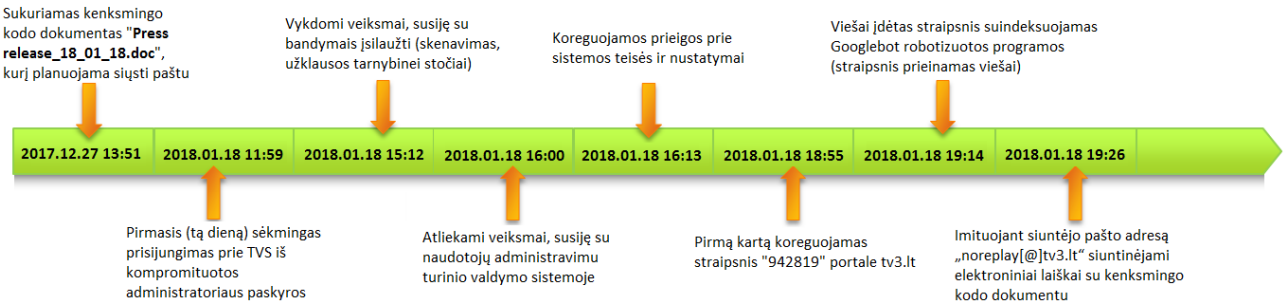
NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
PRIE KRAŠTO APSAUGOS MINISTERIJOS

SUTRUMPINTAS PRANEŠIMAS APIE KIBERNETINIO INCIDENTO TYRIMĄ NR. 152827

2018 m. sausio 29 d.

TLP: WHITE

Kibernetinio incidento tyrimo objektas: 2018 m. sausio 18 d. įsilaužimas į interneto svetainę www.tv3[.]lt, šmeižiančios informacijos paskelbimas ir laiškų su kenksmingu kodu siuntimas tikslinei gavėjų grupei.



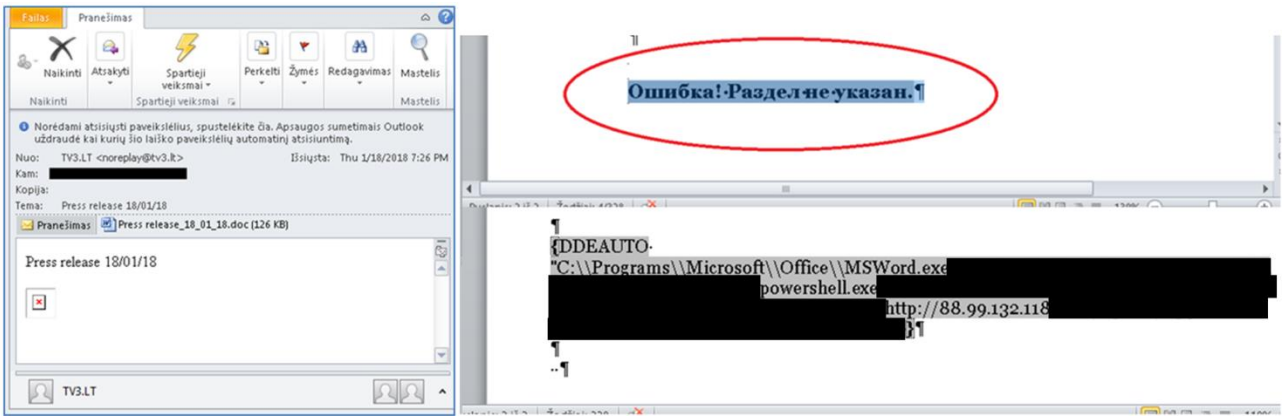
Įvykių laiko juosta

Tyrimo metu nustatyta, kad pasinaudojant tv3.lt svetainės turinio valdymo sistema (TVS) ir užvaldžius administratoriaus paskyrą buvo paskelbtas suklastotas straipsnis. Remiantis tv3.lt specialistų pateiktų tarnybinės stoties ir TVS žurnalų įrašų (angl. *Logs*) informacija, nustatyta, kad prisijungimas prie svetainės ir straipsnio koregavimas buvo įvykdytas naudojantis TOR tinklo paslaugomis. Nustatyti išeities mazgų loginiai IP adresai, kurie buvo naudojami įsilaužimo metu, siejami su užsienio valstybių finansuojamos grupuotės veikla internete.

2018 m. sausio 18 d. 19.26 val. imituojant siuntėjo pašto adresą **noreplay[@]tv3.lt** tikslinei auditorijai išsiunčiami elektroniniai laiškai su priedu, kuriame įterptas kenksmingas kodas. Tikslinė gavėjų auditorija apėmė svarbių Lietuvos valstybės institucijų ir spaudos atstovus, politikus.

Patikrinus laiško techninę antraštę (angl. *header*) nustatyta, kad laiškas siųstas iš IP adreso **103.36.109[.]248**. Siuntimo adresas imituojamas siekiant apsimesti tikru tv3.lt svetainės naujienų prenumeratos el. pašto adresu (noreply@tv3.lt). Laiško turinyje įterptas paveiksliukas, kreipiniai į kurį gali būti stebimi siuntėjų (siekiant sužinoti, kas atsidaro atsiųstus laiškus). Prie laiško prisegtas priedas pavadinimu **Press release_18_01_18.doc** (pav.).

Laiško priedo **Press release_18_01_18.doc** turinyje pateikiama suklastota informacija apie Lietuvos Respublikos krašto apsaugos ministrą Raimundą Karoblį su nuorodomis į straipsnį portale. Dokumente taip pat įterptas automatizuotas kenksmingas kodas (*powershell* komanda), kuris kreipiasi į tarnybinę stotį internete (**88.99.132[.]118**) norėdamas atsisiųsti papildomą kenksmingą kodą. Kenksmingas kodas turėtų būti atsiunčiamas išnaudojant „Microsoft Office“ programos funkcionalumą „Dinamiškas apsikeitimas duomenimis“ (angl. Dynamic Data Exchange) (DDE), taip gaunami duomenys iš kitų resursų kompiuteryje arba tinkle. Kenksmingas kodas įterptas į paslėptą duomenų laukelį, kurio aprašyme taip pat rodomas klaidos pranešimas, pateikiamas rusiško raidyno (kirilicos) simboliais, todėl galima daryti prielaidą, kad šiam dokumentui kurti buvo naudojama rusiška „Microsoft Word“ programinės įrangos versija (pav.).



Pav. El. laiškas ir jo priede įterpta kenksmingo kodo komanda

Išvados:

1. Į interneto svetainę TV3.lt buvo įsilaužta pasinaudojant užvaldyta administratoriaus paskyra. Kadangi buvo aptikta ir ankstesnių nesankcionuotų prisijungimų prie tarnybinės stoties, manoma, kad jos prisijungimo duomenys buvo perimti daug anksčiau, negu įvykdytas pats įsilaužimas.
2. Pasinaudojant suklastota „sensacinga informacija“ tikslingai išplatinami laiškai su kenksmingu kodu, kuris, patekęs į sistemą, galėtų ją išnaudoti (pvz.: suteikti įsibrovėliams prieigą prie joje saugomų dokumentų, sudarytų sąlygas sekti naudotojų veiklą).

Rekomendacijos:

1. Siekiant apsaugoti viešai prieinamas sistemas nuo įsibrovimų, būtina reguliariai atnaujinti tarnybinėse stotyse naudojamą programinę įrangą, apriboti prieigą prie administravimo sąsajos (pvz., prieigos kontrolės sąrašais), naudoti papildomas apsaugos priemones (pvz., tinklo programų užkardą), griežtai kontroliuoti administravimo teises turinčias paskyras, naudoti sudėtingus ir reguliariai keičiamus prieigos slaptažodžius, reguliariai atlikti prisijungimų žurnalo įrašų (angl. *Logs*) auditą.
2. Siekiant apsisaugoti nuo laiškų su kenksmingo kodo priedais, organizacijoms rekomenduojama naudoti elektroninio pašto apsaugos ir filtravimo programinę įrangą. Naudotojų darbo stotyse siūloma išjungti pagal nutylėjimą veikiančius nereikalingus programų funkcionalumo nustatymus (pvz.: makrokomandos, automatinis nuorodų atnaujinimas atidarius dokumentą (angl. *Update automatic links at open*) ir pan.). Apriboti *powershell* veikimą naudotojo lygmeniu. Saugantis nuo programinių pažeidžiamumų išnaudojimo, būtina kuo dažniau atnaujinti darbo stotyse naudojamą programinę įrangą (operacines sistemas, naršykles, biuro ir elektroninio pašto, .pdf dokumentus atidarančias programas).
3. Kadangi dažniausiai naudotojams apgauti naudojami socialinės inžinerijos principai (stengiamasi sudominti, išgąsdinti ar manipuliuoti kitomis emocijomis), itin svarbus nuolatinis darbuotojų sąmoningumo ugdymas: švietimas supažindinant su galimomis grėsmėmis, kibernetinio saugumo pratybų organizavimas, rekomendacijos, kaip elgtis su įtartinais laiškais ar dokumentais.

Grėsmių indikatoriai (kurių galite ieškoti savo tinkle), susiję su šiuo incidentu:

noreplay[@]tv3.lt

Tipas	Data	Grėsmės lygis
El. p.	**2018-01-18** Aprašymas Suklastotas el. pašto adresas, kurio vardu buvo išsiųstas elektroninis laiškas su kenksmingą programinį kodą turinčiu priedu.	Žemas (2/5) Indikatoriaus patikimumas (100/100)

103.36.109[.]248

Tipas	Data	Grėsmės lygis
IP	**2018-01-18** Aprašymas IP adresas, iš kurio buvo išsiųstas elektroninis laiškas su kenksmingą programinį kodą turinčiu priedu.	Vidutinis (3/5) Indikatoriaus patikimumas (90/100)

6BD52A05E1EB703D34B6BCB7F05673A4

Tipas	Data	Grėsmės lygis
Hash	**2018-01-18** Aprašymas Failo **Press_release_18_01_18.doc** md5 kontrolinė suma.	Vidutinis (4/5) Indikatoriaus patikimumas (100/100)

88.99.132[.]118

Tipas	Data	Grėsmės lygis
IP	**2018-01-18** Aprašymas IP adresas, iš kurio atsisiunčiama papildoma kenksmingo kodo dalis atidarius **Press_release_18_01_18.doc** dokumentą.	Vidutinis (3/5) Indikatoriaus patikimumas (90/100)