CENTER FOR CYBERSIKKERHED

29. november 2013

Undgå DNS Amplification attacks

Til: Den it-sikkerhedsansvarlige

Resumé
Center for Cybersikkerhed har i den seneste tid set flere DDoS-angreb mod danske myndigheder og private virksomheder. Det er typisk DDoS-angreb af typen HTTP SYN, ICMP og DNS amplification.

Center for Cybersikkerhed har i sit situationsbillede for første kvartal 2013 beskrevet, hvordan Danmark bliver brugt som angrebsplatform til blandt andet DDoS-angreb. Mange myndigheder og virksomheder har opsat deres DNS-servere som såkaldte 'åbne resolvers' – det vil sige, at serverne tillader DNS fra hvem som helst.

Ved at have åbne resolvers i egen it-infrastruktur risikerer virksomheder og myndigheder at stille ufrivillig angrebskapacitet til rådighed og dermed medvirke til eksempelvis DNS-amplification attacks mod andre.

Virksomheder og myndigheder er ikke altid opmærksomme på, at egne DNS-tjenester er åbne over for denne form for angreb. Derfor har Center for Cybersikkerhed beskrevet en række tests, som it-afdelinger kan gennemføre for at identificere åbne resolvers i egen it-infrastruktur.

Anbefaling
Center for Cybersikkerhed anbefaler at kontrollere egne netværk for åbne DNS-resolvers. Har virksomheden eller myndigheden et forretningsmæssigt behov for åbne DNS-resolvers, anbefaler vi at imødegå denne sårbarhed ved at følge de anbefalinger, som allerede findes tilgængelige på internettet. Se links i bunden af dette dokument.

Sådan finder du åbne resolvers i dine net

Automatiseret metode:
En nem metode til at søge efter åbne resolvers er at bruge en sårbarhedsscanner som eksempelvis Nessus. En sårbarhedsscanner kan desuden scanne efter yderligere sårbarheder, som ofte gør sig gældende på åbne DNS resolvers. Vær opmærksom på eventuelle licensbetingelser.

Manuel metode:
NMAP-portscanning kan lokalisere DNS-servere, der er opsat til at tillade DNS-recursion. DNS amplification attacks udnytter netop disse DNS-servere med åben DNS-resolver. Angriberen vil typisk benytte "DNS ANY"-opslag mod en given DNS-server med spoofet source IP-adresse, hvis denne tillader mange forespørgsler.

NMAP-metoden er beskrevet på Windows, som benyttes af de fleste brugere. Vi anbefaler dog at benytte Linux ved scanninger af store netværk. Det er vigtigt, at man scanner udefra, hvor DNS-serveren forventeligt kan blive misbrugt.

Begrænsning i disse tests:
- Testene kontrollerer ikke for eventuel rate-limit implementering eller andre mitigeringsteknikker
- NMAP scanning er begrænset til IPv4 og kun på IP'er, hvor ICMP svarer
- NMAP scanning undersøger ikke DNS via TCP.

NMAP-scanning:
Fra en command prompt (Windows 7): nmap -oA c:\DNS-Scanning -sU -sV -p 53 -T5 –iL "C:\\Users\\administrator\\Desktop\\LIST-IP.txt" --script dns-recursion

Simpel NMAP-scanning mod en IP-adresse eller enkelte net: nmap -sU -sV -p 53 -T4 --script dns-recursion 10.0.0.*

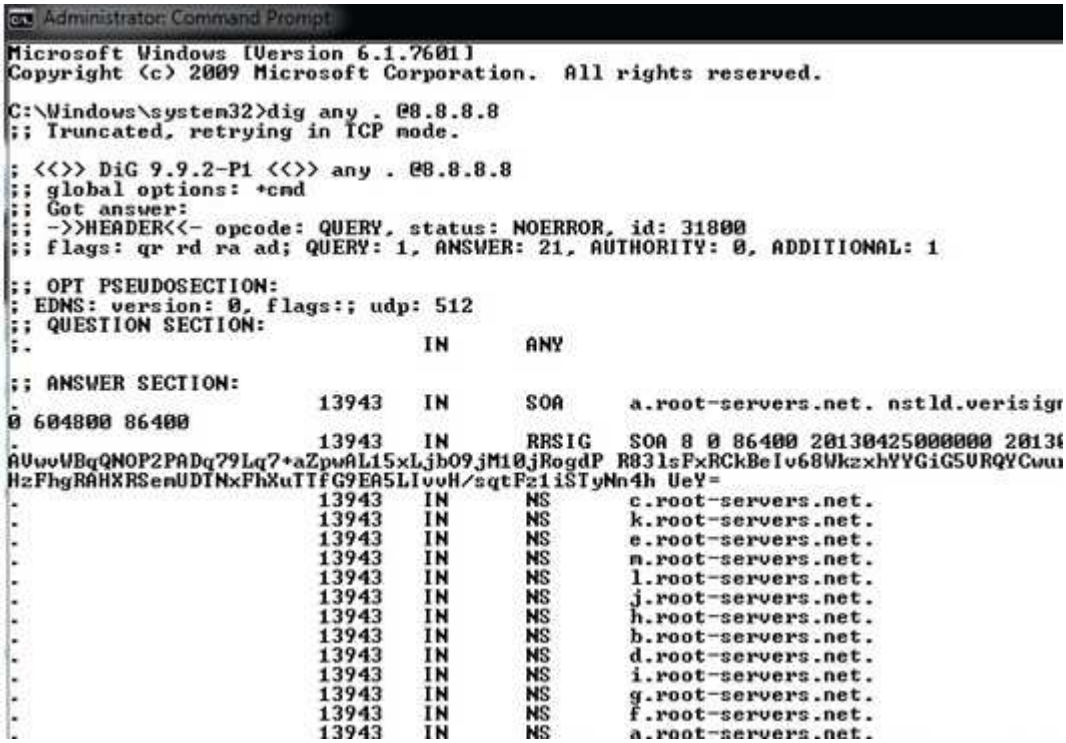
Forklaring:
- oA c:\DNS-Scanning = Gemmer resultatet i tre log-formater i C:\ roden
- sU = UDP scanning
- sV = Service Detection (der kan være problemer med denne på Windows 7 64-bit)
- p 53 = Scanning kun efter port 53
- T4 = Aggressive scanning (hastigheden på scanningen)
- iL = Sti til placeringen af TXT med IP-adresser, der skal scannes (kan undlades)
- script dns-recursion = nmap script, der undersøger, om åben DNS recursion (også kaldet en åben DNS resolver) er tilladt.

Bemærkning:
Scanning af et /19 netværk tager cirka 2½ time på en Windows maskine, og kontrol DNS-opslag bliver foretaget mod www.wikipedia.org. Dette kan ændres i DNS-recursion scriptet i NMAP (anbefalet).

Denne søgestreng kan efterfølgende bruges til søgning i NMAP logfilen: >*Recursion appears to be enabled*<
- Dette betyder, at DNS recursion højst sandsynligt er tilladt.

De åbne resolvers, som NMAP-scanningen har fundet, skal kontrolleres ved at foretage et DNS ANY lookup. Det skal sikre, at der er tale om DNS-recursion, og afgøre, om DNS-serveren kan være "misbrugs egnet" til DNS amplification attacks.

Følgende DIG command kan benyttes: Udskift IP-adressen 8.8.8.8 med den IP-adresse, du ønsker at kontrollere. Eksemplet nedenfor viser et eksempel foretaget mod punktum via 8.8.8.8 (Google DNS).
dig any . @<Den IP-adresse, du vil kontrollere>



Tips til wireshark:
Du kan bruge følgende wireshark eller tilsvarende til opsamling af trafik i forbindelse med scanninger (anbefalet):

Wireshark Capture filter (foretag trafikopsamling fra den pc, der scannes fra) host >host ip< and udp port 53.

Dumpcap capture filter er en alternativ metode til wireshark, som kan anbefales til især store scanninger.

dumpcap" -b duration: 86400 -b files:90 -i 1 -P -f "ether host >MAC addresser på den pc, der scannes fra<" -w C:\Dump-Cap\dns.pcap

DNS Response (bruges til at finde de IP-adresser, der er åbne resolvers i den opsamlede trafik)
dns.resp.name == www.wikipedia.org

Wireshark Display filter – DNS ANY
dns.qry.type == 0x00ff

Yderligere information:

Om sårbarheden

US-CERT
http://www.us-cert.gov/ncas/alerts/TA13-088A

DNS Amplification Attack (Youtube klip)
http://www.youtube.com/watch?feature=player_embedded&v=xTKjHWkDwP0#!

dns.measurement
http://dns.measurement-factory.com/surveys/openresolvers/ASN-reports/

Værktøjer, som kan benyttes

nmap
http://nmap.org

Nessus
http://www.tenable.com

DIG til windows
http://members.shaw.ca/nicholas.fong/dig/

SANS DNS test tool
https://isc.sans.edu/dnstest.html

Wireshark – Inkluderer dumpcap
http://www.wireshark.org/download.html

Teknikker, der kan mitigere denne sårbarhed

IETF
Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
http://tools.ietf.org/html/bcp38

Cloudshiled - Ratelimit
http://www.cloudshield.com/applications/dns-limit-attacks.asp

Rate limit via IP tables - Working guide
http://www.junkemailfilter.com/blog/2013/03/03/how-to-block-dns-amplification-attack-isc-org-any-attack/

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