Frank Brokken / f.b.brokken@rug.nl

Vissen

Frank Brokken is security manager bij het RC. Met het instellen van deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column houdt Frank ons op de hoogte van de stand van zaken met betrekking tot zijn missie.

DE TWENTSCHE COURANT
Tubantia

Vissen is nooit mijn hobby geweest. Ik weet dat dat voor veel mensen anders ligt. Mijn oom Gerrit was een echte visser. Hij woonde naast ons, en regelmatig trok hij er voor dag en dauw op uit om te gaan vissen. 'Dan bijten ze beter', zei hij.

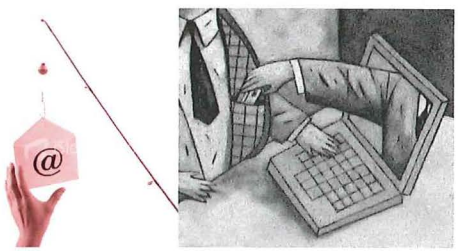
Vissen kon hij wel, die oom Gerrit van mij. Zo ving hij ooit een snoek van een meter en dat was dermate uitzonderlijk dat hij samen met de gevangen snoek (het beest was inmiddels dood, maar oom Gerrit hield 'm op zodat duidelijk werd hoe groot zo'n snoek van een meter wel niet is) in de krant kwam. Tubantia, wel bekend bij iedereen die ook uit Twente komt.

Dierenbescherming

Ik ben een keer met hem mee geweest. Ik moest dus ook voor dag en dauw het nest uit om vervolgens uren aan de waterkant naar een dobbertje te turen, wachten op de dingen die zouden komen. Er kwam niks.

Aan het einde van de ochtend, helemaal doodverveeld, mocht ik weer naar huis. Het zal het eerste indrukseffect zijn geweest, maar het is nooit meer wat geworden tussen dat vissen en mij. Ik ben nog wel een hele tijd daarna lid geweest van de dierenbescherming, maar ik geloof niet dat er een rechtstreeks verband bestaat met mijn viservaring....

Het zal dan ook wellicht geen verbazing wekken dat mijn eerste gedachte bij het zien van het woord *phishing* was dat iemand op frivole wijze met taal aan het stoeien was. Maar korte tijd later begreep ik dat we hier met een bijzondere vorm van computermisbruik te maken hadden.



Toch is er wel degelijk een relatie met 'vissen'. Bij phishing proberen de *bad guys* informatie te ontfutselen van naïeve computergebruikers waarmee zij - de bad guys - dan financieel voordeel kunnen behalen.

Miljoenenschade

De 'computermaffia' richt zich hoe langer hoe meer op dit soort misbruik en in 2007 liepen 194 bedrijven in de VS zo'n $ 3.000.000 schade op doordat deze bedrijven werden gefingeerd bij phishing-aanvallen. Minstens zo interessant lijkt me te weten hoeveel schade de personen opliepen die in de phishing-val trapten.

De computermaffia is niet gek: firewalls, spamfilters, virusscanners maken het *malware* enigszins lastig om door te dringen tot de doorsneecomputer. Dus wordt de 'aanvalsroute' veranderd.

De maffia bedient zich van goede simulaties van websites van banken en stuurt dan serieus ogende e-mail aan klanten van dergelijke banken met – bijvoorbeeld - waarschuwingen over phishing-aanvallen, en hoe belangrijk het is om dergelijke aanvallen tegen te gaan door acuut het wachtwoord te veranderen. Voor het gemak wordt de link naar de website van de bank alvast meegegeven.

Dat de website geen https-verbinding is, maar een http-verbinding, valt de meeste gebruikers niet op. Het verschil is ook maar gering, hoewel wezenlijk: http geeft in Firefox een witte adresbalk zonder slotje, en een crèmekleurige adresbalk met een slotje voor https.

Gecertificeerde verbinding

De https-verbinding is gecertificeerd. Meestal gaat dat goed, en bonafide websites kunnen hun beveiligde https-verbinding laten certificeren. De maffia heeft met die certificering wat meer moeite en maakt regelmatig eigen certificaten aan.

Wat doet uw browser met zo'n eigengemaakt certificaat? Hij piept, in de vorm van een waarschuwingsvenstertje. Lastig hoor, denken de meeste gebruikers, en klikken het venster weg. Om vervolgens snel het wachtwoord te veranderen (uiteraard moet eerst het oude wachtwoord worden ingetypt, want zo gaat dat).

Dank, zegt de maffia, die vervolgens zowel gebruikersnaam als wachtwoord heeft en nog maar een fractie verwijderd is van misbruik van de rekening van de gefopte gebruiker. Tancodes? Tja, nou de meeste gebruikers laten die toesturen per mobiel en dus steelt de maffia het mobieltje of luistert men gewoon het mobiele verkeer af.

Schade? Opnieuw in de VS in 2007: bijna $ 4.000.000 schade als gevolg van diefstal van mobiele hardware, ruim $ 2.000.000 schade door diefstal van vertrouwelijke informatie uit mobiele apparatuur.

TU Delft

De volgende informatie kreeg ik op 28 januari (2008) toegestuurd van mijn collega Alf Moens van de TU Delft:

"Vandaag in de vroege ochtend was TU Delft het slachtoffer van een gerichte phishing scam. Deze bestond uit een e-mailbericht aan 270 medewerkers ogenschijnlijk afkomstig van een TU Delft-instantie (het TU Delft messaging centre). Het bericht was in redelijk Nederlands opgesteld en, hoewel het niet de juiste terminologie gebruikte, redelijk geloofwaardig, tenzij je beter weet.

Het bericht verzocht de gebruiker per e-mail reply gebruikersnaam, wachtwoord en enige persoonlijke gegevens van het e-mail account retour te zenden, als onderdeel van een schoonmaakactie en ter voorkoming van opheffen van het account. Als afzenderadres stond een niet bestaand TU Delft e-mailadres genoemd, als feitelijk reply adres werd account.upgrade@hotmail.co.uk gebruikt.

Op zich eenzelfde strategie als bij zo vele bankphishing mails. Eind vorige week is een zelfde scam gezien bij de universiteit van Utah, eveneens afkomstig van gehackte pc's in Nederland."

De TU Delft heeft de volgende maatregelen genomen:

- afvangen e-mailverkeer gericht aan het reply adres. Dit gebeurt in de uitgaande e-mailcontrole (uitgaand spamfilter);
- profiel van dit bericht toevoegen aan spamfilter;
- waarschuwen surfnet-cert;
- klacht naar *abuse* van afzenderdomein (hccnet.nl);
- klacht naar abuse van reply-to domein;
- nieuwsbericht voor medewerkers op de medewerkersportal.

Door hun snelle en adequate reactie bleef de schade binnen de perken: voor zover bekend was er slechts een (1) slachtoffer.

Aan de bel trekken

Phishing is een vorm van social engineering, wat in het verleden ook in andere situaties een opmerkelijk goede methode is gebleken om je doel als inbreker, dief, of hacker te bereiken. Gevaarlijk hoor! Maar vaak geldt hier ook dat een gewaarschuwd mens voor twee telt.

Door RUG-(CIT-) medewerkers zal u nooit via e-mail om uw p- of s-nummer en/of wachtwoord (of andere persoonlijke informatie) worden gevraagd. Mocht u dergelijke e-mail wel krijgen, dan is dat een goed moment om eens aan de bel te trekken.

Bijvoorbeeld bij:

Frank B. Brokken
(nooit afwezig vanwege het vissen)

- De wikipedia-pagina over phising: **http://en.wikipedia.org/wiki/Phishing**