ftm.nl

Afperssoftware blijkt cyberwapen: vijf vragen over (Niet-)Petya FTM

Luuk van der Sterren

14-18 minuten

Deze week was het raak: duizenden computers wereldwijd werden getroffen door een plotse cyberaanval die zich als een lopend vuurtje verspreidde. Onder andere containergigant Maersk en TNT Express werden slachtoffer. Hoe kon dit gebeuren? En is deze aanval wel wat het lijkt? We zetten de zaak op een rijtje.

Wat gebeurt er als het bedrijf dat bijna een zesde van *alle* wereldhandel vervoert plots geen orders meer kan aannemen? Of dagenlang geen schepen kan in- en uitladen? Niet meer weet welke container zich waar bevindt? Juist: een logistieke nachtmerrie met honderden containerschepen en miljoenen containers in de hoofdrol.

Deze nachtmerrie werd bittere realiteit voor de Deense containergigant A.P. Moller-Maersk. Afgelopen dinsdag werd het bedrijf getroffen door een grootschalige cyberaanval; wereldwijd vielen de computersystemen van Maersk ten prooi aan een virus dat belangrijke data versleutelt en losgeld eist voor de sleutel. Het bedrijf was vrijdagochtend nog altijd niet volledig bekomen van de crash, waarvan de schade met de minuut oploopt.

Maersk was niet het enige slachtoffer: ook andere multinationals, zoals WPP, ‘s werelds grootste reclamebureau,

advocatenkantoor DLA Piper, TNT Express, farmareus Merck, Beiersdorf en Deutsche Post vielen ten prooi aan de 'ransomware', die als een lopend vuurtje rondging.

De totale schade loopt vermoedelijk in de honderden miljoenen. Toch lijkt het er niet op dat de makers van de afperssoftware er veel aan over zullen houden. Sterker nog: als de daders hieraan geld hoopten te verdienen, hebben ze het bijzonder slecht aangepakt.

Het is dan ook goed mogelijk dat deze 'Petya'-ransomware niet is wat het lijkt en dat de beweegredenen voor de aanval niet crimineel, maar politiek van aard zijn. Wat is er hier gaande? En hoe kon deze digitale ramp zich zo snel verspreiden? We zetten de zaken voor je op een rijtje.

1. Wat is er nu gebeurd?

Dinsdagochtend doen de eerste berichten de ronde over een grote cyberaanval. Op de Rotterdamse Maasvlakte staan de containerhavens van APM — een dochteronderneming van Maersk — vanaf dinsdagmiddag stil. Ook bij TNT Express gaan de systemen op zwart. Bij TNT is de chaos zelfs dusdanig groot dat de handel in aandelen van moederbedrijf FedEx tijdelijk gestaakt moet worden.

Al snel duiken er beelden op, veelal uit Oekraïne, van computers die zijn geïnfecteerd door kwaadaardige software. Op de beeldschermen is niets te zien dan een Engelse tekst: in dreigende rode letters meldt deze dat alle gegevens op de computer zijn versleuteld. Om de toegang terug te krijgen, zo staat er, moeten gebruikers 300 dollar in bitcoin overmaken naar de bitcoin-portomonnee van de hackers en een mailtje sturen naar een wegwerp-emailadres. De daders zullen dan een code

terugsturen; daarmee zullen de bestanden weer hersteld kunnen worden.

> ‘Petya’ is een cyberwapen in vermomming

Het lijkt er in eerste instantie dus sterk op dat het hier gaat om grootscheepse digitale gijzelneming, vergelijkbaar met de WannaCry-epidemie van afgelopen maand. Bij die aanval werden in een paar dagen tijd meer dan 200 duizend computers besmet. Antivirusbedrijven als Kaspersky en F-Secure nemen een kijkje onder de motorkap van dit nieuwe virus en vinden sterke overeenkomsten met ‘Petya’, een type afperssoftware dat al in 2016 over het internet ging. Zodoende werd deze kwaadaardige software al snel dezelfde naam toegedicht.

Maar, zo blijkt na verder onderzoek: de 2017-versie van ‘Petya’ is helemaal geen ransomware. Beveiligingsexpert Matt Suiche legt uit dat het programmaatje niet is ontworpen om de versleuteling die het aanbrengt weer op te heffen; in plaats daarvan wordt de harde schijf van besmette computers doodleuk onbruikbaar gemaakt. Even later komt antivirusbedrijf Kaspersky tot dezelfde conclusie.

Met andere woorden: Petya (of ‘NotPetya’, zoals het beestje nu wordt genoemd) is waarschijnlijk niet gebouwd om geld te verdienen — het doel is om zoveel mogelijk chaos te scheppen.

2. Wie (en wat) zit hier dan achter?

Er is nog weinig met zekerheid te zeggen over wie de daders zijn en wat hun motief is. Er zijn echter wel enkele aanknopingspunten.

Om te beginnen: bij ‘normale’ ransomware is het motief vooral financieel. Een grote schare cybercriminelen is er in de afgelopen jaren achter gekomen dat er bergen geld valt te

verdienen aan het gijzelen van persoonlijke data van consumenten. Zo ontdekten onderzoekers van Cisco Systems in 2015 een ransomware-operatie die de daders meer dan 30 miljoen dollar per jaar opleverde.

"Het is onwaarschijnlijk dat het de daders om het geld ging"

Ter vergelijking, de bitcoin-rekening waar slachtoffers van NotPetya hun losgeld naar moeten overmaken bevat op het moment van schrijven nog geen tienduizend euro. Een schijntje.

Dan is er nog een opvallende aanwijzing: NotPetya versleutelt — in tegenstelling tot de originele Petya-ransomware — helemaal geen foto's of video's. Justin Cappos, assistent-hoogleraar Digitale Veiligheid op New York University, vindt dat verdacht: 'Als je je op consumenten zou richten, zou je normaal gesproken juist die bestanden willen versleutelen,' aldus Cappos tegen de Britse technologiewebsite *The Register*. 'Slachtoffers geven namelijk om hun babyfoto's.' Als de daders van plan waren om consumenten af te persen, is dit wel een erg zwakke poging.

Je zou kunnen stellen dat ze zich juist op bedrijven richten, maar ook die vlieger gaat gaat niet op. Het hele verdienmodel van ransomware is gebaseerd op het vertrouwen dat slachtoffers hun gegevens na betaling terugkrijgen. Zoals gezegd is dit bij NotPetya niet het geval: de schade is onherstelbaar. Tenzij de daders bijzonder amateuristisch zijn, is het dus onwaarschijnlijk dat het hier om geld gaat.

> Bij de kerncentrale van Tsjernobyl werd de meetapparatuur voor radioactieve straling uitgeschakeld

Maar wat is dan het motief voor deze aanval? Een belangrijke aanwijzing zit hem in de vraag *waar* de grootste schade wordt geleden: de overgrote meerderheid — volgens antivirusbedrijf ESET ruim 90 procent — van alle infecties werd gevonden in

Oekraïne. Zo werd bij de kerncentrale van Tsjernobyl de meetapparatuur voor radioactieve straling uitgeschakeld. Ook de computersystemen van diverse Oekraïense energiebedrijven, banken, overheden en het vliegveld van Kiev gingen op zwart. Het was ook in dit land dat het virus voor het eerst opdook.

Oekraïne wordt al tijden geteisterd door grootschalige cyberaanvallen, die veelal afkomstig zijn uit Rusland. In een artikel dat onlangs op *Wired* verscheen zegt NAVO-ambassadeur Kenneth Geers dat je 'nauwelijks een plaats in Oekraïne kunt vinden waar er *geen* aanval is geweest.'

Het is dus goed mogelijk dat het hier om een gerichte aanval op het land gaat. In Oost-Oekraïne is op dit moment nog altijd een oorlog gaande en het is niet ondenkbaar dat NotPetya simpelweg een nieuw wapen in deze strijd is.

3. Hoe verspreidt het virus zich zo snel?

NotPetya werd door hackers verstopt in een valse update van de boekhoudsoftware MeDoc. Dat programma is erg populair in Oekraïne — en met reden: data-veiligheidsexpert 'The Grugq' (echte naam onbekend) geeft aan dat het een van de twee financiële softwarepakketten is die door de Oekraïense belastingdienst worden erkend. Als je in Oekraïne een vorm van omzetbelasting moet betalen, is de kans dus groot dat je MeDoc gebruikt.

Op deze manier bekeken is de schade bij Maersk en andere multinationals simpelweg een vorm van '*collateral damage*', veroorzaakt door het feit dat ze ook in Oekraïne opereren. Uit een vacature van Maersk blijkt dat het bedrijf in dit land gebruikmaakt van het MeDoc-pakket.

> In plaats van het lek te melden, besloot de NSA er zelf gebruik

van te maken

Dan is er ook nog het verhaal dat zich onder de 'motorkap' van het virus afspeelt. NotPetya is zo ontworpen dat het zich razendsnel door gesloten netwerken — zoals het intranet van een multinational — kan verspreiden. Het virus is dus mogelijk via deze weg bij Maersk-dochter APM in de Rotterdamse haven beland.

Verder is het grotendeels gebouwd op dezelfde 'exploit' als de WannaCry-ransomware. Deze exploit, ETERNALBLUE geheten, werd in het geheim door de Amerikaanse National Security Agency (NSA) ontwikkeld en maakt misbruik van een lek dat mogelijk al sinds 2000 in Microsoft Windows zit.

Volgens de Amerikaanse burgerrechtenbeweging ACLU weet de NSA al zo'n vijf jaar van het bestaan van het lek af. In plaats van dit aan Microsoft te melden zodat die het probleem konden verhelpen, besloot de inlichtingendienst het lek echter geheim te houden om er zelf gebruik van te kunnen maken.

De NSA doet dit omdat het zich — net als de CIA en FBI — bezig met zogenaamde *offensieve* digitale oorlogsvoering. In plaats van computersystemen veiliger te maken, probeert de Amerikaanse overheid bestaande kwetsbaarheden in te zetten als digitale wapens om bijvoorbeeld criminelen en terroristen af te tappen.

"Zodra je computer besmet is en je de rode letters ziet, is het over en sluiten"

Als het aan onze regering ligt mag de Nederlandse politie dit in de nabije toekomst overigens ook gaan doen. Afgelopen december werd door een meerderheid van de Tweede Kamer het ‘Hackvoorstel’ aangenomen. Deze wet stelt de politie in staat om kwetsbaarheden in software aan te kopen en te gebruiken

om computers en smartphones te hacken. Zodoende hoopt de politie haar digitale opsporingsvermogen uit te breiden.

Het was natuurlijk niet de bedoeling dat de digitale wapens van de NSA in verkeerde handen vielen. Toch is de Eternalblue-exploit april dit jaar in de openbaarheid terechtgekomen, vermoedelijk via een geheimzinnige groep die zichzelf 'The Shadow Brokers' noemt. Deze organisatie houdt zich sinds zomer 2016 bezig met het lekken van diverse NSA-documenten en software. Via anonieme kanalen veilt de groep de geheime informatie voor tienduizenden dollars.

4. Wat als je zelf te maken krijgt met zo'n cyberaanval?

Om met het slechte nieuws te beginnen: zodra je computer besmet is en je de rode letters ziet, is het over en sluiten. NotPetya versleutelt niet alleen een groot deel van je bestanden onherroepelijk; het vernielt ook nog eens je harde schijf zelf.

Het goede nieuws is dat het redelijk eenvoudig is om een besmetting te voorkomen. Het beveiligingslek waarvan NotPetya gebruikmaakt is bekend en praktisch alle populaire virusscanners — inclusief die van Microsoft zelf — hebben het virus inmiddels in hun database opgenomen. Zolang je je software dus up-to-date houdt, is het risico op besmetting gering. Aangezien het virus zich alleen richt op computers met Windows, hoeven mensen met macOS of Linux zich überhaupt geen zorgen te maken.

Mocht je onverhoopt toch besmet raken, dan is niet alles meteen verloren. NotPetya heeft namelijk enige tijd nodig om de bestanden op je harde schijf te versleutelen. Het scherm geeft dan aan dat de harde schijf op fouten wordt gecontroleerd, maar

dat is een nepbericht. Als je op dat moment de stekker eruit trekt, zijn de gegevens mogelijk nog te redden.

5. Hoe nu verder?

In het geval van de NotPetya-malware zal het aantal nieuwe infecties de komende tijd waarschijnlijk sterk terug blijven lopen. Het beveiligingslek is inmiddels gedicht en vrijwel alle populaire virusscanners herkennen het virus. Voor de computers die al besmet zijn, is het echter te laat; alle gegevens die daarop stonden zijn verloren gegaan.

Het zal dus nog wel even duren voordat de getroffen bedrijven en organisaties van de crash hersteld zijn. Zo was containerafhandelaar APM vrijdag nog steeds niet operationeel en had ook TNT Express nog altijd last van de storing.

Maar kijken we verder dan de directe gevolgen van deze aanval, dan zien we ook een groter plaatje. Het geval wil namelijk dat zowel NotPetya als de WannaCry-ransomware in feite gebaseerd zijn op digitale wapens die door de overheid werden gebouwd en vervolgens in de verkeerde handen zijn gevallen.

> De cyberwapens kunnen ook in handen van terroristische organisaties vallen

De ACLU leverde na de WannaCry-epidemie al stevige kritiek op het cyber-beleid van de Amerikaanse overheid. De burgerrechtenbeweging stelt dat het geheim houden van veiligheidslekken ervoor zorgt dat de digitale infrastructuur als geheel kwetsbaarder wordt — en dat zorgt ervoor dat iedereen minder veilig is.

Met de gebeurtenissen van deze week begint dat kritische geluid in kracht toe te nemen. Zo beschuldigde de directeur van Microsoft de NSA ervan de ‘bron’ van de kwetsbaarheden te zijn;

in de *New York Times* waarschuwt een voormalig overheidsmedewerker voor het feit dat cyberwapens als ETERNALBLUE dankzij de Shadow Brokers nu ook in handen van terroristische organisaties — denk aan IS — kunnen vallen.

Digitale wapens zullen in de toekomst hoogstwaarschijnlijk een steeds belangrijkere rol gaan spelen. Naarmate onze economische afhankelijkheid van computersystemen groter wordt, groeit ook de potentiële schade die iemand met het juiste virus in een paar uur tijd aan kan richten.

Dit gegeven roept in ieder geval een aantal vragen op. Willen we dat onze overheid zich actief bezig houdt met het creëren en open houden van nieuwe lekken? Vertrouwen we erop dat deze haar cyberwapens veilig kan bewaren, zeker gezien de slechte resultaten uit het verleden? En is het risico op een digitale ramp — denk bijvoorbeeld aan Amerikaanse ziekenhuizen die operaties moeten annuleren vanwege de cyberaanval in Oekraïne — een acceptabel verlies in de strijd tegen terrorisme?

Het is geen gemakkelijke discussie, niet in de laatste plaats omdat het onderwerp erg technisch is. Toch is het van belang dat we hier bij stilstaan. Zoals we deze week hebben gezien kan het gebruik van digitale wapens ook duizenden kilometers verderop nog tot gigantische *collateral damage* leiden.

Over de auteur

Luuk van der Sterren

Studeerde aan het Amsterdam University College en is tegenwoordig chef eindredactie en huisnerd van FTM.

Lees meer

Volg deze auteur