבע של מכשיר אחר). אשרו את הפעולה והפעילו מחדש את המכשיר.

MagiskHide Props Config v5.4.0

by Didgeridoohan @ XDA Developers

=====
Select an option below.
=====

- 1 - Edit device fingerprint
- 2 - Device simulation (disabled)
- 3 - Edit MagiskHide props
- 4 - Add/edit custom props
- 5 - Delete prop values
- 6 - Script settings
- 7 - Collect logs
- u - Perform module update check
- r - Reset all options/settings
- b - Reboot device
- e - Exit

See the module readme or the support thread @ XDA for details.

Enter your desired option: █

לאחר מכן הריצו שוב את בדיקת ה-SafetyNet וכעת אתם אמורים לעבור אותה.

אם עדיין לא עברתם את הבדיקה נסו לבצע ניקוי נתונים ל-Google Play Services, להפעיל מחדש את המכשיר ושוב לבצע את הבדיקה. וודאו שאתם מצליחים לעבור את הבדיקה באפליקציית RootBeer לאחר שהפעלתם עליה את MagiskHide. אם עדיין לא הצלחתם (מה שיכול להיות בגלל שינויים בצד שרת של SafetyNet) שאלו בקבוצת התמיכה הנהדרת שלנו בטלגרם ונסה לבדוק מה עוד ניתן לעשות.

יש לכם הצעות למדריכים נוספים? דברו איתי בפרטי.

