Secure Computing

06-2014

W.Bosgra taakaccenthouder Digitale Criminaliteit

"Beveiligingsexperts waarschuwen voor de opkomst van een nieuw type malware, gericht op het stelen van bank-gegevens. De nieuwe malware kreeg de naam Dyreza, of Dyre, en is even gevaarlijk dan de bekende en vervelende Zeus-trojan."

"Als je regelmatig door dezelfde persoon gestoord wordt, dan kun je ervoor zorgen dat je onbereikbaar bent. Je kunt op de persoon af nummers blokkeren, om zo te voor-komen dat je gestalkt of lastiggevallen wordt."

"Slechts de helft van alle nieuw uitgebrachte malware wordt de eerste dag herkend door virusscanners. Dat zegt beveiligingsbedrijf Last Line Labs. Volgens het bedrijf is antivirussoftware nog steeds nodig voor veel aanvallen, maar is het beter om malware te voorkomen dan te detec-teren."

"Bitcoins zijn geen geld volgens de officiële definitie. Een Nederlandse rechter heeft bepaald dat de virtuele munt niet als officieel betaalmiddel kan gelden, maar enkel als 'ruilmiddel'."

Gevaarlijke nieuwe dief: Dyreza

Beveiligingsexperts waarschuwen voor de opkomst van een nieuw type malware, gericht op het stelen van bankgegevens. De nieuwe malware kreeg de naam Dyreza, of Dyre, en is even gevaarlijk dan de bekende en vervelende Zeus-trojan.

Dyreza gebruikt een zogenaamde man-in-the-middle-aanval om zo normalerwijs versleutelde data te verkrijgen. Bij zo'n aanval wordt je computer voor de gek gehouden. Je systeem denkt dat het een verbinding tot stand brengt met je bankwebsite, maar in werkelijkheid worden je gegevens naar elders verzonden.

Het nieuwe Trojaanse paard onderschept versleuteld verkeer naar onder meer de Bank of Amerika, Citibank, NatWest, RBS en Ulsterbank, weet Computerworld. De malware schiet in actie op het moment dat je browser versleutelde logingegevens via SSL naar de bankserver wil verzenden. De gegevens worden omgeleid naar de eigenaars van Dyreza.

Spam

Hoewel de malware wat werking betreft veel weg heeft van Zeus, gaan onderzoekers ervan uit dat het een volledig nieuw programma is, met code die niet op Zeus werd gebaseerd. Dyreza wordt gedistribueerd in zipbestanden en wordt gehost op betrouwbare servers zoals cubby.com, de opslagdienst van LogMeIn. Links naar de malware worden via spamberichten verzonden.

Het lijkt erop dat de hackers die gebruikmaken van Dyreza een heel netwerk hebben opgezet om het geld wit te wassen en te versluizen. Het is onduidelijk of de criminelen die de malware gebruiken de software ook zelf hebben geschreven. Het zou kunnen dat het programma, naar analogie met Zeus, aan criminelen wordt verhuurd of verkocht.

Je kan je wapenen tegen de malware door up-to-date antivirussoftware te gebruiken en vooral je gezond verstand in te zetten. Open nooit links en bijlagen die je niet vertrouwt, en je bent al voor 90 procent beschermd.

Nederlanders kraken iCloud

Een bende Nederlands-Marokkaanse hackers, opererend onder de naam Doulci, heeft een manier gevonden om de beveiliging van Apple te kraken. Hierdoor kan de vergrendeling van gestolen iPhones in een handomdraai ongedaan worden gemaakt. Nooit eerder werd de iCloud, Apples online opslagdienst met bijna 400 miljoen gebruikers, gehackt.

Volgens de hackers, die schuilgaan achter de pseudoniemen AquaXetine en Merruktechnolog, zijn alleen al de afgelopen paar dagen 30.000 gestolen iPhones ontgrendeld. Vooral Chinese handelaren kopen op eBay en andere grote veilingsites massaal gelockte Apple-apparaten op voor een snelle winst. iPhones worden voor 50 à 150 dollar ingekocht om deze vervolgens in ontgrendelde staat voor $450 à $700 van de hand te doen.

Ook iPhones en iPads die Apple heeft vergrendeld omdat ze tegen zijn regels in door de eigenaar zijn gemodificeerd, zijn nu gemakkelijk van hun slot te ontdoen.

Apple zet alle zeilen bij om het lek in zijn beveiliging te dichten. Volgens Mark Loman, beveiligingsexpert van SurfRight, hebben de hackers een nepcomputer geplaatst tussen de iPhone en de systemen van Apple in de iCloud die toestemming geeft om een mobiel apparaat te ontgrendelen.

Nepcomputer

Deze nepcomputer manipuleert de aanvragen van de iPhone. De telefoon denkt ten onrechte met de echte Apple-server, die onder meer wordt gebruikt voor het activeren van toestellen, van doen te hebben. Loman vreest dat de hackers nog tot veel meer in staat zijn, zoals het lezen van iMessage-berichten.

Beide hackers, waarvan de een in Nederland zit en de ander in Casablanca, hebben vijf maanden aan de hack gewerkt. Ze hebben gekeken hoe de beveiliging van Apple in elkaar steekt en de zwakke plekken ontdekt. Volgens AquaXetine is hun motief niet om geld te verdienen, maar de Apple-gebruiker ervan bewust te maken dat de iPhone en de online opslagruimte iCloud niet al te veilig zijn.

Het steekt hen dat Apple hoog opgeeft van de veiligheid van zijn producten. De hackers zeggen het bedrijf al eind maart op de hoogte te hebben gebracht van het kritische lek. Het bedrijf heeft niet gereageerd. Ook gisteren onthield Apple zich van commentaar.

Ronald Kingma, directeur van Securelabs te Amersfoort, vindt dat onverstandig. „Heel slecht, dat Apple niets van zich laat horen en het lek op deze manier naar buiten moet komen."

Uit een gesprek met de hackers en getoond bewijsmateriaal maakt hij op dat ook de iCloud waar Apple-gebruikers wachtwoorden en persoonlijke gegevens bewaren, in gevaar kan zijn. Zijn advies is dan ook voorlopig deze online opslagruimte niet te gebruiken. Het kan wel enige tijd duren voordat Apple het probleem heeft opgelost.

Apple roept iPhone-adapters terug in Nederland

Apple roept Nederlandse bezitters van oudere iPhone-modellen op hun usb-adapter te laten nakijken. Als het model A1300 is kan deze oververhit raken. Apple vervangt hem gratis.

Het gaat om modellen uit de periode oktober 2009 tot september 2012 die meeverkocht werden bij de iPhone 3GS, iPhone 4 en iPhone 4s. Het modelnummer A1300 is te vinden onderaan de adapter, tussen de pennetjes, op het gedeelte waar je hem in het stopcontact plugt. Apple heeft voor de inruil een speciale website opgezet, met nadere informatie.

iPhone-adapter inleveren

De adapter kan worden ingeleverd bij een Apple Store of een andere officiële Apple-dealer. "Vanaf 18 juni 2014 kunt u ook bij draadloze partners terecht", meldt Apple op de site. Daarmee wordt waarschijnlijk bedoeld dat de adapter ook bij telco's en hun winkels kunnen worden ingeleverd, althans als ze de iPhone in hun assortiment hebben. In Nederland gaat het om Telfort, T-Mobile en Vodafone.

Bron: telegraaf.nl (www.telegraaf.nl/binnenland/22648117/__Nederlanders_kraken_iCloud__.html)

Zo blokkeer je vervelende contactpersonen op je iPhone

Als je regelmatig door dezelfde persoon gestoord wordt, dan kun je ervoor zorgen dat je onbereikbaar bent. Je kunt op de persoon af nummers blokkeren, om zo te voorkomen dat je gestalkt of lastiggevallen wordt.

Om contactpersonen te blokkeren, heb je het nummer van de persoon nodig en moet je deze als contactpersoon in je contactenlijst zetten. Dit is de basisvoorwaarde om alle digitale communicatie met de persoon over je iPhone te verbreken. Het is niet mogelijk om onbekende nummers ervan af te houden je te bellen.

Contacten blokkeren

Om contactpersonen te blokkeren open je Instellingen en scroll je naar beneden naar Telefoon. Selecteer deze optie en kijk onder Gesprekken naar geblokkeerd. Als je deze optie aandrukt zie je Voeg toe... staan. Hiermee open je jouw contactlijst en kun je op naam zoeken naar de persoon die je wilt blokkeren. Tik de persoon aan en voeg deze toe aan de lijst. Je ontvangt nu geen inkomende oproepen, berichten of FaceTime-gesprekken meer van hem of haar.

Je kunt geen onbekende nummers blokkeren.

Juridische vraag:
mag je e-mail zonder toestemming forwarden?

Als ik een e-mail van iemand heb ontvangen, mag ik die dan overhandigen (forwarden) aan derden zonder dat ik de oorspronkelijke afzender daarvoor toestemming heb gevraagd? Ik vraag dit vanwege een juridische procedure waarbij mogelijk e-mails als ondersteunend bewijsmateriaal gaan worden gebruikt.

Een e-mailbericht zal al snel onder het auteursrecht vallen. Daarvoor is niet veel creativiteit nodig; een mail met meer dan "ik zie je morgen" of iets dergelijks triviaals is al beschermd. Op grond van het auteursrecht mag je mail dus niet zomaar doorsturen. Ook niet een deel bij wijze van citaat: citeren mag alleen als het werk gepubliceerd is, en daarvan is geen sprake bij e-mail. (Tenzij het naar een openbare mailinglijst gaat of zo natuurlijk.)

Het briefgeheim wordt ook vaak als argument gehanteerd, maar a) dat geldt niet voor mail en b) de strafwetbepalingen omtrent wederrechtelijke toegang tot mailboxen zijn niet van toepassing op de ontvanger van een mail. Het is ook geen schending van het briefgeheim om een ontvangen papieren brief naar een derde door te sturen.

De privacy kan een rol spelen, afhankelijk van de inhoud van de mail. Een privémailbericht zal naar zijn aard privégegevens van de afzender (of een derde) bevatten, en die doorsturen kan dan een verwerking van persoonsgegevens opleveren. En dat mag alleen met toestemming, of bij een dringende noodzaak die zwaarder weegt dan de privacy van de betrokken persoon. Maar bij een zakelijk bericht (bv. een offerte) zou ik dit geen sterk argument vinden.

Het enige echte excuus dat ik kan bedenken om zonder toestemming een privémailbericht door te sturen, zou zijn als de inhoud zó belangrijk is dat het belang voor de derde-ontvanger om het te weten, zwaarder moet wegen dan het auteursrecht en de privacy van de afzender. Juridisch beroep je je dan op de vrijheid van meningsuiting, die vereist dat deze informatie met derden wordt gedeeld en waarbij dat vereiste zo ernstig is dat je de rechten van de afzender mag negeren. Dat is geen eenvoudige bewijslast.

Bij een gerechtelijke procedure is het eigenlijk altijd toegestaan om dingen als bewijs te overhandigen. In het Nederlands recht wordt bij burgerlijke (civiele) procedures zelden tot nooit iets uitgesloten wegens "onrechtmatig verkregen", dan moeten er wel héél rare dingen zijn gebeurd om het bewijs te krijgen. Enkel dat er onderaan een mail stond "verboden door te sturen" of "deze mail kan vertrouwelijk zijn" is zeker niet genoeg.

Bron: Arnoud Engelfriet ICT jurist

Nieuwe ransomware schakelt dvd-speler uit

"Ter verduidelijking: de ransomware maakt de CD/DVD speler in Windows onklaar zodra de geïnfecteerde user32.dll geladen wordt. Je kunt dus nog gewoon booten van CD/DVD."

Onderzoekers hebben een nieuwe opmerkelijke ransomware-variant ontdekt die zich in een veelgebruikt Windowsbestand verbergt en de dvd- of cd-romspeler uitschakelt om verwijdering via een opstart-cd te voorkomen. Het gaat om een variant van de zogeheten "Department of Justice" ransomware.

Deze ransomware toont een waarschuwing dat de gebruiker de Amerikaanse wetgeving heeft overtreden. Om weer toegang tot de computer te krijgen moet er een bepaald bedrag worden bepaald. In tegenstelling tot veel andere ransomware die een uitvoerbaar bestand op de computer plaatst, infecteert deze variant het veelgebruikte Windowsbestand user32.dll.

Volgens het Nederlandse anti-virusbedrijf SurfRight, dat de ransomware ontdekte, is dit de eerste keer dat ransomware op deze manier een computer infecteert. Eenmaal actief blokkeert de ransomware het opstarten in Veilige Modus, Windows Taakbeheer, de command prompt en Register editor. Acties die ook veel andere ransomware-varianten uitvoeren.

Dvd-speler

Een andere opmerkelijke eigenschap van deze specifieke variant is dat de ransomware de dvd- of cd-romspeler van de computer uitschakelt. Hoe dit precies wordt gedaan laat het antivirusbedrijf niet weten, maar het zou het lastiger maken om de malware van de computer te verwijderen, wat vaak met een opstart-cd wordt gedaan. De ransomware zou al sinds januari van dit jaar rondgaan, maar wordt vooralsnog door slechts 3 van de 54 virusscanners op VirusTotal gedetecteerd.

Hoe de ransomware zich precies verspreidt wordt ook niet gemeld, maar in veel gevallen gebeurt dit via aanvallen op populaire browsers en browserplug-ins die niet door gebruikers zijn gepatcht, het openen van ongevraagde bijlagen of installeren van bijvoorbeeld valse videocodecs en plug-ins of andere geïnfecteerde software.

Advisory kwetsbaarheden internetbankieren

Een nieuw type aanval maakt het mogelijk om misbruik te maken van internetbankieren door bij uitvoeren van transacties bankrekeningnummers aan te passen en in sommige gevallen ook bedragen aan te passen. Op het scherm wordt de transactie getoond, zoals de gebruiker denkt deze uit te voeren waardoor de fraude niet direct opvalt. De aanval werkt op Wifinetwerken, maar is ook toe passen op bekabelde netwerken of via bestaande kwetsbaarheden d.m.v. APT's.

Voor uitvoeren van de aanval wordt een versleutelde verbinding ongedaan gemaakt, waardoor het slotje van de versleuteling niet meer zichtbaar is. Door het icoon van de website een slotje te maken, oogt de site wel versleuteld. Waar https:// zou horen te staan staat vervolgens echter http:// en is de verbinding dus niet versleuteld. Hierdoor kunnen criminelen de informatie die langskomt manipuleren. Hierdoor kan geld worden overgemaakt naar andere rekeningen dan de bedoeling is. Gebruikers die heel oplettend zijn kunnen detecteren dat een aanval plaats vindt, omdat het uitschakelen van de verbinding te herkennen is.

Ook de meeste banken kunnen de aanvallen detecteren in hun systemen, maar dat is pas nadat de betaling is gedaan en de fraude heeft plaatsgevonden. Een oplossing tegen deze aanval is een nieuwe technologie HTTP Strict Transport Security of kortweg HSTS, waarbij zeker wordt gesteld dat de versleuteling tot in de webbrowser werkt en de beveiliging ook echt afdwingt. Momenteel wordt dit nog niet door banken gebruikt, maar in aanloop naar het waarschuwen van het lek is door de meeste banken besloten deze technologie binnenkort te gaan toepassen. Deze techniek wordt ondersteund door de meeste recente versies van Chromium, Google Chrome, Firefox, Opera en Safari. Microsoft Internet Explorer ondersteunt de techniek nog niet, maar verwacht bij de volgende versie dit te gaan ondersteunen.

Adviezen:

- Indien mogelijk vermeid het gebruik van Wifi bij het internetbankieren. Als dat niet mogelijk is doe het dan alleen bij vertrouwde hotspots en controleer of u daadwerkelijk bij het juiste hotspot bent aangesloten. Doe dit bijvoorbeeld door vlak bij het hotspot te gaan zitten, zodat u maximaal ontvangst heeft;
- Stop (voorlopig) het gebruik van Microsoft Internet Explorer;
- Controleer de website van internetbankieren goed, zodat u zeker stelt dat u een versleutelde verbinding gebruikt;
- Wees waakzaam op veranderingen in de website. Om de aanval goed uit te voeren wil een bedrag of een bankrekeningnummer nog wel eens verspringen;
- Controleer regelmaat uw internetbankieren op een andere locatie of er daadwerkelijk correcte transacties zijn uitgevoerd;
- Voer de adviezen op de website Veilig Bankieren (http://www.veiligbankieren.nl/) uit.

Belangrijkste punten:

1. Aanvallers kunnen de versleuteling van internetverbindingen ongedaan maken;
2. Aanvallers kunnen vervolgens internetbankieren manipuleren en zo geld stelen;
3. De aanval kan ontdekt worden aan de kant van de banken en bij de gebruiker die oplettend is;
4. Een nieuwe techniek kan dit misbruik voorkomen.

iPhone-gebruikers melden 'gegijzelde' apparaten

Meerdere Apple-gebruikers melden dat hun iPhones en iPads "gegijzeld" worden door hackers. Die blokkeren de telefoon of tablet van de gebruiker van een afstand. Om de blokkade te verwijderen, moet de gebruiker een flink bedrag overmaken naar de hacker.

Find my iPhone

De gebruikers berichten dat zij een email krijgen via de 'Find my iPhone'-functie. Daarmee kunnen gebruikers hun gestolen of verloren telefoon via internet terugvinden.

De hackers dringen binnen via iCloud en blokkeren de telefoon op afstand en sturen daarvan een melding. Om het apparaat te deblokkeren moet het slachtoffer een bedrag overmaken naar een Paypal-account.

Het is niet duidelijk om hoe veel gebruikers het gaat, en ook niet of er Nederlandse slachtoffers benaderd zijn.

Onnodig

Overigens is het helemaal niet nodig om het 'losgeld' te betalen, want een geblokkeerd iOS-apparaat is ook te unlocken via iTunes. Hoe dat moet is hier te vinden.

Slechts helft van malware wordt binnen twee weken opgemerkt

Slechts de helft van alle nieuw uitgebrachte malware wordt de eerste dag herkend door virusscanners. Dat zegt beveiligingsbedrijf Last Line Labs. Volgens het bedrijf is antivirussoftware nog steeds nodig voor veel aanvallen, maar is het beter om malware te voorkomen dan te detecteren.

Last Line deed het onderzoek door het afgelopen jaar honderden virussen te testen door Virustotal.com. Aan dat platform, dat opgericht is door Google, werken 47 antivirus- en beveiligingsbedrijven mee.

Net de helft

Met de site keken de onderzoekers naar hoe snel de antivirusmakers reageerden op de bedreigingen. In slechts 51% van de gevallen werd malware de eerste dag opgepikt door de virusscanners. In sommige gevallen duurde dat 2 dagen, maar na 2 weken wist slechts 61% van de programma's de malware te ontdekken.

Voorkomen beter dan genezen

Een tijd geleden maakte antivirusmaker Symantec al bekend te stoppen met antivirussoftware. Volgens het bedrijf is het vechten tegen de bierkaai, en is het beter om malware te voorkomen dan te detecteren. Een virusscanner op je pc is vaak niet meer genoeg, dus blijf alert op welke emails je opent en welke websites je bezoekt.

Bitcoin is geen officieel betaalmiddel

Bitcoins zijn geen geld volgens de officiële definitie. Een Nederlandse rechter heeft bepaald dat de virtuele munt niet als officieel betaalmiddel kan gelden, maar enkel als 'ruilmiddel'.

Hoewel de munt veel overeenkomsten vertoont met echte valuta, zijn er ook grote verschillen waardoor Bitcoins niet dezelfde rechtsgeldigheid hebben als de euro, de dollar of de yen.

Niet van giro-instelling

Het voornaamste verschil zit 'em in het feit dat de Bitcoin in een portemonnee zit die eigendom is van de gebruiker zelf, in plaats van van een giro-instelling als een bank. Daarvoor staat de Nederlandsche Bank garant, dat is bij de Bitcoin niet het geval. Ook het feit dat de Nederlandse staat de Bitcoin niet als geldige valuta zit, telt mee.

Compensatie

De uitspraak werd gedaan naar aanleiding van een rechtszaak die in augustus 2012 begon. De man die werd aangeklaagd wilde toen 2,750 Bitcoins verkopen voor minder dan een tientje per stuk, maar leverde uiteindelijk veel minder dan dat. Toen de prijs van de Bitcoin kort daarna als een raket omhoog schoot, vond de aanklager dat het tijd werd een schadevergoeding te vragen van de man, omdat hij daardoor veel geld was misgelopen.

Koersstijging

De aanklager wilde 100,000 euro als vergoeding hebben, ter compensatie van de koersstijging. De rechter oordeelde echter dat de man wel recht heeft op schadevergoeding, maar omdat de Bitcoin geen echte valuta is hoeft die koersstijging niet meegerekend te worden.

Opsporingsdiensten bezorgd over Bitcoingebruik criminelen

"Een aantal maanden geleden werd het bedrijf Liberty Reserve opgerold, dat volgens de autoriteiten met een eigen virtuele munt 6 miljard dollar zou hebben witgewassen."

"Het Openbaar Ministerie heeft onlangs beslag moeten leggen op een hoeveelheid bitcoins die door een xtc-bende uit Groningen en Drenthe was verdiend. De virtuele munten waren afkomstig uit de handel in harddrugs."

Het gebruik van Bitcoin en andere digitale valuta door criminelen vormt een steeds grotere uitdaging voor opsporingsdiensten, daarom kwamen deze week meer dan 71 opsporingsfunctionarissen uit 21 landen samen in het hoofdkantoor van Europol in Den Haag om over deze problematiek te spreken.

De bijeenkomst was georganiseerd door het Europees Cybercrime Centrum (EC3) van Europol en ICE Homeland Security Investigations (HSI), de primaire onderzoeksafdeling van het Amerikaanse Ministerie van Homeland Security. Er werd gekeken naar verschillende zaken waarbij virtuele valuta werden gebruikt om goederen aan te schaffen, waaronder drugs en andere verboden middelen.

"Opsporingsdiensten zien een verontrustende trend in het gebruik van virtuele valuta om illegale goederen te kopen en verkopen, om vervolgens de opbrengsten van dit soort misdrijven te witwassen", aldus Mark Witzal van ICE HSI.

Anonimiteit

Deelnemers aan de bijeenkomst maakten hun zorgen bekend over de anonimiteit van financiële transacties die digitale valuta zoals Bitcoin bieden, en de uitdagingen die dit vormt om bij crimineel onderzoek het geldspoor te volgen. Ook werd er gesproken over de komst van Bitcoin-automaten en het groeiend aantal winkels dat virtuele valuta accepteert. Daardoor zouden criminele netwerken de virtuele munten kunnen blijven gebruiken.

Volgens Olivier Burgersdijk, hoofdstrategie bij het EC3, is de aandacht van opsporingsdiensten voor virtuele betaalmiddelen essentieel om de georganiseerde misdaad in de toekomst effectief te kunnen blijven bestrijden. "Het geldspoor is traditioneel één van de beste manieren om de criminelen op te sporen, met name de topcriminelen", zo laat hij weten. De aanwezige partijen kondigden aan om informatie met elkaar te blijven delen over het crimineel gebruik van virtuele valuta.

1 Bitcoin is op dit moment 700 euro waard !

Aantal slachtoffers internetoplichting neemt toe

Eind 2013 zijn zo'n 450.000 Nederlanders opgelicht via internet. Dat is een groei ten opzichte van de cijfers uit 2012.

In 2013 waren zo'n 3,3 procent van de Nederlanders ouder dan 15 jaar de dupe van internetfraude. Dat gebeurde vooral bij het kopen of verkopen van producten via internet. De fraude werd gepleegd door bijvoorbeeld het niet leveren van producten of het niet betalen voor producten die wel zijn geleverd.

Van een op de vijf gevallen van koop- of verkoopfraude is afgelopen jaar aangifte gedaan bij de politie. Bij identiteitsfraude was dit nog lager, slechts 13 procent van slachtoffers van identiteitsfraude ging hiervoor naar de politie.

Skimming neemt af

Tegelijkertijd laat het CBS ook weten dat het aantal fraudegevallen met skimming afneemt. Pinautomaten in winkels en bij banken zijn beter beveiligd tegen skimming. Ook worden bankpassen massaal vervangen door nieuwe varianten waarop geen magneetstrip wordt gebruikt, maar een chip.

Anti-Exploit dicht lekken nog voor ze ontdekt worden

Hedendaagse software telt encyclopedieën aan code. Niet verwonderlijk dus dat die code niet altijd even perfect is. Hackers zoeken naar kwetsbaarheden in software om zo hun rommel op je systeem te zetten. En wanneer dat gebeurd is, begint de taak van een klassieke antivirus- of antimalwaretool: de kwaadaardige code detecteren en stoppen.

Een splinternieuw programma van Malwarebytes: Anti-Exploit, wil de taak van antivirusprogramma's verlichten. In de plaats van de wachten totdat schadelijke software op je op je pc staat, zoekt Anti-Exploit de lekken zelf op, om ze vervolgens te barricaderen zodat hackers niet meer binnenkomen.

DOWNLOAD

Hoe gevaarlijk en vervelend lekken zijn werd het afgelopen jaar meer dan duidelijk. Denk maar aan de zeroday-exploit in Internet Explorer 8. Anti-Exploit houdt dergelijke lekken volgens Malwarebytes mooi dicht totdat het bevoegde bedrijf zijn code kan aanpassen.

Anti-Exploit is beschikbaar in twee smaken: de gratis versie en een premiumeditie. De gratis versie houdt je browsers en bijhorende extensies lekvrij, net zoals het kwetsbare Java. De premiumversie kost 25 dollar en beschermt ook tegen kwetsbaarheden in pdf-lezers, Office en de populairste mediaspelers.

De gratis editie van Anti-Exploit download je hier. Via de tabs Shields kan je duidelijk zien welke bescherming er inbegrepen is en welke niet. Bij logs zie je welke van de programma's die je draait werkelijk in de gaten worden gehouden door Anti-Exploit.

De software belooft een erg nuttige en krachtige tool te zijn, zeker voor bedrijven die veel data te beschermen hebben. Toch vervangt Anti-Exploits je antivirus niet. Er zijn immers nog andere manieren voor bedreigingen om op je systeem te geraken. Zie de tool eerder als een extra schild in de constant aanhoudende strijd tegen virussen en malware.

Facebookaccounts kapen is in: hoe krijg je hem terug ?

Facebookaccounts kapen is in: hoe krijg je hem terug ?

De cyberonderwereld blijft nieuwe manieren vinden om geld te verdienen. De meest recente trend: Facebookpagina's kapen, om langs die weg spam te kunnen versturen, informatie te verzamelen voor gerichte aanvallen en zelfs losgeld te vragen. Wij lijsten voor u op wat je kan doen om zo'n scenario te vermijden of desgevallend weer recht te zetten. Hoe kan je dat scenario vermijden?

... Gebruik een voldoende veilig wachtwoord, liefst een vrij lang, onbestaand woord dat niks met uzelf te maken heeft, met kleine letters, kapitalen, cijfers en tekens. Verander het af en toe.

• Cruciaal: stel op voorhand de Trusted Friends-optie in. Daarvoor klik je op het settings-icoontje rechtsbovenaan, daarna op 'security' of 'beveiliging'. Bij 'Trusted Contacts' selecteer je de contacten die bij een kaping van jouw account de nodige codes zullen ontvangen om die te deblokkeren.

Is toch misgelopen en is je account gekaapt? Hier is wat je moet doen:

• Als je account wel spam uitzendt, maar je er nog inkan: verwijder alle spam en verander je wachtwoord zo snel mogelijk.

• Als je niet meer in je account kan: gebruik de 'wachtwoord vergeten'-optie. Die helpt je om je wachtwoord te resetten via je e-mailaccount of telefoonnummer.

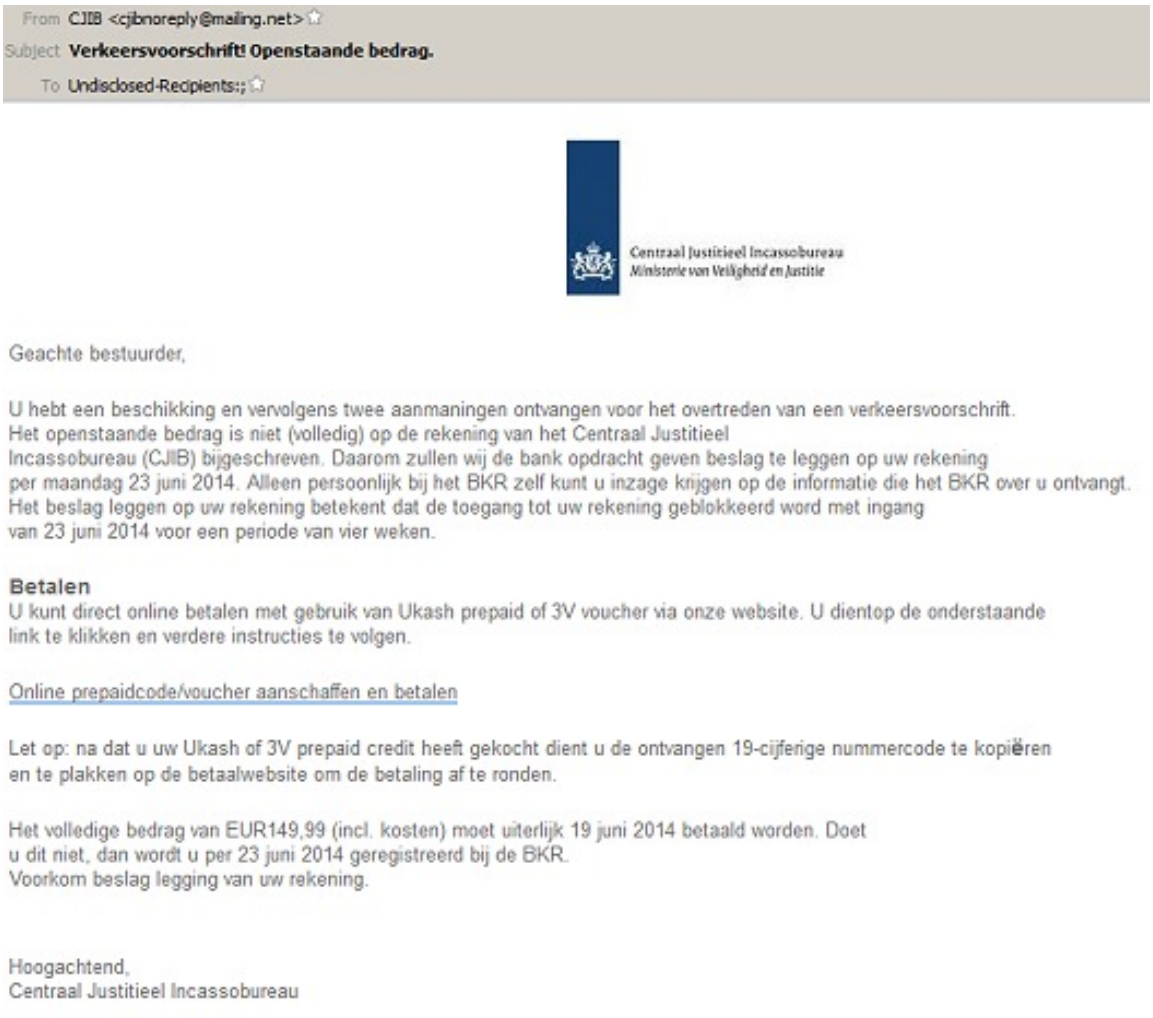
• Een beetje hulp van je vrienden: gebruik de hoger vermelde 'Trusted Friends'-functie.

Justitieel Incassobureau waarschuwt voor dreigmail

Het Centraal Justitieel Incassobureau (CJIB) waarschuwt internetgebruikers voor een dreigmail die rondgaat en stelt dat er beslag op de rekening van de ontvanger wordt gelegd, tenzij er een openstaande boete wordt betaald. De e-mail heeft als onderwerp: "Verkeersvoorschrift! Openstaande bedrag."

Volgens de tekst zou de ontvanger, ondanks eerdere aanmaningen, nog steeds niet hebben betaald. Om te voorkomen dat er beslag op de rekening wordt gelegd moet het bedrag via een Ukash prepaid of 3V voucher worden voldaan. "U kunt direct online betalen met gebruik van Ukash prepaid of 3V voucher via onze website. U dientop de onderstaande link te klikken en verdere instructies te volgen", aldus de instructietekst.

Ontvangers van de e-mail krijgen van het CJIB het advies om niet te betalen en niet op de links in de e-mail te klikken. Het CJIB zou inmiddels aangifte van internetfraude hebben gedaan



From CJIB <cjibnoreply@mailing.net>
Subject **Verkeersvoorschrift! Openstaande bedrag.**
To Undisclosed-Recipients:;

Centraal Justitieel Incassobureau
Ministerie van Veiligheid en Justitie

Geachte bestuurder,

U hebt een beschikking en vervolgens twee aanmaningen ontvangen voor het overtreden van een verkeersvoorschrift.
Het openstaande bedrag is niet (volledig) op de rekening van het Centraal Justitieel
Incassobureau (CJIB) bijgeschreven. Daarom zullen wij de bank opdracht geven beslag te leggen op uw rekening
per maandag 23 juni 2014. Alleen persoonlijk bij het BKR zelf kunt u inzage krijgen op de informatie die het BKR over u ontvangt.
Het beslag leggen op uw rekening betekent dat de toegang tot uw rekening geblokkeerd word met ingang
van 23 juni 2014 voor een periode van vier weken.

Betalen
U kunt direct online betalen met gebruik van Ukash prepaid of 3V voucher via onze website. U dientop de onderstaande
link te klikken en verdere instructies te volgen.

Online prepaidcode/voucher aanschaffen en betalen

Let op: na dat u uw Ukash of 3V prepaid credit heeft gekocht dient u de ontvangen 19-cijferige nummercode te kopiëren
en te plakken op de betaalwebsite om de betaling af te ronden.

Het volledige bedrag van EUR149,99 (incl. kosten) moet uiterlijk 19 juni 2014 betaald worden. Doet
u dit niet, dan wordt u per 23 juni 2014 geregistreerd bij de BKR.
Voorkom beslag legging van uw rekening.

Hoogachtend,
Centraal Justitieel Incassobureau

Politie en OM gaan samen bad hosting aanpakken

"De politie en het Openbaar Ministerie zijn een project gestart genaamd Nederland Schoon om samen met andere partijen 'bad hosters' in Nederland aan te pakken van wie de servers worden gebruikt voor het hosten van cybercrime."

Dat lieten Marijn Schuurbiers van het Team High Tech Crime en Lodewijk van Zwieten, de landelijk officier van justitie Cybercrime, onlangs tijdens de One Conferentie van het Nationaal Cyber Security Centrum (NCSC) tegenover Tek Tok weten.

Nederland is door zijn uitstekende internet-infrastructuur en grote aantal hostingbedrijven en providers ook aantrekkelijk voor cybercriminelen. Volgens Van Zwieten komt het voor dat hostingbedrijven niet weten dat hun servers en diensten voor cybercrime worden ingezet, maar er zijn ook hosters die het oogluikend toelaten of er actief bij betrokken zijn. Bad hosting omvat allerlei vormen van cybercrime, zoals het hosten van kinderpornografie tot het verspreiden van malware.

"Helaas zitten veel van deze bad hosters bij Nederlandse providers. Sommigen weten het niet, sommige weten het misschien niet. Maar we willen dit soort partijen niet in Nederland hebben. Als hostingland moeten we onze verantwoordelijkheid nemen, niet alleen om een goede data-economie te hebben, maar ook om voor die data verantwoordelijk te zijn", stelt Schuurbiers.

Samenwerking

"Omdat dit zo'n groot probleem is zoeken we naar nieuwe samenwerkingsverbanden met publieke en private partijen om te zien hoe we dit probleem van 'bad hosting' kunnen aanpakken", merkt Van Zwieten op. Veel partijen zouden interesse hebben om bad hosters aan te pakken. Daarom werkt justitie samen met de TU Delft in het project om vast te stellen hoe groot het probleem in Nederland is. Zodra die gegevens over een aantal weken binnen zijn, wil het OM met publieke en private partners om de tafel gaan zitten hoe het probleem als coalitie kan worden opgelost.

Het project moet ervoor zorgen dat zowel de hostingindustrie meer bewust van de 'badness' in hun netwerken is en dat het voor criminelen lastiger wordt om naar een hostingbedrijf te stappen en van hun diensten gebruik te maken, gaat Van Zwieten verder. Schuurbiers erkent dat bad hosters overal ter wereld zitten, maar als ze zich in Nederland bevinden het een taak van justitie is om ze aan te pakken. "Als elk land zijn verantwoordelijkheid neemt om het land schoon te maken zou dat fantastisch zijn."

Blauwdruk

Het eerste doel van het project is om te kijken of er een effectieve coalitie in Nederland kan worden opgezet. Is dit het geval, dan kan die blauwdruk mogelijk ook door andere landen worden gebruikt. OM en politie zijn nog op zoek naar partners met creatieve ideeën om de bad hosters aan te pakken. Het is de bedoeling dat de coalitie later dit jaar aan de slag gaat. Naast meer bewustzijn over het onderwerp bij providers en hostingbedrijven hoopt Van Zwieten dat het project uiteindelijk voor een daling van het aantal bad hosters in Nederland zal zorgen.

Wat zijn uw rechten bij webwinkels

Kopen via internet is met een druk op de muis geregeld, maar er kan nog van alles fout gaan. Het is verstandig om pas achteraf te betalen, zegt hoofdredacteur Reinout van der Heijden van de Geldgids. Wat zijn uw rechten bij webwinkels?

Welke rechten heeft iemand eigenlijk die koopt via internet? Wettelijk gezien mag een internetwinkel geen volledige vooruitbetaling eisen. De aanbetaling mag maximaal 50 procent van de prijs zijn. De mogelijkheid tot betalen achteraf moet altijd aangeboden worden. Het is ook niet toegestaan sommige klanten die mogelijkheid wel te geven en anderen niet. Veel winkels - onder andere Peter Hahn en Zalando - doen dat toch, omdat zij via handelsinformatiebureaus zoals Experian of EDR de kredietwaardigheid van klanten checken.

Vanaf 13 juni aanstaande krijgt de consument betere rechtsbescherming bij webwinkels, via de nieuwe door de EU afgedwongen Wet koop op afstand. Wie wil klagen, moet de klantenservice van de internetwinkel kunnen bellen via een informatienummer dat maximaal 1 euro per gesprek kost, naast de normale gesprekskosten.

Met de nieuwe wet wordt de bedenktijd voor aankopen verlengd van 7 naar 14 werkdagen. Dat betekent dat de klant zich bijna drie weken lang kan bedenken en het product kan terugsturen. Hij moet de kosten voor het terugsturen wel zelf betalen, behalve als hij vooraf niet goed geïnformeerd is over zijn recht op bedenktijd. In dat geval mag hij de kosten voor het terugsturen terugvragen bij de internetwinkel.

Een mooie verbetering is dat de bedenktijd van 14 dagen ook gaat gelden voor producten of diensten die op veilingsites gekocht worden..

De belangrijkste wijzigingen op een rij voor de verkopende partij:

Welke nieuwe informatieverplichtingen zijn er?

U moet per 13 juni 2014 meer informatie geven dan voorheen. Nieuwe informatieverplichtingen zijn:

- u moet uitgebreide informatie geven over de bedenktijd en eventuele voorwaarden daarbij. U moet ook een modelformulier beschikbaar stellen voor consumenten. Dit formulier kan de consument invullen als hij van de bedenktijd gebruik wil maken;
- moet de consument betalen voor het terugsturen van het product als hij gebruik maakt van de bedenktijd? Dan moet u de consument hierover informeren voordat hij de bestelling plaatst. Informeert u de consument niet? Dan betaalt u de kosten voor het terugsturen;
- u moet aangeven dat de consument recht heeft op een deugdelijk product;
- er zijn specifieke informatieverplichtingen voor digitale producten, diensten en abonnementen.

Let op

u moet consumenten informeren voordat ze een bestelling plaatsen. U moet de informatie zo aanleveren, dat de consument dit later terug kan lezen. Bijvoorbeeld per e-mail, brief, CD-rom of USB-stick.

Welke nieuwe eisen zijn er voor het bestelproces?

Er gelden per 13 juni 2014 nieuwe eisen voor het bestelproces. Deze zijn:

- u mag extra opties niet vooraf aanvinken. Het gaat daarbij om extra opties waar de consument voor moet betalen;
- direct voordat de consument een bestelling plaatst, moet u een overzicht geven van de bestelling;
- bij of op de bestelknop moet duidelijk en goed zichtbaar worden vermeld dat het gaat om een bestelling waar een betalingsverplichting aan vast zit;
- u mag kosten rekenen voor het betalen. Deze kosten mogen niet hoger zijn dan wat het u zelf kost.

Veranderingen van tarieven voor het bellen naar uw klantenservice

Bellen naar uw klantenservice mag voor consumenten niet duurder zijn dan het basistarief. Rekent u gesprekskosten per gesprek? Dan mag dit niet duurder zijn dan 1 euro per gesprek.

Let op: Bent u telefonisch bereikbaar via 1 090x-nummer? U gebruikt het nummer dan meestal voor meerdere doelen. Bijvoorbeeld:

- voor nieuwe of bestaande klanten om algemene informatie op te vragen
- om klanten bestellingen te laten plaatsen
- voor uw klantenservice. Uw klanten kunnen daar terecht met vragen of klachten over een overeenkomst die zij al met u hebben.

Gebruikt u hetzelfde telefoonnummer voor meerdere doelen en is één van die doelen een klantenservice? Dan gelden de maximum tarieven voor ieder contact van de consument met uw 090x-nummer

Wat verandert er voor de bedenktijd bij internetaankopen?

De wettelijke bedenktijd wordt per 13 juni 2014 14 dagen. Deze 14 dagen gaan in op het moment dat de consument het product ontvangt. Bij diensten gaat de bedenktijd in op het moment dat de consument bestelt.

Maakt een consument gebruik van deze bedenktijd? Dan ontbindt hij de overeenkomst. Dit betekent dat de consument de overeenkomst ongedaan maakt. Totdat de bedenktijd voorbij is, kan de consument de overeenkomst zonder opgave van redenen ontbinden. De consument kan ook al voor de levering van het product of het uitvoeren van de dienst gebruik maken van de bedenktijd.

Bestelt de consument verschillende producten tegelijk? Maar levert u deze niet tegelijkertijd? Dan gaat de bedenktijd pas in nadat het laatste product van de bestelling is geleverd.

Let op

heeft u niet voldaan aan uw informatieverplichtingen over de bedenktijd? Dan wordt de bedenktijd verlengd met maximaal 12 maanden.

Snapshots:

UT laat politiecomputers tweets 'begrijpen' voor veiligheid bij evenementen

Volgens onderzoekers van de Universiteit Twente worden computers steeds slimmer bij het 'begrijpend lezen' van tekst, bijvoorbeeld tweets. De UT onderzoekt de 'meldkamer van de toekomst', waarin de miljoenen tweets die dagelijks verstuurd worden, natuurlijk kunnen helpen om te achterhalen of en wat er aan de hand is. Taal is daarbij lastig: gaat een tweet met het woord kater nu over een incident in café De Kater, om een huisdier of over 'the night before'. En is Paris Hilton nu een tv-sterretje of een hotel in Parijs? De UT participeert in het project TEC4SE dat als doel heeft informatiestromen voor hulpdiensten te verbeteren. Universitair hoofddocent Maurice van Keulen zegt dat het de politie vooral gaat om toepassingen voor twitter als informatiebron, bijvoorbeeld bij voetbalwedstrijden. Het systeem moet informatie uit tweets halen op basis van inhoud, hashtags en auteur.

Politie wil bestrijding cybercrime verder professionaliseren

De politie wil dit jaar de bestrijding van cybercrime verder professionaliseren, zo blijkt uit het jaarverslag van de Nederlandse politie. Zo moet de intake en registratie van cybercrime worden verbeterd en moet de digitale expertise en opsporing van cybercrime binnen de nieuwe politieorganisatie worden verwerkt.

Naast een investering in de professionalisering zijn er concrete afspraken gemaakt over opsporingsonderzoeken op het gebied van high tech crime. In de Nationale Cyber Security Strategie en de Landelijke Prioriteiten is afgesproken dat het aantal onderzoeken naar high tech crime moet stijgen van vier in 2010 naar twintig in 2014.

Doelstelling

Wat betreft de afgesproken doelstelling van vorig jaar heeft de politie die gehaald. Het Team High Tech Crime rondde in 2013 negen volwaardige High Tech Crime-onderzoeken af. Daarnaast heeft het team zes rechtshulpverzoeken van grote omvang afgehandeld, waarmee de doelstelling van vijftien onderzoeken in 2013 werd gehaald. Verder werd de geplande capaciteitsuitbreidingen van het team gerealiseerd.

Den Haag zet 'Big Brother-systeem' in tegen bijstandsfraude

De Gemeente Den Haag gaat een nieuw middel inzetten tegen bijstandsfraude genaamd de Smartbox. Dit systeem gebruikt allerlei gegevens uit verschillende gemeentelijke databases en maakt aan de hand van deze data een risicoprofiel van de mensen die een bijstandsuitkering ontvangen.

In de toekomst moet de Smartbox ook bij het aanvragen van een bijstandsuitkering worden ingezet. Het systeem zal meer dan dertig verschillende variabelen te verwerken krijgen, alsmede tips van ambtenaren en burgers. Het gaat dan bijvoorbeeld of iemand al eerder heeft gefraudeerd, altijd hetzelfde vakantieland bezoekt en honden of auto's bezit.

Wethouder Henk Kool van Sociale Zaken laat tegenover NRC Q weten dat de overheid terughoudend moet zijn met het ontwikkelen van dit soort 'Big Brother-systemen', maar aan de andere kant is de bestrijding van fraude noodzakelijk om de steun voor sociale voorzieningen te bewaren.

Nieuwe functie in Facebook zet u onder druk om informatie te delen

Facebook heeft een manier gevonden om gebruikers licht onder druk te zetten om relatie-informatie te delen. De 'Ask'-functie.

Hoe het werkt? Klik op het tabblad Info, waar staat welke opleiding u heeft genoten, of u op mannen of vrouwen valt, wie uw familieleden zijn en wat uw relatiestatus is. Heeft u die informatie niet ingevuld? Dan is een Ask of in het Nederlands Vragen-knop toegevoegd. Je vrienden kunnen nu dus alles van je vragen en jij kunt alles van je vrienden vragen.

Maar niet alleen vrienden, ook mensen die je alleen van naam kennen kunnen hier gebruik van maken. De bootie call is jaren geleden al vervangen door de sms-functie en later door chatprogramma's als Whatsapp. Maar naderen we nu het tijdperk dat dit type uitnodigingen via Facebook gaan?

Cops in Cyberspace blog

Na publicatie van camerabeelden op facebook hebben twee vrouwen (19 en 20, uit Rotterdam) zich bij de politie gemeld. Ze hadden een verstandelijk gehandicapte vrouw meegelokt naar een park en haar daar van een gouden bedelarmband beroofd. De politie zette de beelden op facebook en dat 'zorgde er mede voor' dat ze zich aangaven.

Politiekorpsen in verschillende landen zijn binnengevallen bij mensen die Blackshades-malware hebben gekocht, melden verschillende omroepen. In Belgie zou bij zeventig huishoudens een inval zijn gedaan, in Frankrijk bij net zo veel mensen en ook in Duitsland, Australië, Denemarken, Zweden, Italië en Nederland zouden zoekingen zijn gedaan. De verdachten zijn mensen die Blackshades kochten, malware die onder meer gebruikersnamen en wachtwoorden verzamelt, maar ook webcams overneemt. Het pakket, dat voor minder dan honderd dollar op verschillende fora te koop is, zou ook gebruikt zijn door de man die eind 2013 werd opgepakt voor het besmetten van tweeduizend computers. Volgens het forum Leaks zou het strafbare feit het 'importeren van Blackshades in een land' zijn. NU.nl meldt dat de politie de huisadressen van de kopers mogelijk achterhaalde via Paypal-betalingen. De originele maker van Blackshades werd overigens in in 2012 al door de FBI opgepakt.

Motorclub No Surrender heeft op de website van Panorama een oproep gedaan om 'foute politiefilmpjes' te maken en op te sturen naar het mailadres van de club. De actie is volgens Klaas Otto van de motorclub een reactie op de toegenomen aandacht van de politie voor motorclubs. 'Ik loof 300 euro uit voor iedereen die ons een filmpje stuurt van een agent die de fout in gaat', belooft Otto.

De filmpjes die politiedistrict Rotterdam Oost het afgelopen jaar op YouTube zette, zijn doorhonderdduizenden mensen bekeken. Elk filmpje wordt zo'n twintigduizend keer bekeken. Zomer 2014 wordt besloten of deze proef ook in andere districten wordt gevolgd. Maar in Oost slaat het goed aan, zegt woordvoerder Nathan Okkerse. Hij is tevreden met de resultaten. 'Met de filmpjes kunnen we ze echt laten zien wat we doen'. Voordat een filmpje, vaak gemaakt door de wijkagent zelf, online gaat, wordt het eerst bewerkt. Verdachten zijn onherkenbaar, collega's ook. En het OM kijkt mee natuurlijk. 'De opsporing moet natuurlijk niet in gevaar komen'.

Tja. Facebook weer. Na planking, whaling, polar baring, teen shaming, car surfing, het versturen van boob tweets ter aanmoediging van je favoriete sportteam, neknominate en baguetting, is er weer een nieuwe facebookrage. Wie daartoe wordt uitgedaagd – en wie wordt dat niet nu iedereen aan iedereen gekoppeld is – moet binnen 48 uur ergens in het water springen en dat met een filmpje bewijzen. Zo niet, moet je een etentje of een krat bier trakteren. In Frankrijk leidde deze rage vorige week tot de eerste dode. Een jongen van 19 uit Béganne verdronk nadat hij vanaf een brug met zijn fiets in het water van de Morbihan was gesprongen. Opvallend genoeg had de politie in Frankrijk de dag ervoor nog gewaarschuwd voor dit 'A l'eau ou au resto'. Eind mei raakte bij Calais al een jongen zwaargewond toen hij in het ijskoude zeewater sprong. Ook uit België komen al meldingen van springende jongeren,schrijft Het Laatste Nieuws. 'Het lijkt onschuldig, maar het is niet zonder gevaar', zegt woordvoerder Manuel Gonzalez van de politie in Gent. Ook de politie in Engeland waarschuwde al.

Volgens de politie zetten families van vermisten veel te snel foto's van de dierbare op internet. Leo Simais, leider van het coldcase- en vermiste personenteam, hoopt dat mensen goed nadenken voor ze dat doen. 'Zo'n bericht blijft altijd bestaan'. Simais verwijst naar tientallen berichten op facebook, twitter en andere sociale media, waarin behalve het signalement ook vaak 06-nummers en andere privacygevoelige informatie gedeeld wordt. 'Het is ieders goed recht, [...] maar het kan nadelig uitpakken bij een latere sollicitatie'. Bijvoorbeeld als iemand niet vermist is, maar gemist wordt, omdat hij/zij een paar uur de kop aan het leegmaken is. Kom je nietsvermoedend thuis, sta je de rest van je leven als vermist op facebook. Bij urgente vermissingen ligt dat anders, maar ook in die gevallen wil de politie graag overleg met de familie voordat die iets op sociale media zet. 'Als het bijvoorbeeld om een minderjarig meisje gaat met een meerderjarig vriendje, dan nemen we eerst contact met hem op, om hem te laten weten dat hij mogelijk strafbaar is, als hij de vermiste bij zich houdt'. Een persoonlijk sms'je doet soms wonderen, weet Simais. 'Dan staat zo'n meisje meestal binnen een paar uur weer op de stoep bij haar ouders'.