Port Fail i trebamo li zbog njega brinuti?

Nedavno otkriveni propust kojem su podložni mnogi davatelji VPN usluga jedna je od relativno rijetkih neugodnosti koje mogu zaskočiti korisnike VPN usluge. Riječ je o kreativnom korištenju ***port forwarding*** opcije na strani napadača; napad je zanimljiv, nije trivijalan, ali nije niti kompliciran i od napadača traži od obavi određene predradnje:

- napadač treba saznati izlaznu IP adresu VPN tunela žrtve;
- zatim, napadač se treba spojiti na isti VPN izlaz kao i žrtva;
- napadač treba aktivirati *port forwarding* svoje veze na izlaznom VPN serveru;
- najzad, žrtvu treba prevariti da kontaktira *forwardirani port* na serveru

Autori otkrića savjetuju klasičnu prijevaru [1] s ugnježđenom grafičkom datotekom, ali poslužit će bilo koja prijevara koja će žrtvu ili softver koji žrtva koristi nagnati na otvaranje veze prema tom portu – količina i sadržaj podataka su posve nebitni, bitno je samo otvoriti komunikacijski kanal.

U trenutku kad žrtva uspostavi kontakt s forwardiranim portom na VPN serveru napadač može saznati njenu stvarnu (tj. ulaznu) IP adresu.

Zanimljivost ovog napada je u jednostavnosti trika: napadaču je dovoljno aktivirati *port forwarding* na serveru kojim upravlja i svaki klijent koji na ovaj ili onaj način klikne na podmetnuti link otkrit će svoju ulaznu IP adresu.

Autori preporučuju dvije metode zaštite: korištenje više IP adresa na strani davatelja VPN usluge (jedna IP adresa za dolazne i jedna za odlazne veze) ili postavljanje odgovarajućih vatrozidnih pravila koja zabranjuju korisnicima pristup preusmjerenim portovima koji nisu njima namjenjeni (tj. koji nisu otvoreni specifično za tog korisnika).

Koliko je uistinu opasan ovaj (nekako simpatičan) trik? U suštini, velike opasnosti nema: sve što napadač saznaje o žrtvi jest njena stvarna IP adresa. Za dobivanje drugih podataka napadač mora koristiti "klasične" tehnike napada ili obmane, no to već izlazi iz domene VPN konekcije.

Naravno, nije bezopasno znati nečiju točnu IP adresu, posebice ako postoji dobar razlog zašto netko komunicira kroz VPN mrežu. S druge strane, postoji tako veliki broj dobrih i posve opravdanih razloga za korištenje VPN mreže pri čemu je korisniku posve nebitno može li netko saznati njegovu stvarnu IP adresu (jer cilj je zaštititi promet, a ne podatak gdje se trenutno nalazite), pa ovaj propust u većini slučajeva nije značajan.

Port Fail možda će otkriti gdje se točno nalazite, ali neće otkriti što točno komunicirate i s kim. Dapače, nalazite li se iza kakvog NAT-a (najčešća situacija, posebice na javnim i otvorenim mrežama gdje postoji najveća potreba za VPN vezama), napadač se neće pretjerano usrećiti saznavanjem vaše IP adrese; s druge strane, valja imati na umu kako je to dobar prvi korak u fazi prikupljanja informacija o žrtvi, čak i ako napadač trenutno nije u fazi izvršenja direktnog napada na žrtvino računalo.

Nešto nervozniji svakako bi trebali biti oni koji VPN veze koriste kako bi skrivali svoje aktivnosti od ruke zakona ili zviždači koji žele na taj način zaštititi svoj identitet; u tom slučaju već i podatak o IP adresi može biti značajna informacija koja se može iskoristiti u otkrivanju lokacije na kojoj se neka osoba nalazi. Skidačima piratluka možda nije svejedno, no zviždači, politički aktivisti i disidenti bi se

itekako trebali čuvati ovog propusta jer omogućuje vrlo precizno otkrivanje njihove fizičke lokacije.

pon, 2015-12-07 15:32 - Radoslav Dejanović**Kategorije:** Sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1588

Links
[1] https://www.perfect-privacy.com/blog/2015/11/26/ip-leak-vulnerability-affecting-vpn-providers-with-port-forwarding/
[2] https://sysportal.carnet.hr/taxonomy/term/30