DDoS na mailserver - klasika v novém kabátě

Vložil/a Sniper [1], 11 Prosinec, 2004 - 23:03

- Apple [2]
- Hacking [3]
- Hacking method [4]

SMTP protokol vznikl v roce 1982 za účelem posílání zpráv po tehdejším internetu. K tomuto účelu slouží dodnes a dodejme, že stále dobře. Pojďme se ale podívat na jednu jeho potenciálně zneužitelnou slabinu.

Konečne jsem se dostal k seznamu příkazů protokolu SMTP. Koukám na to a nikde žádná autorizace. Že by chyba? Možná. A jako taková by se dala zneužít.

Nebudu tady psát zdrojáky kódu, který by to provedl. Kdo o ně bude mít zájem, ten si je najde sám nebo si je napíše. Budu psát o chybě v protokolu, který se již 22 let téměř nezměnil.

SMTP protokol vznikl v roce 1982 pro zasílání zpráv na tehdejším „internetu“. Tomuto účelu slouží i dnes a ještě nějakou dobu bude. Existují sice nové verze (SMTP auth., SMTP over SSL), ale s těmi jsem se ještě nesetkal. Jeho největší slabinou je jeho naprostá volnost – nevyžaduje žádnou autorizaci.

Nejdříve se podíváme, jakým způsobem vůbec SMTP pracuje. Klient se připojí k serveru na port 25 (standartní SMTP port) a zašle příkaz HELO domena. Server pošle stavový kód a svojí doménu. Tímto je odbyto představování. Ještě se zastavím u stavových kódů SMTP. Protokol SMTP zná pouze dva. Stavový kód 250, který znamená OK a stavový kód 500, který znamená chybu. Nic jiného nezná. Ale zpět. Po představení se serveru klient zašle příkaz MAIL FROM: odesilatel@domena. Server zašle v potvrzení zpět adresu odesílatele a čeká na další příkaz. Poté následuje příkaz RCPT TO: prijemce@domena, který slouží k zaslání adresy příjemce emailu. Server zopakuje adresu příjemce a dále čeká. Klient v tento okamžik zašle příkaz DATA. Tím dá serveru na vědomí, že další text je již samotný email. Nejdříve se zašle hlavička emailu, poté jeden volný řádek, text zprávy a nakonec sekvence CRLF.CRLF – prázdný řádek, tečka a další prázdný řádek. Po odeslání této sekvence server vyhodí kód 250, že přijal zprávu a další 250, že zprávu zpracoval. Teď již jen stačí odeslat příkaz QUIT a ukončit spojení.

Tímto postupem se jednoduše dá poslat mail přes telnet. Jak to ale zneučít k DDoS útoku? Jednoduše. Chyba tkví v příkazu **MAIL FROM:**. Doména, ze které se přihlašujeme k serveru se totiž nemusí rovnat, a v praxi většinou ani nerovná, doméně odesílatele. Proto stačí jednuduchá věcička. Stačí nalézt pár tzv. Open-relay SMTP serverů, tj. takových, u kterých je možno posílat mail z jakékoliv domény do jakékoliv domény. Když několik těchto serverů máme, stačí napsat script, který se přikonektuje na jednotlivé servery a zašle z nich email na adresu nejaky-nesmyslny-shluk-znaku@domena1.cz. Jako odesilatele uveďte nejaky-jiny-nesmyslny-shlukznaku@domena2.com. A teď co se stane. Open-relay server A přijme maily pro přeposlání do domény doména1.cz. Mailserver B přijme emaily a začne hledat uživatele nejaky-nesmyslny-shluk-znaku. Uživatele nenajde a tak zašle mailserveru domény2 oznámení o nedoručení zprávy. Mailserver C ve své databázi uživatele nejaky-jiny-nesmyslny-shluk-znaku nenajde a tak pošle oznámení serveru B. Server B tento nápor nevydrží a spadne. Pokud zaslaných e-mailů bude větší množství, řekněme řádově několik desítek tisíc, může tento nápor shodit i server C.

Tento typ útoku je zákeřný v tom, že proti němu prakticky neexistuje obrana. Neexistuje způsob, jak zjistit, jestli je příchozí email platný, nebo jestli je to jen část útoku. Zvláště, pokud je útočících serverů několik desítek a mailů několik desítek tisíc.

A co říci závěrem? No, snad jen to, že autor tohoto článku je lama, 100% lama a nic než lama. A ještě něco – **autor ŽÁDNÝM ZPŮSOBEM NENÍ ZODPOVĚDNÝ** za škody vzniklé použitím nebo zneužitím tohoto návodu nebo její části!

URL článku:
https://security-portal.cz/clanky/ddos-na-mailserver-klasika-v-nov%C3%A9m-kab%C3%A1t%C4%9B

Odkazy:
[1] https://security-portal.cz/users/sniper
[2] https://security-portal.cz/category/tagy/apple
[3] https://security-portal.cz/category/tagy/hacking
[4] https://security-portal.cz/category/tagy/hacking-method