G DATA press release 2018

Vulnerabilitate critica: Primul vierme de Android a fost descoperit

Expertii in domeniul securitatii datelor de la G DATA raporteaza cu privire la constatarile lor si explica modul in care se poate inchide bresa.

Mii de smartphone-uri din intreaga lume sunt afectate de un vierme de Android. Acest lucru se datoreaza unei brese de securitate cauzata de o interfata de depanare uitata. Vulnerabilitatea nu este inca rezolvata. G DATA explica pericolul si arata modul in care utilizatorii pot verifica daca dispozitivul mobil este afectat si, daca este, cum poate fi inchisa bresa de securitate.

O terta parte necunoscuta acceseaza propriile noastre smartphone-uri prin Internet, cu drepturi depline de administrator. Ceea ce se poate interpreta ca un caz complicat si imposibil de imaginat devine un simplu joc pentru atacatorii cibernetici datorita unei brese de securitate din sistemul de operare Android. Datorita portului TCP 5555 deschis, atacatorii se pot conecta la dispozitiv prin intermediul interfetei de debug Android (ADB pe scurt). ADB poate fi utilizat pentru a efectua o varietate de actiuni asupra dispozitivului - de la citirea simpla a informatiilor de pe dispozitiv, la furtul datelor sensibile, pana la instalarile critice de securitate ale programelor malware. "ADB este de fapt utilizat de dezvoltatorii de software pentru a avea acces direct la dispozitive in scopul de a efectua diagnostice sau post-instalari", spune Alexander Burris, Lead Mobile Researcher la G DATA. Implicit, aceasta interfata este in mod normal dezactivata. "Cu toate acestea, exista unii producatori, de exemplu, ca in acest caz din Asia, care par sa fi esuat in tentativa de inchidere a interfetei ADB activata inainte de a comercializa produsele".

Android worm ADB.Miner exploateaza vulnerabilitatea

Primul vierme Android numit ADB.Miner foloseste interfata ADB deschisa. Atunci cand doreste sa se conecteze la un smartphone, o interogare USB de depanare apare. Daca se da clic pe OK, dispozitivul mobil este infectat. Viermele scaneaza Internetul pentru porturile TCP 5555 deschise, creand un botnet criptomining. Dispozitivul este astfel compromis si utilizat in mod gresit pentru a mina o moneda virtuala numita "XMR Coin". Daca dispozitivul este infectat, se cauta automat porturi deschise suplimentare, altele decat 5555 TCP, astfel incat viermele sa se poata raspandi in continuare. "Cu cat mai multe smartphone-uri Android sunt afectate, cu atat mai repede se poate raspandi viermele", spune Burris. "Pentru utilizatori acest lucru inseamna o afectare foarte puternica a performantei telefonului, precum si o viata extrem de scurta a bateriei. Deoarece smartphone-urile nu sunt proiectate pentru o astfel de utilizare permanenta, acest lucru poate duce la deteriorarea dispozitivului pe termen mediu.

Detectarea si inchiderea breselor de securitate

"Pentru majoritatea dispozitivelor Android, vulnerabilitatea este foarte usor de inchis. Proprietarii unui astfel de telefon inteligent ar trebui sa caute optiunile pentru dezvoltatori din setari si sa le dezactiveze", recomanda Burris ca o solutie la problema. Ca utilizator, ar trebui sa examinati rapid setarile pentru a va asigura ca optiunea developer nu este activata. Pentru toti utilizatorii care nu sunt siguri daca viermele este prezent pe telefonul mobil, G DATA recomanda urmatorii pasi:

1. Descarcati ADB for Windows

2. Extrageti continutul fisierului ZIP intr-o locatie usor de memorat - cum ar fi desktopul

3. In Windows 10, apasati Shift + butonul din dreapta al mouse-ului si selectati " Open PowerShell window here". Asigurati-va ca utilizati combinatia de taste din dosarul extras anterior.

4. Se deschide fereastra dezvoltatorului.

5. Conectati smartphone-ul Android la computer prin USB

6. In cazul unei interfete ADB deschise, pe smartphone se deschide o fereastra. Confirmati aici cu OK. Nota: daca nu se deschide o astfel de fereastra, optiunea dezvoltatorului este dezactivata.

7. In fereastra dezvoltatorului, executati urmatoarea comanda:. \ Adb shell list list com.android.good.miner

8. Daca dispozitivul nu este infectat, nu exista raspuns in consola pentru dezvoltator. In caz contrar apare urmatorul mesaj: package: com.android.good.miner.

-###-