Secure Computing



W.Bosgra taakaccenthouder digitale criminaliteit

Oktober 2013

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 !



Wachtwoord vergeten? Deze tools helpen

Sterke stijging politievirussen

200.000 Nederlanders slachtoffer pishing/skimming

Gratis beveiliging goed genoeg?

Safepay: de 'hackvrije' browser

Nieuw in de Schatkist: PC Decrapifier, Revo Uninstaller, Blackberry desktop Software, Asus Ai Charger



Sterke stijging politievirussen en AutoRunmalware



Het gebruik van ransomware die de computer in naam van een politiedienst vergrendelt is nog altijd zeer populair bij cybercriminelen, alsmede het gebruik van malware die zich via de AutoRunfunctie van Windows verspreidt. Het aantal nieuwe ransomware-exemplaren, ook wel politievirussen genoemd, kende een ruime verdubbeling in het tweede kwartaal van dit jaar.

In de eerste drie maanden van dit jaar werden er nog 150.000 nieuwe exemplaren ontdekt, in het tweede kwartaal was dit naar 325.000 opgelopen. "Een reden dat ransomware groeit is dat het een erg efficiënte manier voor criminelen is om geld te verdienen, omdat ze verschillende anonieme betaaldiensten gebruiken", aldus anti-virusbedrijf McAfee in een nieuw kwartaalrapport.

Volgens de virusbestrijder is deze methode om geld binnen te halen superieur ten opzichte van nepvirusscanners, waar slachtoffers de nepsoftware via een creditcardbetaling moeten activeren. Toch werden er in het tweede kwartaal nog altijd meer nepvirusscanners dan ransomware aangetroffen.
Autorun

Een andere categorie malware die al twee kwartalen op rij een sterke stijging kent is AutoRunmalware. Deze malware verspreidt zich via USB-sticks en gedeelde netwerkmappen en gebruikt hierbij de Autorunfunctionaliteit van Windows. McAfee geeft geen verklaring voor de plotselinge toename.

Microsoft had in 2011 namelijk een update uitgebracht die de werking van Autorunmalware moest ontregelen, doordat de functionaliteit niet standaard op USB-sticks werd uitgevoerd. Er was ook nog goed nieuws, aangezien het aantal nieuwe rootkits en nepvirusscanners ten opzichte van de voorgaande kwartalen afnam.



De Wet Computercriminaliteit: Binnendringen

De bekendste vorm van computercriminaliteit is het opzettelijk en wederrechtelijk binnendringen in een computersysteem of netwerk. Dit heet computervredebreuk (soms ook wel computerinbraak of hacken) en is een misdrijf. Hierop staat een straf van maximaal 1 jaar cel of geldboete van 16.750 euro (art. 138ab lid 1).



Onder de oude wetgeving was computervredebreuk alleen strafbaar wanneer een beveiliging werd doorbroken. Deze eis is komen te vervallen. Computerinbraak is nu strafbaar wanneer de dader wist dat hij op verboden terrein was.

Computervredebreuk of hacken is dus het binnendringen ("inbreken") in een computersysteem of netwerk. Dit kan uiteraard op vele manieren, en de wet geeft daar geen algemene definitie voor. Bij de behandeling in de Tweede Kamer gaf de minister aan dat dit van geval tot geval uit de rechtspraak zal moeten blijken.

Vaak wordt de term "hacken" gebruikt om activiteiten zoals computervredebreuk of computerinbraak aan te duiden. Dit is eigenlijk niet juist: een hacker is iemand die zeer goed en creatief met computers om kan gaan, en meestal niet er op uit is om schade aan te richten. Toch worden activiteiten van hackers (in deze positieve betekenis van het woord) gezien als computervredebreuk als ze, om welke reden dan ook, wederrechtelijk in systemen binnendringen.
Voorbeelden uit de wet

Artikel 138ab lid 1 noemt het doorbreken van een beveiliging, gebruik maken van een technische ingreep, valse signalen of een valse sleutel en het aannemen van een valse hoedanigheid als voorbeelden van computervredebreuk. Deze categorieën zijn niet bedoeld als volledige taxonomie, er kan best overlap tussen zitten. Een paar voorbeelden uit elke categorie:

Doorbreken van een beveiliging: het laten crashen van het inlog-programma, zodat iedereen zonder verdere controle naar binnen mag
Een technische ingreep: het systeem zo ver krijgen dat het een instructie uitvoert waardoor de toegang wordt verleend tot bepaalde gegevens (het digitale equivalent van het kortsluiten van een elektronisch slot zodat de deur opengaat)
Valse signalen of een valse sleutel:: een geraden of afgekeken wachtwoord van een ander gebruiken, of je computer andermans IP-adres laten aannemen (IP spoofing)
Het aannemen van een valse hoedanigheid: je computer de naam geven van de printserver en zo toegang tot de map met printjobs krijgen, of de helpdesk bellen, zeggen dat het je eerste dag bij systeembeheer is en vragen wat het wachtwoord ook alweer was. Ook phishing, een e-mail of website laten lijken op die van een bank om zo pincodes en dergelijke te pakken te krijgen, kan hieronder vallen.



Wie dus één van deze handelingen verricht, pleegt in ieder geval computervredebreuk. Het is mogelijk dat er andere vormen van binnendringen zijn (of komen) die niet hier onder vallen. De rechter zal dan moeten bepalen of dit dan een strafbare vorm van binnendringen is.

Cybercrimineel verkoopt besmette Nederlandse PC's

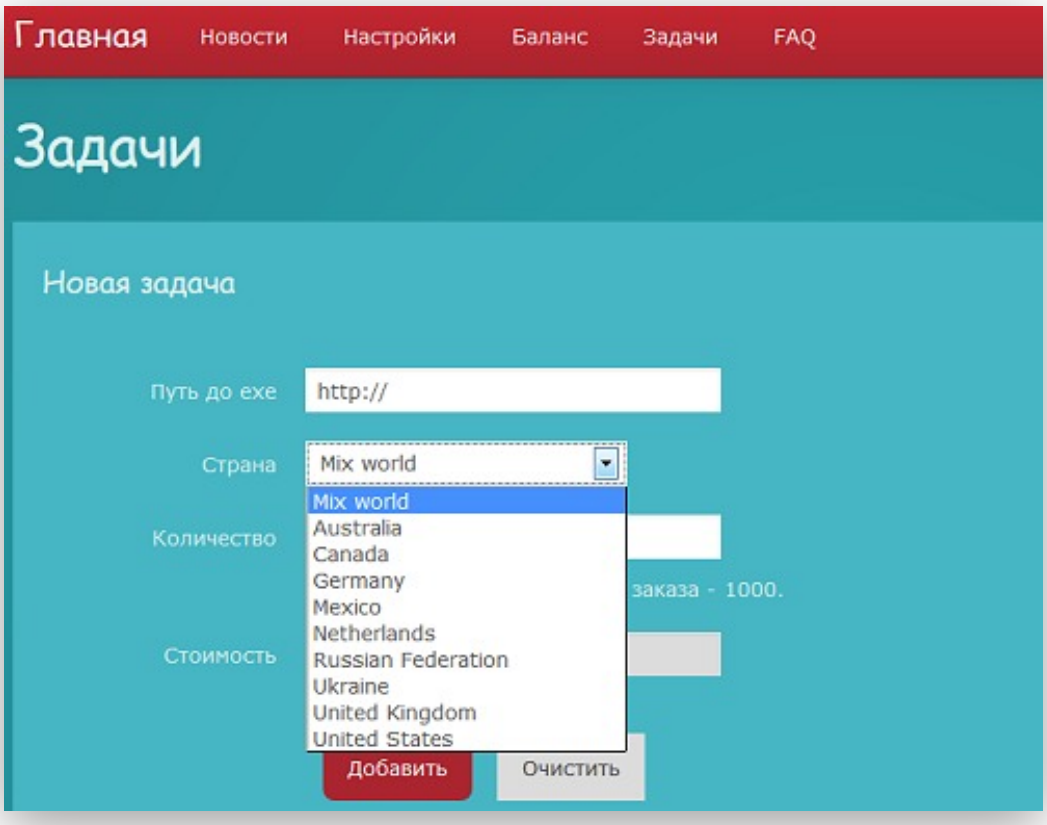
Moesten cybercriminelen vroeger nog vaak zelf computers met malware infecteren, tegenwoordig krijgt de beginnende cybercrimineel met een kleine investering toegang tot duizenden computers die hij vervolgens verder kan besmetten. De markt voor "managed cybercrime-as-a-service" bestaat al enkele jaren en maakt het voor beginners eenvoudig om aan de slag te gaan, aldus beveiligingsonderzoeker Dancho Danchev.

"Het enige wat een beginnende cybercrimineel in 2013 hoeft te doen om toegang tot duizenden computers in een bepaald land te verkrijgen is het doen van een bescheiden investering", aldus de onderzoeker, die onlangs een nieuwe aanbieder ontdekte.

Hebzucht

Potentiële klanten die op de al geïnfecteerde computers hun eigen malware willen installeren hoeven alleen maar een locatie te selecteren en af te rekenen, met een minimale afname van 1000 computers. Onder de negen landen waar kopers uit kunnen kiezen komt ook Nederland voor. Hoeveel de pc's kosten laat Danchev niet weten.

Het gaat om een Russische aanbieder die volgens Danchev een goed voorbeeld van hebzucht is, in plaats dat hij door sociaal-culturele of socio-economische motieven gedreven wordt, aangezien er ook besmette computers uit Rusland en de Oekraïne worden aangeboden.



Politie: zet foto’s smartphonedief niet op internet



De politie adviseert consumenten van wie de smartphone wordt gestolen om foto's van eventuele dieven niet op internet te plaatsen, omdat veel veroordelingen hierdoor lager uitvallen. Het advies volgt na de Gay Pride, waar zakkenrollers honderden bezoekers van hun smartphone beroofden. "Veel veroordelingen vallen lager uit doordat verdachten al publiekelijk aan de schandpaal waren genageld", aldus de politie.

Wraak

"Zoete wraak is soms bijzonder prettig. Zeker als de mobieltjesdief niet in de gaten heeft dat hij of zij per ongeluk privéfoto's uploadt in uw account op Dropbox, iCloud of Google+. Apps als iCaughtU en iGotYa maken zelfs automatisch foto's en mailen die naar uw e-mailadres", aldus de politie.

Die stelt dat het steeds vaker voorkomt dat slachtoffers de foto’s op sociale media zetten om de dader te achterhalen of publiekelijk aan de schandpaal te nagelen. "Dat dit tot lagere straffen leidt als de daders gepakt worden, is vast niet uw bedoeling. Gelukkig kunt u veel doen om het de dieven zo onaantrekkelijk mogelijk te maken."



Onlangs maakte een Duitse toeriste een weblog waar ze foto's plaatste die via haar gestolen iPhone waren gemaakt.

Maatregelen

Om een gestolen telefoon minder aantrekkelijk te maken adviseert de politie eigenaren om het imei-nummer (international mobile equipment identity) te noteren. Daarmee is het mogelijk om een sms-bombardement uit te voeren. De politie bestookt het toestel dan met de melding 'Deze telefoon is gestolen, ga naar de politie'. Doorverkoop is daarmee niet langer interessant.

Ook wordt de installatie van een yunu-code (Your Unique Number) aangeraden. Zonder deze pincode kan een niet-gemachtigde gebruiker geen nieuwe simkaart plaatsen. De code is zonder tussenkomst van de provider te activeren.

Apps

Een andere maatregel die eigenaren kunnen nemen is de installatie van een app waarmee een zoekgeraakt toestel is terug te vinden. Volgens de politie kan een dief de pogingen om het toestel te traceren echter makkelijk omzeilen. "Vergrendel daarom de locatievoorzieningen met een wachtwoord."

Als laatste wordt ook nog geadviseerd om Dropbox, iCloud en Google+ in de gaten te houden. "Niet zozeer vanwege de zoete wraak, maar omdat de foto’s soms heel concrete dingen zeggen over de identiteit van de dader of heler."



Justitie: geen wetswijziging nodig voor stealth-sms



Justitie: geen wetswijziging nodig voor stealth-sms

De politie gaat de procedures bij de inzet van stealth-sms 'verbeteren' nadat het Hof oordeelde dat er geen wettelijke grondslag voor is. Een andere, bestaande grondslag volstaat.

Politie en Justitie gaan het gebruik van stealth-sms'jes om verdachten te lokaliseren beter documenteren en op zoek naar "de juiste wettelijke grondslag". Maar die kan gevonden worden binnen de bestaande wetten, er is geen wetswijziging voor nodig. Dat stelt het ministerie van Justitie in een reactie op de kritiek van het Hof Den Bosch op het gebruik van stille sms'jes. Onderdeel van telefoontap of observatie?

Stealth-sms wordt sinds 2005 ingezet. Hiermee stuurt de politie een leeg sms-bericht naar het mobiele nummer van de verdachte. Diens toestel straalt daardoor de dichtstbijzijnde gsm-antenne aan voor de ontvangst van dit onzichtbare bericht. Op basis van zendmastdata van de mobiele provider kan de politie de locatie van de verdachte op dat moment achterhalen.

De methode wordt niet alleen veelvuldig ingezet bij zware strafzaken, het wordt ook slecht bijgehouden en vaak zelfs bewust achtergehouden uit het strafdossier.



Het Hof oordeelde onlangs in de Begonia-drugszaak dat de inzet van stealth-sms'jes een niet wettelijk geregelde, heimelijk opsporingsmethode is. De rechters stellen dat de techniek een "betekenisvolle inbreuk op grond- en vrijheidsrechten" kan opleveren en "risicovol is voor de integriteit en beheersbaarheid van de opsporing" die niet wordt afgedekt door artikel 2 Politiewet en artikelen 141 en 142 Wetboek van Strafvordering. Een "bijzondere wettelijke grondslag voor het gebruik van deze opsporingsmethode is noodzakelijk", aldus het Hof.

Tot nog toe stelt het openbaar ministerie telkens dat de stealth-sms onderdeel is van een tap op een mobiele telefoon. "Het is geen bijzondere bevoegdheid in de zin van de wet. Het is een bijwerking van het afluisteren van telefoons, de tapbevoegdheid. En voor het aftappen is dan reeds een machtiging van rechter-commissaris verkregen," stelde de woordvoerder van het Landelijk Parket in 2011.



Maar die vlieger gaat na het arrest van het Hof Den Bosch niet meer op. Dat houdt echter niet in dat de wet aangepast moet worden, vindt Justitie. "Het gebruik van stealth-sms is door andere rechters eerder al wel goedgekeurd, en ook in deze specifieke zaak heeft het geen gevolgen voor het verdere proces", aldus de zegsman van het ministerie.

Wel gaat de politie de procedures verbeteren en zal, afhankelijk van de zaak, de juiste grondslag worden aangevoerd, reageert Justitie. Mogelijk komt de stealth-sms dan bijvoorbeeld onder een ander regime te vallen, zoals stelselmatige observatie, artikel 126g van de Wet Bob (Bijzondere opsporingsbevoegdheden). het hangt af van de zaak en de frequentie van de inzet van stealth-sms.

Hacksoftware laat overheden op wifi-netwerken inbreken

Hacksoftware die een Duits bedrijf voor allerlei overheidsdiensten ontwikkelde maakt het mogelijk om op wifi-netwerken in te breken. Het gaat om de FinFisher software van Gamma International, wat uit een verzameling van verschillende aanvalstools bestaat. Zo is er de FinFisher spyware om verdachten af te luisteren en kan via de FinUSB Suite op geheime wijze informatie van systemen worden gestolen, bijvoorbeeld door iemand die zich als schoonmaker voordoet.

Uit een presentatie van FinFisher blijkt dat de populaire Backtrackdistributie als inspiratie voor de spyware diende. Daarbij werd zelfs de oprichter van Backtrack ingeschakeld om een "uitgebreide portfolio" te maken. Naast de twee eerder genoemde tools er ook de FinIntrusion Kit.

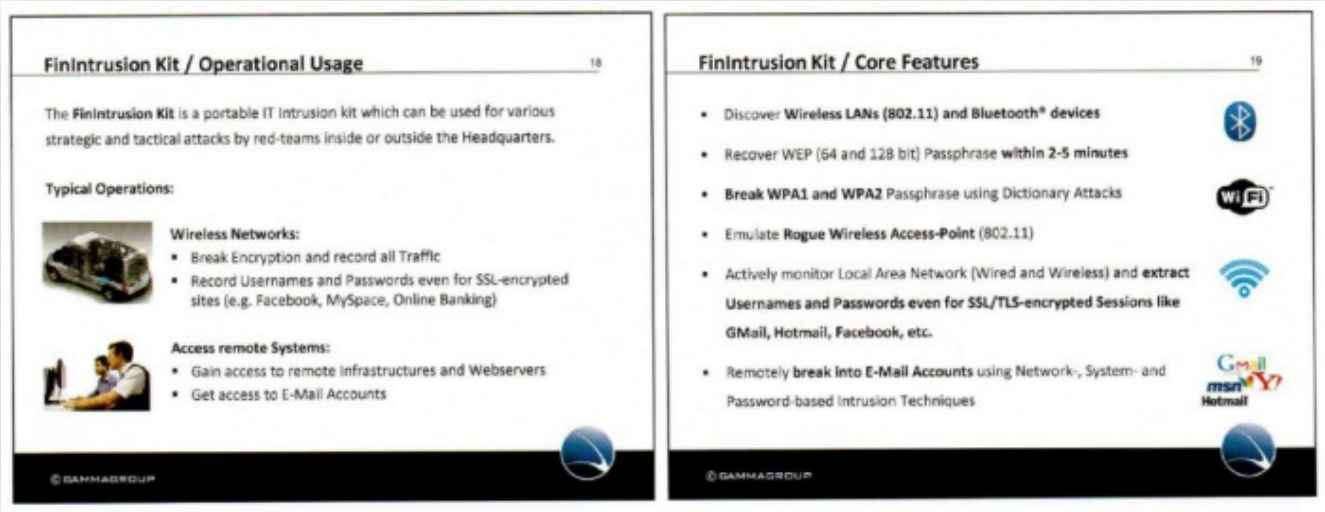
Wifi-netwerken

Via deze software is het mogelijk om wifi-netwerken en apparaten met Bluetooth te ontdekken. De hacksoftware kan WPA1 en WPA2 passphrases via woordenboekaanvallen kraken, WEP-sleutels binnen twee tot vijf minuten achterhalen en zich als een kwaadaardig access point voordoen.

Eenmaal actief zou het ook mogelijk zijn om gebruikersnamen en wachtwoorden van zelfs met SSL-versleutelde websites, zoals Facebook en internetbankieren, te onderscheppen, aldus de presentatie die deels door het Finse F-Secure online werd gezet.

Internetprovider

Voor een andere tool in de FinFisher Suite is het mogelijk om verdachten met behulp van hun internetprovider te infecteren. De FinFly Web exploit, zoals de tool heet, kan door de provider van de verdachte op vertrouwde websites zoals Gmail en YouTube worden geïnjecteerd. Een andere mogelijkheid is dat de internetprovider alle downloads van de verdachte van malware voorziet.



Besmettingsgevaar Java groeit in verontrustend tempo

Java staat al langer bekend als een zwart schaap in de softwarewereld, vanwege het grote aantal openstaande lekken dat cybercriminelen kunnen gebruiken om in te breken op pc's.

Uit een onlangs gepubliceerd onderzoek van Kaspersky Lab blijkt nog maar eens hoe groot het probleem is.

In het afgelopen jaar zijn volgens de Russische beveiliger 161 kwetsbaarheden ontdekt in de Java Environment Runtime (JRE). En aanvallers maken gretig van de gelegenheid gebruik: in zes maanden tijd telde het Russische beveiligingsbedrijf meer dan 2 miljoen aanvallen via Java-exploits.

Eigenaar Oracle heeft aangegeven dat het zijn leven wil beteren en maakte een paar maanden geleden bekend dat het patches op dezelfde wijze gaat distribueren als Microsoft al langer gewend is voor zijn producten.



Maar voor het zijn zaakjes op orde kan krijgen, lijkt de veiligheidssituatie voor Java-gebruikers dramatisch te verslechteren, zo zegt Trend Micro-analist Christopher Budd.

Cybercriminelen hebben een vrijgegeven patch voor Java 7 uit elkaar gehaald (reverse engineering) en gebruiken de verzamelde informatie om exploits te bouwen voor Java 6.

Het probleem is dat Oracle in april van dit jaar de ondersteuning van Java 6 heeft gestaakt, waardoor veel gebruikers een actief gebruikt open lek op hun systeem hebben staan dat nooit zal worden gerepareerd.

De laatste versie van Java installeren lijkt dus bittere noodzaak, maar volgens Trend Micro ben je ook dan niet gegarandeerd veilig.



200.000 Nederlanders slachtoffer van skimming en phishing

Vorig jaar werden ruim 200.000 Nederlanders slachtoffer van ID-fraude via een pinautomaat of via het internet. Het gaat dan om het kopiëren van een bankpas bij een pinautomaat of het achterhalen van betalingsinformatie via het internet, bijvoorbeeld via een gehackte computer of phishingsite.

Dat laat het Centraal Bureau voor de Statistiek (CBS) weten. Het leeuwendeel van de slachtoffers maakt hiervan melding bij de bank, een klein deel ook bij de politie. Hoger opgeleiden worden hier twee keer zo vaak slachtoffer van dan lager opgeleiden, en 25- tot 65-jarigen meer dan jongeren en ouderen.

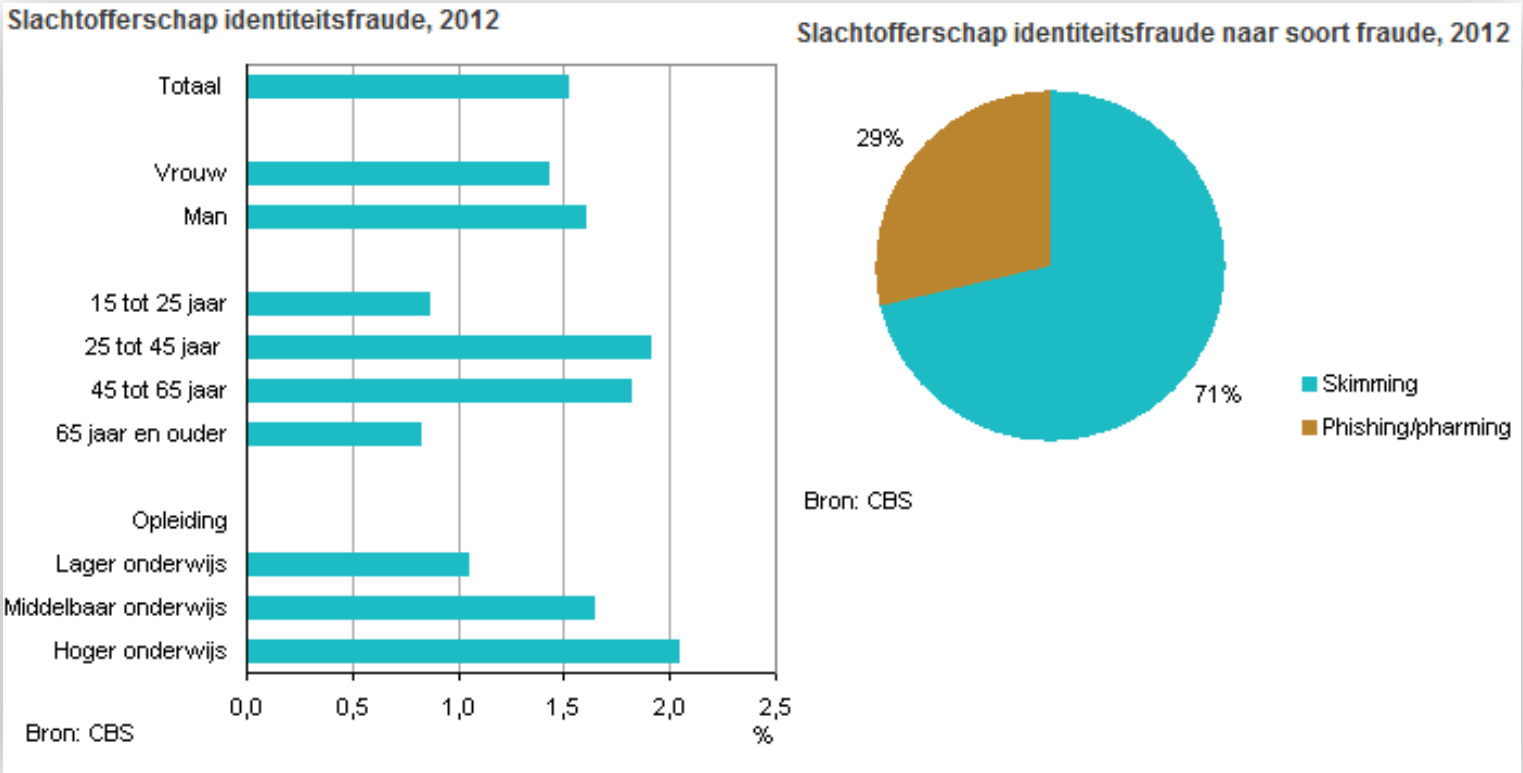
Skimming

Zeven op de tien slachtoffers van identiteitsfraude in 2012 had te maken met skimming. "Phishing en pharming komen dus beduidend minder voor", aldus het CBS. Eerder bleek al uit cijfers van de Nederlandse Vereniging van Banken dat in de tweede helft van 2012 en eerste helft van 2013 skimming meer schade veroorzaakte dan fraude met internetbankieren.

De fraude vond acht op de tien keer in Nederland plaats. In één op de tien gevallen gebeurde de fraude terwijl het slachtoffer in het buitenland een betaalpas, creditcard of het internet gebruikte. Bij de overige 10 procent is niet bekend waar de fraude plaatsvond.

Aangifte

Negen op de tien slachtoffers van skimming of phishing maakt hiervan melding. Dat doen ze vooral bij de bank of een andere financiële instelling. Minder dan 20 procent heeft de fraude in 2012 gemeld bij de politie. De meldingsbereidheid is onder ouderen meestal iets hoger dan onder jongeren.



Gratis beveiligingspakket presteert bijzonder goed

Dat betaalde producten niet altijd beter zijn dan gratis oplossingen blijkt uit een nieuw overzicht van Internet Security Suites. Het Duitse testorgaan AV-Test voerde tussen januari en juni drie tests uit, waarbij tientallen beveiligingspakketten werden vergeleken op Windows XP, Windows 7 en Windows 8. Het gaat hierbij om Internet Security Suites, die naast een virusscanner ook nog aanvullende bescherming bieden.

Over de drie tests genomen weten de Internet Security Suites van Bitdefender, F-Secure en Kaspersky Lab voor de detectie van zowel "real-world" malware als de referentieverzameling 100% te scoren. Het gratis Avast Antivirus Free staat met een score van 98% en 99% verdienstelijk in de Top 10 en scoort als het om detectie gaat beter dan betaalde oplossingen van ESET, AVG en McAfee.

Uitslag

Naast de bescherming tegen malware, waar de producten 6 punten voor konden verdienen, werd er ook naar systeembelasting en bruikbaarheid gekeken. Ook voor deze categorieën waren 6 punten te behalen. Aan de hand van deze onderdelen werd een totaalscore berekend, wat Avast een score van 15,2 punten opleverde.

Daarmee moet de gratis software Bitdefender (17,2), Kaspersky (16) en Symantec (15,5) voor zich laten, maar staat het boven de commerciële programma's van ESET, McAfee, Webroot en Avira.

	Manufacturer	Product	Protection (max. 6 pts)	System Load (max. 6 pts)	Usability (max. 6 pts)	Overall Points Total (max. 18)	Number of Tests	AV-TEST Certificate
1	Bitdefender	Internet Security	6.0	5.2	6.0	17.2	3	YES
2	Kaspersky Lab	Internet Security	6.0	4.2	5.8	16.0	3	YES
3	Symantec	Norton Internet Security	5.7	3.8	6.0	15.5	3	YES
4	Avast	Free AntiVirus	5.2	4.0	6.0	15.2	3	YES
4	F-Secure	Internet Security	6.0	4.0	5.2	15.2	3	YES
4	G Data	InternetSecurity	5.8	4.0	5.3	15.2	3	YES
5	BullGuard	Internet Security	5.7	4.0	5.3	15.0	3	YES
5	Qihoo *	360 Internet Security	5.2	4.3	5.5	15.0	3	YES
6	AVG	Anti-Virus Free Edition	4.8	4.5	5.5	14.8	3	YES
7	Trend Micro	Titanium Maximum Security	5.7	3.7	5.3	14.7	3	YES
8	AVG	Internet Security	5.0	4.0	5.5	14.5	3	YES
8	Tencent	PC Manager	3.8	4.7	6.0	14.5	3	YES
8	Webroot	SecureAnywhere Complete	4.2	6.0	4.3	14.5	3	YES
9	Panda Security	Cloud Antivirus FREE	4.7	4.0	5.5	14.2	3	YES
10	ESET	Smart Security	5.2	3.0	5.5	13.7	3	YES
11	Microworld	eScan internet security suite	5.7	2.3	5.2	13.2	3	YES
11	McAfee	Internet Security	4.8	2.5	5.8	13.2	3	YES
12	Avira	Internet Security	3.8	4.0	4.8	12.7	3	YES
12	Check Point	ZoneAlarm Free Antivirus + Firewall	2.5	4.2	6.0	12.7	3	YES
12	ThreatTrack *	VIPRE Internet Security	4.0	3.2	5.5	12.7	3	YES
13	Comodo	Internet Security Premium	5.2	4.3	3.0	12.5	3	YES
13	Norman	Security Suite Pro	4.3	3.2	5.0	12.5	3	YES
14	Microsoft *	Windows Defender	1.0	3.8	6.0	10.8	3	Base value
15	AhnLab	V3 Internet Security	1.7	3.8	5.0	10.5	3	YES
	Other protection programs with just 2 tests							
–	PC Tools *	Internet Security	4.3	3.5	5.5	13.3	2	YES
–	Kingsoft	Antivirus	4.3	3.3	5.5	13.0	2	YES
	Other protection programs with just one test							
–	Lavasoft	Ad-Aware Pro Security	4.5	3.0	5.5	13.0	1	YES
–	K7	Total Security	1.0	3.5	5.0	9.5	1	NO

Please note: Products with the same points totals are listed in alphabetical order; the PC Tools product was discontinued; ThreatTrack is the vendor formerly known as GFI; the Qihoo product 360 Antivirus was renamed 360 Internet Security; Microsoft results are only provided as base values.

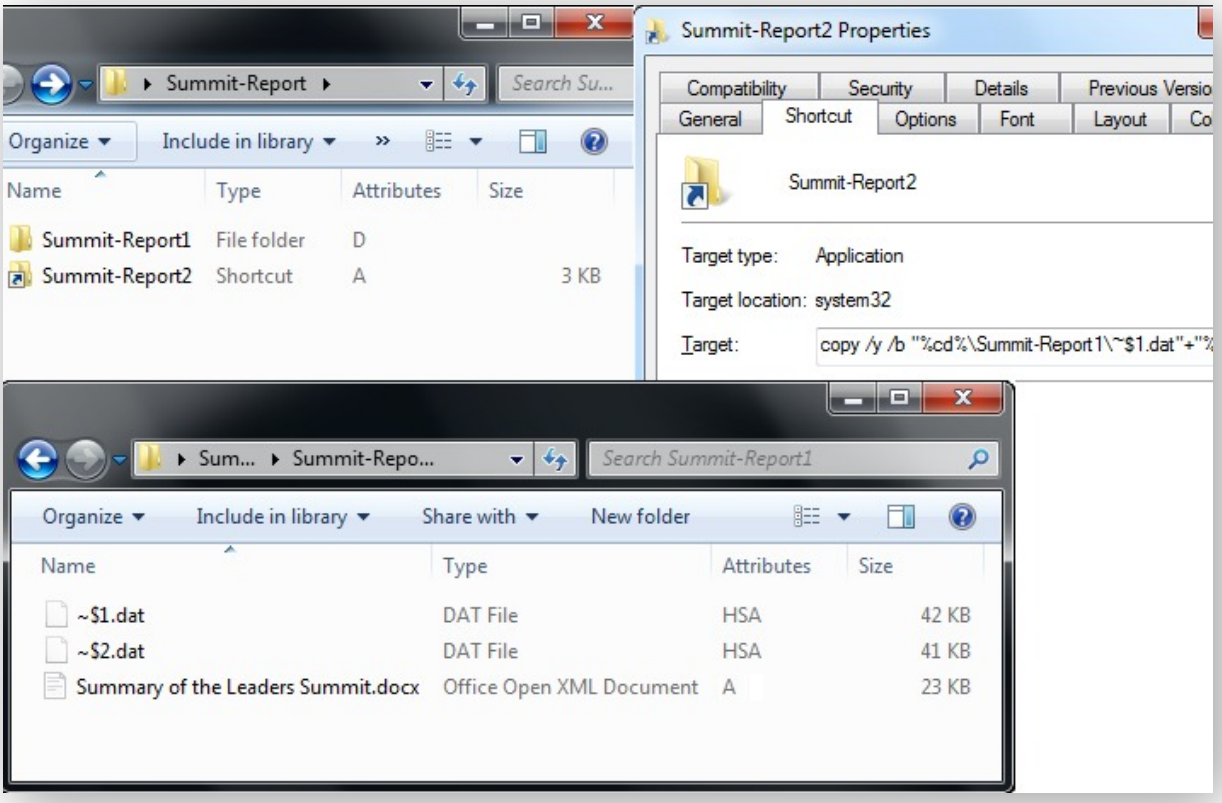
Toename van snelkoppelingen bij gerichte aanvallen

Cybercriminelen gebruiken een nieuwe methode om de netwerken van organisaties en bedrijven te infiltreren, namelijk een combinatie van snelkoppelingen en gedemonteerde malware. Snelkoppelingsbestanden zijn in het verleden al vaker bij gerichte aanvallen gebruikt, maar anti-virusbedrijf Symantec kwam laatst een aanval tegen waarbij de bestanden op een creatieve manier waren ingezet.

Het slachtoffer had als bijlage een archiefbestand ontvangen met daarin gedemonteerde malware en een snelkoppeling. Het archiefbestand bevatte een snelkoppeling met het icoon van een map, alsmede een echte map met daarin een Microsoft document en twee verborgen .dat-bestanden.
Detectie

Zodra het slachtoffer de snelkoppeling opende werd de malware, die uit de twee .dat-bestanden bestond, in elkaar gezet en het systeem geïnfecteerd. De reden dat de aanvallers de gedemonteerde malware pas op het systeem van het slachtoffer in elkaar zetten is mogelijk om detectie te omzeilen.

Het wordt hierdoor lastiger voor beveiligingssoftware om te bepalen of de bestanden kwaadaardig zijn. Een andere reden kan zijn dat sommige gateways uitvoerbare bestanden in e-mails verwijderen. Aangezien het niet nodig is dat een e-mailbijlage een snelkoppeling bevat, stelt analist Joji Hamada dat bedrijven ook hierop kunnen filteren.



Safepay: Veilig internetbankieren in 'hackvrije' browser

Wie het maar eng vindt om via zijn browser online bankbetalingen uit te voeren, is een goede kandidaat voor BitDefender Safepay, een veilige 'hackvrije' browser, die grotendeels gratis is.

Hoewel banken en overheid steeds meer maatregelen nemen om diefstal in je online bankrekening te voorkomen, lukt het cybercriminelen nog altijd om een uitstekende boterham te verdienen.

Safepay, een product van securitybedrijf BitDefender, is daarom zeker het overwegen waard. Deze browser, gebaseerd op het Chromium-project, is een stuk meer dichtgetimmerd dan de reguliere browser en stopt verschillende bekende trucs af die malwareschrijvers en phishers toepassen om je geld afhandig te maken.

Bij de start van elke sessie scant Safepay je computer om te zien of malware zich niet al op je computer heeft genesteld. Vervolgens opent het zichzelf in een beveiligde sandboxmodus, wat het onmogelijk maakt voor externe software om een kijkje te nemen naar je ingevulde gegevens (denk aan keyloggers of schermopnameprogramma's).

De browser start automatisch in schermvullende modus, en je kunt via een speciaal symbool weer terugkeren naar de reguliere desktopomgeving. Dat is nogal onpraktisch als je een digitale factuur wilt betalen. Er is ook een virtueel toetsenbord om het online bankieren nog veiliger te maken.





(Klik op een afbeelding voor de download)

Safepay is gratis, afgezien van een hotspotfunctie die je gebruikt als je wilt internetbankieren op een onbeveiligd netwerk buiten de deur. Als je deze premiumfunctionaliteit wilt gebruiken dien je een betaalversie te gebruiken.

Als je echter je overschrijvingen standaard vanaf je thuiscomputer doet, is dit een efficiënt beveiligingsmiddel van een goed aangeschreven beveiliger. Wie Safepay wil gebruiken, zal zich wel moeten registreren, via een Google- of Microsoft-account of via Facebook.

KLM waarschuwt klanten voor phishingmail

Na de banken probeert men nu vat te krijgen middels grote bedrijven.

Luchtvaartmaatschappij KLM heeft klanten van het Flying Blue frequent flyer-programma gewaarschuwd voor phishingmails. Verschillende Flying Blue-deelnemers ontvingen een e-mail waarin werd geadviseerd om het "Air France-KLM account" extra te beveiligen.

Hiervoor moest de ontvanger op een link klikken en inloggen op "het beveiligd Flying Blue-netwerk", zo stond in de phishingmail vermeld. In het geval deelnemers hun gegevens invulden werd hun Flying Blue-nummer en pincode naar de fraudeurs gestuurd, aldus de luchtvaartmaatschappij.

KLM stelt dat dat de e-mail niet door KLM, AIR France of Flying Blue is verzonden. Deelnemers krijgen het advies om de verdachte berichten te verwijderen. In het geval men toch op de link heeft geklikt wordt geadviseerd om het account meteen te controleren.



AIRFRANCE KLM

FLYINGBLUE

Flying Blue-nummer: :

Deelnemers wordt geadviseerd verdachte berichten te verwijderen

Geachte heer

Enkele Flying Blue-deelnemers hebben een e-mail ontvangen waarin geadviseerd wordt het "Air France-KLM account" extra te beveiligen door op een link te klikken en in te loggen op "het beveiligd Flying Blue-netwerk".

Deze e-mail is niet door KLM, AIR FRANCE of Flying Blue verzonden.

Log niet in via deze link. Zorg ervoor dat u zich alleen aanmeldt bij uw Flying Blue-account vanuit de beveiligde Flying Blue-omgeving.

Indien u op een link in de valse e-mail van Flying Blue heeft geklikt, adviseren wij u uw account meteen te controleren. Wanneer u geen toegang heeft tot uw account, wordt u verzocht contact op te nemen met het Flying Blue Service Centre.

Met vriendelijke groet,

Jean-Marc Pouchol
Director Flying Blue

Virus vermomt zich als Google Chrome in Windows register

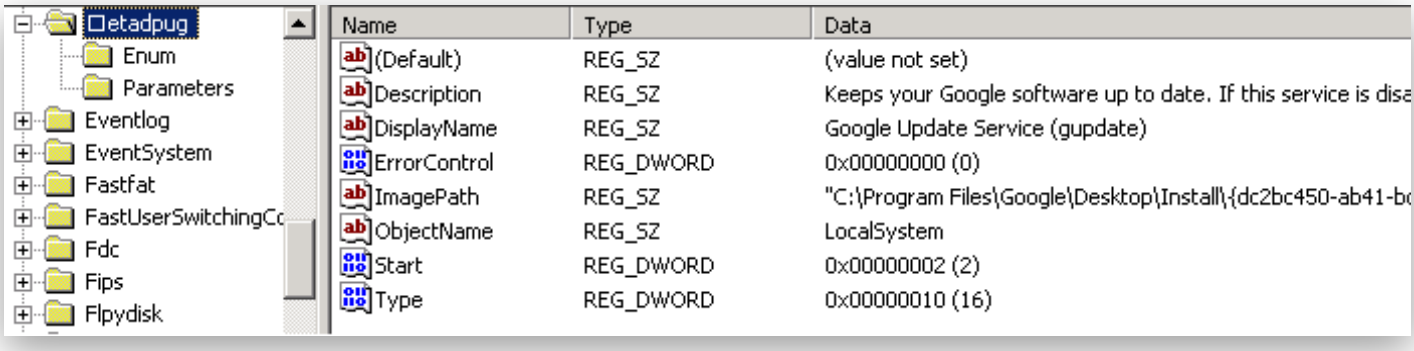


Een truc die cybercriminelen toepassen om malware te verspreiden wordt nu ook gebruikt om de kwaadaardige programma's in het Windows Register te verbergen. Het gaat om de zogeheten RTLO-truc. RTLO staat voor Right-to-Left-Override en zorgt ervoor dat via een speciaal unicode karakter de volgorde van karakters van een bestandsnaam kan worden omgedraaid. Hierdoor wordt SexyPictureGirlAl[RTLO]gpj.exe in Windows als SexyPictureGirlAlexe.jpg weergegeven.

De Sirefef malware gebruikt dit unicode karakter om zich in het Windows Register te verstoppen, waar het zich als een registersleutel van Google Chrome voordoet. Het gaat om de sleutel "gupdate", die identiek lijkt aan de Google Update Service. Wordt de registerwaarde van Sirefef zonder unicode-ondersteuning bekeken, dan wordt de werkelijke naam zichtbaar.

"Dit laat weer een gecoördineerde poging van malware zien om zichzelf in het zicht te verbergen door zich als iets anders voor te doen", aldus Raymond Roberts van het Microsoft Malware Protection Center.





'Onkraakbaar' Tor bouwt anonieme chatclient

De makers van anonimiseringsdienst Tor werken aan instant messaging-software waarmee gebruikers anoniem en veilig kunnen chatten.

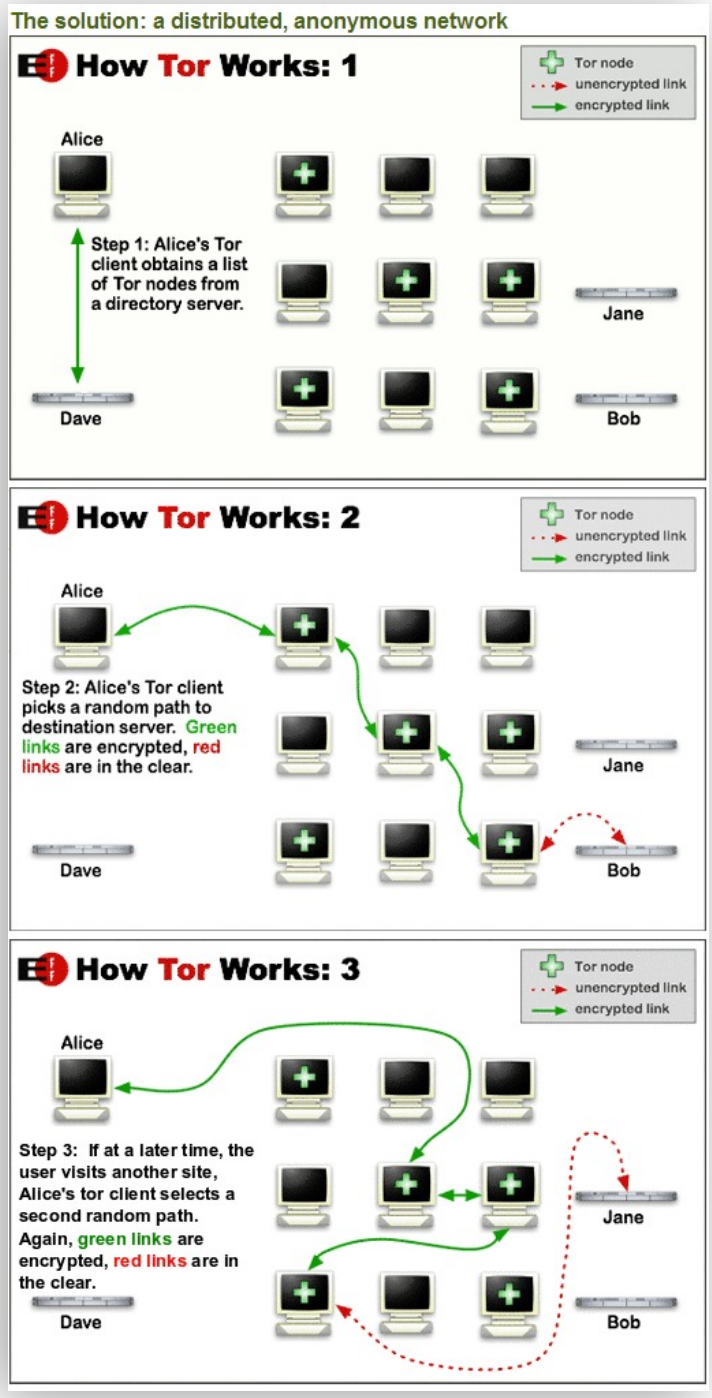
Het Tor-netwerk breidt zich uit met chatten. Tenminste, als het aan de makers ligt. Onder de noemer van project 'Attentive' werkt de 'onkraakbare' anonieme surfdienst aan een eigen chatprogramma. Deze moet aftappen door NSA-achtige instanties onmogelijk maken. Tor mikt qua gebruikers dan ook op activisten die strijden tegen intimidatie, geweld, criminaliteit en corrupte autoriteiten.

Daarbij maakt het chatprogramma gebruik van hetzelfde principe als Tor (The Onion Router), dat anoniem websurfen mogelijk maakt door verkeer via een netwerk rond te pompen. Ook in Nederland weten surfers de dienst inmiddels aardig te vinden. Onderdeel van de Tor-browser

De instant messaging-software zal worden toegevoegd aan de Tor Browser Bundle. Met die bundel is het Tor-netwerk gecombineerd met de Firefox-browser, een oplossing die de lastige installatie en configuratie van Tor vereenvoudigd.

Het project is in juni van dit jaar opgestart. De ontwikkeling van het chatprogramma loopt naar verwachting nog tot mei 2015. Tor-ontwikkelaars over de hele wereld kunnen meedoen. Samen moet gekeken worden welke huidige chatclient als basis kan dienen voor Tor-chat. Er wordt gedacht aan Pidgin en Instantbird.

Het programma krijgt in ieder geval een simpele gebruikersinterface met – naast Engels - ondersteuning in de talen Farsi, Frans, Spaans, en Arabisch.





Welke browser crasht het vaakst



Sauce Labs, een bedrijf dat gespecialiseerd is in het testen van software en internettoepassingen, brengt voor de tweede keer een verslag uit over het aantal crashes van webbrowsers.
Het onderzoeksbureau heeft rapporten bijgehouden van alle crashes op al hun systemen. In de testomgeving speelden tientallen browserversies mee op verschillende besturingssystemen en platformen. Sauce Labs concludeert dat Internet Explorer het vaakst crasht, maar dat is niet het einde van het verhaal.

Internet Explorer is met een foutenmarge van 0,25 % de slechtste geteste browser. Elke browser heeft echter heel wat verschillende versies en sinds IE 7 is de browser van Microsoft aanzienlijk verbeterd.
Terwijl IE 7 nog een foutenmarge van 0,29 % had, heeft de meest recente versie, IE 10, een indrukwekkende foutenmarge van amper 0,05 %.

U vraagt zich ongetwijfeld af welke actuele browser dan het slechtst scoort als Internet Explorer zo aanzienlijk verbeterd is? Het antwoord is Safari 6. De meest recente browser van Apple heeft een foutenmarge van 0,12 %.

De beste browser, in termen van het minst aantal crashes, is Firefox 24. Deze browser van Mozilla wordt op de voet gevolgd door Chrome 27 met een foutenmarge kleiner dan 0,02 %. Internet Explorer 10 heeft een foutenmarge van ongeveer 0,05 % en Opera 12 heeft een foutenmarge van 0,08%.

Sauce concludeert dat Firefox en Chrome de meeste stabiele browsers zijn. In vergelijking met de browsertest uit 2011 blijkt dat de foutenmarges alsmaar blijven dalen.



Gevoelige gegevens onversleuteld in cache van Google Chrome

Google raadt gebruikers aan encryptie te gebruiken, omdat gevoelige op websites ingevoerde gegevens door Chrome onversleuteld worden bewaard.



Beveiligingsbedrijf Identity Finder meldt dat Chrome gegevens die zijn ingevoerd in formulieren op websites, zoals wachtwoorden en creditcardnummers, opslaat in verschillende onversleutelde databases.

Dat gebeurt in kale tekst. De onversleutelde gegevens zijn vervolgens diep in de cache-files op de computer te vinden.

Malware

Iedereen die toegang heeft tot een systeem kan er derhalve naar op zoek gaan. Een aanvaller zou met malware op het systeem de cachebestanden kunnen stelen. Identity Finder ontwikkelde al een proof-of-concept-aanval met malware die dat doet. Op Windows-machines is de data te vinden in de map localappdata\Google\Chrome\User Data\Default\.. De gegevens zijn te verwijderen door Chrome's cache-geheugen te wissen.

Het bedrijf raadt gebruikers dan ook aan elke keer als ze bijvoorbeeld een online aankoop hebben gedaan, direct de cache moeten legen. Ook het uitschakelen van de optie 'Autofill' voor het automatisch invullen van formuliergegevens of het gebruik van de Incognito-modues zou de ingevulde gegevens moeten beveiligen.

Encryptie gebruiken

Google stelt in een reactie dat gebruikers hun lokaal opslagen gegevens het beste met systeemwijde encryptietools kunnen beveiligen. Volgens Google vraagt Chrome wel eerst om toestemming voordat gevoelige gegevens als creditcarddata worden opgeslagen. Chrome OS versleutelt wel standaard alle data die lokaal wordt opgeslagen, aldus Google in een verklaring. "We raden mensen aan om de beveiligingsmaatregelen in hun besturingssysteem te gebruiken."

OM bespreekt cybercrime met jongeren via Facebook



***Het Openbaar Ministerie** (OM) gaat is sinds 10 oktober met jongeren op Facebook over cybercrime aan het discussiëren. Volgens het OM zitten jongeren massaal op het web en komen daar ook vaak in de problemen. "Zij plegen soms zelf strafbare feiten of lopen het risico om slachtoffer te worden."*

Het OM wil dit voorkomen en wil graag van jongeren weten hoe zij tegen cybercrime aankijken en welke ideeën zij hebben voor de aanpak van computercriminaliteit. Vanaf 10 oktober gaat Lodewijk van Zwieten, landelijk officier van justitie op het gebied van cybercrime, een week lang met jongeren via de Facebookpagina van het OM in discussie.
Discussie

De discussies worden gevoerd aan de hand van vijf herkenbare situaties, namelijk het inbreken in computers, het uiten van bedreigingen via social media, heling van gestolen spullen via internet en het online verspreiden van naaktfoto's. De Facebook-discussie is bedoeld voor jongeren van 12 tot 23 jaar.

De jongeren die het actiefst meediscussiëren en met de beste ideeën komen mogen een dag op pad met de landelijk cybercrime-officier. Volgens het OM kunnen de reacties en ideeën van jongeren aanknopingspunten bieden voor de ontwikkeling van maatregelen waarmee cybercrime onder jongeren kan worden voorkomen en bestreden.



Wachtwoord vergeten? Deze tools helpen

Wachtwoord vergeten van Windows, e-mail, FTP of website? Met deze tools is het vaak te achterhalen. Ook beveiligde Word en Excel documenten zijn soms weer te openen.

Windows wachtwoord achterhalen met 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.

Handleiding Ophcrack

Ga naar Ophcrack en klik op Download Ophcrack LiveCD.
Kies het juiste besturingssysteem: XP of Vista (ook voor Windows 7).
Download het bestand. Dit is een - zeer groot - ISO bestand.
Brand het bestand op een CD. Het ISO bestand moet als "image" ge brand worden. Bij de meeste CD/DVD software kies je hiervoor de optie Burn image of Write image.
Start de probleemcomputer op met de gemaakte CD in de CD-speler.
De computer zal opstarten, en een Ophcrack scherm laten zien.
Ophcrack gaat nu automatisch zichzelf installeren, en wachtwoorden zoeken.
Als dat gelukt is wordt het wachtwoord (of meerdere wachtwoorden) getoond.
Neem het wachtwoord over.
Je kan de CD uit de computer halen, opnieuw opstarten en inloggen met het teruggevonden wachtwoord.
Maak direct een wachtwoordherstelschijf.



Wachtwoord vergeten? Deze tools helpen (2)

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.

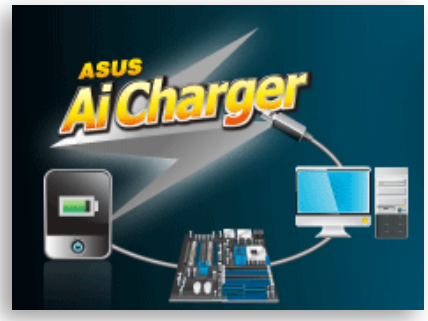
Vergeten wachtwoord van Word en Excel achterhalen

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.



Nieuw in de Schatkist

ASUS Ai Charger:



Tot voor kort was het niet mogelijk om middels uw Usb aansluiting van uw PC, uw iPod, iPhone of iPad fatsoenlijk op te laden. Als het al lukte ging dit zeer traag. Er werd gewoon niet genoeg power geleverd via usb. Dt probleem wordt opgelost door de Ai Charger. Middels dit programma wordt er 50% sneller geladen.

REVO Uninstaller:



Als u een programma wilt verwijderen van uw PC, gaat u normaliter naar het configuratiescherm van Windows en via 'programma verwijderen' wordt u verlost van het betreffende programma. Veelal blijven er dan echter restbestanden op uw pc achter. Dat kan dus beter. Daarvoor gebruikt u Revo Uninstaller. Na het verwijderen van het programma wordt uw PC gescant op achtergebleven restbestanden. Deze kunt u dan alsnog verwijderen.

PC Decrapifier:



**Nieuwe PC of laptop gekocht? Ook zo 'blij' met de voorgeïnstalleerde software en toolbars?
Dit programma verlost u van deze overbodige toegift.**

Blackberry Desktop Software:



Maak volledig gebruik van uw diensttelefoon middels deze softwaresuite. U kunt o.a. Data uitwisselen tussen uw telefoon en uw PC.

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

Wet Computercriminaliteit III

PC Decrapifier

Memorie van Toelichting

Asus Ai charger

Blackberry Desktop Software

Recuva

Bootkit Removal Tool

Format Factory

Twitter handleiding

Revo Uninstaller

UnstoppableCopier



De politie Haarlemmermeer maakt 'opmerkelijk veel gebruik' van twitter, schrijft het Haarlems Dagblad. Agenten Gert Visser en Laura van Bueren hebben een teamaccount, twitteren 'heel breed' – van heterdaadmelding tot preventietip – en zien de 6500 volgers als extra ogen en oren. 'We zitten er direct op en doen een oproep mensen te laten meekijken.' Soms gaat het zo snel dat 'onze afdeling communicatie nog niet eens afweet van de overval'. Visser en Van Bueren zijn tevreden over twitter: 'je hebt snel en prettig contact met burgers'. Toch zien ze ook de nadelen. 'We zijn een politieaccount, dus het is belangrijk hoe je iets op twitter zet'. Gaandeweg hebben ze geleerd wat ze wel en niet kunnen twitteren. 'Met onze afdeling communicatie overleggen we of we iets naar buiten mogen brengen, en zo ja, hoe'. Er zijn meer valkuilen, zoals de verleiding uitspraken te doen over verdachten. 'Soms komen er directe vragen over bepaalde actuele zaken. Vanuit tactisch oogpunt kunnen we niet op alle vragen ingaan, en moeten we soms doorverwijzen naar onze afdeling communicatie.' Dat 'de boefjes ons ook volgen' is niet erg. 'Ze weten precies waar wij de nadruk op leggen, maar wie weet schrikt het ook af'.

Op verzoek van de Kansspelautoriteit blokkeren Facebook en (nu ook) Hyves reclame van illegale aanbieders van kansspelen. Zodra de site daarover melding krijgt, wordt de reclame geblokeerd. Hyves zegt 'haar maatschappelijke verantwoordelijkheid' te nemen; de Kansspelautoriteit spreekt van 'een belangrijke stap' om gokverslaving tegen te gaan. Facebook en Hyves, met respectievelijk acht en twee miljoen actieve gebruikers in Nederland, zijn 'laagdrempelige sociale netwerken' en dus belangrijke partners in deze strijd.

Wereldwijd bedragen de kosten cybercrime tussen de 300 miljard en 1 biljoen dollar per jaar. Dit bedrag, afkomstig uit een gezamenlijk rapport van de Amerikaanse denktank Center for Strategic and International Studies en beveiligingsfirma McAfee, is lager dan in tientallen eerdere rapporten is gesteld. Zo schatte McAfee zelf in 2009 al dat het om één biljoen dollar per jaar ging en herhaalde president Obama dit cijfer enkele malen. Nu roept McAfee, mogelijk ingefluisterd door CSIS en NSA, dat het om veel minder geld gaat. In de VS zou het nu gaan om een bedrag tussen de 24 en 120 miljard dollar – minder dan bij auto-ongelukken. Wat voor invloed cybercrime heeft op het concurrentievermogen van getroffen landen, is nog onbekend, schrijft McAfee.

Onlangs was Trappes, vlakbij Parijs, het toneel van rellen, nadat de politie een vrouw in niqab om een id-bewijs had gevraagd. De politie greep hard in. Op facebook, op het Forum Police-Info, lieten veel collega's zich ongeneerd uit over de rellen. 'Mooi moment voor een grote schoonmaak' en 'neem geen gevangenen' waren nog relatief onschuldige reacties. 'Pas op voor de camera's' adviseerde de ene collega, waar de ander schreef dat het 'met ramadam altijd' fout gaat. Weer een andere collega riep zelfs toch vooral het hele magazijn van de DMP MP7 leeg te schieten. Enfin. Verantwoordelijk minister Manuel Valls van BZK kreeg veel kritiek toen hij geringschattend zei dat mensen niet zo vaak op sociale media moeten kijken en vooral niet alles moeten geloven wat daar staat. Hoe kan een minister anno 2013 nou doen alsof sociale media niet bestaan, vroegen critici.

Blogger

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: (wilt u een magazine opnieuw / alsnog toegezonden krijgen, volstaat een e-mail)

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 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, 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 > Toename 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 mailmalware 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

2013-07/08 > Internetoplichting verschuift naar webshops, Een geautomatiseerd werk, Ransomware dwingt gebruiker tot enquete, Straffen cybercriminaliteit verhoogd in Europa, Hoe wachtwoorden gekraakt worden, Stop je wachtwoorden in een kluis, In 6 stappen buiten bereik van PRISM, Is jouw Ipadres onderdeel van een Botnet, Beveiliginsgtips voor vakantiegangers, Veilig onderweg surfen

2013-09 > Vernielen volgens de Wet Computercriminaliteit, Internettaps verfijfvoudigd, Cloud computing, Cloudopslagdiensten verbinden, Twitter, Aangifte doen van banking trojans, Typosquatting, Cyberpesten, Industriële bestuursystemen hacken, Een 0 voor Security Essentials, Anti-virus test 2013, JonDoNym, Maak bestanden onzichtbaar, De nieuwe Google Maps, Ddos aanval, SOPA

2013-10 > Binnendringen, Sterke stijging politievirussen, Cybercrimineel verkoopt besmette Nederlandse PC,s, Zet foto's smartphonedief niet op internet, Geen wetswijziging voor Stealth-sms, Hackersoftware laat Overheid inbreken, Java besmettingsgevaar neemt toe, Virus vermomt als Google Chrome, Tor bouwt anonieme chatclient, Welke browser crasht het vaakst e.a.