# Žad Deljkić: Android USB vektor napada

## Dnevnik rada

### 1. tjedan (28.3.2016. - 3.4.2016.)

#### Dosadašnji rad

Do sada sam razvio prototip aplikacije za Android uređaje sa instaliranim Kali NetHunterom koja može preko USB-a detektirati OS te pokrenuti USB HID napad, te sam napisao nacrt rada na engleskom.

Napisao sam plan rada koji je okvirno dogovoren na početnom sastanku u petak 24.3. Trenutno istražujem što je moguće sa USB napadima, načine detektiranja OS-a preko USB-a te moguće zaštite protiv USB napada.

Dok sam istraživao zaštite protiv USB napada općenito, došao sam opet i do Qubes-a, OS-a koji je općenito fokusiran na sigurnost te ju postiže gotovo ekstremnom izolacijom, te sam ga sada i instalirao i trenutno ga isprobavam. Autori su svjesni raznih napada, između ostaloga i USB napada. No ako korisnik koristi USB tipkovnicu i/ili miš, ne postoji nikakva ugrađena zaštita od USB napada. I dalje je vjerojatno moguće nekako ručno zabraniti novim USB uređajima da se spoje (što opet nije idealno rješenje). USB HID napad (isprobao sam simuliranje tipkovnice) funkcionira na Qubes-u, moguće je direktno napasti dom0, najsigurniju domenu, no detektiranje OS-a ne funkcionira, računalo se ne spaja automatski na mrežu sa mobitelom.

#### Daljnji koraci

Jednom kada je istraživanje gotovo, osmisliti daljni smjer rada - što je točno problem kojim će se rad baviti, te kako ćemo ga rješiti.

Plan je napraviti nešto novo. Jedna opcija je nastaviti s već razvijenom aplikacijom, završiti ju te joj potencijalno proširiti funkcionalnosti. Druga opcija je osmisliti i implementirati novi USB napad koji do sada nije bio istražen, ukoliko pronađemo nešto takvo.

### 2. tjedan (4.4.2016. - 10.4.2016.)

#### Dosadašnji rad

Prikupio sam literaturu koja bi mogla biti vezana uz ovaj rad te ju sortirao u kategorije:

- USB napadi sa Androida na PC
- Napadi na Android (kojima bi se mobitel mogao “zaraziti” tako da kasnije može napasti računala s kojima se spoji)
- Obrane od USB napada
- Detekcija OS-a preko USB-a

Literatura se nalazi u Zotero grupi.

#### Daljnji koraci

Pročitati i odrediti koja je literatura najrelevantnija, te ovisno o postojećim radovima odrediti daljnji smjer ovog rada kako bi se napravilo nešto novo.

Za sada okvirnim pregledom svih radova nisam naišao na ništa slično aplikaciji koju sam razvio, tako da mi se čini da bi nastavak u tom smjeru bio dobar.

### 3. tjedan (11.4.2016. - 17.4.2016.)

#### Dosadašnji rad

Pročitao sam literaturu, organizirao ju te napisao bilješke o bitnim dijelovima (sve je u Zotero grupi).

Postoji velika količina radova koji se bave USB

#### Daljnji koraci

Pročitati i odrediti koja je literatura najrelevantnija, te ovisno o postojećim radovima odrediti daljnji smjer ovog rada kako bi se napravilo nešto novo.

Za sada okvirnim pregledom svih radova nisam naišao na ništa slično aplikaciji koju sam razvio, tako da mi se čini da bi nastavak u tom smjeru bio dobar.