

Kritische Sicherheitslücke: Erster Android-Wurm entdeckt

G DATA Sicherheitsexperten berichten über ihre Erkenntnisse und erklären, wie die Lücke zu schließen ist

Bochum (Deutschland), 14. Juni 2018

Tausende von Smartphones weltweit sind von einem Android-Wurm betroffen. Schuld daran ist eine Sicherheitslücke durch eine vergessene Debug-Schnittstelle. Die Schwachstelle ist noch immer nicht gefixt. G DATA klärt über die Gefahr auf und zeigt, wie Benutzer überprüfen können, ob ihr Mobilgerät ebenfalls davon betroffen ist und falls ja, wie die Sicherheitslücke geschlossen werden kann.



Ein unbekannter Dritter greift via Internet auf das eigene Smartphone zu – und das mit vollen Root-Rechten als Administrator. Was sich wie ein komplizierter und denkbar unmöglicher Fall liest, wird durch eine Android-Sicherheitslücke zum einfachen Spiel für Cyberangreifer. Dieser kann sich dank des geöffneten TCP-Port 5555 per Androids Debug Bridge-Schnittstelle (kurz: ADB) auf das Gerät einklinken. Über ADB lassen sich eine Vielzahl von Geräte-Aktionen durchführen – angefangen vom simplen Auslesen der Geräteinformationen, über den Diebstahl sensibler Daten, bis hin zu sicherheitskritischen Installationen von schädlichen Programmen. „ADB wird eigentlich von Software-Entwicklern dafür benutzt, direkten Zugriff auf das Gerät zu erhalten, um Diagnosen oder Nachinstallationen vorzunehmen“, sagt Alexander Burris, Lead Mobile Researcher bei G DATA. Per Voreinstellung ist diese Schnittstelle normalerweise deaktiviert. „Dennoch gibt es einige Hersteller, beispielsweise wie in diesem Fall aus dem asiatischen Raum, die es scheinbar versäumt haben, die aktivierte ADB-Schnittstelle vor Verkauf der Geräte an Konsumenten abzustellen.“

„Da Smartphones für eine solch dauerhafte Beanspruchung nicht ausgelegt sind, kann dies mittelfristig zu Schäden am Gerät führen“, warnt Alexander Burris, Lead Mobile Researcher bei G DATA.

Android-Wurm ADB.Miner nutzt Schwachstelle aus

Der erste Android-Wurm, der auf den Namen ADB.Miner hört, nutzt die offene ADB-Schnittstelle aus. Möchte er sich mit dem Smartphone verbinden, so erscheint eine USB-Debugging-Abfrage. Wird hierbei auf OK geklickt, so ist das Mobilgerät im Anschluss infiziert. Der Wurm durchforstet das Internet nach den offenen 5555 TCP-Ports und schafft so ein Cryptomining-Botnetz. Das Gerät wird folglich kompromittiert und zum Schürfen der virtuellen Währung „XMR Coins“ missbraucht. Ist das Gerät befallen, so sucht es selbstständig nach weiteren offenen 5555 TCP-Ports, sodass sich der Wurm

G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299

weiterverbreiten kann. „Das bedeutet im Umkehrschluss: Je mehr Android-Smartphones betroffen sind, desto schneller kann sich der Wurm verbreiten“, sagt Burris. „Für den Benutzer bedeutet das eine sehr starke performancetechnische Einschränkung sowie extrem verkürzte Akku-Laufzeiten. Da Smartphones für eine solch dauerhafte Beanspruchung nicht ausgelegt sind, kann dies mittelfristig zu Schäden am Gerät führen.“

Sicherheitslücke aufspüren und schließen

„Bei den meisten Android-Geräten lässt sich die Sicherheitslücke sehr einfach schließen. Besitzer eines solchen Smartphones sollten in den Einstellungen nach den Entwickleroptionen Ausschau halten und sie deaktivieren“, verrät Burris als Lösung des Problems. Als Benutzer solle man generell den kurzen Blick in die Einstellungen wagen, um sicher sein zu können, dass nicht doch die Entwickleroption eingeschaltet ist. Für all jene Anwender, die sich unsicher sind, ob der Wurm auf dem Mobiltelefon vorhanden ist, empfiehlt G DATA folgende Schritte durchzuführen:

1. Laden sie ADB für Windows herunter
2. Extrahieren Sie den Inhalt der ZIP-Datei an einen leicht zu merkenden Ort – beispielsweise Ihren Desktop
3. Im Falle von Windows 10 nutzen Sie die Tastenkombination Shift + rechter Mausklick und wählen Sie „PowerShell-Fenster hier öffnen“ aus. Achten Sie dabei, dass Sie die Tastenkombination in dem zuvor extrahierten Ordner benutzen.
4. Es öffnet sich das Entwicklerfenster.
5. Verbinden Sie das Android-Smartphone via USB mit dem Computer
6. Im Falle einer offenen ADB-Schnittstelle, öffnet sich nun ein Fenster auf dem Smartphone (siehe Screenshot). Bestätigen Sie hier mit OK.
Hinweis: Sollte sich kein Fenster dieser Art öffnen, so ist die Entwickleroption bei Ihnen ausgestellt.
7. Im Entwicklerfenster gilt es folgenden Befehl auszuführen:

```
.\adb shell pm list packages  
com.android.good.miner
```
8. Sollte das Gerät nicht infiziert sein, so gibt es keine Rückmeldung in der Entwicklerkonsole. Ansonsten erscheint folgende Meldung:

```
package: com.android.good.miner
```

Den Wurm ADB.Miner in wenigen Schritten entfernen

Wenn der Benutzer eine Rückmeldung erhalten hat, so ist das Gerät kompromittiert. G DATA erklärt in wenigen Schritten, wie der ADB.Miner vollständig entfernt werden kann:

1. Bleiben Sie in der Entwicklerkonsole und geben Sie folgenden Befehl ein:

```
.\adb shell pm list packages uninstall  
com.android.good.miner
```
2. Im letzten Schritt gilt es die temporären Dateien zu löschen. Der Vorgang ist besonders wichtig, da ansonsten der Wurm immer wieder automatisch installiert wird. Dies wird mit folgenden vier Befehlen umgesetzt:

```
.\adb shell  
cd /data/local/tmp/  
rm *  
exit
```

Im Anschluss empfiehlt es sich in jedem Falle die Entwickleroption zu deaktivieren. Für generellen Schutz unterwegs empfiehlt sich eine Mobile Internet Security für Android, wie beispielsweise jene von G DATA. Sie

G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG
G DATA Campus
Königsallee 178
44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de
Tel.: +49 (0) 234 9762-239
Fax: +49 (0) 234 9762-299

Pressemitteilung

verhindert nicht nur den Befall von Schadsoftware auf dem mobilen Gerät, sondern bietet darüber hinaus noch viele nützliche Funktionen, wie zum Beispiel das Löschen von Dateien aus der Ferne, sollte das Smartphone einmal verloren gegangen und in falsche Hände geraten sein.



G DATA CyberDefense AG
Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299