



Secure Computing

Nieuwsbrief Juni2013

W.Bosgra taakaccenthouder digitale criminaliteit

In dit nummer:

Wet Computercriminaliteit III

Darknet

Gratis bellen met Facebook app

Klaar voor Ipv6?

Bootsectorvirus

Zoek je eigen digitale sporen

Computercrash en dan..?

en meer.....

(nu met onderwerp index vorige nummers)

Dit digitale magazine wordt verzorgd door Secure Computing.

Doel is bewustwording van wat u doet met de computer, kennis opdoen gericht op de opsporing van strafbare feiten (cybercrime) en veilig computergebruik.

U kunt deze nieuwsbrief opslaan op uw eigen "Home"-omgeving en als naslagwerk blijven gebruiken.

Indien u dit magazine tevens in uw eigen thuisomgeving bewaart, kunt u gebruik maken van de ingebouwde hyperlinks.



[E-mail? klik hier !](#)

Het nieuwe wetsvoorstel bevat een uiteenzetting van hackbevoegdheden van het OM, de mogelijkheid van een NTD bevel en de mogelijkheid van een decryptiebevel.

WET COMPUTERCRIMINALITEIT III: TERUGHACKEN MAG

Doordat steeds vaker draadloze netwerken of cloudcomputing diensten worden gebruikt en doordat elektronische gegevens steeds vaker versleuteld worden, is het voor het OM moeilijk om toegang te krijgen tot communicatie. Normale telefoongesprekken kan het OM in bepaalde omstandigheden aftappen, maar bij elektronische communicatiediensten zoals Skype, Twitter of Gmail gaat dat niet zo gemakkelijk. De communicatie is vaak versleuteld en vindt plaats met gebruikmaking van verschillende apparatuur (telefoon, pc, tablet).

Het nieuwe wetsvoorstel voorziet daarom in de mogelijkheid dat de overheid inbreekt op de computer van een verdachte en daar spyware plaatst die het gebruik van de computer in de gaten kan houden, zoals keyloggers om toetsaanslagen af te vangen of het aanzetten van de microfoon om een gesprek af te luisteren. Daarmee zou veel gerichter kunnen worden getapt. Ook voorziet het wetsvoorstel in de mogelijkheid dat de overheid heimelijk toegang kan verkrijgen tot gegevens die in de cloud zijn opgeslagen, zonder dat de verdachte of dienstverlener daarbij betrokken is.

Een van de kritiekpunten op het wetsvoorstel is dat het ziet op 'geautomatiseerde werken'. Volgens de memorie van toelichting gaat het dan om privé computers, smartphones, routers en servers, maar in werkelijkheid zou dat begrip veel groter zijn. Ook auto's en slimme energiemeters kunnen er namelijk onder vallen.

Ook de extraterritoriale werking van het wetsvoorstel is een punt van kritiek. Hoewel het in de praktijk niet ongebruikelijk is dat opsporingsdiensten van staten zich toegang verschaffen tot gegevens die zijn opgeslagen op computers op het grondgebied van andere staten, is dit niet geheel in lijn met het internationale recht.

Het zogenaamde decryptiebevel, waarbij de verdachte kan worden gedwongen om de sleutel te verstrekken om gegevens te kunnen ontsleutelen, stuit op veel weerstand. Dit lijkt immers in strijd te zijn met het grondrecht om niet mee te hoeven werken aan je eigen veroordeling.



Natuurlijk bevat het wetsvoorstel ook waarborgen. Zo kan een hackbevel bijvoorbeeld voor maximaal 4 weken worden ingezet en moet het door de Centrale Toetsings Commissie worden goedgekeurd.

Het wetsvoorstel en de Memorie van Toelichting vindt u via de Schatkistpagina.

Lees voor een uitgebreide bespreking van het wetsvoorstel de bijzonder [informatieve blog](#) van Jan Jaap Oerlemans.

“Omdat mensen in toenemende mate gegevens niet meer op hun computers, maar op servers van buitenlandse (cloud)dienstaanbieders opslaan, bieden de huidige bevoegdheden voor de vergaring van gegevens van computers op een locatie in Nederland volgens Opstellen onvoldoende mogelijkheden.”

DARKNET

Het net onder het Web

Het DARKNET, soms ook wel ten onrechte DEEPWEB genoemd, is een collectie van webdomeinen, welke niet door zoekmachines geïndexeerd kunnen worden.

Na het downloaden volg de instructies Nauwkeurig om het TOR programma juist te installeren.

De volgende stap is het vinden van de 'Hidden Wiki'.

Een schatting uit 2012 leert ons dat er ongeveer 600 terabyte aan data staat.

Het Darknet wordt gebruikt door activisten, journalisten, militairen en mensen zoals u en ik.

De schaduwzijde is dat het wordt gebruikt voor illegale activiteiten. Wapenhandel, drughandel en kinderporno zijn slechts enkele van deze activiteiten.

Er zijn veel valkuilen op het Darknet. Wees dus gewaarschuwd als u zich daar begeeft.

Elke website met de extensie *.onion* Wordt gehost (-op het internet plaatsen-) als een verborgen TOR service, een volkomen anonieme manier om websites te hosten.

Hoe vind je nu die *.onion* websites? Het eerste wat je nodig hebt is een client welke jou toegang verschaft tot de *.onion* domeinen. De client die je nodig hebt is genaamd TOR. Dit programma maakt het mogelijk webpagina's op het Darknet te bekijken. TOR zorgt tevens voor een extra laag beveiliging omdat het jou 'onzichtbaar' maakt.



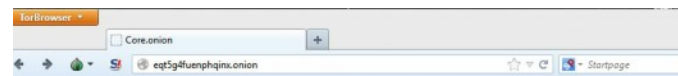
Dit is een index van alle voorkomende soorten pagina's op het Darknet. De index verschaft je de mogelijkheid om op het Darknet te navigeren. Er zijn genoeg pagina's die uitnodigen tot een bezoek, maar onthoud dat

er een groot aantal valkuilen op het Darknet zijn.

Durf je het aan?

[Hier vind je de 'Hidden Wiki'](#)

Een fameuze pagina op het Darknet is [de Core.onion pagina](#).



Welcome to .onion.

Core onion has served as the simple entry-point to the .onion network since July, 2007.

[Talk onion](#) | [OnionBookmark](#) | [TorStatusNet](#) | [Tor Status](#) | [Duck Duck Go](#) | [Hushbox](#)



[Deepweb](#)



[Home](#)

[About Tor](#)

[Documentation](#)

Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.



[Download Tor](#)

- Tor prevents anyone from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, remote logins, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

Let op: de links genoemd in dit artikel functioneren alleen als u dus gebruik maakt van een TOR-client.

TOR via Windows gebruiken? Download dan de [TOR browser bundel!](#)

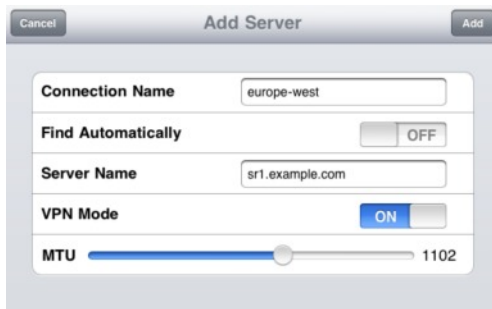
Als sinds juli 2007 fungeert dit als toegangspoort tot het *.ion* netwerk.

De Amerikaanse National Security Agency (NSA) en FBI zouden direct toegang tot de servers van negen grote Amerikaanse internetbedrijven hebben en kunnen zo chatgesprekken, foto's, e-mails en documenten opslaan en analyseren.

NSA tapt servers Microsoft, Facebook en Google

Dat zou blijken uit een geheim document dat de Washington Post in handen heeft gekregen. Het project heeft de codenaam PRISM en zou al jaren actief zijn.

Volgens het geheime document zou de NSA alles wat het wil direct vanaf de servers van Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube en Apple kunnen downloaden. Microsoft zou het eerste bedrijf zijn geweest dat aan PRISM meedeelde. Het programma zou vooral op buitenlands communicatieverkeer zijn gericht, dat vaak via Amerikaanse servers loopt.



[NSA PRISM](#)

Inlichtingen

De Amerikaanse overheid laat in een reactie weten dat de informatie die via het programma wordt verzameld tot de belangrijkste en meest waardevolle buitenlandse inlichtingen behoort die de VS verzamelt. Daarnaast zouden verschillende zaken in het bericht van de Washington Post over PRISM niet kloppen, maar er worden geen details gegeven.

Apple en Facebook zeggen niet met het programma bekend te zijn. "We hebben nog nooit van PRISM gehoord", zegt Apple-woordvoerder Steve Dowling. "We geven geen enkele overheidsinstantie directe toegang tot onze servers."



Geheim

In het document zou de NSA stellen dat de identiteit van de private bedrijven die meewerken het belangrijkste geheim is, uit angst dat de bedrijven zich terugtrekken zodra bekend wordt dat ze de inlichtingendienst helpen. "98% van de productie van PRISM is gebaseerd op Yahoo, Google en Microsoft, we moeten ervoor zorgen dat we deze bronnen geen schade toebrengen."

Eerder werd ook al bekend dat Verizon en mogelijk ook alle andere Amerikaanse telecombedrijven de gespreksgegevens van miljoenen Amerikanen verzamelen en aan de



Tor adviseert privacycocktail tegen afluisteren NSA

Hoewel veel details over het PRISM surveillanceprogramma van de NSA ontbreken, zijn er weldegelijk maatregelen die internetgebruikers kunnen nemen om hun privacy en identiteit op het internet af te schermen.

Dat stellen de makers van Tor, software waarmee internetgebruikers anoniem kunnen internetten en hun communicatie kunnen afschermen.

Zelfs in gevallen waar bijvoorbeeld bestaande gecentraliseerde communicatie-infrastructuur door de NSA, China, Iran of andere landen of diensten zijn gecompromitteerd. Volgens Mike Perry van het Tor Project, de organisatie die Tor ontwikkelt, biedt Tor geen bescherming zodra de communicatie het Tor-netwerk verlaat.



Cocktail

Daarom is het verstandig om Tor in combinatie met andere tools te gebruiken, zoals HTTPS-Everywhere in de Tor Browser, maar ook andere programma's zoals TorBirdy en Enigmail, OTR (Off the Record) en Diaspora. Hierdoor kan Tor de communicatie beschermen, zelfs in het geval de infrastructuur, zoals Google of Facebook, is gecompromitteerd.

Het beschermen van Gmail of Facebookaccounts tegen overheids-surveillance is volgens Perry onmogelijk. Wel kan Tor dienen als een bouwsteen voor een systeem waar het niet meer mogelijk is voor een enkele partij om de volledige metagegevens, communicatiefrequentie of content van internetgebruikers te achterhalen.



Toekomst

Het gebruik van Tor hidden services beschermt gebruikers zowel tegen de analyse van metagegevens als surveillance. Perry geeft als voorbeeld een P2P-communicatiesysteem dat zowel over een client als server beschikt, alsmede een Tor hidden service.

Hierbij zijn de clients meteen de servers. De communicatie via deze systemen is privé en vindt plaats zonder gecentraliseerde partijen of tussenpersonen.

Perry erkent dat het nog wel even kan duren voordat het grote publiek over dit soort tools beschikt of hiermee overweg kan. "We beseffen dat er nog veel werk moet gebeuren voordat zelfs de basis-tools, zoals de Tor Browser, TorBirdy, EnigMail en OTR, naadloos en veilig voor de meeste gebruikers werken, laat staan complexe combinaties zoals XMPP of Diaspora met Hidden Services."



[HTTPS Everywhere](#)



[TOR browser](#)

Virus Information

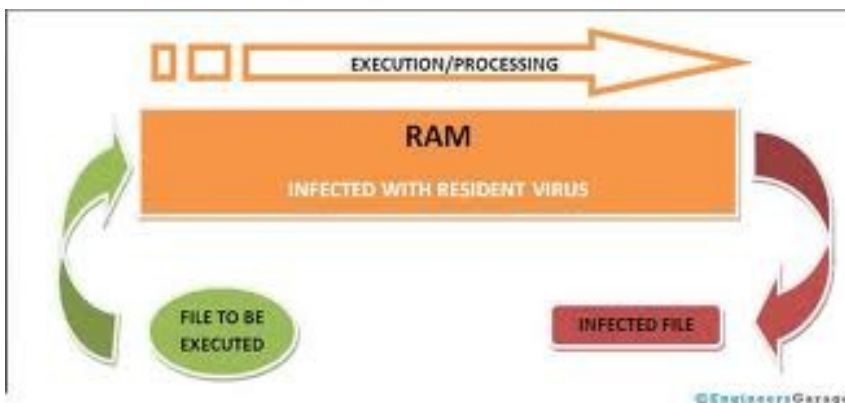
Er zijn verschillende soorten virussen naargelang de manier waarop ze werken, hoe ze zich verspreiden en wat hun bedoeling is. We sommen ze hieronder kort op.

Bestandsvirussen

Bestandsvirussen tasten zogeheten uitvoerbare bestanden aan. Dat zijn computerbestanden, die als je er op klikt, een programma starten. Als je bijvoorbeeld je tekstverwerker start, start je eigenlijk een uitvoerbaar bestand. Niet-uitvoerbare bestanden zijn bijvoorbeeld de documenten die je kunt maken met die tekstverwerker.

Uitvoerbare bestanden of programma-bestanden herken je doordat ze na hun naam een achtervoegsel hebben zoals .EXE, .DLL of .COM (niet te verwarren met de .COM achter de naam van een website).

Bestandsvirussen hechten zich aan uitvoerbare bestanden en starten hun werk wanneer je het uitvoerbaar bestand opent. Ze kunnen gegevens vernietigen en de werking van je computer verstoren.



Geheugenresidente virussen

De naam geheugenresident betekent dat deze virussen zich in het werkgeheugen van je computer nestelen. Het werkgeheugen of RAM-geheugen is het geheugen waarin de programma's draaien als je de computer gebruikt. Wanneer je je computer uitzet, wordt dit geheugen gewist. Wanneer je de computer de volgende keer opstart, zal het virus automatisch opnieuw in het werkgeheugen opduiken.

Omdat het werkgeheugen zo centraal staat in de werking van een computer, kunnen deze virussen makkelijk schade toebrengen aan alle bestanden en programma's die in dat werkgeheugen worden geopend.

Dit type virussen kan bestanden beschadigen en wissen, maar ook de werking van de computer totaal verstoren.

Macrovirussen

Een macrotaal laat toe om binnen het computerprogramma waarvan ze deel uit maken sommige taken te automatiseren.



Zo bevatten tekstverwerkers en rekenbladen een macrotaal. Je kunt daarmee macro's schrijven, die bijvoorbeeld opeenvolgende bewerkingen in één keer kunnen toepassen.

Macrovirussen zijn geschreven in diezelfde macrotalen en doen zich voor als een gewoon tekstbestand, een rekenblad... Als je dat bestand opent in je tekstverwerker of rekenblad en automatisch ook de macro's aanvaardt, dan kan het zijn vernietigende werk beginnen.



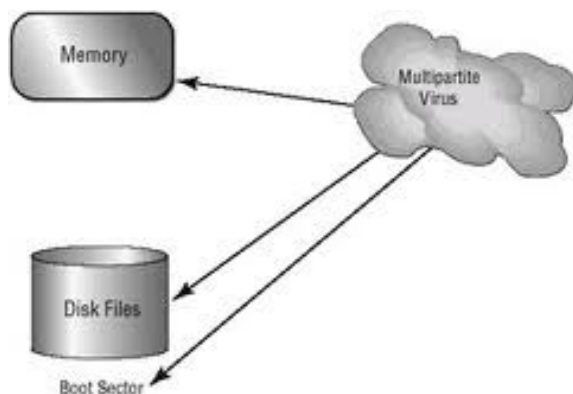
Opstartsectorvirussen

De opstartsector, in het Engels 'boot sector' is een plaatsje op de harde schijf van je computer waar zich een klein programma bevindt dat de computer opstart wanneer je hem aan zet.

Dit wordt in een afzonderlijk artikel verder uitgelegd.

Multipartitie-virussen

Je zou multipartitie-virussen kunnen omschrijven als een combinatie van meerdere andere soorten virussen. Multipartitie-virussen kunnen de computer van het slachtoffer achtereenvolgens op verschillende manieren aantasten: eerst bijvoorbeeld de macro's, dan de bestanden, dan weer de harde schijf en zo verder.



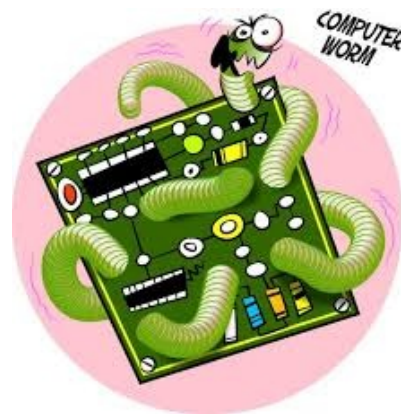
Ze zijn daarom vaak moeilijker te verwijderen en kunnen op verschillende manieren tegelijkertijd schade toebrengen.

Wormen

Ook wormen zijn geen virussen in de strikte zin van het woord. Het zijn programma's die zich vanzelf verspreiden langsheen netwerk- en internetverbindingen, vaak zelfs zonder menselijke tussenkomst.

Zo verspreiden ze zich van computer tot computer. Precies omdat wormen zo sterk gericht zijn op computernetwerken, kunnen ze die vertragen of zelfs helemaal lam leggen. 'Succesvolle' wormen zijn er in het verleden in geslaagd om volledige bedrijfsnetwerken te doen vastlopen.

Wormen komen ook vaak binnen via bestandsbijlagen van een e-mail. Als je er op klikt, verspreidt de worm zich vanzelf verder, bijvoorbeeld naar iedereen in je adresboek.



Trojaanse paarden

Trojaanse paarden zijn geen virussen in de strikte zin. Ze worden meestal meegestuurd met een – gratis – programma zoals een screensaver of een spelletje en nestelen zich ongemerkt op je harde schijf.

Ze kunnen zich niet zelfstandig verder verspreiden. Eens ze op je computer staan kunnen ze wel bestanden vernietigen, of een instelling veranderen. Trojaanse paarden worden vaak geschreven door individuen die op die manier langs een achterpoortje via het internet toegang krijgen tot je PC.

De term Trojaans paard verwijst naar het 'echte' paard van Troje: het gevaarlijke programma zit als het ware in de buik van een leuk of nuttig programma dat er ongevaarlijk uit ziet. Ongemerkt 'opent' het programma een achterpoortje van je computer voor de vijand die dan bijvoorbeeld gegevens kan vernietigen of stelen, of spam versturen.

Trojaanse paarden worden vaak gebruikt door hackers.

“Wormen komen ook vaak binnen via bestandsbijlagen van een e-mail”

Alles over een Bootsectorvirus

Wat is een bootsectorvirus, wat doet een bootsector virus, hoe kom ik er weer van af en hoe kom ik er achter dat ik een boot sector virus heb.

Wat is een Bootsectorvirus precies
Wat is nu een bootsectorvirus. Als we het woord bekijken boot-sector-virus. Het woord boot betekend in het Engels opstarten. Sector betekend een gedeelte van een geheel en virus is een stukje code die kwaadwillende doeleinden heeft.

Als we dat samenvoegen en in de juiste context plaatsen ontstaat er dus een gedeelte van het opstart systeem besmetten met een kwaadwillig stukje code.

Technische uitleg

Als een computer opstart zorgt de BIOS (basic input output system) ervoor dat de computer verder gaat naar de bootsector. In de boot sector staat precies wat de computer moet doen. Zo moet de computer Windows opstarten, de virusscanner aanzetten en bijvoorbeeld msn opstarten. Zoals je ziet is voor die tijd je computer niet beschermt omdat de antivirus niet aanstaat. Dus als een virus voor die tijd op de computer wordt gezet dus in de bootsector wordt geplaatst heeft een virus vrij-spel.

Geschiedenis

De bootsectorvirus is ontstaan in de begin tijd van het pc gebruik. Vroeger had bijna elke pc een floppy drive. Wat de computer dan doet is, kijken als ik eerst op kan starten via de floppy drive en dan pas wat er in de boot sector staat. Als er een bootsectorvirus op de floppy stond paste de floppy je bootsector aan en je was besmet. Gelukkig met de komst van de cd was de floppy overbodig en was er een groot risico verdwenen. Het grootste gevaar van een floppy was namelijk dat een andere virus die op je computer staat een bootsector virus op je floppy kon zetten. Dat kan namelijk niet bij een cd want is cd zijn in de meeste gevallen niet herschrijfbaar. Ook hebben de BIOS ontwikkelaars niet stil gezeten.

Ze hebben een systeem ontwikkeld waardoor je kunt aangeven dat er geen wijzigingen mogen aangebracht worden in de bootsector waardoor een bootsectorvirus een lange tijd uit het zicht is geweest.

De comeback van de boot sector virus

Met de opkomst van de bootable usb stick (opstartbare) hebben als het ware weer een digitale floppy gecreëerd met de zelfde gevaren als toen. Daarom is het verstandig om deze functie uit te zetten in je BIOS en alleen aan te zetten wanneer je echt wilt opstarten via usb. Helemaal is het verstandig is om je usb stick te scannen met een virusscanner als je pc en virusprogramma nog aanstaat.



Malwarebytes ontdekt ook bootsectorvirussen.

Download [hier](#) de gratis versie!



Hoe verwijder je een bootsectorvirus

Dat ligt er helemaal aan, als je een bootsectorvirus te pakken hebt die gewoon op de achtergrond mee draait maar verder niet aan de hoofdprocessen komt dus kun je met een goede antivirus programma je virus verwijderen. Als je weet om welk virus het gaat en je kunt je pc niet meer opstarten vanwege het virus dan zijn er op internet meestal anti bootsectorvirussen te vinden die de bootsector virus tegen gaan. Als het een onbekend virus is of je weet niet wat voor virus het is, is er nog maar 1 optie en dat is de hardeschijf formatteren. Dit is overigens wel je laatste redmiddel.

De Anti-Malware Testing Standards Organization ([AMTSO](#)) heeft deze week op zijn website een aantal gratis tests geplaatst die moeten nagaan of de voornaamste beveiligingsschilden van antiviruspakketten operationeel zijn.



AMTSO wil eindgebruikers en bedrijven zo helpen om te controleren of zij voldoende beschermd zijn tegen moderne malwareaanvallen, zoals drive-by downloads, phishing sites en trojaanse paarden.

Het gebruikt daarvoor standaardbestanden van EICAR.com, die in de beveiligingswereld al jaren worden gebruikt om de respons te testen van securitysoftware.

Minimale bescherming

Bij sommige tests moet je een bestand naar de desktop halen, terwijl je bij andere een website moet openen. Het doel van de tests is om te controleren of alle onderdelen van je antivirusbescherming wel naar behoren zijn ingeschakeld. Het is dus niet bedoeld om een vergelijkende test uit te voeren tussen gratis of betalende beveiligingspakketten.

Want als je antiviruspakket geen alarm slaat bij het doen van deze relatief eenvoudige tests, is het een goed idee om uit te zien naar een ander pakket. Want als je bescherming deze op zichzelf onschuldige testbestanden niet tegenhoudt, maakt het nog minder kans om een daadwerkelijke malwareaanval af te stoppen.

Je kunt de tests van AMTSO [vinden op deze pagina](#).

Het favoriete gereedschap van cyberspionnen

Securityspecialist Kaspersky Lab waarschuwt voor NetTraveler, een set van gevaarlijke programma's die cyberspionnen gebruiken om geheime data van organisaties en ondernemingen te onderscheppen.

Volgens Kaspersky zijn de cybercriminelen er tot hiertoe in geslaagd om belangrijke informatie te ontfutselen van meer dan 350 organisaties in 40 landen.

Het gaat daarbij om overheidsinstellingen, ambassades, olie- en gasondernemingen, onderzoekscentra en militaire bedrijven. NetTraveler zou al sinds 2004 een sluimerend bestaan leiden, maar pas de laatste jaren zeer actief geworden zijn.

Met de groeten van de Dalai Lama

De aanvallers besmetten hun slachtoffers door ingenieuze spear-phishing e-mails te versturen met kwaadwillende Microsoft Office-bijlagen. De bijlagen luisteren naar namen als:

Army Cyber Security Policy 2013.doc,

Report - Asia Defense Spending Boom.doc,

Activity Details.doc,

His Holiness the Dalai Lama's visit to Switzerland day 4 en

Freedom of Speech.doc.



[NetTraveller](#)



Een beetje achtergrond

Elke machine die op het internet is aangesloten, heeft een uniek adres nodig om te kunnen communiceren. Net zoals huizen een adres nodig hebben om er post tussen uit te kunnen wisselen.

Klaar voor Ipv6?

IPv4, het communicatie protocol dat momenteel gebruikt wordt op het internet stamt nog uit de tijd dat computers gigantisch groot en heel duur waren. Toen is besloten dat zo'n 4 miljard mogelijke adressen meer dan voldoende zou moeten zijn.

Natuurlijk zijn computers sindsdien sterk geevolueerd, ze zijn betaalbaar geworden voor veel meer mensen, over de hele wereld. Buiten de traditionele computers zijn er tegenwoordig ook veel kleinere apparaten die met het internet worden verbonden, denk maar aan smartphones, iPads, etc.. allemaal met hun eigen adres.

Dit alles heeft ervoor gezorgd dat de IPv4 adressen bijna op zijn. Om dit op te lossen, is er een nieuwe versie van dit protocol ontwikkeld, genaamd IPv6. Dit bevat verschillende veranderingen maar de belangrijkste is dat er veel meer mogelijke adressen zijn, heel veel. Zoveel dat het niet meer uit te spreken is. Voor zij die het toch eens willen proberen: aantal ipv6 adressen. We kunnen dus wel stellen dat het aantal adressen voor het eerst geen probleem meer zal zijn.

De IPv4 en IPv6 protocols zijn echter niet compatibel, het zijn twee verschillende talen. Iemand met een IPv4 adres kan niet naar een IPv6 site en omgekeerd. De eenvoudigste manier om deze overgang te realiseren is wat men noemt "dual stack". Het komt erop neer dat men de twee kanten de beide talen aanleert.

Websites hebben twee adressen, 1 voor bezoekers die enkel IPv4 spreken en 1 voor bezoekers die IPv6 spreken. Eindgebruikers zullen ook twee adressen krijgen om alle sites op internet te kunnen bereiken, onafhankelijk van welke taal ze spreken.

Door een tijd lang dubbel te blijven draaien, voorkomt men dat iedereen op dezelfde moment zou moeten overschakelen, wat niet realistisch is.

Momenteel zitten we in deze overgangsfase. Een aantal providers leveren al IPv6 adressen aan hun gebruikers. De bekendste in België en Nederland is XS4ALL. De andere providers hebben daar dit jaar of volgend jaar plannen voor.

Er zijn echter nog niet veel websites bereikbaar op IPv6. De reden is dat de eigenaars van websites schrik hebben bezoekers te verliezen. Er zijn namelijk een aantal mogelijke problemen die zich kunnen voordoen wanneer een site zowel IPv4 als IPv6 aanzet. Door fouten in verschillende browsers, besturingssystemen of netwerkcomponenten, is het mogelijk dat een klein percentage van gebruikers de website niet meer zou kunnen bereiken of het heel traag zou kunnen gaan. Dit wordt geschat op minder dan een halve percent van de bezoekers, maar voor grote sites zoals google zijn dat heel veel verloren bezoekers.

Doe de Ipv6 test

Websites verdienen geld en zijn dus niet snel geneigd om dit te riskeren. Dus zijn een aantal grote websites en providers samengekomen en hebben ze afgesproken om voor 1 dag lang allemaal IPv6 aan te zetten. Tijdens deze dag zullen ze registreren hoeveel gebruikers ze juist zouden verliezen en krijgen de providers wereldwijd de kans om eventuele problemen in hun netwerk te lokaliseren.

Bron: PCwereld.be



Het niet leveren van spullen via Marktplaats terwijl daarvoor door slachtoffers wel is betaald, is niet altijd oplichting. De rechtbank in Haarlem heeft een Beverwijker hiervoor vrijgesproken.

Rechtbank spreekt man vrij van oplichting via Marktplaats



Het niet kunnen en willen leveren van spullen terwijl daarvoor wel is betaald, is op zich niet strafbaar als oplichting. Dat heeft de meervoudige kamer van de Haarlemse rechtbank geoordeeld. Een man uit Beverwijk reageerde via Marktplaats op advertenties waarin mensen vroegen naar een bepaald boek of cd. Daarbij meldde hij dat boek te kunnen leveren, maar hij eiste wel vooruit betaling. Na die betaling weigerde hij te leveren.

In totaal ging het zeker om 21 slachtoffers, die ieder voor 15 tot 55 euro het schip in gingen. Justitie had de man voor de rechtbank gehaald onder beschuldiging van oplichting, maar de rechters oordeelden anders. Wel werd bewezen geacht dat de man met voorbedachten rade niet van plan was te leveren terwijl daarvoor wel was betaald, maar volgens de rechters is dat geen oplichting, maar eerder een wanprestatie. Daardoor is de man niet in overtreding volgens het wetboek van Strafrecht, maar moet hij civielrechtelijk worden aangepakt.



Man gebruikte eigen naam en bankrekening



De rechters kwamen onder meer tot deze conclusie doordat de man zijn eigen naam en die van zijn vriendin gebruikte, eigen e-mailadressen gebruikte en ook het geld liet overmaken naar zijn eigen bankrekening of die van zijn vriendin, die overigens met naam en toenaam in het vonnis wordt genoemd in tegenstelling tot de verdachte zelf.

De officier van Justitie, die een werkstraf van 180 dagen eiste, of 90 dagen vervangende celstraf eiste, vond ook dat de man door het gebruik van de naam van zijn vriendin, een valse naam had opgegeven, een van de vereisten voor een vervolging als oplichter. De rechters veegden dat van tafel. Ook de beschuldiging van witwassen klopte volgens de rechtbank niet, omdat niet kon worden bewezen dat het geld dat de man kreeg, uit criminele activiteiten afkomstig was.

De slachtoffers hadden allen een eis tot schadevergoeding ingediend. Omdat de man werd vrijgesproken, zijn ook de eisen van de slachtoffers afgewezen.

Zoeken naar je eigen digitale sporen

Een harde schijf is geen statisch gegeven: voortdurend worden er bestanden verwijderd en komen er nieuwe bij, waarbij niet zelden oude data deels worden overschreven. Je zou dus denken dat er van je oude data al snel geen spoor meer terug te vinden is. Die visie moet je echter al snel bijspijkeren wanneer je er een forensische tool als Autopsy op loslaat.



[Autopsy 3.0.5 gratis download](#)



[Autopsy](#)

Autopsy is eigenlijk een grafische schil, zowel voor Linux (in een iets oudere versie) als voor Windows, rond The Sleuth Kit en aanverwante (opdrachtregel)programma's: een reeks openbrontools die er specifiek op gericht zijn op allerlei manieren "verwijderde" of verloren gewaande gegevens alsnog weer op te diepen. Forensische software van het zuiverste kaliber dus.

In feite is het de bedoeling Autopsy op een schijfimage los te laten, hoewel het ook mogelijk is het programma op een bestaande volume naar sporen te laten zoeken. Dat laatste valt natuurlijk niet aan te raden, omdat er altijd een risico bestaat dat je de originele data (ongewild) wijzigt – wat in forensisch-wetenschappelijke kringen alvast not done is. Maar goed, het kan wel.

Bij het opstarten van deze 'forensische browser' start je logischerwijze een nieuwe 'case' op, waarbij je een of meer volumes (images) kunt betrekken. Je geeft tevens te kennen in welk soort data je zoal geïnteresseerd bent. Houd er wel rekening mee dat zo'n forensisch onderzoek een werk van lange adem is, waarbij het af en toe kan voorkomen alsof Autopsy – of zelfs het complete systeem – vastgelopen is. Een analyse van enkele uren is in elk geval niet uitzonderlijk, vooral afhankelijk van de grootte van de image(s).



Autopsy opereert grotendeels bij de gratie van een reeks (standaard meegeleverde) plug-ins. De namen van deze plug-ins geven al een aardig idee van de gehanteerde methodes: KeywordSearch, Hash-Database, ThunderbirdParser, SevenZip, ExifParser, RecentActivity, enz.

Als het goed is, krijg je dan na afloop de resultaten gepresenteerd. De gevonden data worden netjes gecategoriseerd in (onder meer) ip-adressen, e-mailadressen, cookies, webgeschiedenis, downloads, enz. Daar kunnen overigens ook data tussen zitten, afkomstig van bestanden die al (veel) eerder waren "verwijderd". Een tijdlijn maakt het mogelijk dat je data opvraagt volgens het tijdstip waarop ze zijn gecreëerd. Detailrapporten laten zich bovendien exporteren naar onder meer html en Excel.

Een gecrashte computer weer opstarten



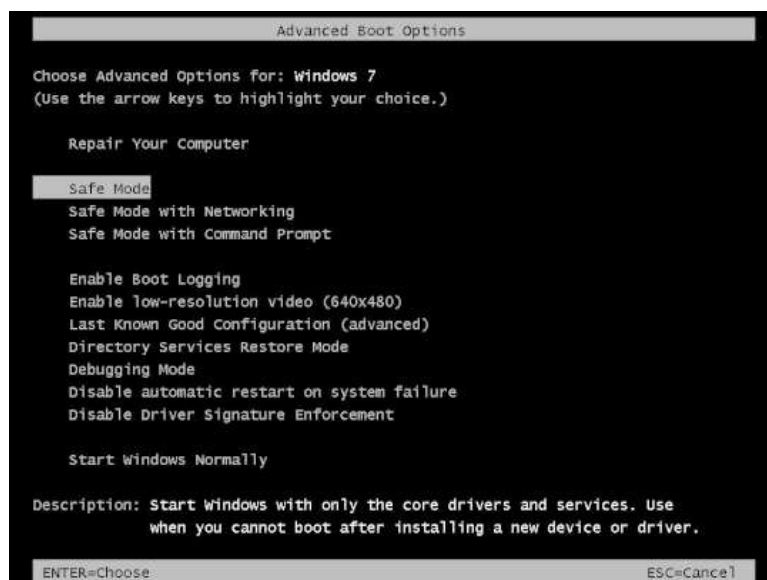
Je computer herstarten is altijd het eerste advies dat je krijgt na een serieuze crash. Maar nadat je de computer een paar keer vruchteloos uit en weer aan hebt gezet, wil je misschien eens iets anders proberen.

STAP 1 / Veilige modus

Wanneer Windows niet meer normaal wil opstarten, is er altijd nog de 'Safe Mode', die dient om problemen op te lossen. Je computer start (hopelijk) op met een standaard configuratie die veel van je normale instellingen achterwege laat. Je kan nu proberen om een voor een je instellingen en drivers aan te zetten, en uit te vissen welke je pc om zeep heeft geholpen.

In Safe Mode kan je ook in het configuratiescherm om recente programma's terug weg te halen, die misschien verantwoordelijk zijn voor je Blauwe Scherm. Je start op in Safe Mode door tijdens het booten van je computer op F5 of F8 te drukken. Met wat geluk krijg je zo het boot menu te zien.

Om je computer alsnog aan de praat te krijgen, kies je Safe mode, of Safe Mode with networking. Bij die laatste kan je ook op het internet, om bijvoorbeeld een antivirustool te downloaden.



STAP 2 / Boot van de installatie-cd

Welk besturingssysteem er ook op je computer draait, een installatie-cd krijgt hem meestal wel terug opgestart. Installatie-cd's zijn per definitie 'bootable', wat betekent dat ze je harde schijf kunnen laden, bijvoorbeeld om er je besturingssysteem op te zetten.

Die cd of dvd heeft meestal ook een herstelfunctie aan boord. En het is die laatste die je nodig hebt om je besturingssysteem na een zware fout terug in de plooi te krijgen. Stop de installatie-cd in je computer en start hem op.



STAP 3 / Opstartschijf maken en gebruiken

Geen installatie-cd? Is je computer bijvoorbeeld door een kleine computerwinkel in elkaar gestoken, dan zit daar niet altijd zo'n cd'tje bij.

En zelfs als je dat ding hebt gekregen, is het nog maar de vraag of het de verhuis overleefd heeft. Je kan gelukkig altijd een nieuwe boot-cd of systeemherstelschijf maken, al zal je dat moeten doen voordat je computer zichzelf naar de vernieling helpt.

In Windows moet je daarvoor naar het Configuratiescherm, waar je in het venster voor Back-ups de optie vindt om een systeemherstelschijf te maken.



De cd zal, net als een installatie-cd, enkele tools aan boord hebben om je systeem te repareren, met als handige extra dat hij ook een systeemkopie van je bestaande computer kan gebruiken en terugzetten ... als die er is, natuurlijk.

STAP 4 / De meubels redden

Lukt het je niet met de ingebouwde tools van je besturingssysteem, dan kan je als ultieme reddingsoperatie nog een cd'tje maken met daarop de treffend genaamde Ultimate Boot CD for Windows

www.ubcd4win.com.

Het programma werkt een beetje zoals een systeemherstelschijf, maar het laat je onder meer backups maken en heeft diagnostische tooltjes, defraggers en malware-scanners aan boord. Dat kan trouwens ook met een USB-stick. Zorg er in dat geval wel voor dat je de opstartvolgorde of 'boot order' van je BIOS instelt, zodat hij kan opstarten van een USB-stick. Je raakt in het BIOS-menu door tijdens het opstarten een toets in te drukken, meestal Esc of Del, al kan het ook F1, F2 of F10 zijn.



You want to crash!!!
I show you how to crash!!!



Wil het allemaal niet baten, dan is het misschien tijd om je pc naar de specialist te brengen. Maar voor je dat doet, kan je nog snel proberen om je belangrijkste bestanden terug te krijgen.

Een van de makkelijkere manieren om dat te doen, is via een 'bootable' cd van een klein besturingssysteem. Puppy Linux www.puppylinux.org, bijvoorbeeld, neemt amper plaats in en laat je snel je harde schijf openen, zodat je alsnog je bestanden kan veiligstellen.

Minder pop-ups door versoepeling cookiewet

De overheid gaat de cookiewet zo aanpassen dat er geen toestemming meer hoeft te worden gevraagd voor cookies die niet privacygevoelig zijn. Het gaat dan onder andere om cookies die de werking van websites verbeteren, de zogeheten analytic cookies. Dit schrijft minister Kamp van Economische Zaken aan de Tweede Kamer. Die merkt op dat de privacy van gebruikers nog steeds beschermd is.

"Ik vind het belangrijk dat de privacy van internetters goed wordt beschermd", aldus minister Kamp. "Tegelijkertijd moeten we er voor zorgen dat

deze bescherming niet doorslaat en burgers onnodig veel hinder ondervinden van pop-ups".

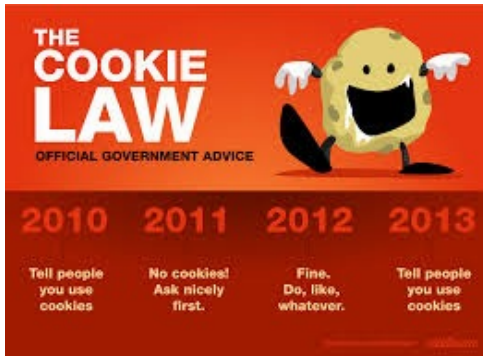
Toestemming

Door de voorgestelde aanpassing hoeven websites bezoekers niet meer te informeren over en toestemming te vragen als met het plaatsen of lezen van een cookie informatie wordt verkregen over de kwaliteit of effectiviteit van een geleverde dienst mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de internetter.

Hierdoor vallen voor die dienstverlening nuttige cookies, zoals analytische cookies, testing-cookies en affiliate cookies, niet langer onder de informatieplicht en het toestemmingsvereiste. Voor cookies die het surfgedrag van internetgebruikers volgen verandert er niets. Hiervoor moet nog steeds vooraf toestemming worden gegeven.

Reacties

De komende zes weken kunnen belangstellenden, eigenaren van websites, consumenten en anderen reageren op het wetsvoorstel. Daarna gaat het voorstel naar de Raad van State. Het wetsvoorstel wordt naar verwachting in het najaar naar de Tweede Kamer gestuurd.



[Cookiewet](#)

Gratis bellen met Facebook-app nu mogelijk

Facebook laat gebruikers in Nederland gratis met elkaar bellen via hun internetverbinding.

Facebookgebruikers in het buitenland kunnen al langer met elkaar bellen via de app van het sociale netwerk. De mogelijkheid is nu ook in Nederland beschikbaar gekomen.

Het gratis bellen is zonder update te gebruiken in de apps voor iPhone, iPad en Android. Ook binnen de Messenger-app van Facebook is de bel-functie toegevoegd.



Verscholen

De optie zit wel wat verscholen. Wie iemand gratis wil bellen moet via het chat-gedeelte van Facebook naar de informatiepagina van die persoon. De knop daarvoor zit zowel op iOS als Android rechtsboven.

In het venster 'Contactgegevens' dat dan opent is nu ook voor Nederlanders de knop 'Bel gratis' beschikbaar. Over wifi zijn de gesprekken geheel gratis, over het mobiele netwerk wordt data uit de internetbundel gebruikt.

Na ieder gesprek geeft Facebook de mogelijkheid om in 1 tot en met 5 sterren aan te geven hoe de kwaliteit van het gesprek was.

Bron: Nu.nl

Forensische scanner vindt TrueCrypt-containers

Een nieuw programma dat opsporingsdiensten en forensisch onderzoekers kunnen gebruiken bij het analyseren van harde schijven is nu ook in staat om versleutelde bestanden en harde schijf images weer te geven, waardoor geen enkel bewijs meer gemist wordt. Voorheen was er volgens ontwikkelaar Passware geen snelle manier om dit soort bestanden te detecteren.



[Passmark](#)

De Passware Kit kan systemen binnen een uur scannen en containers van TrueCrypt, BitLocker, PGP en andere software herkennen. "Eén van de grootste obstakels bij elk digitaal onderzoek is de mogelijkheid om de inhoud van met wachtwoord beveiligde bestanden en harde schijven te onderzoeken", zegt Passware CEO Dmitry Sumin.

Bron: Security.nl

Slaapstand

Volgens het softwarebedrijf zou de nieuwste versie van Passmark garanderen dat geen enkel bewijs verborgen blijft.

De software is nu ook in staat om op Windows 8 computers hibernatiebestanden (hiberfil.sys) te analyseren en encryptiesleutels van BitLocker, TrueCrypt, PGP alsmede wachtwoorden van websites, Windows-gebruikers en MS Office-bestanden te achterhalen.

Daarnaast worden nu ook AMD ATI videokaarten ondersteund voor het achterhalen van MS Office 2013, Zip en Apple iTunes wachtwoorden.

Oude domeinnamen Sovjet-Unie paradijs voor internet-criminelen

Toen het oude Rusland het nieuwe Rusland werd, veranderde .su in .ru. Maar alle oude domeinextensie van de Sovjet-Unie zijn nog steeds in gebruik.

Vooraf bij internetcriminelen en hackers die het .su domein gebruiken voor nepsites, spam, botnets en andere cybercrime.

Volgens Oren David van beveiligers RSA zijn internetcriminelen deze extensie massaal gaan gebruiken toen Rusland in 2011 de regels voor .ru domeinen verscherpte.

Het aantal kwaadwillende .su sites verdubbele sindsdien elk jaar. Beveiligers Group-IB meldt zelfs dat meer dan de helft van alle Russische cybercriminelen een .su extensie gebruikt.





Veilig Nederland spuwt onevenredig veel malware



[Denis Maslennikov](#)

Nederland behoort nog altijd tot de grootste landen wanneer het gaat over het verspreiden van malware. Ondertussen zijn Nederlanders zelf online relatief veilig.

Na de Verenigde Staten en Rusland is Nederland wereldwijd de grootste verspreider van malware. Maar liefst 14,4 procent van de malicieuze hosting services is gevestigd in ons land. Een jaar geleden werd nog 11 procent, van alle malware in Nederlands gehost, terwijl er in november zelfs een piek van 17 procent zichtbaar was.

Daar staat tegenover dat Nederlanders relatief weinig risico lopen om geïnfecteerd te raken. Dat blijkt uit statistieken van virusbestrijder Kaspersky die zijn verzameld in kwartaalrapport geschreven door beveiligingsexpert Denis Maslennikov. Kaspersky krijgt cijfers binnen uit 213 landen via gebruikers die data delen via Kaspersky-producten.

Links zijn grootste dreiging

De top 2 blijft bezet door de Verenigde Staten en Rusland. Door een afname in het aantal Russische malware-verspreiders, wisselen beide landen stuivertje. De Verenigde Staten kende een lichte stijging van 3 procent in het aantal malware-hosts, terwijl er in Rusland 6% minder malware is verspreidt in het eerste kwartaal van 2013. Dat brengt Amerika terug als leider van het malware-klassement.

Uit het rapport blijkt dat kwaadaardige links nog altijd veruit de grootste dreiging op het internet opleveren. Deze links, die leiden naar recent gehackte websites of websites die speciaal gemaakt zijn door malwaremakers, zijn goed voor 91,4 procent.

Geavanceerde malware, zoals trojans, exploits en malware verstopt in adware nemen het overgebleven deel voor hun rekening. Zoals gebruikelijk richten malwaremakers zich bij de desktop op Windows en bij mobiel op Android. Ruim 20.000 nieuwe malware-varianten doken er voor dat mobiele platform op in het eerste kwartaal van 2013. Met name SMS-trojans zijn een populair middel voor aanvallers.

Nederlander is veilig

De malware die vanuit Nederland wordt verspreidt is niet gericht op zijn eigen inwoners. Nederlanders komen relatief bijzonder weinig malware tegen. We behoren tot de categorie met het op één na laagste infectie-risico. Iets meer dan een kwart (26,9 procent) van de Nederlanders heeft te maken gehad met malware.

Niet voor het eerst blijkt Adobe- (Flash, Reader en Shockwave) en Oraclesoftware daarbij het meest onveilig.

De meeste kwetsbaarheden worden aangetroffen in Oracle's Java, maar liefst 45,26 procent van alle computers. Op gepaste afstand volgen Apple (QuickTime), Google (Picassa), Nullsoft (Winamp) en VideoLAN (VLC). Het doel van malwaremakers is vrijwel altijd het verkrijgen van systeemtoegang via gaten in deze software.

Bron: Webwereld

Op dit moment in de schatkist:

(Klik op de kist om het te downloaden)

Wet Computercriminaliteit III

Memorie van Toelichting

Recuva

Bootkit Removal Tool

UnstoppableCopier

Blackberry Desktop Software

Format Factory



Twee miljoen Nederlanders ooit slachtoffer ID-fraude

In totaal twee miljoen Nederlanders zijn ooit slachtoffer geworden van identiteitsfraude. In 2012 ging het om 612 duizend gedupeerden, die ruim 350 miljoen euro schade opliepen. Het aantal slachtoffers bedroeg in 2007 nog ongeveer 75 duizend. Sinds dat jaar is de totale schade opgeteld 2,8 miljard euro. De meeste schade is het gevolg van financiële identiteitsfraude (onder meer skimmen), een op de vijf slachtoffers werd via internet benadeeld. Het kabinet komt najaar 2013 met een bredere aanpak van identiteitsfraude.

Campagne 'Stop Cybercrime.nu'

Met de campagne 'Stop Cybercrime.nu' proberen MKB-Nederland, Digibewust, TNO en het ministerie van VenJ, ondernemers bewust te maken van de beveiligingsrisico's van hun systemen. In 2012 werd zo'n 40% van alle ondernemers slachtoffer van computervirussen, phishing en andere malware; 45% geeft toe er te weinig verstand van te hebben.

Onderzoek: Twitter helpt (wijk)agenten

Twitter helpt! Dat wist u natuurlijk al lang, maar het is nu ook wetenschappelijk bewezen: recent onderzoek van de Universiteit Utrecht en het Center for Public Innovation laat zien dat twitter de politie inderdaad kan helpen bij het oplossen van zaken. Agenten ontvangen veel relevante informatie van burgers, twitter versterkt de opsporing, vooral in zaken als hennepkwekerijen en vermissingen, en verbetert de veiligheid in de wijk. Politieagenten gaven verder aan dat ze veel direct messages met burgers uitwisselen. Volgens onderzoeksleider Albert Meijer is het 'interessant dat burgers bij al die kleine gevallen in hoge mate bereid zijn om mee te denken met de politie en relevante informatie door te sturen'.

Twitterproef in Barneveld voor veiliger wijk

Gemeente en politie in Barneveld gaan samen twitter inzetten om de wijken veiliger te maken. Eind juni is er een 'Blauwe Twitteravond' in de wijken De Lors, Oldenbarneveld en Rootselaar West, waarop buurtbewoners in tweetallen de wijk ingaan en elke verdachte situatie via twitter melden, met daarbij 'een van tevoren afgesproken sleutelwoord'. Volgens veiligheidscoördinator Dirk Klein van de gemeente, is twitter een constructieve manier om burger en overheid te laten samenwerken. De politie kijkt mee met de tweets en garandeert dat elke melding 'wordt opgepakt'. Klein zegt dat alles getwitterd mag worden: 'een verdacht persoon in de wijk die er niet woont, een langzaam rijdende auto, het ruiken van een wietlucht of het zien van loslopende honden. Dat soort dingen'.

Wijkagenten promoten twitter en 'hashtack'

Op Haarlemmermeer Dichtbij hebben de jeugdagent en twee wijkagenten uit Hoofddorp de bevolking opgeroepen niet alleen politie en gemeente te informeren over veiligheid, maar vooral ook elkaar. Volgens hen is twitter daarvoor 'een uitstekend medium'. Als alerte buurtbewoners elkaar attenderen, kunnen ze 'juist met elkaar een vuist maken'. Bij tweets over overlastlokaties, verkeerszaken, onprettige verlichting, signalementen van verdachte personen of verdachte vervoersmiddelen moeten buurtbewoners dan de 'hashtack' (sic) #veiligOverbos gebruiken zodat iedereen kan meelezen.



Dit magazine verschijnt maandelijks. De inhoud bestaat uit verzameld werk uit openbare internetbronnen. Voor zover mogelijk zal de bron worden vermeld.

Opmerkingen kunt u mailen naar [de redacteur](#).

Onderwerp index edities 2012:

12-01 > Computercriminaliteit, Definitie van Cybercrime, Strafbare gedragingen, Aftappen van gegevens, MSN chat via Windows, E-mail headers zichtbaar maken, Botnet, Hacking, Spyware,

12-02 > Kwaadaardige software, Phishing, Keyloggers, DNS aanval, Politiemethodes voor bewijs

12-03 > Man in the Middle, ID alert, Meldingsformulier identiteitsfraude, Meldpunten, Wetsartikelen voor computercriminaliteit in enge zin, Cyberstalking, Grooming

12-04 > E-mail spoofing, Elektronisch briefgeheim, Afgeven klantgegevens, Gebruik een live cd/dvd voor veilig internetbankieren, Cloudcomputing

12-05 > Van password naar passphrase, Nieuwe phishing scams, E-mail blunder, Word documenten kunnen virussen bevatten, Hoe hackers u misleiden, Cyberkatvanger, Gratis Windows-tool voor veilig internetbankieren, HP USB disk storage format tool, Muis smeriger dan wc bril

12-06 > Microsoft calling?, Computer in slaapstand of uitschakelen, EU wil internetidentiteitskaart, BVH kan het nog slechter, Wat is Facebook echt waard, Browser voor liefhebber social media, Politievirus, Wardriving, Vind gratis wi-fi op je vakantiebestemming

12-07/08 > Facebook: Nieuwe tactiek om verblijfsvergunning te krijgen, Facebook scant chatconversaties van gebruikers, Lokpuber ontmaskert pedofiel in chatbox, Uw smartphone virusvrij, Facebook Hyves Twitter: zo komt u van uw accounts af, Hoe hackers hacken, Vakantie? Smartphone mee, Beelden bewakingscamera's sneller online, Nederland mist urgentie in aanpak cyberdreiging, Antivirus bedrijf AVG lanceert social media beheertool

12-09 > Veilig WiFi, ID alert, Versnel je windows PC, Windows 7 administrator account activeren, Anders knippen en plakken, Open DNS, Beter geluid uit uw PC, Instellingen makkelijk terug vinden, XBMC het alternatief voor Windows media center, Windows 7 sneltoetsen, De windows toets, Free Video Converter, Je gegevens zijn op internet gelekt, wat nu, PC gekaapt, Money mules, I-frame injection, Zoekmachine misbruik, Hardware printers, Opinie: Cybercrime, Social engineering, WhatsApp berichten veiligstellen, E-boeken downloaden, Beter zoeken met Google, Studeren doe je met YouTube, Handige freeware, I-doser, Tablet kopen, Smartphone beveiliging, Find my Phone,

12-10 > Is spyware illegaal, Wanneer valt website onder cookiewet, Wapen uit 3d printer, Facebook plug-in beschermt foto's tegen pottenkijkers, Hackpreventie, Libre Office, Hardware videokaart, Apps: wat moet je weten, Variaties op de Nigerian scam, Handige hulpprogramma's voor je PC, Tips om je smartphonebatterij te sparen, Meeste Torrent-downloaders gemonitord, Populaire vingerafdruklezer lekt Windows wachtwoord, Grote bestanden verzenden, De Russen komen, Digitaal onderzoek politie schiet tekort, Facebookfoto's beschermd met plug-in, Nederlanders doelwit valse Rechtspraak.nl e-mails

12-11 > Politievirus waarchuwt slachtoffers via Mp3, Trusteer voor veilig internetbankieren, Veilig internet: behaal het certificaat, Cameratoezicht: mag wel/ mag niet, Panopticon, Laat u niet volgen, Key generators, Opt-in botnet probleem voor banken en landen, Zo redt u foto'd, Facebook: geen toegang voor spammers, Backup van uw online data, repareer je internet explorer, Herken een besmette PC en doe er wat aan, Illegale torrents: wat zijn de gevolgen,

12-12 > Ontsleutelen, Malafide webwinkels, Romance scam, Phiishing mail vraagt om foto van TAN-codes, HTTPS Everywhere, Metadata Cleaner,

Onderwerpen Index edities 2013

2013-01 > Voorspellingen 2013: maatschappelijke trends, Herken jij alle nep-virusscanners, Overheid onthult richtlijnen voor hackers, Anti-virus boot cd/dvd's, Browser plug-ins, Hoe weet je dat je smartphone is gehackt, Hoe gezond is je harde schijf, Halkf miljoen wifi routers lek, Telefoneren via Facebook, Voicemails sturen met Facebook messenger, Data verbergen, USB sneller verwijderen, Beter zoeken met Google, Tips voor Windows 8, Internetprovider, De gevaren van een enkele Net identiteit

2013-02 > Nederlandse politie worstelt met TOR, Nieuwe versie Police Ransomware, Cloudopslag vereist nieuwe wetgeving, Drugs bestellen via de post: sure we can, Cybercrises in aantocht, Ultieme dataredder bij stervende schijf, Virusedoder vermomt zicht om besmette pc's te ontsmetten, Microsoft bestrijdt processor-dief op Windows pc's, WiFi Protector beschermt je WiFi buiten de deur, Politie en NCSC laks na hack duizenden bedrijven, Opinie: opofferen privacy helpt niet tegen cybercrime

2013-03 > Toebyname phishingmails, Angifte phishing: stel de volgende vragen, Cybertaal,: bezemen - Vishing _ Sexting, SSID, Valse Flash player update verspreidt politievirus, Een veilige smartphone in toe stappen, Opinie: het neerhalen van botnets is zinloos

2013-04 > Wat is een Ddos aanval, Cybercriminelen zetten buitenwipper in, Antiwaskist mobiele telefoons, Inbreken op router wel strafbaar, Vaker kinderporno op Nederlandse servers, Meeste mail-malware verstopt in ZIP bestanden, Gestolen mobiel voor de zomer onklaar, Visie rapport Trends in Veiligheid 2013, Zoeken op internet in alle privacy, Sociale media vast onderdeel van politiewerk, Glasvezel internet, PhoXo gratis forobewerking, Geen downloadverbod voor particulieren, 20% websites bevat kwaadaardige code, Nep muiscursor beschermt t wachtwoord tegen gluurders, Zo maakt u sterke wachtwoorden, In de schatkist, Opinie: wij sturen online criminelen de verkeerde boodschap

2013-05 > VPN, PGP, Malware in BING, Notice & Takedown, uKAsh politievirus verwijderen, Wachtwoord kwijt?, Identiteit uitfilteren, Facebookprofiel gekaapt, Beschadigde bestanden leesbaar maken, Steganografie, HOAX, Netneutraliteit

2013-06 > Wet Computercriminaliteit III, Darknet, NSA tapt servers, TOR adviseert privacycocktail, Virusinformatie, Alles over een bootsectorvirus, Klaar voor Ipv6, Marktplaatsoplichting vrijspraak, Zoek je eigen digitale sporen, Herstart gecrashte computer