Secure Computing

03 - 2014

W.Bosgra taakaccenthouder Digitale Criminaliteit

Bitcoin special

Bureau voor digitale sabotage

Het Veiligheidscomplex:Bent u groen, oranje of rood

Meldknop.nl

Uw persoonlijke data zijn goud waard

IWork documenten beschermen

Whats app alternatieven

Microsoft Office gratis online

Het Veiligheidscomplex - de film

en meer.....

Bitcoin special

Er wordt veel gespeculeerd over de virtuele valuta Bitcoin. Maar ondanks al het rumoer rondom dit verzonnen geld, hebben veel mensen moeite om te begrijpen wat Bitcoins precies zijn, hoe ze werken, wat de mogelijkheden zijn en welke gevaren er loeren. Tijd voor verheldering dus.

Het is niet per se een slecht idee om je eigen bitcoin wallet te beginnen. Bitcoins zijn niet gebonden aan het wel en wee van de economie van één enkele natie. Ze zijn gemakkelijk in te ruilen, en ze zijn niet aan transactiekosten onderworpen. Maar er zijn een aantal belangrijke dingen die je moet weten voordat je je geld in de Bitcoin-markt stopt. Je moet begrijpen hoe het Bitcoin-systeem werkt en wat de sterke en zwakke kanten ervan zijn.

Bitcoins worden door het volk gecreëerd, verhandeld, en gecontroleerd

Simpel gezegd, een Bitcoin is een op een algoritme gebaseerde wiskundige constructie - een maateenheid die uitgevonden is om waarde te kwantificeren. Het lijkt in die zin een beetje op de dollar - maar in tegenstelling tot de dollar (of enige andere vorm van fiduciair geld) zijn Bitcoins gedecentraliseerd. Het oorspronkelijke Bitcoin-algoritme is gecreëerd door een ontwikkelaar met het pseudoniem Satoshi Nakamoto, maar de munteenheid zelf wordt gecreëerd, verhandeld, en gecontroleerd door Bitcoin-gebruikers, in plaats van een centrale autoriteit zoals een bank of overheid. Bitcoins zijn ook volledig digitaal: Je zult nooit een fysieke Bitcoin in handen krijgen.

Er is ook een beperkte hoeveelheid van de valuta, die beperkt wordt door het ontwerp. Het algoritme dat het Bitcoin-netwerk bevoorraadt is ontworpen om 21 miljoen Bitcoins te genereren, en het systeem reguleert zichzelf automatisch om ervoor te zorgen dat de voorraad Bitcoins in een vlot, gelijkmatig tempo groeit. Tegen 2140 zouden alle 21 miljoen Bitcoins gegenereerd moeten zijn. En omdat het Bitcoin-netwerk elke Bitcoin-transactie volgt en registreert, kun je precies zien hoeveel Bitcoins er op enig moment gecreëerd zijn op Blockchain.info, een website die het Bitcoin-netwerk volgt en Bitcoin wallets host, de containers die eigenaren gebruiken om hun digitale rijkdom in op te slaan.

Een Bitcoin zeepbel

Bitcoin is momenteel groot, waarschijnlijk groter dan goed voor hem is. Aangezien een Bitcoin geen waarde heeft behalve dan wat iemand bereid is ervoor te betalen, verandert de prijs van Bitcoins doorgaans erg snel. Op een bepaald moment was de waarde van één enkele Bitcoin 15 dollar, terwijl een Bitcoin enige tijd later 260 dollar waard was, waardoor mensen die ze op het juiste moment gekocht en verkocht hebben succesvolle beleggers zijn geweest.

De populariteit van de valuta (en daardoor de prijs) neemt toe op internationale markten die instabiel zijn geworden - wanneer bijvoorbeeld een overheid haar burgers bedreigt met kapitaalcontroles en valutarestricties, zoals Cyprus dat heeft gedaan.

"Bitcoin is een enorm volatiel actief, en de recente ontwikkelingen in de prijs van Bitcoins hebben een aantal van de eigenschappen van een economische zeepbel," zegt Professor Magnus Thor Torfason, Assistent Professor Business Administration bij de Harvard Business School.

Torfason is voorzichtig optimistisch over de toekomst van Bitcoin, maar hij zegt dat het moeilijk is om de munteenheid aan te bevelen aan de gemiddelde pc-gebruiker. "Zelfs wanneer we aan zouden nemen dat Bitcoins uiteindelijk tien keer zoveel waard zouden worden als nu, kunnen ze binnen nu en dat moment naar een tiende van hun huidige waarde zakken," zegt Torfason. "We hebben niet echt goede methodes om waarde toe te kennen aan een munteenheid als deze, dus je moet elke investering in Bitcoins beschouwen als een uiterst risicovolle investering."

Je kunt Bitcoins delven, maar de goudkoorts is voorbij

Je hoeft je eigen geld niet op het spel te zetten als je de Bitcoin markt op wilt gaan. In plaats daarvan kun je Bitcoins "delven" door je pc aan het werk te zetten om code op het Bitcoin-netwerk te verwerken. Als je geluk hebt kun je maar liefst 25 Bitcoins verdienen.

Het werkt als volgt: Er worden batches Bitcoins aan Bitcoin-delvers toegekend - mensen die zich aanmelden om een Bitcoin-client op hun pc te installeren en draaien. De client gebruikt CPU en GPU rekenkracht om uiterst complexe wiskundige problemen op te lossen, en deelt deze oplossingen met het hele netwerk. De problemen zijn ontzettend moeilijk op te lossen, en ze bevatten logs van transacties op het Bitcoin-netwerk. Daardoor volgen en verifiëren delvers Bitcoin-betalingen terwijl ze aan de gang zijn.

De eerste client die een blok transacties oplost krijgt een vast aantal Bitcoins - toen Bitcoin begon waren dat er 50 - zodra het werk geverifieerd is door andere clients op het netwerk. Dat vaste aantal wordt elke vier jaar gehalveerd, totdat er op een gegeven moment geen nieuwe Bitcoins meer gecreëerd zullen worden.

De algoritmen die te maken hebben met de productie van Bitcoins zijn veel te ingewikkeld voor de meeste non-cryptonerds om te begrijpen, en daarom gebruiken de meeste mensen de term Bitcoin mining, of Bitcoin delving. Het is vergelijkbaar met het zoeken naar goud in moeilijke omstandigheden. En net als met goud is er slechts een beperkt aanbod van Bitcoins.

Maar in tegenstelling tot goud, komen Bitcoins de wereld binnen in een tempo met zeer weinig variatie. De Bitcoin-algoritmen veranderen dynamisch van moeilijkheid, afhankelijk van hoe vaak er Bitcoins toegekend worden, en dit zorgt voor een vlotte, stabiele stroom van de virtuele munteenheid in het netwerk. Als het delven vermindert zullen Bitcoins eenvoudiger te delven zijn. Als het delven zeer concurrerend wordt - zoals wanneer Bitcoin-delvers investeren in high-end pc's en serverfarms als onderdeel van een rekenkrachtwedloop - wordt het moeilijker om Bitcoins te delven.

"Op een dergelijk moment is het helemaal geen goed idee om Bitcoins te gaan delven," zegt Vitalik Buterin, hoofdauteur bij Bitcoin Magazine. "Je krijgt in principe helemaal niets. De beste manier om dan aan Bitcoins te komen is ze op een beurs te kopen."

Je verdient op zo'n moment waarschijnlijk niet veel Bitcoins via delving tenzij je deel uitmaakt van een delvingsgroep - een groep gebruikers die hun processorbronnen combineren om sneller oplossingen te vinden en te controleren waardoor ze meer Bitcoins verdienen. Er bestaan talloze delvingsgroepen, elk met hun eigen methodes en regels voor het verspreiden van Bitcoin beloningen. Als je in delving geïnteresseerd bent, kies dan een veelbelovende groep uit deze korte lijst met grote Bitcoin delvingsgroepen en neem contact op met de operator van de groep.

De meeste winkeliers accepteren geen Bitcoins

Als je besluit om de sprong te wagen en een aantal Bitcoins op een beurs als Mt. Gox te kopen, dan zul je ze ergens moeten kunnen spenderen. Bitcoin is nog jong, maar de lijst met handelaars die Bitcoins accepteren groeit gestaag naarmate de munteenheid vanwege media aandacht tractie begint te krijgen. Het leeuwendeel van het Bitcoin gebeuren vindt nog altijd online plaats, zoals dat hoort bij een virtuele munteenheid - je kunt Bitcoins uitgeven op Reddit, WordPress, Mega, en WikiLeaks, bijvoorbeeld. Maar bakstenen bedrijven - vooral cafés en buurtwinkels met connecties met voorstanders van Bitcoin - beginnen de munteenheid geleidelijk ook aan te nemen.

Je zult een veel grotere lijst met websites waar je je hard verdiende Bitcoins kunt spenderen op de Bitcoin wiki, en een groeiende lijst met bedrijven die in de echte wereld Bitcoins accepteren.

Bitcoins worden door niemand beschermd of verzekerd

Bitcoin-transacties zijn onomkeerbaar. Zodra een Bitcoin-transactie naar het netwerk wordt verzoden kan deze niet meer worden ingetrokken. Dus een hacker die toegang krijgt tot de pc waarop je Bitcoin wallet staat opgeslagen kan je volledige Bitcoin-fortuin naar een andere wallet sturen - en daar kun je niets aan doen.

Als de pc die je Bitcoin wallet opslaat in bezit is van een derde partij die het tegen diefstal verzekert - bijvoorbeeld een respectabele Bitcoin wallet hostingdienst - kun je misschien de waarde van (een deel van) je gestolen valuta terugkrijgen. Bijvoorbeeld, de gehackte Bitcoin wallet hostingdienst Instawallet heeft haar deuren gesloten in de nasleep van de verwoestende hackaanval, en gebruikers die 50 BTC of minder verloren hadden terugbetaald.

Niemand weet wie Bitcoin echt gecreëerd heeft

De schepper van Bitcoin was een programmeur en liefhebber van cryptografie die op de cryptografie mailinglist communiceerde onder de naam Satoshi Nakamoto. Nakamoto heeft het netwerk ontworpen en Bitcoin gelanceerd in juni 2009, waarbij hij de eerste 50 Bitcoins dolf die iets wat nu het "genesis blok" genoemd wordt gevormd hebben.

Nakamoto is kort daarna verdwenen. Veel journalisten hebben - zonder succes - geprobeerd Nakamoto's echte identiteit te achterhalen, maar tot nog toe blijft het een raadsel wie de stamvader is van de meest succesvolle virtuele munteenheid ooit.

Bitcoins zijn niet de eerste virtuele munteenheid, en ze zullen ook niet de laatste zijn

Bitcoin lijkt de meest succesvolle virtuele munteenheid ooit te zijn, maar het is niet de eerste. Van e-gold tot Beenz tot Facebook Credits hebben mensen meer dan tien jaar lang geprobeerd om levensvatbare virtuele munteenheden te bouwen.

Deze oude virtuele munteenheden zijn om verschillende redenen mislukt. Sommige werden door de overheid tegengehouden vanwege beschuldigingen van het witwassen van geld. Sommige werden door hun eigenaren gestaakt vanwege uitgebreide oplichting. En sommige zijn uitgedoofd toen mensen ze niet langer kochten. Omdat Bitcoin gedecentraliseerd is kan het door niemand worden stilgelegd. Ja, individuele Bitcoin uitwisselingen kunnen door financiële toezichthouders worden tegengehouden - maar omdat niemand Bitcoin runt, kan het alleen maar vanwege gebrek aan belangstelling uitdoven.

Een hacker zou in theorie het Bitcoin-netwerk kunnen vernietigen door met de code te knoeien. Maar in de jaren sinds de oprichting is de Bitcoin code onaangetast gebleven. Individuele gebruikers en beurzen kunnen gehackt zijn, maar de Bitcoins zelf zijn tot nog toe onaantastbaar gebleken.

Daarom staan er een aantal Bitcoin-klonen klaar om de markt te betreden. Van TerraCoin tot Ripple tot PPCoin, er staan genoeg virtuele munteenheden gebaseerd op de open source Bitcoin-code te springen om met elkaar te concurreren voor je echte geld. Tot nog toe is het waarschijnlijk een goed idee voor de meeste consumenten om op veilige afstand te blijven van virtuele valuta: De hevige schommelingen in waarde die Bitcoins zo interessant on te bestuderen maken zouden je de ene dag miljonair kunnen maken en de volgende dag een bedelaar.

Lek maakt iPhone en iPad kwetsbaar voor keyloggers

Door een fout in iOS kunnen hackers elke toetsaanslag op een iPhone of iPad vastleggen, of die nu gejailbreakt is of niet..

Na de heisa over een fout in de SSL-implementatie door Apple, hebben researchers alweer een nieuwe lapsus gevonden in de software van het Californische bedrijf.

Met een nieuwe kwetsbaarheid in iOS kunnen hackers alle toetsaanslagen op iPhones en iPads registreren en doorsturen naar een server.

Het beveiligingsbedrijf FireEye heeft een proof-of-concept gemaakt die, in theorie, op de achtergrond draait en die, zonder dat de gebruiker er weet van heeft, alle toetsenaanslagen opslaat. Het was de site Ars Technica die er het eerst over berichtte.

Jailbreak of niet, maakt niet uit

De fout zit zeker in iOS 7.0.4 en ook in andere versies van het OS, maar daar gaf FireEye geen details over. Ze kan zowel op gewone als gejailbreakte iPhones misbruikt worden. Aanvallers kunnen dit gebruiken om mensen te bespioneren, in hun accounts in te breken, hen een kwaadaardige apps te laten downloaden of om een phishingcampagne op te zetten.

De functie “Ververs apps op de achtergrond” uitschakelen, helpt niet om de kwetsbaarheid te dichten. De enige manier om een aanval te voorkomen, is door de task manager te openen en alle verdachte apps die in de achtergrond draaien, met de hand te sluiten.

Volgens Ars Technica zou FireEye op zijn blog ook gemeld hebben dat het een app aan de App Store had afgeleverd die de fout uitbuitte en dat het met Apple samenwerkte om het probleem aan te pakken. Die boodschap werd echter snel weer verwijderd.

SSL-fout

Apple moest in allerijl een patch uitbrengen om een SSL-fout in iPhones, iPads te dichten. Met de fout stonden de apparaten bloot aan een ‘man-in-the-middle’-aanval. De patch werkt voorlopig echter alleen op mobiele apparaten met iOS. Wanneer de fout in Mac-computers met OS X 10.9 en 10.9.1 wordt opgelost, is nog niet duidelijk.

Bureau voor digitale sabotage

Wij lijken gevangen in een wereldwijd digitaal web, gecreëerd door overheden en Silicon Valley. Hoe blijven wij de baas over onze eigen data? Zijn er wegen om te ontsnappen aan de digitale dystopie?

We leven in de wereld na Edward Snowden. Elke week komen nieuwe onthullingen naar buiten. De communicatie van burgers en consumenten wordt op grote schaal onderschept en in de gaten gehouden. Wij dachten dat de digitale revolutie ons tot communicerende wereldburgers zou maken. Maar nu lijken wij gevangen in een wereldwijd digitaal web. Je smartphone, je bonuskaart, je modem, je DigiD, je medisch patiëntendossier, je zoekvraag, je Facebook account, je sms'en, je verwarmingsthermostaat. Bij elke krantenkop lijkt het net zich verder te sluiten.

De pleister op onze webcam illustreert het: de Big Brothers and Little Sisters komen steeds dichterbij. Tegenlicht kijkt achter de waan van de dag en stelt zich de vraag: hoe blijven wij de baas over onze eigen data? Zijn er wegen om te ontsnappen aan de digitale dystopie? Regisseur Marije Meerman leent de bril van activisten, voorspellers en sciencefiction schrijvers en surft de wereld over op zoek naar digitale ontsnappingroutes en politieke strategieën voor verzet en sabotage. Zijn wij de laatste generatie die privacy en vrijheid als vanzelfsprekend hebben ervaren? Hoe raken we doordrongen van de nieuwe digitale werkelijkheid?

Bekijk de film >>>>>>>>>>

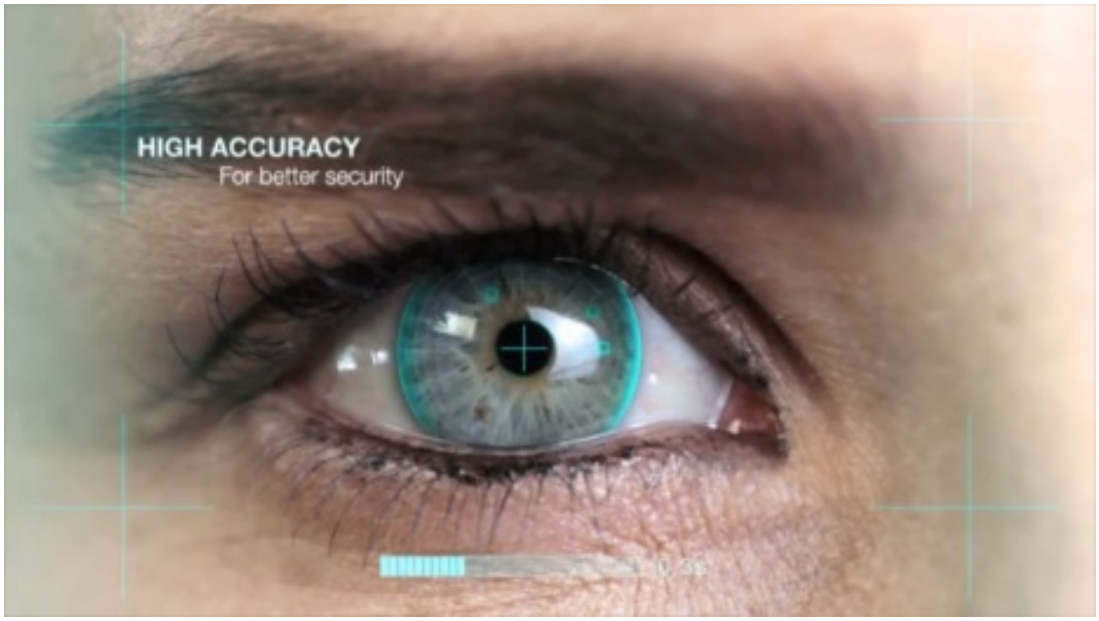
Het Veiligheidscomplex: bent u groen, oranje of rood

Het idee van één Big Brother moet plaatsmaken voor een toekomst/realiteit van vele Little Sisters: een netwerk van surveillancetechnologieën die ons allemaal in de gaten houden en die de wereld indelen in mensen die zich wel vrij over deze planeet mogen bewegen en zij die dat niet mogen.

Met behulp van de nieuwste technieken als drones en de opslag van biometrische gegevens is Europa bezig om een enorme virtuele muur op te werpen tegen de instroom van 'irreguliere' migranten. De drama's met kapseizende bootjes rond het Italiaanse eilandje Lampedusa waarbij vele vluchtelingen verdronken, zijn door Europese politici aangegrepen voor het verder uitbreiden van het controleapparaat. We bouwen tegelijk aan een enorme database waarin alle gegevens worden opgeslagen van alle reizigers die zich door de Schengenruimte bewegen.

Door al deze data te analyseren kan men risicoprofielen bouwen waarmee we straks aan de grens allemaal netjes kunnen worden voorgesorteerd. Bent u groen, oranje of rood, bent u verdacht of heeft u niets te verbergen? En wanneer heeft u niets te verbergen? Het inrichten van dit systeem is uitgegroeid tot een miljardenindustrie die een eigen leven is gaan leiden. De illegale immigrantenretoriek zorgt daarbij voor het geld om het veiligheidscomplex te perfectioneren.

Tegenlicht toog naar het hoofdkantoor van het Europese grensagentschap Frontex, vloog mee met Finse grenswachten in Zuid-Italië en was bij de lancering van een nieuw Europees onderzoeksprogramma tijdens de grote politie- en defensiebeurs Milipol in Parijs. Met o.a. de Franse juriste Claire Rodier, biometriespecialist Max Snijder, de activistische onderzoeker Ben Hayes en wetenschapsfilosoof Huub Dijstelbloem.



Bekijk de film>>>>>>

Uw persoonlijke data zijn goud waard

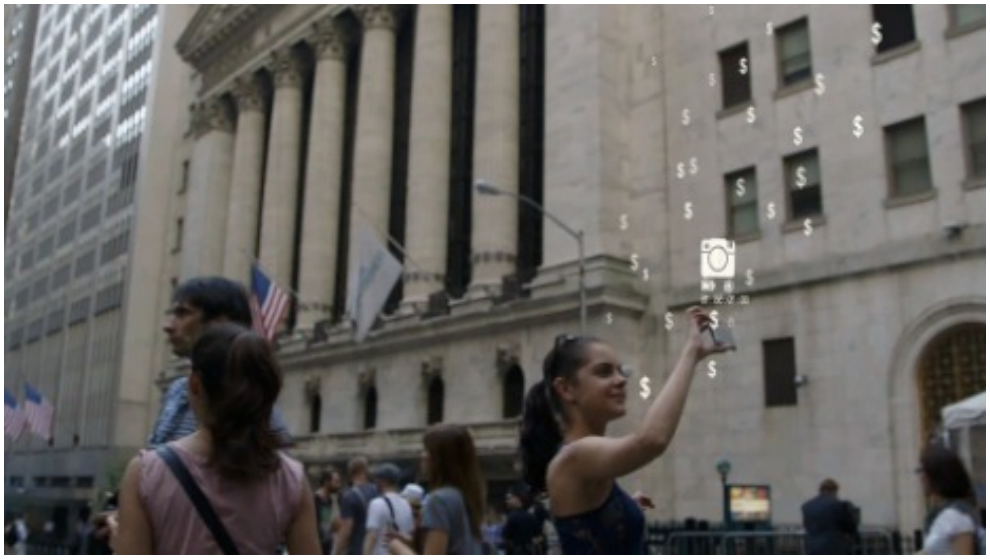
Door enorme informatiestromen kan ons worden verteld wie we vandaag zijn én wat we morgen zullen doen. Kunnen we de controle over onze eigen data nog terug krijgen?

Overal en altijd wordt er informatie over u verzameld en opgeslagen. Via mobiele telefoon en computer wordt elke stap die u zet, bewaard en geanalyseerd. Onder andere door bedrijven als Google, Facebook, Apple en Twitter. Deze persoonlijke data worden niet zomaar bewaard. Er zijn waardevolle nieuwe toepassingen voor, en die zorgen ervoor dat uw persoonlijke data goud waard zijn.

Al die persoonlijke data van u, datacenters vol, zijn het hart van wat Big Data heet. Een schat aan waardevolle nieuwe inzichten, afgeleid uit uw locatiegegevens, e-mails, foto's, sms'jes en wat u nog meer digitaal produceert. Want uw persoonlijke data worden echt niet alleen gebruikt om u op maat gesneden advertenties te sturen.

Uw data worden gebruikt om uw toekomstig gedrag te voorspellen. Door slimme analyses van alle gedragssporen die u achterlaat via uw mobiele telefoon en computer, wordt afgeleid wie u bent. En dat is niet zo moeilijk, blijkt. De Universiteit van Cambridge kan bijvoorbeeld, alleen door te kijken op welke like buttons u klikt op Facebook, zien of uw ouders gescheiden zijn, of u homosexueel bent, en zo verder.

Het voorspellen van menselijk gedrag, mogelijk gemaakt door al uw persoonlijke data, kan helpen om steden beter te ontwerpen, ziektes te bestrijden en oorlogen te voorkomen. Maar als al uw persoonlijke data zo waardevol is, wordt het dan niet eens tijd dat we de controle erover terugkrijgen. En ook zelf een deel van die winst opstrijken?

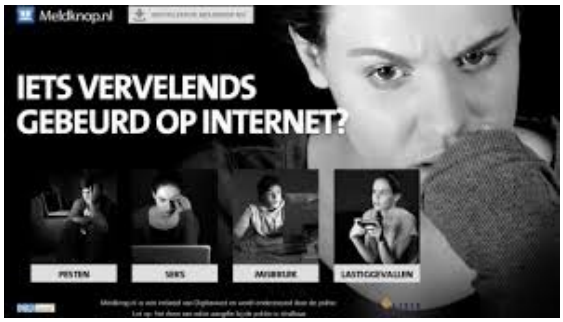


Bekijk de film >>>>>

Eerste hulp online: Meldknop.nl

Twee jaar geleden is Meldknop.nl ingericht. Via Meldknop.nl krijgen jongeren advies over wat zij kunnen doen bij vervelende ervaringen online. De site is gemaakt voor en door jongeren en wordt ondersteund door de politie en andere hulpverlenende organisaties. Ook voor ouders is er veel nuttige informatie te lezen. Inmiddels bezoeken zo'n 100.000 mensen per jaar de site.

Gebeurt er iets vervelends op internet? Dan kunnen jongeren via Meldknop.nl, een initiatief van Digibewust en Helpwanted.nl, meer informatie krijgen over wat ze zelf aan het probleem kunnen doen en indien nodig worden ze doorverwezen naar de Kindertelefoon, Pestweb, HelpWanted.nl, Meldpunt Discriminatie Internet of de Politie (via vraaghetdepolitie.nl) waar jongeren (anoniem) melding kunnen doen en/of advies kunnen krijgen. De website geeft inzicht in wat wel en niet mag en bij strafbare feiten kun je aangifte doen bij de politie.



Marjolijn Bonthuis, verantwoordelijk voor Digibewust, vertelt waarom dit initiatief twee jaar geleden is opgezet: "Uit onderzoek en gesprekken met jongeren merkten we dat er behoefte was aan informatie over hoe zij zelf problemen kunnen oplossen die op internet zijn ontstaan. Natuurlijk kunnen ze ook hulp vragen aan een vriend, hun ouders of een leraar, maar soms willen jongeren het graag zelf oplossen of willen ze anoniem blijven. Als ze zelf op internet gaan zoeken, komen ze vaak ook niet bij de juiste instanties terecht. Er zijn veel verschillende hulporganisaties waar jongeren het bestaan niet vanaf weten. Ook weten jongeren in veel gevallen niet bij welke organisatie ze voor welk probleem terecht kunnen. Wij proberen ze hier bij te helpen door op Meldknop.nl een aantal belangrijke hulporganisaties bij elkaar te brengen en zodanig hun probleem te filteren dat ze bij de juiste organisatie uitkomen voor hulp. Vanaf Meldknop.nl worden jongeren dus doorverwezen naar de organisaties die hen kunnen helpen."

Gebruikers kunnen dus geen klachten doorgeven aan Meldknop.nl zelf. Bonthuis: "Meldknop.nl is een portal. Dat betekent dat jongeren via de site met de juiste hulpverlenende instantie in contact kunnen komen. Het doen van een melding of indienen van een klacht om content offline te halen is vaak slechts deel van de oplossing. Juist het erover praten, weten hoe je ermee om moet gaan et cetera, daar zijn de hulpverlenende instanties, ieder met een eigen expertise, in gespecialiseerd. Naast het offline halen van de betreffende content, kunnen ze jongeren dus veel verder helpen."

Bij de start en ontwikkeling van de site is uitgebreid gesproken met verschillende groepen jongeren over welke problemen ze online hebben en hoe zij dat zelf omschrijven. Want als je wordt uitgescholden om je huidskleur of geloof, is dat dan pesten of discriminatie? De basistip die Meldknop.nl geeft, is dat je vooral over problemen moet praten. Bonthuis: "Als een vriendinnetje een foto van jou op haar Facebook-pagina zet en jij wilt die eraf hebben, dan wordt dat best lastig. We adviseren vooral dat je hier met je vriendin over moet praten. Zeventig procent van alle problemen wordt door de jongeren zelf opgelost."

Bij Meldknop.nl nemen ze de laatste tijd een nieuwe ontwikkeling waar. "Twee jaar geleden was vooral online pesten een groot probleem. Dat is nog steeds zo, maar de problemen rond seksueel lastig gevallen worden, namen vorig jaar substantieel toe. Wellicht komt het door de populariteit van Whatsapp, Snapchat en Instagram, waar vluchtig contact en het uitwisselen van foto's centraal staan. Je bent bovendien vaak overgeleverd aan vaak buitenlandse bedrijven. Daarom is het goed dat er meer druk wordt uitgeoefend vanuit de overheid, ook op Europees niveau, om afspraken te maken over veiligheid maar ook hoe je met elkaar omgaat op internet."

WhatsApp laat Android-gebruikers stiekem chatten

Ook op het meest gebruikte mobiele platform kunnen gebruikers van WhatsApp hun online status afschermen. Maar de laatste Android-update heeft meer.

De populaire chatapplicatie WhatsApp voegt eindelijk het uitschakelen van de veelvuldig gehate 'Laatst gezien'-optie toe. Waar gebruikers van iOS al enkele jaren deze status kunnen verbergen, zodat contacten niet kunnen zien wanneer en of je online bent geweest, moest de Android-gebruiker om onduidelijke redenen lang wachten op de functionaliteit.

Maar de WhatsApp-update voor Android heeft meer privacyinstellingen. Gebruikers kunnen voortaan aangeven wie er toestemming krijgen om je profielfoto en status te bekijken. De opties zijn iedereen, niemand of je enkel je eigen contacten. Een andere nieuwe optie is de widget voor het thuisscherm waar ongelezen berichten verzameld worden. Dit is mogelijk voor Android 3.0 en hoger.

Betalen voor een ander

Opvallend is ook de 'pay for a friend'-service, waarmee je de jaarlijkse kosten van 79 cent ook voor een vriend of vriendin kunt betalen. Tot slot zijn er ook enkele cosmetische aanpassingen gedaan bij de Messenger die recent door Facebook werd opgeslokt. Een overname die inmiddels door privacyorganisaties op scherp is gezet.

iWork-documenten beschermen met een wachtwoord

De iWork-apps kunnen niet precies hetzelfde als de Microsoft Office-programma's, maar je kunt er wel degelijk professionele documenten mee maken. Één groot nadeel was lange tijd dat je de documenten niet kon beschermen met een wachtwoord. Dat is nu voorbij.

Wachtwoorden

Begin dit jaar heeft Apple de mogelijkheid tot het instellen van wachtwoorden toegepast op iWork voor alle platformen. Dat betekent dus dat het niet uitmaakt of je werkt vanaf je iPhone of iPad, je Mac of vanuit je browser, overal waar je werkt met iWork kun je een wachtwoord instellen en dat is natuurlijk wel zo veilig.

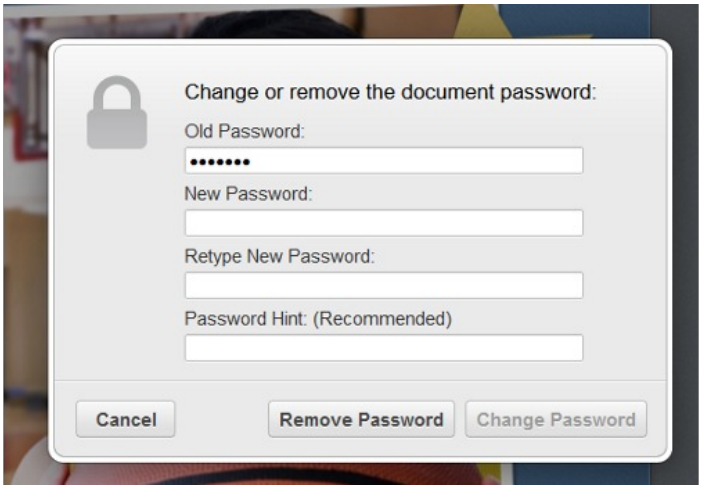
Wachtwoord instellen

We zouden je natuurlijk per afzonderlijk platform kunnen uitleggen hoe je een wachtwoord instelt, maar Apple zou Apple niet zijn als de methode niet voor alle platformen hetzelfde zou zijn. We leggen in dit artikel uit hoe je een wachtwoord instelt in bijvoorbeeld Pages voor iCloud. De methode is dus hetzelfde voor alle iWork-programma's, op alle platformen.

Log in op iCloud en klik op Pages. Open vervolgens het document dat je wilt beveiligen met een wachtwoord (dat kan natuurlijk ook gewoon een nieuw document zijn). Klik nu rechtsboven op het picogram met de waterpomptang en vervolgens op Settings in het menu dat uitklapt (het enige verschil is hier dat iWork voor iCloud in het Engels is, dus in de andere apps zoek je naar de optie Instellingen.

Klik nu op de optie Set password. Typ vervolgens twee keer het gewenste wachtwoord in en daarna een hulpvraag, waarna je klikt op Set password. Het document zal nu met een wachtwoord zijn beveiligd.

Het kan natuurlijk zijn dat je een document met een wachtwoord hebt beveiligd, en later besluit dat je dit wachtwoord toch wilt wijzigen / verwijderen. Dat kan gelukkig ook. Klik op Settings / Set password. Typ bij Old password nu het wachtwoord in dat je hebt ingesteld. Je kunt nu vervolgens een nieuw wachtwoord opgeven en klikken op Change password, of je klikt op Remove password om het wachtwoord helemaal te verwijderen.



Gloednieuwe telefoons en tablets bevatten malware

Een fake Netflix-app is opgedoken op nieuwe smartphones en tablets van Samsung, LG, Asus en Motorola.

Op toestellen van de fabrikanten Samsung en Motorola is in een voorgeïnstalleerde app van Netflix malware opgedoken. Beveiligingsbedrijf Marble Security ontdekte de malware op toestellen van een klant en vond ook tijdens een contra-expertise bij andere klanten de malware terug.

Marble trof de malware aan op de GT-N8013 Galaxy Note tablet, de SGH-1727 Galaxy S III smartphone, the SCH-1605 Galaxy Note 2 phablet, the SGH-1337 Galaxy S4 smartphone, de SGH-1747 Galaxy S III smartphone en de SCH-1545 Galaxy S4 smartphone van Samsung. Ook de Droid Razr, Droid 4 en Droid Bionic van Motorola bleken besmet, evenals de Asus Eee Pad Transformer TF101 en Memo Pad Smart MT301 en LG's Nexus 5 smartphone.

Malwaremakers infiltreren channel

De voorgeïnstalleerde fake Netflix applicatie lijkt echt, maar blijkt aangepast om stiekem wachtwoorden en creditcardinformatie naar Rusland door te sluizen. Ergens in de keten voordat de toestellen aan klanten uitgeleverd worden, zijn malwaremakers erin geslaagd de kwaadaardige software in de meegeleverde applicatiebundel te plaatsen. Waar dat precies gebeurd is en hoe de cybercriminelen te werk zijn gegaan, is nog niet duidelijk.

Microsoft Office gratis online gebruiken

Microsoft Office, de softwaresuite met o.a. Word, Excel en PowerPoint, is een behoorlijk prijzig pakket. Hoewel er vaak van wordt uitgegaan dat iedereen een programma als Word op zijn PC heeft staan is aanschaf van MS Office niet voor iedereen aan de orde.

Gelukkig bestaat er ook een gratis online versie van het pakket. Office Web Apps bevat web-versies van Word, Excel en PowerPoint, plus het databaseprogramma OneNote. De functionaliteit van deze gratis web-software is wat minder dan die van de dure Office software maar alle belangrijke functies zitten er in. En de Office Web Apps zijn volledig compatible met MS Office dus je kunt alle Word, Powerpoint en Excel bestanden gewoon in de Apps lezen en aanpassen.

Office Web Apps is niet alleen gratis, het is software die eenvoudig te gebruiken is. Doordat het volledig webbased is hoef je het niet te installeren en updates hoef je ook niet uit te voeren. Je kunt de Office Web Apps op iedere computer met een internetverbinding en een browser gebruiken. Je hoeft alleen maar in te loggen. Ook de aangemaakte documenten, presentaties en rekenbladen zijn vanaf iedere computer, tablet of smartphone te openen.

Malware-besmettingen via nieuw lek in Microsoft Word

Microsoft waarschuwt gebruikers van Word 2003 en hoger voor een zeroday-gat. Het bedrijf heeft een fix beschikbaar gesteld.

Een exploit voor een verse zeroday bedreigt gebruikers van Microsoft Word 2003, 2007, 2010, 2013, 2013RT, Word Viewer, Office voor Mac, Office Web Apps 2010 en Web Apps 2013. Het gat wordt in beperkte mate het wild misbruikt bij gerichte aanvallen via Word 2010, waarschuwt Microsoft.

Cybercriminelen kunnen malware in systemen pompen via een aangepast RTF-bestand, gehost op een site of bijvoorbeeld als bijlage verstuurd of via een e-mail die wordt voorvertoond met Word. De RTF zorgt ervoor dat het systeemgeheugen gecorrumpeerd wordt, waardoor aanvallers hun eigen code kunnen uitvoeren.

Geen patch, wel fix

Een patch voor de zeroday is momenteel niet beschikbaar, maar gebruikers en bedrijven kunnen een fix toepassen om te voorkomen dat ze slachtoffer worden van een exploit. Ook mitigatietool EMET kan organisaties ellende besparen. Patch Tuesday vindt weer plaats op de dag dat de ondersteuning voor Windows XP stopt, 8 april.

Whats app alternatieven

Telegram

De meeste mensen die Whatsapp verlaten kiezen voor het Russische Telegram. Volgens deze webdienst zelf hebben ze al 800.000 Nederlandse gebruikers. Dat betekent dat veel van je contacten waarschijnlijk al bij Telegram aangesloten zijn. Bovendien is de overstap van Whatsapp naar Telegram eenvoudig omdat beide programma's veel op elkaar lijken.

Telegram is na de overname van Whatsapp door Facebook zo populair dat de webdienst capaciteitsproblemen heeft. Telegram is geheel gratis. Dit in tegenstelling tot Whatsapp dat na het eerste jaar 72 cent per jaar kost.

Line

Line is een Whatsapp alternatief uit Japan. Ook Line is geheel gratis. Geld moet verdiend worden met de verkoop van games en stickers. De gratis software toont geen reclame. Je kunt Line ook op je PC gebruiken. De software heeft 360 miljoen gebruikers.

Een groot voordeel van Line is dat je er ook mee kunt bellen. Het is dus meteen een alternatief voor Skype. Een ander voordeel is dat je je telefoonnummer niet hoeft prijs te geven aan contacten. Deze kunnen je ook via je usernaam benaderen. In Azië is het programma erg populair omdat je je ook kunt abonneren op berichten van beroemdheden. Verder is Line erg leuk omdat het veel emoticons en andere plaatjes kent.

Snapchat

Een ander bekend alternatief voor Whatsapp is Snapchat. Bij Snapchat kun je berichten, chat-gesprekken en video's meteen na het lezen laten verwijderen wat goed voor de privacy is. Helaas werkt Snapchat alleen op telefoons.

KiK

We kikken! Dat klinkt in ieder geval leuk. KiK lijkt sterk op WhatsApp, maar het gebruikt een usernaam in plaats van een telefoonnummer. Ook hier kun je je telefoonnummer dus geheim houden. KiK kun je ook als browser gebruiken. Dat is handig omdat je zo snel links kunt openen die in berichten vermeld worden. KiK heeft 100 miljoen gebruikers.

Tango

Tango werkt op PC's en op iPhones, en op tablets en telefoons met het Android of Windows 7 besturingssysteem. Tango kent veel extra mogelijkheden. Je kunt er niet alleen berichten mee versturen, maar ook filmpjes en foto's. Je kunt er mee telefoneren en spelletjes met anderen mee spelen. Het is zelfs mogelijk om er naar streaming muziek mee te luisteren dankzij een koppeling met Spotify.

Leuk is de mogelijkheid om te zoeken naar Tango gebruikers in je directe omgeving en groepsberichten kun je wel naar tot 50 personen tegelijk sturen.

Threema

Toen Facebook bekend maakte Whatsapp overgenomen te hebben verdubbelde het aantal gebruikers van het Zwitserse Threema in 1 dag naar 400.000. En dat aantal loopt snel op. Dit maakt Threema van een kleine speler tot een belangrijk alternatief voor WhatsApp. En dat terwijl deze software niet gratis is. Al is een eenmalig te betalen prijs van 1,79 euro ook niet duur te noemen.

Threema versleutelt de berichten al bij de verzender zodat zelfs Threema zelf deze berichten niet kan lezen. Ook niet als overheden hier om vragen.

Snapshots:

DigiD-codes per koerier bezorgd in risicogebieden

Woon je in Groningen of Amsterdam Zuid-Oost? Dan wordt je DigiD-inlogcode voortaan per koerier thuisbezorgd. Dit zijn gebieden waarvan bekend is dat criminelen er post onderscheppen. Minister Ronald Plasterk heeft daartoe besloten om fraude met DigiD verder tegen te gaan.

In Amsterdam Zuid-Oost en in Groningen heeft de politie fraude met de DigiD-activeringscodes ontdekt. Daar onderschepten criminelen persoonlijke gegevens van mensen uit de post. Met deze informatie probeerden de ccriminelen een nieuwe DigiD aan te vragen, waarvan de activeringscode vervolgens ook onderschept werd. Het doel van deze actie was om het geld van uitkeringen op een andere rekening te laten storten. In beide gebieden werd de fraude bijtijds opgemerkt door de Belastingdienst, met als gevolg dat in Amsterdam Zuid-Oost en in Groningen nu koeriers worden ingezet.

Strengere regels

Plasterk wil ook dat het nog moeilijker wordt om DigiD-wachtwoorden te kraken. Dat geldt al sinds begin dit jaar gelden voor nieuwe gebruikers strengere regels. Die gaan vanaf mei ook gelden voor bestaande DigiD-gebruikers. Plasterk wil verder onderzoeken of het beter is om activeringscodes helemaal niet meer per post te versturen. Gebruikers zouden dan hun code moeten ophalen bij een gemeentelijke instatie, of deze per koerier thuisbezorgd krijgen.

Betalen met Bitcoins voor kinderporno

In het Verenigd Koninkrijk is een schokkende trend gesignaleerd: handelaars in kinderporno hebben de Bitcoin omgedoopt tot favoriet betaalmiddel. Deze trend werd gesignaleerd door medewerkers van de de Internet Watch Foundation.

De strenge regels voor internetproviders in het Verenigd Koninkrijk hebben volgens de IWF een vervelend neveneffect. De Bitcoin is een uiterst gewild betaalmiddel geworden voor criminelen die kinderporno verkopen. Ze hacken onschuldige websites met een gebrekkige beveiliging en slaan daar digitale beeldbanken op. Het materiaal wordt vervolgens gedeeld en verkocht. Alleen de Bitcoin wordt door deze sites geaccepteerd.

Gehackt

We hebben dit nog niet eerder gezien, dit betaalmechanisme is nieuw voor ons, zegt IWF-onderzoeker Sarah Smith tegen weblog The Register. De sites die worden gehackt zijn vaak van kleine bedrijven en organisaties. De kans dat de beeldbank hier snel wordt ontdekt is het kleinst. Smith verwacht dat deze methode in de toekomst nog vaker zal worden toegepast.

Weinig wetgeving

Dat illegale handelaren Bitcoins als betaling eisen komt mede doordat er nog maar weinig wetgeving is die het gebruik van de Bitcoin als betaalmiddel in goede banen leidt. De opsporing en vervolging van criminelen wordt daardoor bemoeilijkt. Voor de Bitcoin geldt hetzelfde als voor elke andere manier van betalen: een kleine minderheid maakt er misbruik van, aldus Smith.

Apple verhelpt ernstige lekken in iPhone en iPad

Apple heeft een nieuwe versie van iOS uitgebracht waarmee 41 lekken zijn verholpen waardoor iPhone- en iPad-gebruikers op allerlei manieren konden worden aangevallen. Via de kwetsbaarheden was het in het ergste geval mogelijk om willekeurige code op het toestel uit te voeren.

Verder konden websites FaceTime-gesprekken starten zonder dat de gebruiker dit wist, kon een aanvaller met fysieke toegang zonder het opgeven van een wachtwoord Find my iPhone uitschakelen, was het mogelijk om via de autofill-optie gebruikersnamen en wachtwoorden te stelen en bleven de gecachte versies van verwijderde foto's op het systeem staan.

Ook konden kwaadaardige apps de acties van gebruikers bij het gebruik van andere apps monitoren, bleek dat de verplichting dat code gesigneerd was omzeild kon worden, zijn verschillende certificaten uit de lijst met certificaten verwijderd of toegevoegd en was het mogelijk om via een kwaadaardige back-up het bestandssysteem aan te passen.

Een aantal van de lekken is afkomstig van de hackgroep evad3rs, die verschillende jailbreaks van iOS op hun naam hebben staan. Updaten naar iOS 7.1 kan via iTunes en de Software Update-functie. Apple waarschuwt dat het automatische updateproces een week kan duren, afhankelijk van de dag dat iTunes op het apparaat naar updates zoekt.

Assange: mensen hebben geen idee wat er gebeurt

Overheden houden zoveel informatie geheim dat mensen geen idee hebben wat er allemaal gebeurt, aldus WikiLeaks-oprichter Julian Assange. Assange, die zelf nog in de ambassade van Ecuador in Londen vastzit, sprak tijdens het SXSW Festival in Texas via een videoverbinding.

Volgens de Australiër zal over een paar jaar iedereen op aarde in de gaten worden gehouden. Daarnaast houden overheden zoveel informatie geheim dat burgers niet het grotere geheel zien. "We leven in een wereld die we niet begrijpen", vertelde Assange het publiek. Hij noemde het een '"fictieve weergave van de wereld", een illusie waar de werkelijke aard van de machtsstructuren van overheden niet zichtbaar is. "We lopen continu in deze mist rond", merkt hij op

Google en Facebook

Assange haalde verder uit naar Google en Facebook vanwege de grote hoeveelheid data die ze over gebruikers verzamelen. "Wat er plaatsvindt is een ongekende diefstal van rijkdom van een groot deel van de populatie door degenen die al veel macht hebben", antwoordde Assange op een vraag over Facebook en privacy.

"Ze doen het deels door informatie over iedereen te stelen. Kennis is macht en ze verzamelen dus een grote hoeveelheid macht." Ook Google moest het ontgelden, nu er volgens Assange meer dan 1 miljard Android-toestellen in omloop zijn. "Dat is een groot probleem, dat een enkele groep zoveel informatie over mensen kan verzamelen. Jullie zijn allemaal het product."

Door zijn verhaal te doen liet de WikiLeaks-oprichter weten dat hij anderen hoopt te inspireren. "Ik hoop dat het mensen moed geeft, dat je in feite met wat hulp van je vrienden, en door helder na te denken en veel toewijding, je in een positie kunt komen waar je je tegen deze verschrikkelijke...grote machten kunt verzetten. Je kunt ze te slim af zijn, het is mogelijk."

Hoge Raad: politie mag beelden verdachte op internet plaatsen

De Hoge Raad stelt dat het oordeel van het Gerechtshof Amsterdam dat artikel 2 Politiewet 1993 in samenhang met artikel 141 en 142 Sv als wettelijke basis kan dienen voor het tonen van een of meer foto's van de verdachte op internet, juist is. Het tonen van de beelden is niet onrechtmatig en levert geen vormverzuim op als bedoeld in artikel 359a Sv, dat tot bewijsuitsluiting of strafvermindering aanleiding kan geven.

WinRAR-lek maakt spoofen bestandsnaam mogelijk

Een lek in het populaire archiveringsprogramma WinRAR maakt het mogelijk om bestandsnamen te spoofen, wat tot het openen en installeren van malware kan leiden. Het probleem ontstaat door de manier waarop WinRAR met ZIP-bestanden omgaat, zo blijkt uit de uitleg van een Israëlische onderzoeker.

Het ZIP-formaat bevat een veld genaamd 'filename' dat wordt gebruikt voor de bestandsnaam van een uit te pakken bestand in een ZIP-archief. WinRAR voegt bij het maken van een ZIP-archief een tweede veld 'filename' toe en gebruikt dit veld voor de weergave van de bestandsnaam in de WinRAR-gebruikersinterface. Een aanvaller kan het tweede 'filename' veld aanpassen om een bestand in de WinRAR-gebruikersinterface weer te geven, terwijl het in werkelijkheid om een ander bestand gaat.

Daardoor is het mogelijk om de gebruiker te laten geloven dat er in het ZIP-bestand zich bijvoorbeeld een afbeelding bevindt, terwijl dit in werkelijkheid een uitvoer bestand is. De kwetsbaarheid is in ieder geval aanwezig in versie 4.20. Het Nationaal Cyber Security Center (NCSC) laat weten dat de nieuwste versie, 5.01, niet kwetsbaar is. Het NCSC raadt dan ook aan om naar deze versie te upgraden.

XP-malware laat criminelen geldautomaat via sms leeghalen

Malware die geldautomaten met een Windows XP-installatie infecteert maakt het mogelijk voor criminelen om de automaat via het versturen van een enkel sms-bericht leeg te halen. Het gaat om de Ploutus-malware die vorig jaar oktober voor het eerst in Mexico werd ontdekt, maar nu in meer landen actief is.

Twee weken na de ontdekking werd er een nieuwe variant van Ploutus aangetroffen. Deze variant was niet alleen in het Engels vertaald, maar beschikte ook over een modulaire architectuur. Anti-virusbedrijf Symantec heeft deze versie verder geanalyseerd en ontdekt dat criminelen nu ook via het versturen van sms-berichten de geldautomaat kunnen leeghalen.

Aanval

Om de geldautomaat aan te vallen moeten criminelen hier eerst fysiek toegang toe hebben. Vervolgens wordt de geldautomaat vanaf een boot-cd opgestart. Deze boot-cd bevat de Ploutus-malware die tijdens het opstarten het besturingssysteem van de geldautomaat infecteert. Daarnaast schakelt de malware ook de eventueel aanwezige virusscanner uit.Na de installatie is het mogelijk om Ploutus via een speciale toetsencombinatie te activeren en kan er op commando geld worden uitgegeven. Criminelen die katvangers de opdracht gaven om het geld op te halen moesten deze toetsencombinatie delen. Als de katvangers wisten wat er met de toetsencombinatie kon worden gedaan, zouden ze hun opdrachtgever kunnen oplichten, aldus Symantec.

Smartphone

Om dit probleem op te lossen kunnen de criminelen ook een smartphone aan de geldautomaat koppelen. De al geïnstalleerde malware zorgt ervoor dat de crimineel via de smartphone met de geldautomaat kan communiceren. Daardoor hoeft er geen toetsencombinatie meer met de katvanger worden gedeeld. De crimineel kan nu zelf een sms naar de geldautomaat sturen die vervolgens het geld uitgeeft dat door de katvanger wordt opgenomen. De aanvallen zouden inmiddels op verschillende plekken in de wereld zijn waargenomen.

Symantec merkt op dat moderne geldautomaten over betere beveiligingsmaatregelen beschikken, zoals versleutelde harde schijven, die de installatie van de malware kunnen voorkomen. Oudere geldautomaten zouden echter op XP draaien en zijn daardoor nog kwetsbaar. Ploutus werkt bijvoorbeeld alleen op Windows XP. Banken krijgen dan ook het advies om naar Windows 7 of 8 te upgraden. Daarnaast moet de BIOS worden vergrendeld zodat er niet vanaf andere media kan worden opgestart.

Cops in cyberspace Blog

Twitter, politie en 112-meldingen — het blijft een lastige combinatie. Waar de ‘twittercops’ in Nederland op zich een succes zijn – het lost zaken op – blijft het lastig twitter in te zetten als meldkanaal. Dat steeds meer volgers steeds vaker hun meldingen twitteren én niet meer 112 bellen, is geen ‘garantie tot actie’, stelt agent Dirk-Jan Grootenboer uit Dordrecht in het AD: ‘Als ik een melding oppak die binnenkomt via twitter moet ik dat alsnog kortsluiten met de meldkamer.’ Volgens Grootenboer kun je er niet van uit gaan dat agenten alle tweets lezen. ‘Hij is niet 24 uur per dag online, de meldkamer is wel 24 uur per dag bereikbaar’. Niettemin snapt hij de verwarring: de ene twitteraar krijgt te horen dat hij 112 of 0900-8844 moet bellen, de andere twitteraar hoort niks. Weer anderen krijgen via dm het directe nummer van de agent of zelfs bericht dat er direct actie wordt ondernomen. Logisch, zegt Grootenboer, ‘iedere agent is anders en iedere tweet vraagt om een ander soort reactie’. Anderzijds: bewoners zien agenten twitteren over wat ze doen onder werktijd en geven daarom via twitter door wat ze horen en zien. ‘Het lijkt alsof agenten de berichten alleen sturen ter informatie voor volgers’, is dan de kritiek. Grootenboer is begripvol, ‘we gaan graag het gesprek aan’, maar benadrukt de officiële kanalen, al was het maar omdat privacyproblemen te voorkomen én omdat ‘veel zaken te complex zijn om in 140 tekens te bespreken’.

Aangespoord door twitter en andere sociale media gaan steeds meer digitale ramptoeristen op pad om naar incidenten te kijken. Dat is niet zo erg als er een potvis op het strand aanspoelt maar wel als die nieuwsgierigen het werk van hulpverleners belemmeren. In het AD slaat de brandweer alarm. De brandweerkorpsen zien dat het bij branden steeds drukker wordt en dat het aanrijden bij grote incidenten ‘soms lastig is’. Volgens Eric Seugling, voorzitter van het landelijk overleg crisiscommunicatie, komt dat door twitter. ‘De politie houdt toeschouwers op afstand dus er is geen directe overlast maar bij het aanrijden op slecht toegankelijke locaties hebben we soms last van ramptoerisme.’ Voorlichter Hans Coenraads van de brandweer Groningen onderzocht deze nieuwe vorm van ramptoerisme bij incidenten, samen met onderzoekers van VDMMP. De conclusie is dat er meer positieve effecten van dat getwitter zijn dan negatieve. Mensen worden geinformeerd door officiele instanties, er is een kleinere kans op geruchten, je kunt onnodige vragen voor zijn, je kunt waarschuwen voor gevaarlijke situaties én er zijn natuurlijk ook mensen ‘die onze informatie lezen en juist niet gaan kijken’. Uiteraard is wel nodig dat al je al die sociale media goed moet monitoren: om geruchten te ontkrachten, procesinformatie te geven, onzekerheden weg te nemen of onrust te voorkomen. Je kunt bovendien je eigen boodschap verkondigen, bleek al eerder uit het VDMMP-onderzoek ‘Sociale media: factor van invloed op onrustsituaties?’ Daaruit blijkt dat het brandweerverhaal niet uniek is: bij vrijwel elk incident staan foto’s van verdachten of andere betrokkenen, maar ook hun adressen, online. Burgers melden dan dat er ‘opeens’ honderden mensen in de straat staan, omdat een bepaald adres online gedeeld is – zie de zaak Benno L. bijvoorbeeld. Coenraads en Johannink twijfelen over oorzaak en gevolg: wie weet zijn er net zoveel mensen die door de snelle communicatie op een incident afkomen als mensen die beter geïnformeerd zijn en thuis blijven.

Een nieuw wetsvoorstel moet de inzet van lokpubers, agenten die zich op internet voordoen als minderjarigen, weer mogelijk maken. Minister Opstelten heeft het voorstel naar de Raad van State gestuurd voor advies. Vorig jaar verbood de rechter de inzet van lokpubers omdat het in werkelijkheid meerderjarige agenten waren. De nieuwe wet bevat ook maatregelen om computercriminaliteit effectiever aan te pakken. Omstreden is het plan om politie en OM op afstand onderzoek te laten doen in computers van criminelen en die computers ontoegankelijk te maken. Net zo omstreden is het voorstel om verdachten een zogeheten decryptiebevel te geven oftewel om mee te werken aan het openen van versleutelde bestanden op hun computer.