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

Trojaanse Paarden?

Frank Brokken is security manager bij het CIT. 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.

Iedereen is natuurlijk wel bekend met het fenomeen 'Trojaans Paard'. Niet alleen uit Troje, maar ook uit het hedendaags IT-gebruik. Een Trojaans Paard in de IT is net zoiets als een virus, maar dan anders. Hoewel de effecten vergelijkbaar zijn. Een virus zit bijvoorbeeld in het attachment van je e-mail.

Virusverspreider

Iemand stuurt een e-mail met een attachment dat instructies bevat die door de computer (eigenlijk: het programma dat het attachment zichtbaar of leesbaar maakt) kunnen worden uitgevoerd. Het virus 'nestelt' zich dan in je computer en kan daar van alles en nog wat doen, zoals je adresboek opsturen naar de spam-maffia of een key-logger installeren zodat je username en password bij de 'bad guys' terecht komt.

Allerlei varianten komen voor; wat dat betreft lijkt het virus sterk op biologische virussen. Virussen hebben de neiging zich te vermenigvuldigen. Ze infecteren op hun beurt jouw attachments met een kopie van zichzelf waardoor jouw computer ook een virusverspreider is geworden.

Trojaanse paarden werken op vergelijkbare wijze. Als verschil tussen Trojaanse paarden en virussen wordt algemeen genoemd dat een virus op eigen kracht je computer binnenkomt (op eigen kracht is dan ook het geval wanneer het ingebed zit in een attachment dat iemand per e-mail naar je toestuurt), terwijl je -conform de situatie in Troje- een Trojaans paard zelf binnen haalt.

Onwelkome gasten

Het binnenhalen van een Trojaans paard gebeurt in de praktijk wanneer je ergens een programma tegenkomt waarvan je denkt: dat wil ik eigenlijk ook wel hebben. Windows

waarschuwt je dan braaf dat het gevaarlijk is om 'zo maar' vreemde programma's te starten, maar dat is belangrijk minder effectief dan het advies dat we allemaal van onze ouders hebben gekregen: geen snoepjes aannemen van vreemde mannen. Het besluit is immers al genomen en het interessante programma wordt simpelweg opgehaald en geïnstalleerd. Het programma doet waarschijnlijk inderdaad wat ons is beloofd, maar 'achter de schermen' nog wel wat meer: lees bovenstaand stukje over het gedrag van virussen voor details.

Virussen en Trojaanse paarden zijn onwelkome gasten in onze computers. Gelukkig hebben we een up-to-date virusscanner waardoor de indringers tijdig worden gedetecteerd. Ja toch? Nou, in ieder geval is dat waar we voor het gemak maar even vanuit gaan. Je wilt ze niet in je computer en wie de moeite neemt om zo nu en dan eens in het quarantainegebied van de virusscanner te kijken zal, daar doorgaans wel een of meerdere bestanden aantreffen die besmet zijn met bekende virussen en Trojaanse paarden.

Yes, No of Cancel?

Iets vergelijkbaars overkwam Esther, mijn echtgenote, enige weken terug. Terwijl ze rustig aan het werk was (het UMCG, in dit verband,

maar dat terzijde) krijgt ze opeens een melding van de virusscanner. De virusscanner heeft bij een automatische scan tien Trojaanse paarden gedetecteerd en vraagt Esther of ze moeten worden opgeschoond, met de bekende keuzemogelijkheden 'Yes', 'No' en 'Cancel'.

Wat te doen?

Trojaanse paarden zijn onwelkom. Gelukkig kan de virusscanner ze detecteren, dus verwijderen maar? 'Yes', dus?

Hmm...., maar plotseling tien Trojaanse paarden is natuurlijk wel veel. Die lui in Troje hadden al moeite genoeg om één paard te maken, en Esther is nogal voorzichtig met het ophalen van 'vreemde programmatuur'. 'No', dan maar?

Hmm...., maar als het nou wel zo is, dan zit die hele stoeterij nog steeds in haar computer; dat is ook niet wat je wilt. Blijft over 'Cancel'?

Hmm...., tja.... maar wanneer worden ze dan wel opgeschoond?

Kortom, een lastig parket. Wat zou u doen, geachte lezer, in deze situatie?

Valkuil

Esther deed niks. Helemaal niks. Tenminste, niet met haar computer en dat was waarschijnlijk de beste keuze die ze kon maken. In plaats daarvan belde ze mij op om de situatie aan mij voor te leggen. Mijn indruk was dat het geen zuivere koffie was, en dat ze het beste de afdeling IT-support van het Universitair Medisch Centrum Groningen van de situatie op de hoogte kon stellen.

De gedachte erachter was dat het 'pop-up window' helemaal geen melding van de virusscanner was maar zelf het resultaat van 'malware' dat om welke reden dan ook tot haar computer was doorgedrongen. Waarschijnlijk zou elk alternatief, 'Yes', 'No' en 'Cancel' tot verdere besmetting van haar computer hebben geleid. Die avond heeft UMCG IT-support Esther's computer eens goed onder handen genomen en is de computer diepgaand onderzocht op de aanwezigheid van 'malware'. Zo zijn verdere nadelige effecten al zo'n beetje in de kiem gesmoord.

Ik vind het nog steeds een boeiend relaas en vraag me af hoeveel UMCG of RUG IT-gebruikers in de valkuil van de geboden alternatieven zouden zijn getrapt.

Werken aan de grenzen

Wat kun je nou als organisatie ondernemen tegen dit soort steeds slimmere virussen, Trojaanse paarden en phishing-pogingen? De RUG gebruikt als slagzin 'werken aan de grenzen van het weten'. Mooi hè? Kennis is immers macht.

Maar die kennis kan ook bij het gebruik van IT-voorzieningen te pas komen. Een gewaarschuwd mens telt voor twee, dus wellicht kan door goede voorlichting worden voorkomen dat 'phishers', virussen en Trojaanse paarden hun slag kunnen slaan. Nee, de organisatie vraagt NOOIT per e-mail naar uw login-gegevens. Als u een e-mail krijgt of een niet-geauthenticeerde webpagina waarin dat WEL gebeurt, is dat ALTIJD een phising-poging.

Voor het openen van attachments en ophalen van niet-geauthenticeerde programma's blijft iedereen uiteindelijk zelf verantwoordelijk, hoewel een virusscanner kan helpen. Daarnaast doen we als organisatie het nodige om misbruik zo goed mogelijk te voorkomen en te beperken. Zo'n verdediging bestaat altijd uit meerdere en verschillende soorten lagen.

Voorkomen...

Eerder is het quarantainegebied van de virusscanner al genoemd. Een mooi concept: wat niet lijkt te deugen zetten we apart op een plek waar de kwaadwillige programmatuur niks kan uitvreten. Dat kan ook op ruimere schaal.

Na een lange voorbereidingstijd, waarbij allerlei verwachte en onverwachte problemen moesten worden opgelost, begint het CIT deze maand met het testen van Quarantainenet (zie **www.quarantainenet.com**).

Quarantainenet

Het mooie van Quarantainenet is dat het los staat van de computer. Kwaadaardige software zoals virussen, wormen en spyware kan dus niet 'quarantainenet even uitzetten', zoals het de virusscanner 'even uit kan zetten'. Kort samengevat is de gedachte achter Quarantainenet dat een besmette computer afwijkend gedrag vertoont dat te detecteren is. Het Quarantainenet plaatst zo'n computer dan in 'quarantaine': in een apart netwerk waarbij de gebruiker nog slechts de vereiste reparaties kan uitvoeren. Zodra die zijn uitgevoerd, kan de computer weer toegang tot het internet worden verleend.

De komende periode wordt het Quarantainenet binnen het CIT uitgetest, waarna het de bedoeling is Quarantainenet voor de hele RUG in te voeren. Voorkomen is natuurlijk beter dan genezen. Alert reageren op potentieel verdachte situaties helpt plaatsing in het Quarantainenet te voorkomen.

Frank B. Brokken,
(Rijdt geen (Trojaans) paard)