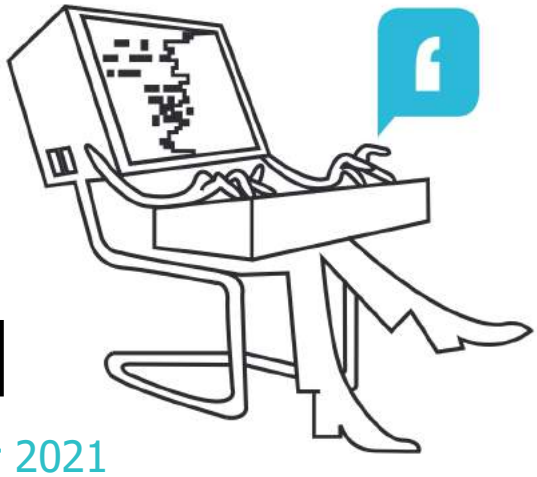
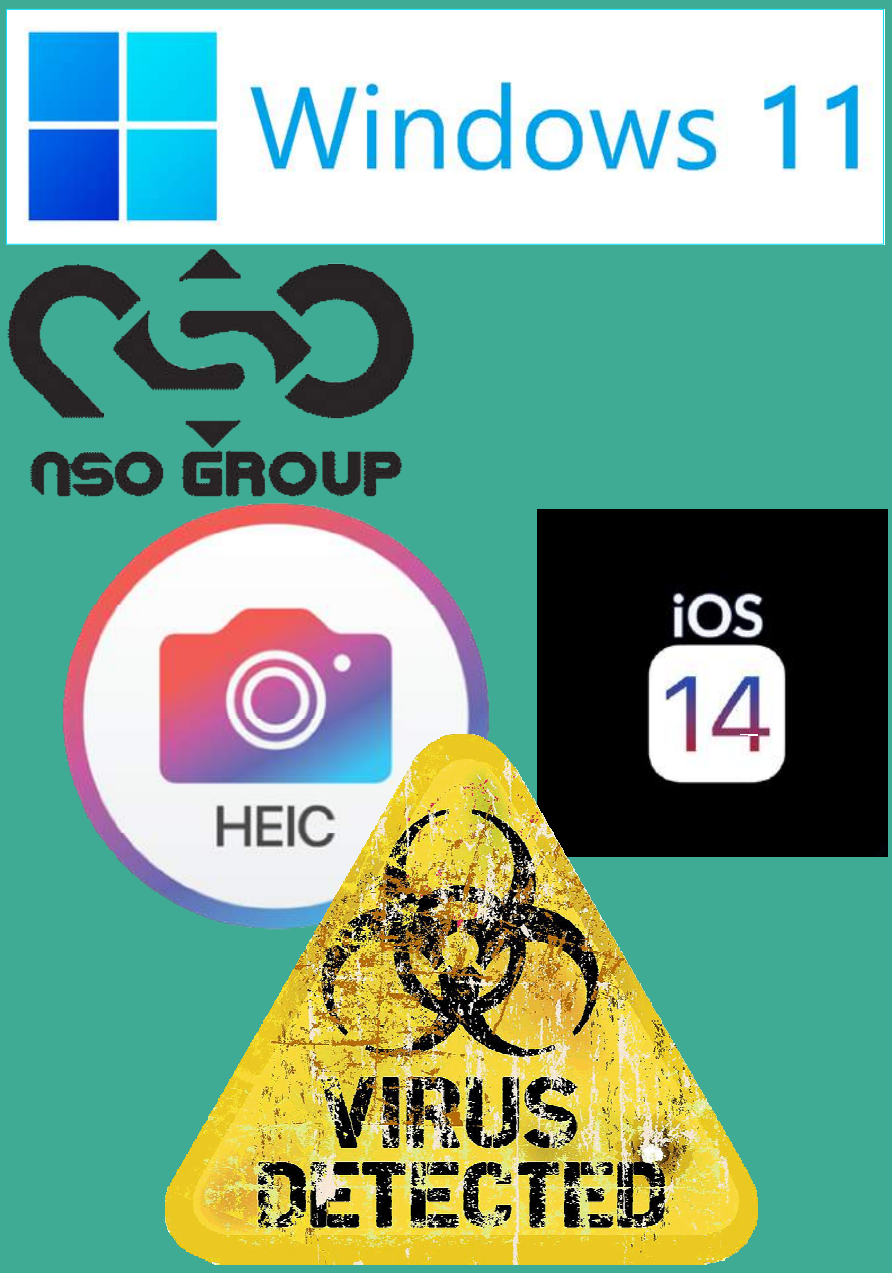
Midden West-Vlaamse Hobby
COMPUTER CLUB ROESELARE



Ons Kompjoeterblad

Jaargang 36 - Nummer 4 - september/oktober 2021



Midden West-Vlaamse Hobby
Computer Club Roeselare
Skaldenstraat 27
8800 Roeselare

info@hccr.be
http://www.hccr.be

Midden West-Vlaamse Hobby
COMPUTER CLUB ROESELARE

☸ HCCR NIEUWS

* Onze kalender voor - 2021/2022

4 september 2021	Internet Of Things Het intelligent huis door Wim
2 oktober 2021	De Cloud One drive, Dropbox door Willy
6 november 2021	Vragen? Wij geven antwoorden door Dimitri
4 december 2021	3D Printing Workshop bij 'RSL op Post' door Niels
15 januari 2022	Smartphone en zijn verbindingen door Willy *+ Nieuwjaars receptie*
16 april 2022	Backup en herstel Macrium Relect door Peter
18 september 2021	Notion door Christophe
16 oktober 2021	Raspberry Pi Demo's door Bram
20 november 2021	Synology als VPN server door Claude
18 december 2021	Marketing door Bram
Dinsdag 5 april 2022	**Bedrijfsbezoek !!** Noteer deze datum nu reeds met 'n stip in je kalender

VERVANGING CLUBNAMIDDAG ...

Onze bedrijfsbezoek INAGRO, aanvankelijk voorzien in 2020, hebben wij door de gekende Corona-maatregelen moeten uitstellen, en dan opnieuw, nogmaals moeten verplaatsen.

Dit gaat nu door op dinsdag 5 april 2022. Dan zijn wij te gast bij Inagro, het praktijkcentrum voor onderzoek en voorlichting in land- en tuinbouw.
Ieperseweg 87 - te 8800 Rumbeke-Beitem

Inschrijvingen kan - *UITSLUITEND* - via ons webformulier:
(*komt zo spoedig mogelijk online*)

inagro
ONDERZOEK & ADVIES IN LAND- & TUINBOUW

❁ NIEUWTJES

* .HEIC - Wat is het, en wat moet je ermee?

Vanaf iOS 11 gebruikt je iPhone en iPad een nieuw bestandsformaat voor foto's en video's: HEIC, ook wel bekend als HEIF en HEVC. Windows is daar eigenlijk nog niet klaar voor, dus hoe houd je alles compatibel? Wat is een .HEIC-bestand en hoe kun je HEIC naar JPG converteren?

iOS 11 gebruikt standaard een nieuw bestandsformaat voor foto's en video's op apparaten die ermee overweg kunnen. Onder de naam HEIC (*of HEIF*) en HEVC hebben nieuwe compressietechnieken het levenslicht gezien in het mobiele besturingssysteem van Apple. Foto's en video's nemen daarmee maar liefst tot zo'n 50% minder ruimte in dan .jpg en het oudere .H264. Nu is er echter wel een probleempje: hoewel HEVC (*ook wel bekend als .H265*) inmiddels redelijk standaard ondersteund wordt door zichzelf respecterende videospelers is dat met HEIC veel minder het geval. Een van de redenen is dat HEIF/HEIC stevig dichtgetimmerd is door patenten van Apple. Je zal ondersteuning dus niet snel aantreffen in populaire viewers als IrfanView, helaas.

Gelukkig is iOS 11 heel slim opgezet en hoef je niet bang te zijn dat je ineens foto's deelt die door niemand zijn te openen. Mail je bijvoorbeeld iets, of upload je een foto naar sociale media dan wordt deze automatisch geconverteerd naar het universele .jpg-formaat. Maar conversie en bijbehorende hercompressie levert natuurlijk ook weer wat kwaliteitsverlies op. Wil je gewoon standaard in de meest gangbare formaten blijven fotograferen en filmen, dan kan dat. Desondanks blijft het nieuwe bestandsformaat onpraktisch en door zijn gesloten karakter voelt het meer als pesterij, dan een vooruitgang.

- ***Standaardformaten kiezen***

Open de app Instellingen en tik op Camera. Tik dan op Structuren en kies voor de optie Meest compatibel. Standaard is in iOS 11 de optie High Efficiency geselecteerd. Let op: als je de optie Structuren niet onder Camera vindt, ondersteunt jouw apparaat HEIF/HEIC niet en is er sowieso niets aan de hand. Helaas is het bij apparaten die de keuzemogelijkheid wél hebben niet mogelijk om bijvoorbeeld het meer ingeburgerde HEVC (*.H265*) wél aan te laten staan en het minder compatibele HEIC uit te zetten. Het is dus een typisch geval van alles of niks.

- ***Automatisch converteren***

We schreven net al dat iOS 11 slim is en foto's van het nieuwe naar het oude formaat converteert bij acties als mailen en uploaden naar social media. Je kunt er ook voor kiezen om wel in HEIF/HEIC te fotograferen en filmen, waarbij iOS foto's ook tijdens het overhevelen naar een Windows-pc naar .jpg converteert. Let wel: daardoor blijf je dus opgezadeld met een hercompressie wat nooit ideaal is als het gaat om kwaliteit. Maar mocht je dit willen, kijk dan in de app Instellingen onder Foto's of de optie Automatisch is ingeschakeld. In dat geval krijg je in Windows altijd .jpg's. Mocht je uiteindelijk een fotobewerker of viewer te pakken krijgen die HEIF/HEIC ondersteunt, dan kan je de optie Behoud originelen selecteren, waarna de oorspronkelijke foto's zonder conversie worden overgeheveld. Kortom: géén paniek betreffende de nieuwe bestandsformaten, maar zorg dat je weet hoe een en ander in de praktijk werkt.

- ***HEIC en jpg***

Het HEIC-formaat of het High Efficiency File Format heeft een veel betere compressie dan de veel populairdere jpg-indeling. Het komt erop neer dat dezelfde afbeelding in heic-formaat de helft minder opslagruimte inneemt dan in het jpg-formaat. Je kunt zo dus veel meer plaatjes kwijt op hetzelfde toestel. Apple belooft zelfs om de kwaliteit en de compressie van heic in de toekomst nog verder te verbeteren. De keerzijde van de medaille is dat andere besturingssystemen dan die van Apple nog geen ondersteuning hebben voor deze nieuwkomer. Totdat het .heic-formaat is ingeburgerd, zijn er gelukkig oplossingen zoals CopyTrans HEIC. Je vindt de software hier, via onze verkorte URL:
https://tinyurl.com/sx5zdats

Tijdens de installatieprocedure moet je bevestigen dat je de software voor persoonlijk gebruik installeert, in een commerciële omgeving zul je langs de kassa moeten.

Nadat je de software hebt geïnstalleerd, is het de bedoeling dat je de HEIC-indeling koppelt aan Windows Photo Viewer. Klik dus met de rechtermuisknop op de HEIC-afbeelding en selecteer Openen met en daarna Windows Photo Viewer. Je kunt met de rechtermuisknop ook de opdracht Kies een andere app selecteren, dan kun je Windows Photo Viewer selecteren en aan-

☸ NIEUWTJES

vinken dat je systeem altijd deze app zal gebruiken om HEIC-bestanden te openen.

Wil je liever het HEIC-bestand omzetten naar het jpg-formaat, dan kun je ook dat nu doen vanuit Windows Verkenner. Klik met de rechtermuisknop op het bestand en gebruik de opdracht Convert to JPEG with CopyTrans. Op die manier kun je in één keer maximaal 100 afbeeldingen in batch converteren. De fotobestanden worden niet op een online server verwerkt, alle conversie gebeurt lokaal. De software zal iedere afbeelding in de achtergrond omzetten naar jpg en daarna in dezelfde map plaatsen. Daarbij zal CopyTrans HEIC tijdens de conversie de oorspronkelijk exif-gegevens van de HEIC-afbeelding overnemen. Dat betekent dat de informatie over datum, locatie, camera-instellingen enzovoort bewaard blijven.

Bovendien voegt deze software ondersteuning toe aan externe freeware viewers zoals bvb IrfanView (*www.irfanview.com*). En voortaan kun je zelfs HEIC-bestanden rechtstreeks in Microsoft Word-documenten toevoegen.

Je hebt ook converters, zoals www.heictojpg.com (*webbased, zeer handig voor enkele foto's*) en iMazing HEIC Converter (*geschikt voor meerdere foto's tegelijkertijd*) die dit voor je kunnen doen.

Bron: Ronald Smit, Computertotaal

Naam	Gewijzigd op	Type	Grootte
B37FAF80-0539-40ED-AA85-488A3C07E78B.heic	18/07/2021 1:03	HEIC-bestand	1 393 kB
B37FAF80-0539-40ED-AA85-488A3C07E78B.jpg	18/07/2021 1:03	IrfanView JPG File	1 180 kB

Nadat uw redacteur een .heic had ontvangen, werd deze door de online converter (www.heictojpg.com) gehaald. Het bewuste bestand was vlot te openen op Android, doch Windows 10 wilde niet meewerken, vandaar die tussenstap.

* Windows 11, een ECO-ramp?

Het besluit van Microsoft om Windows 10 voor een nieuwe Windows 11 te dumpen is een ware ECO-ramp in onze 'milieuvriendelijke' wereld.

Telkens wanneer Microsoft de ondersteuning voor een besturingssysteem beëindigt, moeten miljoenen functionele computers worden afgeschreven omdat ze te oud zijn of omdat hun hardware onvoldoende is om het nieuwe besturingssysteem te laten draaien.
Dit draagt bij aan de bergen elektronisch afval die over de hele wereld worden gegenereerd.
Om de problemen aan te vullen, er is momenteel een wereldwijd tekort aan microchips - een situatie die niet zal verbeteren als we miljoenen computers in de prullenbak van Microsoft gooien.
Wat is er mis met Windows 10?
Waarom moet het worden vervangen?
En hoe past dit in de visie wat Bill Gates ons allemaal predikt over klimaatverandering?

Preview Windows 11

Bron: Andrew Nicol - ComputerActive

☸ NIEUWTJES

* Virussen, malware, spyware en ransomware? WTF!!

In de volksmond is iedere vorm van schadelijke software een computervirus. Toch zijn de digitale tegenhangers van de biologische ziekmakers niet de enige oorzaak van slechtwerkende computers.

Een computervirus is slechts een vorm van malware, bovendien zijn de meeste malwaresoftware overigens ook geen virussen. De term 'malware' is afkomstig van 'malicious software' of 'kwaadaardige software'. Computervirussen zijn ongetwijfeld kwaadaardig ingesteld en vallen dus ook onder malware, net zoals spyware en ransomware. Toch zijn dat zeker niet de enige vormen van malware in het digitale landschap.

- ***Wat is een virus?***

Een computervirus is een vorm van malware die zichzelf verbergt in de code van andere software. De naam is gegeven naar analogie met zijn biologische tegenhanger: het virus dat ziektes veroorzaakt en zichzelf verspreidt door zich te reproduceren in het lichaam van een gastheer. Een computervirus volgt diezelfde werkwijze en verspreidt zich op een geïnfecteerde computer. De lichaamscel die een biologisch virus gebruikt om zich te vermenigvuldigen, is in het geval van het computervirus een geïnfecteerd bestand op je computer. Meer heeft een virus niet nodig om ellende te veroorzaken en zichzelf te verspreiden.

Virussen zijn de enige vorm van malware die zichzelf kunnen reproduceren en verbergen in andere bestanden zonder de toestemming van de gebruiker. Naast het verspreiden, maakt het computervirus ook de gastsoftware onbruikbaar en vertoont het kwaadaardig gedrag dat de computer aantast.

De beste antivirussoftware heeft moeite met het correct afzonderen van virussen en in veel, zo niet de meeste, gevallen plaatst de software de geïnfecteerde bestanden in quarantaine of verwijdert het de dreiging tezamen met het gehele bestand. Tegenwoordig komen computervirussen minder vaak voor en is de dreiging van andere digitale parasieten sterk toegenomen. Een goede zaak, zeker als je weet dat virussen de enige vorm van malware zijn die bestanden 'infecteert' en bovendien moeilijk zijn te elimineren.

- ***Naamsverwarring***

De verwarring tussen de termen malware en computervirussen is mede het gevolg van de softwareontwikkelaars die de begrippen virus en malware door elkaar gebruiken en de illusie creëren dat antivirusoplossingen effectiever werken dan de varianten die beschermen tegen malware, terwijl die laatste in de praktijk net betere bescherming biedt. Het probleem wordt nog gecompliceerder nu de meeste antivirussoftware computer ook tegen andere vormen van malware behoeden. Voor het installeren van antivirus- of antimalwaresoftware, moet je controleren of het programma je ook daadwerkelijk beschermt tegen alle mogelijke dreigingen.

Met een enkele blik op de beschrijving van de software kan je nakijken voor welke types van digitale parasieten de beveiligingssoftware je computer beschermt, ongeacht of het antivirus- of antimalwaresoftware is. Wat telt is de inhoud, niet de naam.

- ***Welke soorten malware zijn er?***

Bijna alle computergebruikers zijn bekend met de term computervirus, maar dat is zeker niet de enige vorm van malware of schadelijke software die het digitale landschap doorkruist. Het beschermen van je computer begint bij het begrijpen en onderscheiden van de verschillende soorten bedreigingen en hoe deze kwaadaardige software onzichtbaar opereert. Iedere vorm van malware is vertoont andere eigenschappen of kenmerken. Hieronder volgt een korte introductie tot de meest voorkomende soorten malware.

Spyware is kwaadaardige software die zonder je medeweten meekijkt over je schouder en gebruikersgegevens verzamelt op je computer om deze later door te sturen naar een onbekende derde partij.

Ransomware is gijzelsoftware die de persoonlijke documenten van een gebruiker codeert en blokkeert in sommige gevallen zelfs de gehele computer om 'ransom' of 'losgeld' te vragen. Na het betalen via een anonieme service, zou je de sleutel verkrijgen om de computer of bestanden te decoderen.

Rogue security software of valse beveiligingssoftware wekt de illusie dat het betrouwbare beveiligingssoftwa-

Afbeelding: pxfuel.com

☸ NIEUWTJES

re is, maar in realiteit misleidt de software gebruikers tot het aankopen van de volledige versie van de gratis software.

Computerworm is schadelijke software die zichzelf snel verspreidt via opslagapparaten zoals usb-sticks, e-mails of kwetsbaarheden in besturingssystemen. Hun verspreiding gebeurt zonder andere software en leidt tot een vermindering van de prestaties van computers of netwerken.

Keylogger is malware die in het geheim alles registreert wat je typt op je toetsenbord en die informatie doorstuurt naar hackers. De data bevat mogelijk wachtwoorden en andere belangrijke gegevens over bijvoorbeeld internetbankieren en die gegevens komen in handen van kwaadwilligen.

Adware is afgeleid van het woord 'advertentie' en toont gebruiker ontelbare hoeveelheden aan advertenties. Op zich is adware niet echt gevaarlijk, maar het weergeven van advertenties wordt over het algemeen als ongewenst beschouwd en dus gedetecteerd door antimalwaresoftware.

Trojaans paard is een kwaadaardig programma dat zich voordoet als een goedaardig programma en virussen en wormen op een computersysteem binnensmokkelt. Het doel is om de gebruiker de software te laten uitvoeren, zodat de meegereisde malware de controle over je computer verkrijgt.

Browser redirect een irritante vorm van malware welke meestal minder schadelijk is en de standaard zoekmachine of homepage in de browser verandert.

Bootsectorvirus is een hardnekkige soort van computervirus dat zich nestelt in de BIOS van je computer waardoor het de volledige controle krijgt over de opstartprocedure en ontzettend moeilijk te verwijderen is.

- ***Hoe verspreidt malware zich?***

Malware is een veelzijdige verzameling van verschillende soorten van kwaadaardige software die zich op allerlei mogelijke manieren weet te verspreiden. Als gebruiker heb je het grootste belang om voorzichtig te handelen op internet en de risico's die je neemt te beperken. Meld je niet zomaar aan op een onbekend wifinetwerk, want besmette computers infecteren toestellen die zich op hetzelfde netwerk bevinden.

Open nooit e-mailbijlagen van afzenders die je niet persoonlijk kent en kijk ook uit voor e-mails van bekende bedrijven, want vaak imiteren cybercriminelen deze e-mails voor het verspreiden van schadelijke software. Hackers en cybercriminelen vertrouwen op de nieuwsgierigheid van de e-mailontvangers om de infecties verder rond te zaaien. Als je toch een bijlage opent om na te gaan waar het allemaal over gaat, ben je al geïnfecteerd met digitale parasieten.

Bovendien kan in de digitale wereld malware ook nog steeds fysiek verder verspreiden door het gebruik van besmette opslagmedia zoals usb-sticks of externe harde schijven die geïnfecteerde bestanden herbergen. Als je een besmet opslagmedium connecteert, kan je schadelijke bestanden overdragen van de ene naar de andere computer. Wees voorzichtig met onbekende usb-sticks of harde schijven van andere gebruikers.

- ***Ben ik geïnfecteerd?***

Als je computer plotseling niet meer goed reageert, langzamer is dan vroeger, software vanzelf opstart en het gezoem van de harde schijf constant op de achtergrond te horen is, dan is je toestel vermoedelijk geïnfecteerd met malware. Het is niet altijd duidelijk of je computer effectief geïnfecteerd is, maar bij twijfel onderneem je best zo snel mogelijk stappen om de bedreiging op te sporen.

De strijd tussen malware en beveiligingssoftware is een kat-en-muisspel. Met iedere stap die antivirus- of antimalwaresoftware onderneemt om de beveiliging van je computer te verbeteren, komen hackers en cybercriminelen met nog geavanceerdere vormen van malware aankloppen. De aanwezigheid van de kwaadaardige software is onzichtbaar voor de gebruiker en wordt pas opgemerkt als het te laat is.

Is je computer geïnfecteerd en weet je niet wat te doen, neem dan contact op met een IT-expert.

- ***Verwijderen van infecties***

Het verwijderen van een malware-infectie vereist alleen een betrouwbare malwarescanner. Voor het opsporen en neutraliseren van malware is het verstandig om twee malwarescanners te gebruiken: een real-time-scanner en een on-demandscanner. De real-time-

☸ NIEUWTJES

scanner, zoals Norton Security 2018, scant je systeem op virussen en werkt in de achtergrond terwijl je de computer gebruikt en de on-demandmalwarescanner van het besturingssysteem, zoals Microsoft Safety Scanner, moet elke keer dat u wilt scannen handmatig worden uitgevoerd. Een van beide moet in staat zijn om de besmetting te identificeren en verwijderen, maar met beide scanners vergroot je de kans op succes.

Het handmatig verwijderen van geïnfecteerde bestanden is complex en enkel aanbevolen voor ervaren gebruikers. Als je niet zeker weet wat te doen, neem dan contact op met een IT-expert die gespecialiseerd is in het verwijderen van malware.

Na het verwijderen van de besmette bestanden, treden mogelijk problemen op met de werking van de eerder geïnfecteerde software. De software opnieuw installeren of de verwijderde bestanden uit een back-up terugplaatsen, lost het probleem in de meeste gevallen op.

Bijna alle computergebruikers zijn bekend met de term computervirus, maar dat is zeker niet de enige vorm van malware of schadelijke software die het digitale landschap doorkruist. Het beschermen van je computer begint bij het begrijpen en onderscheiden van de verschillende soorten bedreigingen en hoe deze kwaadaardige software onzichtbaar opereert.

- ***Hoe bescherm ik mijzelf?***

Het vroegtijdig stoppen van malware vooraleer het je computer infecteert is eenvoudiger dan het verwijderen van een virus of andere kwaadaardige software op je computer. Het bijwerken van je antivirus- of antimalwaresoftware helpt om je te beschermen tegen virussen en malware.

Maak regelmatig back-ups van bestanden en sla ze op een externe harde schijf op. Dat kan helpen om het verlies van belangrijke informatie te voorkomen als met malware te maken krijgt. Als u nog geen back-ups hebt gemaakt, is het nu een goed moment om te beginnen.

- ***Kort samengevat***

Het is van cruciaal belang om de nieuwste antivirus te installeren als een virus of malware wil tegenhouden en verwijden, je computer veilig wenst te houden en persoonlijke gegevens wil beschermen. Als je niet zeker weet wanneer je de antivirus- of antimalwaresoftware op je computer voor het laatst hebt bijgewerkt, is het misschien wel verstandig om de software even te controleer en indien nodig ook te updaten.

Bron: techpulse.be

* Hoe houd ik mijn smartphone veilig?

Een snoodaard kan uw iPhone of Android-smartphone besmetten met de spyware Pegasus door u een berichtje te sturen dat u niet eens hoeft te openen. Is niemand dan veilig? Wel nee, toch niet voor 100 procent. Maar met wat voorzorgen bent u toch behoorlijk beschermd tegen de meest frequente bedreigingen.

- ***Hoe zit dat precies met - Pegasus?***

Pegasus is spyware van wereldklasse. Hij raakt binnen op uw smartphone door een zero click-lek die uw smartphone besmet zonder dat u zelf iets hoeft te doen. Volgens de maker ervan, NSO Group, gebruiken overheden de software alleen tegen zware criminelen. Onderzoek van Amnesty International en een groep onderzoeksjournalisten toonde aan dat dit niet juist is. Maar wat wel klopt: organisaties die aan dit soort peperdure, zeldzame software kunnen komen, zijn waarschijnlijk niet in u geïnteresseerd. Bent u een mensenrechtenactivist met contacten in ondemocratische landen, dan kan dat anders liggen. Wilt u het zeker weten? Amnesty International ontwikkelde een stuk software dat de back-ups van uw smartphone doorzoekt naar signalen dat Pegasus actief is geweest:
https://github.com/mvt-project/mvt

Opgelet, dat stukje software is nu niet bepaald erg gebruiksvriendelijk.

Aan welke risico's staan doorsnee gebruikers wel bloot? Het lek dat Pegasus exploiteert, is niet alleen uitzonderlijk krachtig (*zero click*), maar het is bovendien een zero day. De fabrikant van uw smartphone en de ontwikkelaars van antivirussoftware kenden het nog niet, het kon dus nog niet worden gedicht. Maar doorsnee criminelen exploiteren lekken die al bekend zijn en waartegen u zich wel kan verdedigen. In veel gevallen bent u pas besmet als u uitdrukkelijk toestemming geeft om een kwaadaardige app op uw smartphone te installeren.

- ***Updates installeren en - opletten met links***

Zodra er een beveiligingsupdate is voor uw smartphone, installeer die zo snel mogelijk. Probleem: niet alle Android-fabrikanten zijn zelf even snel in het verdelen van beveiligingsupdates voor hun smartphones. Verder is het altijd uitkijken als u berichten ontvangt waarin een link staat. Grondig lezen voor u ergens op klikt, is de boodschap. Wie is de afzender precies? Kloppen alle

☸ NIEUWTJES

gegevens of schort er iets? Heeft u toch op een link in een mail of sms geklikt, dan is er waarschijnlijk geen man overboord. Meestal wordt gevraagd om een app te installeren. Meer dan negenduizend mensen installeerden eerder dit jaar een app die zogezegd van Bpost was. Helaas: het was de gevaarlijke Teabot-malware. Om die app te installeren, hebben die slachtoffers eerst zelf, manueel, de beveiliging uitgeschakeld die verhindert dat er apps van buiten de Play Store worden geïnstalleerd.

- ***Gebruik een antivirus-app***

Op Android bestaan antimalware-apps die kwaadaardige apps – zelfs Pegasus! – herkennen en blokkeren. Helaas hebben de meeste gebruikers die app niet geïnstalleerd. Op iOS is de situatie anders: de beveiliging van de iPhone laat niet toe dat een app grondig scant naar malware – of dat beter of slechter is, daarover verschillen experts van mening. De gratis antivirus-app Avast op Android, die een goede reputatie heeft, beweert Pegasus al sinds 2016 te detecteren en te blokkeren, al is niet helemaal duidelijk of dat ook geldt voor de meest recente versie van die spyware. Teabot detecteert het zeker.

- ***Fabrieksinstellingen herstellen***

Een smartphone kan je herstellen naar fabrieksinstellingen en daarmee worden de meeste vormen van malware verwijderd. Opgelet: als u daarna alle gegevens en apps terugzet vanuit een recente back-up, kan u zichzelf opnieuw besmetten. Het is dus best om alles volledig vanaf nul te herinstalleren. Nog drastischer is het opnieuw 'flashen' van de smartphone, dat laat u best aan een specialist over.

- ***Nog een paar veiligheidstips***

Op Android installeert u best geen apps van buiten de App Store, op iPhone is dat zelfs onmogelijk. Ook in de App Store zitten schadelijke apps. Soms hebben die bijna dezelfde naam als de app die u eigenlijk zoekt. Het verschil ziet u vaak pas als u naar de details kijkt: hoe vaak is de app al geïnstalleerd (*een laag aantal kan wijzen op zo'n namaak-app*)? En check de recensies in de Play Store. Let ook op welke toestemmingen de app vraagt tijdens de installatie. Zijn dat er verdacht veel, installeer dan niet. In het algemeen: installeer zo weinig mogelijk apps, en verwijder apps die u niet gebruikt. En een algemene beveiligingstip: gebruik zo veel mogelijk multifactor authenticatie om in te loggen.

Bron:De Standaard

* The Complete iOS 14 Manual - downloaden

Voor de liefhebbers, …

Een Engelstalige, complete handleiding iOS 14 (*voor iPad en IPhone*) kan gratis worden gedownload vanaf volgende website:
https://magazinebis.com/the-complete-ios-14-manual-31-july-2021.html
- Scroll een weinig naar beneden.
- Klik op "DOWNLOAD FILE".
- Klik op "Generate Download Link".
- Neem de captcha over en klik op "Submit".
- Klik op "Download Now".

Een .pdf van 208 MB komt binnen. (*Engelstalig, 325 pagina's*)
Suc6