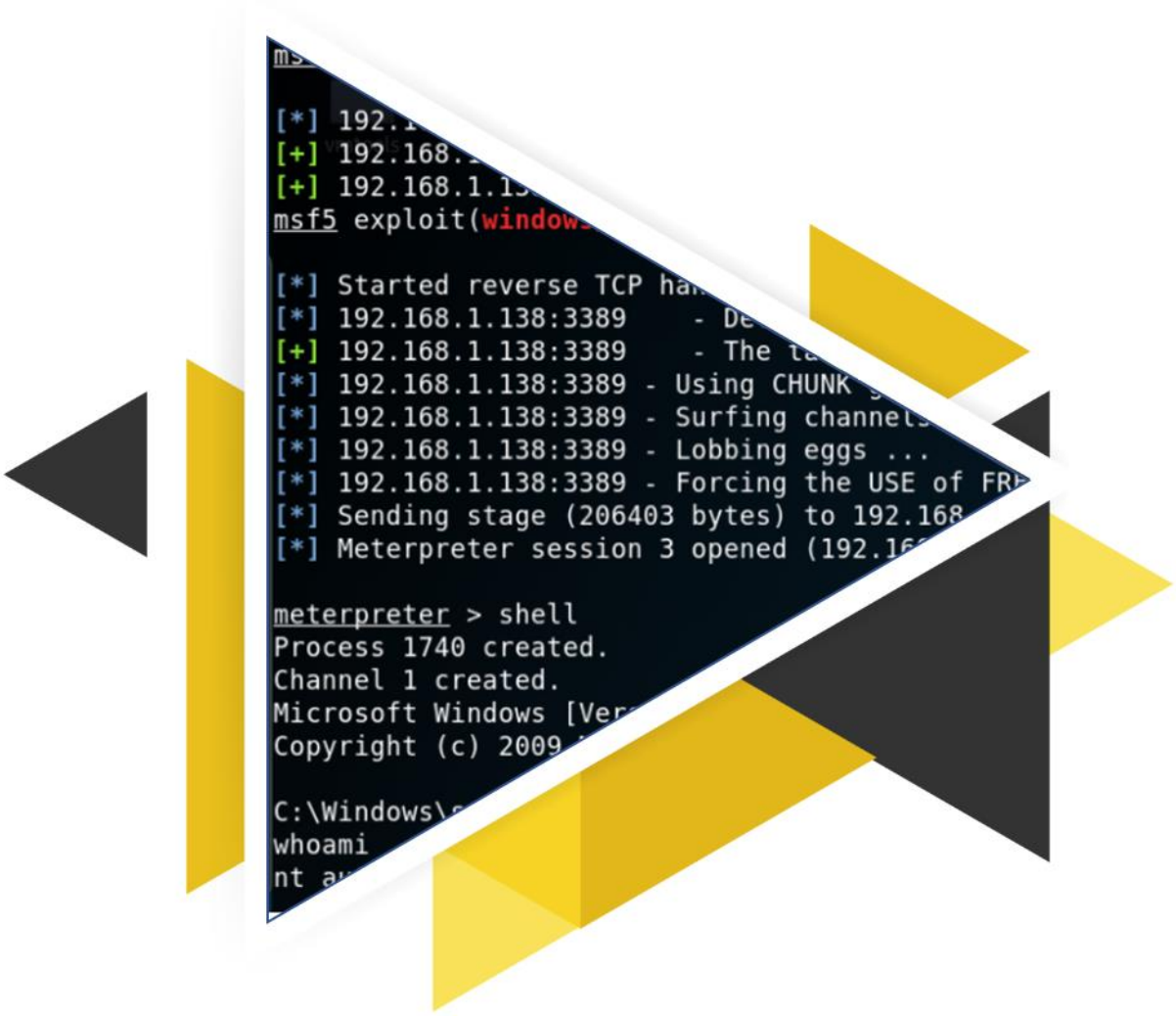
NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS PRIE KRAŠTO APSAUGOS MINISTERIJOS



2021 METŲ I PUSMEČIO NKSC CERT-LT ATASKAITA

TLP:WHITE

2021-07-26
Vilnius

TURINYS

I. SANTRAUKA 4

II. CERT-LT FIKSUOTI KIBERNETINIAI INCIDENTAI 6

2.1 CERT-LT KIBERNETINIŲ INCIDENTŲ TYRIMAI IR ANALIZĖS 11

2.1.1 „CityBee“ duomenų nutekėjimas 11

2.1.2 „Vatesl.lt“ puslapio kopija 11

2.1.3 Vilniaus kolegijos studentų duomenų nutekėjimo atvejis 12

2.1.4 Kenkėjišku programiniu kodu užkrėstos svetainės 13

I. SANTRAUKA

Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) duomenimis, 2021 m. I pusmetį Lietuvoje registruotų kibernetinių incidentų skaičius buvo panašus kaip ir ankstesniais metais. Buvo fiksuota 1780 kibernetinių incidentų, t. y. 2 proc. daugiau negu tuo pačiu 2020 m. laikotarpiu. Iš jų, vertinant pagal poveikio kriterijus[1], 55 kibernetiniai incidentai buvo priskirti vidutinės reikšmės incidentams, iš kurių pusė (27 incidentai) fiksuoti juridinių asmenų[2] ryšių ir informacinėse sistemose. Taip pat buvo bandoma paveikti valstybinį sektorių (10 incidentų) ir interneto paslaugų tiekėjus (4 incidentai).

Vertinant visus 1780 per pusmetį fiksuotus kibernetinius incidentus, didžiausias pokytis nustatytas įsilaužimų kategorijoje. Per pirmą pusmetį buvo fiksuoti 77 tokio tipo incidentai ir tai yra 129 proc. daugiau, negu tuo pačiu laikotarpiu 2020 m. Šis ryškus įsilaužimų padidėjimas yra susijęs su dviem pagrindinėmis priežastimis – visą pasaulį paveikusia „Microsoft Exchange" elektroninio pašto paslaugos spraga ir Lietuvoje šį pavasarį įvykusiais net keliais stambiais asmens duomenų nutekėjimo atvejais. Nuo kibernetinių įsilaužimų daugiausiai kentėjo informacinių technologijų paslaugas teikiančios įmonės.

Reikšmingiausi pirmojo pusmečio kibernetiniai incidentai Lietuvoje buvo susiję su „Microsoft Exchange" elektroninio pašto paslaugos „nulinės dienos” (angl. *Zero day*) spragos atskleidimu. Metų pradžioje patikrinus 1300 IP adresų, šią spragą Lietuvoje turėjo bent 99 elektroninio pašto tarnybinės stotys, vasarą prisidėjo dar dvi ir rugpjūčio pradžioje šią spragą vis dar turėjo 8 elektroninio pašto tarnybinės stotys.

2021 m. pirmas pusmetis yra išskirtinis ir dėl pasikartojančių asmens duomenų nutekėjimo atvejų („CityBee”, „LIEMSIS”, „Kilobaitas” ir pan.). Jų metu šimtai tūkstančių Lietuvos vartotojų asmens duomenų tapo prieinami piktavaliams.

Riziką taip pat kėlė ir kenkėjišku kodu užkrėstos 186 lietuviško domeno interneto svetainės, apie kurias NKSC buvo informuotas Lietuvos kibernetinio saugumo eksperto. Trys ketvirtadaliai svetainių buvo sutvarkytos, nors metų viduryje dar buvo likę 26 proc. svetainių, kurių valdytojai turi pašalinti kenkėjišką kodą.

[1] Kriterijų, kuriais vadovaujantis kibernetiniai incidentai priskiriami kibernetinių incidentų kategorijoms, sąrašas – https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr
[2] Lietuvoje registruotos įmonės, kurios nepatenka į Kibernetinio saugumo subjektų apibrėžimą

Kaip ir ankstesniais metais, buvo fiksuoti ir informaciniai-kibernetiniai išpuoliai, kurių metu buvo platinamos melagienos. 2021 m. pradžioje buvo fiksuotos paskirstyto atsisakymo aptarnauti atakos prieš nuotolinius mokymus mokyklose, o iki vasario mėn. buvo toliau fiksuojami „Emotet" kenkėjiško kodo platinimo atvejai, kuriuos nutraukė sėkminga tarptautinė teisėsaugos ir teisminių institucijų operacija.[3]

[3] https://policija.lrv.lt/lt/naujienos/tarptautines-operacijos-metu-uzkirstas-kelias-vienos-pavojingiausiu-kenkejisku-programu-emotet-plitimui-visame-pasaulyje

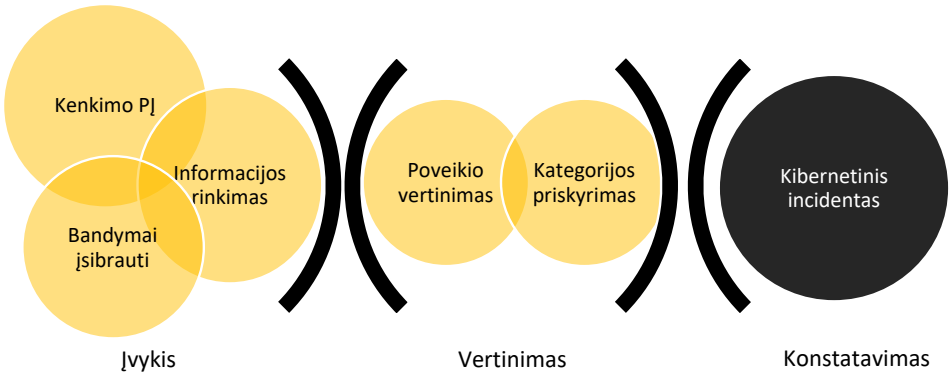
II. CERT-LT FIKSUOTI KIBERNETINIAI INCIDENTAI

1. 2021 m. I pusmetį fiksuoti 1780 kibernetiniai incidentai – 2 proc. daugiau nei 2020 m. tuo pačiu laikotarpiu.

2. Didžiausią grėsmę kėlė „Microsoft Exchange“ paslaugos „nulinės dienos“ spragos atskleidimas ir galimų kibernetinių incidentų identifikavimas.

3. Visuomenėje didžiausią rezonansą kėlė išaugęs asmens duomenų nutekėjimo atvejų skaičius ir vykdomos informacinės-kibernetinės atakos.

NKSC 2021 m. pirmą pusmetį automatinėmis priemonėmis užfiksavo ir apdorojo daugiau kaip 215 000 unikalių Lietuvos IP adresų, susijusių su kibernetiniais įvykiais, t. y. 4 proc. mažiau negu 2020 m. (fiksuota 225 000). Tačiau reikia pažymėti, kad į šią imtį yra įtraukti ir lietuviškų interneto paslaugų teikėjų adresai su kitų šalių IP (Lietuvos paslaugų teikėjai, kurie nuomoja IP adresus kitų šalių subjektams). Vertinant tik lietuviškus IP adresus, fiksuotas 7 proc. didėjimas – 2021 m. fiksuota 136 000 IP, o 2020 m. – 126 000 IP adresų, kurie buvo susisiję su kibernetiniais įvykiais. Apibendrinus – užfiksuotų ir apdorotų įvykių kiekis yra panašus, kaip ir praėjusių metų pirmą pusmetį.



1 pav. Kibernetinio incidento priskyrimo procesas

NKSC Incidentų valdymo padalinys (toliau – CERT-LT) pirmą 2021 m. pusmetį fiksavo 2 proc. didesnį kibernetinių incidentų skaičių, negu tuo pačiu laikotarpiu 2020 m. – iš viso 1780 kibernetinių incidentų (2 pav.).

Nr.	Grupė	Kiekis	Pokytis, palyginus su 2020 m. I pusmečiu
1.	Nepageidaujamų laiškų, klaidinančios informacijos platinimas	94	-26%
2.	Kenkimo PĮ	891	+13%
3.	Informacijos rinkimas (angl. *Phishing*)	510	-8%
4.	Mėginimas įsilaužti	75	-32%
5.	Sėkmingas įsilaužimas	77	+129%
6.	Paslaugų trikdymas (angl. *DDoS*)	25	-56%
7.	Neteisėta veikla, sukčiavimas	58	+9%
8.	Kiti incidentai (individualūs, neatitinkantys nė vienos iš nurodytų grupių aprašymų)	50	+138%
	Iš viso:	1780	+2%

2 pav. Kibernetiniai incidentai 2021 I pusmetį ir pokytis, palyginus su 2020 m. tuo pačiu laikotarpiu

Iš visų 1780 kibernetinių incidentų, vertinant pagal poveikio kriterijus, 55 buvo vidutinės reikšmės kibernetiniai incidentai, iš kurių pusė (49 proc.) fiksuoti juridinių asmenų ryšių ir informacinėse sistemose. Taip pat buvo bandoma paveikti valstybinį sektorių (10 incidentų), interneto paslaugų tiekėjus (4 incidentai) (3 pav.).

Nr.	Grupė	Kiekis
1.	Juridiniai asmenys	27
2.	Valstybės valdymo sektorius	10
3.	Interneto paslaugų teikėjai	4
4.	Prieglobos paslaugų teikėjai	3
5.	Sveikatos priežiūros sektorius	3
6.	Švietimo sektorius	3
7.	Kultūros sektorius	1
8.	Transporto ir pašto sektorius	1
9.	Informacinių technologijų ir elektroninių ryšių sektorius	1
10.	Skaitmeninių paslaugų teikėjas	1
11.	Socialinių paslaugų sektorius	1
	Iš viso:	55

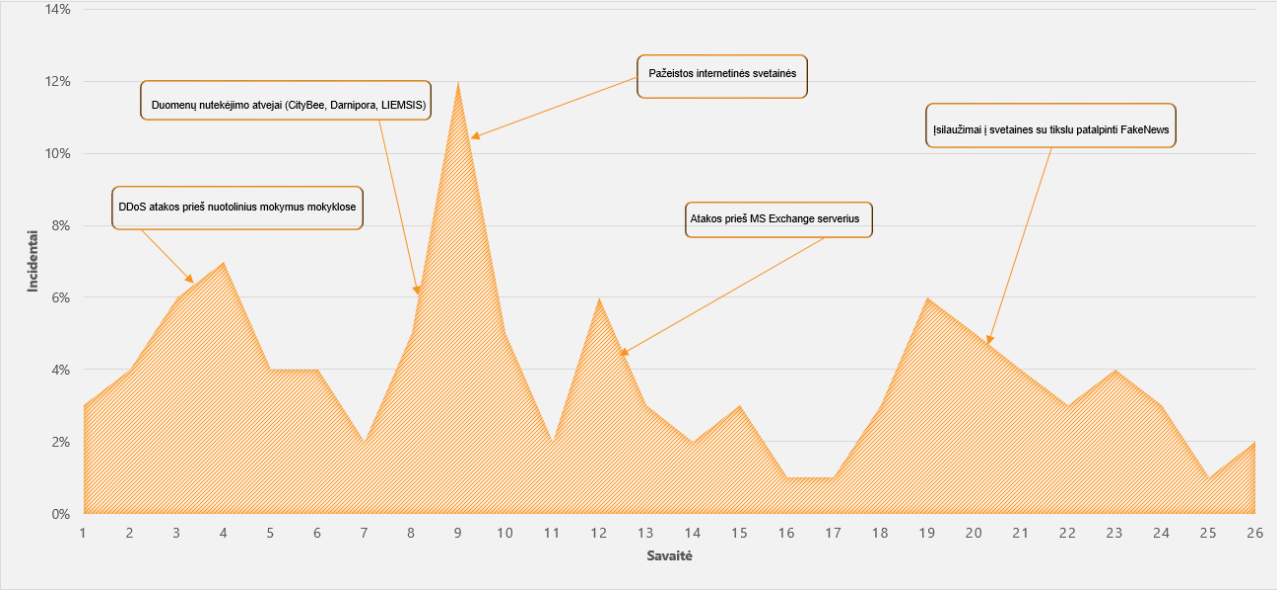
3 pav. Vidutiniai kibernetiniai incidentai pagal sektorius 2021 m. I pusmetį

Didžioji dauguma pirmą pusmetį fiksuotų incidentų buvo nereikšmingo poveikio ir dažniausiai jie buvo fiksuoti prieglobos paslaugų bei interneto paslaugų teikėjų ryšių ir informacinėse sistemose (4 pav.).

Nr.	Grupė	Kiekis
1.	Prieglobos paslaugų teikėjai	736
2.	Interneto paslaugų teikėjai	444
3.	Juridiniai asmenys	120
4.	Fiziniai asmenys	99
5.	Skaitmeninių paslaugų teikėjas	69
6.	Valstybės valdymo sektorius	61
7.	Užsienio subjektai	53
8.	Energetikos sektorius	32
9.	Sveikatos priežiūros sektorius	27
10.	Kiti	84
	Iš viso:	1725

4 pav. Nereikšmingi kibernetiniai incidentai pagal sektorius 2021 m. I pusmetį

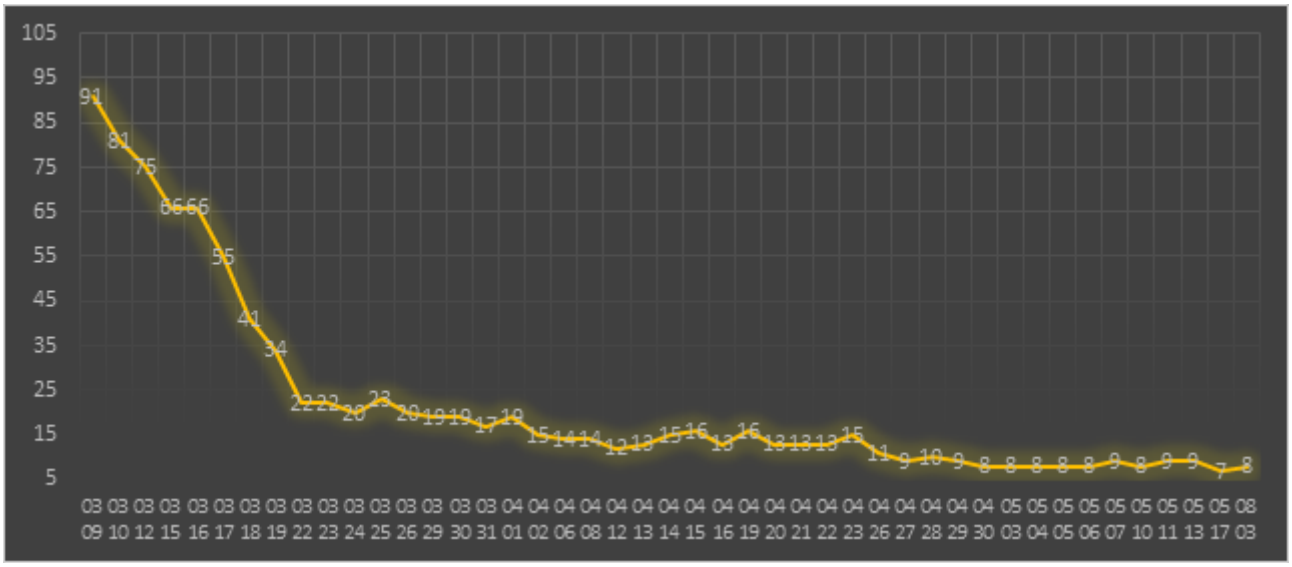
NKSC pažymi, kad 2021 m. pirmą pusmetį eksponentiškai išaugęs sėkmingų įsilaužimų skaičius yra nulemtas „Microsoft Exchange“ elektroninio pašto paslaugos „nulinės dienos” (angl. – *zero day*) spragos identifikavimo ir Lietuvoje šį pavasarį įvykusiais net keliais stambiais asmens duomenų nutekėjimo atvejais.



3 pav. Kibernetiniai incidentai 2021 m. I pusmetį

NKSC specialistai, atsakingi už spragų valdymą, 2021 m. pirmą pusmetį koordinavo „Microsoft Exchange“ elektroninio pašto paslaugos spragos pašalinimą Lietuvos kibernetinio saugumo subjektų ryšių ir informacinėse sistemose (4 pav.). Metų pradžioje patikrinus 1300 IP

adresų, „Microsoft Exchange“ spragą Lietuvoje turėjo bent 99 elektroninio pašto tarnybinės stotys, vasarą prisidėjo dar dvi ir rugpjūčio pradžioje šią spragą vis dar turėjo 8 elektroninio pašto tarnybinės stotys.



4 pav. „Microsoft Exchange“ spragos apimtis iki 2021 m. rugpjūčio 3 d.

2021 m. pirmą pusmetį NKSC fiksavo itin išaugusį asmens duomenų nutekėjimo atvejų skaičių. Pažymėtina, kad tokio tipo incidentų pasitaikydavo ir anksčiau, tačiau išaugęs susidomėjimas naudotojų asmens duomenimis leidžia daryti prielaidą apie augančią Lietuvos naudotojų asmens duomenų vertę. NKSC dalyvavo tiriant duomenų nutekėjimo incidentus, susijusius su „CityBee”, „Darni pora”, „LIEMSIS”, „Kilobaitas” duomenų nutekėjimo atvejais. NKSC vertinimu, dažniausiai prieigos buvo įgautos nerafinuotais metodais, nes nukentėję subjektai netaikė pakankamų rizikos kontrolės priemonių.

Riziką taip pat kėlė ir kenkėjišku kodu užkrėstos 186 lietuviško domeno interneto svetainės, apie kurias NKSC buvo informuotas Lietuvos kibernetinio saugumo eksperto. Kenkėjiško kodo pašalinimą iš interneto svetainių, į kurias patekus iš paieškos sistemų naudotojas būdavo nukreipiamas į kenkėjišką interneto svetainę (angl. *hoax*), NKSC koordinavo su svetainių valdytojais. NKSC pažymi, kad ne visi svetainių savininkai pašalino kenkėjišką kodą iš interneto svetainių – 26 proc. svetainių (49 iš 186) pirmo pusmečio pabaigoje vis dar buvo užkrėstos. Dėl šios priežasties, siekiant apsaugoti vartotojus, NKSC papildomai pagal kompetenciją dar kartą kreipėsi į svetainių savininkus, prieglobos paslaugų teikėjus ir Lietuvos policiją dėl galimai nusikalstamos veikos

vykdymo.

Metų pradžioje buvo stebima paslaugų trikdymo (angl. *DDoS*) kibernetinių atakų tendencija. Dalis tokių išpuolių buvo nukreipta prieš nuotolines pamokas, t. y. sužinojus mokytojų kompiuterių IP adresus prieš juos buvo nukreipiamos atakos, taip sutrikdant nuotolinių pamokų vykdymą. Įvertinus, kad tokio pobūdžio veikla yra vertinama kaip nusikalstama, pagal kompetenciją tokiais atvejais inicijuojamas baudžiamasis persekiojimas, o nustačius tokių atakų vykdytojus – taikoma baudžiamoji atsakomybė.[4]

Iki vasario mėn. buvo toliau fiksuojami 2020 m. pabaigoje prasidėję „Emotet" kenkėjiško kodo platinimo atvejai, kuriuos nutraukė sėkminga tarptautinė teisėsaugos ir teisminių institucijų operacija. Vykdydamos tarptautines koordinuotas priemones visame pasaulyje, teisėsaugos institucijos į savo rankas perėmė kenkėjiškos programinės įrangos infrastruktūros kontrolę ir taip sustabdė masinį kenkėjiško kodo platinimą.[5] NKSC pažymi, kad polimorfinis kenkėjiškas kodas, dėl dažnai besikeičiančių atributų, ir toliau išlieka grėsmę keliančiu kibernetinių incidentų vektoriumi Lietuvos ryšių ir informacinėse sistemose. Iš esmės, tai yra susiję su sąlyginai ribotų kibernetinio saugumo subjektų gebėjimų greitai ir efektyviai aptikti tokio tipo kenkėjišką kodą.

2021 m. buvo ir toliau stebimas netikrų naujienų platinimas, naudojant kibernetinių incidentų elementus – imituojant interneto svetaines, vykdant įsilaužimus. Tokių kibernetinių-informacinių atakų metu siekiama suklaidinti interneto vartotojus, diskredituoti ir paveikti strateginius procesus ar tarptautinius santykius. Pažymėtina, kad kibernetinių-informacinių operacijų veikla neapsiriboja Lietuvos valstybės teritorija.[6] NKSC savo ruožtu 2021 m. fiksavo informacines atakas, nukreiptas ir išimtinai prieš Lietuvoje vykstančius procesus – Galimybių pasą. Pažymėtina, kad kibernetinio incidento poveikio šiuo konkrečiu atveju nebuvo nustatyta ir imituotų Galimybių paso interneto svetainių sklaida buvo ribota. NKSC vertinimu, melagienų platinimas išnaudojant kibernetinių incidentų elementus 2021 m. toliau kartosis.

[4] https://www.etaplius.lt/hakeris-is-alytaus-bausmes-isvenge-tik-per-plauka
[5] https://policija.lrv.lt/lt/naujienos/tarptautines-operacijos-metu-uzkirstas-kelias-vienos-pavojingiausiu-kenkejisku-programu-emotet-plitimui-visame-pasaulyje
[6] https://www.fireeye.com/blog/threat-research/2021/04/espionage-group-unc1151-likely-conducts-ghostwriter-influence-activity.html

2.1 CERT-LT KIBERNETINIŲ INCIDENTŲ TYRIMAI IR ANALIZĖS

2.1.1 „CityBee“ duomenų nutekėjimas

2021 m. vasario 15 dieną internetiniame forume su ribota prieiga paskelbiami „CityBee“ vartotojų duomenys: elektroninio pašto adresas, slaptažodžio SHA-1 kontrolinė suma, vardas, pavardė ir asmens kodas. Naktį iš vasario 15 d. į 16 d. tame pačiame internetiniame forume patalpinamas įrašas apie turimus papildomus duomenis, tai yra pilną „CityBee“ duomenų bazę, įskaitant: vairuotojo pažymėjimo numerius, gyvenamosios vietos adresus, tel. numerius. NKSC, atlikęs kibernetinio incidento tyrimą, nustatė šias aplinkybes:

- Tarp nutekintų 110 tūkst. „CityBee“ klientų duomenų taip pat buvo jų paskyrų slaptažodžiai, kurie buvo saugomi užkoduoti nesaugiu SHA-1 algoritmu be papildomų saugumo priemonių (angl. *Salt*).
- Klientų asmens kodai buvo saugomi atviru tekstu (angl. *Plaintext*)
- Iš pateiktų duomenų negalima nustatyti kuriuo laiku tiksliai buvo pasisavinta „CityBee“ klientų rezervinė duomenų bazė. Taip pat neįmanoma nustatyti, kada tiksliai buvo užkardytas pažeidžiamumas.

2.1.2 „Vatesl.lt“ puslapio kopija

2021 m. kovo 17 dieną NKSC aptiko užregistruotą domeną – *vatesl.lt*, kurio tikslas buvo imituoti tikrąją Valstybinės atominės energetikos saugos inspekcijos (toliau – VATESI) svetainę *vatesi.lt*. Suklastotoje svetainėje buvo patalpinta tikrovės neatitinkanti informacija. Beveik tuo pačiu metu įvykdytas įsilaužimas ir į Lenkijos nacionalinės atominės energijos agentūros svetainę *paa.gov.pl.* Šioje svetainėje taip pat buvo patalpinta tikrovės neatitinkanti informacija, kurioje buvo cituojama melagiena iš netikros *vatesl.lt* interneto svetainės. Tikrovės neatitinkanti informacija toliau sklido per Lenkijos interneto svetainę *www.zdrowie.gov.pl,* kur buvo pateikiamos nuorodos į *vatesl.lt* ir *paa.gov.pl* įkeltas melagienas. Melagienos platinimui taip pat buvo pasitelkti socialiniai tinklai ir galimai užvaldytos su energetika susijusių Lenkijos pareigūnų socialinių tinklų *„Facebook“* ir *„Twitter“* paskyros.

NKSC nustatytos kibernetinio incidento aplinkybės perduotos Lenkijos atstovams.

2.1.3 Vilniaus kolegijos studentų duomenų nutekėjimo atvejis

2021 m. kovo 11 dieną internetiniame forume su ribota prieiga buvo paskelbti Vilniaus kolegijos studentų asmens duomenys: vardas, pavardė, lytis, asmens kodas, namų adresas, miestas, mokykla, mokyklos baigimo metai, gimimo data, tautybė, studijų kryptis, studijų programos kodas, studijų pradžios data, studijų baigimo data, fakultetas ir mokslo įsitaigos pavadinimas. Kažkuriuo momentu anksčiau šie duomenys buvo neteisėtai pasisavinti, pavogti ar prieiga prie jų gauta įvykdžius kibernetinį incidentą. Forume taip pat skelbiama, kad piktavalis turi ir kitų švietimo įstaigų duomenų, susijusių su *www.liemsis.lt* informacine sistema.

NKSC, atlikęs kibernetinio incidento tyrimą, nustatė šias aplinkybes:

- Neteisėtas Vilniaus kolegijos studentų asmens duomenų pasisavinimas galimai įvyko dėl neapribotos ir internetu pasiekiamos sistemos prieigos ir netinkamai organizuoto *www.liemsis.lt* kibernetinio saugumo. Tyrimo metu buvo identifikuota, kad incidento priežastis taip pat galėjo būti neapribotos prieigos prie kitų internetu pasiekiamų informacinių išteklių.
- Iš tyrimo metu disponuotos ribotos informacijos nebuvo galima nustatyti, kada tiksliai ir iš kokios sistemos buvo pasisavinta Vilniaus kolegijos studentų duomenų bazė. To nebuvo galima padaryti dėl nekontroliuojamo aukštųjų mokyklų informacinių išteklių išsiplėtimo (angl. *System sprawl*).
- Nustatytas galimai netinkamas asmens duomenų tvarkymas. Tarp nutekintų 7 tūkst. Vilniaus kolegijos studentų duomenų buvę asmens kodai buvo saugomi atviru tekstu (angl. *Plaintext*).

2.1.4 Kenkėjišku programiniu kodu užkrėstos svetainės

2021 m. kovo mėn. iš fizinio asmens buvo gauta informacija, apie 186 Lietuvos IP rėžyje patalpintas **.lt* domeno svetaines, kurios buvo užkrėstos kenkėjišku programiniu kodu. Patikrinus gautą informaciją buvo nustatyta, kad svetainių lankytojai gali būti nukreipiami į kitas prastos reputacijos svetaines, kuriose vykdoma galimai nusikalstama veika: bandoma išvilioti lankytojų prisijungimo, mokėjimo kortelių, kitus duomenis, apkrėsti kenkėjišku programiniu kodu lankytojų įrenginius, svetainių lankytojai raginami dalyvauti įvairiose loterijose, kurias neva organizuoja „Google“, „Apple“, „Samsung“ ar kitos žinomos kompanijos.

Siekiant apsaugoti svetainių lankytojus, ši informacija raštu buvo perduota prieglobos paslaugų teikėjams ir rekomenduota imtis priemonių, kurios leistų užkardyti kibernetinių incidentų šaltinius:

1. susisiekti su atsakingais asmenimis, kurių vardu yra naudojamos paslaugos ir juos informuoti apie jų svetainių dalyvavimą kenkėjiškoje ir galimai nusikalstamoje veikoje;
2. paslaugų savininkams nesiėmus veiksmų – apriboti teikiamas paslaugas vartotojams iki kol nebus pašalintas svetainėse esantis kenkėjiška programinis kodas;
3. iki 2021 m. kovo 18 d. pabaigos informuoti NKSC apie atliktus veiksmus pašalinant kenkėjišką kodą.

2021 m. kovo 22-23 d. atlikus svetainių pakartotinį patikrinimą, buvo nustatyta, kad 84 svetainės vis dar užkrėstos kenkėjišku programiniu kodu ir dalyvauja kenkėjiškoje veikloje. Vadovaudamiesi Lietuvos Respublikos kibernetinio saugumo įstatymo 14 str. („Tarpinstitucinis bendradarbiavimas tiriant kibernetinius incidentus“) informacija apie pastaruoju metu užfiksuotus tęstinius kibernetinius incidentus, kuriuose dalyvaujantys prieglobos paslaugų naudotojai ar tokiems naudotojams paslaugas teikiantys prieglobos paslaugų teikėjai buvo informuoti, apie tai, kad sukelia kibernetinius incidentus bei juose dalyvauja, tačiau nesiėmė priemonių šių incidentų priežastims pašalinti, buvo perduota Lietuvos kriminalinės policijos biuro Sunkaus ir organizuoto nusikalstamumo tyrimo 5-ajai valdybai (toliau - Policija). Bendradarbiaujant su Policija pavyko uždaryti ar priversti didžiąją daugumą prieglobos paslaugų naudotojus (svetainių savininkus) pašalinti kenkėjišką programinį kodą.