EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

TESTOVÁNÍ BEZPEČNOSTI

Forenzní audit s využitím artefaktů Windows

Metodický list

Autor: doc. Ing. Jaroslav Dočkal, CSc., Metodik: Bc. Jaroslav Tihlařík

Recenzent: Ing. Vladimír Šulc Ph.D.

Rok vydání: 2023

Obsah

Cíle

V rámci této úlohy je třeba dosáhnout těchto výukových cílů:

- Naučit se prakticky pracovat s nástroji Erica Zimmermana
- Vyzkoušet si práci s typickou úlohou letsdefend.io
- Seznámí se s metodami identifikace podezřelých souborů jako jsou např. *Unassociated File Entries*

Dovednosti

V rámci této úlohy je třeba získat tyto dovednosti:

- Extrahovat příslušný soubor artefaktů.
- Identifikovat útoky metodou timestomping[1]
- Analyzovat použití perzistentních technik

Pracovní prostředí

Úlohu lze realizovat v prostředí:

- Cylab JCEKB
- Offline Security Classroom

Pro práci budeme potřebovat následující nástroje:

- FTK imager
- ShellBags Explorer
- RBCmd
- AMcacheParser
- MFTExplorer
- RegistryExplorer
- Bmc-tools
- DeepBlueCLI

FTK Imager Eric Zimmerman's tools:

Umístění https://ericzimmerman.github.io/#!index.md

Heslo: infected

Artefakt je třeba stáhnout z https://drive.google.com/file/d/1flf7YbdsWByT-alpFzBb4Ksb0eFy7dCT/view

[1] Timestomping je technika, při které jsou časová razítka souboru upravena tak, aby se zabránilo obraně.

Průběh výuky

1 Forenzní analýza a forenzní artefakty systému Windows

Forenzní analýza systému Windows se zaměřuje na dvě věci: na hloubkovou analýzu operačního systému Windows a analýza artefaktů.

Forenzní artefakty jsou forenzní předměty, které mají nějakou forenzní hodnotu (tzn. lze je předložit jako důkazy v rámci soudního jednání). Artefakty Windows jsou objekty, které obsahují informace o činnostech prováděných uživatelem Windows. Typ informací a umístění artefaktu se liší od jednoho operačního systému k druhému.

V určitých právních nebo regulačních kontextech může být požadováno pořízení úplné a ověřitelné kopie digitálního paměťového zařízení, včetně veškerého nepřiděleného prostoru, aby byla zajištěna integrita a pravost důkazů. Je to proto, že obrazy (image) vlastního obsahu mohou být považovány za neúplné a potenciálně méně spolehlivé, protože nezachycují celý rozsah úložného zařízení a nemusí poskytovat úplný řetězec správy.

V jiných příp+adech potřebujeme mít artefakty, ale nemáme dostatek místa nebo času na zachycení úplného obrazu systému. Měli bychom tedy shromáždit nejdůležitější artefakty související s řešením případu. U soudu však nemusí být právně přijatelné shromažďovat pouze vlastní obrazy obsahu forenzních artefaktů Windows, na rozdíl od obrazů celého disku.

1.1 Kterými artefakty začít?

V této části si projdeme některé forenzní artefakty, které forenzní vyšetřovatel při provádění forenzní analýzy ve Windows hledá prvořadě.

1.1.1 Koš

Koš systému Windows obsahuje několik artefaktů, jako jsou:

- $1 soubor obsahující metadata. Tento soubor najdete pod cestou C:\$Recycle.Bin\SID*\$Ixxxxxx
- $R soubor obsahující obsah smazaných souborů. Tento soubor může být umístěn pod cestou C:\$Recycle.Bin\SID*\$Rxxxxxx
- Soubor $1 lze analyzovat pomocí nástroje $1 Parse.

1.1.2 Prohlížeče

Webové prohlížeče obsahují mnoho informací jako:

- soubory cookie
- data webových stránek uložená v cache (mezipaměti)
- stažené soubory

1.1.3 Windows Error Reporting

Tato funkce umožňuje uživateli informovat Microsoft o chybách aplikací, chybách jádra, nereagující aplikaci a dalších problémech specifických pro aplikaci. Tato funkce nám poskytuje různé artefakty jako je spuštění programu, pokud se škodlivý program zhroutí během provádění programu.

Tyto artefakty můžete najít na následujících místech:

C:\ProgramData\Microsoft\Windows\WER\ReportArchive
C:\Users\XXX\AppData\Local\Microsoft\Windows\WER\ReportArchive
C:\ProgramData\Microsoft\Windows\WER\ReportQueue
C:\Users\XXX\AppData\Local\Microsoft\Windows\WER\ReportQueue

1.1.4 Cache protokolu RDP

Ke spuštění vzdálené plochy protokolem Remote Desktop Protocol (RDP) se v systému Windows řadu let používá příkaz MSTSC[2]. V zásadě jsou images ukládány lokálně v klientském systému, aby se urychlily relace a snížily latence tím, že se zabrání tomu, aby byly stejné images načteny více než jednou. Jedná se o starší funkci z dob, kdy byl internet extrémně pomalý (předpokládejme vytáčené připojení) a relace RDP byly tudíž rovněž pomalé.

Při použití klienta MSTSC lze RDP použít k laterálnímu pohybu po síti. Vytvářejí se cache soubory obsahující části obrazovky počítače, ke které jsme připojeni, a to se jen zřídka mění. Tyto cache soubory mohou být umístěny v adresáři:

C:\Users\XXX\AppData\Local\Microsoft\Terminal Server Client\Cache

K extrahování obrázků uložených v těchto cache souborech lze použít nástroje BMC-Tools[3].

1.1.5 Soubory LNK

Soubory .lnk jsou soubory zástupců systému Windows. Soubory LNK odkazují nebo odkazují na jiné soubory nebo spustitelné soubory pro snadný přístup. V těchto souborech můžete najít následující informace:

- původní cesta k cílovému souboru
- časové razítko cílových souborů i souborů .lnk
- atributy souborů jako jsou System, Hidden atd.
- podrobnosti o disku
- vzdálené nebo místní spuštění
- MAC adresy strojů

K analýze obsahu těchto souborů lze použít nástroje jako Windows LNK Parsing Library nebo LECmd.

[2] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/mstsc
[3] https://github.com/ANSSI-FR/bmc-tools

1.1.6 Seznamy odkazů

Obsahují informace o naposledy použitých aplikacích a souborech. Tato funkce byla zavedena se systémem Windows 7. V systému Windows lze vytvořit dva typy seznamů odkazů:

- AUTOMATICDESTINATIONS-MS: Tyto seznamy skoků se vytvářejí automaticky, když uživatel otevře soubor nebo aplikaci. Jsou umístěny pod cestou: C:\Users\xxx\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
- CUSTOMDESTINATIONS-MS: Tyto seznamy skoků jsou vytvořeny na zakázku a jsou vytvořeny, když uživatel připne soubor nebo aplikaci. Jsou umístěny v adresáři C:\Users\xxx\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

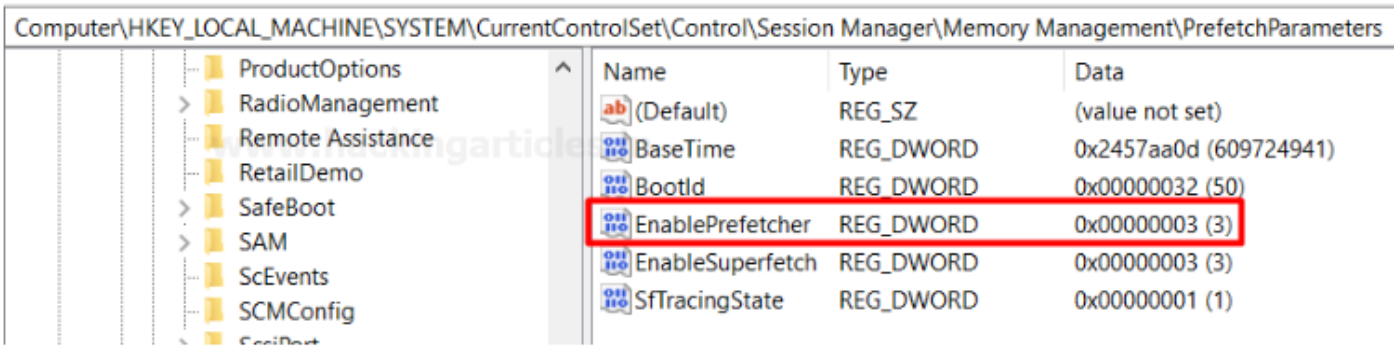
K analýze seznamů skoků lze použít nástroje jako JumpList Explorer, JLECmd nebo Windows JumpList Parser.

1.1.7 Prefetch soubory

Tyto soubory obsahují velké množství informací jako:

- Název aplikace.
- Cesta aplikace.
- Časové razítko posledního provedení.
- Časové razítko vytvoření.

Tyto soubory mohou být umístěny v adresáři: C:\Windows\Prefetch\. Kontrolu lze provést v Registry editoru na: Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters viz obr. 1.1.7.1.



Obr. 1.1.7.1 Prefetcher v Registry editoru.

V souborech se nacházejí tyto údaje[4]:

- název spustitelného souboru
- osmiznakový hash cesty ke spustitelnému souboru.
- cesta ke spustitelnému souboru

[4] Chandel Raj. Forensic Investigation: Prefetch File. Hacking Articles, October 15, 2020. Dostupné z: https://www.hackingarticles.in/forensic-investigation-prefetch-file/

.

- časové razítko vytvoření, úpravy a přístupu ke spustitelného souboru
- počet spuštění (počet doby, po kterou byla aplikace spuštěna)
- doba posledního spuštění
- časové razítko za posledních 8 běhů (1 čas posledního běhu a dalších 7 dalších časů posledního běhu)
- informace o objemu
- soubor, na který odkazuje spustitelný soubor
- adresáře, na které odkazuje spustitelný soubor

Soubory předběžného načtení jsou uloženy pod %SystemRoot%\Prefetch (C:\Windows\Prefetch).

Pro jejich analýzu lze použít specializované nástroje jako jsou Windows Prefetch Parser, WinPrefetchView, nebo PECmd.

1.1.8 Shell Bags

Windows Shell Bags byly zavedeny do operačního systému Microsoft Windows 7 a jsou dosud přítomny na všech pozdějších platformách Windows. Shellbags jsou klíče registru, které se používají ke zlepšení uživatelské zkušenosti a vyvolání uživatelských preferencí, kdykoli je to potřeba. Vytvoření skořepinových vaků závisí na cvičeních prováděných uživatelem.

Jako digitální forenzní vyšetřovatel můžete pomocí shellbagů prokázat, zda konkrétní složka byla přístupná konkrétním uživatelem nebo ne. Můžete dokonce zkontrolovat, zda byla konkrétní složka vytvořena nebo byla k dispozici nebo ne. Můžete také zjistit, zda byly externí adresáře zpřístupněny na externích zařízeních nebo ne.

Z větší části jsou Shell Bags určeny k uchování dat o aktivitách uživatele při prozkoumávání Windows. To znamená, že pokud uživatel změní velikost ikon z velkých ikon na mřížku, nastavení se v Shell Bag okamžitě aktualizuje. V okamžiku, kdy otevřete, zavřete nebo změníte výběr libovolné složky ve vašem systému, ať už z Průzkumníka Windows nebo z plochy, dokonce i kliknutím pravým tlačítkem myši nebo přejmenováním organizátoru, se vytvoří nebo obnoví záznam Shellbag.

Informace ShellBag jsou klíčové, když forenzní pracovníci potřebují vědět, kdy a ke které složce uživatel přistupoval. Například, když má společnost podezření, že zaměstnanec unikl důvěrnému dokumentu uloženému v síti, počítač tohoto zaměstnance může mít informace ShellBag, které prokazují, že složka obsahující tento dokument byla zpřístupněna krátce před únikem dokumentu. Kromě toho mohou ShellBags také zobrazovat složky nebo servery, ke kterým by zaměstnanec neměl přistupovat. Tato zjištění jsou pro vyšetřování kritická. Nebo když má společnost podezření, že zaměstnanec úmyslně smazal důležité soubory v síti, informace ShellBag mohou prokázat, že počítač zaměstnance přistupoval ke složce předtím, než k incidentu došlo.

1.2 Vytvoření vlastního image obsahu – Artefakty Windows 10

Image musí především obsahovat:

```
SAM
SOFTWARE
SECURITY
SYSTEM
Path: %windir%\System32\config
```

SAM, SOFTWARE, SECURITY a SYSTEM jsou podregistry registru, které obsahují důležité informace o uživatelských účtech, nainstalovaném softwaru, zásadách zabezpečení a nastavení systému. Tyto podregistry registru jsou umístěny ve složce %windir%\System32\config.

```
USRCLASS.dat
USRCLASS.LOG[                                                    ]
Path: %appdata%\..\Local\Microsoft\windows\
```

USRCLASS.dat a USCCLASS.LOG[ ] jsou soubory, které obsahují nastavení registru specifické pro uživatele a lze je nalézt ve složce %appdata%..\Local\Microsoft\windows\.

```
$MFT
$LogFile
$I30
$data
$Bitmap
$EXTEND
```

$MFT, $LogFile, $I30, $data, $Bitmap a $EXTEND jsou soubory, které jsou součástí systému souborů NTFS a obsahují informace o souborech a adresářích v systému. Tyto soubory lze nalézt v kořenovém adresáři každého svazku NTFS.

```
.evtx
```

Soubory *.evtx jsou protokoly událostí, které obsahují informace o systémových a aplikačních událostech. Tyto soubory lze nalézt ve složce %SystemRoot%\System32\winevt\Logs.

```
%appdata%
```

Složka %appdata% obsahuje data aplikace pro aktuálního uživatele, včetně nastavení a dočasných souborů.

```
Prefetch
Path: %windir%\prefetch
```

Složka Prefetch umístěná ve složce %windir%\prefetch obsahuje informace o aplikacích, které byly spuštěny v systému.

pagefile.sys
hiberfil.sys
Path: %SystemDrive%\

pagefile.sys a hiberfil.sys jsou systémové soubory, které obsahují data používaná operačním systémem při správě systémové paměti a řízení spotřeby.

Webcache.dat
Path: %appdata%\..\Local\Microsoft\windows\

Webcache.dat je soubor používaný webovým prohlížečem Microsoft Edge k ukládání historie prohlížení a dalších informací. Tento soubor lze nalézt ve složce %appdata%..\Local\Microsoft\windows\.

SRUDB.dat
Path: %windir%\system32\SRU\SRUDB.dat

SRUDB.dat je soubor, který obsahuje informace o využití systémových prostředků a lze jej nalézt ve složce %windir%\system32\SRU\.

INF
Path: %systemdrive%\windows\inf

Soubory INF používá systém Windows k instalaci ovladačů zařízení a obsahují informace o hardwaru a softwaru nainstalovaném v systému. Tyto soubory lze nalézt ve složce %systemdrive%\windows\inf.

AmCache
Path: \%SystemRoot%\AppCompat\Programs\Amcache.hve

AmCache.hve je soubor, který obsahuje informace o aplikacích spuštěných v systému a lze jej nalézt ve složce %SystemRoot%\AppCompat\Programs\.

AppCompatCache (ShimCache)
Path:
HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\AppCompatCache

AppCompatCache (ShimCache) obsahuje informace o kompatibilitě aplikací v systému a lze ji nalézt v klíči registru HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\AppCompatCache.

*.PST
*.OST

Soubory *.PST a *.OST používá Microsoft Outlook k ukládání e-mailových dat.

Thumbs.db
thumbcache_[…].db
Path: %userprofile%\AppData\Local\Microsoft\Windows\Explorer

Soubory Thumbs.db a thumbcache_[…].db používá systém Windows k ukládání miniatur obrázků a lze je nalézt ve složce %userprofile%\AppData\Local\Microsoft\Windows\Explorer.

```
*.lnk
Path: %AppData%\Roaming\Microsoft\Windows\Recent
```

Soubory *.lnk jsou soubory zástupců (shortcuts), které lze nalézt ve složce %AppData%\Roaming\Microsoft\Windows\Recent.

```
Jumplist
Paths: %AppData%\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
%AppData%\Roaming\Microsoft\Windows\Recent\CustomDestinations
```

Soubory Jumplist obsahují informace o nedávné aktivitě aplikací a lze je nalézt ve složkách %AppData%\Roaming\Microsoft\Windows\Recent\AutomaticDestinations %AppData%\Roaming\Microsoft\Windows\Recent\CustomDestinations.

Při shromažďování artefaktů je důležité si uvědomit potenciální dopad na cílový systém a dodržovat správné forenzní postupy, aby byla zajištěna integrita dat. Abyste zachovali integritu důkazů, musíte dodržovat řádné forenzní postupy a dokumentovat proces.

2 Praktická část

2.1 Vytvoření image pomocí FTK Imageru

FTK (Forensic Toolkit) Imager je digitální forenzní nástroj používaný k zachycení obrazů (image) digitálního paměťového zařízení, jako je pevný disk, USB disk nebo paměťová karta. FTK Imager dokáže vytvořit vlastní image obsahu výběrem konkrétních souborů nebo složek z úložného zařízení. Zde je návod, jak zachytit vlastní image obsahu pomocí FTK Imager:

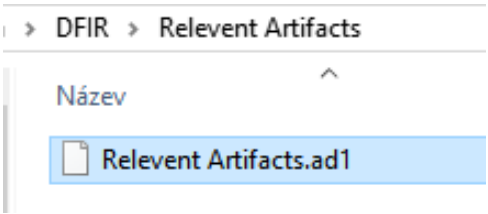
1. Stáhněte a nainstalujte FTK Imager z webu AccessData na *https://www.exterro.com/ftk-imager*
2. Spusťte FTK Imager a vyberte možnost „ **Create Disk Image**“ z nabídky „**File**“.
3. Vyberte úložné zařízení, ze kterého chcete vytvořit vlastní image obsahu.
4. Chcete-li zachytit logický obraz úložného zařízení, vyberte možnost **„Logical**“.
5. V části „ **Select Data to Image**“ vyberte možnost „**Files**“ pro zachycení konkrétních souborů nebo složek.
6. Klepnutím na tlačítko „**Add**“ vyberte soubory nebo složky, které chcete zahrnout do image vlastního obsahu. Systém souborů můžete procházet pomocí stromového zobrazení nebo můžete přímo zadat cestu k souboru.
7. Pokud chcete vyloučit konkrétní soubory nebo složky z obrázku vlastního obsahu, klikněte na tlačítko „**Exclude**“ a vyberte položky, které chcete vyloučit.
8. V části „ **Image Destination**“ vyberte, kam chcete obrázek vlastního obsahu uložit. Můžete jej uložit do souboru, na fyzický disk nebo do síťového umístění.
9. V případě potřeby vyberte úroveň komprese pro soubor image.
10. Kliknutím na tlačítko „**Start**“ zahájíte zachycení vlastního image.
11. Jakmile je proces dokončen, můžete image ověřit pomocí možnosti „ **Verify Image**“ z nabídky „**File**“.

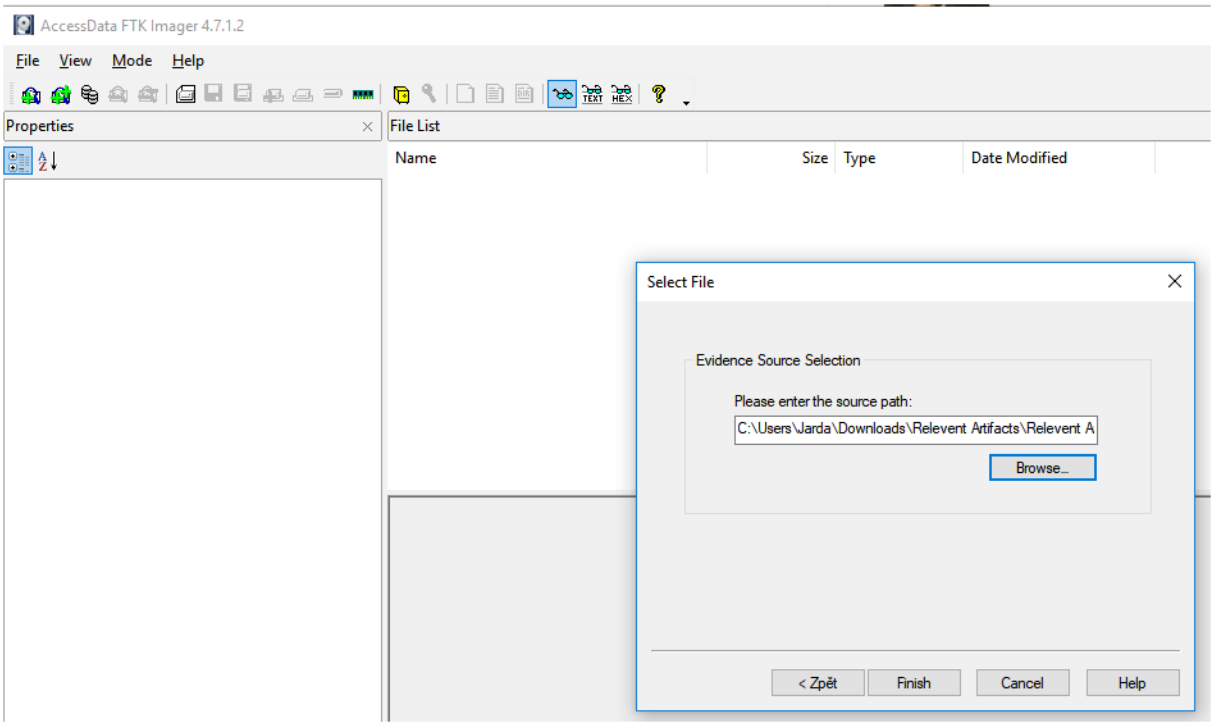
2.2 Řešení konkrétního scénáře

Scénář: Proti naší organizaci je vedena cílená phishingová kampaň a phishingovou poštu zatím otevřely tři systémy v naší síti. Z jednoho z infikovaných systémů byl shromážděn image a poskytnut pro identifikaci TTP (Tactics, Techniques, Procedures) používaných útočníky. Identifikujte techniky a taktiky používané útočníkem, aby náš tým pro reakci na incidenty mohl reagovat a zmírnit jakékoli další kompromitace v síti.

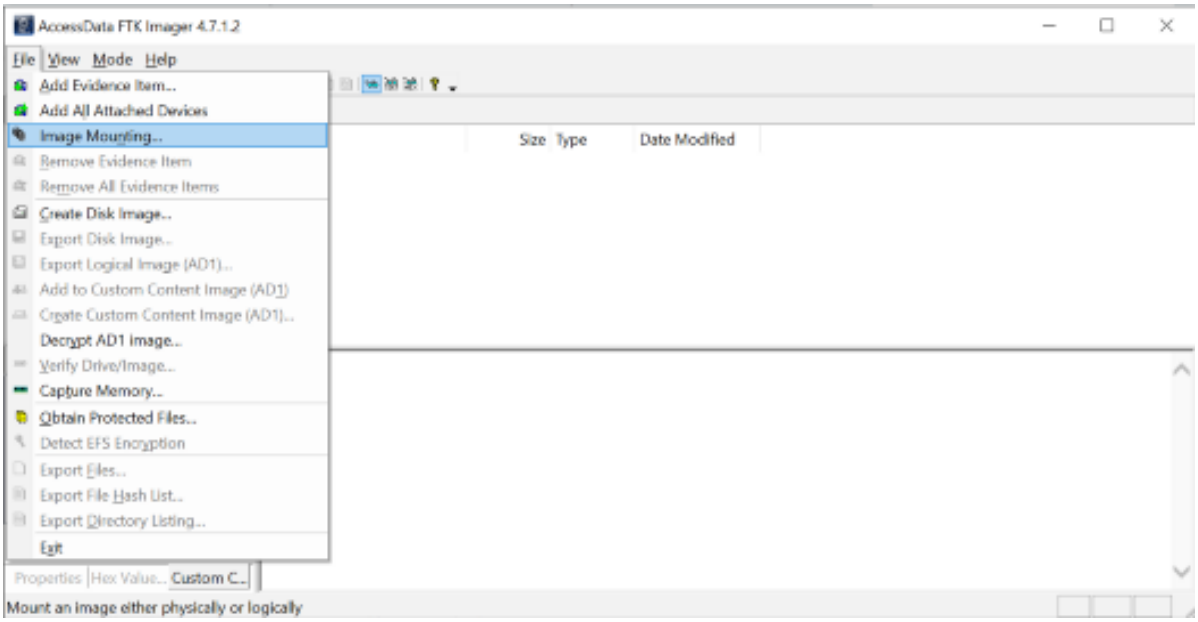
Artefakt je třeba stáhnout z

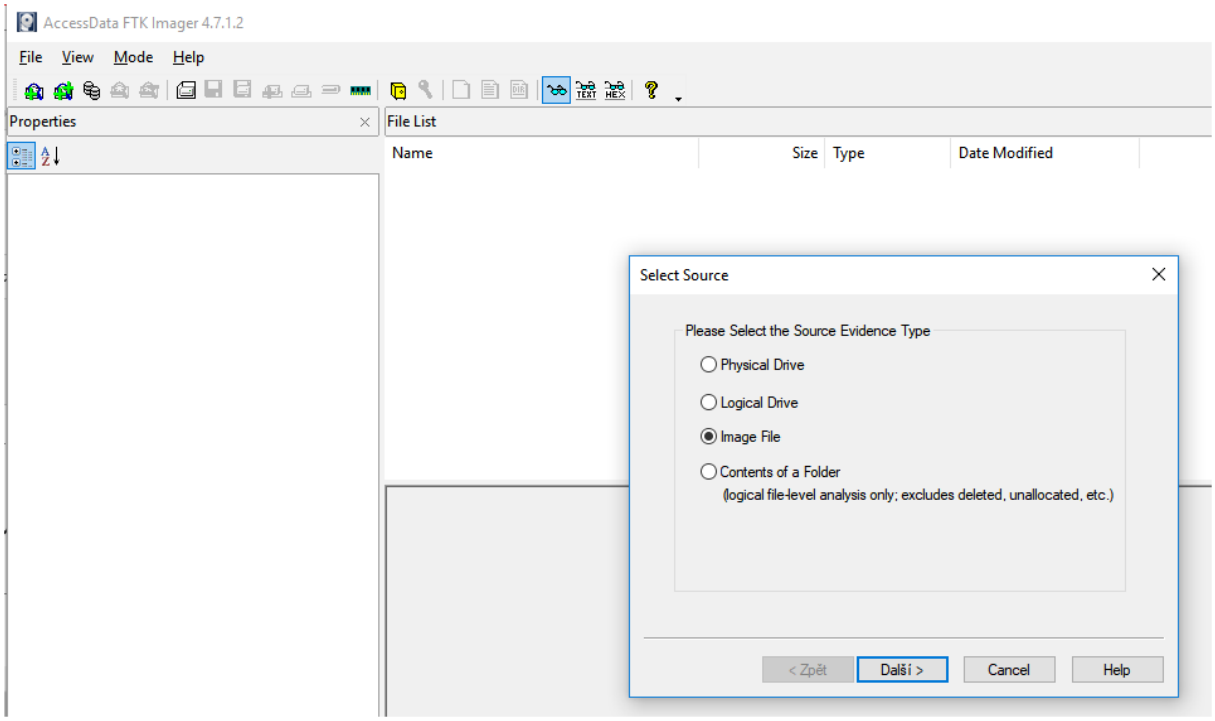
https://drive.google.com/file/d/1flf7YbdsWByT-alpFzBb4Ksb0eFy7dCT/view



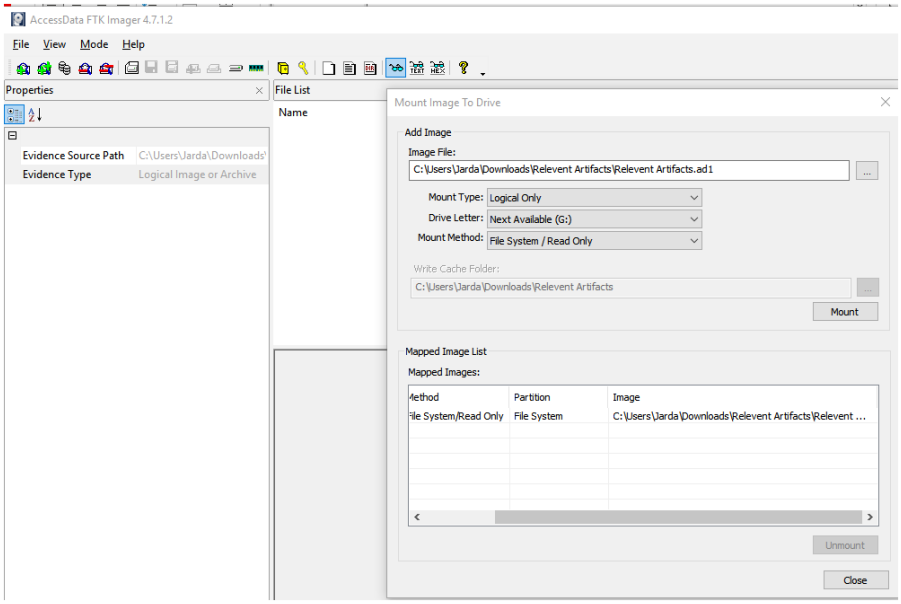


Cílem je analyzovat forenzní artefakty a odpovědět na řadu otázek. Prvním krokem analýzy je připojení image pomocí FTK Imageru:

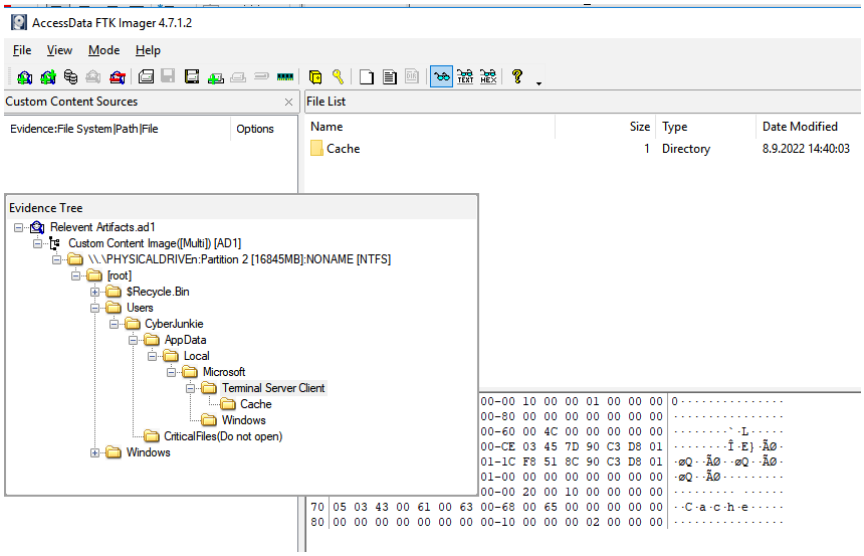




Klepnutím na tlačítko **MOUNT Image To Drive** připojte image.



Nyní je image připojen, prozkoumejte ho v rámci jednotky, kam jste ho uložili, je tam uživatel s názvem „Cyber Junkie“.



Začněme první otázkou

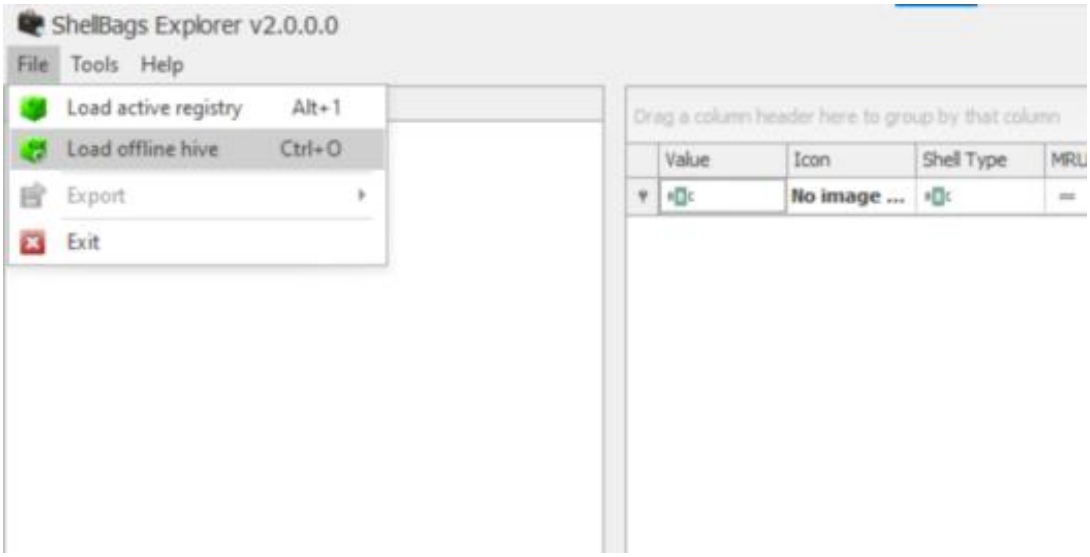
1.*Počáteční přístup byl proveden prostřednictvím škodlivého dokumentu doručeného e-mailem. Jaká byla úplná cesta, kam byl dokument stažen?*

Microsoft Windows sleduje uživatelské předvolby prohlížení oken specifické pro Windows Explorer. Sledované položky zahrnují velikost, zobrazení, ikonu a polohu složky z Průzkumníka (Exploreru) Windows. Tyto informace se označují jako „ShellBags“ a jsou uloženy na několika místech v registru/

Protože útok začal z phishingové pošty, cesta ke stažení by pravděpodobně byla složka Downloads. Každopádně to můžeme zkontrolovat analýzou artefaktu ShellBag.

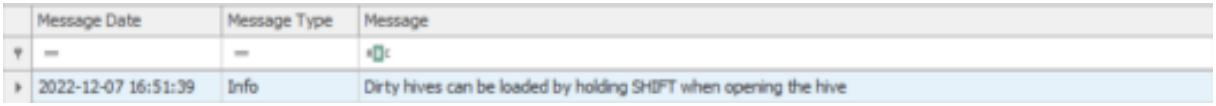
ShellBags jsou uloženy jako vysoce vnořená a hierarchická sada podklíčů v UsrClass.dat.

K tomu slouží nástroj **ShellBags Explorer**, který je ke stažení i na webu SANS (https://www.sans.org/tools/shellbags-explorer/)



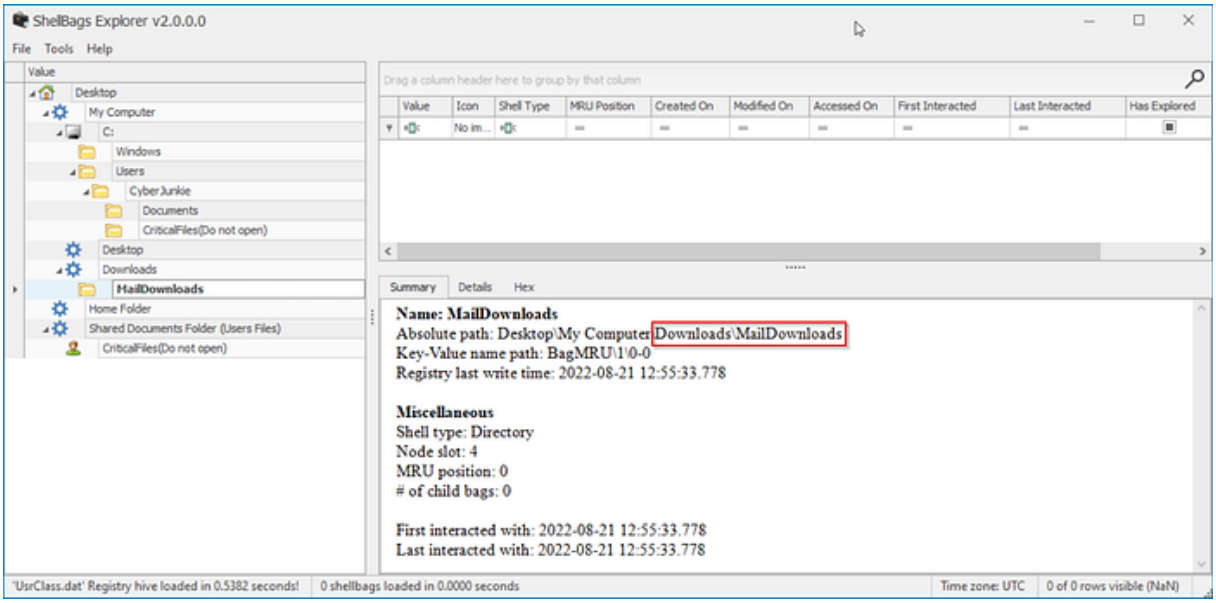
Cesta pro hive je: <logical drive>:__._PHYSICALDRIVEn_Partition 2 [16845MB]_NONAME [NTFS]\[root]\Users\CyberJunkie\AppData\Local\Microsoft\Windows\UsrClass.dat

V případě pokusu o otevření hive dostanete tuto chybu:



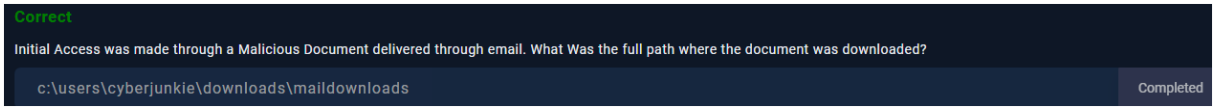
Podržte však **SHIFT** během otevření hive

Nyní, když je hive úspěšně zaveden, přejděte na adresář Downloads. Objevíte adresář **MailDownloads** a uvnitř něj adresář Downloads.



Dokument byl nalezen v adresáři *MailDownloads folder* a plná cesta je:

C:\Users\CyberJunkie\Downloads\MailDownloads



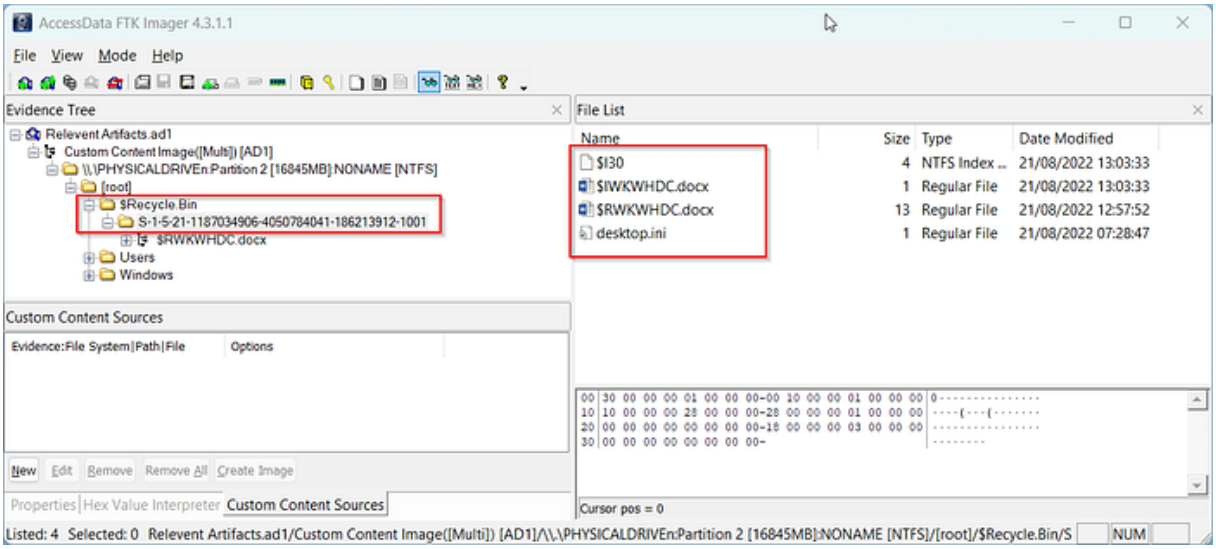
2. Jaký je název dokumentu? (Dokument, který byl doručen prostřednictvím phishingu)

Normálním chováním malwaru je dělat svou práci a smazat se, čímž se stane neobnovitelným.

Takže artefakt, který má být analyzován, se týká Recycle Bin

Nástroj použitý k tomuto účelu je **RBCmd**

Vstupní soubor pro RBCmd je soubor $I files, je třeba přejít do Recycle bin a nalézt soubor $I:



Tam jsou dva soubory:

- $IWKWHDC
- $RWKWHDC

Zkusme dát obojí jako vstup do RBCmd:

```
D:\Windows Forensics>.\RBCmd
Description:
  RBCmd version 1.5.0.0

  Author: Eric Zimmerman (saericzimmerman@gmail.com)
  https://github.com/EricZimmerman/RBCmd

  Examples: RBCmd.exe -f "C:\Temp\INFO2"
            RBCmd.exe -f "C:\Temp\$I3VPA17" --csv "D:\csvOutput"
            RBCmd.exe -d "C:\Temp" --csv "c:\temp"

            Short options (single letter) are prefixed with a single dash. Long commands


Usage:
  RBCmd [options]

Options:
  -d <d>          Directory to recursively process. Either this or -f is required
  -f <f>          File to process. Either this or -d is required
  -q              Only show the filename being processed vs all output. Useful to speed u
  --csv <csv>     Directory to save CSV formatted results to. Be sure to include the full
  --csvf <csvf>   File name to save CSV formatted results to. When present, overrides def
  --dt <dt>       The custom date/time format to use when displaying time stamps. See htt
                  options. Default is: yyyy-MM-dd HH:mm:ss [default: yyyy-MM-dd HH:mm:ss]
  --debug         Show debug information during processing [default: False]
  --trace         Show trace information during processing [default: False]
  --version       Show version information
  -?, -h, --help  Show help and usage information
```

Příkaz má tvar: RBCmd -f <file>

Název dokumentu je: Security Awareness.docx

3.*Jaké je jméno stageru, který se připojil k serveru C2 útočníka (úplná cesta\název)*

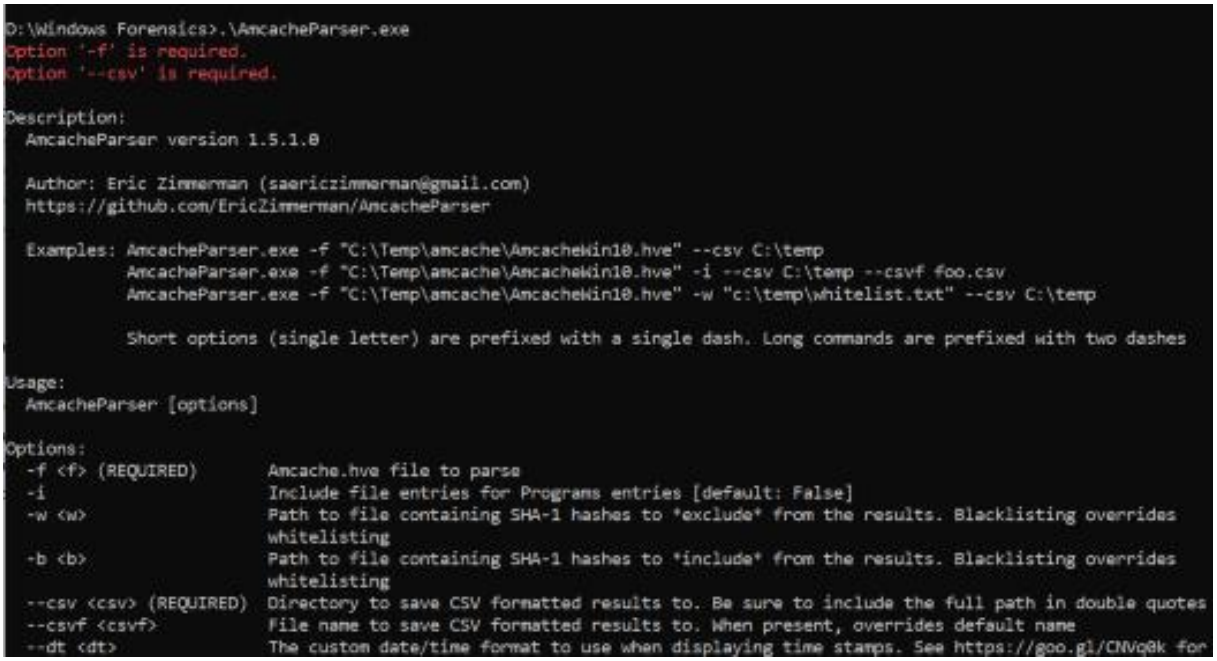
Stager vytváří komunikační kanál mezi útočníkem a obětí a čte datovou část fáze, která se má spustit na vzdáleném hostiteli.

Soubor Amcache.hve je soubor registru, který ukládá informace o spuštěných aplikacích.

Artefakt k analýze je Amcache.

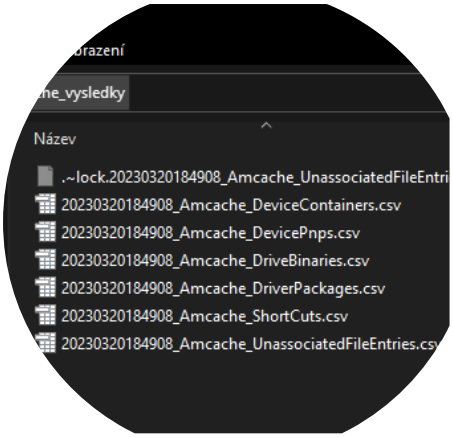
Umístění Amcache.hve je: **<logická jednotka>:__._PHYSICALDRIVEn_Partition 2 [16845 MB]_NONAME [NTFS]\[root]\Windows\appcompat\Programs\Amcache.hve**

K tomu slouží nástroj **Amcache Parser**.



Použitý příkaz: AmcacheParser.exe -f Amcache.hve — csv <directory>

V adresáři budete mít několik souborů csv



Ty, který nás zajímají, jsou Unassociated File Entries

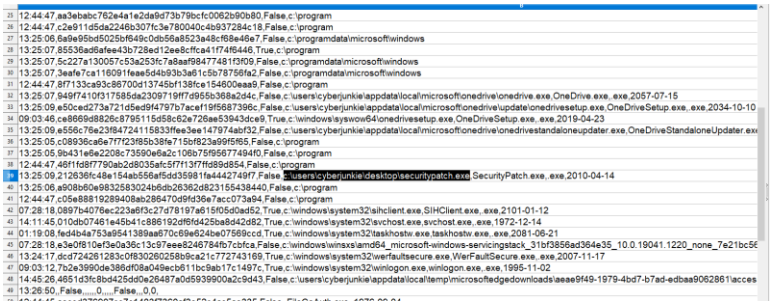
*Unassociated File Entries je program nebo aplikace, která **není** spojena s žádným známým zdrojem, jako je Microsoft, Google, Adobe, HP atd., takže pokud hledáte podezřelé soubory, je velká šance, že je najdete zde.*

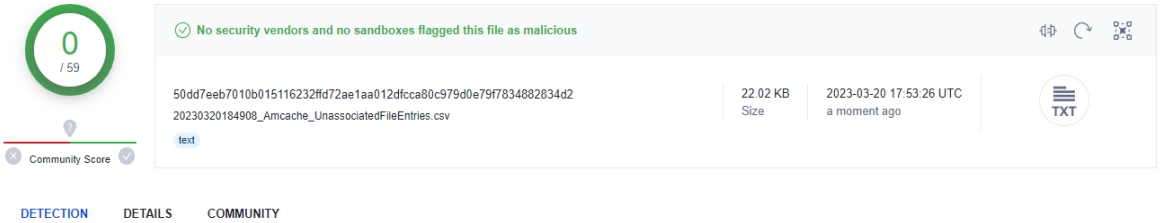
Při procházení názvů v souboru csv se nachází podezřelý soubor „**Security Patch.exe**“

Unassocia	00061baa	########	c08936ca	FALSE	c:\program files\pchealthcheck\pchealthcheck.e› PCHealthCheck.exe .exe
Unassocia	0006ba7e	########	9b431e6e	FALSE	c:\program files\pchealthcheck\pchealthcheckbr PCHealthCheckBroker.exe .exe
Unassocia	0006cb9d	########	46f1fd8f7	FALSE	c:\program files (x86)\microsoft\edgecore\104.0 pwahelper.exe .exe
Unassocia	00065f5d1	########	212636fc4	FALSE	c:\users\cyberjunkie\desktop\securitypatch.exe SecurityPatch.exe .exe
Unassocia	000671f85	########	a908b60e	FALSE	c:\program files (x86)\microsoft\edgeupdate\ins setup.exe .exe
Unassocia	00069621(	########	c05e8881	FALSE	c:\program files (x86)\microsoft\edgecore\104.0 setup.exe .exe

20221207173311_Amcache_UnassociatedFileEntries.csv

Existuje také SHA1 souboru exe uvedeného v souboru csv. Můžeme to zkusit prohledat v Virustotalu a zjistit, jestli nenajdeme nějakou nápovědu, ale pro tento soubor není žádná.





Toto je metasploit stager[5]

Plná cesta je: **c:\users\cyberjunkie\desktop\securitypatch.exe**

[5]Stager je malý spustitelný soubor, který je počátečním užitečným zatížením. Jedná se o relativně malý kousek kódu, který se provádí za účelem přípravy na mnohem větší a schopnější užitečné zatížení známé jako stage payload.

4. Útočník manipuloval s časovými razítky MACB spustitelného programu stager, aby zmátl analytiky. Analyzujte časová razítka stageru a ověřte původní časové razítko a zfalšované. (ORIGINAL TIMESTAMP : TAMPERED TIMESTAMP)

Toto se nazývá **Timestomping**

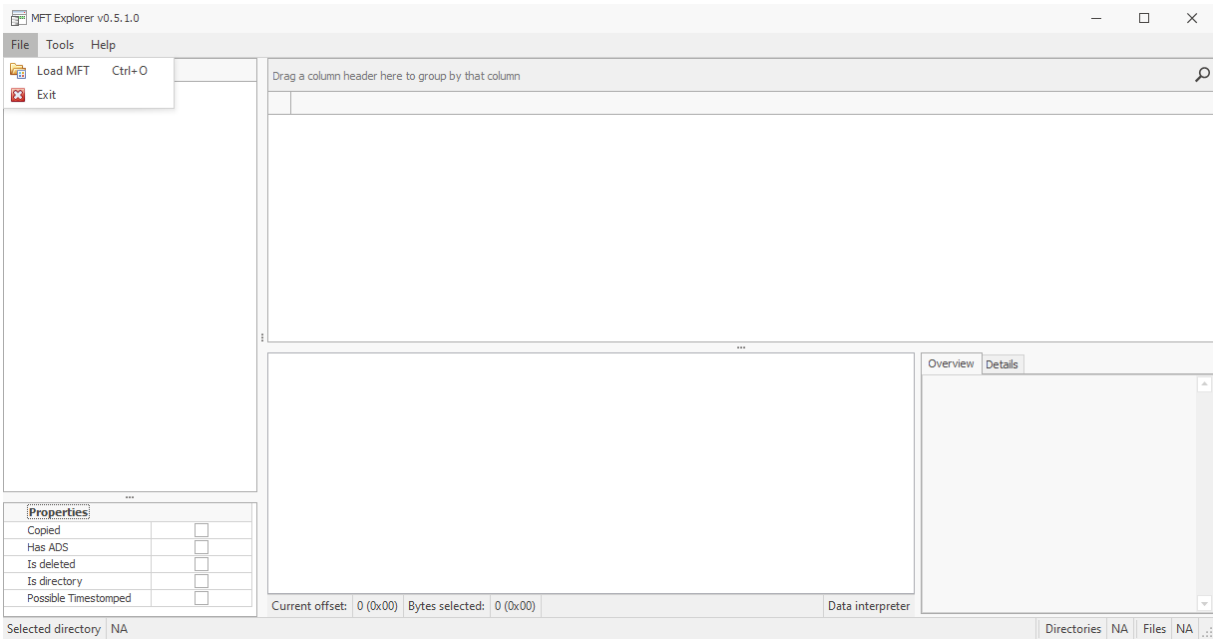
Timestomping odkazuje na **změnu časových razítek souboru v systému souborů NTFS**. Tuto taktiku běžně používají aktéři hrozeb, aby skryli své nástroje v souborovém systému oběti.

Pro manipulaci s časem lze použít nástroje jako timestomp. Zmanipulovaná časová razítka se však zpracovávají na úrovni uživatele, nikoli na úrovni jádra. Takže informace o původním časovém razítku jsou vždy správně uloženy na úrovni jádra.

Artefaktem je **MFT**

Master File Table (MFT) nebo $MFT lze považovat za jeden z nejdůležitějších souborů v systému souborů NTFS. Uchovává záznamy o všech souborech na svazku, umístění souborů v adresáři, fyzické umístění souborů na disku a metadata souborů.

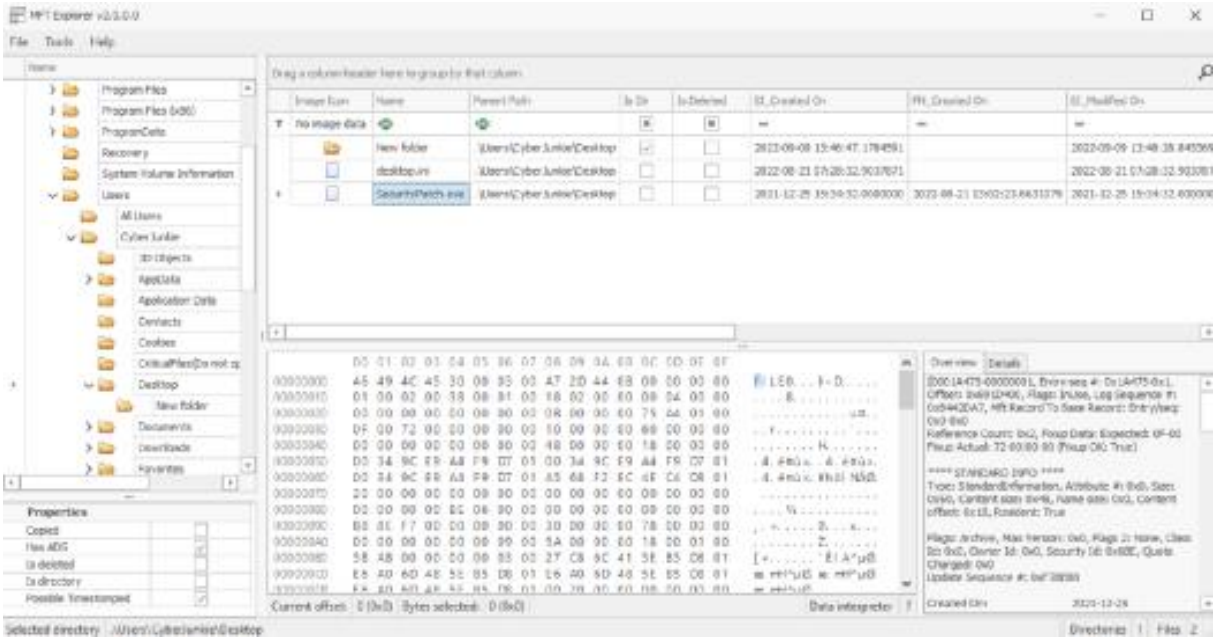
K tomu se používá: **MFT Explorer**



[16845MB]_NONAME [NTFS]\[root]\$MFT

Známe umístění stageru (security patch.exe) (viz poslední otázka)

Vyhledejte stager v MFT Explorer



$Standard_Information(SI) funguje na uživatelské úrovni a $FILE_Name(FN) funguje na úrovni jádra

SI_Created On	FN_Created On	SI_Modified On	FN_Modified On	SI_Last Accessed
2022-09-09 13:46:47.1784591		2022-09-09 13:48:28.8453693	2022-09-09 13:46:47.1784591	2022-09-09 13:48:28.8453693
2022-08-21 07:28:32.9037871		2022-08-21 07:28:32.9037871		2022-09-09 13:20:26.8904295
2021-12-25 15:34:32.0000000	2022-08-21 13:02:23.6631079	2021-12-25 15:34:32.0000000	2022-08-21 13:02:35.4127078	2022-09-09 13:20:26.9232293

Řešení

{2022–08–21 13:02:23.66 : 2021–12-25 15:34:32}

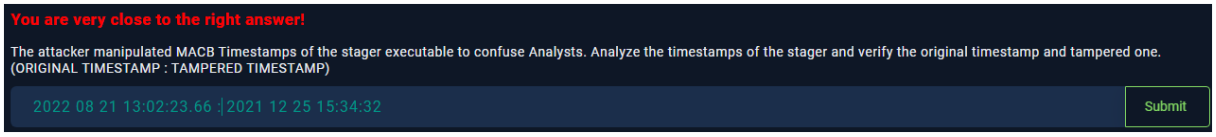
FN je původní časové razítko a SI je upravené časové razítko

Původní časové razítko: 2022–08–21 13:02:23.66

Upravené časové razítko: 2021–12–25 15:34:32

Odpověď: **{2022–08–21 13:02:23.66 : 2021–12-25 15:34:32}**

Poznámka: Zde narazíte na problém s odesláním odpovědi na platformě

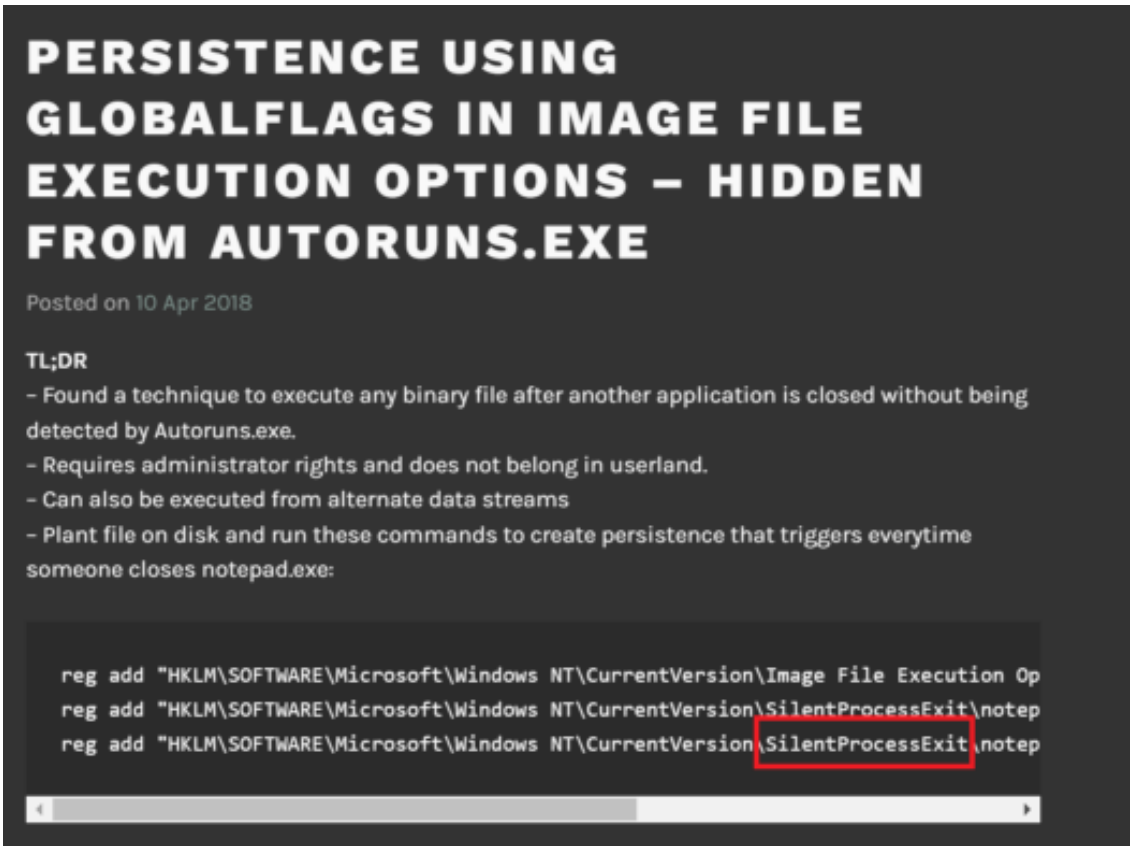


5. *Útočník nastavil perzistenci (odolnost) manipulací s klíči registru. Vše, co víme, je, že k nastavení persistence byla použita technika souborů image GlobalFlags*[6]*. Při ukončení určitého procesu je spuštěn spustitelný soubor persistence útočníka. Jak se ten proces jmenuje?*

[6] Obslužný program Global Flags (gflags.exe) poskytuje jednoduchý způsob nastavení určitých klíčů v systémovém registru, úpravu nastavení jádra běžícího systému a změnu nastavení pro soubory image.

Persistence (udržení) je technika, kterou často používají profesionálové a protivníci červeného týmu k udržení spojení s cílovými systémy po přerušeních, která jim mohou přerušit přístup.

Technika perzistence v kontextu je technika souborů images Global Flags

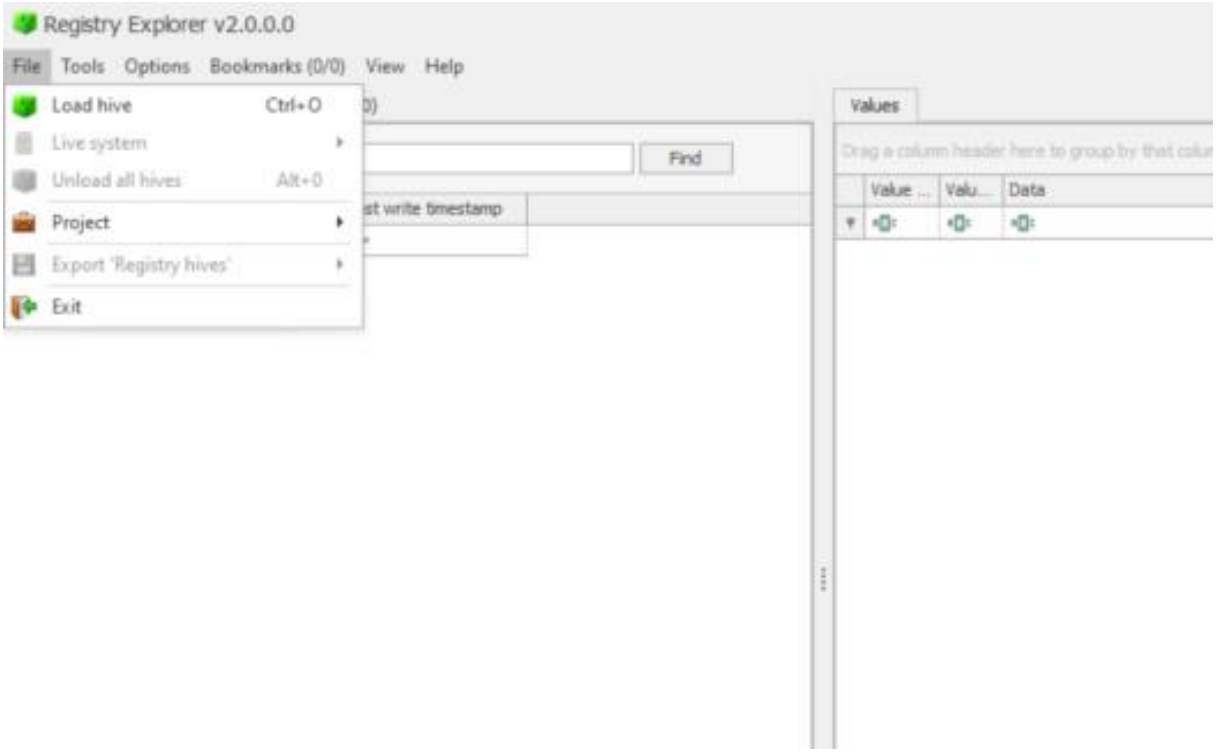


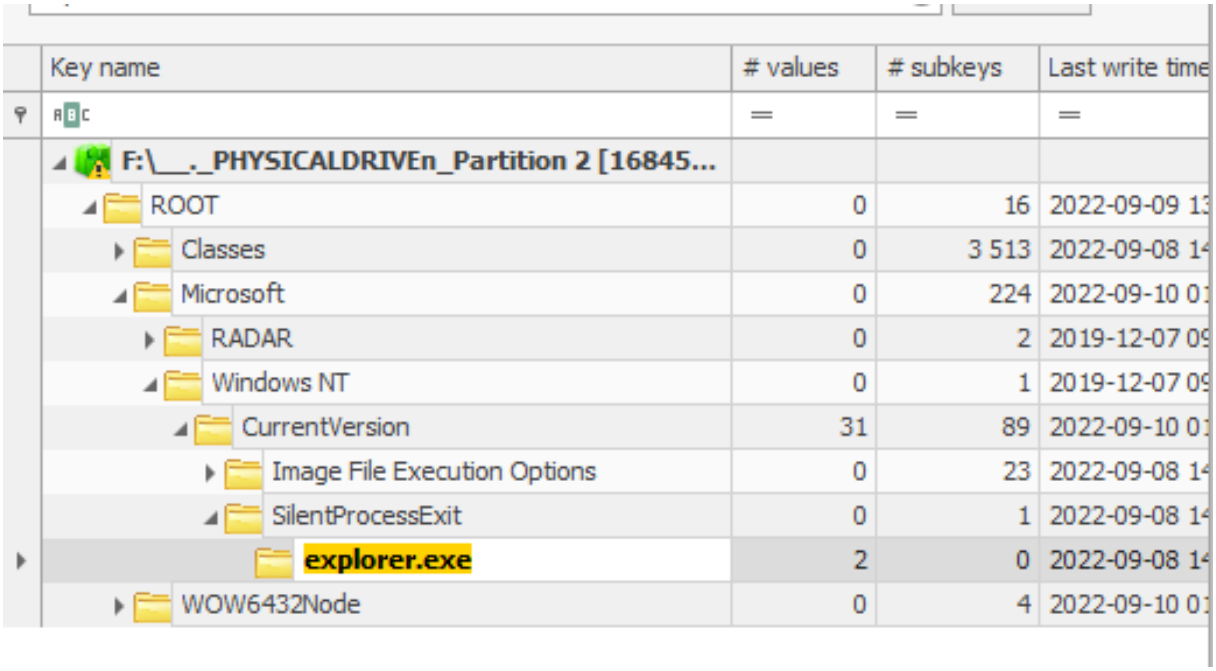
https://oddvar.moe/2018/04/10/persistence-using-globalflags-in-image-file-execution-options-hidden-from-autoruns-exe/

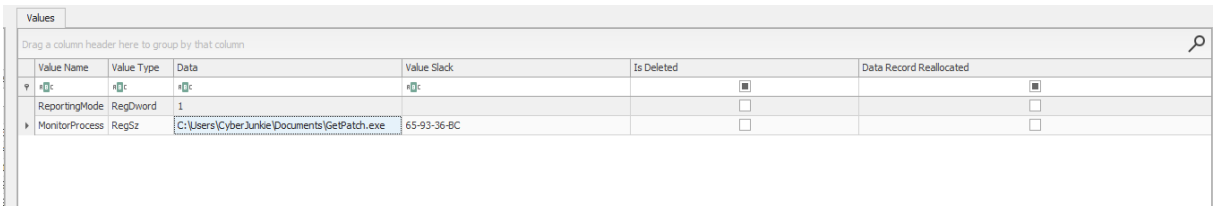
Upravený klíč registru je HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit

Použitým nástrojem je Registry Explorer

Podregistry registru jsou umístěny v adresáři na <logická jednotka>:__._PHYSICALDRIVEn_Partition 2 [16845 MB] _NONAME [NTFS]\[root]\Windows\System32\config\ directory



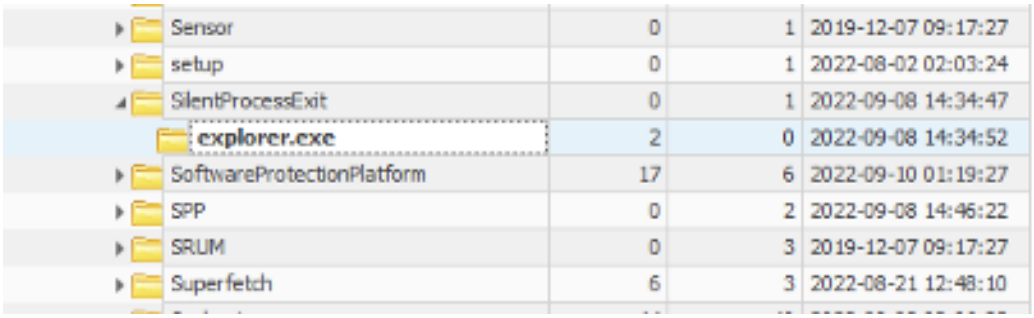




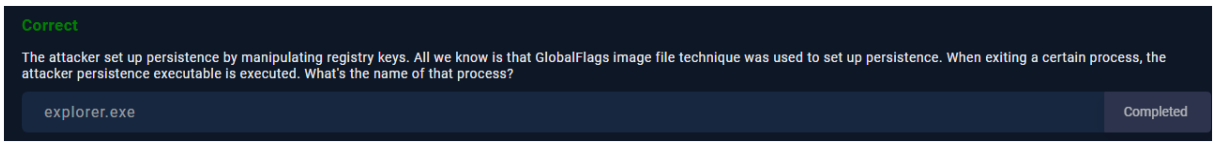
Načtěte registr **Software**

Pokud se při otevření hive zeptá na načtení špinavého hive, ignorujte to a načtěte hive

Vyhledejte **ROOT\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit**



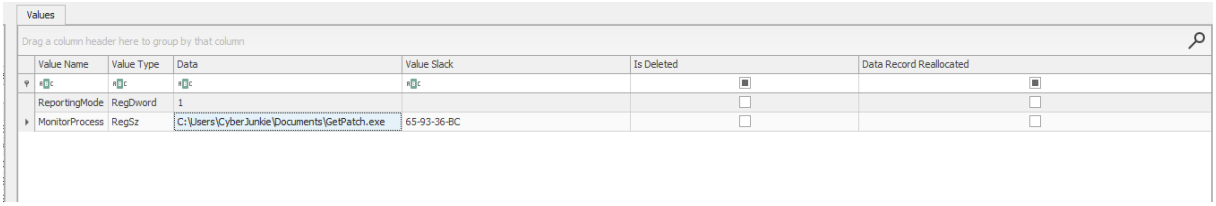
Název procesu je explorer.exe



6. Jaká je úplná cesta vedle názvu spustitelného souboru, který je nastaven pro persistenci? (FULLPATH\Název souboru)

explorer.exe je spustitelný soubor, který je nastaven pro persistenci

Po zavření explorer.exe se spustí GetPatch.exe



Plná cesta: C:\Users\CyberJunkie\Documents\GetPatch.exe

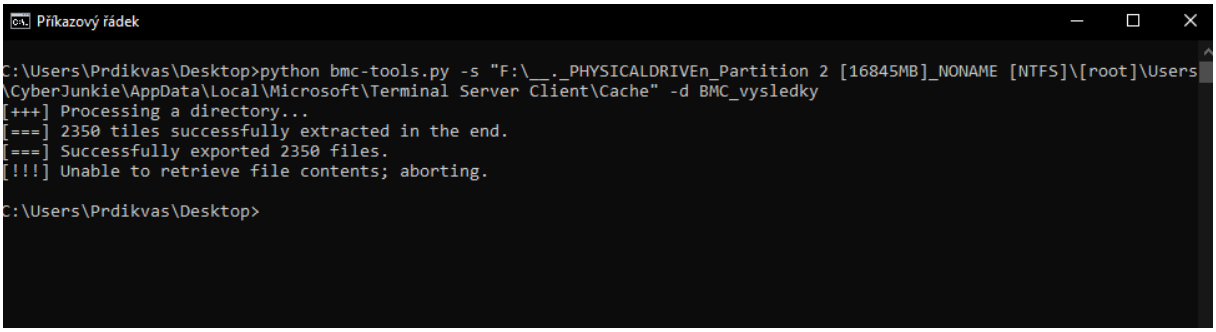
7.*Útočník se přihlásil přes RDP a poté provedl laterální pohyb. Útočník přistupoval k zařízení připojenému k interní síti přes RDP. Jaký příkaz byl spuštěn na cmd po úspěšném RDP do jiného počítače se systémem Windows*?

Útočník provedl boční pohyb, použil infikovaný počítač k přihlášení k jinému počítači přes RDP. Kdykoli vstupujeme přes RDP do počítače, malé bitmapové obrázky jsou uloženy do cache na počítači, ze kterého jsme iniciovali RDP připojení (klient). Ty jsou uloženy v cache souborech v adresáři Windows Terminal Services. Můžeme tedy analyzovat bitmapové obrázky z tohoto client cache souboru a vidět doslova malé obrázky.

Umístění cache adresáře: **<logical drive>:__._PHYSICALDRIVEn_Partition 2 [16845MB]_NONAME [NTFS]\[root]\Users\CyberJunkie\AppData\Local\Microsoft\Terminal Server Client\Cache**

Pro tento skript bmc-tools.py lze použít https://github.com/ANSSI-FR/bmc-tools

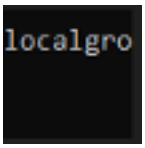
příkaz: **python bmc-tools.py -s “<Cache directory>” -d <directory>**



Poznámka: Adresář by měl existovat, např. v podobě rdp_output

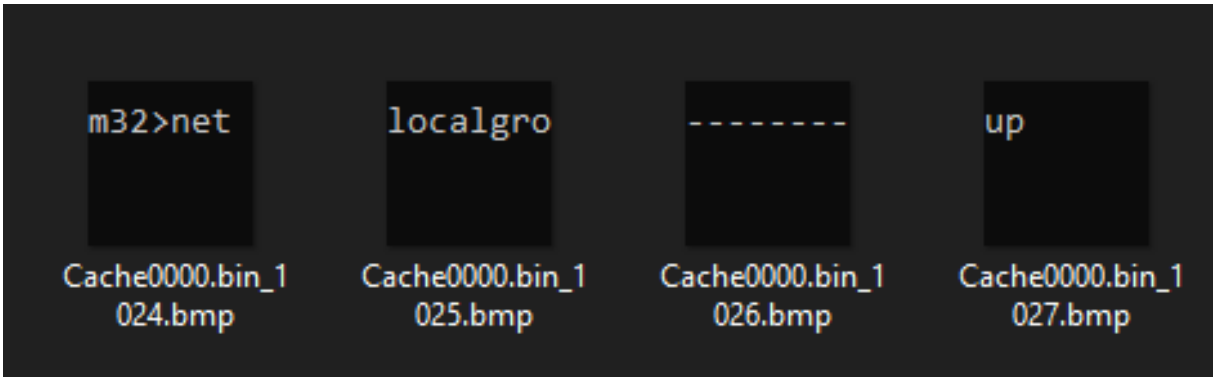
Interakci útočníka se strojem lze vidět v jednotlivývh bitmapách:

:
Cache0000.bin_1024



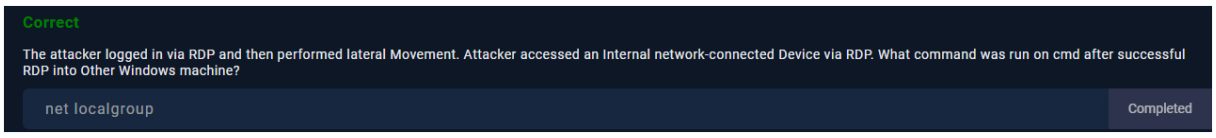
Cache0000.bin_1025

Sdruženo

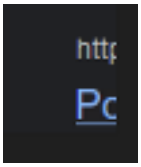


Toto je první příkaz, který útočník provedl v **net localgroup**

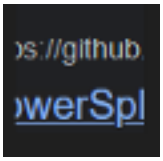
Tento příkaz se používá ke zjištění přehledu dostupných skupin



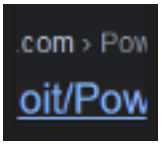
8.Útočník se pokusil stáhnout nástroj z prohlížeče uživatele v tomto druhém počítači. Jaký je název nástroje? (jméno.přípona)



Cache0000.bin_2041

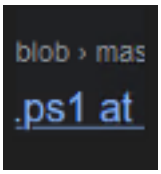


Cache0000.bin_2040



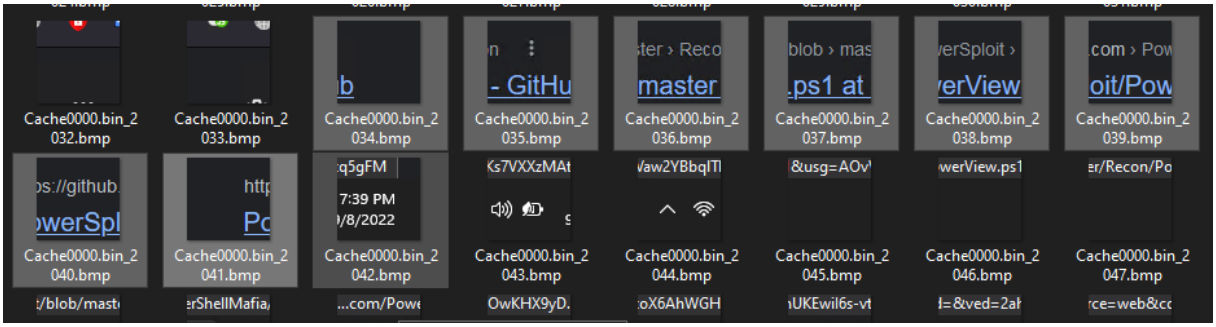
Cache0000.bin_2039

Cache0000.bin_2038

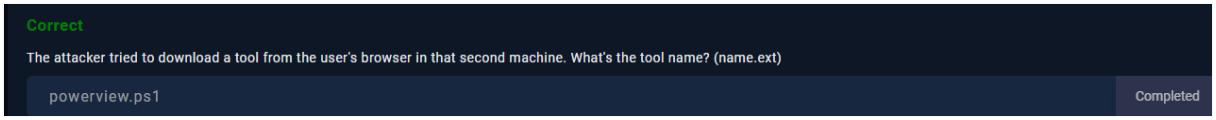


Cache0000.bin_2037

Když dáme dohromady PowerSploit/PowerView.ps1[7], je vidět co je co.



Powesploit je framework (rámec) a PowerView.ps1 je nástroj



[7] Ize také provést vyhledávání Google s dotazem jako „PowerView github“, protože z bitmap je vidět, že se jedná o úložiště github.

9.Jaký příkaz byl proveden, aby došlo k eskalaci oprávnění?

To lze zjistit analýzou protokolů událostí okna pomocí skriptu DeepBlue[8] powershell (https://github.com/sans-blue-team/DeepBlueCLI/blob/master/DeepBlue.ps1)

Cesta k souborům protokolu: ***<logická jednotka>:__._PHYSICALDRIVEn_Partition 2 [16845 MB]_NONAME [NTFS]\[root]\Windows\System32\winevt\Logs***

naklonujte úložiště DeepBlueCLI (nebo) stáhněte úložiště DeepBlueCLI jako soubor zip

cd do adresáře DeepBlueCLI (DeepBlueCLI-master, pokud jste si repo stáhli jako soubor zip)

Zkopírujte příslušné soubory protokolů (System, Setup, Windows PowerShell) a spusťte DeepBlue.ps1

příkaz: **powershell .\DeepBlue.ps1 <log soubor>**

Příkaz, který byl proveden a vedl k eskalaci oprávnění, lze nalézt v systémovém log souboru

```
D:\Windows Forensics\DeepBlueCLI-master>powershell .\DeepBlue.ps1 ..\System.evtx


Date    : 21-08-2022 18:44:42
Log     : System
EventID : 7045
Message : Suspicious Service Command
Results : Service name: kyvckn
          Metasploit-style cmd with pipe (possible use of Meterpreter 'getsystem')

Command : cmd.exe /c echo kyvckn > \\.\pipe\kyvckn
Decoded :

Date    : 02-08-2022 07:36:23
Log     : System
EventID : 7030
Message : Interactive service warning
Results : Service name: Printer Extensions and Notifications
          Malware (and some third party software) trigger this warning
Command :
Decoded :
```

cmd.exe /c echo kyvckn > \\.\pipe\kyvckn

10.Jaký rámec použil útočník?

DeepBlue identifikoval příkaz eskalace oprávnění jako **get system**, což je příkaz meterpreteru, což je zátěž při útoku Metasploitem, který se používá pro eskalaci oprávnění.

[8] Skripty je třeba povolit.

Použitý rámec je **metasploit**

Shrnutí a závěr

Závěrem je třeba shrnout použití nástrojů:

- FTK imager
- ShellBagsExplorer
- RBCmd
- AMcacheParser
- MFTExplorer
- RegistryExplorer
- Bmc-tools
- DeepBlueCLI

Seznam použitých zdrojů

(Belhadjadji 2022) Belhadjadji Ahmed. Windows Forensics Challenge Walkthrough (LETSDEFEND). March 25 2022. Dostupné z: https://belcyber.medium.com/windows-forensics-challenge-walkthrough-letsdefend-dd7a8289b5a7

(Chandel 2020-1) Chandel, Raj. Forensic Investigation: Prefetch File. Hacking Articles, October 15, 2020. Dostupné z: https://www.hackingarticles.in/forensic-investigation-prefetch-file/

(Chandel 2020-2) Chandel, Raj. Forensic Investigation: Shellbags. Hacking Articles. October 26, 2020, Dostupné z: https://www.hackingarticles.in/forensic-investigation-shellbags/

(Lau 2022) LAU Lina. Defence Evasion Technique: Timestomping Detection – NTFS Forensics. INTERSECOS April 28 2022. Dostupné z: https://www.inversecos.com/2022/04/defence-evasion-technique-timestomping.html

(Metasploit 2023) Metasploit Documentation. Github 2023. Dostupné z: https://github.com/rapid7/metasploit-framework

(Offensive 2020) Offensive Techniques & Methodologies. January 13 2020. Dostupné z: https://pentestlab.blog/2020/01/13/persistence-image-file-execution-options-injection/

(RegRipper 2023) Using OSForensics with RegRipper. PassMark Software. Dostupné z: https://www.osforensics.com/faqs-and-tutorials/using-with-regripper.html

(Simmons 2022) Stephanie Simmons. Plumbing the Depths: ShellBags. SA Eric R. Zimmerman, 2022. Dostupné z: https://docplayer.net/61062180-Plumbing-the-depths-shellbags-sa-eric-r-zimmerman-https-binaryforay-blogspot.html

(Vijay 2022) Anantha Vijay. M. DFIR – Windows Forensics. Dec 8 2022. Dostupné z: https://medium.com/@vj35.cool/dfir-windows-forensics-bb49a9b8782c