

SECURE COMPUTING

DIGITAAL COMPUTER MAGAZINE

November 2012

W.Bosgra Taakaccenthouder digitale criminaliteit

INHOUD

In deze editie oa:

Certificaat Veilig internetten

Nogmaals: Cameratoezicht

Facebook: laatste nieuws

Studeren met YouTube

Repareer IE

Keygens

THEMA: besmette PC

Panopticon



@securecomputing

Bronnen: De Waarschuwingsdienst, Nederland veilig, Meldpunt Cybercrime, Digibewust & Digivaardig, Webwereld, Security.nl, Zdnet, Veilig bankieren, You Tube, Internetsporen, Voelspriet, HardwareInfo,



Politievirus waarschuwt slachtoffers via MP3

Cybercriminelen gebruiken een nieuwe manier om slachtoffers van ransomware tot betalen te dwingen, namelijk een audiobestand dat wordt afgespeeld. Ransomware vergrendelt de computer en toont een melding, bijvoorbeeld van de politie, dat het slachtoffer iets strafbaars heeft gedaan en hij daarom geen toegang meer tot de computer heeft. Om weer toegang te krijgen moet een bedrag van meestal zo'n 100 euro worden betaald.

Audiobestand
Naast het gebruik van politielogo's en zelfs het inschakelen van de webcam, laat een nieuwe variant een MP3-bestand horen. Dit bestand laat het slachtoffer herhaaldelijk weten dat de computer wegens bepaalde overtredingen is geblokkeerd.

Om de melding te stoppen en weer toegang te krijgen wordt dit keer geen 100 euro, maar zo'n 155 euro losgeld gevraagd,



Trusteer

De ING biedt alle internetbankierende klanten de veiligheidssoftware Rapport van het Israëlische beveiligingsbedrijf Trusteer aan. Deze tool beschermt klanten tegen banking Trojans en andere malware. De software moet voorkomen dat persoonlijke gegevens zoals gebruikersnaam en wachtwoord in verkeerde handen vallen. Het programma werd eerder al aangeboden aan ING-klanten met een besmette computer.

Nu wordt het ook preventief ingezet als aanvulling op bestaande middelen als een virusscanner en firewall. De ING adviseert klanten het programma te downloaden en installeren.

Rapport wordt door verschillende Amerikaanse, Britse en andere buitenlandse gebruikt, waaronder ING Direct in de VS. Klanten van ING Direct beschikken al sinds 2008 over de beveiligingstool.

Werking
Rapport kaapt verschillende Windows API's op het systeem om misbruik te voorkomen. Ook blokkeert het API calls die op kwaadaardige activiteiten kunnen duiden. Veel malware is in staat om bijvoorbeeld de "WinIntet" API te kapen, die een SSL-verbinding tussen de browser en de website opzet.

Door deze API te kapen, kan de malware gebruikersnamen en wachtwoorden stelen, ook al voert een gebruiker die in op een site die de data versleutelt, omdat de informatie op een lager niveau wordt gepakt, nog voordat het is versleuteld.

Het programma zou dit voorkomen, waardoor de consument toch nog op een veilige manier kan internetbankieren, ook al is zijn systeem geïnfecteerd. De 400KB grote applicatie versleutelt tevens alle toetsaanslagen voordat het de website bereikt. De laatste beveiligingslaag bestaat uit het controleren van het IP-adres en SSL certificaat van de website, zodat consumenten hun login niet op een phishingsite invoeren.

Het beveiligingsprogramma is zowel beschikbaar voor Microsoft Windows als voor Apple OSX. Het werkt op de meest gebruikte browsers Microsoft Internet Explorer, Mozilla Firefox, Google Chrome en Apple Safa-

Veilig Internet

De **Veilig Internet certificering** leert je op een **leuke** manier de **basisvaardigheden** die je nodig hebt om **veilig** te kunnen internetten, namelijk het **up-to-date** houden van je besturingssysteem en je browser. Het Veilig Internet certificaat **garandeert** dat je in staat bent om je computer up-to-date te houden en dat je een aantal veel voorkomende situaties op internet kunt **herkennen** en op een praktische manier kunt **oplossen**.

Behaal het Certificaat

Het certificaat is **gratis** en je haalt het helemaal **online**. Wanneer je voor de verplichte challenges (hier links in het blauw) een **score van 100%** hebt gehaald kun je het **certificaat** direct **downloaden** . Ook is het mogelijk de challenges te doen zonder je te registeren bij Certified Secure, gewoon voor de lol. Je moet dan wel zelf je score bijhouden en het is uiteraard ook niet mogelijk om het certificaat te behalen.

Het eerste gedeelte van de Veilig Internet certificering is de "Internet Fundamentals" quiz. Als je weet waarom software updates belangrijk zijn, en waarom je niet zomaar overal op moet klikken zal het geen probleem zijn om alle vragen goed te beantwoorden en deze challenge succesvol af te ronden.

Het tweede gedeelte van de Veilig Internet certificering is de "Niet Klikken" quiz. Je ontvangt een e-mail met een update voor internetbankieren, wat doe je? Wanneer klik je en wanneer klik je niet?

Extra Content

De extra content is niet direct benodigd om het certificaat te behalen, maar daarom niet minder leuk. Je vindt hier extra challenges, video's, downloads en tools. Als je op zoek bent naar extra uitleg of wanneer je het gewoon leuk vindt om meer challenges te doen, dan moet je hier zijn! Extra content is altijd herkenbaar aan de groene buttons en popups.

Certificaat gehaald?

Ga dan eens te werk als een echte internet detective.

Eerst kun je oefenen via

www.webdetective.nl

Ga daarna voor het zwaardere werk naar

http://www.vtstutorials.ac.uk/detective/getonthecase.html



Doe hier de oefening!





Cameratoezicht blijft de gemoederen juridisch bezighouden. Mag het nu wel, of mag het nu niet?



Het inzetten van camera's kan een prima middel zijn ter beveiliging van zaken en personen, of om het presteren van personeel in de gaten te houden. Maar omdat je met camera's structureel mensen individueel kunt bespioneren, zijn er wettelijke regels aan.

Wanneer cameratoezicht in de openbare ruimte wordt gehanteerd, is de hoofdregel dat je hiervoor tijdig moet hebben gewaarschuwd. Een bordje met een pictogram van een camera is prima, maar ook de camera pontificaal zo ophangen dat deze niet te missen is, is legaal. Natuurlijk wel zo dat je het bordje of de camera kunt zien vóórdat je in beeld bent.



De openbare ruimte is de openbare weg en alles dat vanaf daar bereikbaar is zonder bijzondere hindernissen of de noodzaak van aparte toestemming. Een café is dus óók openbare ruimte, want iedereen mag daar naar binnen. Of het moeten betalen van entree telt als "bijzondere hindernis", daar zijn de geleerden het nog niet over eens. Ik denk van niet, mits maar iedereen na betaling naar binnen mag. Een besloten club met deurbeleid is dan geen openbare ruimte, een dierentuin wel.

Deze regels gelden overigens ook voor particulieren, ook zij mogen de openbare ruimte filmen. Denk aan cameratoezicht op de auto voor de deur. Wel moet het filmen een eigen belang dienen: de auto bewaken valt er wel onder, de hele straat controleren niet.



Worden de beelden opgeslagen, dan moet er een protocol komen waarin staat voor welk doel de beelden worden gemaakt, en wie de beelden inziet en gebruikt. Tevens moet er iets opgezet worden waarmee gefilmde personen een kopie van "hun" moment in beeld kunnen opvragen. Opslaan van camerabeelden (digitaal dan) leidt er namelijk toe dat de Wet bescherming persoonsgegevens geldt, en dan hebben mensen een inzage- en correctierecht.

In besloten ruimtes zijn de regels strenger. Je moet dan een belangenafweging maken van de privacy van de personen die in beeld komen versus jouw belang om te filmen. Kort gezegd mag er geen andere keuze zijn dan cameratoezicht om het doel te halen, én je moet zo veel mogelijk rekening houden met de privacy. Een zwembad mag bijvoorbeeld eigenlijk nooit camera's in de kleedhokjes ophangen: het belang van voorkomen van vechtpartijen of aanranding weegt niet op tegen de privacyschending van de zich omkledende badgasten.



Voor cameratoezicht op het werk geldt een eveneens strenge afweging, omdat ook werknemers recht op privacy hebben. Je moet onder meer de Ondernemingsraad om instemming vragen, en je moet het apart en expliciet vastleggen als je cameratoezicht hanteert om mensen op hun functioneren te kunnen aanspreken. Als je zegt dat je filmt ter beveiliging, mag je luie werknemers niet achteraf ineens aanspreken op wat er op die beelden staat.

En inbrekers hebben géén privacybelang dat geschonden kan worden door cameratoezicht. Privacy geldt alleen voor genode gasten.

FACEBOOK

Uit nieuwe cijfers blijkt dat Azië het continent is met de meeste Facebookgebruikers. Europa volgt op de tweede plaats. Nederland staat wereldwijd 28e.

Facebook waarschuwt voor JavaScript-worm

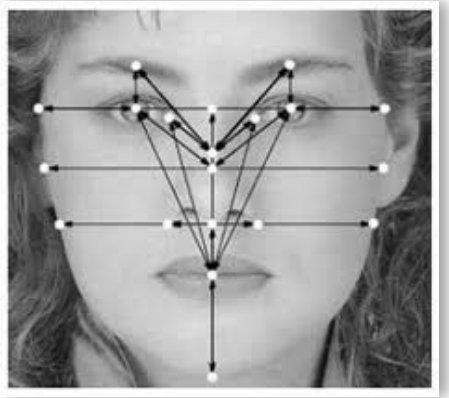
Onderzoekers hebben een nieuwe JavaScript-worm ontdekt die gebruikers van Internet Explorer, Facebook en torrentsites aanvalt. De Proslikefan-worm valt als eerste op door de omvang. Terwijl de meeste wormen die in JavaScript en VBScript zijn gemaakt een paar kilobytes groot zijn, 'weegt' Proslikefan 130 kilobytes. De worm heeft het voorzien op Windows-computers. De malware kan binnen de browser worden uitgevoerd, zolang die ActiveX ondersteunt, wat in de meeste gevallen Internet Explorer betekent, hoewel er ook andere browsers zijn die door middel van plug-ins ActiveX kunnen ondersteunen.

Een andere opvallende eigenschap is dat de malware naar bepaalde sleutelwoorden op Google kan zoeken, waarbij het de URLs van alle zoekresultaten verzamelt. De verzamelde URLs worden vervolgens geanalyseerd op mogelijke SQL Injectie-fouten. Is er een lek in de website gevonden, dan wordt de relevante informatie naar de Command & Control-server gestuurd.

Verder zoekt Proslikefan naar WordPress blogs die de TimThumb plug-in gebruiken. Een lek in de plug-in wordt vervolgens gebruikt om bestanden op de webserver uit te voeren.

Facebook
Op de besmette computer zoekt de worm in de cookies directory naar een geldige Facebook sessie. Is er een geldig cookie aanwezig, dan kan de malware bepaalde pagina's 'liken' of hier fan van worden. Ook kan het chatberichten naar andere Facebook-gebruikers sturen. Facebook detecteert de malware inmiddels en waarschuwt gebruikers die besmet zijn geraakt.

Proslikefan gebruikt daarnaast ook de Autorun-functie van Windows om zich te verspreiden en plaatst zich in de directory van verschillende bestandsuitwisselingsprogramma's. Vervolgens maakt het verbinding met The Pirate Bay om daar een exemplaar van zichzelf te uploaden die vanaf de besmette computer wordt aangeboden.



Valse Facebook plug-in bedreigt 90.000 Chrome-gebruikers

Plug-ins voor Google Chrome die beweren de Facebook Tijdlijn te kunnen verwijderen zijn zeer populair, maar niet allemaal ongevaarlijk. Dat ontdekte beveiligingsbedrijf Barracuda Networks. Op de Google Chrome Store worden verschillende plug-ins aangeboden om de Tijdlijn, die Facebook eerder dit jaar introduceerde, weg te halen. De verschillende plug-ins hebben bij elkaar ruim 760.000 gebruikers.

Verschillende plug-ins, met namen als 'Disable Timeline on Facebook' en 'Remove Facebook Timeline' blijken niet helemaal zuiver. Niet alleen wordt geprobeerd om gebruikers aan enquêtes voor een gratis cadeaubon mee te laten doen, ze vragen ook om meer permissies dan noodzakelijk.

Toegang
Het gaat dan onder andere om toegang tot gegevens op alle websites en toegang tot tabs en surfactiviteiten. Deze valse plug-ins zijn meer dan 90.000 keer gedownload. "In andere woorden staan de potentiële slachtoffers deze kwaadaardige third-party plug-ins toe om hun persoonlijke webgegevens te kapen als ze het internet met Chrome surfen".

Facebook stopt met omstreden gezichtsherkenning

Facebook heeft aangekondigd in Europa met zijn omstreden gezichtsherkenning te stoppen. Tot 15 oktober blijft de functie nog actief, daarna wordt ze definitief verwijderd. Bij nieuwe accounts is de functie standaard al uitgeschakeld.

Wanneer iemand op Facebook in een foto getagd wordt, analyseert het netwerk zijn of haar gezicht en weet het vervolgens in nieuwe foto's wie deze person is. Op die manier werd het mogelijk om de gezichten van contactpersonen makkelijker op andere foto's te herkennen. Zo'n geautomatiseerde gezichtsherkenning zonder instemming van de gefotografeerde is echter in strijd met geldend EU-recht en meerdere landen dienden een bezwaar in.

FACEBOOK

Foto's uitsnijden

Heeft Facebook wel het interessantste deel van uw foto uitgesneden? Nee? Klik dan in de rechterbovenhoek op de potloodknop en selecteer Foto verplaatsen. Daarna kiest u Bewaar.

NIEUWS

Justitie wil filtering op kinderporno bij providers

Provider Leaseweb is positief over een pilot die sedert 2009 is uitgevoerd waarbij uploads naar een fotosite gescreend worden op kinderporno. Bij de proef werden plaatjes die werden geüploaded, vergeleken met plaatjes uit de KLPD-database, met zogeheten md5-technologie. Is er een match, dan blokkeert de klant van Leaseweb de user. Het ministerie van VenJ heeft de pilot geëvalueerd en spreekt van 'een geslaagde pilot' met 'diverse leerpunten'. Het grootste probleem is dat de uploadfiltering alleen werkt met bekende plaatjes en dat verspreiding van kinderporno ook (vooral?) op andere manieren plaatsvindt (tor-servers, peer-to-peer bijvoorbeeld). Het effect zou daarmee 'in brede zin beperkt zijn'. Politie, justitie en enkele private partijen gaan nu onderzoeken hoe de pilot een vervolg moet krijgen.

Engeland aan de Kit Kat

Nestlé stopt GPS-chip in Kit-Kat-reep.

Voedingsmiddelenconcern Nestlé heeft als onderdeel van een wedstrijd in Engeland zes KitKat-repen van een GPS-chip voorzien, waarmee de eigenaren zijn te traceren. Bij het openen van de repen wordt de GPS-chip geactiveerd en een signaal naar de wedstrijdorganisatie bij Nestlé gestuurd.

Vervolgens wordt de winnaar binnen 24 uur door een helikopter gelokaliseerd. Aan boord van de helicopter bevindt zich een team dat de winnaar een koffer met



Nederlandse jongeren geven niets om privacy op sociale media

In Nederland verscheen ook een rapport, over de gevolgen van openbaarheid op sociale media. Masterstudent Mark Kraag (Nieuwe Media, Univ van Amsterdam) onderzocht hoe jongeren (16 tot 21 jaar) omgaan met hun accounts op facebook en twitter. Kraag meldt dat slechts 1% van de jongeren (heel) veel waarde hecht aan die privacy. Nog geen kwart van de ondervraagden heeft de facebookpagina gesloten voor onbekenden, slechts 14% twittert afgeschermd. En die afscherming blijkt ze ook nauwelijks te interessen: velen kozen er zelfs bewust voor. Anderen zeiden niet eens te weten dát je het kon afschermen .

Opstelten wil hackrecht voor politie

Volgens minister Opstelten moet de politie nieuwe bevoegdheden krijgen: inbreken op computers, en daar gegevens ophalen en vernietigen. En dat ook nog eens internationaal. Nu schiet de wet daarvoor te kort, schrijft Opstelten in een brief aan de Kamer. En dus kan cybercrime niet opgelost worden: de politie mist de bevoegdheden, zoals de AIVD die bijvoorbeeld wel heeft.
In de voorstellen gaat het om 'ernstige vormen van cybercrime' maar onduidelijk is wat daarmee precies bedoeld wordt. Cyberspionage? Kinderporno? Fraude? Terroristische plannen? Hoe dan ook, Opstelten wil de politie ook de bevoegdheid geven om informatie op afstand 'ontoegankelijk te maken'. In gewoon Nederlands: te wissen. Dat is al eens gedaan bij kinderporno, aldus de brief maar 'een dergelijke afweging zal ook in de toekomst gemaakt moeten worden bij de bestrijding van bijvoorbeeld botnets.'

”IK HEB NIKS TE VERBERGEN HOOR!!"

Ja, dat zeggen wij Nederlanders opvallend vaak.
Maar klopt dat wel?
Filmmaker Peter Vlemmix gaat op zoek naar de staat van privacy in Nederland.
PANOPTICON is een docu van 60 min, die laat zien hoe en waarom jouw privacy onder druk staat.

Panopticon de film

Begin 2011 las filmmaker Peter Vlemmix een bericht over mobiele naakt-scanners in Nederlandse steden.
Voor hem het zoveelste bericht over de aantasting van privacy,
en het moment dat hij daar een film over wilde gaan maken.
Echter, filmen kost geld, en budget was er nauwelijks.
Maar door de geweldige belangeloze inzet van crewleden en een aantal sponsors,
is het stapje voor stapje gelukt om de docu verder te ontwikkelen.

Als u op de vorige pagina het artikel over Hackrecht heeft gelezen, mag u deze film zeker niet missen.

Vorm u mening…….











GMAIL

Eigen thema-afbeelding

Sinds kort kunt u in Gmail een persoonlijke foto als thema invoegen. Nadat u bent ingelogd, klikt u op het tandwielpictogram om naar de Instellingen te gaan. Daarna kiest u het tabblad Thema's en kunt u onderaan bij de Aangepaste thema's kiezen tussen Licht of Donker. Wanneer u een keuze hebt gemaakt, opent zich een venster waarin u de bron van uw eigen foto's kunt selecteren. Eventueel kunt u ook het internetadres van een afbeelding op het web invoeren.



WINDOWS XP/VISTA/7



M.Z.N. (map zonder naam)

Normaal gesproken voorziet u iedere map van een naam, maar het is ook ook mogelijk om een map zónder naam aan te maken. Selecteer de map en wis de naam. Laat uw muisaanwijzer gewoon in het naamvakje staan en schakel de Numlock van het toetsenbord in. Terwijl u nu de Alt-toets ingedrukt houdt, typt u de getallen 0160, waarna u op Enter drukt. Zo, daar is uw map zonder naam.

MINIWORKSHOP: APPCLEANER

Opgeruimd staat netjes!

Hoe langer u uw pc gebruikt, hoe meer ballast zich opstapelt: tijdelijke bestanden (die niet zo tijdelijk blijken te zijn), cookies, geschiedenis, logs en andere bestanden van allerlei applicaties... Met AppCleaner ruimt u dat allemaal snel weer op!

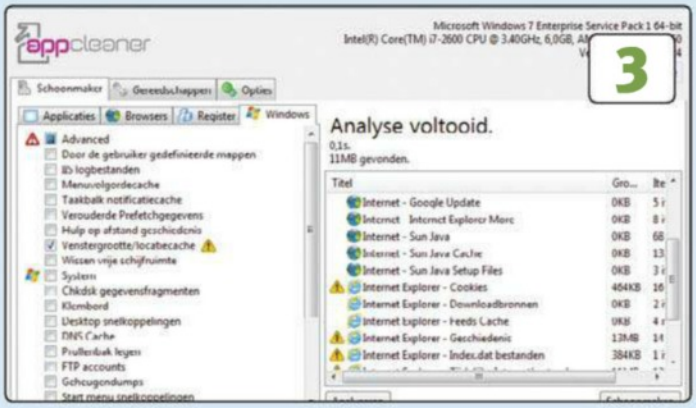
1 U vindt het gratis AppCleaner op client.updatestar.com/en/appcleaner/download (overigens ook in een 'portable' versie). De installatie hebt u in een oogwenk voor elkaar. Start u de tool, dan belandt u standaard op het tabblad Schoonmaker, Applicaties. Het is de bedoeling dat u hier een vinkje plaatst bij de items die u opgeruimd wilt zien.

2 Open ook even de andere tabbladen binnen de schoonmaakdivisie: Browsers, Register en Windows. U zult merken dat er bij sommige items een gevarendriehoekje verschijnt zodra u die selecteert. U krijgt dan nuttige feedback als u de muisaanwijzer even boven zo'n driehoekje houdt. Hebt u alle gewenste items aangevinkt, druk dan op de knop Analyseren.

3 Na afloop van de analyse leest u af hoeveel schijfruimte het opruimen van elk onderdeel u zal opbrengen. Een geel driehoekje hier betekent dat niet alle bestanddelen kunnen worden opgeruimd omdat ze door andere processen in gebruik zijn. Druk op de knop Schoonmaken om de items op te ruimen. Antwoord bevestigend op de (eventuele) vraag of u een backup wilt maken van registeronderdelen die AppCleaner zal verwijderen.

4 Die backup kunt u dan in een reg-bestand bewaren, zodat u de wijzigingen via een dubbelklik op dat bestand alsnog kunt terugdraaien. Vooraf een systeemherstelpunt maken is hoe dan ook aanbevolen. Niet onbelangrijk ook: via het tabblad Opties bepaalt u hoe grondig AppCleaner vrije schijfruimte moet verwijderen en op welke schijven.

In principe volstaat de snelle methode (één keer overschrijven). Merk op dat u op de tabbladen Negeren en Gebruikersbestanden kunt instellen welke bestanden AppCleaner met rust moet laten dan wel ook moet meenemen tijdens zijn schoonmaakoperatie.



CYBER-CARICE

Carice van Houten is de gevaarlijkste cyber celebrity van Nederland. Wie op internet zoekt naar foto's van deze actrice maakt relatief de meeste kans om besmet te worden met malware.

ANDROID-PC



Op 26 oktober komt Windows 8 uit, maar wie liever een Android-pc heeft, kan daarvoor terecht in China. Motorola brengt daar de HMC3260-pc uit.

INSTA-GOOGLE

Google heeft voor een onbekend bedrag de Duitse ontwikkelaar Nik Software overgenomen. Dit bedrijf is onder andere de maker van Snapseed, de concurrent van Instagram.

QIBRALTAR

De Britse kolonie Gibraltar gaat het gebied volhangen met QR-codes om zo toeristen van informatie te voorzien, in het kader van Gibraltarpedia.

GAME OVER



De E-Plaza game-winkels verdwijnen uit het straatbeeld. De 58 winkels krijgen volgens moederbedrijf Blokker een andere bestemming. Online blijft E-Plaza nog wel bestaan.

GROOTSTE QR-CODE



Het doolhof van de boerenfamilie Kraay uit het Canadese Alberta is officieel de grootste QR-code ter wereld: het is dik 29.000 vierkante meter groot.

WII U

Nintendo zegt dat zijn nieuwste videospelsysteem, de Wii U, op 30 november in de Europese winkels ligt. Het hd-spelsysteem kan ook zonder televisie gebruikt worden.



Volg-app op gestolen iPad leidt niet tot huiszoeking

Het OM blijft bij haar standpunt om geen huiszoekingen te doen als volg-apps aangeven waar een gestolen smartphone of ipad zich bevindt.

Terwijl minister Opstelten er bij burgers en politie juist op aandringt om meer gebruik te maken van deze volg-apps. De politie is enthousiast, wil het zelfs tot landelijk speerpunt maken.

Het ministerie lanceerde de campagne Hier waak ik, maar het OM vindt huiszoeking nog steeds 'een te zwaar middel'. Volgens woordvoerder Evert Boersma van het OM kan de volgsoftware een bijdrage leveren aan het opsporen van de betreffende iPhone of iPad.

Maar 'alléén op basis van deze volgsoftware zullen politie en OM waarschijnlijk niet kunnen acteren'. Hij verwijst, ook al omdat landelijke richtlijnen hier ontbreken, naar de officiers van justitie die in de betreffende zaak moeten toetsen of er strafvorderlijke beslissingen zoals een doorzoeking kunnen worden genomen.

Opstelten: 'installeer volgapp'
12 oktober 2012

Minister Opstelten van Veiligheid en Justitie gaf in oktober het startsein voor twee campagnes tegen straatroof. Opstelten riep hierbij burgers ook op een 'volgapp' te installeren op hun smartphone.

Dan kan de locatie van een gestolen toestel op een kaartje worden opgezocht. De dief of heler lokaliseren gaat dan stukken makkelijker. Bruikbare apps staan besproken op www.consumentenbond.nl/traceerapps.

Opstelten wil samen met de providers ook kijken of gestolen telefoons op afstand onbruikbaar kunnen worden gemaakt. In België is dit al een tijdje de praktijk. Daardoor worden drastisch minder telefoons geroofd.



BlackBerry Protect

Ook bij veel BlackBerry-modellen kun je software van de producent installeren om het toestel op afstand te traceren en beheren. De app en aanverwante dienst heet BlackBerry Protect.

Om de app te kunnen gebruiken heb je wel BlackBerry data-abonnement nodig ('BlackBerry Internet Service'). J

e downloadt de BlackBerry Protect app via bijvoorbeeld de BlackBerry Protect website; geef bij de installatie de nodige keren aan dat deze app vergaande rechten heeft, en vervolgens log je met je BlackBerry-ID in op de BlackBerry Protect website om verbinding met de telefoon te maken.

Hierna kun je volgens de BlackBerry-producent:

de telefoon op een kaartje weergeven;
de telefoon vergrendelen;
de telefoon leegmaken;
de telefoon een alarmsignaal laten geven;
een bericht op het scherm weergeven;
een (automatische) back-up maken van gegevens op de BlackBerry

Studeren doe je ~~bij~~ ~~de NCOI~~ met YouTube!

De tijd dat YouTube alleen bestemd was voor zelfgemaakte videofilmpjes en het bekijken van muziekclips, ligt inmiddels achter ons.

Misschien wist u het niet, maar YouTube is onderdeel van het Nieuwe Leren.

Zeker op gebied van PC en internet zijn er legio filmpjes te bekijken. U kunt hier uw voordeel mee doen.

Hiernaast een kleine opsomming van mijn reis door YouTube land.



Internetveiligheid: Draadloos netwerk
http://www.youtube.com/watch?v=g8CYxLJru48&feature=plcp

Internetveiligheid: Drive-by downloads voorkomen
http://www.youtube.com/watch?v=kSsVyJUNLG8&feature=plcp

Internetveiligheid: Firefox Privacy
http://www.youtube.com/watch?v=oaKBWmefwR0&feature=plcp

Internetveiligheid: Firefox veilig instellen
http://www.youtube.com/watch?v=QXzDLSX3EXY&feature=plcp

Internetveiligheid: Gebruik wachtzinnen!
http://www.youtube.com/watch?v=weSgrndsKLI&feature=plcp

Herken een nep-hotspot !
http://www.youtube.com/watch?v=Yl4ugWqOws8&feature=plcp

Doe jij het veilig online?
http://www.youtube.com/watch?v=O2ML4YDGtpM&feature=plcp

Internet via het stopcontact
http://www.youtube.com/watch?v=nP80zWrE7TE&feature=plcp

Goedkope of dure HDMI-kabel?
http://www.youtube.com/watch?v=OVgygdrY3vk&feature=plcp

Laat u niet volgen!

Antitracking blokkeert nieuwsgierige bedrijven

Het volgen van mensen op internet lijkt voor de meeste bedrijven zo vanzelfsprekend dat ze het normaal zijn gaan vinden. In het echte leven ligt dit minder voor de hand: we vertellen zelfs aan de kapper niet wat we de afgelopen 24 uur allemaal hebben gedaan. In deze 123 bespreken we de beste antitracking-hulpjes voor uw webbrowser.

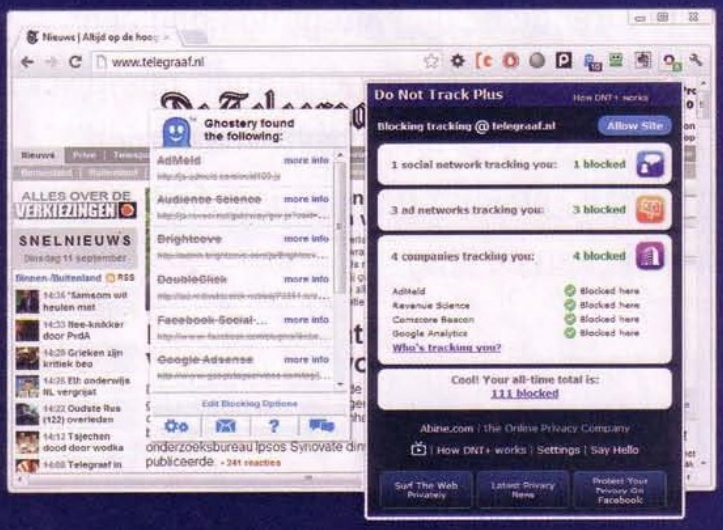
Stap 1: Stempelboekje

De manieren waarop bedrijven u op internet in de gaten houden lopen uiteen, maar dat u constant in de gaten wordt gehouden is geen fictie. Dit is het beste voor te stellen als een stempelboekje dat u overal op internet met u meedraagt. Op bijna elke website wordt uw boekje bekeken en wordt er vrolijk verder gestempeld, zonder uw medeweten. Zo weten bedrijven dat u vorige maand website X bezocht en nu op website Y bent. En ook uw gedrag binnen websites wordt onderzocht. De 'ouderwetse stempelboekjes' werken met cookies. De modernere variant koppelt alles aan elkaar via slimme scripts en socialmedia-plugins. Al dat gespioneer heeft maar één doel: geld verdienen, bijvoorbeeld via gerichte advertenties.

Stap 2: Ghostery & Co

Tracking kunt u het beste tegengaan via een webbrowser-uitbreiding. Geen enkele uitbreiding is waterdicht, maar u kunt ze naast elkaar gebruiken voor een betere 'dekking'. De uitbreidingen Ghostery (www.ghostery.com) en Do Not Track Plus (www.abine.com) werken in elke webbrowser. Tijdens het internetten ziet u via de icoontjes van Ghostery en Do Not Track Plus welke bedrijven informatie proberen te verzamelen. Met Do Not Track Plus kunt u doorklikken voor uitgebreide informatie over de boosdoener. De scripts worden, mits u dit nadrukkelijk aangeeft, geblokkeerd zodat u minder goed bent te volgen.

Do Not Track Plus blokkeert trackingsystemen van social media en advertentienetwerken.



Stap 3: Klassieke cookies

Direct na de installatie van Ghostery en Do Not Track Plus is het flink schrikken als u ziet hoeveel websites proberen meer over u te weten te komen. Met de antitrack-software gaat u geautomatiseerde systemen tegen tijdens het laden van websites, maar de klassieke cookies blijven nog wel binnenkomen. Deze kunt u in uw webbrowser opruimen door op Ctrl+Shift+Del te drukken. De toetscombinatie werkt in Internet Explorer, Firefox en Chrome. Voor het automatisch opschonen van cookies in alle webbrowsers blijft CCleaner (www.piriform.com) de beste keuze.

Niveau stappenplan

Van beginner tot expert. Hiernaast kunt u de moeilijkheidsgraad van het stappenplan zien.





Illegaal downloaden steeds gevaarlijker door besmette keygens

Er wordt steeds vaker malware in keygens gevonden, volgens het halfjaarlijkse rapport van Microsoft.

Uit het rapport dat Microsoft elk half jaar uitgeeft over de trends in de malwarewereld, blijkt dat er in de eerste helft van 2012 een enorme stijging is geweest van malware van het soort 'Win32/Keygen'. Maar liefst vijf miljoen keer werd dit soort kwaadaardige software waargenomen, waarmee het aan de top staat van alle gedetecteerde Windows-dreigingen.

Illegaal downloaden riskant

Keygens worden gebruikt om illegale software zonder officiële sleutel te kunnen gebruiken. Ze genereren een unieke code die de software bruikbaar maakt. Standaard zijn keygens niet kwaadaardig, maar Microsoft zet de software wel massaal op de zwarte lijst. Het bedrijf zegt dat het dit doet omdat 3,8 van de 5 miljoen onderzochte keygens gebundeld was met malware. Het downloaden van keygens is volgens Microsoft daarmee hoe dan ook een riskante onderneming.

Wereldwijd zijn de keygens een grote dreiging volgens het nieuwe rapport. Het Win32/Keygen malwaregenre stond in alle gemeten dichtbevolkte gebieden op zijn minst in de top 10, waarmee de dreiging die ervan uit gaat groter is dan die van beruchte malware soorten als Conficker en FakePav.

De conclusies van Microsoft zijn enkel op basis van de eigen gratis anti-virus software en schoonmaaktools gestoeld. Het werkelijke aantal besmettingen door keygens kan dus nog een stuk hoger liggen



Het woord keygen is een afkorting afgeleid van de Engelse term key generator.

Heel vaak is voor software een licentiecode nodig. Bij illegaal gedownloade software zit vaak een keygen. Deze genereert een licentiecode op basis van een ingevulde naam. Er zit een algoritme achter dat de naam omzet naar een licentiecode.

Een echte keygen hoeft niet illegaal te zijn, maar een keygen is illegaal en dus verboden als het gaat om een programma dat ontsleuteld moet worden waarop de auteur het auteursrecht nog heeft. Als het auteursrecht is verlopen, is de desbetreffende keygen niet (meer) illegaal, omdat iedereen de dan aan het publiek domein vervallen software mag gebruiken.
Keygens zijn altijd toegewijde programma's. Dit betekent dat je een keygen niet voor alle software ter wereld kunt gebruiken, maar slechts voor de bedoelde software.





Opt-in botnet probleem voor banken en landen

Hackers uit het Midden-Oosten legden onlangs een aantal Amerikaanse banken plat via DDoS. De EU zoekt bescherming tegen deze DDoS-aanvallen die hacktivisten inzetten om servers lam te leggen.

Hacktivisten hebben de afgelopen weken een grootschalige DDoS-campagne gevoerd tegen Amerikaanse banken. Hackers konden zich bij de aanval voegen om zoveel mogelijk systemen down te brengen. Onder meer J.P. Morgan Chase ging hard onderuit tijdens de operatie. De groep protesteert daarmee tegen de controversiële film 'Innocence of Muslims'.

Grootschalige oefening
Vorige week voerde de Europese informatiebeveiligingsdienst ENISA in het kader van Cyber Europe 2012 een oefening uit om te zien of publieke en private organisaties bestand zijn tegen cyberdreigingen. Hoog op de agenda stond de Distributed Denial of Service (DDoS), het platleggen van servers door ze te overspoelen met aanvragen. Uit de eerste bevindingen van de cyberoefening blijkt al dat sommige landen hun crisisplannen moeten bijwerken.

DDoS is een groeiend probleem, vooral nu toolkits het makkelijk maken voor aanvallers om zich aan te sluiten bij een DDoS-operatie. Speciale botnets die zombies inlijven om servers te overstelpen met aanvragen zijn in opkomst. Ook de 'terroristische aanval' op Amerikaanse banken gebruikte een slimme methode om nietsvermoedende servers te misbruiken om een DDoS uit te voeren.

Grootschalige DDoS op banken
Een betrekkelijk nieuwe aanvalsvector is het opt-in botnet. Het opt-in botnet wordt specifiek opgezet om iedereen mee te laten doen aan een grootschalige cyberaanval. De C&C stuurt zombies aan met aanvragen naar specifieke servers om een DDoS te veroorzaken. Volgens analisten is het gebruik van deze botnets de sleutel voor succes voor betrekkelijk kleine hacktivistengroeperingen.
Beveiligers vermoeden dat het volume van de DDoS-aanval op Amerikaanse banken nog is toegenomen door het inzetten van DDoS-kits die Content Management Systemen misbruiken. Hackers gebruiken ongepatchte gaten in onder meer Joomla om zo servers het werk op te laten knappen.
Servers kregen op het hoogtepunt van de aanval 30 miljoen packets per seconde te verwerken, zo beschrijft een beveiligingsfirma die het DDoS'en probeerde te stoppen aan Dark Reading. Volgens één bron zou de grootschalige aanval een bandbreedte van 100 Gbps hebben gebruikt.

Afschermen tegen DDoS
De bescherming tegen DDoS ligt volgens sommige deskundigen in het voorkomen van de aanval door de botnets die erachter zitten neer te halen. Maar het praktische probleem daarvan is dat ze wijdverspreid zijn en in een mum van tijd opnieuw zijn in te zetten voor andere doeleinden, van klikfraude, naar het verspreiden van bankingtrojans, naar het meewerken aan DDoS.
Daarom proberen bedrijven en overheden serververkeer zoveel mogelijk af te schermen voor DDoS'ers. Door serverrecources te configureren kan een deel worden afgevangen, firewalls moeten ongewenste pakketjes uitfilteren, via IDS wordt het netwerk gemonitord op verdachte activiteiten en bepaalde appliances helpen met het filteren van webverkeer. Andere methodes zijn geo-blocking als de aanval uit een specifiek gebied komt en het inzetten van reverse proxy's.
Grote bedrijven wijken daarnaast uit naar het inkopen van meer bandbreedte en het gebruik van nog meer redundancy. Zo moet een DDoS-aanval langer duren en een grote golf serveraanvragen versturen om succesvol te zijn. Zo wordt in ieder geval de middelgrote of kortstondige aanval afgeslagen.

Het probleem van een te fanatieke DDoS-bescherming is echter dat het écht webverkeer ook afwijst, zoals bij de tarpit nogal eens voorkomt. Een netwerkbeheerder zoekt de balans tussen het daadwerkelijke risico op een DDoS en de performance-issues die mogelijk optreden met beveiliging.

Europa zet cyberaanval in scène
De aanvallen van de afgelopen weken demonstreren dat hacktivisten sneller en beter in staat zijn dan ooit om effectieve DDoS'en op grote instituten uit te voeren. In het recente verleden was vooral Anonymous succesvol met dit soort aanvallen vanwege een verspreide toolkit die door allerlei aangesloten hackers werd misbruikt.
Het toevoegen van DDoS aan de serie oefeningen van CyberEurope was een logische stap, stelt ENISA-baas Evangelos Ouzounis tegen TechWeek Europe. De impact van DDoS verschilt per organisatie maar met de trend naar toolkits die breed worden ingezet om servers neer te halen, is DDoS een dreiging waar Europa niet omheen kan, aldus Ouzounis.

Zo redt u uw foto's!

Velen van u hebben tijdens de vakantie weer mooie reizen gemaakt en dito ervaringen opgedaan. Maar ergens onderweg ging wat mis met het kaartje waarop de dierbare herinneringen zouden moeten staan. Geen paniek: er is een oplossing!

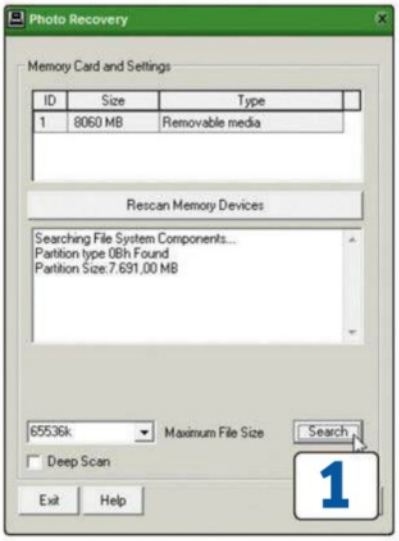
U komt terug van vakantie en u nam mee... Een miniatuur van de Eiffeltoren, een sombrero, een theelepel met de Paus erop, van die dingen. En natuurlijk unieke foto's die het tastbare bewijs zijn van al uw dierbare herinneringen! Zul je nét zien dat de geheugenkaart is gecrasht als deze in de computer wordt gestoken. Of per ongeluk geformatteerd. Of die paar essentiële kiekjes zijn verwijderd. Ga dát maar eens aan de reisgenoten vertellen. Voelt u al een aanval opkomen van acute paniek? Mooi!

In eerste instantie verwijzen we u graag naar Computer Idee nummer 6/2012, waarin een uitgebreide workshop over dataherstel stond die ook van toepassing is op het redden van gegevens die op geheugenkaarten staan. Maar of dat voldoende is? Dat is niet één-twee-drie te zeggen, vandaar deze extra workshop. Hierin introduceren we een absoluut paardenmiddel, waarmee u zelfs de hardnekkigste gevallen van fotoverlies te lijf kunt gaan!

MjM Data Recovery

We sturen u daarvoor naar **data recovery.mjm.co.uk**, de site van het bedrijf MjM Data Recovery, een serieuze datahersteller. Normaal gesproken is het de bedoeling dat u de kapotte datadrager naar het bedrijf opstuurt, waarna men op 'no cure no pay'-basis gaat kijken of er nog wat te redden valt. Zo nee, dan hebt u pech gehad en heeft het niets gekost. Zo ja, dan gaat de meter tikken. Kennelijk is het redden van foto's vanaf geheugenkaarten niet echt lucratief en dat is wellicht de reden geweest om de door MjM zelf gefabriekte tool Data Recovery gratis ter beschikking te stellen. Hierbij gaat het om een programma dat uitsluitend is bedoeld om foto's van geheugenkaarten af te halen – en laat dat nu precies het hulpmiddel zijn waar we op dit moment naar op zoek zijn! Aan u de eer en het genoegen om deze tool – die u vindt door in het menu rechts op de homepage op Free Photo Recovery Software te klikken – te downloaden en te installeren. Gedaan? Dan kunnen we ermee aan het werk.

U kunt het kaartje in een lezer steken of de camera aan de pc hangen: zolang Data Recovery het kaartje maar herkent is er niets aan de hand.



Ziet u grijze vlakken in plaats van thumbnails? Dan moet de maximale bestandsgrootte wat ruimer worden ingesteld.



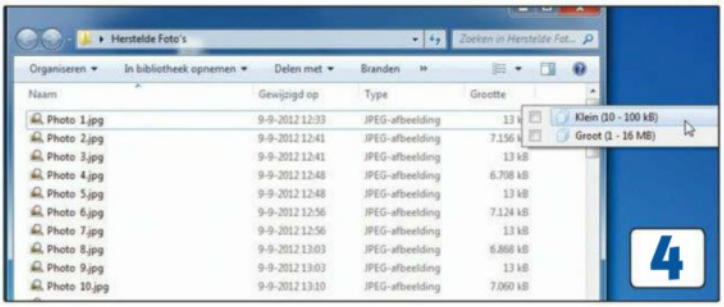
Geheugenkaart aanbieden

Het werken met Data Recovery is niet moeilijk. U start het programma en u gaat een geheugenkaart bij de computer aanbieden. Dat mag via een normale geheugenkaartlezer, maar ook kunt u de digitale fotocamera als 'mass storage device' in een usb-poort van de pc prikken. Binnen Data Recovery dient u dan steeds op de knop Rescan Memory Devices te klikken, want de enige voorwaarde die het programma stelt is dat het de geheugenkaart moet kunnen zien en herkennen (**afbeelding 1**). Dat wil zeggen, de geheugenkaart moet dan fysiek nog wel enigszins in orde zijn, want anders gaat de reddende vlieger helaas niet op...

Verder moet u bij de optie Maximum File Size opgeven wat de maximale bestandsgrootte van uw foto's is. Als u dat niet precies weet, dan stelt u gewoon in op 64 MB, want dat is altijd goed. Eventueel kunt u nog een vinkje plaatsen voor de optie Deep Scan, want dan kan de geheugenkaart nóg grondiger worden benaderd. Modale instellingen zijn een maximale bestandsgrootte van 16 MB zonder Deep Scan en daarmee komt u in 99 van de 100

Via een druk op de knop Save All worden alle foto's die door Data Recovery zijn herkend overgeheveld naar een andere locatie.





gevallen prima weg. Alles akkoord? Dan een klik op de knop Search om te kijken wat Data Recovery voor u kan weten te redden. Meteen vragen we u om enig geduld, want het herstelproces heeft z'n tijd nodig, soms zelfs héél veel tijd. Aan de andere kant doet de computer al het werk en het gaat tenslotte om het eindresultaat. Niet dan?

Foto's veiligstellen

Als Data Recovery voor u bezig is, moet u – zeker de eerste keer – naar de miniatuurweergaven kijken. Als u grijze vlakken ziet, betekent dit dat de Maximum File Size een ietsje moet worden opgerekt **(afbeelding 2)**. Dat doet u door het herstelproces te stoppen, door de bestandgrootte te vergroten en door het herstelproces opnieuw te starten. Ziet alles er goed uit? Dan kunt u achterover leunen totdat Data Recovery helemaal klaar is of totdat u het herstelproces zelf afbreekt.

Meteen daarna klikt u op de knop Save All, om aan te geven dat u alle door Data Recovery gevonden foto's wilt bewaren. Dat bewaren geschiedt uiteraard niet (!) op de geheugenkaart zelf, maar in een map ergens op een harde schijf **(afbeelding 3)**. Het overhevelen van alle foto's kan wat tijd in beslag nemen, waarna u zult zien dat er mogelijk ook wat rommel is meegekomen. Die rommel herkent u in het Details-venster aan de kleine bestandsgrootte. In datzelfde Details-venster kunt u ook een sortering op grootte maken door de kolomkop Grootte aan te klikken **(afbeelding 4)**. Eenmaal gesorteerd op grootte, gaat u alle – te – kleine bestanden selecteren. Die gooit u weg door middel van een druk op de Delete-knop **(afbeelding 5)**.

Opgelucht ademhalen

En vervolgens kunt u opgelucht ademhalen, want al uw foto's zijn weer netjes hersteld en ze staan veilig apart op een harde schijf **(afbeelding 6)**. Met als enige opmerking dat de oude bestandsnamen niet langer bestaan, maar we durven u een kniesoor te noemen als u dáár nog op let. Vanaf nu kunt u de foto's weer naar believen bewerken en ook kan de geheugenkaart weer opnieuw worden gebruikt; iets wat na een formatteeropdracht altijd weer mogelijk moet zijn. Rest het ons om u succes toe te wensen tijdens het terugwinnen van de foto's die, op wat voor manier dan ook, verloren zijn gegaan.

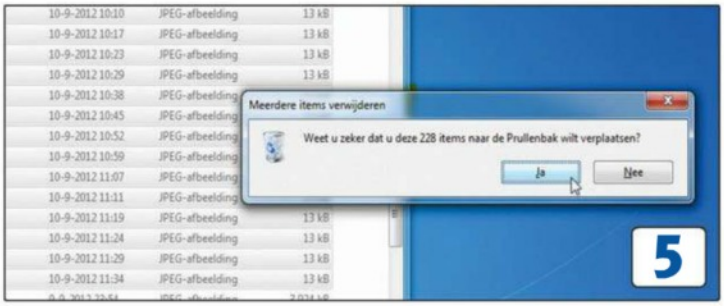
Een foefje... We gaan de veiliggestelde foto's sorteren op grootte. Dit om de kleine en onjuiste bestanden bij elkaar te krijgen.



We kunnen opgelucht ademhalen, want alle foto's zijn netjes hersteld.



De kleine bestanden met rommel hebben we op grootte gesorteerd. Daarna de hele foute boel geselecteerd en op Delete gedrukt.



Ooit het vermoeden gehad dat spammers toegang hebben tot uw Facebook-account? Hoog tijd dan om uw account te herstellen en zó in te stellen dat het kraken ervan een stuk moeilijker wordt, zo niet onmogelijk.

Bent u een Facebook-gebruiker en hebt u last van irritante berichten op uw Facebook-pagina? Ziet u bijvoorbeeld wel eens een link naar een filmpje met een pikante naam? Of hebt u applicaties in gebruik die uw vrienden lastigvallen? Het zijn allemaal aanwijzingen dat uw Facebook-account is gehackt. Ofwel, u zult uw account moeten herstellen en de beveiliging ervan moeten verbeteren.

Hoe dat moet, laten we in dit artikel zien. Voordat we een aantal instellingen op een rijtje zetten, dient u echter ook een aantal dingen te weten over hoe hackers te werk gaan. Meer inzicht hierin kan namelijk helpen om een account beter te beschermen.

Feit is dat het web een goudmijn is voor Facebook-hackers. Zo zijn er gidsen, handleidingen en instructiefilmpjes op YouTube te vinden. Het web biedt daarnaast tal van programmaatjes voor het hacken of terughacken van Facebook-accounts. Veelgebruikte kraakmethodes zijn vooral phishing en keylogging. Via phishing worden reeds eerder gehackte accounts gebruikt om oproepen te kunnen plaatsen op accounts van willekeurige Facebook-gebruikers. Een oproep kan bijvoorbeeld zijn: claim uw mailadres bij Facebook. De pagina waarop het adres kan worden geclaimd, oogt daarbij als een normale Facebook-pagina. In werkelijkheid is deze nep en worden gebruikers naar een externe website gestuurd waarop ze hun gebruikersnaam en wachtwoord dienen in te vullen.



Speciale hacksoftware maakt van Facebook hacken knip- en plakwerk.

Keylogging gaat even listig te werk. Door afluistersoftware op gehackte computers te installeren, kunnen keyloggers screenshots van schermen maken en toetsaanslagen vastleggen. Het doel hierbij is hetzelfde als bij phishing: het stelen van zoveel mogelijk inloggegevens van gebruikers.

Het stelen van cookies is een derde, minder gebruikte hackmethode. In de praktijk werkt deze methode als volgt: een gebruiker logt via een onbeveiligd wifi-netwerk in op een Facebook-account en ontvangt hierbij cookies om zichzelf te kunnen identificeren. Door de cookies met een speciale hacktool te onderscheppen, komen hackers echter eenvoudig in het bezit van een heleboel informatie die in cookies wordt opgeslagen, zoals gebruikersnamen en wachtwoorden op sociale netwerken. Een aantal maanden geleden slaagde een Russische hackerssite erin om zo 6,5 miljoen accounts op de zakelijke netwerksite LinkedIn te kraken.



Slecht beveiligde accounts bieden hackers toegang tot creditcardgegevens onder de link 'Betalingen'.



Identificatie is noodzakelijk om uw account te kunnen herstellen.

Spam

Dagelijks wordt er ruim 600.000 keer op gehackte Facebook-accounts ingelogd. Het cijfer werd vorig jaar door Facebook zelf via het eigen blog naar buiten gebracht. De redenen dat accounts worden gehackt, verschillen echter nogal. De mogelijkheid om grote hoeveelheden spam te versturen, is er eentje van. Gehackte accounts worden daarnaast gebruikt om aankopen te kunnen doen via één of meer door gebruikers geïnstalleerde apps. Alle kosten zijn daarbij voor rekening van de gebruiker. De hiervoor benodigde creditcardgegevens zijn ook simpel te vinden, aangezien deze worden opgeslagen onder de link 'Betalingen' in de accountinstellingen van een gebruiker.

Bezoek het Facebook-helpcentrum

Het helpcentrum van Facebook, te vinden onder het driehoekje rechtsbovenaan een Facebook-pagina, biedt allerlei tips ter beveiliging van een account. Zo vindt u hier allerlei praktische vragen en antwoorden. Hoe rapporteert u bijvoorbeeld misbruik aan Facebook? Of hoe maakt u een veilig wachtwoord?
www.facebook.com/help

Tip!

Louche apps kunnen worden gebruikt om toegang te krijgen tot uw profiel en – in het ergste geval – uw account over te nemen. Controleer dus regelmatig de op uw account geïnstalleerde apps en verwijder onbetrouwbare apps via de link 'Advertenties, apps en websites' onder 'Privacyinstellingen'.

Een andere belangrijke reden dat accounts worden gekraakt, is het feit dat inloggegevens verhandeld kunnen worden op de zwarte markt.

Facebook-accounts worden echter niet alleen gekraakt voor financieel gewin. Hacken kan ook een vorm van pesterij zijn. Bekend hierbij is vooral het voorbeeld van de ex die Facebook gebruikt om te kunnen stalken. Het oude wachtwoord vervangen door een nieuw wachtwoord is in dat geval nodig om een account te beveiligen. Om dit nieuwe wachtwoord te verkrijgen, dient u naar uw accountinstellingen te gaan. Klik vervolgens op de link 'Algemeen' en bij wachtwoord op 'Bewerken'. Facebook zal u vervolgens vragen om het oude wachtwoord te vervangen door een nieuw persoonlijk wachtwoord.

In de praktijk hoeft een hack niet eens op te vallen. Een Facebook-gebruiker wordt soms pas wakker als vrienden hem wijzen op rare berichten of links op zijn Facebook-prikbord. Signalen die erop wijzen dat een account is gehackt, zijn echter vrij divers. Een belangrijk signaal is vooral een toename van spam op iemands account. Andere aanwijzingen kunnen verdachte links zijn, maar ook vage YouTube-filmpjes en onbekende apps. Een malafide app die al veel gebruikers in de val lokte, is de Facebook Profile Viewer. Doordat gebruikers massaal op deze nep-app klikten, kregen hackers toegang tot duizenden profielen.

Maatregelen

Hebt u het vermoeden dat hackers toegang hebben tot uw account? Dan wordt het tijd om een aantal maatregelen te nemen. Check bijvoorbeeld eerst alle eerdere sessies op uw account. Ga hiervoor naar uw accountinstellingen en klik vervolgens op 'Beveiliging' in het menu links bovenaan. Door onderaan de rechterkolom naast 'Actieve sessies' op 'Bewerken' te klikken, ziet u wie er recentelijk heeft ingelogd en met welk apparaat. Zit er een verdachte sessie tussen? Klik dan op 'Activiteit beëindigen' om de sessie af te kunnen sluiten.



De link 'Actieve sessies' toont wie recentelijk op uw account heeft ingelogd.



Via de herstelprocedure is uw wachtwoord opnieuw in te stellen en uw account te beveiligen.



De optie 'Meldingen over aanmelding' staat ter beveiliging standaard ingeschakeld.

Een gehackt account kan in een aantal stappen worden hersteld. Facebook biedt hiervoor een aparte herstelprocedure, waarin de identiteit van de gebruiker wordt gecheckt en het account opnieuw beveiligd. Om de procedure te kunnen volgen, logt u eerst uit op uw account. Klik vervolgens op 'Je wachtwoord vergeten?' rechts bovenaan de pagina.

Op de volgende pagina zal Facebook vragen om uw account 'aan te geven'. Geef hiervoor uw mailadres, telefoonnummer of gebruikersnaam op. Facebook vraagt nu uw gegevens te checken, zoals uw mailadres (en eventueel uw mobiele telefoonnummer). De site laat verder weten een bericht met een code hierheen te sturen om uw wachtwoord te kunnen resetten. Klik op 'Wachtwoord opnieuw instellen' om het bericht te kunnen ontvangen. Is de code binnen? Stel dan uw wachtwoord opnieuw in. Op dezelfde pagina staat ook uitleg wat u moet doen indien u geen code hebt ontvangen.

Is het account weer beveiligd, eventueel ook met een nieuwe gebruikersnaam? Dan zijn er nog een paar extra beveiligingsmaatregelen te nemen. Op het tabblad 'Beveiliging' onder uw accountinstellingen klikt u hiervoor op de optie 'Meldingen over aanmelding'. Door deze optie in te schakelen zal Facebook u via een mailtje of sms'je op de hoogte houden indien er wordt ingelogd op uw account via een niet eerder gebruikte pc of mobiel apparaat.

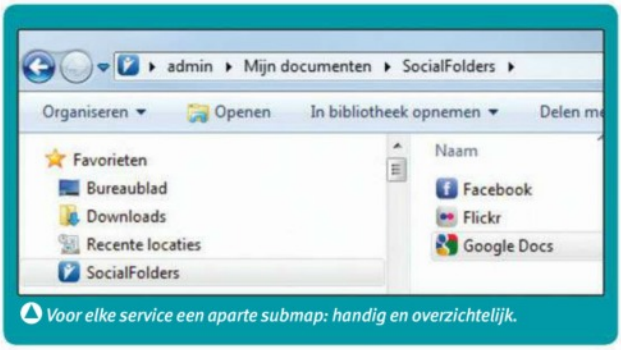
Op hetzelfde tabblad kunt u ook nog de optie 'Aanmeldgoedkeuringen' aanvinken, een functie die bedoeld is om het apparaat te identificeren waarmee een gebruiker inlogt op Facebook. Door gebruikte apparaten een naam te geven, zoals 'thuis' voor een computer of 'mobiel' voor een telefoon, herkent Facebook vervolgens het betreffende apparaat. Wordt het apparaat niet herkend, dan stuurt Facebook ter beveiliging weer een beveiligingscode per sms. Doordat nu eerst uw toestemming nodig is voor toegang tot uw account, voorkomt u simpel dat onbevoegden zich uw account kunnen toe-eigenen.



Via de optie 'Aanmeldgoedkeuringen' kunt u telefonisch bericht krijgen als een onbevoegde toegang probeert te krijgen tot uw account.

Backup van uw online data

Enig idee hoeveel bestanden u op allerlei online services hebt geplaatst? En wat als u ze kwijt zou raken? Met SocialFolders kunt u gegevens van populaire diensten veilig backuppen naar uw eigen pc, of ze overhevelen van de ene dienst naar de andere.



Voor elke service een aparte submap: handig en overzichtelijk.

Met SocialFolders kunt u makkelijk uw foto's van Facebook, uw documenten van Google Docs of andere bestanden die u online hebt staan backuppen op uw computer. Als u zelf nieuwe data in zo'n backupmap plaatst, uploadt SocialFolders die bovendien automatisch naar de juiste online service(s). Bij de gratis versie van SocialFolders bent u beperkt tot tweeduizend bestanden, verdeeld over maximaal drie verschillende services. De premium-versie kent deze beide beperkingen niet, maar kost wel ongeveer 8 euro per jaar.

Installeren & registreren

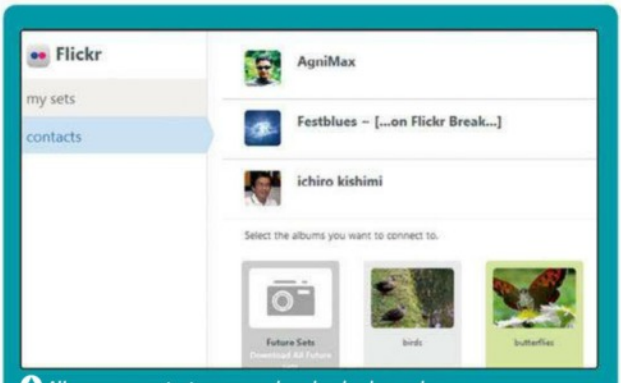
U kunt de backuptool downloaden op socialfolders.me. Na de eenvoudige installatie moet u zich nog wel even registreren. Daarna komt u op https://socialfolders.me/social_folders/services terecht, waar u op Connect to your first service klikt. Vervolgens kiest u welke diensten u wilt backuppen. U zult de gekozen service wel toestemming moeten geven om informatie door te spelen aan SocialFolders. Als u die toestemming weigert, kan SocialFolders uiteraard niet bij uw data komen – en er dus ook geen backup van maken. Meteen daarna bevestigt u met Download all my files.

Backup checken

In principe begint SocialFolders onmiddellijk met het downloaden van uw online gegevens. Klik met uw rechtermuisknop op het pictogram van SocialFolders, in het systeemvak van de Windows-taakbalk. Het contextmenu vertelt u hoeveel procent u hebt gedownload en om hoeveel bestanden het al gaat. Kiest u hier Open SocialFolders, dan wordt de lokale map geopend. Standaard is dat C:\Users\<gebruikersnaam>\Documents\SocialFolders. Voor elke online service vindt u daar een aparte submap. U kunt de boel verhuizen via de Preferences in het contextmenu, waar u op het tabblad Advanced op Change drukt.

Gegevens aanpassen

Om een extra dienst toe te voegen, opent u opnieuw het contextmenu van SocialFolders en kiest u Connect to my services. Links ziet u dan de knop Add a new service, en de rest van het verhaal kent u. Via de optie Settings kunt u ook per service aangeven wat u al dan niet mee in de backup wilt. Bij Flickr en Facebook geeft u bijvoorbeeld aan welke albums uit uw eigen sets u wilt backuppen, maar het is ook mogelijk om albums van contactpersonen of vrienden toe te voegen. Het aanklikken van de gewenste albums volstaat (waarna ze groen kleuren). Via de link Back to all services, linksboven, keert u terug naar het hoofdmenu. Blijkt het downloaden niet meteen of helemaal niet te gebeuren, dan kunt u dat alsnog forceren. Open alweer het contextmenu en kies deze keer Refresh all my services. In de praktijk blijkt dat wel eens nodig te zijn.



Albums van contactpersonen downloaden kan ook.

Data uploaden

SocialFolders werkt zoals gezegd ook in omgekeerde richting: bestanden die u zelf in de map SocialFolders op uw computer plaatst, pikt het programma automatisch op en zal het even later ook netjes online zetten. Wel opletten dus dat u daar per ongeluk geen al te gevoelige data neerzet. Blader bijvoorbeeld naar Google Docs\my files. Daarbinnen maakt u een nieuwe submap en naar die submap kopieert u bijvoorbeeld een xls-bestand. Een paar minuten later vindt u datzelfde bestand ook online terug wanneer u zich bij Google Documenten aanmeldt. U kunt via uw lokale SocialFolders-map dus ook gegevens uit de ene service kopiëren naar de andere. Maar wanneer u data verwijdert uit uw lokale map, worden die niet (!) online gewist. En aangezien die data online behouden blijven, zullen ze ook lokaal opnieuw verschijnen bij de volgende synchronisatieronde.

Service stopzetten

Wilt u een bepaalde dienst uit de greep van SocialFolders halen, meld u dan online aan en klik op Disconnect bij de betreffende service. De lokale backup van die service verdwijnt nu eveneens. Is het echter uw bedoeling om de synchronisatieservice van SocialFolders op een bepaald moment stop te zetten, maar wel met behoud van de map SocialFolders, open dan de Preferences in het contextmenu en klik op Unlink this computer op het tabblad My account.

Repareer je Internet Explorer

Als malware lelijk heeft huisgehouden

Malware of een vervelend neefje kunnen je browserinstellingen lelijk overhoop halen. Gebruik dit handige tooltje om alles weer in de oude staat te herstellen.

Een browser is net zo persoonlijk als het interieur van je slaapkamer. Je hebt favoriete werkbalken, instellingen en een startpagina waar je je dag mee begint. Maar als je besmet wordt, of als iemand anders je computer heeft gebruikt, kan het zo zijn dat je favoriete instellingen onherroepelijk zijn verdwenen. Of toch niet?

Met het gratis programma Browser Repair Tool is het mogelijk om een herinstallatie van Internet Explorer te vermijden. Het tooltje werkt voorlopig alleen samen met de Microsoft-browser, maar we de makers zeggen dat binnenkort ondersteuning komt voor Mozilla Firefox en Google Chrome.

Deze assistent is niet meer dan een checklist waar je onderdelen van de browser kunt afvinken die je hersteld wilt hebben. Maar het is ook mogelijk om irritante trekjes van IE uit te schakelen of enkele handige opties in de Windows-instellingen in- of uit te schakelen.

Die laatste categorie komt vooral van pas voor malware, die vaak instellingen diep in je systeem aanpast om je slinks om te leiden naar malwaresites of ellendige reclames op je scherm te tonen.



Download



Herken een besmette pc en doe er wat aan

Vang het virus en genees je zieke computer

Hoewel er veel nieuwe malware uitkomt, zijn de meeste besmettingen niet uniek. Meestal verandert de malware net genoeg om de bestaande beveiliging te omzeilen. Om het overzicht te bewaren, delen beveiligers malware daarom in in families. Als er een aangepaste versie komt, wordt een bestaande familienaam gewoon voorzien van een nieuw serie-nummer.

De manier waarop malware een computer infecteert, wordt in eerste instantie gebruikt om de verschillende families in categorieën te verdelen. Dit kan verwarrend zijn, omdat de meeste malware zich op meerdere manieren verspreidt. Daarom biedt een familienaam als Trojan bijvoorbeeld geen garantie dat het tegelijk niet ook om een virus gaat. Omdat onderzoekers van verschillende organisaties gelijktijdig aan detectiemethodes werken, hebben malwarefamilies bij ieder bedrijf bovendien een andere naam.

Payload
Naast de infectiemethode heeft malware ook nog een uitwerking, de zogenaamde payload. Die payload kan van alles zijn, bijvoorbeeld het plaatsen van ongewenste advertenties of het stelen van bankgegevens. Omdat de payload binnen een malwarefamilie van generatie op generatie kan wisselen, is het lastig om van een bepaalde besmetting te beweren dat ze alleen gegevens steelt of enkel de browser kaapt.

Kortom, malware verandert constant. Dat maakt het overzicht houden net zo lastig als je computer fatsoenlijk beschermen. Door op regelmatige basis een volledige systeemscan te draaien, geef je de beveiliging de kans om eventuele missers alsnog van het systeem te halen. Daarom plannen beveiligingstoepassingen deze scans maandelijks, wekelijks of zelfs dagelijks in. Ik zocht de symptomen van acht recente infecties die aangeven wanneer het tijd is voor een grondige systeemscan.

1. Onbereikbare bestanden
Malware die je computer kaapt, is makkelijk te herkennen, maar erg akelig. De Trojan.Ransomlock-familie legt zich al sinds 2009 toe op deze activiteit. Zodra je computer geïnfecteerd is, gaat het scherm op slot. De versie van Ransomlock die op dit moment (bijvoorbeeld via Skype) de ronde doet, geeft bij het opstarten de melding dat de politie illegale software op je computer ontdekt heeft. Je dient een bepaalde som over te maken om de controle over je computer terug te krijgen.



Het gemene aan deze besmetting is dat je computer zelfs in veilige modus niet meer bereikbaar is. Opstarten met een bootdisk en de computer scannen op virussen zal in veel gevallen wel helpen. Haalt je beveiligingssuite Ransomlock niet weg, dan bieden verschillende andere bedrijven een verwijdergereedschap op hun website.

2. De zoekmachine doet raar
Als de resultaten van de zoekmachine plots sterk afnemen in kwaliteit, of als er tijdens het zoeken advertenties verschijnen in nieuwe vensters, dan is de kans groot dat je computer geïnfecteerd is. Dat kan een infectie zijn van een lid van de Trojan.Sirefef-familie. Deze malwarefamilie past onder meer de zoekresultaten aan.

De mensen achter Sirefef verdienen aan advertenties die ze je tonen door je de verkeerde kant op te sturen. Andere varianten van deze besmetting brengen popup-reclames in beeld, of sturen je browser ongeacht je instructies naar andere, met advertenties behangen websites.

3. Veel netwerkactiviteit of traag internet
Als je hele thuisnetwerk ineens traag wordt, of als je computer druk contact lijkt te maken met internet terwijl je niets aan het doen bent, dan kan malware die gegevens steelt daar de oorzaak van zijn. Een voorbeeld van zulke malware is Win32:Agent-ANTB. Deze malware steelt gegevens van je computer en stuurt die vervolgens door naar specifieke chatservers en websites. In het geval van Win32:Agent-ANTB gaat het vooral om gegevens om in te loggen bij online casino's. Andere varianten gaan voor inlogcodes bij clouddiensten of online games.

4. Overal popups
Besmetting met adware (malware die ongewenste advertenties op je computer zet) komt veel voor. De laatste maanden doen leden van de Win32.Adware.WSM-familie de ronde. De makers van deze malware verstoppen hun toepassingen in installatiebestanden van legitieme, gewenste software en bieden die geïnfecteerde software vervolgens als download aan op hun eigen websites. Zo raken ook mensen besmet die nooit op illegale websites komen en alleen legitieme software gebruiken.



Een eenvoudige extra maatregel tegen dergelijke besmettingen is vooraf nagaan wie de fabrikant is, om dan de software te downloaden via de website van deze fabrikant. Advertenties die spontaan in beeld springen (zelfs als je niet met de browser bezig bent) of qua inhoud sterk afwijken van de websites waarop ze staan (porno op een nieuwswebsite bijvoorbeeld), zijn duidelijke symptomen van besmetting.

5. Webpagina's onbereikbaar

Als bepaalde webpagina's – bijvoorbeeld die van je computerbeveiliger – niet meer bereikbaar zijn, dan kan dat komen omdat de DNS-verwijzing op je computer veranderd is. De DNS (Domain Name Server) van je provider zorgt ervoor dat het webadres dat je in de browser typt omgezet wordt naar het IP-adres van de server waarop de webpagina staat.

Malware zoals die van de Backdoor.Eminoc-familie verandert meteen na besmetting de DNS-verwijzing op je computer. In plaats van je provider zijn het dan de makers van de malware die regelen naar welk adres je gaat als je de naam van een website opgeeft. Op die manier zorgen ze bijvoorbeeld dat je geen updates voor je beveiligingssoftware meer kan ontvangen. Als je tijdens het surfen ontdekt dat de pagina van je beveiliger niet meer werkt, surf dan ook eens naar een paar pagina's van concurrenten. Als die allemaal tegelijk 'technische problemen' hebben, is het tijd voor een grondige scan.

6. Online bankieren doet vreemd

Aangezien de meeste malwaremakers geld willen verdienen met hun activiteiten is het niet verwonderlijk dat malware die je online bankgegevens tracht te stelen vaak voorkomt. Infecties met zogenaamde banking trojans vangen je inlogcodes op en sturen die door naar de criminelen. Die kunnen dan bijvoorbeeld transacties inplannen op je bankrekening.

In Europa is de trojan Spy Eye een groot probleem geweest, hoewel hier recent behoorlijk wat actie tegen ondernomen is. Het is quasi onmogelijk om zonder beveiligingssoftware te zien dat deze malware op je computer draait. Wel kan het opvallen dat de pagina van je bank niet werkt zoals anders. Dat kan bijvoorbeeld een dubbel verzoek om in te loggen zijn, of een doorgestuurd totaalbedrag dat niet overeenkomt met de bedragen die je overmaakt. Neem bij de geringste twijfel met online bankieren contact op met de helpdesk van je bank en scan je computer.



7. Software verschijnt steeds opnieuw

Klassieke malware gaat niet met pensioen, maar blijft gewoon werken. Dat blijkt wel als we de tot nu toe meest waargenomen infectie van 2012 bekijken. Trojan.Wimad.Gen.1 doet zich voor als een normaal wma-geluidsbestand, maar wie erop dubbelklikt, krijgt de melding dat er een speciale codec nodig is om het af te spelen.

Geef je toestemming om die codec te installeren, dan installeer je onverhoeds een zogenaamde dropper.
Dit standaardonderdeel in bijna alle malware-infecties geeft de malwareverspreider de mogelijkheid om software te installeren op je computer. En vervolgens gebruikt hij deze toegang om naar eigen inzicht nieuwe infecties toe te voegen. Als je computer zich vreemd gaat gedragen, en zeker als malware die je verwijderd hebt maar blijft terugkomen, is de kans groot dat een dropper zich schuilhoudt op je systeem.

8. Beveiligingswaarschuwingen uit het niets
Als je ineens gewaarschuwd wordt door een beveiligingstoepassing die je zelf niet geïnstalleerd hebt, dan heb je waarschijnlijk met nepbeveiliging te maken. Varianten van deze pakketten zijn al jaren in omloop.



Op dit moment zijn bijvoorbeeld de 'suites' van de SmartFortress-familie bijzonder actief. Die installeren zich soms ongevraagd en vaak als onderdeel van andere software op je systeem. Na installatie krijg je meteen de melding dat je systeem gevaar loopt. De enige redding is betalen voor de volle versie. Scannen met een betrouwbare beveiligingssuite is op zo'n moment een beter idee. Dat haalt namelijk de waarschuwingen weg, terwijl betalen alleen maar geld kost.

Doe er wat aan!
Zelfs met een up-to-date beveiligingsprogramma op je computer kan je besmet raken. Een gemiddeld stuk malware heeft een levensduur van drie dagen voor een nieuw lid van de familie het vervangt. Daar staan beveiligers tegenover die de gulden middenweg moeten vinden tussen beveiliging en gebruiksgemak. Als de beveiliging maximaal is, kan je niets meer met je computer doen. Maar is de beveiliging te laag, dan komen er ongewenste bestanden binnen. Dat spanningsveld tussen gebruiksgemak en beveiliging geeft malwaremakers de kans om hun slag te slaan. Maar wie denkt dat beveiliging daarom zinloos is, vergist zich. Want zonder beveiliging is het risico om geïnfecteerd te raken talloze keren groter.

Als je computer symptomen van besmetting begint te vertonen, is er nog niet meteen reden tot paniek. Doorloop de volgende stappen tot je probleem is opgelost.

1. Start je beveiligingstoepassing en geef opdracht om de definitiebestanden van een update te voorzien. Doe vervolgens een uitgebreide scan op de hele computer.

2. Werkt de update niet (meer)? Bezoek dan de website van je beveiliger en gebruik diens online scanner. Werkt de site van je beveiliger niet? Stuur dan een mail naar de ondersteuning van die beveiliger.

3. Ga naar de site van een andere beveiliger en probeer de online scanner op die locatie.

4. Kan je geen enkele beveiliger meer bereiken, ga dan naar vrienden of bekenden om op hun computer een gratis boot-cd te downloaden. Onder meer AVG, Kaspersky en F-Secure bieden op hun website een zogenoemde Rescue Disc aan. Start je systeem vanaf deze cd en volg de instructies van de scanner, zodat je hele computer uitgebreid gescand wordt.

5. In een aantal gevallen krijg je van de boot-cd scanner wel een melding met de naam van de besmetting, maar ook het bericht dat automatisch verwijderen niet lukt. Dit komt (meestal) omdat het besturingssysteem op de boot-cd niet kan schrijven naar de harde schijf van je computer. Maar met de naam van de besmetting kan je op de website van de producent van de boot-cd een programma ophalen om de besmetting handmatig te verwijderen.



Illegale torrents: wat zijn de gevolgen?

Een overzicht van de eeuwige strijd

Torrentsites hebben het moeilijk. Ze worden niet alleen steeds vaker op ISP-niveau geblokkeerd, sinds kort filtert ook Google zijn automatische zoekresultaten op malafide torrentsites. Een overzicht van de gevolgen voor een technologie die zo nauw verweven is geraakt met illegale downloads.

1. Moeilijk bereikbaar

De Zweedse torrentsite The Pirate Bay is al jarenlang een doorn in het oog van belangenorganisaties en – met dank aan stevig lobbywerk – zelfs regeringen. Ondanks alles blijft The Pirate Bay overeind, al zul je soms wat moeite moeten doen om de site effectief te bereiken.

2. Censuur

Ook Google gaat nu piraterijsites censureren in de automatische aanvulling van zoektermen en de automatische zoekresultaten. De maatregel was begin december 2010 al aangekondigd, maar wordt nu dus effectief uitgevoerd. Wie termen als Bittorrent, torrent, utorrent, Rapidshare en Megaupload ingeeft, krijgt geen suggesties voor zoektermen meer. Ook het automatische zoeken wordt uitgeschakeld bij zoektermen die met piraterij te maken hebben. Als je dan doorklikt op de zoekknop, kun je nog wel zoekresultaten vinden.

3. Verwijderen van url's

Googles censuur komt er uiteraard onder druk van de muziekindustrie. Google was trouwens op eigen initiatief begonnen met het verwijderen van url's. Volgens het transparantierapport dat Google in mei vrijgaf, is het bedrijf bezig met het verwijderen van miljoenen url's die naar verluidt auteursrechtelijk beschermd materiaal bevatten. Het haalt de url's systematisch neer op basis van vragen van auteursrechtenhouders.

4. Magnet-links

Maar de geviseerde torrentsites laten zich niet onberoerd. Zo biedt The Pirate Bay, sinds begin 2012 naast torrentbestanden ook zogenaamde magnet-links aan. Deze bevatten de hashcode van de torrent, die dan gebruikt wordt om de te downloaden bestanden op te sporen bij medegebruikers. Ze kunnen ook bestandsnaamdata bevatten, of links naar trackers die door de torrent gebruikt worden. Met onschuldige magnet-links hoopt men minder snel aansprakelijk gesteld te kunnen worden als torrentsite.

5. ISP's mengen zich in het debat

Ook de ISP's mengen zich in het torrentdebat. Zo bleek eind 2011 dat het Belgische Telenet al sinds 2008 bepaald torrentverkeer op zijn netwerk vertraagt. Ook in andere landen is dit een gangbare praktijk. ISP's werpen als verdediging op dat ze hun netwerk niet willen laten overbelasten door torrentverkeer. Zelfs regeringen moeien zich. Demonoid, een van de grootste torrentsites, wordt sinds deze zomer offline gehouden door de Oekraïense autoriteiten. Die willen mogelijk zo de VS tonen dat het auteursrechten ernstig neemt.

6. Pirate Pay

Technologie bestrijden met technologie, dat is Pirate Pay. Een Russisch bedrijf bouwt een systeem dat de distributie van illegale werken via torrents flink hindert. Sony en Disney probeerden 'Pirate Pay' al met succes uit. Hoewel het bedrijf niet specifiek uitlegt wat zijn methoden zijn, lijkt het de communicatie tussen torrentcliënten in de war te brengen, waardoor zij de verbinding met elkaar verbreken en het beschermde bestand zo niet kan worden gedeeld. De uitvinding zou een effectief middel kunnen zijn om de illegale verspreiding van juist gelanceerde kaskrakers voor korte tijd te ontmoedigen.

Secure Computing