Plinta duomenis užšifruojantis ir išpirkos bitkoinais reikalaujantis virusas

Išpirkos reikalaujantys virusai nėra naujiena, o nesusekama virtuali bitkoino valiuta tokių kenkėjiškų programų kūrėjų gyvenimą dar palengvino.

Pastaruoju metu didelio saugumo specialistų dėmesio sulaukia aktyviai plintantis virusas „CryptoLocker“, kuris užšifruoja kompiuteryje įrašytus dokumentus, o už iššifravimo raktą reikalauja sumokėti išpirką. Dažniausiai išpirkos reikalaujantys virusai grasina ištrinti dokumentus ar suformatuoti kietąjį diską (nors yra ir subtilesnių variantų – pavyzdžiui, raginančių susimokėti baudą, antraip į namus bus iškviesta teisėsauga).„CryptoLocker“ elgiasi dar įžūliau: patekęs į kompiuterį, šis virusas užšifruoja jame esančius failus (nuotraukas, vaizdo įrašus, dokumentus ir t.t.), panaudodamas 2048 bitų versijos RSA kriptografinį algoritmą. Maža to, virusas gali pasiglemžti ir kitų prie tinklo prijungtų kompiuterių failus.Auka informuojama, kad turi 72 valandas sumokėti 300 dolerių arba 300 eurų išpirką į nurodytą sąskaitą bitkoinų valiuta.Jei to nepadarys, iššifravimo raktas bus sunaikintas ir naudotojas rizikuoja visiems laikams prarasti savo failus ar dokumentus.Arstechnica.com rašo apie atvejį, kai „CryptoLocker“ buvo atsiųstas į vienos kompanijos buhalterijos skyriaus darbuotojo el. paštą. Laiškas su prisegtu „zip“ archyvu bei jame esančiu diegimo failu eiliniam vartotojui išsyk sukeltų įtarimą apie galimą virusą, tačiau laiškas buvo atsiųstas iš finansinės institucijos, todėl darbuotojas nepagalvojo imtis atsargumo priemonių. Atidarius failą ekrane šmėstelėjo baltas langas, bet daugiau nieko įtartino neįvyko, todėl darbuotojas užrakino kompiuterį ir išėjo iš kabineto – jam reikėjo sudalyvauti keliuose susitikimuose.Po kelių valandų kompanijos IT skyriui buvo pranešta apie sugadintą failą prie tinklo prijungtame kompiuteryje. Pradėję aiškintis situaciją IT skyriaus darbuotojai rado daugiau tokių failų ir pastebėjo įtartiną užkrėstojo kompiuterio veiklą.Nuskubėję atjungti šį kompiuterį nuo tinklo, darbuotojai jo ekrane pamatė pranešimą apie reikalaujamą išpirką. „CryptoLocker“ spėjo atlikti savo užduotį ir užšifravo kelis šimtus gigabaitų kompanijos dokumentų. Kadangi kito būdo atstatyti svarbių failų nebuvo, kompanija nusprendė sumokėti nurodytą išpirką.Socialinio tinklaraščio „Reddit“ nariai teigia, kad veiksmingo būdo iššifruoti šios kenkėjiškos programos paliestus failus kol kas nėra. Taigi jei virusas spėjo pasidarbuoti ir dokumentai yra gyvybiškai būtini, norint juos atgauti, teks sumokėti išpirką. Tiesa, jei kompiuteryje yra įjungta sistemos atstatymo funkcija, ji gali padėti susigrąžinti bent dalį anksčiau įrašytų failų.Didelė dalis antivirusinių aptinka virusą ir sugeba jį pašalinti, bet jei virusas spėjo užšifruoti failus, jo ištrynimas susigrąžinti duomenų nepadės.Atsižvelgiant į šio viruso išplitimą, manoma, kad jo kūrėjai per metus gali uždirbti apie 5 mln. dolerių.Norint apsaugoti kompiuterį nuo kenkėjiškų programų, patartina naudoti patikimą antivirusinę programą, vengti įtartinų interneto svetainių, neatidarinėti prie el. laiškų prisegtų įtarimą keliančių failų. Ypač svarbių failų ar dokumentų kopijas patariama saugoti atsarginiame prijungiamame kietajame diske ar kitoje atminties laikmenoje. Būkit atsargūs.

Date created: 2013/10/21-