FACTSHEET

Ransomware: het ‘politievirus’

Wat is ransomware?
‘Ransomware’ betekent letterlijk: gijzelingssoftware. Hiermee blokkeren criminelen je computer. Deze digitale afpersers doen zich vaak voor als de politie. Je zou je schuldig hebben gemaakt aan strafbare feiten en daarom een boete moeten betalen. Niets is minder waar: het bericht is niet afkomstig van de politie. De computer blijft ook na betaling geblokkeerd.

Welke varianten bestaan er?
Bij de politie zijn tientallen varianten van ransomware bekend, ook wel het politievirus genoemd. Ook in andere landen heeft men hier last van. Vrijwel altijd wordt de naam van de politie misbruikt om onschuldige computergebruikers op het verkeerde been te zetten. De ernst van de ransomware neemt toe. Zo toonde de eerste versie alleen een geschreven tekst, in jongere versies word je plotseling toegesproken door een stem of worden er door de webcam opnames van je gemaakt.

Voorbeelden van ransomware

Hoe word je slachtoffer van ransomware?
Tot nu toe worden computers vooral met ransomware besmet bij het surfen op het internet. Ransomware wordt daartoe vaak verstopt in advertenties. Je hoeft niet eens altijd bewust op een advertentie te klikken: criminelen verstoppen hun kwaadaardige programmatuur ook soms op 'onzichtbare' plekken op sites. Ransomware kan je in principe overal op het internet oplopen. Wel bevatten pagina's met veel (seks)advertenties gemiddeld genomen vaker ransomware. Websites van bekende 'sterke merken' hebben er juist vaak minder last van. Maar een besmetting is nooit helemaal te vermijden.

Wie zitten erachter en wat doet de politie?
De politie ziet dat er verschillende versies van ransomware bestaan met hun eigen vormgeving, taalgebruik en techniek. Er wordt daarom aangenomen dat er meerdere groepen achter de productie en verspreiding zitten. De criminelen gaan op slimme wijze te werk door vrijwel geen digitale sporen achter te laten, een anonieme betaalwijze aan te bieden en anderen het geld te laten incasseren. Toch worden regelmatig betrokkenen ontmaskerd. De politie doet in internationaal verband onderzoek naar de criminelen en zet zich daarnaast in voor preventie. Bij een besmetting met ransomware is het niet verplicht om aangifte te doen.

Waarom blijft deze ransomware bestaan?
Ook digitale afpersers worden gedreven door geld. Zolang computergebruikers blijven betalen als zij slachtoffer zijn geworden van ransomware, blijft dit probleem bestaan. De criminelen achter de ransomware spelen slim in op het schaamtegevoel door te refereren aan het bezit van illegale bestanden of het downloaden van porno. Veel mensen schrikken van dit bericht en hopen er snel vanaf te zijn na betaling. Niets is minder waar! De politie adviseert met klem om nooit te betalen. Deze blokkade is niet afkomstig van de politie en je computer blijft geblokkeerd, ook als je betaalt.

Hoe groot is het probleem?
In een recent onderzoek (oktober 2013) ontdekte de politie honderden Nederlandse besmettingen in één maand, voor één (nieuwe) variant. Er zijn echter tientallen varianten van ransomware in omloop en hun aantal is groeiende. Antivirusorganisaties hebben een beeld van de hoeveelheid ransomware die door hun software wordt tegengehouden. Hieruit blijkt dat Nederland één van de meest getroffen landen is in Europa. Dat heeft waarschijnlijk te maken met de internetdichtheid, maar mogelijk ook met de betalingsbereidheid. Naar schatting betaalde in 2012 zo'n tien procent van de Nederlandse slachtoffers. Dit percentage daalt inmiddels. Een betaling bedraagt doorgaans 50 of 100 euro.

Wat kunnen winkeliers doen?
De slachtoffers moeten betalen via anonieme betaalcodes, die in veel Nederlandse winkelketens als voucher worden verkocht. Winkeliers kunnen helpen door het eigen personeel goed voor te lichten, zodat niet zomaar vouchers worden verkocht aan slachtoffers van ransomware. De politie heeft tevens een adviesposter ontwikkeld om (tijdelijk) op te hangen. En in Groot-Brittannië is veel succes geboekt met het afdrukken van een waarschuwing op de kassabon waarop ook de betaalcode wordt geprint. De politie hoopt dat de winkeliers in Nederland dit voorbeeld willen volgen.

Hoe kun je besmetting voorkomen?
De kans op besmetting kan worden verkleind door het besturingssysteem en programma's altijd up-to-date te houden, door niet te surfen op het internet zonder antivirusprogramma, door geen onbekende bijlagen van e-mails te openen en door alert te zijn bij het downloaden van software, muziek, films, tv-series, PDF's en andere populaire bestanden. Besmetting is nooit volledig te voorkomen. Soms raken computers besmet via een reguliere website die door de criminelen is gehackt. Een besmetting met ransomware zegt dus niets over het (surf)gedrag van de computergebruiker.

Wat moet je doen als je besmet bent?
Surf op een andere computer (of bijvoorbeeld een smartphone of tablet) naar www.waarschuwingsdienst.nl of www.fraudehelpdesk.nl/virus. Op deze sites vindt u instructies en stappenplannen over hoe ransomware eenvoudig verwijderd kan worden. Komt u hier niet verder mee, dan adviseren we u naar een erkend computerreparateur te gaan. Deze factsheet is digitaal te vinden op www.politie.nl/politievirus.