ZBS | Združenje bank Slovenije

Sporočilo za javnost

Banke in hranilnice opozarjajo na pazljivost pred okužbo telefonov z zlonamerno programsko opremo

Banke in hranilnice, članice Združenja bank Slovenije (ZBS), v zadnjem času opažajo porast števila napadov na mobilne telefone z namenom zlorab mobilnih bančnih aplikacij. Po podatkih policije je doslej ugotovljenim primerom oškodovanja skupno to, da je bilo prek mobilnih bank opravljeno **nakazilo finančnih sredstev oškodovancev na druge bančne račune**, od tam pa je denar potoval na **kripto menjalnico**.

Način okužbe z zlonamerno programsko opremo še ni znan oz. potrjen, verjetno pa gre za **izrabo ranljivosti** posameznega telefona ali pa celo za nenamerno **namestitev trojanske programske opreme**, ki je bila vključena v eno od aplikacij, ki so na voljo v trgovini Google Play Store. Po podatkih SI-CERT-a sta bili zlonamerni aplikaciji, ki sta omogočili okužbo mobilne naprave, dostopni v Google Play Store pod imenoma **"Phone Cleaner – File Explorer"** in **"PDF Reader: File Manager"**.

Ugotovljeno je bilo tudi, da je bila na telefonih oškodovancev nameščena **zlonamerna programska oprema**, ki je spremljala aktivnosti uporabnikov (npr. vnos PIN-a), nato pa je ta ista programska koda namestila še dodatno programsko opremo, s katero so prevaranti pridobili oddaljeni dostop do žrtvinega telefona (AnyDesk, TeamViewer). Tako so lahko kriminalci v ozadju, brez vednosti žrtve, opravili nakazila denarja z njenega računa na kripto menjalnico. V tem času je telefon postal **neodziven**.

Članice ZBS, banke in hranilnice, strankam svetujejo, da:

- redno **nadgrajujete** svoje mobilne naprave in imate nameščen protivirusni program,
- ste **pazljivi pri nameščanju programske opreme** tudi z zaupanja vrednih spletenih mest,
- ste **pazljivi pri dodeljevanju pravic za dostopnost**, saj tako posamezni programi pridobijo pravice za branje vsebine zaslona in izvajanje klikov brez uporabniške interakcije. Na ta način napadalci **prevzamejo poln nadzor** nad napravo.

Uporabnikom, ki ste škodljivo aplikacijo prenesli, jo odprli in ji dodelili pravice za dostop do vašega telefona, svetujemo, da svojo napravo **zaženete v varnem načinu** in zlonamerno aplikacijo **odstranite**. To storite tako, da držite **tipko (ali tipke) za izklop naprave**, s čimer se na zaslonu odpre meni z možnostmi za izklop naprave kot pri običajnem postopku izklopa (novejše različice telefonov po izbiri ikone za izklop nemudoma ponudijo varen način izklopa, ki ga je treba izbrati). Za zagon naprave v varnem načinu je nato treba na meniju prikaza držati **ikono za izklop,** dokler naprava ne ponudi ponovnega zagona v varnem načinu. V tem načinu se ob vklopu naprave zlonamerna aplikacija ne zažene in **jo lahko varno odstranite.**

Vodja PR aleksandra.zibrat@zbs-giz.si
tel.: 01 24 29 758, 031 716 589
www.zbs-giz.si

Več informacij o tej obliki spletnih prevar je na voljo na spletni strani slovenskega nacionalnega odzivnega centra za kibernetsko varnost SI-CERT na povezavi Kraje sredstev iz mobilnih bank preko okužbe z Anatsa trojanskim konjem - SI CERT .

Združenje bank Slovenije
Ljubljana, 26. februar 2024

Vodja PR aleksandra.zibrat@zbs-giz.si
tel.: 01 24 29 758, 031 716 589
www.zbs-giz.si