

NIEUWE MALWARE TREFT BELGISCHE INTERNETGEBRUIKERS

Kwaadaardige software blokkeert computers van eindgebruikers en **lijkt** afkomstig van eCops

Sinds enkele dagen worden steeds meer mensen slachtoffer van een kwaadaardige software die de computer van de slachtoffers blokkeert. De geblokkeerde computer beeldt onderstaande schermen af:



Hoewel het scherm laat geloven dat de blokkering is gebeurd door de eCops omwille van overtredingen van de Belgische wetgeving, is dit geenszins het geval. Achter deze blokkering zitten cybercriminelen die u er op deze wijze toe willen brengen om hen geld over te maken.

Wijze van verspreiding - schadelijke effecten

De personen die een dergelijk scherm afgebeeld zien op hun computer, zijn het slachtoffer van een infectie. Uit de eerste verklaringen van slachtoffers, blijkt dat de meesten werden geïnfecteerd terwijl ze online spelletjes speelden. Na het heropstarten kregen zij het scherm dat de computer blokkeert.

Andere gekende manieren voor verspreiding van dergelijke virussen zijn:

-
- via een bijlage in een e-mail
- via illegale kopies van software die wordt verspreid in peer-to-peer netwerken
- via berichten in sociale netwerken zoals Facebook die doorverwijzen naar websites om video's te bekijken (die website meldt dan dat je videosoftware moet worden bijgewerkt en toont een setup-popup).

De computer van het slachtoffer wordt geblokkeerd en enkel het scherm met de betalingsmogelijkheid is nog toegankelijk. Momenteel hebben we geen zicht op de verdere effecten die deze kwaadaardige software veroorzaakt. De eerste analyse van de computer van een slachtoffer is momenteel aan de gang.

Gekende gevallen in het buitenland

Soortgelijke gevallen zijn reeds gekend in het buitenland. Daar bleek deze software niet alleen de computer van het slachtoffer te blokkeren maar ook alle gebruikersbestanden te

vercijferen.

Het slachtoffer krijgt hierdoor geen toegang meer tot zijn bestanden. Beschikt de gebruiker op dat ogenblik niet over een back-up, dan wordt werken wel heel moeilijk.

Ervaring uit de buitenlandse dossiers toont aan dat slachtoffers die betaalden, vaak niet eens een code kregen om hun systeem te deblokkeren of te ontcijferen.

Wat te doen als je nog geen slachtoffer bent?

Installeer een antivirus, update naar de laatste versie en voer onmiddellijk een scan uit van je volledige computer.

Maak een back-up van je gegevens op een externe harde schijf en bewaar deze daarna zonder dat de harde schijf nog is gekoppeld aan je systeem.

Wat te doen als je wel slachtoffer bent?

Onmiddellijke actie

Neem een foto van alle mogelijke afbeeldbare schermen van je computer en bewaar deze om bij je dossier te voegen.

Noteer welke acties je laatst op je systeem hebt uitgevoerd en het tijdstip.

Betaal niet!

Klacht

Je kan als slachtoffer van deze kwaadaardige software klacht indienen bij de lokale politie en vragen om het FCCU (Federal Computer Crime Unit) hiervan in te lichten.

Heb je al betaald, kom dan zeker klacht neerleggen met alle informatie omtrent de bestemming van de betaling en omtrent de reactie vanwege de cybercriminelen.

Verdere acties

Het FCCU (Federal Computer Crime Unit) zal de coördinatie uitvoeren tussen de verschillende dossiers om zo snel mogelijk een beter zicht te krijgen op de omvang van de infectie en de technische aspecten ervan.