DIGITAAL COMPUTER MAGAZINE

December 2012



SECURE COMPUTING



W.Bosgra Taakaccenthouder digitale criminaliteit

December. Ook voor mij een drukke maand. Derhalve een wat kortere editie dan u van mij gewend bent (aangezien ik dit in mijn spaarzame vrije tijd doe). Maar hopelijk wel weer interessant genoeg.

December is een tijd van geven. Daarom heb ik voor de lezers van dit medium een (uiteraard) digitaal kado.

Ik heb vanaf nu mijn SecureComputing SkyDrive box voor u opengesteld. Via onderstaande link kunt u deze benaderen. Hierin vindt u (hopelijk) interessant digitaal materiaal.
U kunt het vanuit deze box naar u eigen computer downloaden.

In de box momenteel de programma's:
Mp3Gain - hiermee kunt u uw gehele muziekverzameling dezelfde geluidssterkte geven
Freemake Video Converter - converteer elk bestand naar het door u gewenste format

Tevens alle voorgaande edities van dit magazine en een 'must see' documantaire van KROreporter over niet beveiligde scanners, WiFi printers en NAS schijven.

Veel plezier ermee.

(O ja ……. u weet het nu. Eerst testen met uw virusscanner en dan pas gebruiken)



sdrv.ms/VeiqRj

INHOUD

In deze editie oa:

Ontsleutelen

Malafide webwinkels

Romance Scam

Studeren met YouTube

Metadata Cleaner



@securecomputing

Bronnen: De Waarschuwingsdienst, Nederland veilig, Meldpunt Cybercrime, Digibewust & Digivaardig, Webwereld, Security.nl, Zdnet, Veilig bankieren, You Tube, Internetsporen, Voelspriet, HardwareInfo.

Ontsleutelen



Minister Opstelten wil in de wet opnemen dat verdachten verplicht worden bestanden te ontsleutelen. Zo'n bevel zou - net als eerder het tapbevel - terughoudend worden ingezet.
Minister Opstelten van Veiligheid & Justitie stelt dat het verplichten van verdachten een sleutel voor beveiligde bestanden af te geven niet in strijd met de wet is. Maar aan zo'n bevel hangen nogal wat haken en ogen.
Opstelten zegt dat onderzoek uitwijst dat een decryptiebevel 'niet onverenigbaar' is met het beginsel dat een verdachte niet hoeft mee te werken aan zijn eigen veroordeling. Hij werkt al langer aan een wetsvoorstel om verdachten te dwingen hun sleutel af te geven.

Wet zal breed worden ingezet
Om aan de strikte voorwaarden van het Europees Verdrag voor de Rechten van de Mens (EVRM) te voldoen, mag de maatregel slechts terughoudend worden ingezet. Maar daar zijn twijfels bij.
"Ik heb niet de illusie dat deze wet terughoudend zal worden toegepast", zegt advocaat Tjalling van der Goot. Hij wijst op het recente verleden met de introductie van het tapbevel.
"Dat zou terughoudend worden toegepast, maar inmiddels is Nederlands koploper in het aftappen geworden. Ook een decryptiebevel zal ruimhartig worden ingezet", voorspelt de advocaat. In 2008 bleek dat Nederland wereldwijde tapkampioen is. Per dag worden evenveel mensen afgeluisterd als in de Verenigde Staten in een heel jaar gebeurt.

Onafhankelijke toezichthouder
Hoogleraar Bert-Jan Koops van de Universiteit van Tilburg schrijft in het onderzoek dat Opstelten aanhaalt (PDF) dat er wel aan drie voorwaarden moet worden voldaan om aan het EVRM te voldoen. Er moet sprake zijn van aantoonbare ernstige gevallen, de wet moet terughoudend worden toegepast en er moet een stelsel van procedurele waarborgen zijn.
In het Verenigd Koninkrijk wordt de ontsleutelverplichting al toegepast. "De Britse regeling - die de meeste aanknopingspunten biedt voor de Nederlandse beleidsvorming - past enerzijds in de Britse tendens van een surveillance-maatschappij (die Nederland niet op alle onderdelen volgt) maar kent anderzijds ook waarborgen die Nederland niet kent, zoals een onafhankelijke toezichthouder", schrijft Koops.

Verdachte werkt mee aan veroordeling
Opstelten schrijft aan de Tweede Kamer dat het dwangbevel alleen in zware gevallen zal worden gebruikt en dat alleen de rechter-commissaris het bevel kan uitvaardigen bij een 'dringend opsporingsbelang'. Volgens hem zal dat alleen bij 'doortrapte criminelen' gaan waarbij het de bedoeling is dat er direct een einde wordt gemaakt aan strafbare handelingen, vaak met betrekking tot minderjarigen.
Het meest aangehaalde voorbeeld is de Amsterdamse zedenzaak. De verdachte daarin, Robert M., werkte volgens zijn advocaat Tjalling van der Goot mee aan het ontsleutelen van zijn bestanden. Hij heeft praktische bezwaren op het plan. "Je weet niet wat erop de computer staat, maar om er toegang tot te krijgen moet je juist onderbouwen wat er op het systeem te vinden is. Dat is lastig te onderbouwen."
Ook op principiële gronden vindt de advocaat het wetsvoorstel geen goed idee. "We hebben in Nederland een fundamenteel beginsel van een eerlijk proces. Een dwangbevel om bestanden te ontsleutelen staat wat mij betreft gelijk aan het afdwingen van een bekentenis", aldus Van der Goot.



Bewijs voor versleuteling
Digitale burgerrechtenorganisatie Bits of Freedom (BoF) is fel tegen een decryptieverplichting. Rejo Zenger schrijft op de site van BoF dat zo'n wet niet effectief is en Nederland zelfs onveiliger maakt. BoF vreest dat mensen worden verplicht bestanden te ontsleutelen waarvan ze allang geen sleutel meer hebben. Met een verplichting zou het zomaar kunnen zijn dat verdachten extra gestraft worden voor het bezit van versleutelde bestanden.
"Als je je wachtwoord écht niet meer kunt herinneren, moet je daarvoor dan gestraft worden?", vraagt Zenger zich af. Op deze manier worden burgers ontmoedigd om versleuteling te gebruiken. BoF ziet liever dat om bijvoorbeeld kinderporno te bestrijden, de opsporing effectiever wordt gemaakt. "Van schijnoplossingen wordt niemand beter", aldus Zenger.
Opstelten wil dat het weigeren mee te werken aan een decryptiebevel zwaarder wordt gestraft dan het weigeren van een dwangbevel. Bij het gebruik van zulke zwaardere straffen, moet er aan de drie strengere voorwaarden worden voldaan. In het voorjaar komt Opstelten met een wetsvoorstel waarin duidelijk moet worden wat de precieze straf is voor weigering.

Malafide webwinkels

Hoe voorkom je dat je opgelicht wordt door een malafide internetshop of webwinkel
Voorkomen is beter dan genezen zegt het spreekwoord, en het moet gezegd worden: tegenwoordig moet je dubbel uitkijken of je niet met een ordinaire oplichter te maken krijgt. Je betaalt wel de goederen, maar vervolgens wordt niets geleverd. Er zijn jaarlijks tienduizenden meldingen van oplichting die met dergelijke praktijken te maken hebben. De vraagt rijst natuurlijk, wat kan ik daar als gewone consument tegen doen? Dat wordt hieronder uitgelegd.

Oplichters lijken tegenwoordig met hun gladde praatjes vrij spel te hebben, zeker als het om het internet gaat. Stel, je ziet een mooi artikel in een webshop, je bestelt het artikel en rekent af. 14 Dagen later heb je het bestelde artikel nog steeds niet in huis en wat erger is, er blijkt geen contact mogelijk met de webshop. E-mails worden niet beantwoord en ook de telefoon wordt niet opgenomen. Bange vermoedens beginnen de arme klant te bekruipen. Later blijkt dat de consument met een malafide webshop in zee is gegaan. Weg artikel, weg geld. Het zal je maar gebeuren!

Gelukkig hoeft dat nu een minder groot probleem te zijn, want de Nederlandse politie heeft op de website mijnpolitie.nl de mogelijkheid ingebouwd om een verkoper/webshop na te trekken en of deze bij de politie als oplichter bekend staat. Daarvoor moet je wel inloggen met je Digid. Als je er nog geen hebt, dan is het raadzaam om er een aan te vragen. Na een aantal werkdagen krijg je de gegevens toegestuurd.

Natuurlijk geldt hier het credo: houd je Digid-inloggegevens altijd voor je zelf, wees er zorgvuldig mee en geef deze nooit door aan een ander. Behandel je Digid alsof het de inloggegevens zijn van je bank. Er zijn helaas schrijnende gevallen bekend van identiteitsfraude doordat oplichters met andermans Digid aan de haal gingen.

Na inlog op de politiesite zie je een blauwe knop met de tekst “Internetoplichting”. Wanneer je daar op klikt dan verschijnt een webpagina met een tekst over internetoplichting en daaronder vind je een blauwe knop met de tekst: “CHECK – controleer verkoper-gegevens”. Vervolgens kom je op een pagina waar je de gegevens van de verkoper/shop kunt invoeren. Dat kan een rekeningnummer zijn, een IBAN-nummer, een e-mailadres, telefoonnummer of de URL van de webwinkel.

Is inderdaad de betrokken verkoper een bekende bij de politie, dan word je gewaarschuwd via een tekst dat deze verkoper geregistreerd staat. Een malafide verkoper of webshop wordt op de politiesite online gezet als er meerdere aangiftes over deze personen of shop bekend zijn. Dit is overigens niet de enige methode om vast te stellen of de partij betrouwbaar is of niet. Wil je nog zekerder zijn (omdat de Aangiften tegen een shop bijvoorbeeld nog in de pijpleiding zitten), dan is het verder controleren van de shop of verkoper via het internet wel – als dubbelcheck - aan te raden.



1). Controleer of het keurmerk van de webshop voorkomt in het register op Consuwijzer. Als dat NIET het geval is, is de kans zeer groot dat er sprake is van een fake webshop. Ga dan niet met deze shop in zee.

2). Gebruik de ervaringen van andere consumenten en controleer met de online ShopScan die je ook kunt vinden op Consuwijzer

3). Trek na hoe lang de webshop in de lucht is. Ga daarvoor naar de site sidn.nl en voer de naam in van de webshop en kijk hoe lang deze geregistreerd staat. Shops die pas zijn opgericht moet je voor alle zekerheid links laten liggen.

4). Trek de shop of verkoper na via de site van opgelicht.nl en trek na of er klachten zijn over de webshop c.q. verkoper. Om in te loggen moet je je wel registeren. Via de site van Opgelicht worden tips gegeven over webshops en waar je op moet letten.

5). Er zijn nog meer websites over oplichting te vinden. Je kunt ook via de zoekmachine Google proberen iemand verder na te trekken.

Romance Scam



Verliefd?! Trap er niet in.....!!

Door het toenemend aantal alleenstaanden neemt de Romance scam steeds grotere vormen aan. In tegenstelling met USA of andere vnl. engelstalige landen is er in Europa erg weining tot geen informatie over romance scamming. Nochtans is dit een veel voorkomende vorm van fraude met een miljoenen omzet en de trend is helaas dankzij het toenemend aantal echtscheidingen nog stijgend.

OK, je bent het alleen zijn moe en wil stilaan terug een relatie opbouwen.
Een van mogelijkheden is dus inschrijven op een dating site en daar ben je dan een potentieel slachtoffer geworden van scammers. Een scam is een vorm van fraude, hoofdzakelijk door contact te maken via diverse dating sites. Deze vrouwen (maar ook mannen) vertellen je in betrekkelijk korte tijd dat je liefde van hun leven bent, maar in werkelijkheid zijn ze enkel uit op je geld.
Er zijn 3 grote vormen van scam
- de russian scam
- de nigerian scam
- de filipino scam

De filipino's zijn eerder bedelaars en oplichters en geen echte romance scammers, dus ik ga me beperken tot de Lads (Nigerianen) en de Vlads (Russen)

Scammers werken in teamverband, vaak vanuit een internetcafé.
Datingsites worden afgezocht om in contact te komen. Dit is georganiseerde misdaad en iedereen, ongeacht wie of wat je bent kan worden gescamd.
Eens gevonden wordt je dan al snel gevraagd om je uit te schrijven van de datingsite (je hebt immers je droompartner gevonden, niet ?)
Yahoo/Google en Hotmail adressen zijn veel gebruikt door scammers omdat die gratis zijn.

Vlads (Russian scams)

De meesten zijn uit Rusland of ex-Rusland (Oekraïne).
Als je gaat rondsurfen op scamlists lijkt het alsof er duizenden scammers zijn maar dat is absoluut niet zo.
De meeste Russische vrouwen zijn geen scammers.
De meeste Russische scams komen uit Republic of Mari El (Rusland) of Lugansk (Oekraïne) en komen van georganiseerde misdaad.
Hoewel hun profiel vermeld dat ze uit verschillende locaties in Rusland komen, verraad hun IP profiel dat ze uit Mari El of Lugansk komen.
Er zijn enkele grote verschillen maar een ding hebben ze gemeen. Alle Russische mannen zijn slecht en agressief en zijn continue dronken.

Republic of Mari El

Dit is de grootse en werkt heel professioneel. Dit is georganiseerde misdaad, geleid door mannen die goedkope meisjes inhuren in Yoskar Ola. Zij doen het vuile werk, ze plaatsen profielen (soms wel honderd per dag) en doen de correspondentie met potentiële slachtoffers. Het is moeilijker te achterhalen want ze gebruiken ook foto's van meisjes die ze betalen te poseren en gebruiken dus niet enkel van modellen bureaus. Meestal hebben ze mededaders in west Europa om het geld op te pikken.

Lugansk

Alle Oekraïense profielen komen uit Lugansk ook al proberen ze je wijs te maken dat ze uit Donetsk, Kharkov of Kiev komen.
Ze hebben zich voornamelijk gespecialiseerd in translations scam waar het in Mari El vnl. om visa of vliegtuigtickets gaat. Ze vragen dus om hun tolk te betalen. Scams uit Lugansk zijn makkelijk te detecteren aan de foto's. Dit zijn overduidelijk foto's van een modellenbureau en vallen onmiddellijk op.
Eens ze betrapt zijn haken ze snel af en laten niets meer van zich horen terwijl Mari El meisjes toch nog zullen proberen om via een omweg in contact te blijven om nog wat geld los te krijgen.

Hoe herken je ze ?

In vele gevallen eindigt hun e-mail op een nummer, bvb olga77@ of love4you@ enz
Hun mail start veelal met "I the xxxx girl", vb "I the nice girl"
Verder kom je vrijwel zeker tegen "To me of 25 years" maar dit kan eender welke leeftijd zijn. Als dit er in staat, wees maar zeker dat het scam is !
In de meeste profielen vindt je terug dat ze van Kazan, Cheboksary of Yoskar Ola zijn maar ook USA
Daar het bijna massa productie is, elke mail, elk profiel lijkt op elkaar.
Als je contact hebt lijkt het alsof ze je mail niet gelezen heeft.
Er zitten rare zinsconstructies in de mail alsof ze door een slechte vertaalmachine gemaakt zijn.
Ze zijn ongelooflijk snel verliefd en willen naar je toe komen want je bent hun grote liefde.
De meesten hebben wel een vriend in het westen die hen verteld heeft om hun grote liefde in het buitenland te zoeken.
En de belangrijkste manier om scam te ontdekken, hun IP adress ! Dit kan je vinden in de hoofding van hun mail
Check het IP adres en je weet onmiddellijk vanwaar ze komen maar meestal zal er staan Mari El of Yoskar Ola.
Nog iets belangrijk dat je daar kan terug vinden is het volgende.
Als er ergens X-Mailer: The Bat, Becky of Voyager staat mag je er vergif op nemen dat het scam is.



Lads (Nigerian scams)

Hier is veel minder over gekend dan russian scams
Het gaat ook niet enkel over Nigerianen maar ook over Ghanezen, Ivorianen, Senegalezen
Vaak zal deze zeggen dat hij/zij naar West Afrika gaat voor zaken/werk of erfenis of er al is (vnl. Nigeria, Ghana) maar van een andere nationaliteit is (VS, UK, West Europees).
Meestal zeggen ze enig kind te zijn van een gemengd huwelijk (papa Nigeriaan en mama Nederlands)
Ze uploaden enkele mooie foto's van meestal blanke personen.
Zijn veelal ook enig kind en hebben geen familie, vrienden of kennissen ter plaatse.
Eens je vertrouwen gewonnen gaan ze achter je geld. Dit kan op vele manieren
In sommige gevallen sturen ze zelfs een geschenkje op!

Dit is een voorbeeld van een typische nigerian scammail

Hallo, Ik hoop dat het leuk je te ontmoeten en weten meer over u, mijn naam en XXXXX XXXXX , ik kom uit Nederland, ik woon in Limburg Vaals worden, ben ongetrouwd, geen kinderen, en ben hier op zoek naar een serieuze en langdurige relatie , en ik hoop dat dit leven draait alles om nieuwe mensen aan en het kiezen van het beste uit hen, het zal mooi zijn wetenschap dat u meer beter, mijn msn is xxxxxxx@hotmail.com, zorg en hebben een leuke tijd en ik heb een mooie foto te delen met je op msn

Dit zijn meest gekende scenario's die erop volgen

Na enkele mails of chats zijn ze dolverliefd en willen ze naar jouw land verhuizen of terugkomen om je beter te leren kennen
Op weg naar jou worden ze overvallen, zijn ze hun papieren en geld kwijt en hebben jouw hulp nodig. Meestal gevolgd door dat de ambassade ze niet kan helpen. Dit is nonsens, op de ambassade ken je altijd terecht



Hun werkgever betaald hun uit met Money orders en ze kunnen niet aan hun geld, dus vragen ze je een check (via Qchec.com te innen voor hen en het geld door te sturen (via Western Union) of voor te schieten. Doe dit nooit, de check die je gaat innen is niet gedekt en je kan in stevige problemen komen. Meestal vragen ze om geld te storten op neen andere naam, van en vriend. (Hoezo? Ze kenden toch niemand daar?)

Ze zijn daar om de erfenis te regelen van hun overleden ouders en hebben een voorschot nodig om de notaris te betalen

Ze zijn plotseling ziek geworden of hebben een ongeval gehad en liggen in het ziekenhuis (en toch kunnen ze raar maar waar in het ziekenhuis hun PC gebruiken) en hebben geen geld om de dokter te betalen

Hoe herken je ze ?
Meestal hebben ze een Europese naam ! (Wouters, Roberts, Williams)
Ze gebruiken ook nog al makkelijk een verkeerde voornaam Marry ipv. Mary, Jenifer ipv. Jennifer
Meestal klopt de foto niet met hun leeftijd, iemand van 34 met een foto van een meisje van ong 25 jaar is geen uitzondering.
Zeggen gemakkelijk "am" in plaats van "I am" of XX by name of XX by age, vb. "32 by age" in plaats van "I am 32 years old"
Ze zijn meestal nurse of model, De mannen ingenieur of een of andere hoogopgeleide functie
Zijn onmiddellijk uit de database van de datingsite verdwenen en vragen van jou hetzelfde, ze vragen ook om contact verder te zetten via MSN, minder via mail.
Je bent al snel hun "darling" soms zelfs al na 1 chat en vragen honderduit over jouw leven, je kinderen en vragen ook je foto of die van je kinderen maar vermijden het om informatie over zichzelf te geven en houden niet van persoonlijke vragen, daar zal je meestal geen of ontwijkende antwoorden op terugkrijgen.
Ze zeggen je wel dat ze niet uit zijn op geld maar enkel een relatie zoeken. (yeah right)
Het Engels is niet altijd hun sterkste kant en bevat vele foutjes.

Hun webcam is altijd stuk of ze hebben er geen.
Vragen vrijwel onmiddellijk of je een GSM hebt en sturen ook hun nummer.
Als je hen ontwijkt, even niets laat weten krijg je wel een SMS "of je haar al beu bent"
Eens betrapt op leugentje of je zegt dat ze scammers zijn, kunnen ze verbaal redelijk agressief reageren.

Wat doe je er mee ?
In elk geval, zowel in geval van russian als nigerian scams eens ze geld van je hebben en je begint door te hebben dat je opgelicht bent verdwijnen ze en laten nooit meer iets van zich horen
En je geld, daar kan je naar fluiten

Wat kan je doen ?

Leer je een scammer kennen of vermoed je dat je benaderd bet door een scammer.
Stuur absoluut nooit geld op, dit ben je kwijt en is niet traceerbaar.
Pak nooit iets ergens voor hen op zoals pakjes of incasseer nooit een check.
Verbreek en blokkeer alle communicatie zoals e-mail met die persoon



ING gaat extra controleren bij internetbankieren
Vanaf begin december gaat de ING klanten in sommige gevallen vragen om een extra code bij het inloggen in Mijn ING. Deze PAC-code (Persoonlijke Authenticatie Code) is een extra veiligheidsmaatregel van de bank die kan worden gevraagd in bepaalde situaties, bijvoorbeeld als er vanaf een computer wordt ingelogd waarmee de klant anders nooit internetbankiert.

"Met de PAC-code kunnen we indien nodig extra verifiëren of de persoon die inlogt ook de persoon is die hij of zij zegt te zijn. Bekende social media platformen en online e-maildiensten maken al geruime tijd gebruik van een vergelijkbaar systeem. Zij vragen een extra code ter verificatie als klanten op een andere locatie inloggen. Ook maken meerdere banken in het buitenland hiervan gebruik", zegt Max Mouwen, Directeur Verkoop en Service Internet.

Systeem
Het systeem treedt alleen in werking als klanten anders inloggen dan gebruikelijk. Dit kan bijvoorbeeld zijn als zij internetbankieren op hun vakantieadres. Klanten die gebruik maken van sms TAN, zullen de PAC-code per sms op hun mobiele telefoon krijgen.

Klanten die gebruik maken van een TAN-lijst, zullen binnenkort een nieuwe lijst ontvangen. Dit wordt een lijst met nieuwe TAN-codes en PAC-codes. De PAC-code wordt voor zowel particuliere als zakelijke klanten ingevoerd. De maatregel moet voor extra veiligheid zorgen, toch is er ook malware die dit kan omzeilen door de frauduleuze transactie direct vanaf de computer van het slachtoffer uit te voeren.

ING-tool voor veilig internetbankieren slaagt test
De beveiligingstool die ING sinds kort aan klanten aanbiedt om veilig te internetbankieren is zeer effectief in het beschermen van gebruikers. Dat blijkt uit het vierde Online Banking Browser Security report van MRG Effitas. Trusteer Report, zoals het programma heet, moet ervoor zorgen dat vanaf een besmette computer nog steeds veilig is te internetbankieren en malware geen vertrouwelijke gegevens in handen krijgt.

Veel banking Trojans voeren een man-in-the-middle-aanval uit waarbij gegevens al op de computer worden onderschept. De Zeus Trojan is een bekend Trojaans paard dat op deze manier gebruikers van internetbankieren aanvalt. Uit onderzoek van Effitas blijkt dat Zeus-bestanden die tussen de nul en twaalf uur oud zijn een detectiepercentage van tussen de 5% en 20% hebben.

Test
Het onderzoeksbureau gebruikte drie simulaties om zowel virusscanners als speciale fraude- en keylogpreventie-tools te testen. Van de vijftien virusscanners weten alleen Avast!, Comodo, Emsisoft en Kaspersky een voldoende te halen. Bij de speciale tools voor veilig internetbankieren slagen alleen Quarri Protect On Q, SoftSphere DefenseWall, Trusteer Rapport en Zemana AntiLogger.

"Zoals in het begin van het rapport vermeld en gebaseerd op het bewijs en de gegevens die we hebben gezien bij gerichte aanvallen, was het de verwachting dat de meeste applicaties zouden falen en de tests bevestigen dit", aldus de onderzoekers. Die zijn vooral verbaasd dat de speciale tools zo slecht scoren.

Handel in PaySafeCards door politievirussen
Door de groei van ransomware is ook de handel in PaySafeCards en UKash-bonnen toegenomen. Ransomware is malware die in naam van de FBI, politie of andere opsporingsdienst de computer vergrendelt en 100 euro aan slachtoffers vraagt om ze weer toegang tot de computer te geven. De betalingen verlopen via PaySafeCards of Ukash-bonnen, die bij benzinestations en kiosken verkrijgbaar zijn.

Hierdoor wordt het een stuk lastiger om het geldspoor te volgen en bij de uiteindelijke cybercrimineel uit te komen. Bij nep-virusscanners en scareware werd nog in grote mate met creditcardbetalingen gewerkt, maar voor ransomware kozen de cybercriminelen bewust voor een andere betaalmethode.

"Het grootste probleem bij het volgen van het geldspoor van PaySafeCard/Ukash transacties is dat er geen record is dat de bon in andere handen terecht is gekomen totdat die wordt uitgegeven", aldus anti-virusbedrijf Trend Micro.

Marktplaats
De oplichters kunnen de bonnen verkopen totdat die aan een klant wordt verkocht, die er iets mee koopt. Inmiddels is er een levendige zwarte markt waar cybercriminelen PaySafeCards en Ukash-bonnen uitwisselen. De bonnen worden voor 40% tot 50% van de nominale waarde verkocht. De websites verkopen de bonnen vervolgens voor 90% van de nominale waarde aan internetgebruikers die tegen een gunstig tarief de bonnen willen.

Trend Micro pleit ervoor om de fora en marktplaatsen die PaySafeCards en Ukash-bonnen uitwisselen aan te pakken. "Dit zorgt ervoor dat cybercriminelen een-op-een communicatiemethoden moeten gebruiken, wat het verzilveren van de bonnen vertraagt en hun kosten vergroot, wat de lange termijn haalbaarheid van dit businessmodel verkleint."

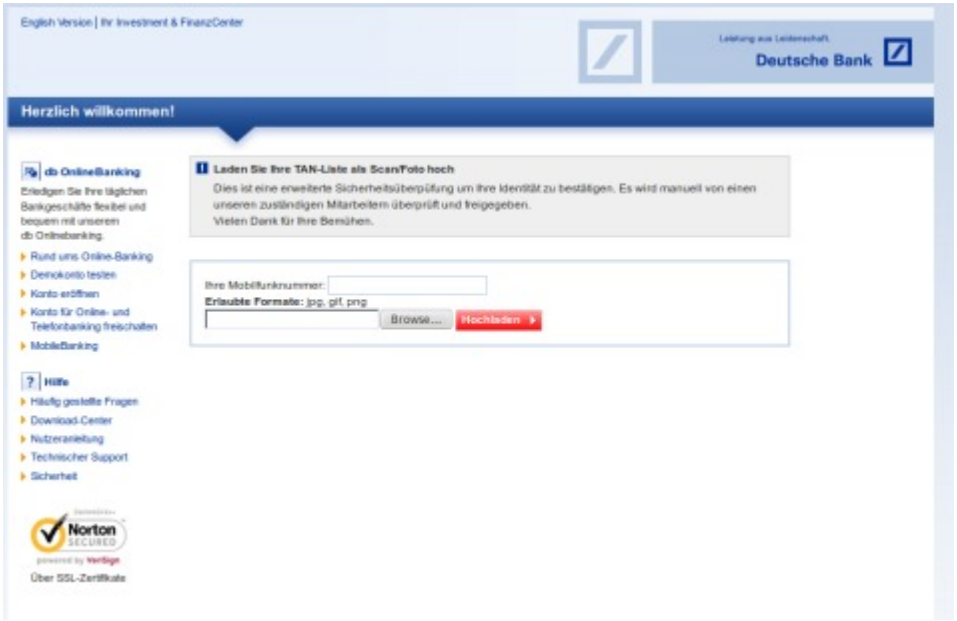
Daarnaast zouden de bonnen ook in kaart moeten worden gebracht. Voor frauduleuze doeleinden gebruikte bonnen zouden uiteindelijk door het bedrijf ongeldig kunnen worden gemaakt.

Phishingmail vraagt om foto van TANcodes



Er gaat in Duitsland een nieuwe phishingmail rond die ontvangers vraagt om een foto van hun lijst met TAN-codes te maken en die naar een website te sturen. Volgens de e-mail, die uit naam van de Deutsche Bank verstuurd zou zijn, moeten ontvangers de lijst uploaden omdat de bank vanaf 1 januari 2013 de papieren TANcodes door een mobiel TANsysteem gaat vervangen. Om de controle uit te voeren moet er op een link in de mail worden geklikt.

De link leidt naar een phishingsite, waar staat dat er een veiligheidscontrole moet plaatsvinden. Door het uploaden van de lijst met TANcodes zou de bank de identiteit van de klant kunnen bevestigen. "De lijst wordt handmatig door één van onze bevoegde medewerkers beoordeeld en vrijgegeven", aldus de tekst op de website.



HTTPS Everywhere

Over het internet versturen we een schat aan gevoelige gegevens, zoals adresgegevens, bankgegevens, maar ook e-mail en chatberichten. Het is dus zaak om ervoor te zorgen dat die gegevens niet door kwaadwillenden worden onderschept. Je voorkomt dit gemakkelijk door het gebruik van een beveiligde verbinding, die je gegevens versleutelt waardoor ze onleesbaar worden voor derden. Een handige tool hiervoor is "HTTPS Everywhere", die werd ontwikkeld door onze Amerikaanse zusterorganisatie The Electronic Frontier Foundation (EFF) en The Tor Project. DeSecurity Tip van dit nummer: investeer in je online veiligheid en installeer "HTTPS Everywhere".

Hoe werkt HTTPS Everywhere?
HTTPS Everywhere is een plug-in voor je Firefox of Chrome browser. Voor elke site die je bezoekt controleert de plug-in of die site ook een versleutelde verbinding (HTTPS-verbinding) aanbiedt en maakt dan gebruik van die verbinding. Hierdoor komt een beveiligde verbinding tot stand die je dataverkeer op drie manieren beschermt:

Authenticatie: de tool controleert of de verbinding tussen de browser en de server niet onderweg wordt omgeleid, bijvoorbeeld naar een server die in handen is van cybercriminelen. Als daarvan sprake lijkt, krijgt de gebruiker van de browser een waarschuwing.

Vertrouwelijkheid: de data die tussen de browser en de server wordt uitgewisseld wordt versleuteld en is zo onleesbaar voor derden.

Integriteit: het voorkomt dat een data tijdens verzending niet kan worden gewijzigd.

Word je door HTTPS Everywhere volledig beschermd?
Door gebruik van HTTPS Everywhere zorg je ervoor dat bij websites waar HTTPS beschikbaar is, je ook HTTPS gebruikt. Zo kan je je gevoelige gegevens zo vaak mogelijk veilig versturen. De tool kan echter geen volledige veiligheid creëren: als je een website bezoekt die niet of slechts deels in HTTPS voorziet, dan blijf je daar ook mét gebruik van de tool onbeschermd. Controleer dus altijd eerst of de tool op een site bescherming biedt voordat je gevoelige gegevens verstuurt.

Verder beschermt HTTP Everywhere alleen de inhoud van je dataverkeer. De tool verhult níet welke site je bezoekt, hoeveel tijd je daar doorbrengt, of de hoeveelheid data die je daar uploadt of downloadt. Wil je verhullen welke sites je bezoekt, dan zal je gebruik moeten maken van een anonimiseringstechniek zoals Tor.

Tot slot is het HTTPS-systeem niet waterdicht: zo hadden de inbrekers bij Diginotar, waarschijnlijk van de Iraanse overheid, valse certificaten aangemaakt om versleuteld Gmail verkeer te onderscheppen. In zo een geval is zelfs HTTPS-verkeer dus niet veilig meer. HTTPS biedt dan ook vooral beveiliging tegen minder geavanceerde aanvallers, zoals het afluisteren van je verkeer in een open Wifi-netwerk.

Investeer in online veiligheid
Het gebruik van HTTPS Everywhere is een belangrijke investering in je online veiligheid en kost maar weinig tijd en moeite. Je kan de plug-in downloaden op de website van EFF.



Metadata Cleaner



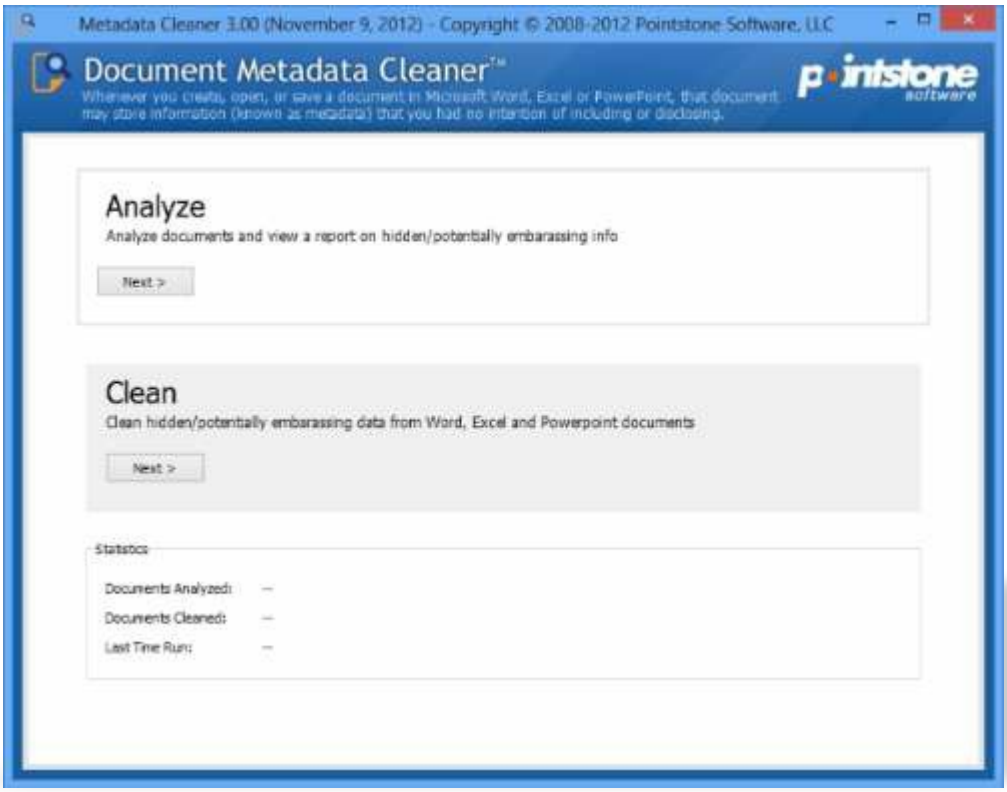
Verwijder privégegevens uit Office-documenten

Document Metadata Cleaner schrobt Word, Excel en PowerPoint

Ook in Office-documenten zit persoonlijke informatie die je niet altijd wilt prijsgeven. Document Metadata Cleaner schrobt daarom namen en commentaren uit Word- of Excel-documenten.

In veel digitale bestanden zit tegenwoordig metadata, waarmee individuele bestanden eenvoudig door software en diensten kunnen worden herkend. Bij foto's weten we hoe gevaarlijk dat kan zijn, omdat iemand je thuisadres kan opsporen aan de hand van foto's die je online hebt gepubliceerd.

Maar ook Office-documenten, zoals Word-teksten, Excel-spreadsheets en PowerPoint-presentaties, bevatten informatie waarmee anderen je kunnen herkennen. Zo voegt het kantoorpakket informatie toe over auteurs, revisies en ook op welke computer een document is aangemaakt.



Omdat we goed begrijpen dat dit lang niet altijd wenselijk is, verwijzen we je naar Document Metadata Cleaner, dat aan de lopende band de metadata stript uit bovengenoemde bestandstypen.
Je kunt daarbij zelf kiezen welke gegevens moeten verdwijnen, waarna het programmaatje volautomatisch begint met schoonmaken.

Dit kleine programma is niet perfect, maar het doet zijn werk naar behoren, en is bovendien gratis voor gebruik thuis of op het werk.

Studeren doe je ~~bij~~ ~~de NCOI~~ met YouTube!

De tijd dat YouTube alleen bestemd was voor zelfgemaakte videofilmpjes en het bekijken van muziekclips, ligt inmiddels achter ons.

Misschien wist u het niet, maar YouTube is onderdeel van het Nieuwe Leren.

Zeker op gebied van PC en internet zijn er legio filmpjes te bekijken. U kunt hier uw voordeel mee doen.

Hiernaast een kleine opsomming van mijn reis door YouTube land.

Harde schijven, boterzachte beveiliging
http://www.youtube.com/watch?v=ettw7LjcCEg

Inbreken op facebook via WiFi
http://www.youtube.com/watch?v=PyqaKzU4h4Y



Secure Computing