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

INFORMACINIS BIULETENIS
DUOMENIS ŠIFRUOJANTIS IR IŠPIRKOS REIKALAUJANTIS KENKĖJIŠKAS KODAS (ANGL. RANSOMWARE)

2021 m. lapkričio 5 d.
Vilnius

Duomenis šifruojantis ir išpirkos reikalaujantis kenkėjiškas programinis kodas (angl. *ransomware*) yra plačiai paplitęs kenkėjiško programinio kodo tipas, kurio pagrindinis tikslas yra užkoduoti įrenginyje esančius duomenis ar sistemas, už kurių iššifravimą vėliau yra prašoma išpirkos. Programišių, naudojančių šio tipo kenkėjišką programinį kodą, taikiniai yra įvairūs – nuo namų naudotojų iki ypatingos svarbos paslaugas teikiančių organizacijų. Šio informacinio biuletenio tikslas supažindinti naudotojus su pagrindiniais tokio tipo kibernetinių incidentų vektoriais bei apsisaugojimo būdais.

I. Kas yra duomenis šifruojantis ir išpirkos reikalaujantis kenkėjiškas programinis kodas?

Išpirkos reikalaujantis kenkėjiškas programinis kodas dažniausiai būna dviejų tipų: užkoduojantis įrenginyje esančius duomenis arba užkoduojantis sistemas. Abiem atvejais įrenginyje esantys duomenys yra nepasiekiami, kol nėra gaunamas specialus iššifravimo raktas. Dažnu atveju nusikaltėliai prieš užkoduodami įrenginyje esančią informaciją, ją dar ir pasisavina. Taip pat yra kenkėjiško kodo variantų, kurie išnaudodami „plokščią" tinklo architektūrą išplinta ir į kitus tinkle esančius įrenginius.[1] Po sėkmingos atakos sistemos naudotojas įrenginyje randa detalią instrukciją, kokiu būdu ir kiek sumokėjus gali tariamai atgauti prarastus duomenis ar sistemų kontrolę. Pažymėtina, kad išpirkos sumokėjimas negarantuoja prieigos prie informacijos atgavimo. Tikėtina, kad išpirką sumokėję asmenys ar subjektai vėliau vėl bus atakuojami programišių.

II. Pagrindiniai atakos vektoriai

Dauguma duomenų užkodavimo ir išpirkos reikalavimo atakų yra vykdomos automatizuotų procesų pagalba. Kertinis šių atakų tikslas yra gauti pirminę prieigą prie vidinių tinklų. Pagrindiniai nusikaltėlių naudojami būdai šiai prieigai gauti:

1. Atvirų nuotolinių prieigų prie sistemų paieška

1.1. Atliekama masinė perimetro žvalgybos kampanija, kurios metu aptinkami iš išorės pasiekiami nuotolinės prieigos taškai (pvz., atvirai pasiekiami RDP prievadai);
1.2. Vykdoma slaptažodžių parinkimo (angl. *brute force*) ataka prieš pasirinktą nuotolinę prieigą;
1.3. Vykdomos prisijungimų informacijos vagystės, naudojantis socialinės inžinerijos metodais. (angl. *phishing*). Šių kibernetinių atakų metu siunčiami specialiai sukurti el. laiškai įmonės darbuotojams, kurie galimai turi prieigą prie nusikaltėliams dominančių sistemų, bandant išvilioti prisijungimo duomenis.

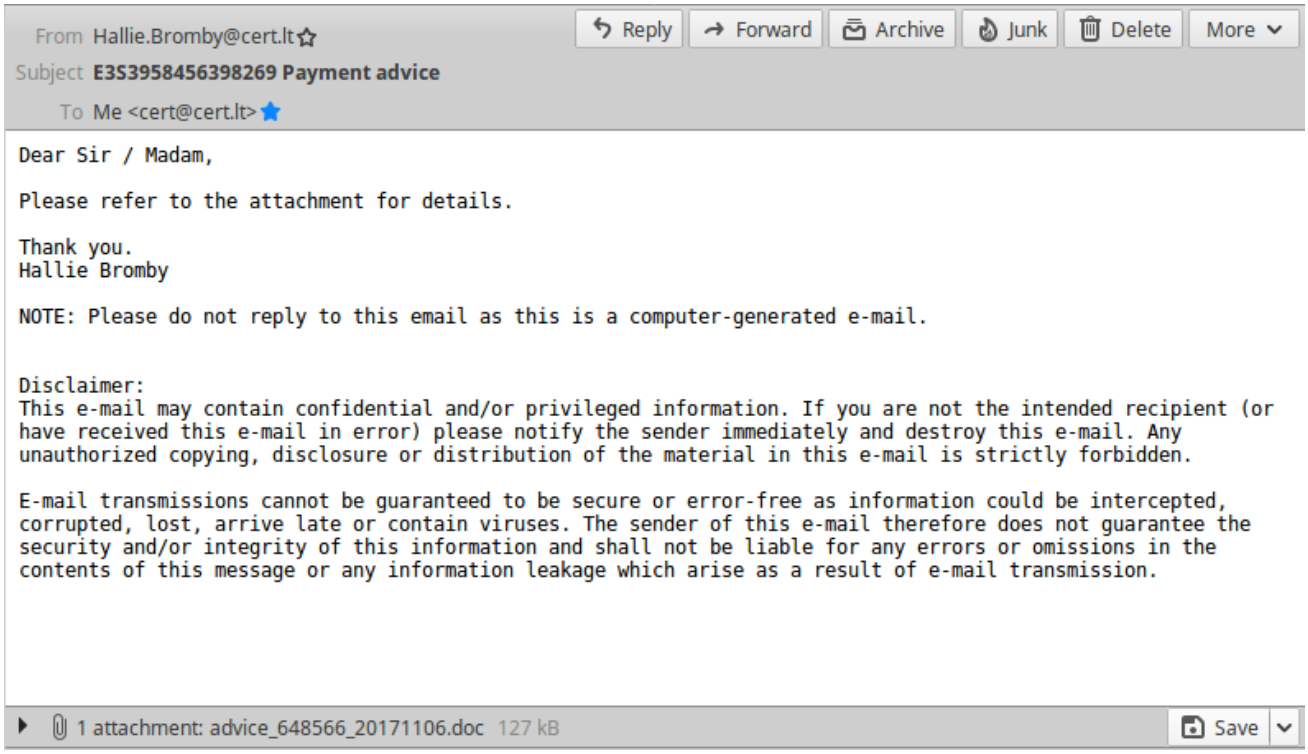
[1] „Plokščia" tinklo architektūra laikomas į atskirus potinklius nesegmentuotas tinklas, kuriame programišiai gali iš darbo stočių pasiekti tinklo įrenginius, tarnybines stotis ir kitus informacinius išteklius.

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

2. Siunčiami el. laiškai su pridėtu kenkėjišku prisegtuku

2.1. El. paštu dažniausiai būna siunčiami laiškai imituojantys realias organizacijas, pvz., siunčiamos sąskaitos už neva atliktus darbus ir pan. Laiškuose būna prikabintas failas (galimi įvairus plėtiniai), tačiau dažniausiai pasitaiko *Microsoft Office* dokumentai (pvz., *.docx, .xlsx*) su paslėptomis *macros* komandomis iki vykdomųjų failų, kurie užmaskuojami nešiojamų dokumentų formatu (angl. Portable Document File – .pdf), arba yra įtraukiami į archyvus su slaptažodžiais (1 pav.).

2.2. Atidarius tokio pobūdžio prisegtukus ir įgalinus *macros* komandas *Microsoft Office* programose yra paleidžiamas vykdomasis kodas, kuris pagal savo specifiką vykdo komandas leidžiančias įgauti pirminę įrenginio kontrolę.



1 pav. Galimo el. laiško su žalingu prisegtuku pavyzdys

3. Siunčiami el. laiškai su žalingomis nuorodomis

3.1. El. paštu taip pat būna siunčiami laiškai su nuorodomis į užvaldytas arba specialiai sukurtas interneto svetaines, kurioje būna patalpintas kenkėjiškas kodas;

3.2. Paspaudus nuorodą naudotojas parsisiunčia failą į savo įrenginį – tokiu būdu yra apeinamos el. pašto saugumo priemonės;

3.3. Naudotojui atidarius kenkėjišką prisegtuką būna paleidžiamas vykdomasis kodas, kuris pagal savo specifiką vykdo komandas, leidžiančias gauti priminę įrenginio kontrolę.

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

III. Prevenciniai būdai apsisaugojimo būdai

Ransomware atakų pasekmės dažniausiai būna vienodos – apribota prieiga prie duomenų arba sistemų. Dėl šios priežasties ypatingai svarbu prevenciškai daryti ir saugoti aktualias atsargines duomenų kopijas (angl. *backup*), laikant jas atskirtas nuo tinklo (aktualu naudotojams ir organizacijoms). Pažymėtina, kad svarbu ne tik kaupti, bet ir reguliariai pasitikrinti, jog duomenis įmanoma atstatyti iš atsarginių kopijų.

1. Rekomendacijos naudotojams

1.1. Dažniausiai naudotojų įrenginiai būna užšifruojami pasinaudojus nesaugiomis nuotolinėmis prieigomis, todėl svarbu apriboti išorinio prisijungimo galimybes tokiais protokolais kaip *Windows Remote Desktop Protocol*, daiktų interneto *SSH* prievadais ir pan.;
1.2. Prie maršrutizatorių leistis jungtis tik iš žinomų IP adresų (angl. *allow list*) arba prisijungimui naudoti virtualaus privataus tinklo technologijas (angl. *virtual private network*, VPN);
1.3. Naudoti legalią programinę įrangą, nuolat diegti atnaujinimus;
1.4. Turimuose įrenginiuose įsidiegti antivirusinę programinę įrangą;
1.5. Kritiškai vertinti gaunamus įtartinus el. laiškus su prisegtukais, nuorodomis bei pasiūlymais;
1.6. Atidarytuose *Microsoft Office* dokumentuose neįgalinti *macros* komandų, nebent būnant įsitikinus siuntėjo patikimumu ir tokių komandų būtinumu;
1.7. Periodiškai daryti svarbiausių dokumentų ir duomenų kopijas, saugoti jas į tinklą nepajungtuose įrenginiuose ar laikmenose.

2. Organizacijoms

2.1. Užtikrinti, jog sistemos, įrenginių operacinės sistemos, ypatingai, pasiekiamos iš išorės, ir naudojama programinė įranga būtų reguliariai atnaujinama iki naujausios gamintojo siūlomos versijos;
2.2. Reguliariai atlikti pažeidžiamumų patikrą įrenginiams net tik pasiekiamiems iš išorės, bet iš vidinių tinklų;
2.3. Užtikrinti, jog išoriniai įrenginiai būtų tinkamai sukonfigūruoti (išjungti nenaudojami prievadai, protokolai (*TELNET, SSH, RDP, SMB* ir pan.) ir pasenusios jų versijos) ir įjungti turimi saugumo nustatymai;
2.4. Leisti prieiga tik iš žinomų IP adresų arba prisijungimui naudoti virtualų privatų tinklą;
2.5. Audituoti tinklo įrenginius, naudojančius nuotolinę prieigą ir centralizuotai kaupti prisijungimų žurnalinius įrašus;
2.6. Įgalinti paskyrų blokavimą po 3-5 nesėkmingų bandymų prisijungti;
2.7. Nenaudoti tų pačių slaptažodžių skirtingoms paskyroms;
2.8. Naudoti kelių faktorių autentifikavimą (el. pašto internetiniai prieigai, VPN prieigai, paskyroms kurios turi prieigą prie kritiškai svarbių sistemų);
2.9. Įdiegti el. pašto filtravimo mechanizmus, gebančius filtruoti laiškus pagal žinomus grėsmių indikatorius ir specifinius raktažodžius;
2.10. Blokuoti el. laiškais siunčiamus specifinių plėtinių, galinčius vykdyti komandas, prisegtukus;
2.11. Mažinti galimybes darbuotojams gauti ir patiems būti suklastotiems (angl. *spoofed*). Siunčiant el. laiškus, taikyti papildomas el. pašto saugumo priemones, tokias kaip siuntėjo politikos nustatymas (angl. *sender policy framework, SPF*), domeno apsaugos (angl. *domainkeys identified mail, DKIM*) ir el. pašto autentifikavimo mechanizmo (angl. *message authentication, reporting and conformance, DMARC*);
2.12. Apsvarstyti *macros* išjungimą *Microsoft Office* dokumentuose siunčiamuose el. laiškais;
2.13. Nuolatos vykdyti budrumo, įtartinų laiškų ir anomalijų atpažinimo mokymus darbuotojams (angl. *awareness training*)
2.14. Užtikrinti, jog antivirusinė ir kita saugumo programinė įranga ir kenkėjiško kodo aprašų duomenų bazė būtų nuolatos automatiškai atnaujinama (ne rečiau kaip kartą per parą);
2.15. Įrenginiuose įgalinti leistinos programinės įrangos autorizaciją, kurią galimą įgalinti naudojant *Microsoft Software Restriction Policy* arba *AppLocker* funkcionalumus;
2.16. Leisti programas vykdyti tik iš specifinių katalogų tokių kaip: PROGRAMFILES, PROGRAMFILES(x86), SYSTEM32 arba kitų žinomų vietų;
2.17. Uždrausti darbuotojams savarankiškai diegti programinę įrangą į organizacijos įrenginius;

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

2.18. Įvertinti trečiųjų šalių teikiamų paslaugų riziką ir naudojamas saugumo priemones ir kontroles, nes nekontroliuojamos trečiųjų šalių teikiamos paslaugos taip pat gali būtų atakos vektoriumi;

2.19. Įdiegti kontrolės ir stebėsenos mechanizmus prisijungimams iš tariamai patikimų trečiųjų šalių infrastruktūros;

2.20. Darbuotojams priskirti tik darbo funkcijoms vykdyti reikalingas teises;

2.21. Periodiškai audituoti esamas paskyras ir jų turimas teises;

2.22. Įdiegti tinklo segmentavimą, atskiriant organizacijos išorinius, vidinius ir technologinius tinklus, resursus ir paslaugas;

2.23. Darbuotojams apriboti galimybę naudotis *Microsoft Windows* operacinių sistemų administravimui skirtu *PowerShell* komponentu. Taip pat įgalinti papildomą *Powershell* kodo blokų (angl. *script block*) auditavimą;

2.24. Naudoti tik ne senesnę nei *Powershell 5.0* versiją, senesnes versijas išdiegti.