No More Ransom! nu volledig in het Nederlands

Handleiding van Helpmij.nl

Auteur: CorVerm

januari 2017

We hebben al eerder geattendeerd op de website No More Ransom!. Toen was de site nog Engelstalig, maar gelukkig is de site nu ook in het Nederlands. Heel fijn voor wie slachtoffer is geworden van Ransomware en de Engelse taal niet machtig is.

Op de site worden programmaatjes aangeboden die bepaalde Ransomware kunnen ontsleutelen. Je krijgt dan weer toegang tot je bestanden zonder dat je er losgeld voor hoeft te betalen. Hoe de tools werken, tips voor het voorkomen van Ransomware-infecties, en de stappen die je moet ondernemen om aangifte te doen: alle informatie is nu in het Nederlands te lezen.

Link naar No More Ransom!.

Ransomware, of gijzel-software, versleutelt een of meerdere bestanden op je computer. Na betaling wordt het gegijzelde, als je geluk hebt, weer vrijgegeven. Dat gebeurd echter lang niet altijd. De vraag is of het wel verstandig is om “losgeld” te betalen. De kans dat je bestand(en) vrijgegeven worden is niet erg groot. Bovendien is het toegeven aan crimineel gedrag en daar zouden we niet aan mee moeten werken. Maar wat dan wel?

No More Ransom! Beschikt over een twintigtal tools waarmee Ransomware om zeep geholpen kan worden. Een bezoek aan de site is dan ook noodzakelijk. Het eerste dat je te zien krijgt is de vraag:

Klik op **Ja** als dat zo is. Je krijgt nu de mogelijkheid om bestanden, of het bestand (.txt of .html) met het afpersbericht dat is achtergelaten door de criminelen, te uploaden .

Slecht nieuws

Sorry! We hebben nog geen tool voor deze variant van Ransomware maar we zijn druk bezig een oplossing te vinden.
We willen je vragen om een Ransomware-melding en een versleuteld bestand van de onbekende Ransomware te uploaden. Dit helpt ons in ons onderzoek.
We raden je aan om een back-up te maken van je versleutelde bestanden, omdat we in de toekomst hopelijk wel een oplossing hiervoor kunnen vinden.
Check hier om te zien welke oplossingen we wel hebben.
Je kunt ook Aangifte doen.

Gaat het om een bekende Ransomware-variant dan zet No More Ransom! een tool in om je te bevrijden van de narigheid.

Nieuwe Ransomware aangepakt

No More Ransom! werd opgericht door Europol, de Nederlandse politie, Kaspersky en Intel. Aanvankelijk bood de site software aan voor acht verschillende soorten gijzelsoftware, waaronder Teslacrypt, Coinvalt en Wildfire. Dankzij de samenwerking met nieuwe security-bedrijven is het aantal programma's toegenomen tot 20 stuks.

Hulptroepen

Antivirusbedrijven als Check Point, ESET en Bitdefender stellen nu hun kennis beschikbaar rond malware aan No More Ransom!. Hierdoor kunnen meer slachtoffers gratis geholpen worden. Autoriteiten uit 22 verschillende landen zijn ook bij het initiatief betrokken. Voor een overzicht van alle Ransomware die zonder hulp van criminelen te ontsleutelen zijn, kun je kijken op nomoreransom.org.
Maar wat als je helemaal geen toegang meer hebt tot je computer? In dat geval zou je gered kunnen zijn als je back-ups van je bestanden hebt maakt. Dat kan in de Cloud of op een externe harde schijf. Mocht je er (nog) niet aan toegekomen zijn om back-ups te maken, maak er dan een prioriteit van. Een back-up kan ook voorkomen dat je alle bestanden verliest in het geval van diefstal, brand of hardware die niet meer werkt.

Malware voorkomen

- Installeer een goede virusscanner en zorg dat deze minimaal 1 keer per dag automatisch bijwerkt.
- Houd alle software up-to-date, waaronder besturingssysteem, internetbrowser, browseraanvullingen en populaire programma's, zoals Adobe Reader. Met Flexera PSI of ScanCircle zie je hoe je pc ervoor staat. Voor software als Adobe Flash of Javascript is uitschakelen of beperkt instellen aan te raden.
- Klik niet op bijlagen en links in e-mails, tenzij je zeker weet dat het vertrouwd is. Twijfel je, kijk dan op Fraudehelpdesk of de e-mail daar voorkomt. Zo niet, wacht dan een dag en controleer nogmaals.
- **Cryptoware** is vaak een uitvoerbaar .exe bestand, vermomd als ander soort bestand, bijvoorbeeld een pdf-document. Schakel daarom bestandsextensies weergeven in.
- En nogmaals: back-ups maken. Dat is sowieso verstandig, maar bij Ransomwarebesmetting vaak het enige redmiddel om verlies van al je gegevens te voorkomen.

Wat is cryptoware?

Cryptoware gijzelt bestanden door middel van versleuteling en zijn dus niet meer te openen. Openen van bestanden kan alleen door middel van betaling. Betalen kan alleen met Bitcoins en omgerekend wordt er een bedrag van enkele honderden euro’s gevraagd. Besmetting vindt plaats via e-mailbijlages of niet bijgewerkte software. Verdachte bestanden zijn: zip-, exe-, js-, ink- en wsf-bestanden. Ook Word bestanden die vragen om macro's in te schakelen zijn gevaarlijk. Nepmedewerkers van Microsoft dien je “buiten de deur” te houden, zij beweren dat je pc problemen heeft en willen op afstand inloggen. Geheid dat je bestanden daarna zijn geblokkeerd. Cryptoware kan ook bestanden besmetten op aangesloten externe harde schijven of netwerkopslag die in Windows Verkenner een schijfletter hebben. Bewaar een back-up daarom op een andere pc.