Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
PRIE KRAŠTO APSAUGOS MINISTERIJOS

KIBERNETINIO INCIDENTO TYRIMO ATASKAITA „EMOTET“ KENKSMINGO PROGRAMINIO KODO PLATINIMAS

2021 m. sausio 11 d.
Vilnius

Kibernetinio incidento apibūdinimas

2020-12-21 – 2020-12-29 dienomis el. pašto priemonėmis vyko ***„Emotet“*** kenksmingo programinio kodo (toliau – ***„Emotet“***) platinimas. ***„Emotet“*** buvo platinamas klastojant siuntėjus ir naudojant tikrų el. laiškų susirašinėjimo įstoriją. Prie el. laiško buvo prisegtas ****.zip*** formato failas, kuriame ir buvo slepiamas ***„Emotet“***. Incidentų metu buvo paveikta nemažiau kaip 15 organizacijų. El. pašto paskyros naudojamos tolimesniam ***„Emotet“*** platinimui.

Incidento įvykių laiko juosta

2020-12-22
- Fiksuojami pirmieji galimai „Emotet“ užkrėsti galiniai įrenginiai (kompiuteriai)

2020-12-29
- NKSC identifikuoja Lietuvos organizacijų el. pašto paskyras per kurias platinamas „Emotet“, informuojami atitinkami subjektai

2020-12-29/30
- Nustatomi nauji „Emotet“ grėsmių indikatoriai, fiksuojami galimai "Emotet" užkrėsti galiniai įrenginiai (kompiuteriai), informuojami atitinkami subjektai

2020-12-31
- NKSC atlikus analizę pagal turimus „Emotet“ kodo grėsmių indikatorius, naujų „Emotet“ tinklo komunikacijų aptikta nebuvo (t. y. nepavyko identifikuoti galinius įrenginius užkrėstus „Emotet“) , informuojami subjektai

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

Išvados

- ***„Emotet“*** vis dar sparčiai plinta pasaulyje. NKSC turima informacija Lietuvoje ***„Emotet“*** suaktyvėjimas pastebimas nuo 2020 m. gegužės – birželio mėn. NKSC ne kartą savo svetainėje ir ***„Facebook“*** socialinio tinklo paskyroje informavo visuomenę apie plintantį ***„Emotet“*** ir teikė rekomendacijas kaip valdyti grėsmę;
- ***„Emotet“*** platinimui naudojamas toks pat metodas – siunčiami el. laiškai su prisegtuku (****.doc***, ****.xls*** ar ****.zip*** formato failais) arba el. laiške pateikiama nuorodą į ***„Emotet“*** atsisiuntimą – organizacijos vis dar skiria nepakankamą dėmesį naudotojų mokymams apie socialinės inžinerijos grėsmes bei saugų naudojimąsi el. paštu, nėra taikoma griežta el. pašto kibernetinio saugumo politika (pvz., vykdomųjų failų, archyvinių bylų, dokumentų su *macros* komandomis sustabdymas patikrinimui prieš laiško turintį pristatant galutiniam naudotojui);
- Nuo **2020-12-21** iki **2020-12-30** nemažiau nei 15 organizacijų buvo paveiktos ***„Emotet“***;
- Kibernetinio saugumo subjektai vis dar nepakankamai dėmesio skiria kibernetiniam saugumui: negeba identifikuoti kibernetinių incidentų (el. laiškais platinamo ***„Emotet“***), laiku ir teisės aktų nustatyta tvarka neinformuoja NKSC apie įvykusius / vykstančius kibernetinius incidentus;
- ***„Emotet“*** pasižymi didele ***„botnet“*** tinklo infrastruktūra: naudojamos įvairios, dažniausiai kompromituotos svetainės ***„Emotet“*** platinimui. Šimtai skirtingų IP adresų naudojami komandų ir kontrolės serverių veikloje. ***„Botnet“*** tinklo infrastruktūra nuolat kinta, todėl neturint naujausių ***„Emotet“*** kodo grėsmių indikatorių negalima greitai ir efektyviai aptikti organizacijas, kurių galiniai įrenginiai užkrėsti ***„Emotet“***;
- Kibernetinio saugumo subjektams laiku ir nustatyta tvarka informavus NKSC apie įvykusius / vykstančius kibernetinius incidentus ar pastebėtą įtartiną veiklą, pateikus el. laiškų pavyzdžius, kibernetinių incidentų aptikimas ar jų pasekmių šalinimas taptų žymiai efektyvesnis;

Rekomendacijos

- Dažniausiai naudotojams apgauti naudojami socialinės inžinerijos metodai, kai stengiamasi sudominti, išgąsdinti ar manipuliuoti įvairiomis emocijomis, todėl itin svarbus nuolatinis darbuotojų sąmoningumo ugdymas: vartotojų švietimas, supažindinant su galimomis grėsmėmis, kibernetinio saugumo pratybų organizavimas, rekomendacijos, kaip elgtis su įtartinais laiškais, jų priedais ar dokumentais;
- Gavus keisto ar įtartino turinio elektroninį laišką nuo žinomo asmens ar organizacijos tikrinti elektroninio laiško antraštes (*angl. headers*), kuriose matoma, kas yra tikrasis laiško siuntėjas (laukelis „*From*“). Analizuojant antraštę, reikėtų žiūrėti į pirmą „*Received*“ parametrą nuo apačios. Šis parametras nurodys, iš kurio serverio buvo išsiųstas elektroninis laiškas. Jeigu „*From*“ laukas yra *siuntejas@imone.lt*, tai ir „*Received*“ laukelyje dažniausiai turi matytis adresų sritis (*domenas*) „*imone.lt*“;

- Neaktyvuoti elektroninio pašto skaitymui naudojamos programinės įrangos nustatymų, kurie automatiškai inicijuotų laiško turinyje esančių paveikslėlių atsisiuntimą. Įtartinuose elektroniniuose laiškuose neinicijuoti paveiksliukų atsisiuntimo;
- Nuolatos tobulinti el. pašto apsaugos priemones. Šio kibernetinio incidento galima buvo išvengi, jei el. pašto apsaugos sistemos automatiškai stabdytų / blokuotų / specialia žyma žymėtų el. laiškus kuriuose prisegtas archyvinis, vykdomasis failas, dokumentas su *macros* komandomis, arba failas apsaugotas slaptažodžiu. Incidento mąstą galima buvo sumažinti užblokavus siunčiamus el. laiškus pagal turinį ar raktažodžius turinyje, pavyzdžiui blokuojant ***„Arkivadgangskode“***, ***„Archive pass“*** ar pan.
- Naudoti ir nuolat atnaujinti galinių įrenginių (kompiuterių) antivirusinę programinę įrangą, kadangi praėjus 2 – 4 val. daugelių antivirusinių gamintojų programinė įranga jau geba identifikuoti naujas ***„Emotet“*** versijas.

Kibernetinio incidento analizė

2020-12-22 atliekant Lietuvos kibernetinės erdvės stebėseną, buvo pastebėtas ***„Emotet“*** platinimas - el. laiškų siuntimas. Atlikus el. laiške prisegto kenksmingo kodo analizę, buvo nustatyti nauji kenksmingo programinio kodo grėsmių indikatoriai – svetainė **http://countsquare[.]com/standardservices/mnR4/** iš kurios parsisiunčiamas ***„Emotet“***, o taip pat nustatytas komandų ir kontrolės serverio IP adresas **197[.]87.160.216.**

2020-12-22 11:38 nauji ***„Emotet“*** kenksmingo programinio kodo grėsmių indikatoriai buvo perduoti organizacijos atstovams su rekomendacijomis blokuoti svetainę ir IP adresą savo tinkluose.

2020-12-22 12:42 surinkus tai dienai ir valandai žinomus ***„Emotet“*** kodo grėsmių indikatorius ir atlikus NKSC analizę, buvo nustatytos dvi organizacijos, kuriose tikėtina buvo galiniai įrenginiai (kompiuteriai) užkrėsti ***„Emotet“***. Informacija apie organizacijų išorinius IP adresus ir tinklo komunikacijas buvo perduota organizacijų atstovams.

2020-12-23 atlikus pakartotinę NKSC analizę pagal tai dienai ir valandai turimus ***„Emotet“*** kodo grėsmių indikatorius, naują ***„Emotet“*** tinklo komunikacijų aptikta.

2020-12-29 10:10 atlikus detalesnę analizę pavyko nustatyti neįprastą el. laiškų siuntimą iš Lietuvos organizacijų el. pašto tarnybinių stočių, pasinaudojus šių organizacijų el. pašto paskyromis. Ši informacija buvo perduota organizacijų atstovams.

2020-12-29 10:44 NKSC gauna informaciją, kad tam tikros organizacijos darbuotojai informavo apie klaidinančio turinio informaciją siunčiamą el. paštu. Laiškai siųsti užmaskuoti kaip iš kito darbuotojo el. pašto, bet adresas visai neatitinkantis jų įstaigos. Tačiau rašomas turinys parašytas taisyklinga lietuvių kalba.

2020-12-29 13:21 surinkus tai dienai ir valandai žinomus ***„Emotet“*** kodo grėsmių indikatorius ir atlikus NKSC analizę, buvo nustatytos dvi organizacijos, kuriose tikėtina buvo galiniai įrenginiai

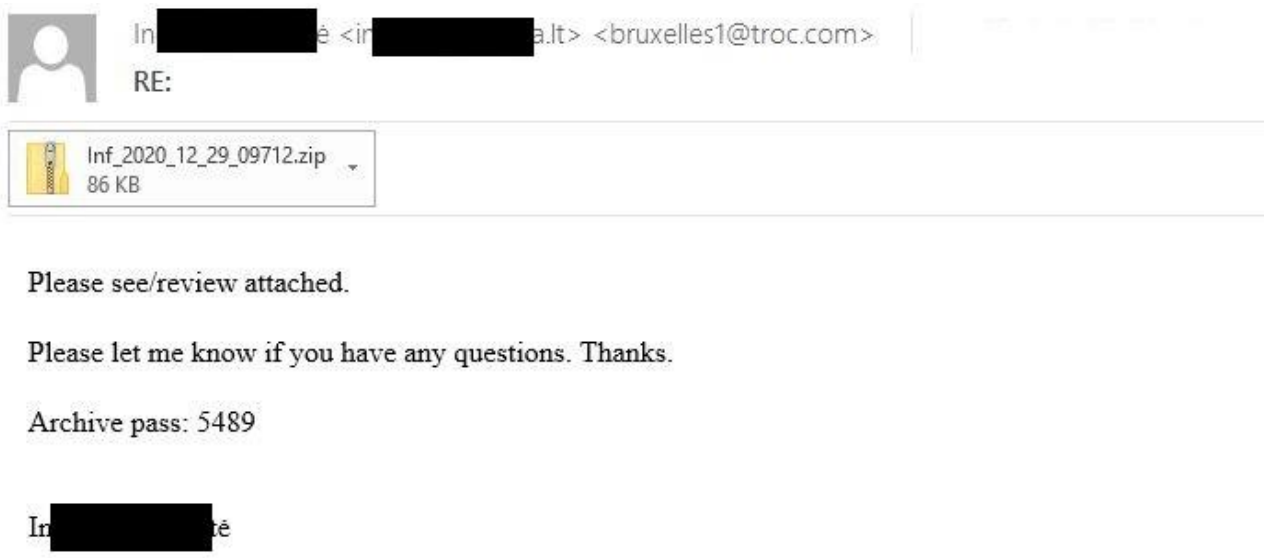
(kompiuteriai) užkrėsti ***„Emotet“***. Informacija apie organizacijų išorinius IP adresus ir tinklo komunikacijas buvo perduota organizacijų atstovams.

2020-12-29 13:31 NKSC pavyko nustatyti dvi naujas svetaines ***„dynamicsteels[.]com“*** ir ***„members.nlbformula[.]com“*** kuriose buvo talpinamas ***„Emotet“***. Papildomai pavyko identifikuoti tris organizacijas, kurios atidarė el. laiškus, kuriuose buvo patalpintas ***„Emotet“***. Informacija apie organizacijų išorinius IP adresus ir tinklo komunikacijas buvo perduota organizacijų atstovams.

2020-12-30 08:58 surinkus tai dienai ir valandai žinomus ***„Emotet“*** kodo grėsmių indikatorius ir atlikus NKSC kaupiamų srauto metaduomenų analizę, buvo nustatyta viena organizacija, kurioje tikėtina buvo galiniai įrenginiai (kompiuteriai) užkrėsti ***„Emotet“***. Informacija apie organizacijų išorinius IP adresus ir tinklo komunikacijas buvo perduota organizacijų atstovams.

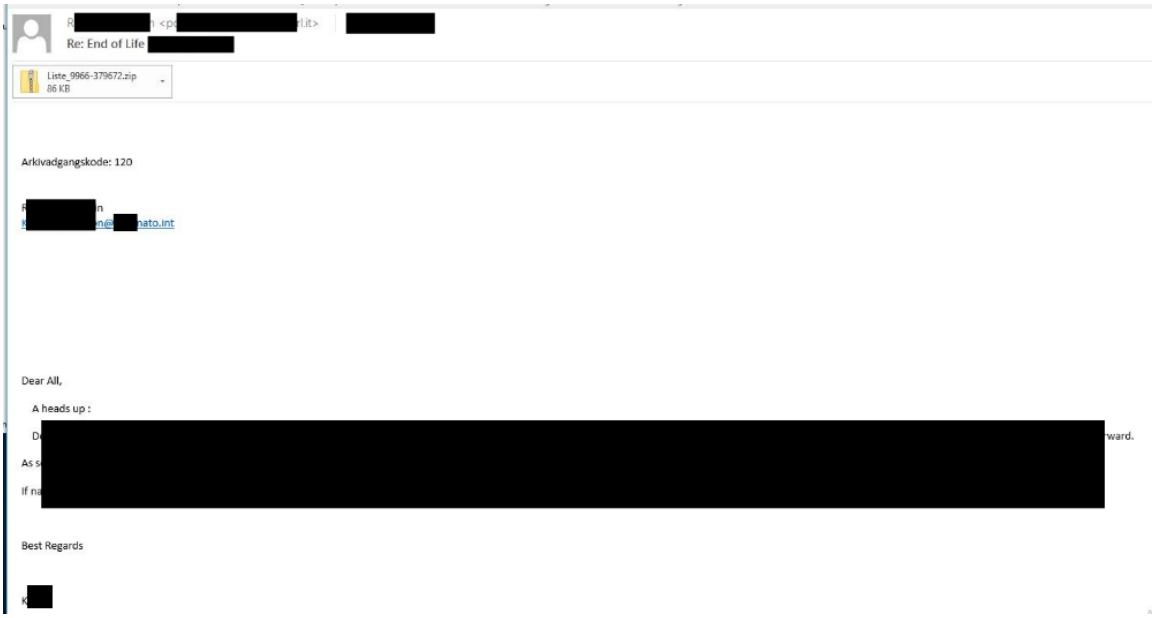
2020-12-30 12:11 surinkus tai dienai ir valandai žinomus ***„Emotet“*** kodo grėsmių indikatorius ir atlikus NKSC analizę, buvo nustatyta viena organizacija, kurioje tikėtina buvo galiniai įrenginiai (kompiuteriai) užkrėsti ***„Emotet“***. Informacija apie organizacijų išorinius IP adresus ir tinklo komunikacijas buvo perduota organizacijų atstovams.

2020-12-31 NKSC atlikus analizę buvo nustatyta, kad **2020-12-29** įvairioms viešojo sektoriaus organizacijoms buvo nusiųsta daugiau kaip 22 000 el. laiškų su prisegtu ****.zip*** formato failu, kuriame buvo patalpintas ***„Emotet“***. (5 pav.) El. laiškai buvo siunčiami iš daugiau, kaip 650 skirtingų IP adresų. Siunčiamo el. laiško pavyzdys pateiktas 1 - 2 pav.



1 pav. Siunčiame el. laiško pavyzdys

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt



2 pav. Siunčiame el. laiško pavyzdys

Galiniam įrenginiui užsikrėtus ***„Emotet“*** dažniausiai (priklauso nuo ***„Emotet“*** versijos) iš jo pavagiama el. pašto informacija (nustatymai, prisijungimo vardas / slaptažodis, adresatų sąrašas, susirašinėjimo istorija ir pan.). Priklausomai nuo ***„Emotet“*** versijos iš galinio įrenginio gali būti pavagiama ir interneto naršyklėse išsaugota prisijungimo informacija (vardai / slaptažodžiai), gali vykti vidinio tinklo skenavimai, slaptažodžių parinkimo atakos ir pan.

Iš aukščiau pateiktų faktų matosi, kad kibernetinio saugumo subjektai vis dar nepakankamai dėmesio skiria kibernetiniam saugumui: negeba identifikuoti kibernetinių incidentų (el. laiškais platinamo ***„Emotet“***), laiku ir teisės aktų nustatyta tvarka neinformuoja NKSC apie įvykusius / vykstančius kibernetinius incidentus. Reikia pažymėti, kad ***„Emotet“*** pasižymi didele ***„botnet“*** tinklo infrastruktūra: naudojamos įvairios, dažniausiai kompromituotos svetainės ***„Emotet“*** platinimui. Šimtai skirtingų IP adresų naudojami komandų ir kontrolės serverių veikloje. Kibernetinio saugumo subjektams laiku ir nustatyta tvarka informavus NKSC apie įvykusius / vykstančius kibernetinius incidentus ar įtartiną veiklą, pateikus el. laiškų pavyzdžius, kibernetinių incidentų aptikimas ar jų pasekmių šalinimas taptų žymiai efektyvesnis.