BUURT-BIN

NIEUWSFLASH

20-06-'12

NR 44-B **Voor KAMMENSTRAAT en OMGEVING**

(Kammenstraat-Hondsberg-Hemelrijkweg-Lazaret-Schuurblok-Kloosterstraat-Grensstraat-Handelsstraat-Hemelrijklaan-Statievelden)

Noodnummer: 101 of **112** of **03/620 29 29** (zie ook: www.binkammenstraat.tk)

Rekeningnummer voor BIN-lidmaatschap: BE79-7795-9630-7433

Geachte Binleden,

AANVULLING van de Politie, betreft de COMPUTERCRIMINALITEIT:
In het verleden hebben wij reeds melding gemaakt van feiten van "randsomware". Momenteel krijgen wij nog steeds deze meldingen. Gelieve de nodige preventieve maatregelen te treffen, eventueel een bootable USB-stick achter de hand houden. Hieronder de uitleg van de FederaleComputerCrimeUnit met oplossing voor het verhelpen van het probleem.

Mvg

Sven Vleugels Hoofdinspecteur
Politiezone Grens
03/620.29.29
email: info@pzgrens.be
website: www.pzgrens.be

Criminaliteit op internet: Ransomware

Kwaadaardige software blokkeert PC's van eindgebruikers en lijkt afkomstig van Ecops, FCCU of een andere buitenlandse politiedienst

Sinds enkele maanden blijken steeds meer mensen slachtoffer te worden van een kwaadaardige software die de PC van de slachtoffers blokkeert.
Hoewel het scherm laat geloven dat de blokkering is gebeurd door de eCops omwille van overtredingen van de Belgische wetgeving, is dit helemaal niet het geval.

Achter deze blokkering zitten cybercriminelen die u er op deze wijze ertoe willen brengen om aan hen geld over te maken.

Recent dook er een variatie op van de scherm-layout:

Wijze van verspreiding - schadelijke effecten

De personen die een dergelijk scherm afgebeeld zien op hun PC, zijn slachtoffer van een infectie van hun PC. Uit de eerste verklaringen van slachtoffers, blijkt dat de meesten werden geïnfecteerd terwijl ze online spelletjes speelden. Na het heropstarten van de PC kregen zij het scherm dat de PC blokkeert.
Andere gekende manier 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 uw videosoftware moet worden bijgewerkt en toont een setup-popup.)

De PC van het slachtoffer wordt geblokkeerd en enkel het scherm met de betalingsmogelijkheid is nog toegankelijk.

Momenteel hebben we geen verder zicht op de verdere effecten die deze kwaadaardige software veroorzaakt. De eerste analyse van de PC van een slachtoffer is thans aan de gang.

Gekende gevallen in het buitenland

Soortgelijke gevallen zijn al gekend in het buitenland. Daar bleek deze software niet alleen de PC van het slachtoffer te blokkeren maar ook alle gebruikersbestanden op de PC 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 tonen 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 uw volledige PC.

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

Wat te doen als je slachtoffer bent ?

Betaal NIET

Als u betaald heeft, neem dan zo snel mogelijk contact op met:

Ukash	**PaysafeCard**
Blokkeren van de PIN via de telefoonnummer - 00 800 000 85274 of - 00 800 247 85274 Met de PIN nummer en het bedrag van het ticket	Blokkeren van de PIN via de telefoonnummer - 078/ 158 157 (hotline op het ticket) of - 00 800 0729 7233 Met de PIN nummer en het bedrag van het ticket.

Klacht

U kunt als slachtoffer van deze kwaadaardige software klacht neerleggen bij de lokale politie en vragen om FCCU hiervan in te lichten.
Hebt u al betaald, kom dan zeker klacht neerleggen met alle informatie (code voucher) omtrent de bestemmeling van de betaling en omtrent de reactie vanwege de cybercriminelen. Breng, indien u kunt, de voucher mee naar de lokale politie.

Verdere acties

FCCU zal de coördinatie uitvoeren tussen de verschillende dossiers om zo snel mogelijk een beter zicht te krijgen op de omvang van de infectie en van de technische aspecten ervan.Zodra er meer informatie gekend is, zullen navolgende berichten worden verspreid.

MOGELIJKE OPLOSSING

Verwijderen van de ransomware "Ecops", "FCCU", of andere buitenlandse politiedienst

Benodigdheden:
- Niet geïnfecteerde computer verbonden met het internet
- USB drive

Op de website : http://windows.microsoft.com/en-US/windows/what-is-windows-defender-offline?SignedIn=1 is er de mogelijkheid gratis software te downloaden, **"Windows Defender Offline"** genaamd.

Deze software is bedoeld om een USB drive te maken om de besmette computer via deze USB drive op te starten. De software zal dan de computer scannen op virussen en malware.

Stappen:

- Download de juiste versie van de software in functie van het besturingssysteem van de besmette computer (32 bit of 64 bit) op: http://windows.microsoft.com/en-US/windows/what-is-windows-defender-offline?SignedIn=1

Voer vervolgens de software uit. U krijgt dan volgend scherm:

Klik op Next..

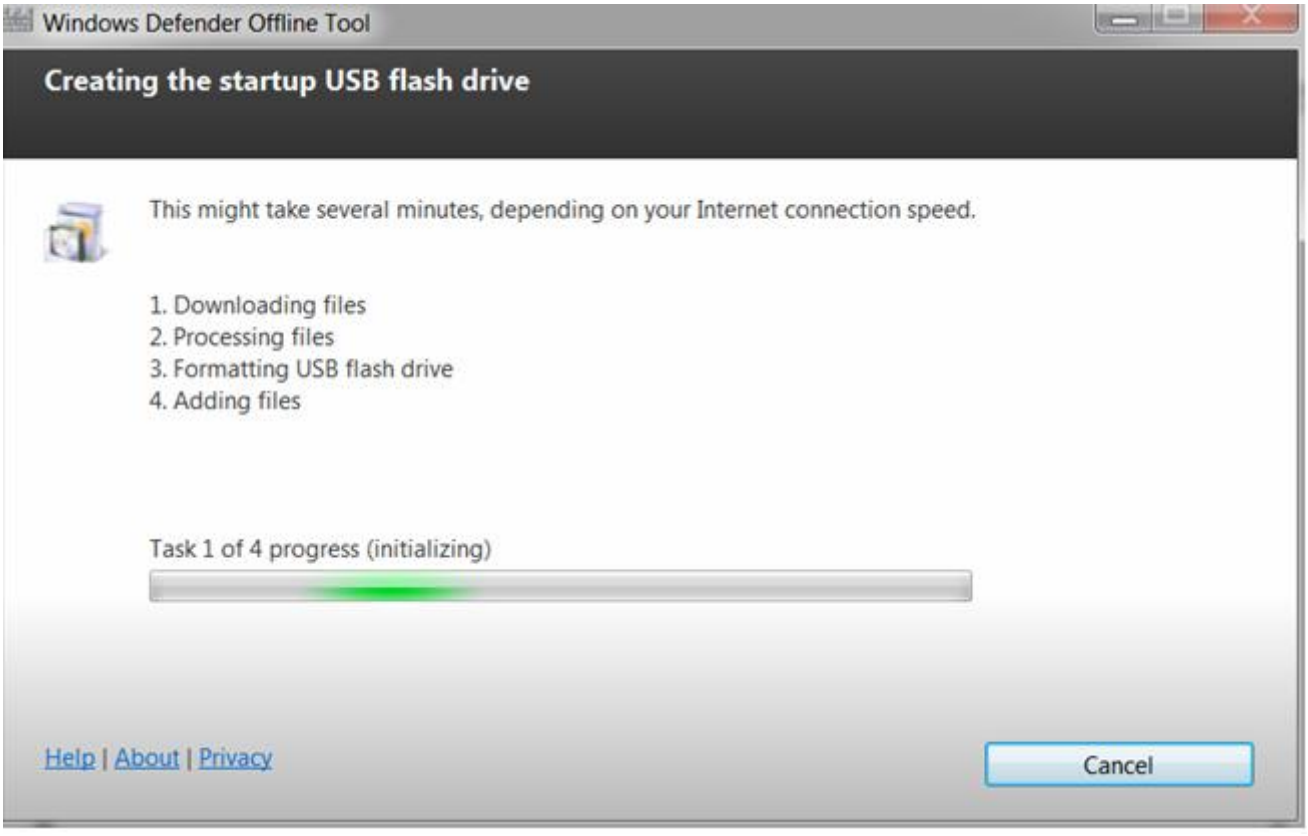
- Steek vervolgens een USB drive in je computer. Let op dat er geen gegevens op deze USB drive staan want deze wordt geformatteerd.

k

- U hebt de keuze om verschillende media te beschrijven. Wij opteren hier voor een USB drive, de 2de keuze in het scherm.

  Klik op Next.

De bootable USB drive wordt nu aangemaakt.

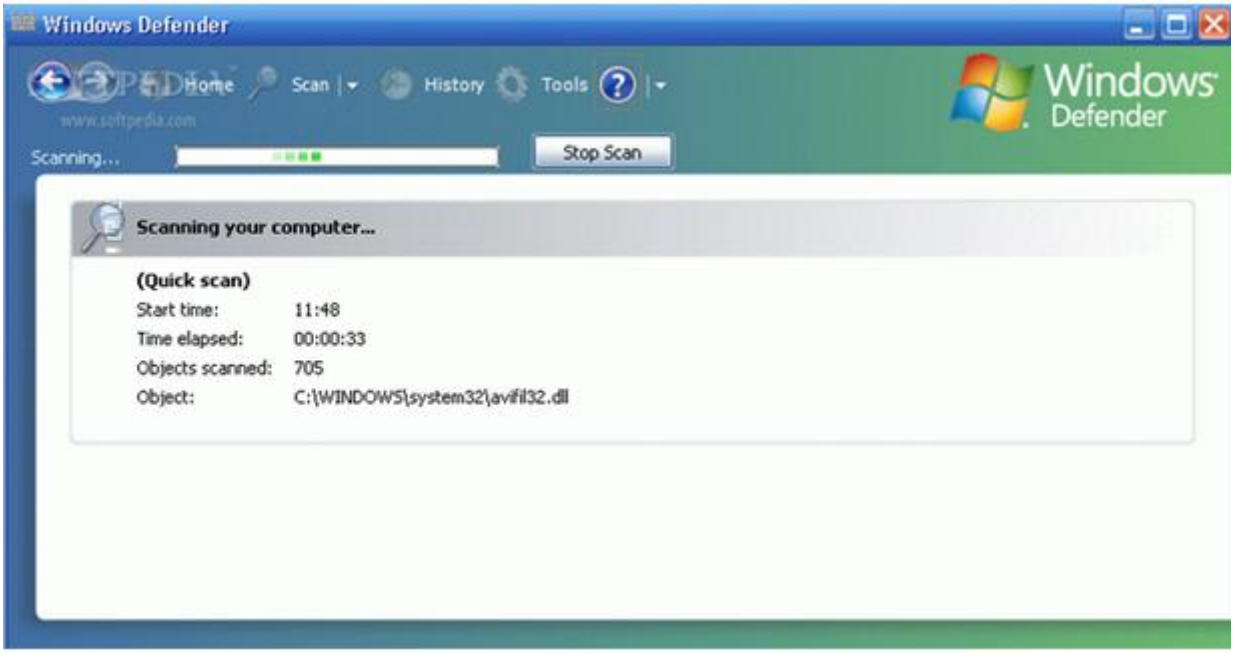


Wanneer stap 4 bereikt is, heb u een bootable USB drive aangemaakt. D.w.z. dat u hiermee uw geblokkeerde computer kan opstarten. Let wel dat uw computer zo ingesteld staat dat hij, wanneer hij

opstart, eerst gaat kijken naar de USB drives. Hiervoor dient u uw BIOS aan te passen of bij opstarten de toest F12 te gebruiken. Wanneer u hiermee niet vertrouwd bent, kunt u best hulp inroepen.

Als de BIOS juist is ingesteld, en de USB drive steekt in, zal de computer opstarten vanaf de USB drive.

De computer zal dan gescand worden.



Wanneer de scan is voltooid, werkt de computer terug normaal. U dient nu wel nog een volledige scan uit te voeren met een antivirus- en een antimalwareprogramma die up to date zijn. Nog beter is om Windows op uw computer te herinstalleren.

Met vriendelijke groeten,

Uw BIN-bestuur van KAMMENSTRAAT EN ZIJSTRATEN.

BIN : SAMEN VEILIG.