Nieuwsbrief 5-2012

W.Bosgra *Taakaccenthouder digitale criminaliteit*

Digitale nieuwsbrief verzorgd door Secure Computing.

Doel is bewustwording van wat u doet met de computer en kennis opdoen voor de opsporing van strafbare feiten gepleegd middels de computer. U kunt deze nieuwsbrief opslaan op uw eigen "Home"-omgeving en als naslagwerk blijven gebruiken.

Deze nieuwsbrief zal met enige regelmaat in uw mailbox verschijnen.

Middels deze nieuwsbrief houden wij u op de hoogte van:

- Onderwerpen die betrekking hebben op het veilig gebruik van de computer en het internet
- Nieuws uit de media
- Juridische vragen
- Nieuwe technieken
- Vele andere wetenswaardigheden

In deze editie o.a.

Van password naar passphrase

Smishing en vishing

Virussen in Microsoft Word

Van password naar passphrase(zin)

Als het gaat om het maken van veilige wachtwoorden zwerven er allerlei verschillende adviezen rond. Hoofdletters, cijfers, bijzondere tekens gebruiken enz. Maar waarom zou u volstaan met 1 woord?

De meeste wachtwoorden worden tegenwoordig via gehackte databases buitgemaakt. Aangezien veel websites nog altijd voor SQL Injection (deze term mag u rustig weer vergeten) kwetsbaar zijn, is het kinderspel voor een aanvaller om de volledige database te stelen, inclusief gebruikersgegevens.

Sommige websites bewaren de wachtwoorden in platte tekst. Andere gebruiken alleen een zogenaamd MD5 algoritme. Hierbij wordt het wachtwoord versleuteld zodat een aanvaller niet het originele wachtwoord kan zien. Het is namelijk niet mogelijk om de hash (unieke berekening in cijfers)uitkomst terug te rekenen naar de oorspronkelijke invoer. Het is wel mogelijk om een "woordenboek" van alle woorden en hun bijbehorende hash aan te leggen. Elk woord heeft namelijk een unieke hashwaarde.

Zodra een aanvaller een database met MD5 gehashte wachtwoorden vindt, kan hij in dit woordenboek de MD5-hash opzoeken en kijken welk woord hierbij hoort. Voor alle woorden tot en met acht karakters zijn de MD5 hashes berekend,

De oplossing is een passphrase; een zin van meerdere woorden. Passphrases hebben verschillende voordelen. Ze zijn lang, eenvoudig te onthouden en makkelijk uniek te maken.

Een voorbeeld van een passphrase "mijn wieldoppen uit 1967 zijn roestig". Met spaties meegeteld 37 karakters lang. Een aanvaller die van alle zinnen die 37 karakters lang zijn de MD5 hash wil berekenen, is wel een aantal jaren bezig. Het is natuurlijk wel belangrijk om een unieke passphrase te maken. Het gebruik van speciale tekens is niet verplicht, maar maakt de passphrase wel sterker. Het blijft natuurlijk belangrijk om hem te kunnen onthouden. Een aanvulling op het gebruik van passphrases is het opzettelijk toevoegen van typ- of spelfouten. Dat laten wij natuurlijk over aan uw eigen creativiteit.

Mobiele internetters worden bedreigd door nieuwe soorten phishing scams

Door de toenemende populariteit van online winkelen en bankieren via mobiele apparaten, worden meer gevoelige persoonlijke gegevens in mobiele telefoons opgeslagen dan ooit tevoren.

Deze enorme hoeveelheden persoonlijke gegevens vormen voor dieven en gewetenloze hackers een onweerstaanbaar doelwit. Daarom verzinnen ze continu nieuwe manieren om misbruik te kunnen maken van mobiele apparaten en hun eigenaars.

De nieuwste bedreigingen: smishing en vishing

Vishing lost een hoop problemen van traditionele phishing scams op. Er is geen sprake van duidelijke spelfouten, wazige logo's of andere indicaties die erop wijzen dat er iets mis is. In plaats daarvan hoort u een zelfverzekerde, gezaghebbende stem die u vertelt over een probleem dat u onmiddellijk moet oplossen. Een vishing scam verloopt vaak op de volgende manier:

- U ontvangt een voicemail van uw bank en krijgt te horen dat er een dringend probleem is met uw pas en/of rekening. De stem klinkt officieel, dus waarom zou u eraan twijfelen?
- U krijgt een gratis telefoonnummer dat u moet bellen. Dit nummer verbindt u door met een systeem dat vraagt naar uw rekeningnummer, pincode en andere persoonlijke gegevens. Net als bij een ***smishing (SMiShing = SMS phishing, gemanipuleerde berichten die van uw bank lijken te komen***)aanval gebruiken de dieven uw informatie om bijvoorbeeld creditcards en bankpassen te kopiëren. Zo kunnen ze uw legitieme rekeningen leeghalen en u het leven zuur maken.
- Soms krijgt u te horen dat u zich op een website moet aanmelden. Zodra u dat doet, wordt er vanaf de site vaak malware gedownload waardoor dieven toegang krijgen tot alle informatie die in uw telefoon is opgeslagen, waaronder uw contactenlijst. Hierdoor krijgen ze toegang tot nog meer potentiële slachtoffers.

Hoe kunt u uzelf beschermen tegen smishers en vishers?

Hier zijn enkele tips over hoe u criminelen die het op uw mobiele apparaat hebben voorzien, kunt dwarsliggen:

- Reageer niet op een sms-bericht of voicemail van een geblokkeerd of onbekend nummer. Als u niet weet met wie u spreekt, is er een goede kans dat u dat ook helemaal niet wilt weten.
- Download niets tenzij u zeker weet dat het van een betrouwbare bron afkomstig is. Dit geldt zeker voor downloads en bijlagen van geblokkeerde of onbekende gebruikers.
- Reageer niet op e-mails, sms-berichten of telefoontjes waar u niet om gevraagd hebt en waarin om persoonlijke gegevens wordt gevraagd.
- Klik nooit op links of bijlagen in ongevraagde e-mails.
- Als u naar de website van een zakelijke of financiële instelling wilt gaan, moet u het webadres rechtstreeks in de adresbalk typen.
- Controleer apps voordat u ze downloadt. Download nooit een app via een link in een sms-bericht.

Sommige mobiele telefoonproviders bieden gebruikers de mogelijkheid verdachte sms-berichten door te sturen, zodat ze onderzocht kunnen worden. Gebruikers moeten contact opnemen met hun provider als ze zorgwekkende sms-berichten hebben ontvangen.

Hoe bindend is een e-mailblunder?

De wet kent een regel voor het geval je iets anders verklaart (per mail, schriftelijk, mondeling of hoe dan ook) dan je eigenlijk bedoelt hebt.. Wanneer de wederpartij "onder de gegeven omstandigheden redelijkerwijze [een bepaalde betekenis] mocht toekennen" aan het bericht, kan de verzender zich niet meer beroepen op het feit dat hij niet bedoelde dit te sturen (art. 3:35 BW).

Het komt dan vaak neer op de exacte formulering van de mail. Met een mail die als inhoud heeft "Ik ben akkoord" gevolgd door een signature met "Met vriendelijke groeten" mag de wederpartij redelijkerwijs denken dat dit bericht onvoorwaardelijk juist is. Je zit dus vast aan de inhoud. Lees daarom je mail nog een keer extra na, voordat je op Verzenden klikt.

Word-documenten kunnen virussen bevatten

Waarom Microsoft Word kwetsbaar is

Omdat het nou juist Word-bestanden zijn die vaak worden uitgewisseld, hebben Word-virussen zich gemakkelijk weten te verspreiden. Zo werkt het:

- Microsoft Word-bestanden bevatten kleine programma's die 'macro's' worden genoemd. Dit zijn aanpasbare snelkoppelingen waarmee taken automatisch kunnen worden uitgevoerd, zoals het opmaken van tekst of het toepassen van genummerde lijsten.
- De programmeertaal voor macro's kan ook worden gebruikt voor het schrijven van virussen.
- Het virus kan als onderdeel van een Word-document worden verzonden.
- Het virus wordt automatisch geactiveerd wanneer u het Word-bestand opent.

Hoe hackers u misleiden

Hackers gebruiken verschillende trucjes om u over te halen om een geïnfecteerd Word-bestand te openen. Zij kunnen:

- het adres van een vriend of een bedrijf gebruiken, of bijvoorbeeld van iemand die u de week ervoor in de kroeg hebt ontmoet.
- zich voordoen als een belangrijk bericht van uw bank, de belastingdienst of een loterij waarin u een prijs hebt gewonnen.
- actuele nieuwsonderwerpen als lokmiddel gebruiken. Vorig jaar bijvoorbeeld, toen er wereldwijde aandacht was voor de pro-democratieprotesten in Myanmar, lieten hackers een geïnfecteerd Word-bestand circuleren dat ogenschijnlijk een steunbetuiging van de Dalai Lama bevatte.

Zo kunt u uzelf beschermen

- Open alleen e-mailbijlagen die u verwacht en afkomstig zijn van een betrouwbare bron.
- Gebruik een programma voor internetbeveiliging, dat automatisch e-mailbijlagen op virussen en andere schadelijke software scant, voordat u ze opent.
- Verwijder verdachte berichten zonder ze te openen.
- Klik niet op internetkoppelingen en open geen bestanden bij e-mail en expresberichten die u hebt gekregen van iemand die u niet kent.

Conclusie

Wees op uw hoede voor elk bestand dat u als bijlage via een e-mail binnenkrijgt, zelfs voor onschuldig lijkende Microsoft Word-bestanden. Deze bestanden zouden virussen of andere schadelijke software kunnen bevatten die uw systeem zouden kunnen beschadigen of uw identiteitsgegevens zouden kunnen stelen. Gebruik altijd een programma voor internetbeveiliging om u tegen virussen, spyware en spam te beschermen.

Cyberkatvanger

Cybercriminelen zijn nog altijd bezig om Nederlandse katvangers te zoeken die helpen met het witwassen van geld dat via phishing en malware van online bankrekeningen is gestolen. De afgelopen week zijn er verschillende campagnes gelanceerd, waarbij er steeds via andere e-mails en domeinnamen wordt geprobeerd om Nederlandse internetgebruikers te laten reageren.

Die moeten vervolgens hun bankgegevens opsturen, zodat de criminelen het geld van andere bankrekeningen naar de rekening van de katvanger kunnen overmaken. Die neemt het geld op en stuurt het bijvoorbeeld via Western Union naar de rekening van de criminelen, of maken het direct over.

De nieuwste e-mails hebben als onderwerp:

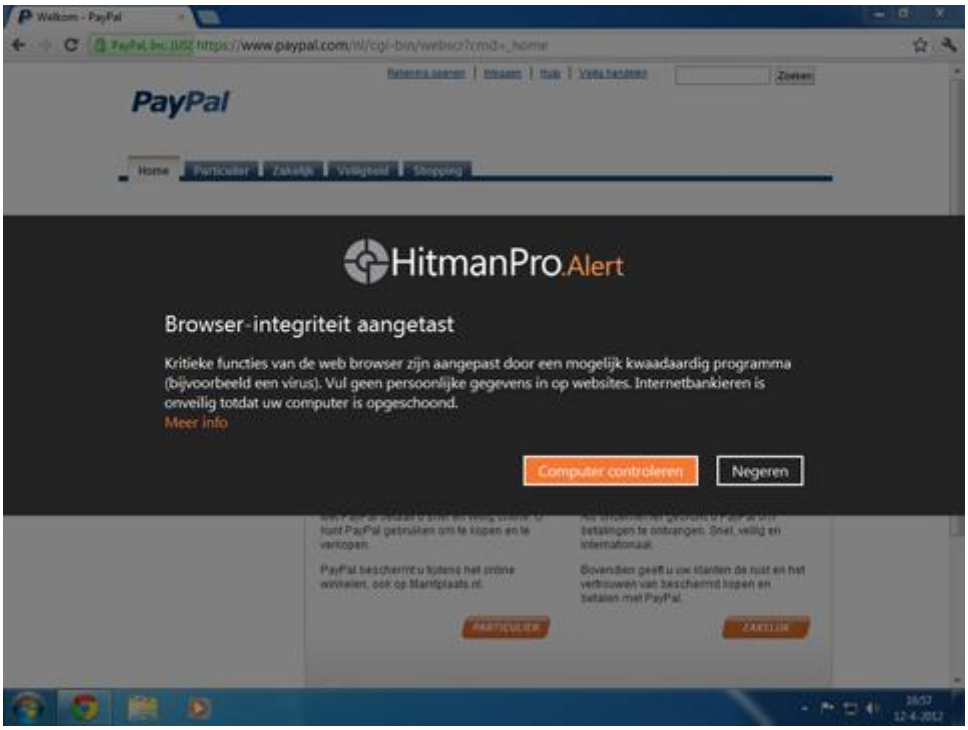
- Wilt u 2000 euro per maand meer verdienen dan u nu verdient?
- Wij bieden aan u een extra inkomen van 200 euro per dag.
- Komt te weten hoe mensen van uw beroep met 30% meer kunnen verdienen!
- U kunt meer verdienen! Wij bieden u een persoonlijke oplossing.
- U kunt 200 euro per dag extra verdienen.
- De mensen zijn bereid 125 euro per uur aan u te betalen voor uw hulp. Help hun!

In de e-mail wordt gevraagd om een reactie naar @tophollandjob.com,en te sturen. De domeinnaam is op 8 april geregistreerd. Ook dit keer waren de criminelen creatief met de namen van de afzenders. Zo zouden de berichten afkomstig zijn van Dokter Little, Dokter Humphrey, Dokter Waller. Dokter Harmon en Dokter Chaney.

Gratis Windows-tool voor veilig internetbankieren

Het Nederlandse anti-virusbedrijf SurfRight heeft een gratis programma aangekondigd dat Windows-gebruikers veilig laat internetbankieren. HitmanPro.Alert, zoals de tool heet, waarschuwt gebruikers wanneer het niet veilig is om op hun online bankrekening in te loggen of creditcardgegevens in te voeren. De waarschuwing verschijnt voordat de vertrouwelijke informatie tussen de browser en de bank of online winkel wordt onderschept door malware in de browser.

Malware zoals banking Trojans kunnen transactiegegevens wijzigen voordat die naar de bank worden gestuurd. HitmanPro.Alert detecteert deze zogenaamde Man-in-the-Browser aanvallen en informeert de gebruiker wanneer belangrijke systeemfuncties zijn omgeleid naar een niet-vertrouwd programma. HitmanPro.Alert werkt zonder virushandtekeningen zodat gebruikers altijd gewaarschuwd kunnen worden. HitmanPro.Alert laat de gebruiker automatisch Hitman Pro anti-malware downloaden, waarmee het direct mogelijkheid is de bedreiging van de computer te verwijderen.



HitmanPro.Alert moet dit kwartaal uitkomen en verschijnt voor alle browsers, waaronder Internet Explorer, Chrome, Firefox en Opera.

HP USB Disk Storage Format Tool

Alhoewel ze over het algemeen zeer betrouwbaar zijn hebben usb-sticks en flash-geheugenkaartjes toch niet het eeuwige leven. Soms zorgen fouten in dat geheugen dat ze niet meer bruikbaar zijn. Nou, ja, dan maar opnieuw formatteren, zult u denken. Helaas lukt zelfs dat niet altijd en dan komt de HP USB Disk Storage Format Tool goed van pas. Da's een hele mond vol voor een programma dat in feite hetzelfde doet als Windows' eigen format-commando – maar dit programma doet het dus ook vaak als format weigert.

http://download.cnet.com/HP-USB-Disk-Storage-Format-Tool/3000-2094_4-10974082.html

Muis smeriger dan wc-bril

De gemiddelde computermuis is drie keer zo vuil als een toiletbril volgens het Britse Initial Washroom Hygiene.

Hiermee is de computermuis de grootste bacteriebron op kantoor. De tweede plek wordt ingenomen door toetsenbord, derde plek is voor de telefoon en op plaats vier vinden we de stoel. Muizen van mannen zijn 40% smeriger dan die van vrouwen.