Kübergrupeering Poseidon tegeleb küberväljapressimise ja katusepakkumisega

8 aastat tagasi Autor: AM

Kas metsikud 90ndad väljapressimiste ja katusepakkumistega on jõudmas digimaailma? Kaspersky Lab leidis jäljed kübergrupeeringust, mis varastab konfidentsiaalseid andmeid ettevõtetelt üle maailma juba aastast 2005 ning nõuab peale infonäppamist ohvrilt infoturvalisuse teenuse nõustamisteenuste lepingu sõlmimist, ähvardades muidu andmete müügiga. Grupeeringu Poseidon tegevusest rääkis Kaspersky Lab Kaspersky Security Analyst Summitil.

Rünnakute ohvriteks on sattunud finants-, telekommunikatsiooni-, tööstus- ja energiakompaniid, riigiasutused, meedia, suhtekorraldusagentuurid ja isegi *catering*-firmad, kelle klientideks on suurkorporatsioonide tipp-juhid. Venemaal, Kasahstanis, USAs, Prantsusmaal, Araabia Ühendemiraatides ja Indias on kannatada saanud 35 organisatsiooni. Küberspionaaži kampaania puudutas ka Brasiiliat. Peamise keelena kasutab grupeering portugali keele brasiilia varianti.

Erilist huvi näitavad kurjategijad korporatiivsete sisevõrkude vastu. Rünnakuteks kasutatakse spetsiaalselt väljatöötatud kahjutoovat arvutitarkvara, mis on allkirjastatud võltsitud digitaalsete sertifikaatidega. Kõige sagedamini imbub see süsteemi RTF- ja DOC-manustega *phishing*- ehk õngitsuskirjade abil, mis tavaliselt laekuvad personaliteenistuste teadaannete kujul. Peale süsteemi kinnitumist kogub kahjutoov arvutitarkvara suure mahu konfidentsiaalseid andmeid, sealhulgas finantsandmeid. Ründajad kasutavad varastatud andmeid väljapressimise tööriistana, sundides kannatanud kompaniid koostööle või siis müüvad neid andmeid edasi kolmandatele isikutele.

„See on kübergrupeering, mis oli mitme aasta jooksul tegutsedes avalikkusele tundmatu, otsiti ohvreid väga erinevates valdkondades. Näiteks meie avastasime rea Poseidoni käsuservereid internetiühenduse pakkujate infrastruktuuris, kes teenindavad merelaevu," räägib Dmitri Bestužev, Kaspersky Lab'i Ladina-Ameerika Uuringukeskuse juht. „Oma tegevuse jälgede peitmiseks kasutasid kurjategijad tervet rida kavalaid vahendeid, sealhulgas meie poolt avastatud väga lühikese elutsükliga pahavara (*malware*)."

> Aruande täisversioon koos vahendite ja saastamise statistika detailse kirjeldusega asub siin: securelist.com.

- Uudised
- Turvalisus