DHA támadás elleni védekezés lehetősége a támadók felismerése és központosított tiltása segítségével

Bevezető:

Az emberek az egyre növekvő kéretlen levelek áradatának és levélben terjedő vírusok és más kártékony kódok hatására egyre jobban meggondolják azt, hogy kinek is adják oda az e-mail címüket. Átgondolják, hogy meg merjék-e kockáztatni, hogy valamilyen online fórumon címüket használják, vagy akár azt is, hogy egyáltalán a weblapjukon vagy névjegyükön rajta hagyják-e ezt a fontos személyi adatukat. A fenti okok miatt a felhasználók általában tartanak más, akár egyszer használatos e-mail címet, gyakran valamilyen ingyenes szolgáltatónál, ami ha "odavész", sem baj. Ha a címet elkezdik elárasztani kéretlen levelek, akkor a felhasználó rövid idő után átvált egy másik címre, a régit lemondja, vagy magára hagyja és később a szolgáltató is törli.

A DHA problémája az SMTP protokollban gyökeredzik: az e-mail szerverek, ha megfelelő e-mail címre kapták a levelet, úgy nem adnak visszajelzést, elfogadják a levelet.
A szerver, ha nem létező felhasználó címére kap levelet, úgy vagy azonnali, vagy későbbi visszajelzést ad arra nézve, hogy a felhasználó postafiókja nem létezik. . Ez a folyamat információval szolgál a levelező-szerver által karbantartott e-mail címekről. A támadók ezt az információt használják ki, rengeteg levelet küldve az adott e-mail szervernek. Azokról a címekről, amelyekről nem érkezik válasz (a szerver negatív visszajelzés nélkül elfogadja a levelet), nyilvántartást vesznek fel. Ezek a címek minden valószínűség szerint érvényes felhasználói azonosítókhoz tartoznak, így érdemes lehet rájuk a későbbiekben kéretlen leveleket küldeni.

A cím kijutás mellett problémát jelenthet a levelezést kiszolgáló szerver DoS jellegű támadása. Az e-mail címek megszerzése érdekében a támadó rengeteg téves levelet küld a szervernek, amely így jelentősen, hosszú időre, és akár több támadótól is leterhelésre kerül. A leterhelés leköti a kiszolgáló hálózati kapacitását és processzorát is.

A DHA támadásnak, azaz a címlista kinyerő támadásnak, két típusa létezik: egyik "brute force" jelleggel az összes lehetséges karakterkombinációt kipróbálja, mint e-mail címet, a másik jóval szofisztikáltabb: tipikusan előforduló e-mail címeket generál emberek vezeték és keresztnevéből, illetve gyakran előforduló szavakból, szóösszetételekből, továbbá ismert e-mail azonosítókból.

A védekezés a DHA támadás ellen ellen történhet egyszerűen bonyolultra választott e-mail címekkel, ami a szótáras támadás ellen ideig-óráig véd, de a környezetünk nehezen fogja tudni megjegyezni új e-mail címünket.A védekezés brute-force támadások ellen haszontalan.
Másik megoldás, ha a szervert egyszerűen úgy konfiguráljuk, hogy fogadjon el minden e-mailt és ne jelezzen vissza róla senkinek, a téves leveleket egyszerűen eldobjuk. A megoldás több okból is problémás: A levélküldők nem tudják meg, hogy a cím nem létezik, és elárasztathatják a szervert téves levelekkel. Fontos az is, hogy a legitim felhasználó sem kapnak visszajelzést a tévesen címzett levelekről. Mindezek miatt a visszajelzés letiltása nem javasolható.
A legmegfelelőbb természetesen az SMTP protokoll finomítása lenne, de mit tudunk addig is tenni, amíg ez nem következik be?

Javasolt megoldásunk:

Egy olyan komponensekből álló rendszert javaslunk a probléma megoldására, ami a meglevő működő rendszerünk mellé beépül és megakadályozza az ilyen típusú támadásokat. Ez a rendszer egyrészt áll egy syslog elemzőből, egy spam detektorból és egy víruskereső részből. Az eredményeket központi nyilvántartásban összegezzük, azaz nyilvántartjuk azokat a gépeket, amelyek DHA támadásban érintettek. A központi nyilvántartás segítségével a komponenseinket használó összes résztvevő profitál egymás bajából is, azaz egy támadó nem csak egy helyen lesz kitiltható, de másoknak sem fog károkat okozni.
A syslog elemző rendszer az e-mail kiszolgáló jelentéseiből megnézi, hogy a téves címzéssel rendelkező e-mailek honnan jönnek hozzánk (milyen IP címről), és ezekről részletes jelentést tesz a központi adatbázisnak. A téves riasztások alacsonyan tartása érdekében módszert mutatunk be arra, hogy az egyedi téves levelek elválaszthatóvá tehetők legyenek a valódi támadóktól.

Rendszerünk összeköthető spam-felismerő szoftverekkel is. A megoldás lehetővé teheti erőforrások megtakarítását azáltal, hogy az ismert DHA támadó szerverekről érkező leveleket, vagy azok egy részét már nem vetjük alá erőforrásigényes tartalomszűrési eljárásoknak, hanem tiltjuk azokat. Rendszerünk más módszerekkel kombinálva azok hatékonyságát is jelentősen növelheti.