Servers botnet offline

Laatst gewijzigd op: 02-10-2019 | 11:10

Middelburg, Veendam, Amsterdam, Driebergen - De politie heeft vijf servers offline gehaald die gebruikt werden voor de aansturing van een versie van een zogenoemd botnet. De hardware is in beslag genomen en de bedrijfsvoering stilgelegd. Een 24-jarige man uit Veendam en een 28-jarige man uit Middelburg zijn dinsdagavond aangehouden. Zij worden onder andere verdacht van computervredebreuk en het verspreiden van malware.

Rechercheurs van de Dienst Landelijke Recherche kwamen de servers op het spoor via informatie afkomstig van het Nationaal Cyber Security Centrum. Na onderzoek kwam de politie uit bij een Nederlands hostingbedrijf dat gebruikmaakte van servers in een datacentrum in Amsterdam. De servers zijn offline gehaald en worden onderzocht door de politie.

Mirai-botnet

De aansturingsservers van een versie van het Mirai-botnet werden bij een zogenoemde bulletproof hoster gehost. Dat is een hostingprovider die online criminele diensten levert. De servers die offline zijn gehaald stuurden een botnet aan dat voor een groot deel bestond uit Internet-of-Things (IoT) apparaten. Denk bijvoorbeeld aan slimme thermostaten, koelkasten, eigenlijk alles wat gekoppeld kan worden aan het internet. Een botnet maakt van al deze apparaten een netwerk. Met behulp van het Mirai-botnet werden steeds meer IoT-apparaten geïnfecteerd. De apparaten werden vervolgens ingezet om Distributed Denial of Service (DDoS) aanvallen uit te voeren op onder andere websites of betaaldiensten.

Hosting

De servers die in Nederland geplaatst waren, zorgden voor de aansturing van dit botnet, de ‘Command-and-Control’ servers. Met behulp van deze servers werden besmette IoT-apparaten (bots) aangestuurd. Deze bots scannen voortdurend IP-adressen op zoek naar andere kwetsbare IoT-apparatuur. Indien er werd vastgesteld dat er zich achter een IP-adres kwetsbare apparatuur bevond, werd er een aanval uitgevoerd en malware geïnstalleerd. De C&C-servers stuurden het botnet van geïnfecteerde apparaten vervolgens aan, zodat ze gebruikt konden worden voor een DDoS-aanval.

Servers uit de lucht

Met het offline halen van deze servers bij de bulletproof hoster is een slag toegebracht aan een infrastructuur die wereldwijd aanvallen uitvoerde. Hiermee is de aansturing van het bestaande Mirai-botnet onmogelijk gemaakt en infecties van nieuwe apparaten door dit botnet voorkomen. Over de betreffende bulletproof hoster werden ruim drieduizend meldingen gedaan van malwareverspreiding in een periode van een jaar. Ook kwam in het onderzoek naar voren dat dit botnet zeer agressief andere apparaten probeerde te infecteren, tot ruim een miljoen pogingen per maand op een apparaat. Welke DDoS-aanvallen kunnen worden toegeschreven aan dit botnet maakt deel uit van het verdere onderzoek.

Hoe kun je misbruik van IoT-devices voorkomen?

De meeste IoT-devices zijn ‘slim’ gemaakt door ze te koppelen aan het internet. Omdat ze in veel gevallen met standaardwachtwoorden beveiligd zijn en er ook geen algemene standaarden voor de beveiliging worden gehanteerd of zijn afgesproken door producenten, blijven deze systemen kwetsbaar. Door het resetten of opnieuw opstarten van het apparaat wordt de malware gewist. Het resetten van apparaten maakt ze echter niet minder kwetsbaar voor een aanval, want bij een volgende scan kunnen ze opnieuw worden geïnfecteerd. Gebruikers van IoT-apparaten kunnen misbruik van hun apparatuur voorkomen door de apparatuur te resetten en standaardwachtwoorden aan te passen, mits dit mogelijk is.

Wat is een DDoS-aanval?

Een DDoS-aanval houdt bijvoorbeeld in dat via een slimme thermostaat, koelkast of IP-camera een aanval op een website kan worden gelanceerd. Door een aanval met zoveel mogelijk geïnfecteerde apparaten tegelijkertijd uit te voeren worden er zoveel informatieverzoeken gedaan dat een website dit niet aankan en uit de lucht gaat.