MOBIELE
RANSOMWARE

LET GOED OP UW PERSOONLIJKE BESTANDEN

Ransomware houdt uw mobiele apparaat en alle gegevens die erop staan gevangen en laat ze pas weer vrij als u betaald heeft. Deze variant van malware vergrendelt het scherm van uw mobiele telefoon of voorkomt dat u bepaalde bestanden of functies kunt gebruiken.

HOE WORDT UW APPARAAT BESMET?

Door geïnfecteerde websites te bezoeken.

Door imitaties van legitieme apps te downloaden.

Door te klikken op kwaadwillende links en bijlagen in phishing-mails.

WAT ZIJN DE RISICO'S?

Verlies van al uw gegevens doordat u de fabrieksinstellingen op uw apparaat moet terugzetten.

Cybercriminelen kunnen volledige toegang tot uw apparaat krijgen en uw gegevens delen met derde partijen.

WAT KUNT U DOEN?

Maak regelmatig een back-up van uw gegevens en zorg ervoor dat al uw apps en uw besturingssysteem up-to-date zijn.

Download geen apps van onbekende appstores.

Schakel automatische updates in. Installeer, indien mogelijk, een mobiele-beveiligingsapp die u laat weten wanneer u het slachtoffer bent geworden van ransomware.

Let goed op bij verdachte e-mails en websites die u een onwaarschijnlijk aantrekkelijk aanbod doen of om andere redenen verdacht lijken.

Geef niemand anders beheerderstoegang tot uw apparaat.

Betaal het losgeld niet. U financiert hiermee criminelen en moedigt ze aan om hun criminele activiteiten voort te zetten.

EUROPOL EC3 European Cybercrime Centre | POLITIE | ALERT online | Betaalvereniging Nederland

#MobileMalware