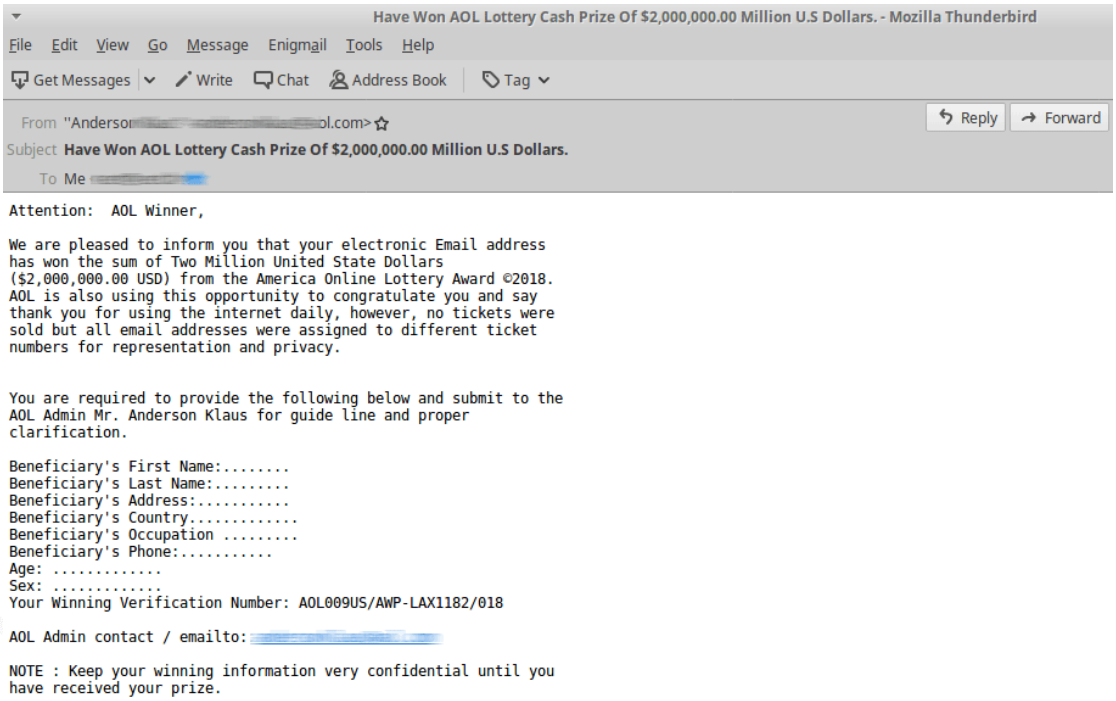
Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS PRIE KRAŠTO APSAUGOS MINISTERIJOS

INFORMACINIS BIULETENIS
APSAUGOS PRIEMONĖS KOVAI SU BRUKALU

2018 m. gruodžio 31 d.

Per dieną kiekviena el. pašto dėžutė sulaukia nuo keleto iki kelių dešimčių brukalo (angl. *SPAM*) laiškų. Neva asmuo laimėjo loterijoje (pav. 1) ar gavo palikimą iš tariamo tolimo giminaičio ir milijonai yra pasiekiami tik pateikus savo asmens ir mokėjimo kortelės duomenis. Dalis brukalo laiškų - nepavojingi, nes yra tik įmonių vykdomų reklaminių kampanijų dalis - reklamuojamos realiai teikiamos paslaugos ar prekės. Kita dalis laiškų gali bandyti apkrėsti jūsų kompiuterį žalinga programine įranga, stengtis išgauti jūsų asmeninius duomenis, kad nuskaitytų pinigus, pavogtų tapatybę ar vykdytų kitą žalingą veiklą.



Pav. 1 Brukalas apie laimėjimą loterijoje

Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

Nacionalinis kibernetinio saugumo centras apibendrina pagrindines saugumo priemones, kurių galėtų imtis sistemų administratoriai, siekdami labiau apsaugoti savo naudotojus nuo nepageidaujamų laiškų bei sumažinti dėl to kylančias rizikas.

Įdiekite SpamAssassin. Tai populiariausia serverio lygmens atvirojo kodo priemonė kovoje su nepageidaujamais laiškais, naudojanti skirtingus brukalo atpažinimo metodus. „SpamAssassin“ programinė įranga vertina laiškų antraštes (angl. *headers*) bei turinį ir pagal tai suteikia tam tikrą balą, nusakantį, kokia tikimybė, kad atitinkamas elektroninis laiškas yra brukalas. Remiantis šiuo vertinimu, pašto serverį aptarnaujanti programinė įranga gali reaguoti atitinkamai - atmesti laišką, pažymėti jį kaip brukalą arba pristatyti gavėjui, jeigu balas neviršija jūsų nustatytos normos.

Naudokite juoduosius RBL sąrašus (angl. *Real-time Blackhole List*). Šiuose sąrašuose publikuojami serverių adresai, kurie yra žinomi dėl brukalo siuntinėjimo. Jeigu jūsų serverį pasiektų laiškas iš vieno tokių adresų, jis būtų automatiškai blokuojamas. Šį sprendimą galima naudoti tiek kaip atskirą priemonę, tiek kaip „SpamAssassin“ papildymą. Tokie juodieji sąrašai yra plačiai naudojami, todėl sistemų administratoriams svarbu rūpintis savo sistemų saugumu, kad jos netaptų brukalo siuntinėjimo židiniais.

Tikrinkite SPF įrašus. Tai viena iš priemonių kovai su suklastotais siuntėjais (angl. *spoofing*) - tokie įrašai nurodo, kokie IP adresai gali siųsti el. laiškus iš atitinkamo domeno. Jeigu tikrasis domeno savininkas savo sistemoje yra apsirašęs SPF įrašus, o gavėjo sistema šiuos įrašus sutikrina, suklastoti laiškai gavėjų nepasieks. Tai taip pat gera priemonė apsisaugoti, kad nuo jūsų domeno nebūtų siuntinėjami suklastoti el. laiškai kitiems, todėl apsirašykite SPF DNS įrašus ir savo sistemose.

Filtravimas pagal turinį. Viena iš priemonių galėtų būti filtravimo sprendimas, paremtas laiško turinio vertinimu, ieškant uždraustų žodžių arba naudojant taisykles (angl. *regular expressions, regex*). Vis tik toks sprendimas dažniausiai apsaugo tik nuo elementariausių brukalo variantų, o kartais ir legitimūs laiškai būna atmetami, todėl turėtų būti naudojamas atsargiai.

Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

Kitos priemonės, kurias turėtų apsvarstyti administratoriai:

- Suteikite brukalo statusą laiškams, kurie siunčiami iš IP adresų, neturinčių *reverse DNS* (PTR įrašo);
- Blokuokite laiškus, kurie siunčiami iš neegzistuojančių domenų;
- Blokuokite sujungimus, kuomet siuntėjo tarnybinė stotis nepateikia HELO / EHLO parametro;
- Pagal finansines galimybes galėtų būti naudojamos ir mokamos filtravimo priemonės tiek serverio, tiek galutinio vartotojo lygmenyse.

Administratoriai taip pat turėtų reguliariai mokyti savo sistemų naudotojus:

- Nespausti jokių brukalo nuorodų ir neatidarinėti prisegtų bylų;
- Reguliariai tikrinti brukalo skiltį, siekiant aptikti neteisingai nufiltruotus laiškus ar taisyklių atnaujinimui;
- Niekada neatsakinėti į nepageidaujamus laiškus;
- Neaktyvuoti juose paveikslėlių, kurie būna automatiškai išjungti;
- Žymėti nepageidaujamus laiškus kaip brukalą atitinkamai pagal naudojamą kliento pašto programinę įrangą.

Baltieji sąrašai (angl. *whitelisting*). Dėl daugybės naudojamų brukalo filtravimo priemonių reikėtų apsvarstyti siuntėjų, su kuriais bendraujama dažniausiai, pašto serverių įtraukimą į baltuosius sąrašus. Tokiu būdu apsisaugosite nuo netinkamai atmestų jums svarbių laiškų. Turėkite omenyje, kad į tokius sąrašus įtraukus domenus, net ir suklastoti laiškai iš šių domenų pasieks adresatą, todėl įtraukti patartina tik IP adresus.