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

Losgeldwaar

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.

Een beetje rommelige vertaling van 'ransomware'. Wat is dat nou weer? Nou, iets waar je ècht voor uit moet kijken. De leden van de SCIRT-groep (SURFnet Community van Incident Response Teams, **https://www.surf.nl/diensten-en-producten/surfcert/csirts/surfnet-community-van-incident-response-teams-scirt/index.html**) zijn IT-securityspecialisten van Nederlandse universiteiten, academische ziekenhuizen en hogescholen. Begin februari was er binnen SCIRT een klein e-mailstormpje over ransomware. Belangrijk genoeg om er ook in deze Pictogrambijdrage aandacht aan te besteden.

Detectivefilm

Ransom is losgeld. Je neemt iemand in gijzeling, en belooft (bijvoorbeeld) de familie om de gijzelaar weer vrij te laten wanneer je een zeker losgeld hebt ontvangen. Een dankbaar onderwerp voor talrijke detectivefilms (bijv. 'Ransom', 1996, **https://www.surf.nl/diensten-en-producten/surfcert/csirts/surfnet-community-van-incident-response-teams-scirt/index.html**).

Wat heeft dat nou met computers te maken, zo vraag je je wellicht af. Wel, de parallel is eenvoudig: iemand neemt je computer in gijzeling en je krijgt 'm pas terug wanneer er een flink losgeld is betaald.

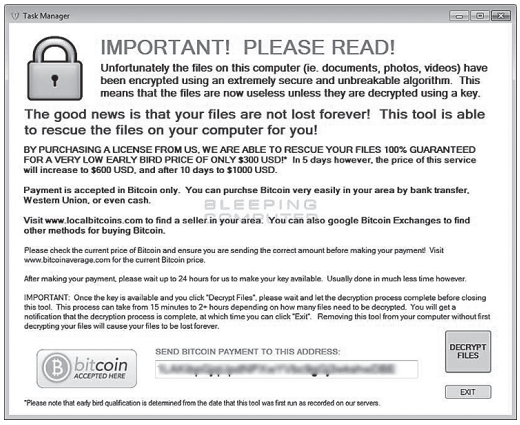
Oké, maar zo eenvoudig is dat toch niet? Word je computer ontvoerd en in een schuurtje ergens achteraf opgesloten?

Nee. Het ligt iets subtieler. Vrijwel alle computers zijn verbonden aan het internet, en de meeste computergebruikers lezen e-mail, downloaden bestanden, bekijken documenten, etc. etc. Kortom: normaal computergebruik. En daarvan maakt de potentiële gijzelnemer misbruik.

Verleidelijke link

We weten natuurlijk al dat het niet verstandig is om domweg te reageren op e-mail waarin ons wordt verteld dat 'ons account moet worden gereactiveerd' en of we maar even op deze of gene link willen klikken. Phishing dus.

Maar de gijzelnemers doen iets anders. Je krijgt een e-mailtje met mogelijk een verleidelijke link (klik hier, beantwoord een paar vragen



en je krijgt een cadeaubon van Albert Heijn ter waarde van € 50), of een bijlage die je gedachteloos opent (of, nog mooier, je gebruikt een 'user-friendly' besturingssysteem, die de bijlage alvast voor je opent). En dan ben je de sigaar.

Wat er dan gebeurt, is het volgende: alle bestanden die vanuit jouw account toegankelijk zijn, worden versleuteld. Die versleuteling is geen kinderspel: er is geen manier om de versleuteling binnen afzienbare tijd te doorbreken. Tevens krijg je de informatie dat de versleuteling ongedaan kan worden gemaakt door bitcoins over te maken naar een bepaald adres (**https://en.bitcoin.it/wiki/**).

Bitcoins bestaan al jaren, en hebben een eigen koers ten opzichte van de euro. Op dit moment is één bitcoin ruim € 200 waard, maar de koers, die oorspronkelijk enige eurocenten was, heeft ook al eens rond de € 1.000 geschommeld. Het losgeld moet weliswaar in bitcoins worden betaald, maar het bedrag van het losgeld is vermeld in US dollars. Is de koers van de bitcoin laag, dan dien je wat meer bitcoins over te maken; is de koers toevallig hoog, dan wat minder.

Slecht en goed nieuws

Waarom bitcoins? Omdat bitcoin-transacties niet kunnen worden getraceerd. Er is geen bijbehorende bank die een overzicht bijhoudt van bitcoin-transacties. Wanneer ik bitcoins overmaak naar een bitcoin-adres is het niet mogelijk om de transactie te volgen om zo te achterhalen bij wie dat adres nou eigenlijk hoort. Bitcoin-adressen zien er misschien wat vreemd uit. Probeer voor de aardigheid eens een euro of zo (dus op dit moment BTC 0.005) over te maken naar bitcoin-adres 3GHs8ffsgEJNwUK-2wQPx6GXzhnqNG4HMU6.

Ik verklap een geheimpje: dat is één van mijn bitcoin-adressen. Maar wanneer ik die informatie niet geef, dan is het onmogelijk om te achterhalen dat het genoemde adres door mij wordt gebruikt. Bitcoin-adressen zijn niet zo stabiel als bijvoorbeeld een huisadres of e-mailadres. Op elk gewenst moment kan ik mijn bitcoin-adres wijzigen, en die methode wordt bijvoorbeeld gebruikt door de gijzelnemers om te bepalen of het losgeld voor jouw computer is ontvangen: elke gegijzelde computer is geassocieerd met een eigen, uniek bitcoin-adres waar het losgeld naar moet worden overgemaakt.

Tot zover het slechte nieuws.

Het goede nieuws is natuurlijk dat een gewaarschuwd mens voor twee telt. Wie weet dat er zoiets als ransomware bestaat, is wellicht extra voorzichtig met het openen (of laten openen, bijvoorbeeld automatisch door het besturingssysteem) van bijlagen bij e-mail of met het downloaden van programma's waarvan de herkomst niet kan worden achterhaald. Dat helpt al. Maar er zijn nog meer manieren om gijzeling te voorkomen of, mocht het je ooit overkomen, om de effecten ervan te minimaliseren.

Volgens mij bestaat de belangrijkste verdediging eruit dat er te allen tijde een goede, actuele, frequent bijgewerkte, en operationele back-up is, die is opgeslagen op een andere computer. Controleer in ieder geval of de back-up operationeel is: selecteer zo nu en dan eens een willekeurig bestand, en controleer of dat bestand kan worden opgevraagd van de meest recente back-up.

Controleer ook of het bestand in de versie van bijvoorbeeld vorige week kan worden opgevraagd. Als dat lukt, dan is de meest vervelende consequentie van ransomware dat alle files die vanaf je account kunnen worden beschreven van de disk moeten worden verwijderd om vervolgens weer van de back-up te worden hersteld.

Elektronische handtekening

De frase 'alle files die vanaf je account kunnen worden beschreven' is belangrijk. Omdat 'admin'- of 'root'-accounts toegang tot alle files hebben, is het onverstandig om die accounts voor dagelijkse werkzaamheden te gebruiken. Wie dat toch doet, loopt het risico dat *alle* files worden versleuteld door ransomware. En dat betekent uiteraard dat de bijbehorende herstelwerkzaamheden overeenkomstig complex worden. Niet doen, dus.

Veel ellende kan ook worden voorkomen door e-mail standaard elektronisch te ondertekenen. Wanneer iedereen dat zou doen, dan zouden we in één klap verlost zijn van phishing en ransomware. De bad guys kunnen dat namelijk niet doen omdat hun identiteit dan bekend is.

Het is relatief eenvoudig om e-mail te signeren. Voor RUG-medewerkers kan een e-mailcertificaat worden aangevraagd op **https://mijncertificaat.surfnet.nl**.

Een alternatief, op ruime schaal gebruikt binnen FWN, is het gebruik van Pretty Good Privacy (PGP). Zie bijvoorbeeld **https://www.enigmail.net en https://security.rug.nl/docs/gpg/howto-pgp.pdf**.

Frank B. Brokken
(telt minstens voor vier...)