CENTER FOR CYBERSIKKERHED

11. november 2013
Dokumentnr.: 2

SNMP Reflected Amplification DDOS Attacks

Simple Network Management Protocol

Til: Den it-sikkerhedsansvarlige

Resumé

Center for Cybersikkerhed har i den seneste tid set flere DDOS-angreb, typisk af typen DNS amplification, mod danske hjemmesider tilhørende myndigheder og private virksomheder.

Center for Cybersikkerhed ser angreb af typen "SNMP Reflected Amplification DDOS attacks". Dette angreb kan typisk være op til 15 gange kraftigere pr. IP adresse end et typisk DNS amplification angreb. Det skyldes et langt større omfang af data i retur svaret mod den angrebne IP-adresse.

Center for Cybersikkerhed har analyseret danske IP-adresser, som har været misbrugt i forhold til SNMP Reflected Amplification DDOS attacks. Det viser sig, at alle IP-adresser har haft SNMP stående åben, således at denne type angreb kunne gennemføres.

Center for Cybersikkerhed har set angreb, hvor mere end 118.000 IP-adresser er blevet benyttet til SNMP Reflected Amplification DDOS angreb mod danske myndigheder. Angrebene involverer forholdsvist få danske IP-adresser. Angrebene kan stamme fra både Windows, Linux, Routers, firewalls, printers og andet, der understøtter SNMP, og som ikke er beskyttet tilstrækkeligt.

Virksomheder og myndigheder er ikke altid opmærksomme på, om egne systemer er åbne over for denne type angreb, og derfor har Center for Cybersikkerhed beskrevet en række tests, som de respektive it-afdelinger selv kan gennemføre. Formålet er at identificere åbne SNMP-servises i it-infrastrukturen, der ufrivilligt kan bidrage med angrebskapacitet til denne type angreb.

Anbefaling

Center for Cybersikkerhed anbefaler at kontrollere sine egne netværk for åbne SNMP-services. Har virksomheden eller myndigheden et forretningsmæssigt behov for åbne SNMP, anbefaler Center for Cybersikkerhed, at man imødegår denne sårbarhed ved at følge de anbefalinger, som allerede findes på internettet, i forhold til det udstyr, man benytter. Se eventuelt links i bunden af dette dokument.

Sådan finder du åbne SNMP i eget net

Automatiseret metode:
Den nemmeste metode er at bruge en sårbarhedsscanner som eksempelvis Nessus eller tilsvarende. Center for Cybersikkerhed kan anbefale denne metode, fordi den ofte finder yderligere sårbarheder på åbne systemer, som ikke er beskyttet tilstrækkeligt. Vær opmærksom på eventuelle licensbetingelser.

Manuel metode:
NMAP port scanning kan lokalisere åbne SNMP-servises, som vil tillade retursvar til enhver IP-adresse, der forespørger SNMP-information.

NMAP-metoden er beskrevet på Windows, som er det mest anvendte operativsystem. Center for Cybersikkerhed anbefaler dog at bruge Linux ved scanninger af store netværk. Det er vigtigt at scanne både udstyr fra internettet og indefra imod lokalt placeret udstyr. En gennemførsel af en NMAP-scanning på et /24 net tager cirka to minutter.

Begrænsning i disse tests:
Testene kontrollerer ikke for eventuel rate-limit implementereing, eller om andre mitigeringsteknikker er implementeret. Desuden er NMAP-scanningen begrænset til IPv4.

NMAP scanning:
Fra en command prompt (Windows 7)
nmap -oA c:\SNMP-Scanning -sU -p 161 –T4 –A -n –iL "C:\\Users\\administrator\\Desktop\\LIST-IP.txt"

Simpel nmap scanning imod 1 IP-adresse eller enkelte net.
nmap -sU -p 161 -T4 -A -n -Pn 10.0.0.x

Forklaring:
-oA c:\DNS-Scanning = Gemmer resultatet i 3 log formater i C:\ roden.
-sU = UDP scanning
-A = OS genkendelse
-n = Ingen DNS opslag
-p 161 = Scanning kun efter port 161
-T4 = Aggressive scanning (hastigheden på scanningen)
-iL = Sti til hvor TXT ligger placeret med IP-adresser der skal scannes. (kan undlades)

Kontakt
Har du spørgsmål, er du velkommen til at kontakte Center for Cybersikkerhed på mail contact@govcert.dk.

Key ID 6740E2CD
Fingerprint: 2CE4 BA61 B873 B089 0BE9 4ED2 3CDA 6879 6740 E2CD.

Yderligere information:

Sårbarheden forklaret
BITAG
http://www.bitag.org/report-snmp-ddos-attacks.php

Hvad er SNMP
SNMP - Simple Network Management Protocol
http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Anbefalede værktøjer
nmap
http://nmap.org

Nessus
http://www.tenable.com

Center for Cybersikkerhed
Sådan kan DDOS angreb imødegås
http://fe-ddis.dk/cfcs/CFCSDocuments/S%C3%A5dan%20undg%C3%A5r%20du%20Ddos%20angreb.pdf

Situationsbillede af sikkerhedstilstanden på internettet
http://fe-ddis.dk/cfcs/CFCSDocuments/Situationsbillede%20-%20April%202013.pdf