



Bent u een zombie?

Het aantal PC's wat besmet is met een virus, waardoor de besturing van de PC door de verspreider van de virus kan worden overgenomen, is sterk aan het groeien. Deze zogenaamde "zombie-PC's" lijken zorg te dragen voor een grote toename van de hoeveelheid spam en Denial of Service attacks. Er zijn zeer professionele programma's in omloop die (onvoldoende beveiligde) PC's kunnen infecteren, waarna de besturing kan worden overgenomen. Op deze manier ontstaan botnets, netwerken van zombie-PC's die door een aanvaller worden beheerd.

Het beheeren en exploiteren van botnets is georganiseerde criminaliteit. Het is criminaliteit met een hoge opbrengst en een lage pakkans.

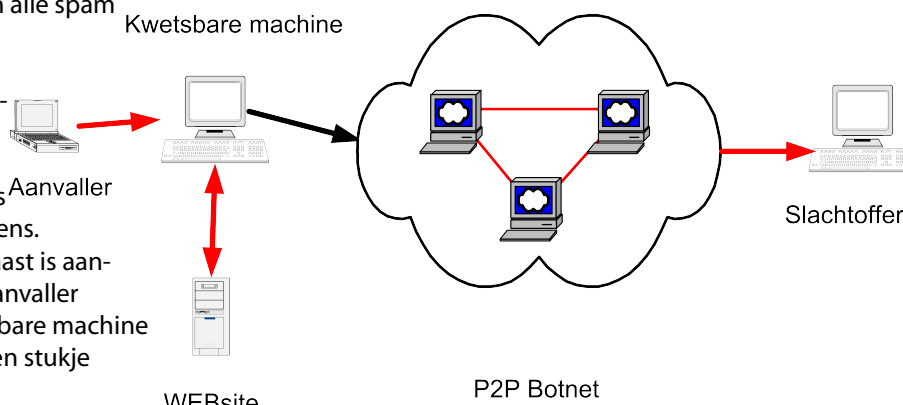
Zo ontdekte een security specialist in het voorjaar van 2006 een stuk programma, wat bij de kustwacht systematisch zocht naar scheepsinformatie en deze informatie vervolgens doormailde naar een bepaald email adres.

De schattingen over botnets lopen nogal uiteen, maar vaak wordt aangenomen dat ongeveer 11% van alle PS's wereldwijd in een botnet zitten.

Botnets worden ondermeer gebruikt door spammers. Het is een ideale manier om grote hoeveelheid email kwijt te raken, omdat op deze manier het "kwaad" van vele kanten komt, waardoor het moeilijker is om deze te bestrijden. In het jaarlijkse "intelligence report" van Messagelabs wordt gesteld dat 80% van alle spam via botnets komt.

Een ander doel van botnets is het vergaren van vertrouwelijke informatie, zoals inloggegevens en creditcardgegevens. In het plaatje hiernaast is aangegeven hoe een aanvaller probeert een kwetsbare machine te infecteren met een stukje programmatuur.

Via bijvoorbeeld spam of zelfs het surfen naar bepaalde sites kan een stukje programmatuur (een "stub") op uw PC worden geplaatst. Deze download vervolgens een compleet trojan horse programma, wat daarna wordt geïnstalleerd. U wordt toegevoegd aan het bestaande netwerk van de aanvaller. Het komt ook voor dat een medewerker binnen een bedrijf met de laptop thuis onderdeel wordt van een botnet, deze laptop vervolgens meeneemt naar het bedrijf en vervolgens de andere PC's binnen het bedrijf besmet. De kwetsbare machine is hierbij aanvaller geworden.



Hoe voorkomt u dat u een "zombie" wordt?

Het feit dat uw PC een zombie is geworden, is ondermeer te herkennen aan: traagheid van de computer, (hoewel moderne bots altijd resource vrij laten voor gebruik door de eigenaar), wijziging van het hostbestand, problemen om een virusscanner te downloaden en te installeren, het open staan van poorten op de (personal) firewall.

Het is verstandig om regelmatig te (laten) controleren of u onderdeel bent van een botnet. Hierbij dient te worden gescand op malware. Hiervoor zijn diverse scanners beschikbaar, zoals spybot en adaware. Ook dient er regelmatig op virussen te worden gescand met een up-to-date virusscanner. Daarnaast dient u de instellingen van de (personal) firewall te (laten) controleren op poorten die open staan, waardoor services vanaf de PC het internet op kunnen.

Op <http://www.auditmypc.com/security-scan.asp> is een gratis online scanner die op open poorten kan scannen.

Secure Connection brengt nieuwe website in de lucht

Secure Connection heeft haar producten en diensten overzichtelijk op een nieuwe website geplaatst: <http://www.assutools.com>. Via onze oude website <http://www.seccon.nl> wordt u doorgeleid naar de nieuwe website. Op deze website kunt u verder alle voorgaande nieuwsbrieven en onze brochures over de producten downloaden.

Actueel

Phishers lichten zweedse bank op voor 1 miljoen euro.

De Zweedse bank Nordea is voor 1 miljoen euro opgelicht door phishers. Via 250 klanten van deze bank wisten zij dit geld binnen te halen.

De klanten van deze bank kregen een mailtje met daarin de mogelijkheid om anti-spam software te downloaden.

In werkelijkheid werd een trojan, genaamd haxdoor.ki gedownload.

Deze trojan houdt alle key aanslagen in de gaten. Zodra naar de Nordea bank wordt gegaan (intypen URL) worden de login gegevens opgeslagen.

Bij het intypen van de transactiecode, wordt een foutmelding gegenereerd met het verzoek de code nogmaals in te toetsen. Met de logingegevens en twee codes, is het mogelijk om geld van het slachtoffer over te boeken.

Alle klanten zijn schadeloos gesteld door de bank. Een medewerker van de bank gaf aan dat de klanten die slachtoffer geworden waren veelal geen virusscanner op hun PC hadden. In 2005 is deze bank overigens ook al slachtoffer geweest van een phishing aanval.

Bron:

<http://news.bbc.co.uk/1/hi/business/6279561.stm>