Secure Computing

Nieuwsbrief Mei 2013

W.Bosgra taakaccenthouder digitale criminaliteit

In dit nummer:

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 !

Gratis VPN diensten:

Hamachi

CyberGhost

RiseUp

Betaalde diensten:

TorGuard

BT Guard

BlackVPN

VPN (Virtueel Particulier Netwerk)

Een VPN is een versleutelde verbinding met een beveiligd netwerk. In veel gevallen kun je via dat netwerk vervolgens het internet op. Het VPN (Virtual Private Network) waarmee je surft zal nog steeds zijn aan te wijzen, maar jouw persoonlijke apparaat is niet meer direct te herleiden. De keuzes voor de sites die je bezoekt zijn nog steeds te volgen en de sites waarop je inlogt weten nog steeds welke gebruiker inlogt. Daarom ben je nog steeds herkenbaar aan jouw surfgedrag. Een VPN is daarom niet 100% anoniem.

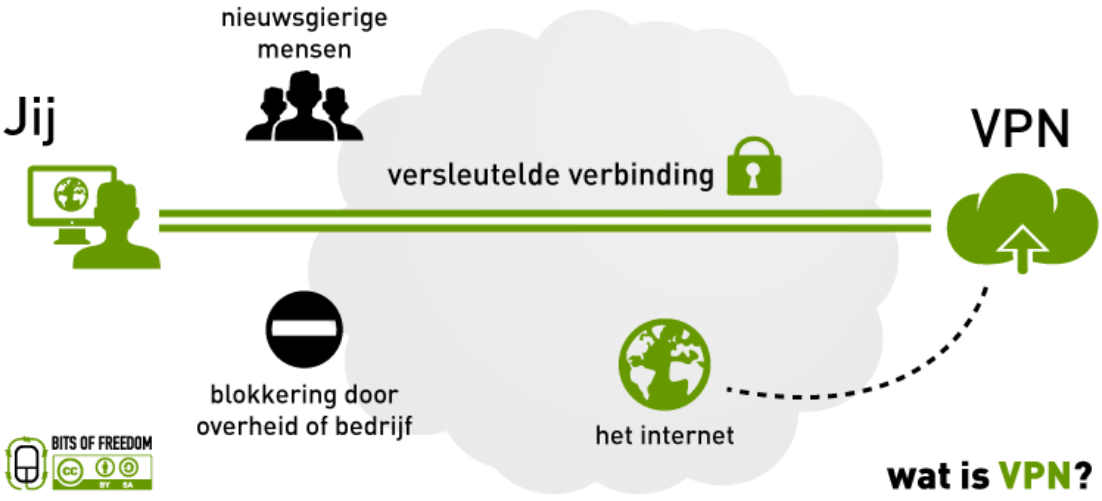
Toch biedt een VPN een ideale eerste barrière bij verbinding met een open WiFi in de trein of café, aangezien alles op jouw verbinding is versleuteld tot aan het VPN. Vanaf het VPN kun je met HTTPS de verbinding versleutelen tot aan de websites die je bezoekt.

Staat het VPN waarmee je verbinding maakt in een ander land, dan gebruik je ook het internet via dat land. Je hebt dan geen Nederlandse verbinding met het internet, maar bijvoorbeeld een Duitse of Zweedse. Je kunt via een VPN in Nederland geblokkeerde websites bereiken. Zo kun je al het BBC materiaal bekijken met een Brits VPN of je kunt diensten zoals Netflix of Hulu gebruiken via een Amerikaans VPN.

Studenten kunnen vaak gebruik maken van de VPN van hun universiteit. Veel werkgevers vragen werknemers ook om met een VPN te verbinden wanneer ze werkgerelateerde bestanden gebruiken. Let wel dat de VPN-verlener jouw verbinding kan nagaan.

Voor privé-gebruik van een VPN kun je een eigen VPN-server opzetten, een abonnement afsluiten of een gratis variant kiezen. Gratis varianten hebben als nadeel dat fabrikanten er iets voor terug willen hebben. Soms moet je advertenties accepteren, ze plaatsen cookies of geven je gebruik door als instanties daar om vragen.

"Het belangrijkste om te weten betreffende een VPN: het beveiligt jouw internetverbinding en garandeert dat alle data die je verstuurt en ontvangt is versleuteld en vrij is van spiedende ogen"



PGP (Pretty Good Privacy)

(Gratis encrypter)

BoxCryptor
(versleutelt automatisch bestanden in de cloud)

PGP-bedenker lanceert versleutelde e-maildienst

Het Amerikaanse bedrijf dat door PGP-bedenker Phil Zimmermann en twee Navy SEALS werd opgericht biedt nu ook een versleutelde e-maildienst aan. Silent Circle versleutelde al de telefoongesprekken en sms-berichten van klanten, maar daar is nu ook e-mail bijgekomen. Via een apart e-mailadres voor vertrouwelijke informatie kunnen gebruikers nu versleuteld e-mailen.

De e-maildienst vereist verder geen acties van de gebruiker. Het aanmaken en beheren van sleutels wordt automatisch door 'Silent Mail' gedaan, dat alle verstuurde berichten via PGP Universal versleutelt. Dit zou menselijke fouten moeten voorkomen. Toch is het ook mogelijk voor gebruikers om hun eigen PGP-sleutels en Secure/Multipurpose Internet Mail Extensions (S/MIME) certificaten te beheren.

E-mail is als een ansichtkaart die je op de bus doet. Iedereen die je kaart in handen krijgt, kan hem lezen. Jouw e-mail gaat langs vele schakels en verbindingen waardoor veel partijen jouw e-mail kunnen inzien.

Waarschijnlijk gebruik je Outlook of Gmail zodat zij jouw e-mail voor je opslaan. Daardoor geef je het feitelijke beheer van jouw elektronische post uit handen. Deze processen zijn vaak geautomatiseerd, maar dat is geen geruststelling. Tegenwoordig is het opslaan van informatie goedkoop en is het doorzoeken van die informatie makkelijk.

Zorg ervoor dat persoonlijke informatie privé blijft. Het is daarom verstandig jouw e-mail te versleutelen.

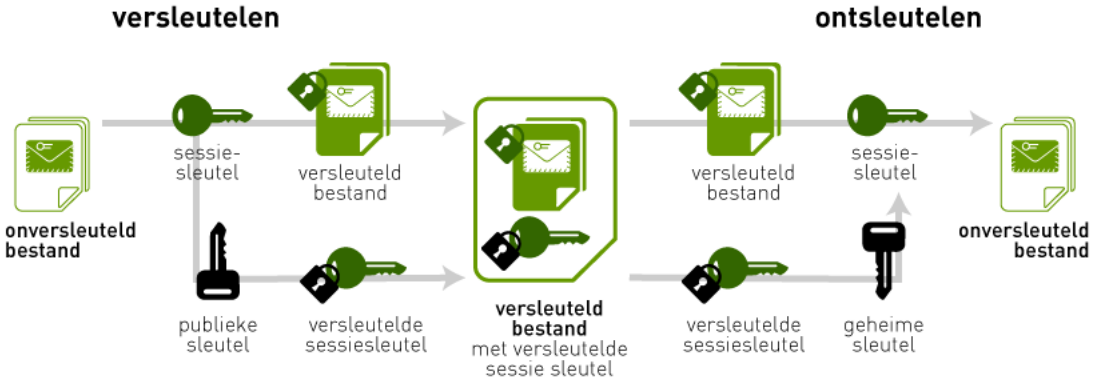
Een oplossing hiervoor is PGP (Pretty Good Privacy). Met deze software kun je e-mail digitaal ondertekenen en versleutelen. Jouw eigen computer versleutelt de berichten en alleen de ontvanger van het bericht kan het bericht ontsleutelen. De ontvanger moet ook PGP gebruiken om je bericht te kunnen lezen. Er is geen mogelijkheid voor een onderschepper om de inhoud van het gecodeerde bericht te ontcijferen.

Er zijn PGP-plugins voor Outlook, Thunderbird en Mail.

Om tekst te versleutelen heeft de ontvanger een publieke en geheime sleutel nodig. Dan maakt PGP een willekeurige eenmalige sessiesleutel aan. Met deze sessiesleutel wordt de tekst versleuteld. De sessiesleutel zelf wordt met de publieke sleutel van de ontvanger versleuteld, waarna beide delen verstuurd worden.

Ontsleutelen werkt precies andersom. De ontvanger gebruikt zijn of haar geheime sleutel om de versleutelde sessiesleutel te ontcijferen.
Daarna ontcijfert PGP met behulp van de sessiesleutel de ontvangen tekst. De geheime sleutel bewaar je zelf en de publieke sleutel geef je vrij.

"Zorg ervoor dat persoonlijke informatie privé blijft"



wat is PGP?

Bing bevat meer malwaresites dan Google

Hoewel de meeste zoekmachines maatregelen in huis hebben om hun gebruikers te beschermen tegen malware, gebeurt het toch regelmatig dat besmette websites bovenaan de zoekresultaten terecht komen.

Dat concludeert het Duitse AV-test, een onafhankelijk testlab dat zich normaliter bezig houdt met het beoordelen van de efficiëntie van antivirussoftware. De organisatie testte (PDF) over een periode van anderhalf jaar 40 miljoen websites in zeven verschillende zoekmachines en vond een bijzonder klein aantal besmette sites: 5.000 sites, ofwel 0,000125 procent van het totaal.

"Bing slordiger"

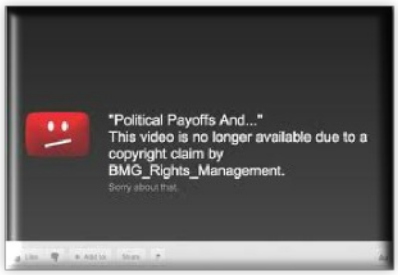
Bing slordiger
Google en Bing, die beiden werden getest met 10 miljoen websites, waren van alle zoekmachines het beste in verwijderen van malwaresites. Maar het moet toch worden opgemerkt dat er een flink verschil was tussen de twee. Bing miste 1.285 sites, terwijl dat bij Google maar 272 exemplaren waren.

AV-test waarschuwde daarnaast dat cybercriminelen steeds beter worden in het manipuleren van de zoekresultaten, waarbij ze Search Engine Optimisation (SEO) gebruiken om hun besmette lading bovenaan de lijst te krijgen. Gebruikers lijken meer vertrouwen te hebben in de hoogst geklasseerde resultaten, wat tot gevaarlijke situaties kan leiden.

Ondanks dit toenemende gevaar is de kans blijkbaar bijzonder klein dat je op een site klikt die een trojan naar je pc haalt. Zorg daarom dat je antivirussoftware de laatste definities bevat en controleer of je software de nieuwste versies draait.

Verschillende beveiligingsbedrijven hebben daarnaast diensten in huis om verdachte links te kunnen controleren, zoals AVG Linkscanner, Norton Safe Web of McAfee SiteAdvisor.

Notice and Takedown



De gedragscode Notice and Takedown

De gedragscode is vrijwillig en beschrijft hoe particulieren en bedrijven in de online sector omgaan met klachten over onrechtmatige inhoud op internet, zoals kinderporno, plagiaat, discriminatie en aanbod van illegale goederen.

ISP's en webhosters zijn bijvoorbeeld aansprakelijk voor de informatie die ze hun klanten aanbieden, wanneer zij deze informatie na een terechte klacht niet weghalen.

Daarnaast biedt de gedragscode meer duidelijkheid bij het bepalen of een klacht terecht is en welke stappen bij afhandeling gevolgd dienen te worden.

Wat is Notice-and-Take-Down?

Online-dienstverleners, zoals internet service providers, ontvangen regelmatig verzoeken om bepaalde informatie die op een website staat, die zij beheren, te verwijderen. Dat kan gaan om criminele phishingsites of kinderporno, maar ook om bijvoorbeeld misbruik van logo's of discriminatie. In het verleden was vaak onduidelijk hoe zij konden optreden tegen deze informatie op het internet. De Gedragscode Notice-and-Take-Down is in het leven geroepen om de onlinedienstverleners duidelijkheid te geven hoe ze kunnen optreden als zij zo'n verzoek binnen krijgen.

Notice-and-Take-Down is een procedure die start op het moment dat iemand een melding doet over vermeende onrechtmatige en/of strafbare inhoud op internet bij een service provider. Dat is de "Notice". De procedure kán eindigen met het uit de lucht halen van de betreffende website, de zogenoemde "Take Down". Het doel van de NTD-code is om te zorgen dat een melding altijd afgehandeld wordt. Dit betekent dus niet dat de inhoud altijd verwijderd moet worden. Het kan immers zijn dat er melding wordt gemaakt van een site die uiteindelijk niet in strijd met de wet blijkt te zijn.

Hoe weet ik welke bedrijven de code onderschrijven?

"De code is alleen van toepassing op het Nederlandse deel van het Internet"

De code is alleen van toepassing op het Nederlandse deel van het internet. Bedrijven die ermee werken, maken dit kenbaar op hun eigen website. Op de website van de werkgroep Notice and Takedown kunt u een lijst vinden van de onderschrijvers van de Code.

Voor wie is de NTD-gedragscode bedoeld?

De Code wordt gehanteerd door tussenpersonen die in Nederland een openbare (telecommunicatie) dienst op Internet leveren. Wil van een openbare dienst sprake zijn dan dient deze voor iedereen beschikbaar te zijn. Ook is er sprake van een openbare communicatiedienst als die toegankelijk is voor leden van een bepaalde groep als (vrijwel) iedereen lid kan worden van die groep.

Bij tussenpersonen kunt u bijvoorbeeld denken aan hostingbedrijven of Internet Service Providers (ISP's). Websites waarvoor de code bedoeld is, zijn bijvoorbeeld discussiefora en sites met ruimte voor (links naar) (zelfgemaakte) filmpjes of muziek.

Kan iedereen een Notice and Takedown verzoek uitbrengen?

Tussenpersonen hebben een eigen, openbaar toegankelijke Notice-and-Take-Down procedure in overeenstemming met deze code. Deze procedure beschrijft hoe de tussenpersonen omgaan met meldingen van strafbare of onrechtmatige inhoud op Internet. Er zijn tussenpersonen die voor bepaalde meldingen een duidelijke link tussen melder en de gemelde content vereisen (bijvoorbeeld bij schending van auteursrechten).

Bij wie moet ik een Notice and Takedown verzoek uitbrengen als ik onrechtmatige of strafbare informatie op internet ontdek?

Bij voorkeur bij degene die de informatie geplaatst heeft. Maar dat is niet altijd wenselijk of mogelijk. In dat geval stelt de code dat u moet opschalen naar de organisatie die het dichtste bij de bron zit. Dat kan bijvoorbeeld de beheerder van een webforum zijn, of als die onbekend is de eigenaar van de website. Als ook die niet bekend is, wordt er gekeken naar degene die de website host. Dus hoe dichter u bij de bron bent, hoe beter. Per situatie moet bekeken worden wie de eerstvolgende partner is in de hele keten.

Wanneer kan een verzoek tot Notice and Takedown worden ingediend?

Een concreet verzoek kunt u doen indien u informatie tegenkomt waarvan u denkt dat deze onrechtmatig en/of strafbaar is. Let wel, het gaat daarbij om een vermoeden. U hoeft dus niet 100% zeker te weten of de informatie ook daadwerkelijk onrechtmatig en/of strafbaar is. Wel zult u moeten aangeven waarom u van mening bent dat de informatie onrechtmatig en/of strafbaar is.

Enkele voorbeelden van verschillende soorten informatie die strafbaarheid en/of onrechtmatigheid kunnen opleveren zijn:

- Inbreuken op auteurs en/of merkenrecht
- Verspreiden van kinderporno
- Haatzaaiende en racistische uitlatingen
- Smaad en lasterlijke teksten
- Cyberstalking
- Publicatie van andermans persoonsgegevens

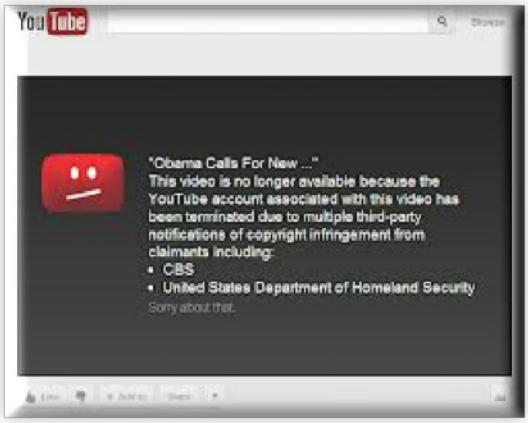
Hoe kan een verzoek tot Notice and Takedown worden ingediend?

Partijen die de Code onderschrijven, melden dit op hun website. Zij geven daarbij ook aan hoe u bij hen een verzoek kunt indienen. Kijk daarom op de website van de partij bij wie u een dergelijk verzoek wilt indienen.

Wat moet er allemaal in zo'n verzoek tot Notice and Takedown worden vermeld?

De onderschrijvers van de code geven op de eigen website aan hoe u een dergelijk verzoek kunt indienen. U dient in ieder geval de volgende informatie te verstrekken:

- uw contactgegevens,
- de gegevens die de tussenpersoon nodig heeft om de inhoud te kunnen beoordelen waaronder ten minste de locatie (URL),
- een beschrijving waarom de inhoud volgens u onrechtmatig of strafbaar is of waarom deze volgens u strijdig is met door de tussenpersoon gepubliceerde criteria ten aanzien van onrechtmatige of strafbare inhoud en
- een motivering waarom deze tussenpersoon wordt benaderd als meest geschikt om op te treden.



Hoe weet u nu zeker of een website onrechtmatige of strafbare informatie bevat?

Uiteindelijk weet u dat pas zeker als de rechter zich heeft uitgesproken.. Een tussenpersoon zal elke melding eerst zelf beoordelen om te zien of er sprake is van een onmiskenbare onrechtmatigheid of strafbaarheid.

Onderschijvers van de NTD code

De NTD-gedragscode is van belang voor Internetgebruikers, overheid, bedrijfsleven en belangenorganisaties.
Initiatiefnemers:

- *KPN - (inclusief dochterondernemingen als XS4ALL)*
- *SIDN (Stichting Internet Domeinregistratie Nederland)*
- *DHPA (Dutch Hosting Provider Association)*
- *Vereniging ISPConnect Nederland*
- *NLkabel (vereniging van kabelbedrijven met als leden onder meer UPC, Ziggo, CAIW en Zeelandnet)*

Wat is een redelijke termijn voor de afhandeling van een verzoek?

De redelijke termijn voor het maken van een beoordeling en het afhandelen van een verzoek hangt af van verschillende factoren: de daadwerkelijke onmiskenbaarheid van onrechtmatige of strafbare inhoud, de ernst en maatschappelijke onrust, de aard en omvang van de schade, de betrouwbaarheid van de bron etc.
In geval van onmiskenbare onrechtmatigheid of strafbaarheid kan de afhandeling binnen enkele dagen plaatsvinden, in de overige gevallen zal het langer duren, waarbij bijvoorbeeld 5 werkdagen een redelijke termijn is.
Uiteindelijk is het echter aan de individuele inhoudsaanbieder om hiervan een inschatting te maken en te bepalen welke termijn(en) hij hanteert. De inhoudsaanbieder maakt deze termijn(en) in zijn NTD-procedure bekend.

Wat is 'ongewenste' inhoud?

Tussenpersonen kunnen criteria opstellen van inhoud die zij ongewenst vinden en waarvan zij niet willen faciliteren dat die inhoud via hen op Internet beschikbaar is. Feit is wel dat onrechtmatige en strafbare inhoud door de wet is bepaald. Ongewenste inhoud daarentegen, wordt bepaald door de tussenpersoon. Een melding over ongewenste inhoud wordt door de tussenpersoon beoordeeld aan de hand van diens opgestelde criteria.

Wat gebeurt er nadat een verzoek is ingediend?

Nadat een verzoek is ingediend zal de tussenpersoon beoordelen of er sprake is van onmiskenbaar onrechtmatige en/of strafbare inhoud. De tussenpersoon zal u op de hoogte stellen van het oordeel en het eventuele vervolg dat daaraan gegeven wordt.

Wat gebeurt er als een verzoek wordt goedgekeurd?

Indien de tussenpersoon oordeelt dat sprake is van onmiskenbaar onrechtmatige en/of strafbare inhoud dan zorgt deze er voor dat de betreffende inhoud onmiddellijk verwijderd wordt.

Naast de initiatiefnemers zijn de volgende organisaties betrokken geweest bij de totstandkoming van de gedragscode en vinden dit een goede ontwikkeling:

- Marktplaats/Ebay
- Google.nl
- Stichting BREIN
- Meldpunt Kinderporno
- Meldpunt Cybercrime
- Meldpunt Discriminatie Internet
- Algemene Inspectiedienst (dienstonderdeel Opsporing)
- Inspectie voor de Gezondheidszorg
- Belastingsdienst
- Nationaal Coördinator Terrorismebestrijding (NCTb)
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Ministerie van Economische Zaken
- Ministerie van Justitie
- Leaseweb
- SNB-React

Verwijder uKash politievirus van een computer: een upgrade.

Iedereen is inmiddels wel bekend met het zogenaamde Politievirus. Uw PC wordt gekaapt en gemeld wordt dat u tegen betaling van 100€ uw PC weer tot uw beschikking komt.
Op moment van schrijven van dit artikel overkwam het een goede vriend van mij. Met de volgende tips heb ik hem kunnen helpen. Mocht het u of een van uw naasten overkomen, gebruik dan de volgende tips:

OPLOSSING 1 OM U COMPUTER VRIJ TE MAKEN VAN HET POLITIE VIRUS MET WINDOWS HERSTELPUNT VIA OPDRACHTPROMPT
DEZE INSTRUCTIE WERKT OVER HET ALGEMEEN VOOR ALLE VARIANTEN

Oplossing om terug in Windows te geraken:

1. Start u geïnfecteerde computer opnieuw op
2. Klik tijdens het opstarten nog voor het windows scherm op F8 en start Windows in veilige modus met opdrachtpromp (wat is veilig modus?)
3. Als de opdracht-prompt geopend is type: rstrui.exe
4. Er opent een nieuw venster om u computer terug te zetten in een tijd waarin u het politievirus nog niet had. Selecteer deze en kies voor doorgaan.
5. Volg instructies, u computer gaat zich nu herstellen en u bent verlost van het politievirus.

OPLOSSING 2OM U COMPUTER VRIJ TE MAKEN VAN HET POLITIE VIRUS MET WINDOWS HERSTELPUNT

Oplossing om terug in Windows te geraken:

1. Start u computer opnieuw op
2. Klik tijdens het opstarten nog voor het windows scherm op F8 in veilige modus (wat is veilig modus?)
3. Klik aan veilig modus met netwerkondersteuning
4. Voer systeemherstel uit en plaats u computer terug in een tijdsbestek waarin u nog niet last had van het virus. (hoe voer ik systeemherstel uit ?)

OPLOSSING 3 (WINDOWS OFFLINE DEFENDER OPSTART-CD/DVD)

1. Download Windows Offline Defender en maak een startup cd/dvd of usb stick. (zie hier hoe je een startup disk maakt en meer..)
2. Start daarna de pc op met de Windows Offline Defender disk
3. Scan u computer op malware met de Windows Offline Defender software.
4. Scan daarna u computer met MalwareBytes AntiMalware om het politie virus te verwijderen of te detecteren.
5. Scan nogmaals met ComboFix! om deze malware nog dieper te detecteren en te verwijderen. (instructies vind u hier)

OPLOSSING 4 (HITMAN PRO KICKSTART - USB STICK)

Het enige wat u hoeft te doen is uw gegijzelde computer op te starten met behulp van de HitmanPro.Kickstart USB-stick. De programma's op de stick zorgen ervoor dat uw gegijzelde Windows opstart en starten dan automatisch HitmanPro zodat u malware en ransomware kunt verwijderen. Alle noodzakelijke stuurprogramma's (drivers) voor uw systeem en alle draadloze netwerk wachtwoorden (wie herinnert zich deze nog?) zijn beschikbaar. Het is niet nodig om kennis te hebben van programma's van andere besturingssystemen, bijvoorbeeld Linux.

HitmanPro.Kickstart omzeilt het gijzelvirus en leidt de gebruiker door het verwijderingsproces.
Het is zo eenvoudig dat iedereen HitmanPro.Kickstart kan gebruiken. In slechts een paar minuten is je computer weer vrij van het gijzelvirus.

Opmerking: Een actief gegijzelde Windows-omgeving bevat tal van forensische informatie zoals welke processen zijn gestart en welke processen beeldvullend actief zijn (waardoor het bureaublad ontoegankelijk wordt). Deze feiten geven HitmanPro een duidelijke aanwijzing welke bestanden en registersleutels bij het gijzelvirus horen. Een duidelijk voordeel ten opzichte van rescue-cd's welke een afzonderlijke omgeving starten en afhankelijk zijn van virushandtekeningen.

Hitman PRO Kickstart USB Stick aanmaken

De volgende video toont hoe eenvoudig het is om een USB-stick te veranderen in een HitmanPro.Kickstart USB-stick waarmee politievirussen kunnen worden verwijderd:

http://www.youtube.com/watch?feature=player_embedded&v=bz8F6-_Oebo

Het Politievirus verwijderen middels de Hitman Pro Kickstart USB Stick

Kickstart
Gebruikshandleiding
In PDF formaat

Als u een HitmanPro.Kickstart USB-stick heeft aangemaakt, kunt u deze gebruiken om een gegijzelde computer te ontgrendelen. Voordat u hiermee begint moet u de gegijzelde computer eerst uit zetten.
Stop de HitmanPro.Kickstart USB-stick in een vrije USB poort van de gegijzelde computer en zet deze daarna aan. Zodra de computer opstart gaat u naar het bootmenu van uw BIOS waar u de USB-stick selecteert waarop HitmanPro.Kickstart staat. Druk dan op 'Enter' om de computer op te starten van deze stick.

Het is ook nog steeds mogelijk het virus te verwijderen middels een zogenaamde Rescuedisk. Meerdere antivirusbedrijven voorzien in een dergelijke disk, waaronder de firma Kaspersky.

U kunt de image van een dergelijke disk downloaden van hun website.

Let op: om in het bootmenu van uw BIOS te komen moet u de toets F8, F11 of F12 indrukken, dit is afhankelijk van welk type BIOS u heeft.

Deze video toont hoe het gijzelvirus verwijdert wordt middels de Kickstart USBstick:

http://www.youtube.com/watch?feature=player_embedded&v=OFmKutHJmG0

Hoe is het mogelijk dat dit virus op mijn pc terecht is gekomen ?

Op dit moment word er veelvuldig misbruik gemaakt van een grote bug in internet explorer en java. Deze tweetal bugs worden door cybercriminelen misbruikt om via een website of link malware te installeren op u computer. Als u computer niet helemaal up-to-date is met de laatste windows en java patches dan is het mogelijk dat u op deze manier besmet bent geraakt. Het is ook algemeen bekend dat u niet moet klikken op links die u niet vertrouwd en bijvoorbeeld toeverzonden krijgt per mail.
Om u computer te checken op de laatste patches van windows kijkt u op www.windowsupdate.com en voor java raden wij u aan de laatste java update te installeren. Heeft u nog geen virusscanner, download dan een gratis virusscanner om de kans te verkleinen dat u besmet raakt met een nieuwe variant van dit of een ander virus.

Help andere mensen, dit virus verspreid zich snel!

Als deze oplossingen u hebben geholpen, help dan ook andere mensen. Dit kunt u doen door onze link te delen op andere internet sites te twitteren, of te delen op facebook. Steeds meer mensen raken besmet met virus, en het is relatief makkelijk te verwijderen. Helaas verdienen cybercriminelen ontzettend veel geld met deze ransomware. Teveel mensen betalen ervoor om hun computer vrij te krijgen van deze ransomware, helaas word het virus dan niet verwijderd maar simpelweg uitgeschakeld. Na een maand of wat krijgt u weer een melding en word verzocht weer te betalen. Laat u niet foppen en betaal nooit voor de ransomware, en help andere mensen.

HitmanPro.Kickstart

Wachtwoord kwijt?

Windows wachtwoord achterhalen met Ophcrack
Ophcrack
Ophcrack is een Open Source programma voor het kraken van Windows gebruikersaccounts. Hiermee kun je in de meeste gevallen een vergeten Windows XP, Vista of Windows 7 wachtwoord terugvinden. Je kan ook een administrator wachtwoord terughalen. Ophcrack is een paardenmiddel: gebruik dit alleen als er geen wachtwoordhersteldiskette is, en niemand meer kan inloggen op een PC. Als een andere gebruiker nog wel toegang heeft kan deze een nieuw wachtwoord aanmaken.
Platform: Windows, Linux/Unix, Mac OS X.
Nederlands: Nee.
Gratis: Ja.

Vergeten wachtwoord van Outlook achterhalen
Protected Storage PassView
Klein programma dat een wachtwoord kan achterhalen uit Windows, bijvoorbeeld de wachtwoorden van websites (als je die laat onthouden door Internet Explorer). Ook het wachtwoord van een e-mail account in Outlook en Outlook Express is terug te vinden.
Platform: Windows 95, 98, ME, 2000, XP, Vista met Internet Explorer.
Nederlands: Nee.
Gratis: Ja.

Vergeten wachtwoord van e-mail achterhalen
MailPass
Dit programma haalt wachtwoorden terug - en de andere gegevens - van e-mail accounts in o.a Outlook Express, Outlook, Thunderbird, Windows Mail, Outlook.com en IncrediMail. In sommige gevallen werkt het ook voor Gmail en Yahoo Mail accounts.
Platform: Windows (alle versies).
Nederlands: Ja (apart taalpakket).
Gratis: Ja.

Wachtwoord zichtbaar maken achter asterisks
Asterisk Key
Eenvoudig programma dat een afgeschermd wachtwoord zichtbaar maakt. Dit kan gebruikt worden als het wachtwoord onleesbaar is gemaakt door sterretjes: * * * *. Bijvoorbeeld bij FTP-programma's, mail-programma's, netwerkverbindingen of websites.
Platform: Windows 2000, NT, XP, 2003, Vista, Windows 7, Windows 8.
Nederlands: Nee.
Gratis: Ja.

Wachtwoorden uit Firefox halen
PasswordFox
Klein programma dat de wachtwoorden zichtbaar maakt van websites die zijn opgeslagen in Firefox.
Platform: Windows (alle versies).
Nederlands: Nee.
Gratis: Ja.

Vergeten wachtwoord van Word en Excel achterhalen
Free Word Excel Password Wizard
Om wachtwoorden terug te vinden van Word en Excel documenten. Dit programma slaagt alleen als een wachtwoord niet te lang is.
Platform: Windows (alle versies) met .NET framework geinstalleerd.
Nederlands: Nee.
Gratis: Ja.

Politiesoftware filtert slim identiteiten uit digibewijs

Forensische uitleesprogramma Tracks Inspector filtert identiteiten uit digitaal bewijsmateriaal. De steeds slimmere tool krijgt inmiddels internationale aandacht.

Het forensische uitleesprogramma, dat agenten zonder technische specialisme moet helpen door bij het onderzoeken van grote hoeveelheden digitaal bewijsmateriaal, spitst zich verder toe op het filteren van identiteiten. Daarbij wordt de wetenschappelijke benadering van Kunstmatige Intelligentie gebruikt.

Hiermee worden uit verschillende digitale opslagapparaten identiteiten aan elkaar gekoppeld en wordt via een aparte database gekeken welke verschillende bronnen zijn te koppelen. De resultaten worden in een los dashboard getoond en moet de agenten verder op weg helpen.

Ontwikkeling in volle gang

De ontwikkeling van uitleesprogramma Tracks Inspector is nog in volle gang. Politieagenten die al sinds juni 2012 met de software werken, zijn laaiend enthousiast. Met name de tijdswinst bij het onderzoeken van de groeiende hoeveelheid digitaal bewijsmateriaal is van groot belang.

Bovendien kunnen agenten zonder technische achtergrond werken met de software. De rechercheur in kwestie kan in een webbrowser op een PC of tablet de video's, foto's, e-mail, internetgeschiedenis en andere zaken in het bewijsstuk doorzoeken.

Identiteitsextractie

Het tweede speerpunt is de identiteitsextractie. Dit standaard onderdeel is van groot belang voor Tracks Inspector en wordt sinds eind 2011 door Fox-IT in samenwerking met universiteit Twente ontwikkeld. Professor Data Management Technology Maurice van Keulen heeft dit onderdeel van Tracks Inspector in samenwerking met student Jop Hofste – inmiddels afgestudeerd en in dienst bij Fox-IT – geprogrammeerd en wil dit verder uitbouwen.

Met behulp van Kunstmatige Intelligentie wordt het digitale bewijs wetenschappelijk benaderd. Van Keulen: "De bedoeling is dat we steeds meer informatie kunnen analyseren. Daarmee kan Tracks Inspector een krachtiger instrument worden voor een inspecteur. Zo kan informatie over met wie iemand in contact is geweest en op welk locatie iemand is geweest slim worden onderzocht. Daarbij is het belangrijk dat het programma weet welke twee namen op dezelfde persoon slaan."

"Politiemensen zijn laaiend enthousiast"

Nieuwe malware kaapt je Facebook-profiel

Een nieuw virus dat zich vermomt als een browserextensie voor Chrome en Firefox heeft het gemunt op nietsvermoedende Facebook-gebruikers.

Microsoft waarschuwt voor nieuwe malware die het heeft gemunt op je Facebook-account. Het virus vermomt zich als een Chrome-extensie of Firefox-addon.

Meer bepaald gaat het om Trojan:JS/Febipos.A. Dat trojaans paard nestelt zich in je browser en gedraagt zich als een legitieme browserextensie.

De malware houdt in de gaten of je computer is ingelogd op een Facebook-account en probeert een bestand met een lijst commando's voor de extensie te downloaden.

Met die commando's kan het vervolgens een hoop acties op Facebook uitvoeren, zoals het liken van een pagina, delen of posten van berichten, aansluiten bij Facebook-groepen en chatten met vrienden van de eigenaar van het account.

Het virus werd ontdekt in Brazilië en lijkt zich in de eerste plaats op Braziliaanse Chrome- en Firefox-gebruikers te richten. Maar volgens Microsoft kan de malware makkelijk worden aangepast om ook gebruikers uit andere landen te treffen.

Wis de sporen uit van je usb-stick

Telkens je een usb-opslagapparaat aan je pc koppelt, slaat Windows automatisch bepaalde informatie op in het register, waaronder de fabrikant van het apparaat, de datum waarop het apparaat de laatste keer werd ingeplugd, enz. Met USB Oblivion haal je die informatie in één keer weg.

Misschien wil je om privacyredenen de sporen van eerder aangesloten usb-apparaten (sticks, externe schijven, iPods, …) verwijderen, maar het kan ook wel gebeuren dat bepaalde registeringangen corrupt zijn geworden waardoor Windows je usb-apparaat niet meer correct herkent.
USB Oblivion (oblivion betekent 'vergetelheid') haalt de spons over al deze registerinformatie.

Standaard voert het tooltje alleen een simulatie uit, waarbij je dan het resultaat van de schoonmaakoperatie te zien krijgt. Als je die operatie effectief wil uitvoeren, start je nogmaals USB Oblivion op, maar deze keer met de optie Do real clean. Merk op dat standaard ook een back-up van het register wordt gemaakt, zodat je desnoods de toestand nog kan terugdraaien. Heb je dat liever niet, verwijder dan eerst het vinkje bij Save backup .reg-file.

Houd er rekening mee dat USB Oblivion zich alleen richt op usb opslagapparaten en dus een eventuele usb-muis en –toetsenbord of een usb wifi-adapter ongemoeid laat. Het programma bestaat zowel in een 32-bits als in 64-bits versie.

‘Social media kunnen politiewerk frustreren’

Na Boston en Leiden biedt de zoektocht naar de vermiste Ruben en Julian de zoveelste kans om de rol van sociale media te duiden. Zeker in relatie tot politiewerk. Twitter en facebook kunnen veel goeds betekenen, maar ook voor flink wat frustratie zorgen.
Volgens criminoloog Henk Ferwerda van Bureau Beke kunnen al die extra ogen en oren ook vervelende gevolgen hebben. ‘Laat de politie de regie voeren’, stelt Ferwerda die niet alleen wijst op het risico van sporen uitwissen. De politie kan prima zelf zoeken en heeft soms ‘hele goede redenen’ om een bepaald gebied juist niet uit te kammen.

“Laat politie de regie voeren!”

Zoals bekend heeft burgerparticipatie bij politieonderzoeken met twitter en facebook een hoge vlucht genomen. ‘Ook voordat die media bestonden, maakte de politie al gebruik van de burger’, zegt Ferwerda. Hij geeft toe dat de relatie tussen politie en burgers is veranderd. ‘Sociale media stellen burgers in staat zelf hun rol in te vullen maar dat kan verkeerd uitpakken. Een burger mag niet op de stoel van een rechter gaan zitten.’
Misdaadverslaggever Gerlof Leistra van Elsevier wijst op andere risico’s. ‘
Neem bijvoorbeeld ontvoeringszaken. Als mensen dan op eigen houtje gaan handelen, kunnen ze het leven van mensen in gevaar brengen’. Leistra vindt dat de politie op die sociale media meer moet doen om burgers duidelijk te maken dat ze niet op eigen houtje moeten gaan opsporen. ‘Als je op sociale media uitlegt waarom mensen niet zelf een bos moeten uitkammen, kan je een heleboel duidelijkheid aan een heleboel mensen scheppen en een heleboel problemen voorkomen.’

‘Winkelier zit fout met foto dief op internet’

Particulieren mogen niet zomaar een foto van een vermeende winkeldief online zetten, zegt een woordvoerster van het College Bescherming Persoonsgegevens (CBP).
Ook al zag de winkelier met eigen ogen hoe twee jongens er met de kassa vandoor gingen, ook al heeft die winkelier een dag voor niks gewerkt, ook al klinkt het nog zo onrechtvaardig.

Toen Hilde Smits van de dierenspeciaalzaak in Best overvallen werd, zette ze beelden van de winkeldieven op haar facebookpagina. Inclusief oproep aan andere winkeliers om de mannen ‘buiten te schoppen’.
Volgens het CBP mag dat dus niet, en al helemaal niet als het wetsvoorstel van staatssecretaris Fred Teeven aangenomen wordt. Teeven wil de regels zelfs nog aanscherpen om juist te voorkomen dat particulieren foto’s en filmpjes online gaan publiceren. ‘Dat blijft het primaat van politie en justitie.’

Boete voor dreigtweet aan agenten

De officier van justitie heeft een man (29, uit Zoetermeer) een boete van 300 euro opgelegd omdat hij via twitter politieagenten had bedreigd.

De man dreigde agenten neer te schieten. De tweet werd snel ontdekt en bijna net zo snel werd de verdachte aangehouden.

Onderzoek op zijn telefoon leverde op dat hij de tweet had verstuurd.

Krrr-krrr. Niet meteen een geluid dat je van je schijf gewoon bent, en al helemaal verontrustend is dat je favoriete programma's sommige bestanden weigeren te openen. Leesfouten dus! Wat je nodig hebt, is een Koppige Kopieerder, een van het kaliber van Unstoppable Copier.

Beschadigde bestanden weer leesbaar maken

STAP 1 / Downloaden & installeren

Het kan gebeuren dat de tand des tijds of een minder zachtaardige aanpak (het schijfoppervlak van) je dvd's of harde schijf aantast, met krassen en slechte sectoren als gevolg. De meeste programma's gooien de handdoek in de ring zodra ze bij het inlezen van zo'n bestand op een onleesbare bit botsen. Niet zo met Roadkil Unstoppable Copier, dat precies gemaakt werd om dergelijke klussen te klaren! De magie van deze tool? Koppig volhouden, alle leesbare bytes alsnog aan elkaar rijgen en samen met jou hopen op het beste. Je vindt de tool op www.roadkil.net/program.php/P29/Unstoppable%20Copier. Kies het juiste besturingssysteem (een Windows- of Linux-versie) en geef aan of je een installeerbare dan wel een standalone (lees: 'draagbare') variant verkiest.

STAP 2 / Kopie starten

Je start de tool bij voorkeur op als administrator. Klik met de rechtermuisknop op de snelkoppeling, kies Als administrator uitvoeren en bevestig met Ja. Het hoofdvenster van Unstoppable Copier verschijnt, hopelijk ook bij jou in het Nederlands. Toch niet? Ga dan naar het tabblad Settings en kies Nederlands. Straks keer ik hier nog even naar terug, maar we beginnen bij het eerste tabblad: Kopiëren. Daar merk je onder meer de velden Bron en Doel op. De bedoeling is duidelijk: in het eerste veld verwijs je via de knop Verkennen naar de juiste locatie (map) op het nukkige medium, in het tweede veld geef je aan waar de kopie terecht hoort te komen. Met de knop Kopiëren zet je de operatie in gang.

STAP 3 / Kopiëren

Tijdens het kopiëren zie je welke bestanden er op elk moment overgezet worden, en hoe het met de data-integriteit van die bestanden gesteld is. Interessant is ook de kolom Status. Die vertelt je hoeveel procent van de originele bestandsgegevens er al gekopieerd is en hoeveel fouten er tijdens dat proces zijn opgetreden. Onderaan kan je aangeven welke soort bestanden je opgelijst wil zien: Gekopieerde bestanden, Overgeslagen bestanden (tijdens het kopiëren hoef je hiervoor maar op de knop Overslaan te drukken) en/of Beschadigde bestanden. In het onderste paneel krijg je nog allerlei bijkomende informatie, zoals het aantal gekopieerde (goede of beschadigde) bytes, het aantal leesfouten en de overdrachtsnelheid. Bekijk zeker de lijst met beschadigde bestanden van nabij: het zijn met name die bestanden die je in de kopie grondig zal moeten testen.

STAP 4 / Optimaal instellen

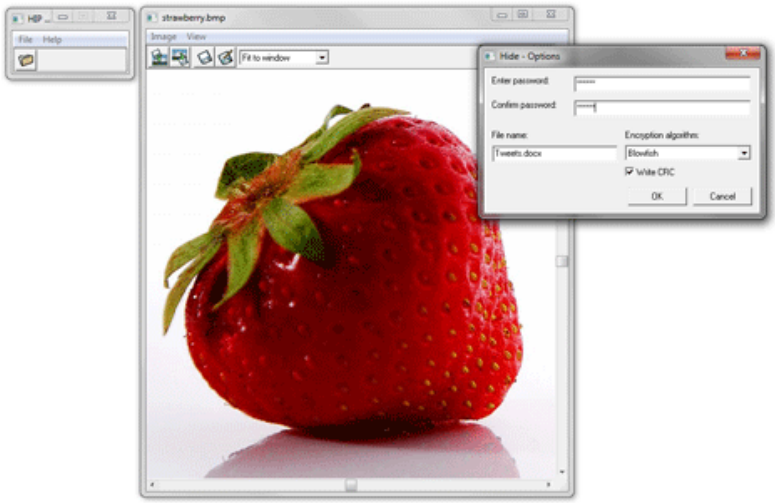
Je kan voor een groot stuk zelf bepalen hoe Unstoppable Copier omspringt met het inlezen en kopiëren. Je raadt het al: daarvoor klop je aan bij het tabblad Instellingen. Een vinkje plaatsen bij Automatisch beschadigde bestanden overslaan is niet meteen aangewezen – toch niet als je juist uit bent op dataherstel! Voor het grondigste recuperatieproces laat je ook het vinkje achterwege bij Stel maximaal aantal keer opnieuw proberen in en plaats je de schuifknop helemaal naar links, bij Beste gegevensherstel. Hou er wel rekening mee dat het inlezen van beschadigde bestanden met deze instellingen erg tijdrovend kan zijn – een klus voor de nachtelijke uurtjes? Verder tref je hier onder meer nog opties aan om bestaande bestanden in de doelmap al dan niet te laten overschrijven, de pc na het kopiëren uit te schakelen, alleen nieuwere bestanden te kopiëren en eventueel ook onderliggende mappen mee te kopiëren.

Tijdens de Tweede Wereldoorlog werden geheime boodschappen in onzichtbare inkt op de rug van boodschappers geschreven, of in morse op een draad getekend. Van die draad werd vervolgens een sjaal gebreid om de verzetsstrijder lekker warm te houden. Hetzelfde principe kan je ook op digitale boodschappen toepassen.

Criminelen mailen niet meer; ze sturen elkaar een foto

Tekst verbergen in een foto = Steganografie

Het leuke aan steganografie is dat het niet opvalt dat er een geheime boodschap staat. Stop je die boodschap in een doodnormaal beeld, pakweg een kat met een hoedje op of iemand die plat op zijn gezicht valt, dan moet Big Brother al bijzonder grondig filteren om je verdachte bestand te vinden.



Hide in Picture is een gratis steganografieprogrammaatje voor Windows. Het werkt alleen met bitmaps, maar je kan er wel hele bestanden mee verbergen, en niet alleen een beetje tekst. Wil je echt helemaal veilig zijn, dan kan je die verdachte foto's bijvoorbeeld ook nog eens in een versleuteld zip-bestand steken, voordat je ze in de bitmap verbergt.

Laad een beeldje in HIP en klik vervolgens op de linkse knop om een bestand te kiezen. Geef het eventueel een wachtwoord mee en kies het encryptiealgoritme. Bewaar je nieuwe bestandje met de derde knop van links en stuur het door. Ook je contactpersoon zal HIP in huis moeten halen om de geheime boodschap uit je beeld te halen.

Wat is een « hoax » ?

Met de toename van het aantal internauten die een elektronische postbus bezitten, hebben een paar 'slimmeriken' een nieuwe pest via het elektronisch berichtenverkeer uitgevonden: de "hoax".
Het VANDALE woordenboek verklaart HOAX als een e-mailbericht met een onterechte viruswaarschuwing.
"Hoax" is een Engels woord dat grap betekent. Een "hoax" is dus verkeerde, vervallen of oncontroleerbare informatie, die spontaan door Internauten wordt verspreid. De "hoax" kunnen de meest gevarieerde vormen aannemen en verband houden met alle onderwerpen die een positieve of negatieve emotie bij de Internaut kunnen opwekken. Te weten: valse virusalarmen, valse beloften, valse winsten –om het even welke-, valse solidariteitsketens, etc. Etc.

Wie heeft nog nooit zo'n bericht ontvangen van een vriend, een familielid of van een collega?
Het principe is heel eenvoudig: de ontwerper van de "hoax" stuurt die naar enkele personen. Die personen gaan op hun beurt het bericht naar hun contacten sturen enz. Als iemand een "hoax" ontwerpt en die naar 10 contacten stuurt en die 10 contacten allen de hoax naar 10 contactpersonen sturen, dan zijn er in 2 stappen al 110 personen 'besmet'.
Dit laatste gegeven toont duidelijk de belasting voor het internet door hoax… en dat uiteindelijk voor niets.
Bovendien heeft dat soort van berichten de hardnekkige eigenschap te blijven voortbestaan. Na meerdere keren de wereld rond te zijn gegaan, kunnen ze na jaren plots weer opduiken.

Hoe te weten of het om een « hoax » gaat?

De meeste berichten met een aangrijpende, revolterende of alarmerende inhoud die spontaan op het internet circuleren, zijn hoax. Men moet dus in geen geval dergelijke berichten gaan doorsturen omdat de inhoud "waar zou kunnen zijn", maar ze wel met de nodige alertheid benaderen; twijfel speelt immers altijd in de kaart van de geruchten en de grappen.

De meeste hoax zijn goed opgestelde berichten die sterke argumenten bevatten waardoor de waarheid ervan voor zich spreekt. Men moet dus niet stilstaan bij waarachtige elementen in het bericht, maar kijken naar twijfelachtige elementen of elementen waarvoor geen enkel bewijs naar voren wordt gebracht. Hoax vermengen immers handig de waarheid en de leugen.

"Verstuur dit bericht naar al uw contactpersonen"

In elke situatie, het bericht:

Is altijd "dringend", zoniet "zeer dringend".
Eindigt met het aanzetten tot het doorsturen ervan naar al uw contacten:
hoax bevatten altijd een vermelding van het type:

"maak dit bericht over aan al uw contacten",

"verstuur deze e-mail naar elk van uw contactpersonen",

"maak een kopie van deze e-mail en verstuur deze naar iedereen die u kent";

"a.u.b. verspreid dit bericht naar zoveel mogelijk personen";

"geef de informatie door, die actie kan een leven redden!"

"Dit is ook geldig voor SMS!"

Valse virussen

Het bericht benadrukt dat :

Het steeds om een nieuwe virus gaat.
Het virus nog niet bekend is bij de grote anti-virus ondernemingen zoals McAfee, Symantec, F-Secure of anderen.
Het virus altijd het meest verwoestende is ooit gevonden tot nu toe.
Het meestal afkomstig is van beroemde ondernemingen zoals IBM, Microsoft, Disney, AOL, enz.

Kettingbrieven

Het bericht:

Voorspelt u geluk indien U het doorstuurt aan een aantal personen.
Voorspelt ongeluk indien U het bericht gewoon wist.
Speelt in op de gevoelens van mensen (bv : het redden van een mensenleven door een donor te zoeken met een bepaalde zeldzame bloedgroep).

De valse winsten

"U bent de winnaar!"

Het bericht geeft weer dat:

U de gelukkige bent en een maximum aan geld kan verdienen op zeer korte tijd.
Om het winnende lot te incasseren U dit bericht aan zoveel mogelijk personen moet sturen. Een programma zal het aantal verzendingen optellen.
De personen die al deelnamen, op korte tijd zeer veel geld verdiend hebben (dikwijls in US dollars). Onderaan het bericht wordt als "bewijs" het verhaal van een winnaar vermeld.

Andere elementen die kunnen wijzen op een « Hoax »

Indien U een van de volgende punten kan aantreffen in een bericht, kan U veronderstellen dat het bericht een hoax is:

Het bericht komt van een "vertrouwenspersoon": de bron blijkt een bekende media-instelling te zijn (CNN, Reuters, enz.), een commerciele instelling (Microsoft, AOL, Symantec, enz.) of een bekende (« mijn vriend », « een van onze klanten », enz.). Niemand kan echter een referentie van het artikel of de betrokken persoon geven.
De zogezegde waarheidsversterking : enkele « hoax » maken melding van de tekst « Dit is een waargebeurd verhaal », « dit is geen mop » of ook wel « reële feiten! Aandachtig lezen! ».
Het bericht verwijst naar een aangrijpende situatie of naar een directe bedreiging: het klassieke psychologische element van de « hoax » zit in de beschrijving van een aangrijpende situatie (onrecht, solidariteit, enz.) of alarmerend (virusaanval, probleem met voedingsmiddelen, enz.) meestal fictief, maar vragend naar een steeds weerkerende onmiddellijke reactie zijnde het waarschuwen van alle contactpersonen.
Het bericht maakt melding van een virusinfectie door bijvoorbeeld het bestand « jdbgmgr.exe ». Dit bestand is inderdaad op de harde schijf te vinden en maakt deel uit van de noodzakelijke JAVA-bestanden. Dit bestand moet dan ook zo spoedig mogelijk gewist worden.
Het aanbod is te mooi om waar te zijn: de « hoax » belooft een gratis dienst of een gratis product (een GSM, enkele flessen champagne, enz.) en waar u ook nog eens voor betaald wordt om er gebruik van te maken ... op voorwaarde dat U dit bericht doorstuurt aan alle contactpersonen.

Wat te doen als men denkt een « hoax » ontvangen te hebben ?

Het eerste wat U kan doen indien er gedacht wordt aan een « hoax » is het bericht NIET door te sturen naar uw contactpersonen! Indien de afzender van het bericht U onbekend is, neem geen risico en verwijder het bericht.

Op een van de volgende websites kan er nagekeken worden om te zien of een gelijkaardig bericht al dan niet als hoax gekend is :

VirusAlert (http://www.virusalert.nl) Nederlandstalig.
Hoaxkiller (http://www.hoaxkiller.fr) Franstalig
Hoaxbuster (http://www.hoaxbuster.com) Franstalig
Symantec (http://www.symantec.com/avcenter/hoax.html) Engelstalig
F-Secure (http://www.f-secure.com/en_EMEA/security/security-lab/latest-threats/hoax-descriptions/) Engelstalig

Als het bericht onbekend is hebt u misschien een nieuwe « hoax » ontvangen… of is het bericht dan toch waar.
Om na te gaan of het hier om een al dan niet nieuwe versie van een hoax gaat, kan U steeds een kopie ervan overmaken aan één van bovenvermelde websites voor verdere analyse. Nogmaals, verstuur het bericht niet verder alvorens u het resultaat van deze analyse hebt ontvangen.
Opgelet : verstuur dit bericht niet door simpelweg op doorsturen te klikken, maar maak eerst een nieuw bericht waarbij u dan deze « hoax » als bijlage kan voegen. Op deze manier worden de technische gegevens (emailheaders) van de hoax meeverzonden.

Vraagstelling…

Alvorens een "verdacht" bericht door te sturen aan een contactpersoon, stel U eerst de volgende vragen:

Durf ik de inhoud van dit bericht rechtstreeks aan deze contactpersoon mededelen?
Durf ik deze persoon zelf zeggen dat Bill GATES een deel van zijn fortuin aan mij afstaat en dat hij mij persoonlijk 245$ overmaakt, telkens ik zijn bericht aan een contactpersoon verstuur?
Durf ik deze persoon zelf zeggen dat ik de enige persoon op aarde ben die het bestaan van een gevaarlijk computervirus ken, er bestaat nog geen bescherming tot op heden, zelfs de media en de uitgevers van antivirusproducten hebben nog nooit horen spreken van dit virus...
Neen ?
Verzend dan ook geen berichten die dat beweren!

Miljoenen downloads met Android malware

Lookout heeft een nieuwe malware familie ontdekt in 32 verschillende applicaties van vier verschillende ontwikkel accounts in Google play. Volgens de statistieken van Google Play zijn de getroffen applicaties tussen de 2 en 9 miljoen keer gedownload. Nadat Lookout melding had gemaakt van de aangetroffen malware heeft Google de betrokken apps onmiddellijk uit Google Play verwijderd. De betrokken ontwikkelaars zijn geschorst in afwachting van nader onderzoek.

Badnews lijkt in eerste instantie op een onschuldig reclame netwerk. Het heeft echter de mogelijkheid om gebruikers te pushen om aanvullende applicaties te installeren en stuurt gevoelige informatie zoals telefoonnummers en apparaat-ID's naar specifieke servers. Tijdens onderzoeken door Lookout is onder andere vastgesteld dat de app AlphaSMS werd gepushed. Deze malware is bekend vanwege de premium rate SMS fraude (het versturen van SMS berichten naar kostbare diensten).

De bedreiging zit vooral in de vertraging bij de verspreiding van mogelijke malware. Het gedraagt zich in eerste instantie als een bonafide reclame app waardoor het zonder problemen door de eerste controles heen kan komen. Pas in een later stadium wordt het 'platform' misbruikt voor het verspreiden van malware via specifieke servers. Dit brengt de volgende aandachtspunten naar voren:

Ontwikkelaars moeten aandacht besteden aan het gebruik van bibliotheken van derden.
Bij grotere bedrijven moet men er rekening mee houden dat het vooraf doorlichten van applicaties niet voldoende bescherming kan bieden. Het probleem gedrag zal pas later gaan plaatsvinden. Het is dus van belang om continue monitoring in te richten.

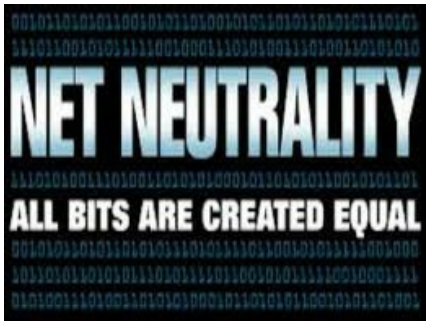
Nep scanner tegen kleine betaling

Het Russische anti-virus bedrijf Doctor Web waarschuwt voor een programma dat een virus van je toestel kan verwijderen. Het begint met een advertentie waarbij de gebruiker wordt verleid om zijn toestel op virussen te laten scannen.
Als de gebruiker daar op in gaat dan wordt deze naar een website gedirigeerd waarbij het anti-virus programma gedownload kan worden. Dit is echter geen echt anti-virus programma maar een trojan.

Dit is de malware Android.Fakealert.4.origin van de Android.Fakealert familie.

Deze Android.Fakealert trojans zijn actief sinds oktober 2012 en doen zich allemaal voor alsof ze bepaalde kwetsbaarheden kunnen opsporen en kunnen verhelpen.
Dit soort malware is bij gebruikers van PC's een langer bekent fenomeen. Door slechts een klein bedrag van bijvoorbeeld US$1,99 te betalen kan een gevonden virus verwijderd worden.

Het advies is dan ook om niet te zwichten voor dit soort advertenties. Gebruik indien nodig altijd alleen anti-virus van bekende leveranciers.



Nederland is netneutraal!

Op 1 januari 2013 trad in Nederland een wijziging van de Telecommunicatiewet in werking waarin netneutraliteit wettelijk wordt geregeld. Daarmee is Nederland na Chili het tweede land in de wereld en het eerste land in Europa dat dit principe in de wet verankert. Wat is netneutraliteit eigenlijk, wat houdt de nieuwe regeling in en wat zijn de consequenties van deze wetswijziging voor bedrijven?

Netneutraliteit

Netneutraliteit gaat uit van het principe dat een telecomprovider zich niet mag bemoeien met het verkeer dat over zijn netwerk vloeit. Voorstanders van netneutraliteit voeren hier twee redenen voor aan. Ten eerste vinden zij dat het internet open en vrij moet zijn. Ten tweede zijn zij van mening dat aanbieders van infrastructuur hun macht over deze infrastructuur niet mogen misbruiken om hun eigen diensten of verdienmodellen te beschermen. Voorstanders van netneutraliteit stellen dat na de invoering van dit principe het onmogelijk wordt voor telecomproviders om hun eigen bedrijfsvoering en belangen op oneigenlijke wijze te beschermen.

Wettelijke regeling

In 2011 werd het voornemen van KPN, als aanbieder van mobiel internet, bekend om VOIP en online chatdiensten Skype en WhatsApp te gaan blokkeren op smartphones, tenzij consumenten extra zouden gaan betalen. Doordat steeds meer consumenten Skype of WhatsApp gebruiken in plaats van bellen en sms'en, wilde KPN het verlies in opbrengsten door bel- en sms-verkeer compenseren door een 'Skype-heffing'.

Dit voornemen van KPN was de directe aanleiding om het principe van netneutraliteit in de Nederlandse Telecommunicatiewet in te voeren. In mei 2012 werd het Staatsblad met de tekst van de wetswijziging gepubliceerd. Bedrijven hebben tot 1 januari 2013 de tijd om hun verdienmodel aan deze wetswijziging aan te passen.

Inhoud wettelijke regeling

Het principe van netneutraliteit staat in artikel 7.4a van de Telecommunicatiewet. Dit wetsartikel verbiedt het belemmeren of vertragen van diensten of toepassingen op internet. Dit betekent ten eerste dat een provider geen specifieke partij het gebruik van internet mag weigeren. Het betekent daarnaast ook dat een provider geen specifieke dienst, zoals Skype, of informatie mag blokkeren of vertragen.

Let wel: deze wetswijziging heeft alleen betrekking op toegang tot Internet. Services zoals op IP-gebaseerde televisie die niet via internet worden aangeboden vallen buiten deze regeling.

Verder blijft het voor internetproviders mogelijk om hun internetabonnementen te differentiëren op andere manieren, bijvoorbeeld naar beschikbare bandbreedte en datalimieten. Ook blijft het mogelijk dat providers losse diensten aanbieden via internet. Zo kan een aanbieder een los abonnement aanbieden voor mobiel bellen via VOIP in plaats van met de gewone mobiele telefoon. In deze gevallen is het toegestaan het overige internetverkeer te blokkeren.

Uitzonderingen

Op bovenstaand verbod bestaan een viertal uitzonderingen, deze moeten echter beperkt worden uitgelegd.

Een internetprovider mag verkeer op het internet vertragen of belemmeren om congestie op het net op te lossen. Echter de provider mag geen specifieke diensten vertragen. Dezelfde soorten verkeer moeten hetzelfde worden behandeld. Ten tweede mag een provider internetverkeer blokkeren dat de veiligheid en integriteit van het internetverkeer aantast. Hierbij gaat het bijvoorbeeld om activiteiten van hackers. Ten derde mag een provider spam blokkeren. De laatste uitzondering is een rechterlijk bevel. Het blokkeren van bijvoorbeeld The Pirate Bay door internetproviders is dus onder de nieuwe wet nog steeds mogelijk.

Op dit moment in de schatkist:
(Klik op de kist om het te downloaden)

Bootkit Removal Tool

Trends in Veiligheid 2013

Zdnet Security Guide 2013 deel 2

Zdnet Security Guide 2013 deel 1

UnstoppableCopier

PrivaZer Free

Keyfinder Thing Lite

Format Factory

'Te weinig internetcriminelen voor de rechter'

Internetcriminaliteit komt te weinig voor de rechter. Te vaak grijpt de politie in zonder dat daar vervolging uit voortvloeit. Of de resultaten van opsporingszaken komen alleen maar ten goede aan buitenlandse opsporingsdiensten.

Volgens Christiaan Baardman, vanaf volgende week coördinator bij het Kenniscentrum Cybercrime van de Rechtspraak, blijft de rechtspraak achter bij de explosieve groei aan computercriminaliteit. Dat komt doordat voor de politie vaak het kapot maken van de zaak "van groter belang" kan zijn dan een dader veroordeeld krijgen, constateert Baardman in een artikel op rechtspraak.nl. Daarnaast heeft cybercrime een grensoverschrijdend karakter, waardoor veel onderzoek van de politie ten goede komt aan het oplossen van zaken door buitenlandse opsporingsdiensten.

"De politie is dan bezig om zaken voor andere landen op te lossen, waarvan bij voorbaat vaststaat dat ze nooit voor onze rechter zullen komen", zegt Baardman. "Jammer is alleen wel dat onze politie veel meer onderzoeken doet voor andere landen dan andersom, en de capaciteit is toch al zo beperkt."

Bestanden wissen in plaats van arresteren

Het niet voor de rechter brengen van internetcriminelen gebeurde onder meer bij het onderzoek naar het netwerk van Robert M. in de bekende kinderpornozaak. Daarbij brak de politie in in computers, werden bestanden vernietigd en waarschuwingen achtergelaten dat de politie de websites in de gaten hield, vertelt Baardman, die die informatie weer heeft van het OM.

"De politie is dan bezig om zaken voor andere landen op te lossen, waarvan bij voorbaat vaststaat dat ze nooit voor onze rechter zullen komen"

Het nadeel van deze werkwijze is dat een toetsing achteraf door de rechter van de inzet van opsporingsmiddelen uitblijft en de rechters nauwelijks ervaring krijgen met internetcriminaliteitszaken, net als overigens Officieren van Justitie. Overigens verwacht Baardmans wel een flinke toename van het aantal zaken als het wetsvoorstel van minister Opstelten wordt aangenomen.

Hacken van computers van verdachten

In dat wetsvoorstel wordt onder meer de uitbreiding van opsporingsbevoegdheden op het internet geregeld. Zo zou de politie voortaan computers van verdachten mogen hacken, spionagesoftware mogen plaatsen en wordt het meewerken aan het ontsleutelen van bestanden door verdachten verplicht gesteld.

Om rechters daarop voor te bereiden, gaat het Kenniscentrum Cybercrime de magistraten onderwijzen. "Om optimaal te profiteren van de weinige zaken die wel voor de rechter komen, proberen we hoger beroepszaken over cybercrime binnen het Haagse hof te concentreren", zegt Baardman.

Doe-het-zelfterreur is nieuwe dreiging

Over de rol van internet – en steeds vaker: sociale media – bij terrorisme is al veel geschreven.
Ook na 'Boston' worden er vele regels aan gewijd. Dit keer in de New York Times waar Scott Shane schrijft over Inspire, de glossy van Al Qaida.

Dat blad is onder 'doe-het-zelfterroristen' zeer populair. Ze lezen er behalve propaganda ook hoe ze kleinschalige solo-acties kunnen uitvoeren, 'how to make a bomb in the kitchen of your mother', inclusief links naar instructiefilmpjes uitleg op internet hoe ze dat moeten doen.

Aanslagen als in Boston zijn, mede daarom, steeds moeilijker te voorkomen, zei president Obama al. Zoals het er nu naar uitziet, zijn de gebroeders Tsarnajev thuis, via internet dus, geradicaliseerd. Dzjochar zei al tegen zijn verhoorders dat ze het scenario van Inspire volgden … Dat blad is in veel landen al verboden verklaard – maar bij Scribd gewoon te lezen.

In Groot-Brittannië zijn de afgelopen anderhalf jaar zelfs al twintig mensen veroordeeld voor het downloaden en verspreiden ervan. Behalve Inspire is op internet ook het 'Handboek voor Moedjahedien Eenlingen' te vinden, 64 pagina's met doe-het-zelfartikelen als 'Droom je van jihadistische aanvallen op de ongelovigen?'

Maar aanslagen voorkomen, dat wordt lastig, zeggen alle experts.

In 2011 probeerde korporaal Naser Abdo een bom te maken met een snelkookpan. Hij liep tegen de lamp toen een werknemer van een wapenwinkel alarm sloeg toen Abdo alleen kruit wilde kopen. Toen de gebroeders Tsarnajevs vuurwerk kochten en vroegen naar 'het zwaarste vuurwerk dat je hebt', sloeg niemand alarm. Logisch, aldus de baas van de vuurwerkwinkel. 'Dat klinkt verdacht. Maar 90 procent van de mannen vraagt dat'.

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

Gebruikte bronnen voor dit nummer:

Webwereld
Security.nl
Ixquick
Voelspriet
Zdnet
De Waarschuwingsdienst
Europol
Computable
Politiebronnen.nl
Nu.nl
PCMweb

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 uituw 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 engeneering, 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 TANcodes, 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, Virusdoder 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 > Toebname 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