|  |  |  |
| --- | --- | --- |
| Лабораторија за дигиталну форензику Факултет техничких наука | | Фрушкогорска 1 21102 Нови Сад |
| 17.6.2023. | Невена Атић | Тополска 18, 11000 Београд |

**ОПИС СЛУЧАЈА**

Дана 20. 2. 2023. године, ангажовани смо од стране Богољуба Гагића из Београда, директора фирме „Муња транс“, да извршимо вештачење и сачинимо налаз и мишљење за случај тешког кривичног дела које обухвата шверц дроге. Недозвољене супстанце су заплењене у транспортном камиону регистарских ознака BG584XX, који припада фирми на чијем се челу налази Гагић. Фирма се изворно бави шпедицијом и транспортом робе и Богољуб Гагић тврди да лично није повезан са недозвољеним активностима, као и да је превоз дроге подметнут у сарадњи са неким од запослених.

Задатак вештачења је да прегледамо и анализирамо електронску опрему која укључује следеће уређаје:

− Десктоп рачунар произвођача Acer, моделa Aspire E1-571 и серијског броја 589-87VQW389FSF-3FG преузет од директора Богољуба Гагића.

− Десктоп рачунар произвођача HP, модела Pavilion G6 и серијског броја HP98-556FRWQ98DFL-258F преузет од запослене Душанке Свиларевић.

− Десктоп рачунар произвођача Toshiba, модела Satellite Pro L450 и серијског броја 897526 преузет од запосленог Павла Пандуровића.

− USB флеш меморија произвођача SanDisk, модела Cruser Force и серијског броја 0xd585e28 преузета од запосленог Павла Пандуровића.

− Мобилни телефон произвођача Google, модел Pixel 5 и серијског броја EMULATOR32X1X11X0 преузет од запослене Душанке Свиларевић.

и у циљу разрешења случаја:

1. утврдити да ли је постојао малициозни софтвер на рачунару Богољуба Гагића помоћу ког је злонамерни запослени могао да дође до креденцијала за приступ веб сервису за вођење евиденције о поласцима камиона
2. анализом чбрстог диска извађеног из кућишта Павла Пандуровића утврдити постојање сумњивих датотека у application/pdf формату чија екстензија не одговара датом формату
3. анализом USB флеш меморије преузете од запосленог Павла Пандуровића утврдити њен садржај.
4. пронађемо обрисане датотеке сумњвог садржаја у jpg формату од 100 до 150 KiB са чврстог диска извађеног из кућишта Павла Пандуровића
5. анализом радне меморије прикупљене са рачунара Павла Пандуровића пронаћи,

анализирати и документовати активне процесе везане за апликације за директну

комуникацију

1. анализом радне меморије прикупљене са рачунара Павла Пандуровића пронаћи,

анализирати и документовати сумњиве команде које је корисник уносио у терминал, а које указују на коришћење стеганографских алата и алата за криптовање фајлова, партиција, дискова и доћи до датотека којима је руковао током спровођења команди

1. пронаћи све AES кључеве који се налазе у радној меморији прикупљеној са рачунара Павла Пандуровића
2. анализом радне меморије прикупљене са рачунара Душане Свиларевић пронаћи, анализирати и документовати процесе који су покренути, а који нису системски
3. применом алата RegRipper над кошницом System пронаћи доказ да је USB флеш меморија која припада Павлу Пандуровићу, била маунтована на рачунару Богољуба Гагића
4. Анализом конфигурационе датотеке оперативног система Linux, која се налази на чврстом диску Павла Пандуровића пронаћи апликацију за директну комуникацију која се покреће аутоматски након покретања оперативног система
5. Увидом у датотеку access.log издвојити јавне IP адресе фирме „Муња транс” (и одговарајуће портове) са којих је приступано веб сервису за евидентирање полазака

камиона

1. Увидом у логове сервиса NAT конфигурисаног на рутеру фирме „Муња транс”, одредити приватне IP адресе са којих је приступано веб сервису за евидентирање полазака камиона, а потом одредити којим запосленима те адресе припадају
2. Увидом у снимaк мрежног саобраћаја Душанке Свиларевић, одговорити на питање да ли је и ако јесте, када, успостављена безбедна комуникација са сервером чије је име домена airserbia.com
3. Анализирати масовну меморију прикупљену са рачунара Павла Пандуровића. Пронаћи који веб претраживач је коришћен, анализирати и документовати резултате претраге везане за туристичке агенције и дестинације
4. Анализирати масовну меморију прикупљену са рачунара Павла Пандуровића. Пронаћи мејл клијента који је коришћен, анализирати мејлове који су везани за контекст путовања, документовати учеснике у комуникацији (њихове мејл адресе), време слања порука, садржај порука и прилоге, уколико постоје.
5. Претходно пронађене датотеке које су биле прикачене као прилог унутар пронађених мејл порука извести, анализирати садржај и метаподатке докумената. Утврдити да ли је реч о авионским картама за одређену дестинацију и уколико јесте, документовати назив документа, компанију која је издала карту, на чије име гласи карта, за коју дестинацију је везана, датум и време лета и који је формат документа.
6. Анализирати масовну меморију прикупљену са рачунара Павла Пандуровића. Пронаћи, анализирати и документовати мејлове везане за малициозни програм keylogger и извештаје које је послао програм.
7. Анализирати масовну меморију прикупљену са рачунара Душанке Свиларевић. Пронаћи који веб претраживач је коришћен, анализирати и документовати резултате претраге везане за куповину авионских карата
8. Анализирати прикупљене податке са мобилног телефона од Душанке Свиларевић, њене контакте, поруке и позиве. Потребно је приказати све контакте у именику, све SMS поруке и метаподатке о телефонским позивима везане за комуникацију са Павлом Пандуровићем
9. Анализирати комуникацију смештену у бази података WhatsApp апликације. Издвојити преписке које је Душанка Свиларевић размењивала са Данилом Језеркићем. Документовати све фајлове које су размењивали.
10. Анализирати базу података Gmail апликације коришћене за размену мејлова. Издвојити мејл поруке које је Душанка Свиларевић размењивала са Павлом Пандуревићем везане за куповину авионских карата.

**Н а л а з**

Дана 6. 3. 2022. године у 10.30 часова, приступили смо вештачењу у просторијама Лабораторије за дигиталну форензику. Из рачунара Acer, моделa Aspire E1-571 и серијског броја 589-87VQW389FSF-3FG, извадили смо чврсти диск произвођача Seagate, модела ST1000DM010 и серијског броја 3660619402182 (у наставку чврсти диск Богољуба Гагића). Из рачунара Toshiba, модела Satellite Pro L450 и серијског броја 897526, извадили смо чбрсти диск произвођача SYNOLOGY, модела HAT5300-12T и серијског броја 4711174724130 (у наставку чврсти диск Павла Пандуровића). Из рачунара HP, модела Pavilion G6 и серијског броја HP98-556FRWQ98DFL-258F, извађен је чврсти диск произвођача Western Digital, модела WD10SPZX и серијског броја 718037845319 (у наставку чврсти диск Душанке Свиларевић).

Направили смо форензичку копију чврстих дискова помоћу алата FTK Imager верзије 3.1.1.8 чији се лог извршавања налази у прилогу 1.

Форензичка копија је копија складишта података идентична оригиналу, а алат FTK Imager служи за креирање форензичке копије складишта података.

Алат FTK Imager коришћен је и за прикупљање рам меморије са рачунара Душанке Свиларевић на ком је подигнут WindowsXP оперативни систем.

Рам меморија са рачунара запосленог Павла Пандуровића на ком је подигнут Ubuntu 14.04 оперативни систем, прикупљена је помоћу AVML алата.

AVML је X86\_64 кориснички алат за прикупљање радне меморије. AVML се може користити за прикупљање меморије без неопходног познавања циљне ОС дистрибуције или кернела.

Помоћу алата adb, направили смо форензичку копију података ускладиштених у интерном складишту података мобилног телефона произвођача Google, модел Pixel 5 и серијског броја EMULATOR32X1X11X0 (у наставку Душанкин мобилни телефон).

Алат adb, између осталог, служи за преузимање података из складишта података мобилног телефона.

Помоћу алата Autopsy 4.19.3 извршили смо прегледање и анализу форензичких копија чврстог диска Богољуба Гагића, Павла Пандуровића и интерног складишта Душанкиног мобилног телефона.

Алат Autopsy служи за прегледање и анализу форензичких копија складишта података.

Анализирали смо интерно складиште мобилног телефона Душанке помоћу модула аLEAPP алата Autopsy. aLEAPP служи за прегледање и анализу података преузетих из складишта података мобилног телефона.

На основу изнетог налаза, дајемо следеће

**М и ш љ е њ е**

|  |  |
| --- | --- |
| Нови Сад, 20. 6. 2023. | Судски вештак за информационе технологије  Невена Атић, дипл. инж. |

Прилози:

1. Прилог 1: Лог алата FTK Imager 3.1.1.8

2. Прилог 2: Размењена електронска писма

3. Прилог 3: Размењене SMS поруке

4. Прилог 4: Фотографије пронађене на чврстом диску