Kære Internetudbyder

Vi henvender os på vegne af et internationalt netværk af offentlige myndigheder og anmoder din organisation om at deltage i en verdensomspændende aktion for at forhindre spammere i at sætte private forbrugers netsikkerhed på spil ved at bruge deres computere som "spam zombier". Vores respektive organisationer er nationale håndhævelsesmyndigheder hvad angår spam-bekæmpelse, og står i den forbindelse for teknisk research, vejledning af forbrugere og erhvervsliv, udarbejdelse af lovgivning samt public private partnerships.

Spammere bruger hjemmecomputere til at udsende millioner af spam-mails. Ved at udnytte sikkerhedsfejl får de skjult software til at installere sig selv - software som omdanner private computere til mail- eller proxyservere. Spam-mails bliver herefter ledt igennem disse "spam zombier" for at sløre den oprindelige afsender af spam-mailen.

Som internetudbyder har din organisation en interesse i at mail-systemer generelt fungerer optimalt, sikkert og pålideligt. Når spammere bruger privates computere som spam zombier kan tiltroen til mail-systemerne blive alvorligt kompromitteret. Ydermere vil modtagerne måske tro, at din virksomhed eller en af dine kunder er afsenderen, da spam-mailen ser ud til at stamme herfra. Spam kan også overbelaste dine netværksforbindelser, øge administrative udgifter mm.

Vi vil opfordre dig til at implementere følgende frivillige anti-zombie foranstaltninger, hvis du ikke allerede har gjort det[1]:

- Blokér port 25 undtagen for de autentificerede kunder som har brug for udgående SMTP. Undersøg hvorvidt den autentificerede SMTP på port 587 for brugere der har deres egne udgående mailservere kan implementeres.
- Anvend kontrolforanstaltninger på email relays (kan være defineret ved antal mails pr. tidsenhed).
- Identificér computere som udsender atypiske mængder af emails, og tag foranstaltninger der kan hjælpe til at fastslå hvorvidt en computer bliver brugt som spam zombie. Om nødvendigt må den berørte computer tages af netværket indtil problemet er løst.
- Forklar på en let forståelig måde hvordan kunden undgår at maskinen bliver angrebet af orme, trojanske heste og andet malware, der omdanner hjemmecomputeren til en spam zombie, og sørg for at kunden har adgang til de nødvendige værktøjer og assistance.
- Hvis uheldet er ude bør du sørge for, at dine kunder har adgang til let anvendelige værktøjer til at fjerne zombie kode med samt give dem den nødvendige assistance.

Udover at bede internetudbydere om at hjælpe med at forhindre spammere i at skabe spam zombier, er vi også i færd med at udvikle en plan til at identificere ikke alene potentielle spam zombier rundt om i verdenen, men også internetudbydere og andre udbydere af netværksforbindelser, der ser ud til at være indehavere af de berørte IP-numre. Undersøgelsen vil være baseret på offentlig tilgængeligt materiale fra spam- og WHOIS databaser. Vi vil så kontakte de internetudbydere, som ser ud til at administrere IP-numre hvorfra en mulig spam

[1] Hvis du vælger at implementere de foranstaltninger, vi anbefaler, skal du dog først sørge for at tjekke, at de ikke er i strid med gældende lovgivning i dit land i forbindelse med databeskyttelse samt opbevaring af persondata og andre oplysninger – eller andre lovmæssige krav eller forpligtelser. Bemærk venligst at vore anbefalinger kan være påkrævet allerede i forhold til dit lands lovgivning.

Amagerfælledvej 56
2300 København S
CVR nr. 10 29 48 19

Tlf. 32 66 90 00
Fax 32 66 91 00
www.forbrug.dk

Medlem af International
Consumer Protection &
Enforcement Network (ICPEN)
www.icpen.org

zombie opererer. Et nyt brev fra os vil bede de berørte internetudbydere om at styrke indsatsen mod spam zombier i disse systemer.

Hvis du vil vide mere om projektet og se hvem der deltager, kan du se følgende link.
http://www.ftc.gov/bcp/conline/edcams/spam/zombie/index.htm

Tak for din hjælp til at bekæmpe spam.