BELGISCH INSTITUUT VOOR POSTDIENSTEN EN TELECOMMUNICATIE

PERSBERICHT

Het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT) en het Centrum voor Cybersecurity België waarschuwen opnieuw voor tsunami aan smishing berichten na valse sms'en.

Brussel, 14 september 2021 - Sinds vorige week werden meer dan 2 miljoen sms'en per dag geblokkeerd door de mobiele operatoren. Het gevaarlijke Flubot-virus doet immers opnieuw de ronde. Het virus kan de volledige controle over een GSM-toestel overnemen en in naam van het slachtoffer sms'en versturen naar alle telefooncontacten van het toestel en ook andere gsm-nummers. Meer dan 2.000 geïnfecteerde GSM-toestellen werden door de mobiele operatoren reeds geblokkeerd de afgelopen dagen wegens abnormaal veel sms-verkeer.

"De verdachte sms'jes lijken opnieuw in naam van een pakjesdienst te komen. Als je op de link klikt die je krijgt via een SMS, wordt er gevraagd om een applicatie te downloaden. Doe dit in geen geval. Er wordt dan een virus op je toestel geïnstalleerd dat toegang kan krijgen tot je persoonlijke gegevens zoals wachtwoorden, bankkaartgegevens en je volledige contactenlijst.", aldus Katrien Eggers woordvoerder van het CCB.

De sms'en komen van toestellen van klanten die geïnfecteerd zijn met de mobiele malware Flubot (naam van het virus dat wordt verspreid via de sms'en). Het is moeilijk de precieze herkomst van de sms-berichten vast te stellen, omdat de mobiele telefoon van de klant, eenmaal geïnfecteerd, de transportvector wordt naar andere gebruikers. Met andere woorden, deze sms'en komen dus van de legitieme klanten van de telecomoperatoren.

Dringende waarschuwing

Jack Hamande, Raadslid van het BIPT: "Wanneer operatoren vaststellen dat een klant geïnfecteerd is, bijvoorbeeld aan de hand van abnormaal sms-verkeer, blokkeren zij de klant tijdelijk en geven de reden van blokkering en instructies om de malware te verwijderen. Het is dan aan de klant zelf om de mobiele malware van zijn toestel te verwijderen. Het is belangrijk dat de klanten dit doen. De malware verstuurt namelijk ook internationale berichten en kan dus mogelijks leiden tot hoge facturen."

De operatoren blokkeren tijdelijk de nummers van geïnfecteerde klanten. De klant kan dan nog bellen een sms'en ontvangen, maar geen sms'en meer sturen. Na een periode of nadat de klant heeft aangegeven dat de malware is verwijderd, kan de klant opnieuw sms-berichten sturen. Indien er opnieuw verdacht sms-verkeer wordt vastgesteld, wordt de klant opnieuw tijdelijk geblokkeerd.

Sinds vorige week werden meer dan 2 miljoen sms'en per dag geblokkeerd door de mobiele operatoren. Meer dan 2.000 geïnfecteerde GSM-toestellen werden door de mobiele operatoren reeds geblokkeerd de afgelopen dagen wegens abnormaal veel sms-verkeer.

Daarom lanceren het BIPT en het CCB een dringende oproep naar mobiele telefoongebruikers:

1. Wees altijd op je hoede als je onverwacht een berichtje krijgt

2. Klik niet op een link in sms'jes!

3. Installeer nooit applicaties via een link in een bericht
Installeer alleen applicaties uit een standaardapplicatiestore (Google Play, App Store). Als je tijdens de installatie van een app een boodschap krijgt die de installatie verhindert of die waarschuwt voor de veiligheid, ga dan zeker niet verder.

Wie Flubot geïnstalleerd heeft op een mobiel telefoontoestel dient het virus onmiddellijk te verwijderen. Hoe?

Methode 1: Door het toestel terug naar de fabrieksinstellingen te zetten

Methode 2: Door het toestel te herstarten in "safe mode" en vervolgens de valse app te verwijderen

Na het verwijderen van het virus dienen alle wachtwoorden van accounts waar men via de smartphone toegang tot heeft te worden veranderd. Aangezien het kan zijn dat er in naam van het slachtoffer een sms-bericht werd verstuurd naar al de contacten, dienen deze zo snel mogelijk te worden verwittigd.

Slachtoffers zullen ook niet altijd onmiddellijk opmerken dat er zeer veel sms'en werden verstuurd. Op de afrekening van de telefoonkosten kan men echter zien of er massaal berichten verstuurd zijn. In dat geval dient het slachtoffer best contact op te nemen met zijn operator. Pas wanneer de app verwijderd wordt, kan het nummer niet meer misbruikt worden.

Screenshots van frauduleuze berichten kunnen steeds gestuurd worden naar verdacht@safeonweb.be.

Meer info: https://safeonweb.be/nl/actueel/opgepast-voor-het-gevaarlijke-flubot-virus-klik-niet-op-verdachte-smsjes

---

Contactpersonen voor de pers
Katrien Eggers (Woordvoerder CCB, NL/FR) : 0485 765 336, katrien.eggers@cert.be
Jimmy Smedts (Woordvoerder BIPT): 0478/63.91.82, jimmy.smedts@bipt.be

Over het Centrum voor Cybersecurity België
Het Centrum voor Cybersecurity België (CCB) is de nationale autoriteit voor cyberveiligheid in België. Het CCB superviseert, coördineert en waakt over de toepassing van de Belgische cyberveiligheidsstrategie. Door optimale informatie-uitwisseling kunnen bedrijven, de overheid, aanbieders van essentiële diensten en de bevolking zich gepast beschermen. www.ccb.belgium.be

Over het Belgisch Instituut voor postdiensten en telecommunicatie
Het BIPT is de federale regulator die bevoegd is voor de markt voor elektronische communicatie, de postmarkt, het elektromagnetische spectrum van de radiofrequenties en radio- en televisieomroep in het Brussels Hoofdstedelijk Gewest.

Voor meer informatie:

Jimmy Smedts | Woordvoerder

Belgisch Instituut voor postdiensten en telecommunicatie
Ellipsgebouw C | Koning Albert II-laan 35 bus 1 | 1030 Brussel
T +32 2 226 88 22 | **M** +32 478 63 91 82 | **www.bipt.be**