Secure Computing

02 - 2014

W.Bosgra taakaccenthouder Digitale Criminaliteit

Oplichting door nepshops explodeert

Afplakken webcam verstandig

Loterijfraude op Facebook

Internetfraude verdrievoudigd

Harde schijf legen

Telegram veilig?

en meer.....

Microsoft waarschuwt XP-gebruikers via pop-up

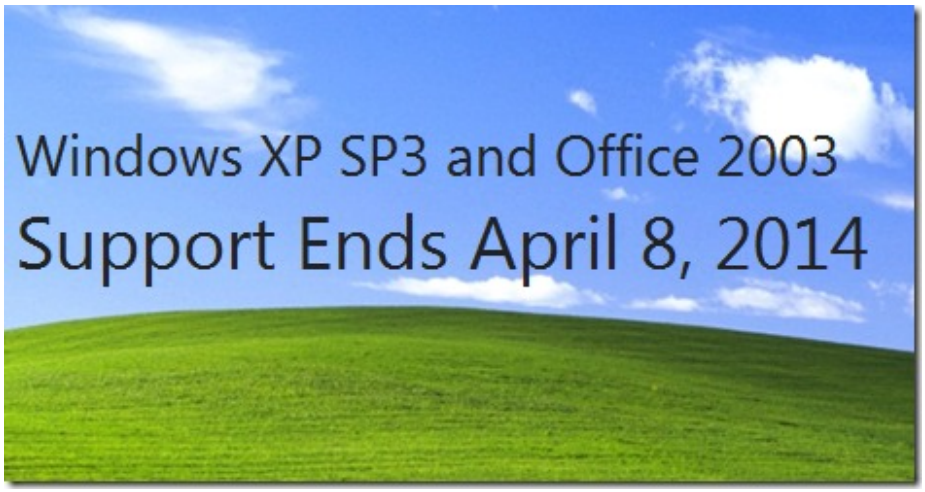
Microsoft zal aanstaande zaterdag 8 maart gebruikers van Windows XP via een pop-up voor het naderende einde van het besturingssysteem waarschuwen. Op 8 april stopt de softwaregigant de ondersteuning van het 12-jaar oude besturingssysteem en zullen er geen updates meer verschijnen.

In de pop-up staat dat de ondersteuning op 8 april 2014 stopt en kunnen gebruikers via een link meer informatie krijgen. De link wijst naar deze website, waar wordt uitgelegd wat het einde van de ondersteuning precies inhoudt en wat XP-gebruikers kunnen doen om te voorkomen dat ze straks zonder updates komen te zitten. Zolang de gebruiker de waarschuwing niet uitschakelt wordt die elke 8ste van de maand opnieuw getoond, aldus Microsofts Brandon LeBlanc op het Windowsblog.

XPocalypse

Het einde van Windows XP wordt ook de XPocalypse genoemd, gezien het grote aantal gebruikers dat nog steeds met Windows XP werkt. Naast consumenten gaat het ook om overheidsinstanties en bedrijven. Volgens de laatste cijfers zou XP nog een marktaandeel van tussen de 17% en 29% hebben. Hoewel organisaties een apart onderhoudscontract kunnen afsluiten, zullen de meeste van deze machines geen update meer ontvangen als er na 8 april een lek in het besturingssysteem wordt ontdekt.

Om XP-gebruikers bij de migratie naar een nieuwer besturingssysteem te helpen biedt Microsoft samen met het bedrijf Laplink een gratis migratietool aan. Deze tool kopieert persoonlijke bestanden, muziek, video's, e-mail en gebruikersprofielen naar een computer die op Windows 7, 8 of 8.1 draait.



Oplichting door nepshops explodeert

Het afgelopen jaar is fraude door malafide webshops verdriedubbeld. Onder meer met een slinkse driekhoekstransactie met iDeal en Bitcoin.

Het afgelopen jaar is fraude door malafide webshops verdrievoudigd. Dat bevestigde de politie vorige week in het tv-programma Meldpunt. Het gaat onder meer om een nieuwe en specifieke variant, die misbruik maakt van iDeal en bitcoin.

Betaalproviders en Bitcoinwisseldiensten nemen extra maatregelen om deze vorm van oplichting de kop in te drukken. De laatste tijd is namelijk sprake van een golf van fraude met nepwebwinkels via iDeal en Nederlandse bitcoinhandelssites zoals Bitonic en BitmyMoney.

'

Gewoon' betalen via iDeal

Het vereist wel enige naïviteit bij slachtoffers, maar is wel sluw opgezet. De iDeal-betaling geeft de zaak de nodige legitimiteit, en door euro's om te zetten naar Bitcoin is de crimineel en zijn frauduleuze geld niet of in elk geval veel moeilijker te achterhalen.

Het slachtoffer wordt naar een legitiem uitziende webshop gelokt, niet zelden via Marktplaats-advertenties. De meeste gevallen gaat het om zeer scherp geprijsde smartphones of computers. De klant bestelt en vermeldt zijn bank, om zo via de iDeal te kunnen betalen. Daarna krijgt de klant echter eerst een 'bevestigingsmail' met daarin een hyperlink naar de iDeal-module van zijn bank.

Bitcointransactie stiekem klaargezet

Ondertussen heeft de crimineel echter een transactie van euro's naar bitcoin naar zijn eigen bitcoinadres klaargezet op bijvoorbeeld Bitonic, BitmyMoney of een andere Nederlandse bitcoinwisseldienst. Deze transacties verlopen gewoon met iDeal. Maar de oplichter voltooit de transactie zelf niet, maar stuurt de link door naar het slachtoffer. Die betaalt dus niet voor een mobieltje, maar voor bitcoins voor de oplichter. Dat is op dat moment voor veel mensen te moeilijk te zien in de iDeal-module. Een voorbeeld van deze truc speelde via prepaid-simyo.com, dat inmiddels uit de lucht is.

De politie is bekend met de driehoekstruc van Bitcoins via iDeal. Het fenomeen valt echter onder het 'reguliere' fraudeonderzoek. Het Team High Tech Crime houdt zich er niet mee bezig.

Internetfraude in Nederland verdrievoudigd

Het aantal meldingen over internetfraude in Nederland is in een jaar tijd verdrievoudigd. De politie doet er niets aan, zegt de Fraudehelpdesk.

Het aantal medlingen van internetfraude is gestegen van 9000 naar 28.000, zegt de Fraudehelpdesk vandaag. Niet duidelijk is waarom de stijging zo groot is, maar wat wel naar voren komt is dat de melders het gevoel hebben dat de politie niets met de aangiftes doet. "En de fraudeurs weten dat", zegt een woordvoerder van de Fraudehelpdesk.

In het overgrote deel van de gevallen (22.000 keer) gaat het om phishingmails die lijken van een bank af te komen. De andere gevallen gaan vooral om oplichting, zoals het winnen van een loterij of een aanbod om mee te doen aan een lucratieve financiële deal. Daarbij wordt dan een voorschot gevraagd aan de ontvanger van de e-mail.

Werkelijke schade tien keer zo groot

De Fraudehelpdesk denkt dat de ontvangen meldingen slechts het topje van de ijsberg is en dat het eigenlijke cijfer tien maal hoger moet zijn. Phishingfraude lijkt steeds minder succesvol, de fraude via datingsites als Facebook blijken moeilijker te herkennen door de betrokkenen.

Grootste slachtoffer die bekend is geworden is een makelaar uit het oosten van het land, die 86.000 euro verloor aan een investering in een miljoenenproject in Zuid-Afrika.

FRAUDE HELPDESK.nl

Loterijfraude op Facebook

Niet alleen in de mail kunt u berichten krijgen dat u de gelukkige winnaar bent van een loterij. Ook Facebook blijkt een terrein voor oplichters die geld proberen binnen te halen met loterijfraude. Dit is een vorm van advance fee-fraude.

Facebookaccount of the Year

Zo is er nu een bericht in omloop waarbij het Facebookaccount van de ontvanger 'willekeurig is geselecteerd' voor de prijs 'Facebook Account of the Year'. Het gaat om een geldbedrag van 1 miljoen dollar.

Voorschot betalen

Om dit geld in handen te krijgen, moet de Facebookgebruiker enkele gegevens doorgeven om de prijs te claimen. Dit betekent niet dat u de prijs gelijk krijgt. Integendeel, er zal worden gevraagd om vergoedingen voor bijvoorbeeld belastingen, juridische kosten en bankkosten. Uiteindelijk raakt u dit geld kwijt en ook het 'gewonnen geldbedrag' krijgt u nooit in handen.

Overigens is het bericht over de Facebook Rewards zeer slecht geschreven. Ook ontbreekt een logo van de netwerksite. Onthou, net als bij phishing, dat slecht taalgebruik een indicatie kan zijn dat het bericht afkomstig is van fraudeurs.

Tips

- Ga niet in op brieven, e-mails of sms'jes over loterijen: gratis loterijen bestaan niet: je kan nooit een prijs winnen als je geen lot hebt gekocht.

- Betaal nooit om een prijs in ontvangst te kunnen nemen: geen enkele rechtmatige loterij stelt dit voor.

Justitie: afplakken webcam heel verstandige zet

Landelijk officier van justitie Cybercrime, Lodewijk van Zwieten raadt alle Nederlanders aan om hun webcam af te plakken. "Een heel verstandige zet."

Justitie wil dat wij allemaal onze webcams afplakken. Lodewijk van Zwieten, landelijk officier van justitie Cybercrime, vindt dat wij niet moeten wachten op fabrikanten van laptops, pc's en andere apparaten met een webcam. Justitie heeft hen namelijk geadviseerd snel met een (fysieke) knop te komen.

Die moet permanent dicht staan wanneer de webcam niet gebruikt wordt. Het kapen van een webcam is volgens Van Zwieten een trend geworden: steeds meer hackers maken misbruik van camera's en microfoons. Dat kan ook omdat er tegenwoordig zoveel apparaten op de markt verschijnen waarbij deze functionaliteit standaard is ingebouwd. Een 18-jarige Rotterdammer stond onlangs voor de rechter die deze software op zeker 2000 computers zou hebben geïnstalleerd, in Nederland en het buitenland.

Zelfs de FBI doet het

Slachtoffers merken doorgaans niets van een webcam-hack. Geavanceerde malware voorkomt dat het indicatielampje gaat branden wanneer de pc-of laptopcamera wordt ingeschakeld. Van Zwieten noemt daarom nu al afplakken "een heel verstandige zet." Eind vorig jaar nog werd duidelijk dat ook de Amerikaanse inlichtingendienst FBI geavanceerde malware inzet waarbij webcams van verdachten ongemerkt worden ingeschakeld.

Zo ziet het eruit als iemand je webcam hackt

Juridische vraag:
kan bedrijf aangifte van ransomware doen?

Recent is een bedrijf getroffen door de Cryptolocker-worm. Alle bestanden zijn nu onbruikbaar geworden, inclusief de back-up op het netwerk. Kan men nu bij de politie aangifte doen? Dit is toch strafbaar als afpersing of zo?

Software zoals Cryptolocker wordt wel ransomware ("gijzelsoftware"). Dergelijke software wist geen gegevens maar versleutelt ze, zodat ze onbruikbaar zijn totdat de juiste sleutel wordt ingevoerd.

De verspreider van deze software geeft de sleutel pas af nadat de eigenaar van de gegevens heeft betaald. De gegevens worden dus als het ware in gijzeling genomen tot het losgeld is betaald. Dit is apart strafbaar gesteld (art. 350a lid 1 Strafrecht), met maximaal 2 jaar cel.

Meestal zal gijzelsoftware worden verspreid via een virus of worm. Dan is deze vorm van malware strafbaar onder art. 350a lid 3, verspreiding van virussen. Dit kan maximaal vier jaar cel opleveren, en bovendien kan de verdachte dan in voorlopige hechtenis worden genomen en mogen dan zwaardere opsporingsmiddelen ingezet worden.

Afpersing is het heel formeel niet, omdat art. 317 Strafrecht eist dat er sprake is van "geweld of bedreiging met geweld" en je kunt veel zeggen van Cryptolocker maar fysiek gewelddadig is het niet.

Juridisch allemaal prima geregeld dus, maar wat heb je hieraan in de praktijk? De criminelen zitten achter Tor en accepteren alleen betaling in anonieme valuta. Hoe spoor je ze op? Hoe ga je ze vervolgen?

Bron: Arnoud Engelfriet ICT jurist

Cryptolocker verwijderen

Cryptolocker is een gevaarlijke ransomware, die duidelijk uitgebracht is door dezelfde groep van cyber criminelen die verantwoordelijk zijn voor het FBI virus, Police Central e-crime Unit virus, Department of Justice virus en vele andere dreigingen. Net zoals de bovenvermelde virussen, blokkeerd Cryptolocker persoonlijke gebruikers bestanden en toont een enorme waarschuwing waarin het vraagt om $300 USD losgeld te betalen. Er zijn echter een paar nieuwigheden aan deze dreiging: Cryptolocker blokkeert deze bestanden met een asymmetrische codering, dit wil zeggen dat je twee sleutels moet kennen om aan je bestanden te raken.. Terwijl de vorige bedreigingen nog konden verwijdert worden door het volgen van specifieke instructies, vind deze dreiging een manier om hier aan te weerstaan. Het lijkt erop dat de enige manier is het verkrijgen van de tweede persoonlijke sleutel die enkel gekend is door de cyber criminelen. Volgens de waarschuwing van Cryptolocker, krijgt de gebruiker maar een bepaalde tijdspanne om het losgeld te betalen en de connectie met zijn bestanden opnieuw te verkrijgen. Anders kan zij/hij 'Vaarwel' zeggen tegen zijn betanden.

Volgens experten wordt, Cryptolocker verspreid door middel van officieel uitziende e-mails. Meestal maken deze melding van een ontbrekende betaling, belastingen, aankopen en gelijkaardige dingen waardoor mensen makkelijk het kwaadaardige bestand openen. Van zodra zo'n bestand geopend is wordt de pc besmet met dit gevaarlijk virus wat onmiddellijk de bestanden van de gebruiker codeert. Typisch voor het virus is dat het bestanden met de volgende extenties zoekt: 3fr, accdb, ai, arw, bay, cdr, cer, cr2, crt, crw, dbf, dcr, der, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, indd, jpe, jpg, kdc, mdb, mdf, mef, mrw, nef, nrw, odb, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, r3d, raf, raw, rtf, rw2, rwl, srf, srw, wb2, wpd, wps, xlk, xls, xlsb, xlsm, xlsx.

Als je denkt dat je pc aangetast is door Cryptolocker, verlies dan geen tijd en volg de volgende handleiding:

In de meeste gevallen kunne gebruikers de connectie met hun bestanden herstellen door System Restore te gebruiken of door een volledige systeemscan uit te voeren met één van deze toepassingen: STOPzilla, SpyHunter, Malwarebytes Anti Malware. Om de systeem blokkering te omzeilen kun je deze stappen volgen:

Herstart je geïnfecteerde PC in 'Veilige modus met opdrachtprompt' om het virus uit te schakelen (dit zou bij alle versies van de dreiging moeten werken)

Start Regedit

Zoek naar WinLogon Waarden en noteer alle bestanden die niet explorer.exe of blanco door explorer.exe.

Zoek in het register naar de waarden die je genoteerd hebt en verwijder de registersleubestanden reffereren.

Herstart je pc en voer een volledige systeemscan uit met een bijgewerkte anti-spyware.

Als dit echter niet werkt voor jou is er een grote kans dat je niet in staat zal zijn om je bestanden te recupereren…

We raden je ten zeerste aan om na te denken hoe zulke infecties te voorkomen. Hiervoor kun je de bovenvermelde programma's gebruiken. Vergeet bovendien ook niet te denken aan de onschendbaarheid van je bestanden en maak een backup. Hiervoor kun je een USB stick, een externe harde schijf, CD's, DVD's, of gewoon simpelweg online backups, zoals Google Drive, Dropbox, Flickr en andere oplossingen gebruiken.

Bewaarplicht internetdata blijkt nutteloos

De bewaarplicht werkt niet en daarom zou die moeten worden uitgebreid. Dat is in het kort de conclusie uit de Evaluatie Wet bewaarplicht telecommunicatiegegevens.

et rapport van het Wetenschappelijk Onderzoeks- en Documentatiecentrum beschrijft in hoeverre de bewaarplicht voor telco's en ISP's van nut is geweest in onder meer rechtszaken. En dat valt tegen.

Vooral de metadata die zijn verzameld over het gebruik van e-mail en websurfen is nauwelijks van nut geweest in de afgelopen jaren. De data zijn vaak te oud, en "daarmee is een situatie ontstaan waarin gegevens van burgers worden bewaard die niet of nauwelijks worden gebruikt door opsporingsdiensten", zo staat in het rapport dat uitgebreid wordt belicht in dit artikel op Computerworld.nl.

Uitbreiding van bewaarplicht is nodig'

Daarom moet de bewaarplicht worden uitgebreid, vinden experts die geciteerd worden in de evaluatie. Nu is de bewaartermijn zes maanden en het moet langer. Dit om te voorkomen dat data alweer zijn verdwenen voordat een onderzoek wordt gestart of in een fase is waar die data belangrijk worden. Ook moeten de data worden uitgebreid met het eindpunt van gesprekken in telefonie en van internetsessies. Daarbij moeten locatiegegevens worden betrokken om mobiele internetsessies ook locatiegericht te volgen.

Internetdata blijken slechts in een aantal gevallen gebruikt te zijn en dan vrijwel alleen in kinderpornozaken. In 26 vonnissen in vier jaar komt het gebruik van die data naar voren. Historische verkeersgegevens van telefonie worden meer gebruikt.

De evaluatie zelf dateert al van 2012, maar verschaft een goed beeld van de eerste jaren praktijk met de bewaarplicht, die in september 2009 in werking trad en sinds begin 2010 wordt geregistreerd. Een evaluatie was afgesproken. Veel documentatie is nagetrokken en er zijn interviews met zo'n 40 personen gehouden. Lees meer op Computerworld.nl: Politie snapt bewaarplicht internetdata niet.

'Politie detecteert spoofing van belgegevens'

Spoofing van telefoongegevens wordt al tien jaar gebruikt en is voor politie en justitie geen onbekend fenomeen. De politie "beschikt over diverse middelen" om spoofing te herkennen.

Dat schrijft minister Opstelten in een brief aan de Tweede Kamer. "Verificatie van telefoonnummers en de gebruiker is een belangrijk onderdeel van een strafrechtelijk onderzoek en dus ook de detectie van spoofing", schrijft Opstelten verder.

Onderzoek naar impact van spoofing

De minister laat een onderzoek doen naar "genoemde aspecten en andere relevante aspecten" die met spoofing te maken hebben naar aanleiding van Kamervragen eind januari. "Rekening houdend met nieuwe technologische ontwikkelingen wil ik met de betrokken instanties inventariseren of de detectie van spoofing voor verbetering vatbaar is. Naar aanleiding van de inventarisatie zal ik bezien of er aanleiding is maatregelen te treffen die eventuele nadelen van spoofing voor strafrechtelijke onderzoeken kunnen ondervangen."

Die inventarisatie, die door het ministerie samen met politie, justitie, telecomproviders en andere betrokkenen wordt gedaan, gaat nog even duren, maar hoe lang vermeldt Opstelten niet.

Manipuleren van afzenderinformatie

Spoofing is het manipuleren van de afzenderinformatie bij e-mailcommunicatie en telefoongesprekken. In dat laatste geval is het met de komst van digitale telefonie alleen maar makkelijk geworden om te doen alsof de beller belt met een ander telefoonnummer dan die in werkelijkheid heeft.

Volgens Opstelten zijn er verschillende diensten die spoofing commercieel aanbieden. Daarvan zou onder meer door criminelen gebruik worden gemaakt, waardoor het aftappen door politie moeilijker wordt.

Overheid staakt Waarschuwingsdienst na ruim 10 jaar

Nog dit jaar verdwijnt de ruim tien jaar oude Waarschuwingsdienst van het Ministerie van Veiligheid en Justitie. De overheid werkt aan een vervangend systeem.

We nemen dit jaar afscheid van de Waarschuwingsdienst van de overheid. De website die informeert over veilig computer- en internetgebruik wordt vervangen door een nieuwe dienst. Die wordt samen met ECP (Platform voor de InformatieSamenleving) opgezet, wat duidt op een privaat-publieke samenwerking. "Niet-professionals en andere overheden zijn nog steeds belangrijk, maar hiervoor worden andere kanalen opgezet", zo laat het Ministerie van Veiligheid en Justitie weten aan Webwereld.

Vitale sectoren

Waarschuwingsdienst.nl alarmeert al sinds 2003 bij computervirussen, wormen en beveiligingslekken en geeft achtergrondinformatie, voorlichting en adviezen over computerbeveiliging. De dienst is opgezet in de tijd dat Govcert.nl de overheid en burgers in Nederland als primaire doelgroep bediende.

Vervolgens is Govcert.nl in 2012 uitgegroeid tot het NCSC (Nationaal Cyber Security Centrum) en is de focus komen te liggen op de Rijksoverheid en de vitale sectoren in Nederland. Ook worden de meer inhoudelijke beveiligingsadviezen via de website van het NCSC beschikbaar gesteld.

Einde in zicht

Dit zorgt er nu voor dat de Waarschuwingsdienst langzaam wordt uitgefaseerd. Dat begon ook al op te vallen: tussen begin oktober en twee dagen geleden is er geen enkele 'actuele dreiging' gemeld. Maar zolang de nieuwe site nog niet actief is zal de Waarschuwingsdienst online blijven om het algemene publiek voor ernstige dreigingen te waarschuwen.

"We verwachten dat er maximaal tien keer per jaar zo'n ernstig bericht verschijnt. Verder worden nog met enige regelmaat inhoudelijke artikelen geplaatst met meer achtergrond. Gezien de verschuiving van de focus is de frequentie hiervan ook lager dan tijdens de GOVCERT.NL periode", aldus woordvoerder Edmond Messchaert van het Ministerie van Veiligheid en Justitie.

Cybercriminelen stelen creditcardgegevens via winkelmandje

Cybercriminelen gebruiken een innovatieve manier om online creditcardgegevens te stelen zonder dat dit wordt opgemerkt. Bij gehackte webwinkels krijgen klanten die de inhoud van hun winkelmandje willen afrekenen kwaadaardige JavaScript-code toegestuurd die in de browser wordt uitgevoerd.

Zodra klanten hun bestelling afrekenen zorgt de JavaScript-code ervoor dat de browser de creditcardgegevens naar een PHP-bestand stuurt. Dit PHP-bestand schrijft de creditcardgegevens vervolgens naar een JPG-bestand, waardoor het lijkt alsof het gewoon om afbeeldingen gaat. Dit moet voorkomen dat de creditcardgegevens worden ontdekt. Daarnaast kan het PHP-bestand de zogenaamde JPG-afbeelding ook verwijderen.

"Nu aanvallers steeds creatiever in het verbergen van hun kwaadaardige activiteiten, is het essentieel dat eigenaren en beheerders van webwinkels weten wat er plaatsvindt op hun servers", zegt Richard Wells van Trustwave SpiderLabs. Hij ontdekte de JPG-bestanden en kon zo achterhalen hoe ze gestolen waren. Wells merkt op dat hij de bestanden bij meer gehackte webwinkels heeft aangetroffen.

Nederlandse tool beschermt Windows en webcam

Het Nederlandse anti-virusbedrijf SurfRight heeft een nieuwe versie van de tool HitmanPro.Alert aangekondigd die over een anti-spionagemodule beschikt om te voorkomen dat gebruikers stiekem via de webcam worden bespioneerd en hun toetsaanslagen worden opgeslagen.

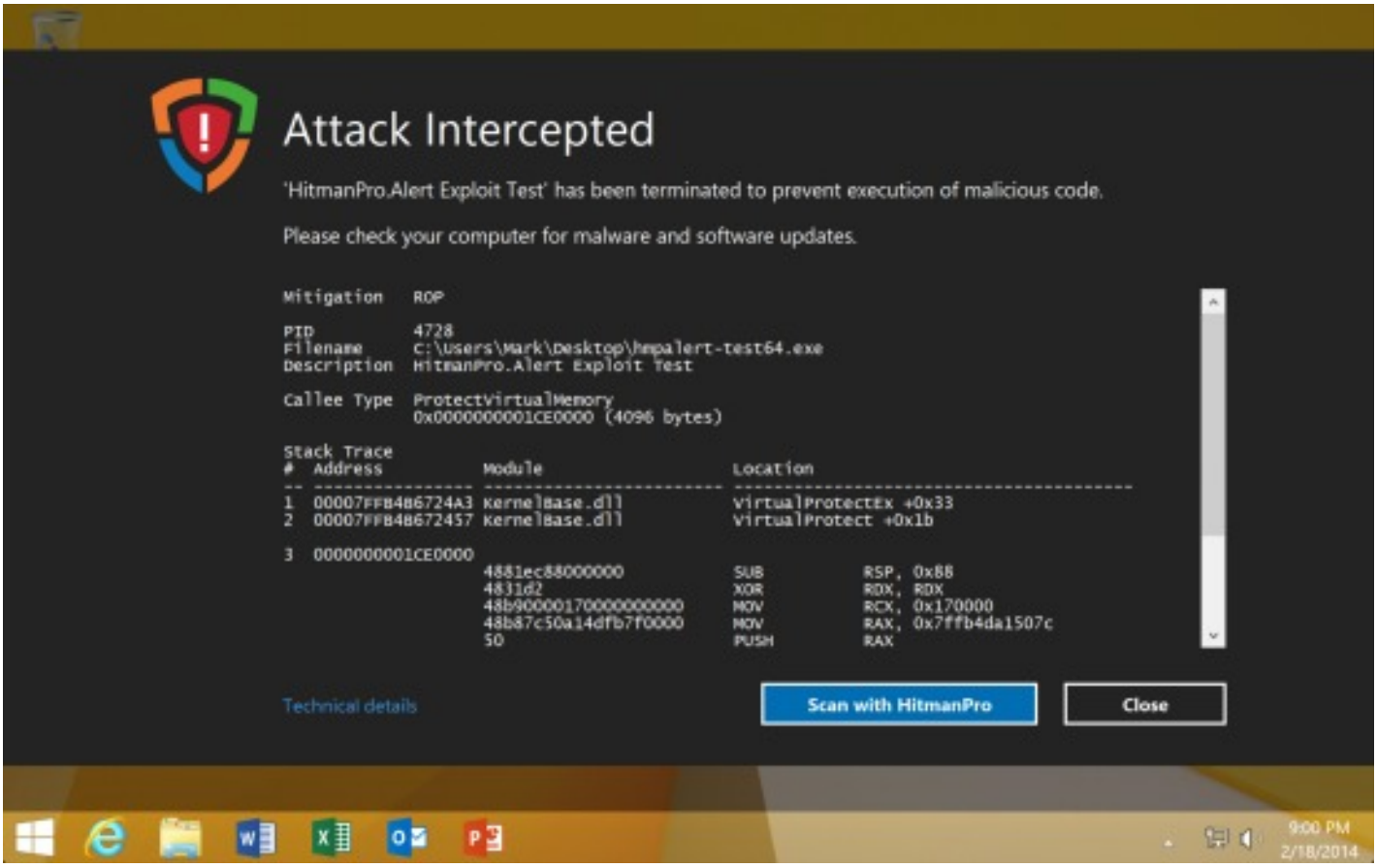
Daarnaast beschermt de tool Windows door misbruik van beveiligingslekken tegen te gaan door allerlei exploits te stoppen, net zoals Microsofts beveiligingstool EMET (Enhanced Mitigation Experience Toolkit) dit doet. HitmanPro.Alert zou zowel tegen misbruik van bekende als onbekende lekken bescherming moeten bieden en doet dat volgens de datasheet van het Nederlandse bedrijf beter en effectiever dan de software van Microsoft. Uit dit filmpje blijkt dat de tool ook aanvallen op het nieuwe lek in IE9 en IE10 herkent en stopt.

"EMET vereist .NET Framework 4 en is daardoor bijna 900MB groot. HitmanPo.Alert 3 is nog geen 3MB en is in C++ geschreven, met stukken in assembler. Onze tool is geschikt voor zowel thuisgebruikers als IT-professionals", laat Mark Loman tegenover Security.NL weten. Net als bij Microsofts EMET is het mogelijk om verschillende beveiligingsmaatregelen per programma in te stellen.

De 'Webcam notifier' in het programma waarschuwt gebruikers zodra een programma de webcam benadert. Deze functie werd toegevoegd naar aanleiding van de zaak met de Rotterdamse tiener die duizenden computers met malware infecteerde en slachtoffers vervolgens via hun eigen webcam bespioneerde, merkt Loman op. HitmanPo.Alert 3 zou vanaf volgende week te downloaden moeten zijn.

Gratis

In eerste instantie werd gezegd dat HitmanPro.Alert een gratis tool is, maar dat klopt niet helemaal. De bescherming tegen keyloggers en CryptoLocker, man-in-the-browser detectie en de waarschuwing bij gebruik van de webcam zijn gratis te gebruiken, maar voor het onderdeel dat bescherming tegen exploits biedt zullen gebruikers een licentie moeten afnemen.



'Veilige' WhatsApp-kloon Telegram verre van veilig

Na de geruchtmakende overname van WhatsApp door Facebook, komen de eerste berichten al binnen over gebruikers die per direct willen overstappen naar een andere berichtendienst. Eén van de veelgenoemde alternatieven is het veiligheids- en privacyvriendelijke Telegram, dat inmiddels steeds meer aan populariteit wint. Maar is Telegram wel echt zo veilig als het pretendeert?

Telegram wordt aangeprezen als een "veilige, versleutelde manier van berichten versturen." In eerste opzicht lijkt de dienst als twee druppels water op WhatsApp, al zijn er enkele opties die verschillen. Zo kun je een "beveiligde chat" beginnen, waarmee de berichten standaard van eind tot eind versleuteld worden, en bovendien kun je instellen of je wilt dat die berichten na een tijdje bij de ontvanger verdwijnen. Ook is het voor de ontvanger niet mogelijk dat bericht door te sturen.

Goede app. Toch?

Telegram lijkt op het eerste gezicht een goede app te zijn. Het werkt goed (en snel, zoals we merkten!), werkt op zowel Android als iOS en er is zelfs een onofficiële desktopversie. Maar is de app wel veilig? Daar verschillen de meningen over. Sowieso is een gratis dienst zonder advertenties dubieus; want waar verdient Telegram zijn geld mee?

Eigen beveiligingsprotocol

En dan is er nog de discussie over de encryptie van Telegram. Het bedrijf heeft namelijk een eigen beveiligingsprotocol opgebouwd. Volgens cryptografie-experts is het extreem onveilig om je eigen protocol te bouwen in plaats van de bestaande te gebruiken.

Zo gebruikt Telegram de SHA1-hash in zijn encryptieprotocol. Dat is een opmerkelijke keuze voor een app die veiligheid zo belangrijk vindt, want SHA-1 staat al een tijdje bekend als een onbetrouwbaar protocol.

Geen TLS

Daarnaast gebruikt Telegram niet het standaard TLS-protocol (zoals WhatsApp), maar een zelfgeknutselde beveiliging. Die zorgt ervoor dat de versleuteling alleen tussen de gebruiker en de server plaatsvindt.

Dat zelfgemaakte protocol is zonder veel moeite te manipuleren, zodat berichten niet bij de bedoelde gebruiker terecht komen maar bij iemand anders.

Man in the middle'

Er is wel de "beveiligde chat", die de berichten wel van eind tot eind versleutelt, maar in die berichten wordt volgens het zelfgemaakte protocol geen authenticatie voor de eindgebruiker gebruikt. Dat betekent dat het heel makkelijk is om op de server een 'Man In The Middle'-attack te plaatsen, waarmee het verkeer kan worden afgeluisterd door hackers of overheidsorganisaties (zoals de NSA). Erger nog, het protocol maakt het mogelijk dat een dergelijke attack niet op te merken is.

Onbekende afkomst

Buiten de zwakke encryptie is ook de afkomst van de app dubieus te noemen. Telegram is namelijk gemaakt door medewerkers van de Russische tegenhanger van Facebook, VKontakte. Zeker omdat er geen direct verdienmodel achter Telegram zit (geen advertenties, gratis), is het maar de vraag wat er met je informatie gebeurt. De app wil namelijk wel toegang tot je adresboek, waardoor het al je nummers heeft. En als de beveiliging echt zo zwak is, is het maar de vraag hoe veilig je gegevens zijn.

Advies: wacht er maar even mee om Telegram als volwaardige vervanger te gebruiken.

Pas op voor drammende 'lover' op Facebook

Facebook is tegenwoordig steeds meer het terrein van datingfraudeurs. Dat merkte ook een getrouwde vrouw van 36 die voortdurend berichten kreeg van iemand die zich voordeed als Bobby Chris(topher). Deze man bestaat helemaal niet, maar is een verzinsel van oplichters.

Weduwnaar

De vrouw kreeg via Facebook een vriendschapsverzoek. De afzender deed zich voor als een Engelse weduwnaar met een 4-jarige zoon. Hij zei te werken in Maleisië. Hij vertelde haar dat ze de vrouw van zijn dromen was. 'Ik hou van je en wil mijn leven met je doorbrengen', vervolgde de 'Engelsman'.

Geen interesse

Al snel vertelde de vrouw dat ze is getrouwd en geen interesse had. Maar hij bleef maar aandringen en dreigde zelfs met zelfmoord. Ook begon hij haar te bellen. De echtgenoot van de vrouw stuurde uiteindelijk een bericht naar 'Chris' dat hij geen contact meer moest zoeken. Het hielp niet, want opnieuw werd er gebeld. Dit keer kreeg hij de man van zijn doelwit aan de lijn. Die had al snel door dat Chris helemaal niet uit Engeland kwam. Toen de oplichter dat te horen kreeg, lachte hij en hing op. De boodschap was blijkbaar overgekomen, want de vrouw heeft niets meer van hem gehoord.

Advies

Wees op uw hoede als u op Facebook een vriendschapsverzoek krijgt. Facebook is voor oplichters namelijk een ideaal middel. Ze kunnen daar precies uitzoeken hoe het leven van hun slachtoffer eruit ziet en er zo op inspelen. Ook zijn Facebookgebruikers minder alert op bedriegers, omdat ze via het sociale netwerk niet op zoek zijn naar een relatie.

Een aantal aanwijzingen waaruit blijkt dat een nieuwe liefde alleen maar uit is op uw geld:

- Hij/ zij dringt erop aan te communiceren via persoonlijke e-mail of chat.

- Hij/ zij uit onmiddellijk zijn gevoelens.

- Hij/ zij stuurt een foto van zichzelf die zo uit een tijdschrift zou kunnen komen.

- Hij/ zij beweert Amerikaans te zijn en in het buitenland te werken.

- Hij/ zij maakt plannen om u te bezoeken, maar is niet in staat om dit te doen vanwege een tragische gebeurtenis.

- Hij/ zij vraagt geld voor bijvoorbeeld een ticket, medisch noodgeval, visa, hotelrekening, ziekenhuisrekening of voor een kind of ander familielid.

Harde schijf legen:
met software, hardware of hamer?

Of je een oude harde schijf nu wil weggooien of doorverkopen: iemand anders mag jouw informatie zeker niet te pakken krijgen. Er zijn drie manieren om dit goed en veilig aan te pakken.

Een verouderde harde schijf die je hebt vervangen door een sneller, nieuwer exemplaar. Een schijf die defect is of die net een keer te veel van je bureau smakte. Die ene harddrive die jij niet meer nodig hebt, maar die je best nog kan doorverkopen.

Of je schijf nu defect is of niet, of je hem nu wil weggooien of doorverkopen: je wil liever niet dat iemand anders jouw al-dan-niet gevoelige informatie te pakken kan krijgen. Laat je dit soort werkjes echter liggen, dan zit je na een tijdje met een hele stapel ongebruikte harde schijven.

Er zijn drie verschillende, veilige manieren t om alle data onherroepelijk van een harde schijf te verwijderen. Met software, met hardware, en met de oervader der hardware: jawel, een hamer.

Software

De goedkoopste, maar helaas niet de snelste manier om die stapel harddrives weg te werken is om er met een software-eraser overheen te gaan. Gebruik een programma zoals het gratis te downloaden Darik's Boot And Nuke.

Installeer het op een wipedisk op je pc, verbindt de harde schijven met je computer en run de software. Wees wel erg nauwkeurig - je wil zo'n eraser niet loslaten op de foute schijf!

Hardware

Een tweede methode die je kan toepassen is het gebruik van een hardwaretool om je schijven schoon te vegen. Je verbindt de harde schijf met het bakje, en met een druk op de knop wordt hij volledig gewiped. Qua gebruiksgemak, snelheid en risicobeperking (je hoeft hiervoor niet je eigen pc te gebruiken) is dit veruit de beste methode. De catch zit hem natuurlijk in de prijs: een apparaatje als de snelle en betrouwbare Wiebetech's Drive eRazer Ultra kost je al snel 250 euro. Een dure zaak dus, maar als je echt een hoop drives hebt om te wissen, dan is het de investering zeker waard.

Die andere hardware

Het nadeel van de vorige twee methodes is dat ze niet werken op defecte schijven - terwijl die wel nog informatie kunnen bevatten - en dat ze veel moeite, tijd of geld kunnen kosten voor schijven die je gewoon wil weggooien. De snelste manier om komaf te maken met overgebleven data is praktisch, en een goede manier om te ontstressen!

Wat heb je nodig? * Een stevige hamer * Een lange, dikke spijker per schijf * Dikke werkhandschoenen, omdat alleen de handigsten onder ons een spijker door een metalen schijf kunnen slaan zonder één vinger te raken * Een stuk hout - om te vermijden dat je de nagel in je vloer slaat * Oogbescherming

Het enige wat je nu nog te doen staat, is een beetje brute kracht gebruiken. Als je de spijker op de juiste plaats door de schijf volledig door de harddrive slaat, verniel je in één klap zowel de disk waarop de informatie staat als de magneetkoppen. De rode X op onderstaande foto duidt de beste plaats aan; als je ook door de twee groene sterretjes een nagel heenslaat, dan kan zelfs de meest paranoïde schijfeigenaar gerust zijn.

Bladwijzers organiseren

Van een favoriete website kun je een bladwijzer maken in de browser. Maar er is meer mogelijk: bladwijzers online opslaan, en synchroniseren tussen verschillende computers.

Bladwijzers synchroniseren

Chrome

De webbrowser van Google bewaart alle favorieten op internet: ze zijn dan vanaf elke computer beschikbaar. Je hebt hiervoor een Google account nodig.

Platform: Windows 8, Windows 7, Vista, XP, Mac, Linux.

Nederlands: Ja.

Gratis: Ja.

Google Toolbar

De Google Toolbar is een balk met extra functies voor Internet Explorer. Hiermee worden de bladwijzers opgeslagen op internet: ze zijn dan terug te vinden op elke computer waarop de Google Toolbar is geïnstalleerd. Google account nodig.

Platform: Windows 8, Windows 7, Vista, 2000, XP met Internet Explorer.

Nederlands: Ja.

Gratis: Ja.

Xmarks

Deze handige plugin bewaart je bladwijzers op internet, en zorgt ervoor dat ze op verschillende computers - bijvoorbeeld thuis en op het werk - gelijk blijven. Het maakt daarbij niet uit welke browser er wordt gebruikt: Xmarks werkt met Internet Explorer, Firefox, Chrome en Safari. De favorieten zijn ook op te zoeken op de Xmarks website, en je kan

Bookmarks opslaan op internet

Bookmax

Mooie online dienst om bladwijzers te organiseren in mappen, en te doorzoeken. Bookmax is zeer overzichtelijk, en synchroniseert je bladwijzers tussen verschillende computers (en verschillende browsers). Je kan er ook contacten in opslaan, en to-do lijstjes aanmaken.

Nederlands: Nee.

Registreren: Ja.

Mister Wong

Overzichtelijke website om bladwijzers te organiseren en te delen met anderen. Toevoegen van links is eenvoudig - via een button in de browser - en je kan favorieten ook importeren. Het is ook mogelijk om de bladwijzers af te schermen van anderen. De website is toegankelijk voor mobiele telefoons. Mister Wong is o.a. beschikbaar in het Engels, Duits, Frans en Spaans.

Nederlands: Nee.

Registreren: Ja.

MyLinkCloud

Mooie online dienst om startpagina's te maken met je favoriete links en apps. Je kan snel meerdere pagina's aanmaken, en links zijn gemakkelijk toe te voegen via een browser plugin. De kleuren van elke pagina zijn aanpasbaar.

Nederlands: Nee.

Registreren: Ja.

Pinterest

Bij deze dienst kun je foto's of video's van websites op een eigen pagina zetten: pinnen. Zo maak je eigen pagina's met je favoriete dingen online. Er wordt automatisch gelinkt naar de oorspronkelijke website. Je kan openbare of privé-pagina's maken, en ook pagina's samenstellen met andere mensen.

Nederlands: Nee.

Registreren: Ja.

Symbaloo

Symbaloo is een persoonlijke startpagina met een indeling in blokjes. Je kan hier ook zelf je favorieten opslaan. Je kan tabbladen aanmaken, direct zoeken in populaire websites, en eigen feeds toevoegen.

Nederlands: Ja.

Registreren: Ja.

Snapshots:

Opgepast voor Whatsapp trojan!

Pas op voor een link die meldt dat de populaire smartphoneberichtendienst Whatsapp eindelijk beschikbaar is voor de PC. Volgens security-expert Kaspersky Lab brengt de link je naar een gehackte server in Turkije die vervolgens een trojan voorschotelt.

Kaspersky Lab waarschuwt voor een zojuist ontdekte Trojan die claimt dat WhatsApp eindelijk beschikbaar is voor de PC en dat de ontvanger reeds 11 verzoeken van vrienden heeft ontvangen. De link in het bericht leidt de gebruiker echter naar een gehackte server in Turkije die vervolgens doorverwijst naar een Hightail (Yousendit) account waar de oorspronkelijke trojan gedownload kan worden. Deze ziet eruit als een 64-bits installatiebestand.

Microsoft verandert naam opslagdienst Skydrive naar Onedrive

Microsoft's cloudopslagdienst Skydrive gaat vanaf nu door het leven als Onedrive. Het computerbedrijf heeft een rechtszaak verloren van de Britse omroep British Sky Broadcasting Group en moest de naam van Skydrive aanpassen.

In een video maakt Microsoft de naamswijziging officieel. De Britse omroep Sky heeft het recht op de term Sky, dus Microsoft heeft de naam Onedrive uitgekozen voor zijn online opslag- en synchronisatiedienst. De naam Onedrive moet volgens Microsoft benadrukken dat de dienst dé plek is voor de opslag van alle documenten en foto's op het internet. In de video benadrukt Microsoft: "voor huidige gebruikers van Skydrive en Skydrive Pro verandert er niks".

Nederlands initiatief moet legaal downloaden makkelijker maken

Het Nederlandse platform The Content Map moet het voor consumenten gemakkelijker maken om via legale bronnen multimedia te kunnen vinden en downloaden. De website biedt links aan naar aanbieders van multimedia. The Content Map is door minister Jet Bussemaker gepresenteerd tijdens het muziekfestival Eurosonic in Groningen. Op de bijbehorende website geven de initiatiefnemers, 'vertegenwoordigers van de creatieve industrie', links naar aanbieders van multimedia. Er worden links gegeven naar onder meer muziek, video, e-books, foto's en games.

De website van The Content Map deelt de media in op de methode waarop ze te verkrijgen zijn. Audio wordt bijvoorbeeld opgedeeld in dowload- en streamingdiensten. E-books zijn opgedeeld in 'te koop' en 'te huur'. Wie interesse heeft in het aanbieden van zijn producten op The Content Map kan een aanbod op de website plaatsen.

Verder bevat de website informatie over het downloaden en het delen van bestanden. De site is duidelijk bedoeld voor mensen met weinig kennis over digitale content en het downloaden van multimedia. De initiatiefnemers hopen vermoedelijk het downloaden uit illegale bron te verminderen.

Apple repareert afluisterlek in iPhone en iPad

Apple heeft een nieuwe versie van iOS voor iPhone, iPad en iPod uitgebracht die voorkomt dat aanvallers beveiligde SSL-verbindingen toch kunnen afluisteren. Het lek zorgde ervoor dat een aanvaller die zich tussen de gebruiker en een website of online dienst bevond, bijvoorbeeld bij een open wifi-netwerk, het verkeer dat met SSL/TLS was beveiligd kon manipuleren of onderscheppen. SSL moet dit juist voorkomen en in het geval van een 'man-in-the-middle-aanval' de gebruiker waarschuwen.

Het probleem werd veroorzaakt doordat Secure Transport de authenticiteit van de verbinding niet controleerde. Apple heeft het probleem opgelost door de ontbrekende controles weer toe te voegen. Voor eigenaren van een iPhone 4 en nieuwer, iPod touch (5e generatie) en een iPad 2 en nieuwer is iOS 7.0.6 beschikbaar. Eigenaren van een iPhone 3GS of iPod touch (4e generatie) kunnen naar iOS 6.1.6 upgraden. Upgraden kan via iTunes en de Software Updatefunctie op het toestel.

Opstelten wil cybercrime effectiever aanpakken

De ontwikkeling van een effectieve aanpak van cybercrime is één van de speerpunten van minister Opstelten van Veiligheid en Justitie. Dat laat de minister in het 'Werkprogramma 2014' van de Inspectie Veiligheid en Justitie' weten. Ook wil Opstelten de cybersecurity in Nederland bevorderen.

De minister heeft voor de periode 2013-2015 de opname en afhandeling van cybercrime door de politie, de aansluiting van de opsporings- en vervolgingsdiensten bij de aanpak van cybercrime en de kwaliteit van beveiligingsadviezen van het Nationaal Cyber Security Centrum (NCSC) centraal gesteld.

De inspectie zal op deze onderwerpen toezien en controleren of datgene wat is afgesproken daadwerkelijk ook is uitgevoerd en of het werkt. Ook zal de inspectie toetsen of de cyberomgeving van burgers adequaat wordt beschermd. Dit moet volgens Opstelten voor een verbetering van de taakuitvoering zorgen en het vertrouwen van burgers in het functioneren van organisaties en instellingen binnen het domein veiligheid en justitie vergroten.

Internetcriminelen komen met een nieuwe IBAN-phishingcampagne gericht op klanten van Nederlandse banken. Een opgerichte nepsite verzamelt persoonsgegevens.

De overgang op IBAN wordt opnieuw aangegrepen om klantgegevens van Nederlandse banken te plunderen. De campagne bestaat dit keer uit een phishingmail en een speciaal opgerichte website. De mail misbruikt de logo's van de Rabobank en ING en is afkomstig van het gespoofte e-mailadres 'overopiban@iban.nl', meldt Security.nl op basis van e-mailbeveiliger MX Lab.

Zelf in actie

De ontvangers worden verleid om zelf in actie te komen. De link in de mail leidt naar een vervalste 'Over op IBAN'-website. Daar wordt na inloggen gevraagd om het invullen van persoonlijke gegevens, waaronder naam, geboortedag, bankrekeningnummer en vervaldatum. Daarmee kan zogenaamd een betaalkaart worden aangevraagd die IBAN ondersteund.

De echte campagnesite van De Nederlandsche Bank (DNB) waarschuwt al langer voor valse e-mails die in omloop zijn. Zij verwijzen daarbij door naar de site Veilig Bankieren waar de veiligheidsregels en enkele voorbeelden van phishingmails staan. De afgelopen twee jaar waren er meerdere malen vervalste IBAN-mails in omloop.

Cops in cyberspace Blog

De politie is op facebook. Maar is het wel de echte? In Sint Willebrord wordt momenteel de naam van wijkagent Wim Mikkers misbruikt: onverlaten hebben op zijn naam een nep-Facebookaccount gemaakt. Op de pagina staat onder meer een oproep om tips over twee andere facebookpagina's te sturen naar een mailadres dat niets met de echte Mikkers te maken heeft. De maker van (een van?) die pagina's noemt zich directeur bij de eenheid Zeeland-West-Brabant. De politie is een onderzoek gestart, aldus woordvoerder Henk Snepvangers. 'We proberen het zo snel mogelijk uit de lucht te krijgen'. Naam en foto van Mikkers zijn inmiddels verwijderd, het profiel is nu van 'Piet Friet'.

HelpWanted.nl, een voorlichtingssite van het Meldpunt Kinderporno, waarschuwt voor afpersers die via chatsites als Omegle en Chatroulette contact proberen te leggen met minderjarige jongens. Ze verleiden de jongens zich voor de webcam uit te kleden, niet om blootfilmpjes te verzamelen maar om ze af te persen. In sommige gevallen hebben slachtoffers al honderden euro's overgemaakt om te voorkomen dat de beelden naar alle facebookvrienden van het slachtoffer worden gestuurd. Volgens Maaike Pekelharing van het meldpunt zijn er sinds oktober al 24 meldingen over deze 'hele nieuwe vorm van online seksueel misbruik' gedaan, allemaal van jongens. En dat is opvallend, zegt Pekelharing en dus reden om te waarschuwen. De werkwijze van de criminelen is iedere keer dezelfde: een leuke jonge Engelssprekende meid legt contact op een chatsite, op Skype gaat de camera aan en 'zij' verleidt hem om bloot te gaan. Direct daarna wordt om geld gevraagd. Maak geen geld over, adviseert Pekelharing. 'En besef dat dit altijd kan gebeuren als je iets voor de webcam doet met iemand die je niet kent. Als je graag webcamseks wil, doe het dan met iemand die je ook in het echte leven kent en vertrouwt'.

In 2013 heeft het Nationaal Cyber security Center 779 incidenten afgehandeld, vooral DDoS-aanvallen op banken. Volgens woordvoerder Edmond Messchaert steeg het aantal incidenten vooral doordat het werkterrein van het NCSC is verbreed. Het centrum publiceerde verder 91 alerts op Waarschuwingsdienst.nl, beantwoordde tachtig adviesvragen en assisteerde 35 keer bij phishing aanvallen op klanten van Nederlandse banken. Het NCSC ziet ook de samenwerking met het bedrijfsleven van vorm veranderen: was het aanvankelijk vooral publiek-private samenwerking, nu verschuift het zwaartepunt meer naar het bedrijfsleven. 'De private sector krijgt meer verantwoordelijkheid, we gaan naar een private participatie waarin kennis onderling wordt gedeeld'. Het NCSC repareerde in 2013 negen keer een veiligheidsrisico in de eigen infrastructuur.

Het Team High Tech Crime meldt dat ze meedeed aan het onderzoek naar supercybercrimineel Aleksandr Panin, ook bekend als het brein achter banking trojan SpyEye. Panin staat in de VS terecht, hij bekende inmiddels schuld. Zijn handlanger Hamza Bendelladj zit ook vast. SpyEye, onder meer aangestuurd door een server bij de Nederlandse provider Ecatel, besmette ongeveer anderhalf miljoen computers in de VS en daarbuiten. Onduidelijk is wat de precieze rol van het THTC is geweest, maar het was wel 'een belangrijke bijdrage' aldus het persbericht. De straf tegen Panin wordt april as uitgesproken.

In Engeland is de twitteraccount van police inspector Michael Brown, bekend vanwege zijn werk op het gebied van politiestress, mentale weerbaarheid en psychiatrische hulpverlening, offline gehaald. Brown, prijswinnend blogger en twitterend als @MentalHealthCop, ligt onder vuur vanwege zijn tweets. In Britse media wordt druk gespeculeerd over de redenen. Brown zou kritiek hebben gehad op een nieuwe plan voor triage waarbij verpleegsters met de noodhulp moeten meerijden om verwarde personen naar huis, de cel of een inrichting te sturen. 'A nurse in a car with a cop' is geen goed idee, vond Brown al eerder. Overigens was het een kwestie van tijd dat Brown in de problemen zou komen met zijn getwitter, schrijft een website. 'The combination of a press-friendly police commissioner with an enthusiasm for social media and a West Midlands police force where information is controlled through firm rules and procedures was always going to be an explosion waiting to happen'.

Een man die op naam van zijn bijna-ex een Facebookpagina opende en daar allerlei naaktfoto's plaatste, is door de voorzieningenrechter in Overijssel verboden dat nog eens te doen. Het stel was eind 2007 getrouwd maar rond kerst 2013 uit elkaar gegaan. De man maakte daarop onder meer een pagina op facebook, op háár naam. Verder benaderde hij haar via Whatsapp. De rechter legde de man voor één jaar een contactverbod op en verbood de man 'zich opnieuw op enige internetsite te registreren onder de naam van eiseres'.

In Engeland moet Jordan Barrack (20) veertig uur 'community service' doen en achthonderd pounds boete betalen omdat hij politieagenten heeft beledigd. Barrack was op een zaterdagavond getuige van een vechtpartij en moest op het politiebureau zijn verhaal doen. Toen hij zat te wachten om gehoord te worden, maakte hij uit verveling wat fotootjes van de dienstdoende agenten. Op die foto's tekende hij met zijn telefoonpennetje wat piemels en vervolgens zette hij zijn kunstwerkjes op Snapchat en Facebook. Police constable Charles Harris zag wat Barrack deed en was 'not amused'. Harris nam de telefoon in beslag en bekeurde Barrack voor 'posting a grossly offensive, obscene picture on a social media site'. De rechter ging daar in mee en legde een straf op.

Onlangsrolde de Nederlandse politie de verborgen internetsite Utopia op. Bij die actie blijken in totaal vijf mannen te zijn aangehouden, meldt het OM. Drie van hen (29, 30 en 31) werden aangehouden in Enschede en Utrecht, de vierde (46) in de gevangenis en de vijfde (21) in Duitsland. De mannen handelden in drugs, wapens, creditcards en munitie. De politie nam bij de verdachten ook 900 bitcoin in beslag, omgerekend circa een half miljoen euro, plus computers, usb-sticks en zelfs de servers waarop Utopia draaide. De verdachten werden achterhaald door undercover-agenten die op Utopia én op Black Market Reloaded xtc, mdma en cocaïne kochten. Toen ze wat coke bestelden, kregen ze te horen dat het ook per kilo kon … De undercover-agenten kregen 'tot hun verbijstering' ook een verzoek om 'iemand naar de andere wereld te brengen'. Bij een ontmoeting met de verdachten werd een aanbetaling voor afpersing en huurmoord gedaan. Volgens het OM is de zaak een 'duidelijke boodschap naar iedereen die denkt misdrijven te kunnen plegen binnen de digitale anonimiteit'. Ook binnen de anonieme Tor-omgeving is niemand onaantastbaar, klinkt het strijdvaardig.