firstcom europe

Nyhedsbrev Juni 2021

Bølge af trojanske sms'er rammer danskerne

Danskernes mobiltelefoner er i øjeblikket udsat for en stor stigning i virusangreb. Mængden og alvoren af angrebene er af en sådan karakter, at danske teleselskaber nu sender en kraftig advarsel til danskerne om, at der er falske og skadelige sms'er og apps i omløb. Advarslen gælder særligt den internationalt kendte FluBot-virus, som nu er nået til Danmark.

Denne virus vækker bekymring, da den potentielt kan bruges til identitetstyveri og kreditkortsvindel ved at aflure indhold og koder på Android-telefoner. Samtidig kan download af falske apps eller klik på links i falske sms'er efterlade ejere af både iPhones og Android-telefoner med ekstraudgifter for udlandsopkald eller beskeder, de ikke selv ved eller kan se, at deres mobil har foretaget.

Risiko for spyware på mobilen

Svindlen kan ske via falske sms'er, som fx fortæller modtagerne, at de har fået en ny telefonsvarer og beder dem om at klikke på et link for at få adgang til denne. Ved klik på linket ledes modtagerne hen til en hjemmeside, hvor de bliver bedt om at indtaste personlige oplysninger eller kreditkortoplysninger, eller til en hjemmeside, hvor de opfordres til at downloade en app.

Det er ikke farligt at modtage sms'en, men klikker man på linket og installerer app'en, bliver det muligt for IT-kriminelle fx at foretage opkald til udlandet og sende lignende falske sms'er videre til andre uskyldige fra ens telefon – og i værste fald lægger app'en spyware på mobilen, så indhold og koder kan aflæses. Derfor opfordrer telebranchen nu danskerne til at være særligt forsigtige overfor sms'er med links – også selvom sms'en ser ud til at komme fra en anerkendt og troværdig virksomhed eller et kendt nummer. Er man som forbruger det mindste i tvivl, så opfordrer branchen til, at man kontakter afsenderen, inden man installerer ukendte apps på sin mobil.

Da svindlerne løbende skifter metode, er det vanskeligt at bremse denne type af it-kriminalitet. Endvidere kan teleselskaberne ikke forhindre download og installation af falske apps. Det er derfor vigtigt at brugerne advares.

Telebranchen er i dialog med både Rigspolitiet og Center for Cybersikkerhed omkring spredningen af FluBot-malware i Danmark.

Har du modtaget en fup sms-besked:

1. Klik ikke på linket i meddelelsen og installer ikke nogen apps, hvis du bliver bedt om det.

2. Undlad at indtaste personlige oplysninger eller bankoplysninger

3. Slet meddelelsen

Kommer sms'en fra en virksomhed, du afventer en sms fra eller normalt modtager sms'er fra, gå da i stedet ind på virksomhedens hjemmeside eller kontakt virksomheden på andre kanaler. Lad være med at klikke på links i sms-beskeder, hvis du er det mindste i tvivl.

Har du har klikket på linket for at downloade app'en:

Har du klikket på et farligt link og installeret app'en, så anbefaler vi, at du renser din mobil for at undgå, at dine adgangskoder og onlinekonti potentielt kan hackes.

Indtast ikke adgangskoder på mobilen, før den er renset.

• Genetabler fabriksindstillingerne og genskab en tidligere sikkerhedskopi fra før, den falske app blev installeret. Ved du ikke, hvornår appen er installeret, må telefonen nulstilles

• Hvis du har logget ind på konti eller apps ved hjælp af en adgangskode, siden du downloadede appen, skal adgangskoden til disse konti ændres fra en anden enhed eller efter telefonen er renset. Er samme adgangskoder brugt til andre konti, skal disse også ændres hurtigt