# Ransomware

PDF Versie

## Wat is Ransomware ?

Je hebt geen toegang meer tot de gegevens op je computer. Deze gegevens werden versleuteld.  Er wordt losgeld gevraagd onder de vorm van virtueel geld zoals bitcoin om de gegevens terug beschikbaar te maken of te decrypteren.

Ransomware is malware (kwaadaardige software) die een ongewenste handeling op een computersysteem uitvoert, bestanden/gegevens versleutelt en vervolgens losgeld ("ransom") eist om deze handeling ongedaan te maken.

De malware verspreidt zich meestal :

- per e-mail in netwerken van bedrijven, administraties, verenigingen of zelfs individuen door een eenvoudige klik op een bijlage (.pdf, .zip of .exe) of op een besmette link ;
- door een eerder besmette website te raadplegen.

De betaling van het losgeld dient meestal te gebeuren via crypto-valuta (voornamelijk bitcoin).

**Opgelet :** Ransomware mag niet worden verward met andere soorten van oplichting (scams of afpersing) waarmee zij bepaalde kenmerken gemeen hebben.

## Wat heb je nodig om klacht neer te leggen?

Indien mogelijk of beschikbaar kan je de volgende zaken meenemen om de klacht sneller te kunnen verwerken:

- Schermafdruk van het "ransomware" scherm dat je ziet op de computer. Of een duidelijke foto hiervan.
- Het Bitcoin-adres naar waar de betaling moet gebeuren. (Een Bitcoin-adres kan er als volgt uitzien: *15KJMTunaXuSjGuVX68k4hZvG6Y7hqauy3*)
- Informatie over het besmette systeem (Merk en model, operating system, serienummer, etc...)
- Indien u weet of vermoedt hoe de besmetting werd opgelopen, zoveel mogelijk informatie hierover verzamelen (bijvoorbeeld: website, pop-up, e-mail, bestand, ...)
- Alle informatie waarover u beschikt omtrent eventuele financiële transacties.
- Alle informatie waarover u beschikt omtrent eventuele communicaties met de dader.

## Wat kan je nog doen?

- Schakel de computer zo snel mogelijk volledig uit en verbreek de connectie met internet en externe harde schijven.
- Verwijder eerst de malware, zodat bestanden niet opnieuw worden versleuteld. Vraag desnoods hulp van een expert.
- Plaats een back-up van de bestanden terug. Voorwaarde is natuurlijk dat er een (recente) back-up is en dat deze niet versleuteld is door de cryptoware.
- Encryptiemethoden verschillen per type software. Sommige decryptiesleutels (van gekende malware) staan gepubliceerd op de website: **nomoreransom.org**

## Hoe vermijd je om opnieuw slachtoffer te worden?

- Installeer een anti-virusprogramma en voer regelmatig updates uit. Een anti-ransomwarefunctie is belangrijk.
- Hou alle software up-to-date, waaronder besturingssysteem, internetbrowser, browseraanvullingen en populaire programma's, zoals Adobe Reader.
- Klik niet op bijlagen en links in e-mails, tenzij je zeker weet dat het vertrouwd is.
- Ransomware is vaak een uitvoerbaar .exe-bestand, vermomd als ander soort bestand, bijvoorbeeld een pdf-document. Schakel  bestandsextensies weergeven, zodat je de vermomming kunt doorzien.

- Maak back-ups. Dat is sowieso verstandig, maar bij ransomware-besmetting vaak het enige redmiddel om verlies van al je gegevens te voorkomen.

## Waar vind je meer informatie?

nomoreransom.org

https://www.safeonweb.be/nl/actueel/laat-belgie-niet-lamleggen-door-ransomware

https://www.nomoreransom.org/declarations/aangifte-doen-van-ransomware.htm