# CERT-LT pakartotinai informuoja Lietuvos vartotojus, kaip apsisaugoti nuo sparčiai visame pasaulyje plintančio viruso „WannaCry“

Lietuvos Respublikos ryšių reguliavimo tarnybos (RRT) nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) prašo interneto vartotojus būti atsargius ir imtis priemonių, apsaugančių nuo kompiuteriuose su „Windows“ operacinėmis sistemomis sparčiai plintančio išpirkos reikalaujančio viruso „WannCry“, kuris jau palietė daugiau kaip 200 000 kompiuterių visame pasaulyje.

Kaip įprasta šio tipo kenkimo programoms, „WannaCry“ virusas pradžioje atkeliauja el. laišku. Vartotojas, gavęs laišką su užkratu, yra įtikinėjamas atidaryti kartu prisegtą bylą (angl. file). Ją atidarius, kenkimo programa užrakina kompiuteryje esančias bylas ir prašo sumokėti išpirką elektronine valiuta bitkoinais, jei norima jas atgauti.

Apkrėtęs vieną kompiuterį, virusas toliau plinta tiek vietiniame, tiek pasauliniame tinkle (išnaudodamas SMB protokolo spragą, TCP prievadu 445).

**RRT teikia atnaujintas rekomendacijas interneto vartotojams, kokių veiksmų jie turėtų imtis:**

***Atnaujinti savo „Windows“ operacinę sistemą iki naujausios versijos. Gamintojų pataisą rasite čia – MS17-010.** Plačiau: http://www.esaugumas.lt/lt/windows-vartotojams/sistemos-atnaujinimas.html.

* Senesnių „Windows“ operacinių sistemų („Windows XP“, „Windows 8“ ir „Windows Server 2003“), kuriems automatiniai atnaujinimai nebėra siunčiami, naudotojams būtina įdiegti specialią pataisą, kurią rasite adresu https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/.

*Pažeidžiamose sistemose, kuriose nėra galimybės įdiegti jokių pataisų, turėtų būti išjungtas SMBv1 palaikymas. Kaip tai padaryti, skaitykite šioje nuorodoje: https://support.microsoft.com/en-us/help/2696547.

* Izoliuoti komunikaciją organizacijų tinkluose TCP prievadu 445.

* Jeigu aukščiau išvardytų priemonių pritaikyti pažeidžiamoms sistemoms galimybės nėra, prietaisus patariame išjungti, kol tokia galimybė atsiras.

CERT-LT primena, kad antivirusų programinės įrangos kūrėjai nuolat atnaujina jų kuriamų apsaugos priemonių galimybes, todėl antivirusinių programų atnaujinimas kompiuteryje taip pat padėtų apsisaugoti nuo pavojų, ir atkreipia kompiuterių naudotojų dėmesį, kad svarbių

duomenų kopijos atskirose laikmenose yra geriausias būdas išsaugoti savo informaciją netikėtiems atvejams. Jeigu sistema jau pažeista, o atsarginių duomenų kopijų nėra, prieš išvalant sistemą, patariama išsaugoti apkrėstas bylas, nes ateityje gali būti išleistas viešas raktas byloms atrakinti. Tokios garantijos vis tik nėra, kaip ir nėra garantijos, jog atgausite savo duomenis, sumokėję išpirką.

Nuolat atnaujinamą informaciją rasite CERT-LT svetainėje:

https://www.cert.lt/naujienos/didziausia_istorijoje_ransomware_ataka_plinta_wind.html

Apie CERT-LT

CERT-LT – Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys, kurio misija yra užtikrinti elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimus, koordinuoti veiksmus stabdant incidentų plitimą ir vykdyti incidentų prevenciją. CERT-LT koordinuoja ir įgyvendina IT sprendimus, susijusius su tinklų ir informacijos saugumu, atlieka prevencinę veiklą, teikdamas informaciją apie naujausias grėsmes kompiuterių naudotojams. Informacija skelbiama specializuotose svetainėse www.cert.lt ir www.esaugumas.lt, kuriose kompiuterių naudotojams taip pat pateikiamos rekomendacijos ir įspėjimai, kaip išvengti didesnių pavojų. Sprendžiant tarptautinius incidentus, CERT-LT bendradarbiauja su kitose valstybėse dirbančiais CERT padaliniais. CERT-LT yra visateisis „Trusted Introducer“ ir FIRST (angl. Forum of Incident Response and Security Teams) organizacijų narys.