RIIGI INFOSÜSTEEMI AMET

DNS teenuses avastatud haavatavus / DDoS NXNSAttack

Ülevaade

19. mail avalikustasid Iisraeli teadlased disainiveast tuleneva haavatavuse ülemaailmses domeeninimede lahendamise süsteemi (DNS) teenuses. Haavatavust ära kasutades on võimalik läbi viia ulatuslikke teenusetõkestusründeid (DDoS) ründaja valitud veebilehtede või siis DNS teenusepakkujate kogu kliendibaasi vastu. Ründemeetodit, mis seda haavatavust kasutavad, nimetatakse NXNSAttack ja suure võimendusefekti tõttu ei ole ründajal vaja suurt infrastruktuuri. Seni ei ole teateid, et NXNSAttack meetodiga ründeid oleks ellu viidud, ent informatsioon on ka üsna uus.

Rünnaku võimaliku efekti kirjeldamisel tuuakse paralleele 2016 sügisel toimunud ründega, kus internetifirma Dyn kliente DNS kaudu rünnates muutusid ligipääsmatuks mitmed globaalse tähtsusega lehed ja teenused nagu PayPal, Twitter, Visa, CNN, Airbnb, Amazon jne. Tookord kasutasid ründajad Mirai robotvõrgustikku tuhandete mõjutatud seadmetega. Teadlased hoiatavad, et nüüd leitud haavatavus võimaldab saavutada sama suure efekti kordades väiksema seadmete arvuga.

Haavatavus ise tuleneb DNS protokollist ja seda kõrvaldada ei ole võimalik, ent saab paremini tõrjuda tarkvarauuendustega. Enamik suuri internetiteenuste pakkujaid nagu Google, Microsoft, Cloudflare, Amazon, Dyn, Versign jõudsid seda teadlaste eelhoiatuse põhjal ka teha, enne kui informatsioon avalikuks tehti.

DNS ehk domeeninime süsteem – mis see on?

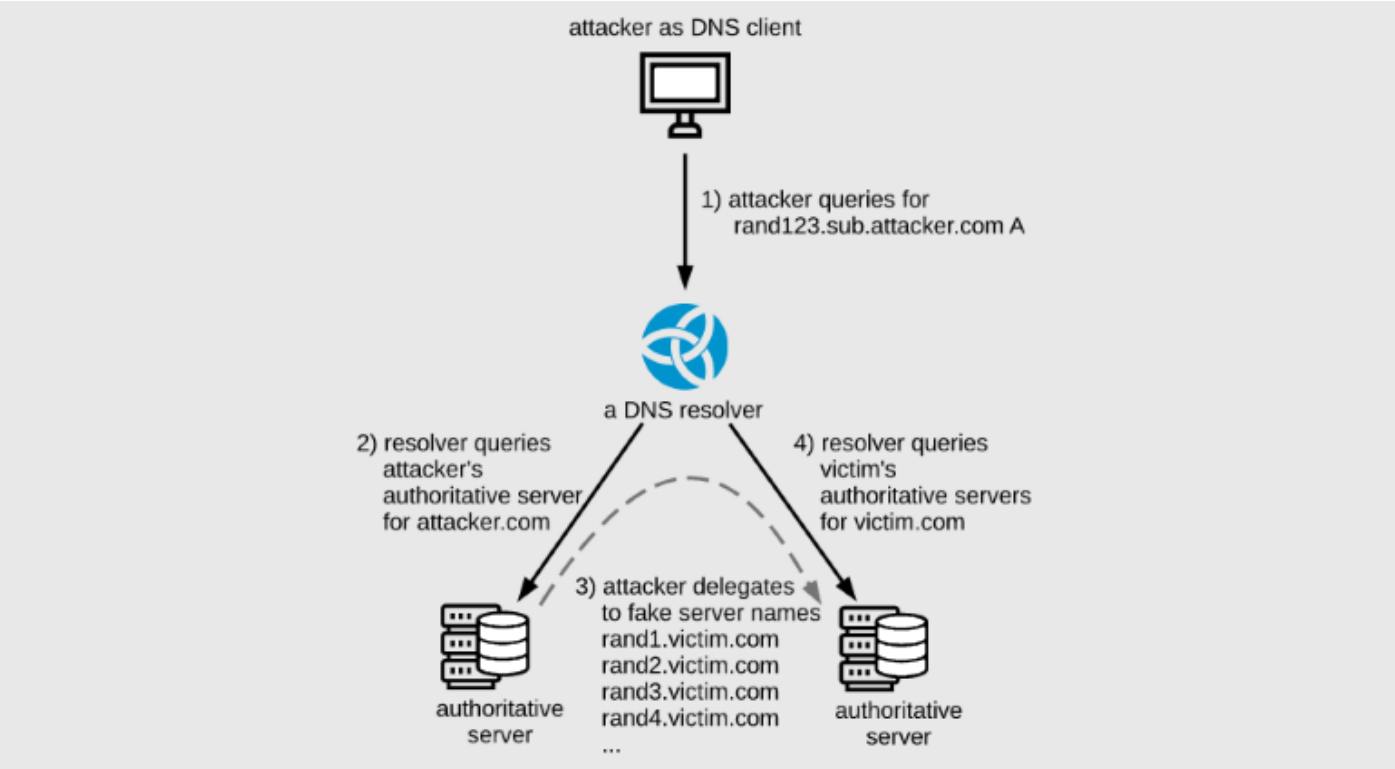
DNS on andmesidevõrgus töötav teenus, mis tõlgib domeeninimed internetis või intranetis kasutatavateks IP-aadressideks – seetõttu nimetatakse seda teenust vahel ka „Interneti telefoniraamatuks“. Näiteks kui kasutaja trükib brauserisse www.bbc.com, siis DNS server teeb teatud päringud ning tagastab kasutajale õige IP-aadressi(d), mille peal vastav veebileht on. Ilma DNS teenuseta saaks võrgus olevatele ressurssidele ligi ainult nende IP-aadressi teades. Reeglina on igal internetiteenuse pakkujal oma DNS serverid.

Rünnaku meetod:

NXNSAttack on oma olemuselt ummistusrünne, mille peegeldajaks on DNS serverid. Ummistusründed toimivad lihtsalt seletatuna nii: ründaja teeb päringu DNS serverile, server genereerib vastuse ja saadab selle ohvrile. Ründaja üritab küsida DNS serverilt võimalikult palju andmeid, et võimendusefekt oleks võimalikult suur. Kuna ründaja päringu pakett on väiksem kui DNS serveri vastus, siis saab ründaja väikse vaevaga väga efektiivse tulemuse.

NXNSAttack meetod kasutab ära DNS serverite hierarhiat päringutele vastamisel. Ründaja loob domeeni, näiteks attacker.com, ning seejärel saadab oma arvutist või arvutite võrgustikust erinevaid päringuid olematute domeeninimede kohta, lisades ohvri õigele domeeninimele näiteks suvalise arvujada. Selliste päringutega tegelevad reeglina teenusepakkuja nimelahendajad ehk resolverid, mis esitavad ründaja kontrolli all olevale nimeserverile päringu olematute alamdomeenide IP aadresside kohta. Nimeserver vastab, et soovitud IP aadressi leida ei ole võimalik ja suunab resolveri

tegema uusi päringuid teistele DNS serveritele. Niimoodi on võimalik panna DNS serverid tegema tuhandeid asjatuid päringuid vastuseks ründaja saadetud ühele päringule.



Allikas: nic.cz, https://www.zdnet.com/article/nxnsattack-technique-can-be-abused-for-large-scale-ddos-attacks/

Mõju

Haavatavus puudutab enamikke nii vabavara kui kommertstarkvara kasutavaid DNS servereid. Kuna haavatavus võimaldab potentsiaalselt läbi viia suure võimendusefektiga ründeid, tuleb seda pidada tõsiseks: kui enamike DDoS rünnete puhul on võimendusefekt vahemikus 2 – 10, siis teadlaste hinnangul on NXNSAttack meetodil võimalik saavutada isegi kuni 1000x suurem paketivõimendusfaktor. Konkreetne võimendusefekt sõltub DNS tarkvarast, mida rünnatavad serverid kasutavad.

Siiani teateid NXNSAttack meetodil läbi viidud edukatest rünnakutest ei ole. Enne haavatavuse avalikustamist tegid teadlased koostööd suuremate teenusepakkujatega, aidates neil välja töötada tarkvarauuendused ja muud abinõud, mis selle ründe eest kaitsevad – seetõttu reaalse ründe võimalus on juba suures osas maandatud. Siiski ei ole tänaseks kaitstud kõik kasutusel olevad DNS serverid.

Avastatud haavatavus väärib tähelepanu ka seetõttu, et puudutab DNS-i ehk ühte kõige kriitilisemat internetiteenust. Just see komponent võimaldab meie arvutil leida ja kuvada sisu meile arusaadaval moel. Ka meiliteenused ja sotsiaalmeedia sõltuvad DNS-ist täielikult.

Soovitused

1. Kui sinu ettevõte kasutab DNS teenust mõne suurema internetiteenuse pakkuja kaudu (Telia, Elisa, Zone, Veebimajutus vmt), pead lootma, et nemad globaalsete tarkvaralahenduste kasutajatena on vajalikud uuendused ära teinud.

2. Kui haldad oma nimeserverit ise, siis kontrolli, et kasutaksid vastava tarkvara (BIND, Microsoft DnS vms) kõige viimast versiooni. Suuremad tarkvaratootjad on avaldanud ka oma hinnangu / soovitused antud haavatavusega seonduvalt, vt nt https://support.microsoft.com/en-gb/help/4564355/guidance-for-dns-amplification-discussed-in-adv200009.
Samuti soovitame rakendada DNS teenuses Response Rate Limit-i (RRL) võimekuse.

3. Kaalu oma domeeni kaitsmist täiendava turvakihi ehk DNSSEC abil. Ehkki see DDoS-ide eest otsest kaitset ei paku, võimaldab see nimelahenduste puhul kasutada nn. DNSSEC puhvrit, mis vähendab tühjade päringute hulka ning seeläbi ründe mõju sinu domeeni suunas. DNSSEC teenust pakuvad mitmed Eesti akrediteeritud registripidajaid ning enda nimeserverite puhul ei ole rakendamine väga keerukas.

Kasutatud kirjandus:

1. Iisraeli teadlaste uurimistöö „NXNSAttack: Recursive DNS Inefficiencies and Vulnerabilities,“ www.nxnsattack.com/dns-ns-paper.pdf

2. https://en.blog.nic.cz/2020/05/19/nxnsattack-upgrade-resolvers-to-stop-new-kind-of-random-subdomain-attack/

3. https://www.wired.com/story/dns-ddos-amplification-attack/

4. https://www.zdnet.com/article/nxnsattack-technique-can-be-abused-for-large-scale-ddos-attacks/