RANSOMWARE

Informatiefolder voor melders

FRAUDEHELPDESK.nl

INLEIDING

Criminelen verdienen veel geld door computers, netwerken en mobiele telefoons te besmetten met ransomware. Dat is kwaadaardige software waarmee apparaten of bestanden worden versleuteld. De gebruiker heeft dan niet langer toegang tot zijn of haar bestanden. De impact van deze vorm van cybercriminaliteit kan enorm zijn. Het verlies van persoonlijke foto's of het tijdelijk stilleggen van een bedrijf kan tot grote emotionele en financiële schade leiden.

In deze brochure gaat de Fraudehelpdesk dieper in op het fenomeen ransomware. We geven antwoord op de meest gestelde vragen en geven tips over hoe u het beste kunt handelen als uw systeem besmet is geraakt.

Wat is ransomware?

Ransomware, ook wel gijzelingssoftware, is een vorm van kwaadaardige software. Het is een klein programma dat een computer, tablet of telefoon blokkeert. Meestal merkt een gebruiker dit vlak na het opstarten van het apparaat. De gedupeerde krijgt een melding op zijn scherm waarin staat dat pas toegang wordt gegeven na betaling van losgeld (*ransom*).

Er zijn verschillende varianten ransomware, die allen op een andere manier werken. Ook is er verschil in impact als een besmetting plaatsvindt. Zo is er ransomware die bestanden versleutelt, ook wel cryptoware genoemd. Deze versleutelde bestanden kunnen dan niet zonder een code geopend worden. Tegen betaling, die vaak in Bitcoins moet worden voldaan, kunnen slachtoffers de code krijgen waarmee ze de versleuteling kunnen opheffen. Overigens wordt afgeraden het gevraagde losgeld te betalen. Hierover verderop meer.

Bij een andere vorm van ransomware verschijnt een venster in beeld dat alle andere schermen wegdrukt. In deze variant worden bestanden niet versleuteld. Wel verlangen de criminelen achter deze malware ook een betaling. Zo niet, dan blijft het venster in beeld, dreigen ze. Dit type heet ook wel *lock screen ransomware*.

Ook zijn er varianten van ransomware die servers besmetten of die diep in het systeem van een computer toeslaan, waardoor deze weigert om op te starten. Deze soorten zijn tot nu toe echter vrij zeldzaam. Ransomware die speciaal is ontwikkeld voor mobiele telefoons komt steeds vaker voor.

Het doel van de criminelen achter de aanvallen met ransomware is natuurlijk geld verdienen. Omdat ze hebben gemerkt dat ze meer geld kunnen vragen aan bedrijven dan aan particulieren, is er een trend zichtbaar waarbij het bedrijfsleven actief wordt aangevallen.

Ik heb ransomware op mijn computer(systeem), hoe kan dit?

Ransomware verspreidt zich meestal via bijlagen bij e-mails. Gedupeerden verwachten een factuur of cv te openen. Later blijkt dit de kwaadaardige software te zijn die vermomd is als bijvoorbeeld een pdf-bestand. Ook kan gijzelsoftware worden aangeboden op websites of via besmette advertenties. Zonder dat de bezoeker het doorheeft, wordt de ransomware op zijn systeem geïnstalleerd.

Ik ben slachtoffer, wat nu?

De criminelen achter de ransomware willen natuurlijk dat u het losgeld betaalt. Toch is ons advies dat niet te doen. Ten eerste biedt betaling geen garantie dat u de gijzeling opheft. Daarnaast houdt u onbedoeld het verdienmodel in stand. Daardoor blijft het voor criminelen aantrekkelijk met deze praktijken door te gaan.

Slachtoffers kunnen een melding doen bij de Fraudehelpdesk. Wij raden gedupeerden aan om ook aangifte te doen bij de politie.

De code is meestal niet te kraken. Slechts in enkele gevallen bleek de ransomware zo slecht gemaakt dat de versleuteling kon worden opgeheven. Wel is een bezoek aan de website Nomoreransom.org de moeite waard. Hier stelt de politie, in samenwerking met verschillende beveiligingsbedrijven, verschillende sleutels beschikbaar. Mogelijk is er al een sleutel te vinden voor de ransomware waardoor u getroffen bent. In dat geval kan de versleuteling kosteloos worden opgeheven. De site wordt regelmatig geüpdatet. Als uw sleutel nog niet de op de site is gepubliceerd, kunt u het na enkele dagen nog eens proberen.

Stappenplan bij besmetting

Stap 1	Blijf rustig. Ook al wordt de druk om te betalen flink opgevoerd, laat uw hoofd niet op hol brengen.
Stap 2	Verbreek de verbinding met internet en ontkoppel externe harde schijven en usb-sticks die nog in verbinding staan met uw computer. Mogelijk kunt u hiermee verdere verspreiding voorkomen.
Stap 3	Betaal niet het gevraagde losgeld. U heeft geen enkele garantie dat u weer toegang krijgt tot uw bestanden. Bovendien helpt u onbedoeld mee deze criminele activiteiten in stand te houden.
Stap 4	Ga naar Nomoreransom.org en bekijk of deze site een sleutel aanbiedt voor de ransomware waardoor u getroffen heeft. **Extra tip:** staat uw sleutel er nu niet bij? Check het over een tijdje nog eens. De site wordt steeds aangevuld.
Stap 5	Komt u niet verder via bovenstaande site, neem dan contact op met een computerexpert bij u in de buurt.
Stap 6	Doe een melding bij de Fraudehelpdesk en doe aangifte bij de politie.

Waarom melden bij de Fraudehelpdesk?

Als u aangifte heeft gedaan bij de politie, valt de omvang van een fraudezaak niet altijd meteen op. Dat komt omdat de aangiften verspreid door het hele land worden gedaan. De Fraudehelpdesk werkt landelijk en bundelt meldingen. Daardoor neemt de kans toe dat de politie er mee aan de slag gaat. Dat heeft tot nu toe al meermaals tot arrestaties en veroordelingen geleid.

Door alle meldingen die we krijgen, houden we ook zicht op de laatste ontwikkelingen. Duikt er een nieuwe vorm van fraude op? Dan kunnen we daar direct voor waarschuwen.

Als slachtoffer van oplichting is het niet altijd eenvoudig uw weg te vinden naar alle instanties die er in Nederland zijn. De medewerkers van de Fraudehelpdesk weten dit wél en kunnen u precies vertellen bij welke organisatie u het best kunt aankloppen. Met onze ondersteuning vergroten we bovendien de kans dat u resultaat boekt bij deze instanties. Ook kunnen we helpen de schade te beperken en onderzoeken of u deze eventueel vergoed kunt krijgen.

Er zijn een hoop bedrijven die onbewust fraudeurs faciliteren, zoals banken, internetproviders of beheerders van datingsites. Hebben wij een vermoeden van fraude, dan stellen wij deze bedrijven op de hoogte zodat zij actie kunnen ondernemen.

De Fraudehelpdesk doet ook een aantal dingen niet. We zijn bijvoorbeeld geen opsporingsinstantie en gaan dus niet zelfstandig achter fraudeurs aan. Ook vergoeden wij niet de geleden schade.

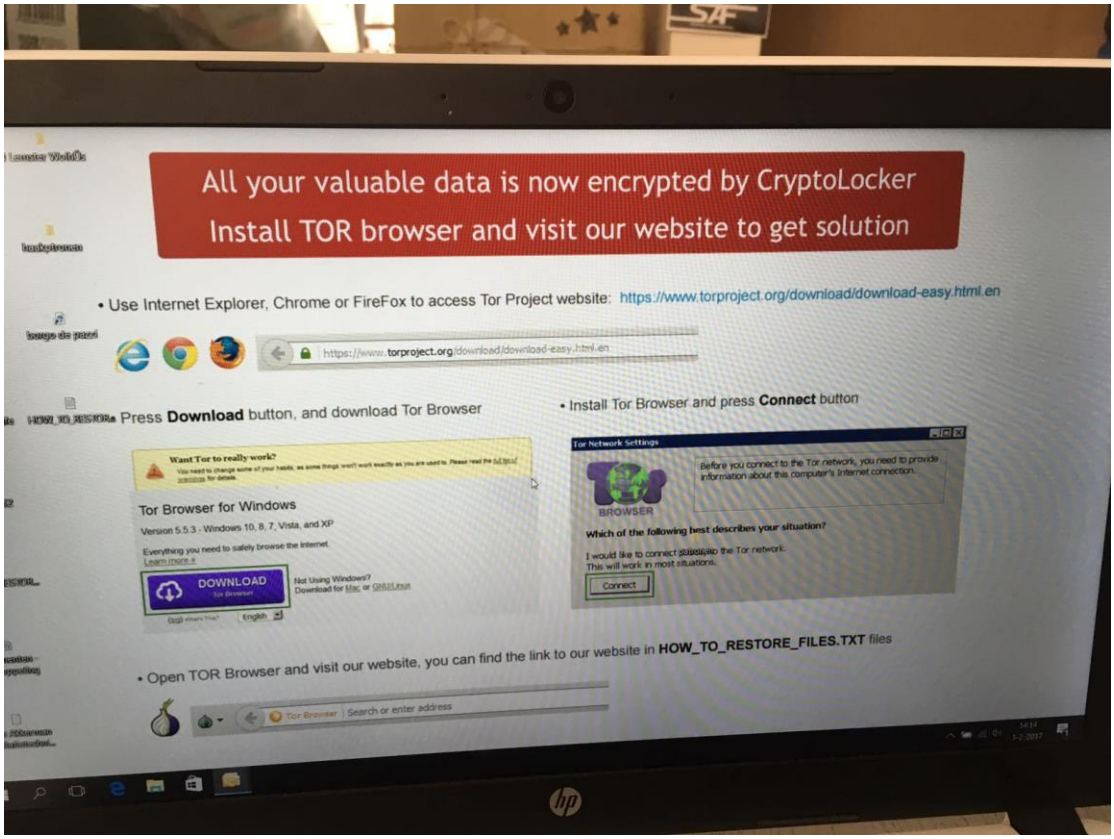
Ervaringsverhaal | ‘Factuur’ geopend, computer op slot

‘Ongelooflijk dat het juist mij overkwam!’

Eigenlijk is Omar* altijd heel erg oplettend. In zijn werk heeft hij met IT te maken, en hij waarschuwt zijn collega’s regelmatig om niet op verdachte linkjes of onbekende bijlagen te klikken. Maar die dag was Omar iets minder alert. Zijn zuster had eerder die maand een auto-ongeluk gehad en lag in het ziekenhuis, en er moest van alles geregeld worden in de familie. Een hectische en emotionele tijd.

En toen kwam dat mailtje van de telecomprovider, persoonlijk aan Omar gericht. Hij stond net op het punt weer naar het bezoekuur te gaan, maar besloot dit even snel af te handelen. De laatste rekening was inderdaad waarschijnlijk niet betaald; vanwege alle drukte was hij namelijk vergeten geld over te boeken naar zijn betaalrekening voor de vaste overschrijvingen. En hij kon nu even geen problemen met afgesloten telefoons gebruiken.

In de haast klikte Omar op de link. Het bleek geen factuur, maar ransomware. ‘Ongelooflijk dat het juist mij overkwam’, zegt Omar terugkijkend. ‘Al mijn bestanden niet meer toegankelijk, waaronder mijn zakelijke administratie, maar ook de trouwfoto’s van mijn zus en foto’s van de geboorte van mijn zoon.’ Toch raakte hij niet in paniek, maar maakte foto’s van het computerscherm.



‘Hopelijk kan ik anderen hiermee helpen, door te waarschuwen voor deze vorm van cybercrime’, zegt Omar. Op de foto is te zien dat het gaat om de ransomware-variant CryptoLocker. De criminelen willen dat Omar een TOR-browser installeert. Dat is een internetprogramma waarmee je anoniem het internet kunt gebruiken. Vervolgens krijgt een slachtoffer dan informatie over wat hij moet doen om weer toegang te krijgen tot zijn bestanden. ‘Ik moest voor een bepaalde datum € 499,- betalen, en als ik dat niet deed, zou het losgeld worden verhoogd tot € 1000,-. Gelukkig maak ik heel regelmatig back-ups, dus ik was niet zo veel bestanden kwijt. Nee, ik heb niets betaald. Dat gun ik die lieden gewoon niet. Bovendien is het geen enkele garantie dat je de bestanden echt terugkrijgt.’

* Omar is een verzonnen naam in verband met privacy.

Met wie neem ik contact op?

- Laat aan de Fraudehelpdesk weten wat er gebeurd is. Wij kunnen u verder verwijzen en adviseren.
- Doe aangifte bij de politie. Vraag eventueel of een digitaal expert aanwezig kan zijn.
- Kijk op Nomoreransom.org om te zien of de sleutel voor uw type ransomware wordt aangeboden.
- Houdt er tevens rekening mee dat de Autoriteit Persoonsgegevens een besmetting met ransomware bij een bedrijf kan beschouwen als datalek.

Meer weten?

Kijk op www.fraudehelpdesk.nl/ransomware voor meer informatie.

KvK Arnhem
09138148

Postadres:
Postbus 963
7901 BE Apeldoorn

T: 088 - 786 7372
E: communicatie@fraudehelpdesk.nl

De Fraudehelpdesk is een activiteit van Stichting Aanpak Financieel-Economische Criminaliteit in Nederland (SafeCin)

www.fraudehelpdesk.nl

FRAUDEHELPDESK.nl