Het Parool
05-10-2016

Je krijgt je bestanden alleen terug als je het ontsleutel-wacht- woord koopt voor €299

Een pakketje dat niet kon worden bezorgd; duizenden mensen trapten deze zomer in dit onschuldig ogend mailtje. Voordat ze het wisten, was hun computer gegijzeld. Hoe voorkom je dat?

HERMAN STIL

Het gaf een aardig inkijkje in de wereld van de digitale gijzelnemers, toen het digiteam van de Nationale Recherche onlangs na een tip een aantal computerservers observeerde van waaruit sinds begin juli aanvallen waren uitgevoerd. In een paar dagen hadden 5800 computeraars - onder wie zo'n drieduizend Nederlanders - plotseling een Engelstalige boodschap op hun computerscherm gekregen: 'Al je bestanden zijn versleuteld met de Wildfire Locker.' Ze hadden geklikt op een op het oog betrouwbaar mailtje van het Utrechtse Transportbedrijf Buitink: 'Mislukte afleverpoging BT-32084' stond er boven. Een chauffeur had 'geprobeert' (de spelfout is opzettelijk) een pakketje af te leveren, maar was daar kennelijk niet in geslaagd. Geen paniek: 'U kunt een nieuwe afspraak maken door het volgende formulier te downloaden, in te vullen en retour te mailen'. Met vriendelijke groet, Anna Dorst. Zowel Buitink als Anna Dorst bestaan alleen in cyberspace. Wie op het genoemde tranportbedrijfbuitink.nl klikte, kreeg de mededeling dat de site eventjes buiten gebruik was, vanwege onderhoud. Dat formulier was een echt Wordbestand. Alleen, zo flitste bij veel gebruikers een mededeling op, was het formulier gemaakt in een oude versie van de Microsofttekstverwerker. Of de gebruiker in zijn Wordversie maar even de functies 'bewerken' en 'inhoud' wilde inschakelen. Die zogeheten macro's staan standaard uit, juist omdat ze kunnen worden misbruikt. De 5800 mensen die dat deden, haalden zo via een onbeschermd achterdeurtje in Word ongemerkt het versleutelvirus binnen, ook omdat het op dat moment van de vijftig meestgebruikte virusscanners door maar vijftien als kwaadaardig werd bestempeld. Het virus nestelde zich bij Windowsgebruikers op de harde schijf, vertakte zich in het

besturingssysteem, om vervolgens in razend tempo alle bestanden door elkaar te husselen, tot de bestandsnamen aan toe. De bestanden en de bestandsnamen werden zodanig versleuteld dat de gebruiker ze niet eens meer kon vinden. Het enige begrijpelijke was een barse mededeling op het scherm: 'De enige manier waarop je je bestanden terugkrijgt, is door het ontsleutelwachtwoord te kopen voor 299 euro'. Snelheid was geboden. Als niet binnen acht dagen werd betaald, ging het losgeld naar 999 euro. 236 getroffenen rekenden daarop 299 euro af. Daarmee was het niet eens een grote aanval geweest. Maar met een opbrengst van 135,9 bitcoin (omgerekend toen 69.322,75 euro) was het wel een heel succesvolle.

botnets

Wildfire, dat eind juni voor het eerst opdook als variant van een ander gijzelprogramma, Zyklon, is een van de vele gijzelvirussen die de ronde doen. Volgens Europol vormen zulke afpersvirussen inmiddels de belangrijkste bedreiging voor computers, mobieltjes en tablets. Logisch vanuit het perspectief van de cybercrimineel. Wie persoonsgegevens en creditcardnummers steelt, zal deze toch eerst te gelde moeten maken, waarbij de digiboeven het risico lopen zichzelf bloot te geven. Bij cybergijzeling is dat niet nodig; het slachtoffer betaalt. En het aloude follow the money gaat niet op. Door zich te laten uitbetalen in bitcoin of andere virtuele munten loopt het spoor vrijwel meteen dood. Digitale gijzelnemers hoeven zich slechts te verschuilen achter een netwerk van gekraakte computers (botnets) en servers die vaak worden 'gehuurd' van andere criminelen. Ook de benodigde virussen kunnen, naar believen aangepast, worden aangeschaft via het donkere web. Zo vond cyberbeveiliger Kaspersky deze zomer een criminele marktplaats waar vanaf zes dollar per dag een gekraakte server 'te koop' stond waarmee aanvallen konden worden uitgevoerd, zonder dat deze direct naar de bron was te herleiden. Het Wildfiremailtje was afkomstig van tientallen gekraakte mailadressen. Het kon worden herleid naar een gekraakt computeradres in Sint-Petersburg, Rusland. De genoemde internetnaam was geregistreerd in de Verenigde Arabische Emiraten, op een gehackte server waar nog veel meer fictieve transportbedrijven een domeinnaam hadden. En de taalinstellingen van het bestand wezen dan weer op een Poolse herkomst. Tegenover dat lage risico staan hoge verdiensten. Zo volgde cyberbeveiliger Symantec het gijzelvirus Reveton. De virusbestrijder telde in enkele dagen een half miljoen besmettingen. Daarvan bleken uiteindelijk 15.000 slachtoffers bereid losgeld te betalen, gemiddeld honderd dollar. De cyberbende zette zo anderhalf miljoen dollar om.

Stockholmsyndroom

Geen wonder dat gijzelvirussen een enorme bloei doormaken. In de eerste helft van het jaar vond Europol vijf keer zo veel besmettingen als een jaar geleden. Nederland

laat zich daarbij volgens virusbestrijder Kaspersky van zijn onnozele kant zien: ons land is de nummer vier in de wereld waar het gaat om ransomware-besmettingen. Volgens een recent cyberrapport van het Centraal plan Bureau (CPB) is in een jaar ruim één procent van alle computergebruikers getroffen door losgeldsoftware. In twee derde van de gevallen gaat het om besmetting bij particulieren. Die zwijgen daar meestal over - uit schaamte, angst of vanwege de digitale variant van het stockholmsyndroom: dat de gegijzelde sympathie krijgt voor de gijzelnemer. In Nederland werd tussen april 2014 en april 2015 maar 87 keer aangifte gedaan bij de politie van ransomware-besmettingen. Onwaarschijnlijk laag, omdat in die periode het rabiate gijzelvirus Coinvault90 alleen al ruim duizend Nederlandse pc's besmette. Al betaalt het overgrote deel van de slachtoffers niet, de schade is toch groot. Afhankelijk van de impact zijn slachtoffers gemiddeld zo'n acht uur bezig om de schade te herstellen, of ze maken kosten door het inschakelen van gespecialiseerde beveiligingsbedrijven. Volgens het CPB is het dan ook niet langer houdbaar om de verantwoordelijkheid voor beveiliging vooral bij computergebruikers neer te leggen. Het stelt voor dat softwaremakers die consequent lekken open laten staan, worden beboet. Microsoft bijvoorbeeld, dat ondanks alle waarschuwingen het Wordlek nog altijd niet afdoende heeft gedicht. Transportbedrijf Buitink is allang opgevolgd door een reeks andere koeriersdiensten, toeleveranciers of zakenpartners die bedelen om een nieuwe bezorgafspraak. Zo doen alweer koeriersmailtjes de ronde van het eveneens Utrechtse Steehouwer Transport of van transportbedrijf Grijpmans, met vriendelijke groet van Carla Woestenburg. Want zolang er mensen zijn die zulke mailtjes voor waar aannemen, zijn er criminelen die ze zullen versturen.

HELP, IK BEN AL GEGIJZELD

- Doe aangifte. - Ga op een andere computer naar www.nomoreransom.org, een actiesite van Europol, de Nederlandse politie, Kaspersky en Intel. Daar staat een aantal gratis 'sleutels', waarmee bestanden weer kunnen worden vrijgegeven. - Google anders de naam van het gijzelvirus; goede kans dat er fora zijn waar slachtoffers hun ervaringen uitwisselen. - Geregeld geback-upt? Start de computer in veilige modus, verwijder alle bestanden - inclusief het besturingssysteem - formatteer de harddisk en installeer alles opnieuw vanaf de externe back-upschijf. Lukt opstarten niet, installeer via een andere computer Hitman Pro op een usb-stick en volg de stappen. - Wie geen actuele back-up heeft, zal geneigd zijn te betalen. Het blijft een gok of bestanden dan worden ontsleuteld, al willen veel cybercriminelen een goede 'reputatie' houden. - De politie raadt betalen af, om te voorkomen dat weer nieuwe pogingen worden gefinancierd. - Bovendien: wie betaalt, is bekend in het wereldje van de cybercriminelen. Dat vergroot de kans dat die vaker zullen aankloppen.

IK WIL GEEN GIJZELAAR WORDEN

- Gebruik altijd betrouwbare virusprogramma's en zet de beveiliging van de computer of smartphone op zijn strengste stand, update besturingssysteem en programma's automatisch. - Maak zeer regelmatig, bij gemiddeld computergebruik tweewekelijks, een complete back-up (image back-up) van alles wat op de computer staat. Gebruik daarvoor een externe harde schijf en koppel deze na de back-up los. - Open nooit zomaar bestanden of url's in mailtjes, trek deze eerst na. Ga nooit in op verzoeken instellingen aan te passen, hoe betrouwbaar deze er ook uitzien.