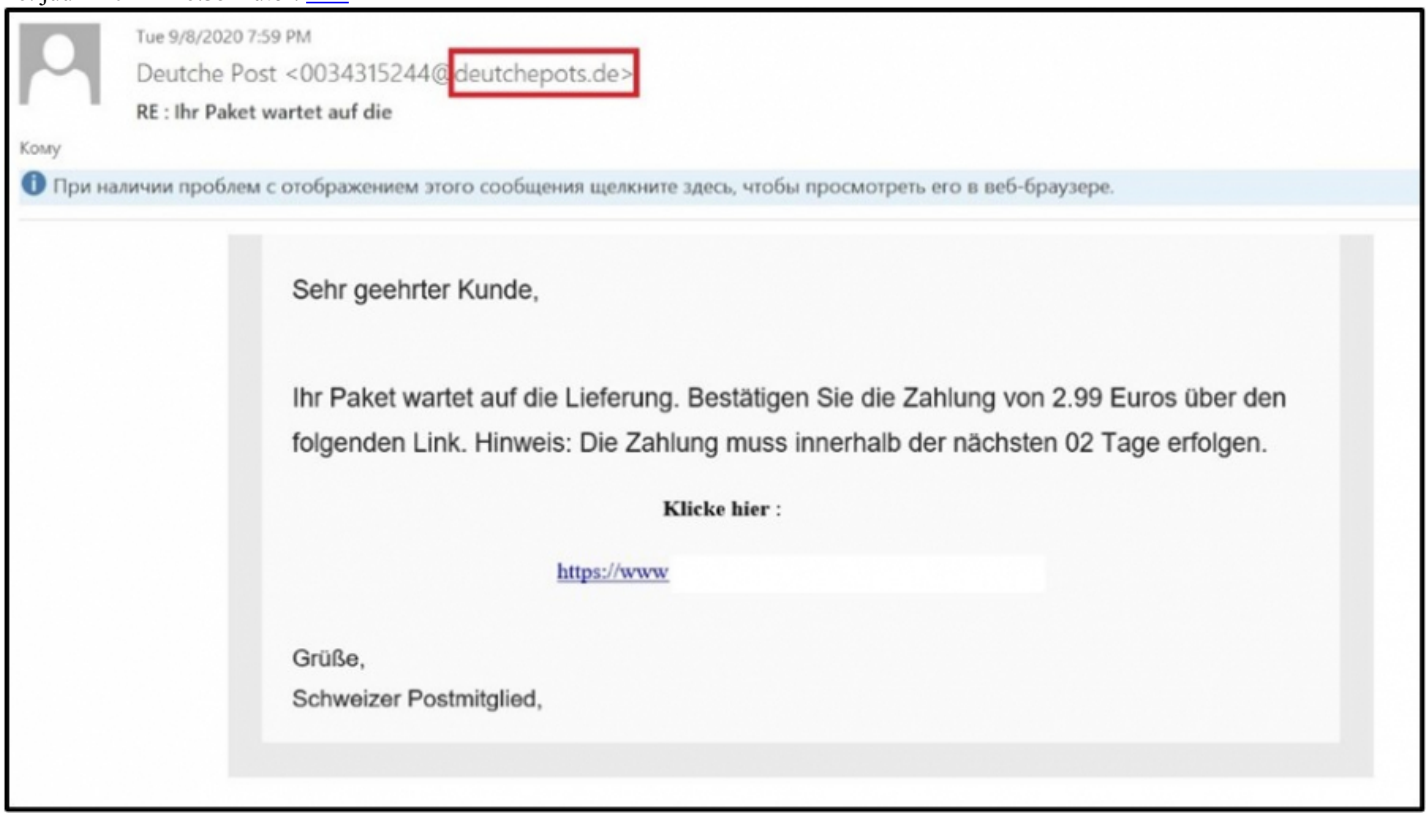
Võltsmeilid jälle tõusuteel: e-posti nn spuufimisrünnete arv kahekordistus aprillist maini

16. juuni 2021 - 16:35 Autor: AM



2021. aasta aprillist maini kahekordistus e-posti nn spuufimisrünnete koguarv, tõustes 4440-lt 8204-le. Keerukamad spuufimisründed hõlmavad näilisi domeene: ründajad kasutavad konkreetseid registreeritud domeene, mis sarnanevad tuntud organisatsioonide omadega.

E-posti spuufimine tähendab õigetena näivaid võltsmeile, et meelitada kasutajaid tegema ründajale kasulikke toiminguid. Selleks võib olla pahavara allalaadimine, süsteemidele või andmetele juurdepääsu võimaldamine, isikuandmete pakkumine või raha ülekandmine. Tihti tundub nende e-kirjadega, et need pärinevad mainekatelt organisatsioonidelt, mis seab ohtu mitte ainult linkidel klõpsajad, vaid ka nende ettevõtete maine, kelle domeeni kuritarvitati. Veelgi enam, spuufitud meilid võivad olla osa suurematest mitmeastmelistest rünnetest. Sellised rünnakud on tõusuteel.

Taolisi ründeid saab teha mitmel viisil. Lihtsaim on õige domeeni võltsimine. Selle puhul sisestab keegi päisesse „Saatja" spuufitava organisatsiooni domeeni nime, muutes võltsmeili pärismeilist eristamise väga keeruliseks. Kui äriühing on aga kasutanud mõnd uuemat e-posti autentimismeetodit, peavad ründajad kasutama mõnda muud meetodit. See võib toimuda sarnase nimekujuga, kui ründajad petavad inimest, kes meili saab, jättes mulje, nagu oleks selle saatnud mõni ettevõtte tegelik töötaja.

Avapildil toodud näites saatsid ründajad meili, mis näis olevat pärit Saksa postiettevõttelt Deutsche Post (deutschepost.de). Sõnumis väidetakse, et peab maksma paki kohaletoimetamise eest, kuid klõpsates lingil selgub, et kaotate mitte ainult kolm eurot, vaid annate petturitele ka oma pangakaardi andmed. Lähemal uurimisel õnnestuks kasutajail märgata õigekirjaviga domeeninimes ja seega mõista, et e-kiri oli võlts. See pole aga UNICODE spuufinguga võimalik.

UNICODE on domeenide kodeerimiseks kasutatav standard, ent kui domeeninimed kasutavad mitte-ladinakeelseid elemente, teisendatakse need elemendid UNICODE'ist teiseks kodeerimissüsteemiks. Tulemuseks ongi see, et koodi tasemel võivad kaks domeeninime erineda, näiteks kaspersky.com ja kaspersky.com kirillitsas y-ga, ent kui meilid välja saadetakse, kuvatakse need mõlemad päises „Saatja" ühtemoodi.

"Spuufimine võib tunduda primitiivne, kui võrrelda seda mõne muu küberkurjategijate kasutatava tehnikaga, kuid see võib olla väga tõhus. See võib olla ka lihtsalt keerulisem ettevõtte e-posti kahjustamise ründe esimene etapp: need on ründed, mis võivad tuua kaasa identiteedivarguse ja ettevõtte töö seisaku, samuti märkimisväärsed rahalised kaotused. Hea uudis on see, et saadaval on hulk spuufimisvastaseid kaitselahendusi ja uusi autentimisstandardeid, mis võivad teie ettevõtte meiliaadressi turvalisena hoida," kommenteeris Kaspersky turvaekspert Roman Dedenok.

Lisateavet spuufimisrünnete esinemise võimaluste ja ohutuse tagamise kohta saab Securelistist.

Et vähendada ettevõtte sattumist spuufimise ohvriks, soovitavad Kaspersky turvaeksperdid järgmist:

1. Võta oma ettevõtte meiliaadressi jaoks kasutusele e-posti turvalise autentimise meetod, nagu nt SPF, DKIM või DMARC.
2. Vii läbi turvateadlikkuse koolituskursus, mis hõlmab e-posti turvalisuse teemat. See aitab õpetada töötajatele aadressi põhjalikumat kontrollimist, kui nad tundmatult inimeselt e-kirju saavad, ja õppima muid e-posti turvalisuse põhireegleid.
3. Kui kasutada Microsoft 365 pilveteenust, tuleb ka seda kaitsta.

- Uudised
- Turvalisus