Министерство образования республики Молдова

Технический Университет Молдовы

Департамент Программной Инженерии и Автоматики

Отчёт

Лабораторная работа №6

По предмету: Infractiuni informatice si tehnici de investigare

Выполнил студ. гр. SI-202 Абабий Эдуард

Проверил Масютин Максим

Кишинёв – 2023

**Scopul** acestui laborator este de a-i învăța pe studenți să extragă și să analize fișierele de Registru pentru orice artefacte relevante.

**Sarcina:**

1. Completați câmpurile libere de mai jos cu informația corespunzătoare, obținută în urma analizei fișierelor!

**Rezolvarea sarcinilor:**

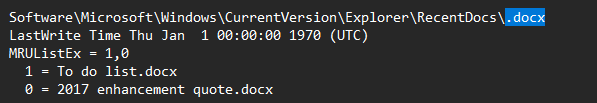
Folosiți produsul din NTUSER.DAT pentru a răspunde la următoarele întrebări.

1. Din ce fus orar sunt datele și orele care apar pentru artefactele de registru?

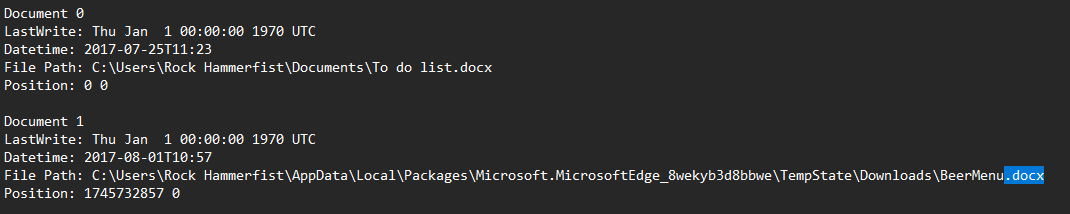
UTC

1. Câte documente word au fost vizualizate recent prin Explorer? Care au fost numele de fișiere?

2 / To do list.docx / 2017 enhancement quote.docx

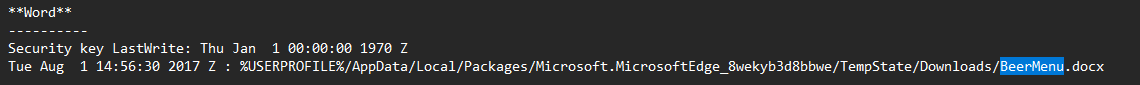


1. Au fost alte documente menționate în NTUSER.DAT? Dacă da, de ce acestea nu s-au regăsit în Registru?

Да, они подверглись записи, но не открывались из file explorer

1. Pe ce cale a fost accesat acesta și la ce oră? (Sugestie: adăugați în cronologie)

Файл был открыт 1 августа 14:56:30 2017  
%USERPROFILE%/AppData/Local/Packages/Microsoft.MicrosoftEdge\_8wekyb3d8bbwe/TempState/Downloads/BeerMenu.docx



1. A fost instalat CCleaner și dacă da, când?

Да, 18 марта 18 20:58:39 2017 года



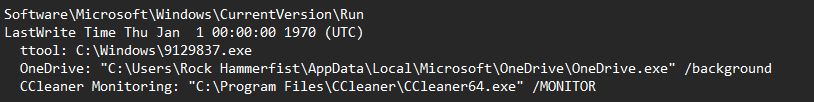
1. Ce a fost executat pe 8/1/17 la 17:56:12? În ce cheie s-a găsit acesta? (Sugestie: adăugați în cronologie)

Был запущен файл javainstall.exe



1. Ce aplicații au fost setate la autorun? Având în vedere că este NTUSER.DAT, ce înseamnă acest lucru?

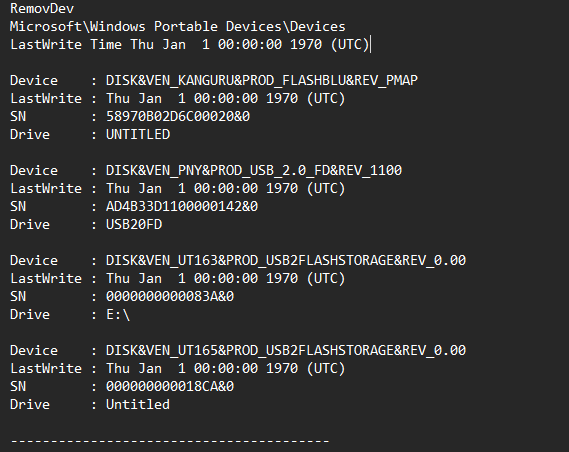
9129837.exe / OneDrive.exe / CCleaner64.exe были установлены в автозапуск. Имея ввиду, что файл NTUSER.DAT, это значит что эти программы были установлены в автозапуск для пользователя Rock Hammerfist



Folosiți produsul din SOFTWARE pentru a răspunde la următoarele întrebări.

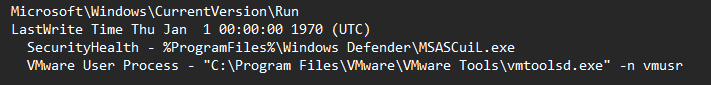
1. Câte dispozitive USB au fost introduse în acest sistem? Care cheie v-a spus acest lucru?

4 / ключём для поиска было USB



1. Ce programe au fost setate la autorun?

MSASCuil.exe / vmtoolsd.exe

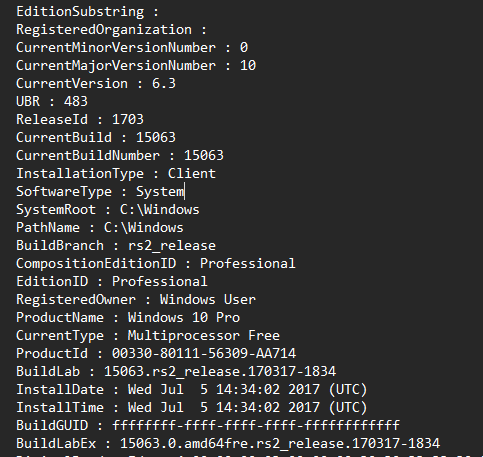


1. Comparativ cu NTUSER.DAT, sunt aceleași programe? Dacă nu, de ce?

Нет, это не те же программы. NTUSER.DAT содержит в себе настройки для определенного пользователя, а SOFTWARE сохраняет информацию вне зависимости от пользователя

1. Ce versiune de Windows a fost instalată pe acest sistem? Când a fost instalată aceasta?

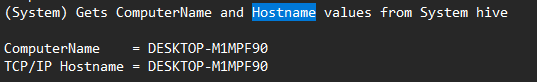
Windows 10 Pro, установлена 5 июля 14:34:02 2017 года



Folosiți produsul din SYSTEM pentru a răspunde la următoarele întrebări.

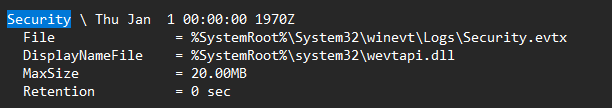
1. Care este numele gazdei sistemului victimă?

DESKTOP-M1MPF90



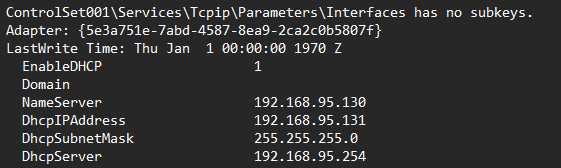
1. Care este dimensiunea maximă pentru Security Event log?

Максимальный размер для Security Event Log – 20.00 MB



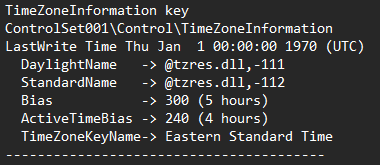
1. Ce adresă IP a fost atribuită ultima dată adaptorului de rețea?

192.168.95.131



1. La ce fus orar a fost configurat sistemul?

UTC Eastern Standard Time



Folosiți instrumentul lui Eric Zimmerman AppCompatCacheParser pentru a răspunde la următoarele întrebări. Deschideți un prompt de comandă(cmd) și navigați către folderul unde ați salvat instumentul descărcat și tapați comanda “AppCompatCacheParser.exe –f SYSTEM --csv *filename*”.

1. Se afișează aici vreunul dintre programele setate la autorun? Care este marcajul temporal?

9129837.exe Год создания 2008, несмотря на то, что система была установлена в 2017 году



1. Are acest marcaj vreunul dintre alte programe?

Javainstall.exe



1. Chiar dacă marcajul temporal este oprit, ce ar putea însemna faptul că au același marcaj temporal?

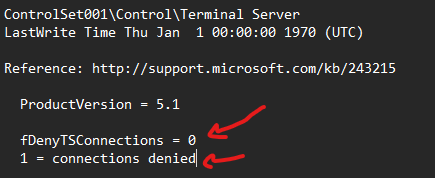
Есть 2 варианта:  
1. Этот файл мог попасть в компьютер после запуска javainstall.exe и это может быть троян или шпионское ПО.

2. Этот файл попал иным способом в компьютер и является трояном-загрузчиком, которому для полноценной работы необходим был файл javainstall.exe, который он успешно загрузил и запустил

1. Există vreun artefact care ar arăta că PSEXEC a fost rulat? Care este marcajul temporal și posibila semnificație criminalistică? (Sugestie: PSEXEC este un instrument Sysinternals care permite utilizatorului să ruleze de la distanță aplicații pe un sistem. Atunci când este executat, numele fișierului nu este psexec.exe, dar este aproape de acesta.) (Sugestie: adăugați în cronologie)

fDenyTSConnections показывает что подключений на момент не было, но 1 подключение было отказано, возможно, что PSEXEC был запущен





Вывод: В данном лабораторной работе я научился работать с файлами HIVE и анализировать их. Благодаря такому способу, можно узнать какие шаги и пути предпринял злоумышленник.