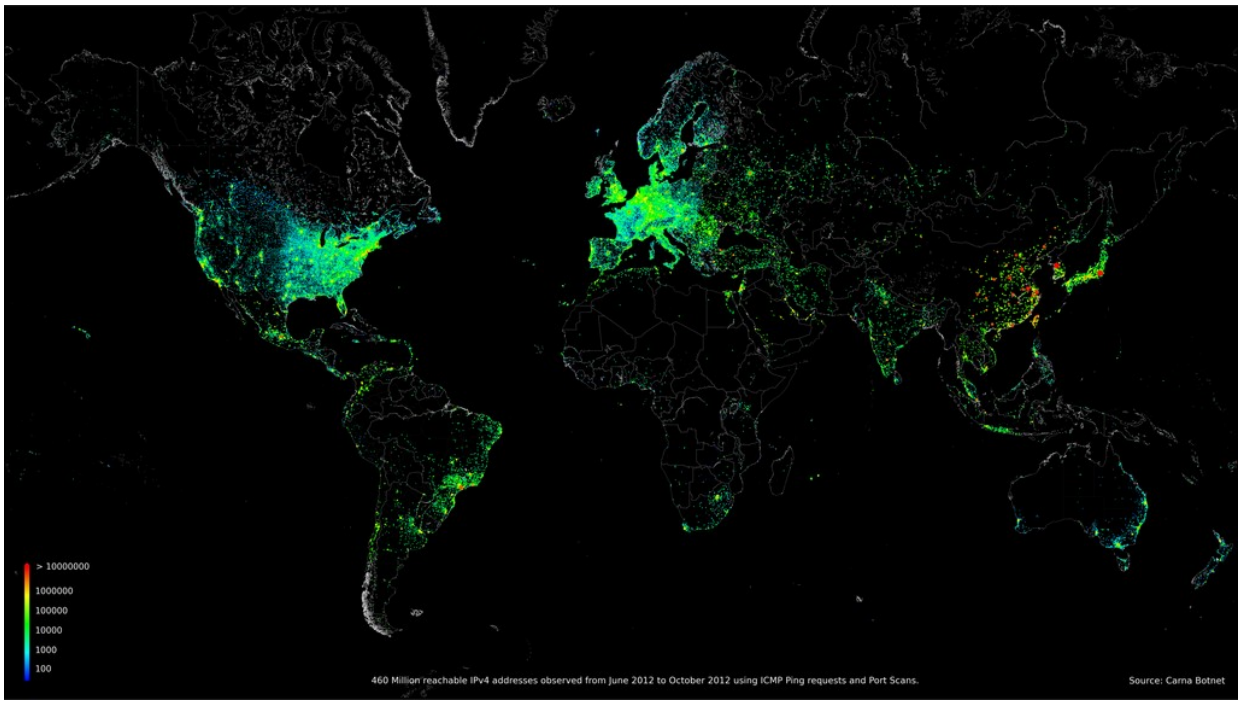
25-9-2015 5:45 Leestijd 3 minuten

Via internet kun je apparaten binnendringen en hun kwetsbaarheden misbruiken. Een onderzoeker had zo maar even het hele internet op kwetsbaarheden gecontroleerd. Wat dat opleverde lees je in dit stuk.

# In één nacht het internet scannen. Deze onderzoeker bewijst dat het kan

Correspondent Hacken

Dimitri Tokmetzis




Wereldkaart van gescande computers door het Internet Census 2012 Project.

# Het begon als grap.

Een onderzoeker *Die onderzoeker bleef anoniem.* wilde kijken hoeveel apparaten Telnet gebruikten. Dat is een programma waarmee je op afstand een computer kunt besturen. Probleem: het is erg onveilig. *Het verkeer wordt bijvoorbeeld niet versleuteld. Tegenwoordig wordt vooral SSH (secure shell) gebruikt om toegang tot andere computers te krijgen.* Daarnaast worden bij installatie een gebruikersnaam (root) en

wachtwoord (root) aangemaakt, die vaak niet veranderd worden.

Met Nmap, een opensourceprogramma waarmee je netwerken in kaart kunt brengen, vond de onderzoeker al snel duizenden computers waar je met behulp van root:root kon inloggen.

Lachen?

# In één nacht het internet overnemen

Nmap is snel. Afhankelijk van je internetverbinding, kun je algauw tien IP-adressen per seconde scannen. Maar als je enkele miljarden adressen *Je hebt twee verschillende IP-adressen. Een IP-adres is een uniek adres van ieder aan internet aangesloten apparaat. IPv4 is het meest gebruikte soort adres. Dit bestaat uit vier*

*blokken, zoals 192.168.178.129 (in dit geval een intern netwerk). Hier zijn bijna 4,3 miljard van beschikbaar. Deze IP-adressen zijn bijna op. Daarom wordt al jaren gewerkt aan de veel langere IPv6. Die zijn zo'n beetje oneindig. Met IPv4 bereik je vrijwel het hele internet, maar dus niet helemaal.* wilt scannen is dat nog veel te traag.

De onderzoeker bedacht daarom een list en liet een botnet het vuile werk opknappen.

> De internetscan kon in één nacht worden afgerond

Een botnet is een groep controleerbare geïnfecteerde computers. Dat werkt zo. Je dringt andermans computer binnen en installeert daarin software. De geïnfecteerde computers praten met elkaar, of, zoals vaak, met een *command and control center*.

Als de onderzoeker een computer aantrof met Telnet en daar met root:root kon inloggen, installeerde hij er een Nmap-scanner. Die ging dan weer op zoek naar andere kwetsbare computers waar ook weer een Nmap-scanner geïnstalleerd kon worden.

Binnen een dag waren dertigduizend computers overgenomen die Telnet draaiden en kon dit leger ingezet worden voor het scannen van het complete internet. De internetscan kon in één nacht worden afgerond.

Om schade te voorkomen, nam de onderzoeker een aantal veiligheidsmaatregelen. De scanner werkte alleen als er geen andere belangrijke processen op de computer bezig waren (die kregen altijd voorrang).

Als de computer opnieuw startte, werd de scanner verwijderd. En als dat niet gebeurde, werd de scanner na een paar dagen automatisch onklaar gemaakt.

Wat de onderzoeker te weten kwam? Na miljarden scans kon hij vaststellen dat 1,3 miljard IP-adressen daadwerkelijk worden gebruikt door een computer en dat dat van 2,3 miljard adressen niet is vast te stellen. Ook bleek dat honderdduizenden van die apparaten kwetsbaar zijn voor een simpele telnet-hack.

# Wat moeten we met deze informatie?

Het lijkt een wat omslachtige manier om kwetsbaarheden op internet te vinden.

De onderzoeker is naar eigen zeggen zes maanden bezig geweest om dit plan uit te vogelen en op te zetten.

Maar hij staat niet alleen. In 2013 stond er een aardig artikel in *Technology Review* over de Amerikaanse veiligheidsonderzoeker HD Moore. Vanuit zijn woonhuis scande hij zes maanden lang het hele internet . Hij toonde aan dat honderdduizenden computers kwetsbaar waren voor aanvallen op hun plug-and-playsoftware.
*Plug-and-playsoftware zorgt ervoor dat wanneer je hardware aan je computer koppelt, een muis bijvoorbeeld, die meteen werkt.*

Een onderzoeksgroep van de Universiteit van Michigan heeft een opensourceprogramma gebouwd waarmee het internet gescand kan worden: zmap. In theorie kun je daarmee

in 45 minuten het hele internet (IPv4) scannen en:

- Onderzoeken hoe bepaalde kwetsbaarheden zich over internet verspreiden of juist worden verholpen. De academici konden bijvoorbeeld bedrijven en instanties helpen die kwetsbaar waren voor de zogenoemde Heartbleed-bug.
- Zien waar het internet goed werkt en waar niet. Nadat orkaan Sandy in 2012 over het noordoosten van de Verenigde Staten raasde, konden de onderzoekers in kaart brengen waar het internet was uitgevallen.
- Mondiale diensten in kaart brengen. De onderzoekers hebben bijvoorbeeld onderzoek gedaan naar de uitgifte van certificaten die voor de beveiliging van webverkeer worden gebruikt. Op die

manier konden ze ook malafide certificaten opsporen.

Het valt dus te verwachten dat dit soort grootschalig onderzoek veel vaker zal plaatsvinden. Reken er in ieder geval maar op dat je internetapparaten nog vaak gescand zullen worden.

Oproep

Wat vinden jullie van het idee dat iemand zomaar je computer binnendringt? Is dat gerechtvaardigd?