de Correspondent

02.02.2016 • Leestijd 10 - 13 minuten

Een Nederlandse student, enkele onderzoekers, enkele securitybedrijven en de FBI haalden een berucht crimineel netwerk offline. Een reconstructie van een bijzondere zaak.

Hoe een opmerkelijke coalitie een Russische crimineel bestreed

Correspondent Hacken

Dimitri **TOKMETZIS**

Illustratie: Erwin Kho (voor De Correspondent)

Het was een enorme bende. Aan de top stonden zo'n vijftig fraudeurs, die honderden onderknuppels aanstuurden, die weer bijna 200.000 handlangers in konden zetten.

Die handlangers waren overal geïnfiltreerd: in ziekenhuizen, bij banken, bij overheidsdiensten, bij bedrijven. Soms verstopten ze zich zelfs bij mensen thuis. Vervolgens probeerden ze andere criminelen te werven, inlogcodes te stelen en bankoverschrijvingen te onderscheppen.

Het ging nog verder. Vier jaar geleden wist een handlanger geïnfiltreerd bij een Amerikaanse zakenbank bijna zeven miljoen dollar over te boeken naar een vriend in Zwitserland. Hij kreeg daarbij hulp van duizenden andere handlangers. Op commando van een van de fraudeurs belden ze een week lang met zijn allen de bank, de klantenservice met vragen overspoelend. Zo kon die ene handlanger ongemerkt fraude plegen. Tot de FBI op het laatste moment de overboeking wist op te sporen en ongedaan kon maken.

Het gekke: geen van de handlangers wist wie zijn bazen of collega's waren. Wel had ieder bendelid een lijstje met zo'n vijftig adressen van andere handlangers. Regelmatig liepen ze die adressen af om te kijken of de bendeleden nog actief waren. Raakte het lijstje leeg, dan schreef de handlanger adressen over van de lijstjes van collega's die nog wel actief waren. Op die manier was iedereen altijd bereikbaar voor instructies.

Heel soms gebeurde het dat een handlanger niemand meer kon vinden. Dan pakte hij een ander papiertje met namen van onderknuppels erop. Een van hen gaf hem dan een nieuw lijstje. Soms waren ook die onderknuppels niet meer actief. Dan mocht het bendelid een geheim doosje openmaken met duizend adressen. Op een van die adressen lag dan een nieuw lijstje handlangers klaar. Zo kon hij zich weer aansluiten bij het criminele netwerk. En doorgaan met bankmedewerkers bellen.

Het lijkt erg veel moeite om een bende zo te runnen, maar in de praktijk werkte het erg goed. Hoeveel handlangers en onderknuppels de politie ook oppakte, de bende leed er niet onder en de bazen bleven buiten zicht. Tussen 2011 en 2014 kon de bende daardoor alleen al in de VS voor meer dan honderd miljoen dollar aan fraude plegen. Dat schat althans de FBI, die jarenlang op de top van de bende jaagde. In de rest van de wereld, vooral in Europa, zou de bende twee tot drie keer dat bedrag hebben buitgemaakt.

De naam van de bende was Gameover ZeuS, een groep criminelen die een volstrekt nieuwe vorm van georganiseerde criminaliteit bedreef. De handlangers en onderknuppels waren namelijk geen mensen, maar besmette computers van bedrijven en personen. Deze computers, ook wel zombies, bots of drones genoemd, maakten onderdeel uit van een van de succesvolste botnets ooit.

Was, bedreef, maakten - ik schrijf in de verleden tijd omdat het botnet succesvol bestreden is.

En wel door een Nederlandse student, zijn collega's en het Delftse securitybedrijf Fox-IT. Deze reconstructie laat zien hoe een veelvoorkomende vorm van online criminaliteit nu eigenlijk werkt: georganiseerde online criminaliteit lijkt niet op *The Sopranos*, maar eerder op Marktplaats. Daarnaast laat de val van Gameover ZeuS zien dat de opsporing en bestrijding van criminelen door nieuwe coalities wordt gedaan, van bedrijven, academici en binnen- en buitenlandse opsporingsdiensten.

Iemand nog een leuk scriptieonderwerp?

Het is zomer en Dennis Andriesse is op zoek naar een interessant onderwerp voor zijn masterscriptie. Hij studeert computerwetenschap aan de Vrije Universiteit en is geïnteresseerd in online veiligheid.

Het is 2011 en vanuit de securitygemeenschap is er veel interesse voor een relatief nieuw botnet, Gameover ZeuS, dat grote sommen geld weet te stelen van banken. ZeuS, dus zonder Gameover ervoor, is dan al een beruchte naam. Sinds ene 'Slavik' dit trojaanse paard ontwikkelde rond 2005, heeft de malware zich in miljoenen computers genesteld. Het virus blijkt uiterst effectief in het onderscheppen van inloggegevens voor onder andere internetbankieren. Volgens de FBI was ZeuS in 2010 en 2011 verantwoordelijk voor 60 tot 90 procent van alle online bankfraude.

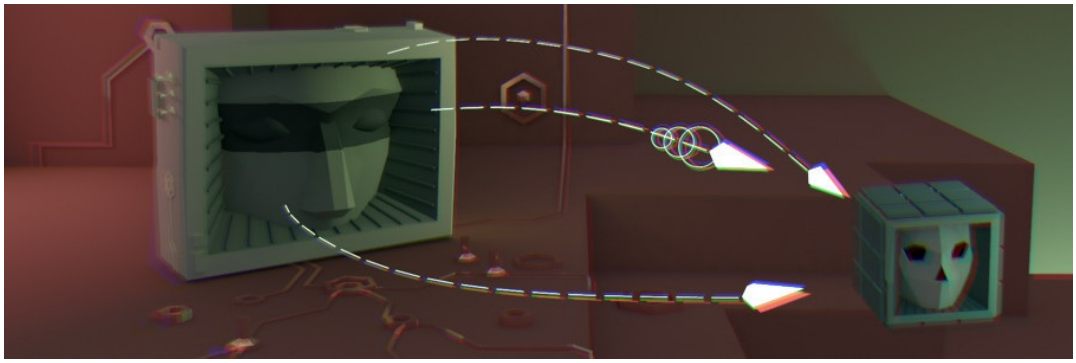
Volgens de FBI was ZeuS in 2010 en 2011 verantwoordelijk voor 60 tot 90 procent van alle online bankfraude

Maar in 2010 verdwijnt Slavik plotseling. Hij zegt met pensioen te gaan, maar maakt zich een tijdje onzichtbaar. Een concurrent, ene Gribodemon, neemt zijn werk over. Al snel komt de broncode online te staan. Hierna verschijnen duizenden varianten van de software die door verschillende criminelen wordt gebruikt om geld te stelen.

Rond dezelfde tijd heeft de politie redelijk goed door hoe ze ZeuS moet bestrijden: zoek de centrale server die alle bots aanstuurt en haal die offline. Ze krijgt daarbij hulp van websites als Abuse.ch en Shadowserver.org, die bijhouden welke websites besmet zijn.

In september 2011 komt Slavik met een nieuw wapen: Gameover ZeuS. Slaviks truc: geen gecentraliseerde, maar een gedecentraliseerde netwerkstructuur. Niet één server die commando's uitdeelt, maar bots die informatie bij andere bots ophalen - de handlangers van het begin van dit verhaal.

Terug naar Dennis Andriesse. Hij wil voor zijn masterscriptie onderzoeken hoe weerbarstig deze zogenoemde peer-to-peerbotnets zijn. Kun je het criminele netwerk ontregelen of zelfs overnemen?



Illustratie: Erwin Kho (voor De Correspondent)

Een exemplaar vangen

Ik spreek Andriesse in zijn werkkamer aan de VU. Het is een kale ruimte, enkel ontsierd door een enorme verzameling lege limonadeflessen van een collega. Andriesse (27) praat snel, maar geeft op alle vragen een zeer gestructureerd en precies antwoord, alsof hij een programma uitvoert. Ik had op een interview van twee uur gerekend, maar na drie kwartier sta ik buiten met alle informatie over zijn bizarre zoektocht.

Andriesse zorgde er eerst voor dat hij Gameover ZeuS te pakken kreeg. Gewoon door spam aan te trekken. En inderdaad: Gameover ZeuS dook al snel op in een paar e-mails.

De kunst was vervolgens om uit te vogelen wat de code van Gameover ZeuS nu eigenlijk deed. Zo'n code is niet meer dan een hoop nullen en enen die moet worden omgezet in een programmeertaal die door mensen te lezen is. Daarnaast is de code ingepakt in een zogenoemde *packer*. Die versleutelt een groot deel van de malware. Het kleine beetje code dat niet versleuteld is, scant eerst de computer die geïnfecteerd moet worden. Pas als alles goed is, pakt hij de rest van de code uit.

Na maanden puzzelen lukte het Andriesse om de basale werking van de malware te doorgronden. Daarmee kon hij ook inzicht krijgen in hoe geïnfecteerde computers met elkaar communiceren. Kennis die kon helpen een criminele bende op te sporen die voor miljoenen aan fraude had gepleegd.

De eerste aanval (en de eerste tegenaanval)

Inmiddels had Andriesse hulp gekregen van zijn begeleiders aan de VU en van academici en malwareonderzoekers uit Duitsland en Amerika. Het doel was om alle bots van Gameover ZeuS over te nemen, het botnet dat ontworpen was om nooit overgenomen te worden. Maar hoe? De onderzoekers wilden proberen de adreslijsten van de handlangers te vergiftigen door nieuwe adressen op die lijsten te plaatsen vanaf een server die zij controleerden. Die zou dan lege en dus onschadelijke commando's naar de handlangers sturen, waardoor die dachten nog steeds tot het Gameover Zeus-netwerk te behoren.

De eerst aanval vond plaats tussen 27 april en 17 mei 2012. De onderzoekers kwamen in Amsterdam bijeen om in intensieve codeersessies het botnet over te nemen, meestal bij iemand thuis, met een laptop op schoot. Ze slaagden erin om driekwart van de bots naar hun server te laten luisteren.

Pas na ongeveer drie weken kwamen Slavik en zijn kompanen achter de aanval. Hun antwoord was digitaal geweld: ze voerden meerdere DoS-aanvallen uit op de server van de onderzoekers. Die kon daardoor niet meer met de handlangers communiceren, die zich dus weer bij de servers van Slavik meldden om nieuwe adreslijsten op te halen.

Gameover ZeuS was nog niet verslagen.

Illustratie: Erwin Kho (voor De Correspondent)

Binnendringen in de krochten van Slavik

Andriesse wist op dat moment nog niet dat zeventig kilometer verderop een groep onderzoekers ook probeerde de bende van Slavik te bestrijden.

Het Delftse securitybedrijf Fox-IT namelijk. Dat volgt de ontwikkeling van ZeuS al bijna tien jaar op de voet omdat veel klanten schade ondervinden van de malware, bijvoorbeeld omdat hun rekeningen worden geplunderd. En daar waar Andriesse zich vooral op de netwerktechnologie richt, probeert Fox-IT inlichtingen te verzamelen over de bende zelf. Die inlichtingen deelt het bedrijf dan met de FBI.

Ik spreek af met Michael Sandee, securityexpert van Fox-IT. Hij nuanceert het beeld dat we hier te maken hebben met een strakke hiërarchische organisatie. Slavik was belangrijk, maar was niet de Godfather die de FBI later van hem maakte. Hij was vooral een slimme programmeur en handige zakenman die een veelgevraagde dienst leverde: het schrijven van goede malware.

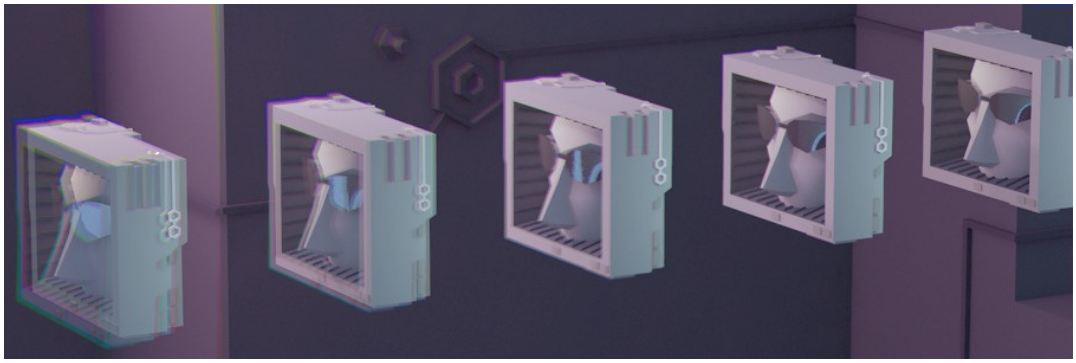
Sandee en zijn onderzoeksteam brachten de organisatie achter ZeuS in kaart door te infiltreren in ondergrondse fora. Slavik werkte samen met een klein kernteam met criminelen die luisterden naar namen als 'Temp Special,' 'Ded,' 'Chingiz 911' en 'mr. kykypyky.'

Slavik werkte samen met een klein kernteam met criminelen die luisterden naar namen als 'Temp Special,' 'Ded,' 'Chingiz 911' en 'mr. kykypyky'

Zij hadden een soort minimarktplaats gecreëerd waar enkele tientallen criminelen toegang tot hadden. Sommigen verhuurden delen van het botnet aan andere criminelen, anderen verleenden technische ondersteuning. Ook in de ondergrondse fora: leveranciers van malware die de bende niet zelf kon of wilde ontwikkelen én klanten die sub-botnets huurden voor eigen spam- of fraudecampagnes. Sommige criminelen konden zich inkopen in deze '*businessclub*' en kregen, als ze betrouwbaar werden bevonden, meer rechten.

Dan was er nog de afdeling debiteuren/crediteuren, de zogenoemde *money mules*. Die wisten vaak niet eens dat ze deel uitmaakten van een criminele organisatie en moesten een bedrijfsrekening openen en geld doorsluizen naar rekeningen in China, Hongkong, Cyprus en Letland. Volgens Sandee was dit de kunde en effectiviteit van het team dat Gameover ZeuS zo succesvol maakte: ze wisten als geen andere online criminele groepering grote sommen geld door te sluizen.

Er waren dus veel criminelen bij Gameover ZeuS betrokken. En daar waar veel mensen zijn, wordt er veel gepraat, zeker als sommigen ontevreden zijn. Van een of meerdere ontevreden klanten of medewerkers kreeg Fox-IT een aantal inlogcodes van Gameover Zeus-servers toegespeeld. Daarmee kwamen ze bij de administratie die inzicht gaf in alle transacties tot aan 2012, de Jabberaccounts en chatlogs van de aangesloten criminelen en een ticketsysteem met klachten over software en hoe en door wie die opgelost waren. Door dat ticketsysteem kon Fox-IT eenvoudig bij elkaar puzzelen wie welke taken had binnen de organisatie



Illustratie: Erwin Kho (voor De Correspondent)

Alle puzzelstukken op hun plaats

Terwijl Fox-IT de organisatie in kaart bracht en inlichtingen doorgaf aan de FBI, werkten Andriesse, inmiddels promovendus, en zijn collega's aan een tweede en derde aanval tegen

Gameover ZeuS. In september 2012 kwam de groep bij elkaar voor een paar huiskamercodeersessies in Oberhausen en wist ze 95 procent van de bots over te nemen. Maar ook deze bots konden ze niet vasthouden.

De onderzoekers besloten om de FBI erbij te halen. Die was toen ook al een tijd bezig om de organisatie achter Gameover ZeuS te pakken te krijgen. De FBI had zelf uitgevogeld wie achter de naam Slavik schuilging: de 33-jarige Evgeniy Mikhailovich Bogachev, woonachtig in het Russische Anapa. Ook hadden agenten toegang weten te krijgen tot een server in Groot-Brittannië met daarop een uitgebreide administratie van de bende. En de FBI kon iets wat de onderzoekers niet konden: een zaak opbouwen, de verschillende onderzoeken coördineren en beslag laten leggen op de domeinnamen die Gameover ZeuS gebruikte. Daarnaast kon de FBI mensen arresteren, althans de Oekraïense en Russische autoriteiten verzoeken dat te doen. De puzzelstukken vielen in elkaar.

In de eerste helft van 2014 bereidde de groep academici waar Andriesse deel van uitmaakte een nieuwe aanval voor. Op 30 mei kwam alles bij elkaar. De FBI legde beslag op meer dan duizend domeinnamen van het backupsysteem. De arrestatieverzoeken voor Bogachev en enkele handlangers gingen de deur uit. Een paar ingevlogen academici begonnen vanuit het FBI-kantoor het botnet te vergiftigen. Operatie-Tovar was begonnen. En de ploeg achter Gameover ZeuS kon alleen maar toekijken hoe hun geavanceerde netwerk in elkaar donderde.

Maar waar waren Slavik en zijn directe collega's? Die waren weer verdwenen.

Hoe dat kan? Het is allemaal speculatie, zegt Michael Sandee erover, maar het heeft er de schijn van dat Slavik en zijn bende hand-en-spandiensten verrichtten voor de Russische geheime dienst en in ruil daarvoor bescherming kregen. Fox-IT kreeg toegang tot een botnet dat voor de meeste businessclubleden verborgen was. Dat botnet was niet gericht op fraude, maar op spionage. De doelwitten bevonden zich in Turkije, Georgië en Oekraïne en waren ministeries van Defensie en Binnenlandse Zaken, inlichtingendiensten en informatie die betrekking had op (wapenleveranties aan) Syrië.

Om de druk op Bogachev op te voeren, loofde de FBI in februari vorig jaar een beloning van drie miljoen dollar uit voor informatie die zou leiden tot zijn aanhouding. Mogelijk heeft die beloning ertoe geleid dat Slavik zich rustig houdt. Er zijn nog wel twee varianten van Gameover ZeuS verschenen, waarschijnlijk opgezet door criminelen uit de oude kerngroep, maar ze waren niet succesvol. Blijkbaar misten ze de malwarekunsten van Slavik.

Wat mij aan dit verhaal opvalt, is hoe informeel de groep rond Gameover ZeuS, maar ook de bestrijding ervan, opereerde. Deze online georganiseerde criminaliteit heeft meer weg van een soort minimarktplaats waar ontevreden klanten hardop lopen te klagen. De bestrijding ervan is, in dit geval, geen kwestie van nationale politiediensten die formele samenwerkingen vormen. Nee, in dit geval besloot een aantal academici om een crimineel

netwerk aan te vallen, was een privaat bedrijf daarin geïnfiltreerd en zochten ze zelf contact met een buitenlandse opsporingsdienst om een einde te maken aan een online bedreiging.

Goed, de bende houdt zich stil, de fraude is gestopt. Maar de malware huist nog steeds in honderdduizenden computers, als een geest die ieder moment de bewoner de stuipen op het lijf kan jagen. Opschonen gaat niet, want er draaien misschien wel vitale systemen op de besmette computers die niet mogen crashen. En honderdduizenden eigenaars achterhalen en actie laten ondernemen is onbegonnen werk.

Bovendien gaat de aandacht van onderzoekers en opsporingsdiensten uit naar nieuwe dreigingen, nieuwe criminele groepen en nieuwe botnets. Online spoken zullen ons blijven achtervolgen. En nieuwe, verrassende coalities zullen zich blijven vormen om die spoken te verdrijven.

Verder lezen?