België opnieuw overspoeld door het FLUBOT-virus: telecomoperatoren blokkeren 2 miljoen phishingberichten per dag

Proximus, Telenet en Orange hebben de afgelopen week elke dag tot 2 miljoen valse sms-berichten geblokkeerd. De sms'jes bevatten een link waarachter het gevaarlijke FLUBOT-virus schuilgaat. Dat virus deed in het voorjaar al de ronde en circuleert nu dus opnieuw. Wie het nietsvermoedend installeert, riskeert met een geplunderde bankrekening achter te blijven

Wim Schepens

In het voorjaar zat het FLUBOT-virus verscholen in een bericht dat zogezegd afkomstig was van Bpost. Nu zit het in een bericht dat afkomstig lijkt van pakjesdienst DHL, maar dat verstuurd is door oplichters die via phishing persoonlijke gegevens proberen te ontfutselen. Het bericht meldt dat je een pakje gaat ontvangen, en vraagt om een link te openen. Wie dat doet, krijgt de vraag een app te installeren. Maar wie de app installeert, installeert in werkelijkheid het FLUBOT-virus.

Het virus gaat op zoek naar het adressenboekje in je smartphone en verspreidt zich zo naar de toestellen van al je contacten. Via het virus krijgen de oplichters ook controle over je smartphone. Ze kunnen bijvoorbeeld meekijken als je bankverrichtingen doet en op die manier je rekening leeghalen. De telecomoperatoren hebben de voorbije dagen al 2.000 gsm's geblokkeerd die wellicht besmet waren met het virus, en het verder probeerden te verspreiden. Als dat gebeurt, kun je wel nog bellen en sms'en ontvangen, maar geen sms'en meer versturen. Na een tijd, of nadat je hebt aangegeven dat je het virus hebt verwijderd, kun je opnieuw sms'en.

Wat als je het virus geïnstalleerd hebt?

De valse app verschijnt tussen de andere apps op je scherm en valt niet te verwijderen. Je kan je toestel alleen maar van het virus ontdoen door het terug te zetten naar de fabrieksinstellingen (waardoor je meteen ook alle andere apps verliest die je hebt geïnstalleerd). Een andere manier is je toestel te herstarten in 'safe mode'. Zo kun je wel de valse app (met het virus) verwijderen.

Het is natuurlijk beter de link niet te openen. "Kijk altijd uit als je een link krijgt via sms, en klik daar nooit op", zegt Katrien Eggers van het Centrum voor Cybersecurity België (CCB). "Als je toch op die link klikt, dan zal je gevraagd worden om een app te installeren. Doe ook dat nooit: een app mag je alleen downloaden vanuit een officiële app store." Een screenshot van de valse sms kan je doorsturen naar verdacht@safeonweb.be.

Bron: VRT Nieuws