Laboratorinis darbas Nr.4

# Kenkėjiškos programos tyrimas

Darbo tikslas – susipažinti su paprastos kenkėjiškos programos aptikimu ir išvalymu, kompiuteryje su Windows XP operacine sistema.

**Laboratorinio darbo užduotis**

1. Įjunkite virtualų kompiuterį su Windows XP naudotą trečiajame laboratoriniame darbe. Patikrinkite tinklo nustatymus. Išjunkite Windos ugniasienę: Control Panel/Fireweall/Disable…
2. Sukurkite C diske katalogą pavadinimu **Malware**, o jame katalogą pavadintą savo varianto numeriu **XX**. Padarykite ta kataloga prieinamą tinkle (share) su galimybe į jį rašyti.
3. Viešai prieinamas turetų būti tik šis katalogas, patikrinkite ar nesidalinate kitais: **Start**, ant **My Computer** spauskite dešinį pelės klavišą, pasirinkite **Manage**, ten **Shared Folders** ir **Shares**. Naujai sukurtas katalogas turetų būti vienintelis be **$** zenklo pabaigoje. Jei dalinatės ir kitais nesisteminiais katalogais, nutraukite dalinimasi jais. Paruošę katalogą praneškite dėstytojui.
4. Kenkėjiškos programos pavyzdys, registro ir procesų analizės įrankiai bus nukopijuoti į jūsų katalogą.
5. Naudodamiesi Windows priemonėmis patikrinkite vykdomus procesus ir atvirus prievadus kompiuteryje. **Windows Task Manager** gali būti iškviestas klavišų kombinacija **Ctrl+Shift+Esc**. Atviri prievadai su vykdomais procesais gali būti iš komandinės eilutės paleidus komandą *netstat –anb* .
6. Gavę dėstytojo patvirtinimą, kad reikiami failai nukopijuoti išjunkite virtualiaus kompiuterio tinklą: **VirtualPC/ Settings/ Networking** visi tinklo adapteriai turėtų būti **Not Connected** būsenos.
7. Surinkite informaciją apie pradinę tinkle būseną. Paleiskite programą **Autoruns** iš **C:/Malware/XX** katalogo. Ji parodys veikiančius procesus ir kur yra jų paleidimą nusakantys įrašai. Kokia informacija apie procesus yra pateikiama? Paleiskite programą **Process Hacker**. Kokia informaciją apie procesus ir tinkle veiklą yra pateikiama? Paleiskite programą **Regshot** ir mygtuku **1st shoot/ Shoot and save** sukurkite ir išsaugokite faile **1.hivu** pradinį kompiuterio registro atvaizdą.
8. Išarchyvuokite kenkėjišką programinę įrangą, slaptažodis: infected. Ją paleiskite.
9. Kokie nauji procesai atsirado, kokie nauji prievadai buvo atidaryti, kokie procesai juos kontroliuoja? Kokios naujos Windows registro vertės atsirado? Tai nustatykite analizuodami **Autoruns** ir **Process Hacker** programų pateikiamą informaciją.
10. Perkraukite virtualų kompiuterį.
11. Naudodami programas **Autoruns** ir **Process Hacker** patikrinkite kaip paikeitė procesai ir tinklo veikla. Atkreipkite dėmesį, kad kenkėjiško proceso vardas labai panašus į operacinės sistemos procesą. Nustatykite kaip pasikeitė registras naudodami program **Regshot,** kurioje mygtuku **2nd shoot/ Shoot and save** sukurkite ir išsaugokite faile **2.hivu** dabartinį kompiuterio registro atvaizdą. Palyginkite kaip pasikeitė kompiuterio registras naudodami mygtuką **Compare**.Raskite informaciją apie įtartinas vertes, pastebėkite, kad keičiasi gana daug registro verčių dėl įprasto operacinės sistemos ir programų veikimo.
12. Sustabdykite kenkėjišką procesą **Process Hacker** programoje jį pažymėdami ir dešiniojo klavišo meniu pasirinkdami **Terminate**. Kartais procesas bando gintis nustatydamas kompiuterio perkrovimą po minutės. Jei taip įvyktų reikia skubiai iš komandinės eilutės paleistkite *shutdown –a* komandą kuri nutrauks persikrovimo laukimą. Ištrinkite registro vertę kuri kraunantis kompiuteriui paleidžia kenkėjišką procesą. Ištrinkite paleidžiamajį failą kompiuterio diske ir failą kuris buvo naudojamas užkrėsti kompiuterį, failus galite ištrinti pilnai, taip kad šie neatsidurtų šiukšlių dėžėje (Recycle Bin) naudodami kombinaciją **Shift+Del**.
13. Paleiskite kenkėjiškos programinės įrangos skenerį **Microsoft Safety Scanner** msert.exe. Patikrinkite ar nebeliko kenkėjiškos programos elementų. Baigus skenuoti žurnalą peržiūrėkite failą C:\Windows\Debug\msert.log.

**Ataskaita:**

1. Darbo tikslas
2. Kenkėjiškos įrangos analizės seka
3. Kenkėjiškos programos tirtos šiame laboratoriniame darbe veikimas ir jos komponentai
4. Kenkėjiškos programinės įrangos aprašymas pagal laboratorinio darbo variantą.

**Variantai:**

|  |  |
| --- | --- |
| Variantas | Programa |
| 1 | Bagle |
| 2 | Blaster |
| 3 | Code Red |
| 4 | ILOVEYOU |
| 5 | Kak worm |
| 6 | Klez |
| 7 | Melissa |
| 8 | Morris |
| 9 | Mydoom |
| 10 | Netsky |
| 11 | Nimda |
| 12 | Sircam |
| 13 | Sobig |
| 14 | SQL Slammer |
| 15 | Welchia |
| 16 | Zotob |