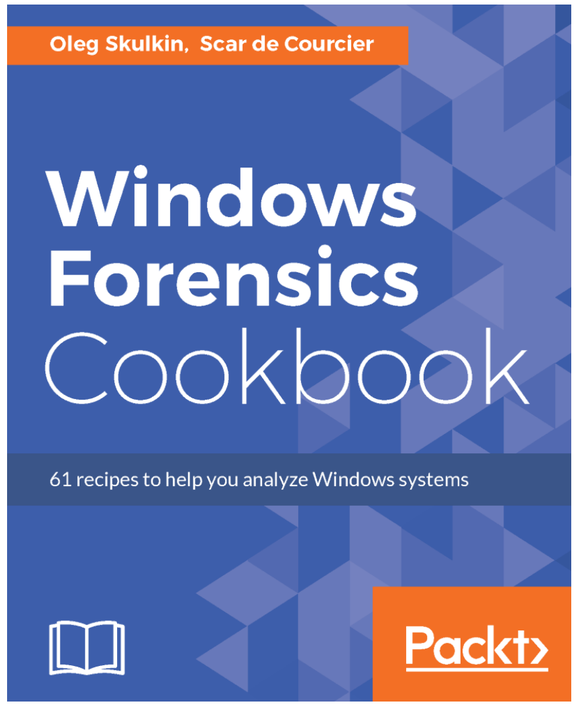
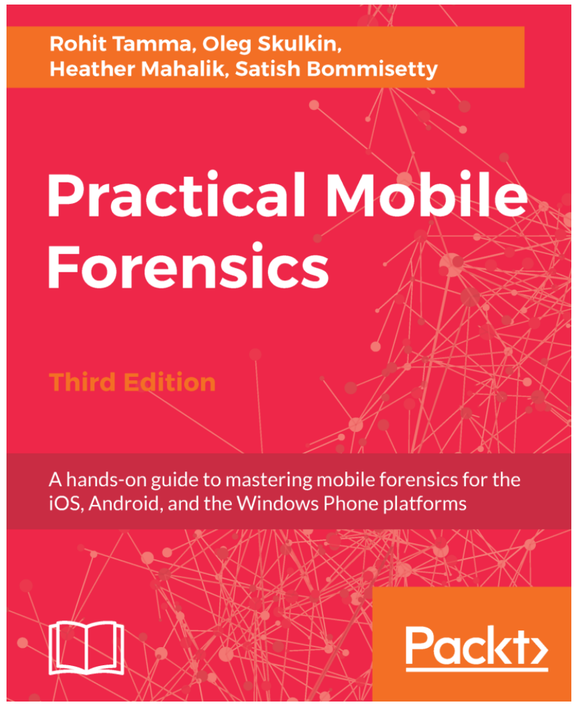
Обнаружение криминалистических артефактов функционирования ПО Metasploit в слепках оперативной памяти

whoami

Олег Скулкин | GCFA, MCFE, ACE | skulkin@group-ib.ru
Специалист по компьютерной криминалистике Group-IB





Публикации: Forensic Focus, eForensics Magazine, Cyber Forensicator, Хакер…

Почему криминалистическое исследование слепков оперативной памяти?

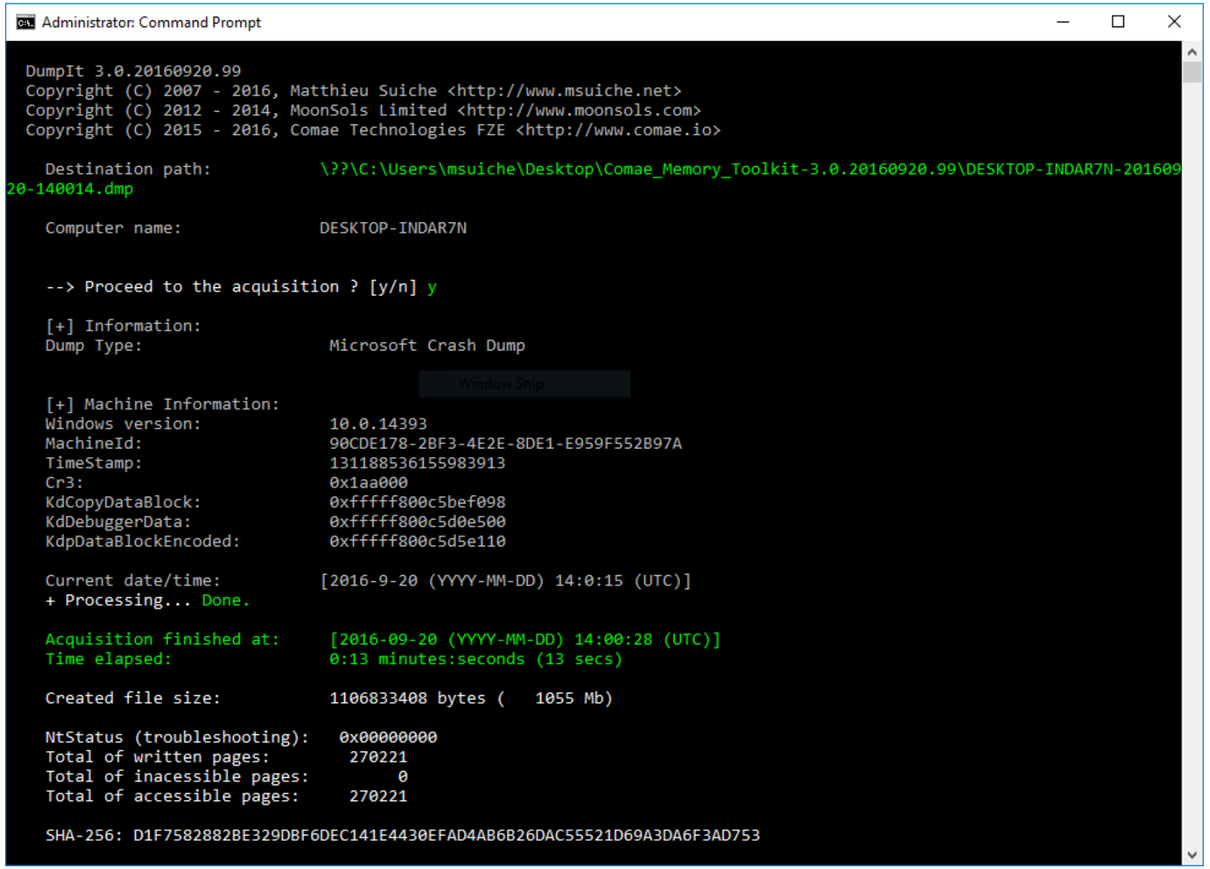
Дамп памяти может содержать массу полезных, с криминалистической точки зрения, артефактов:

- активные и завершенные процессы;
- сокеты, URL-ы, IP-адреса;
- открытые файлы;
- пароли, кэш, содержимое буфера обмена;
- ключи шифрования;
- сведения о конфигурации программного и аппаратного обеспечения;
- ключи реестра и записи журналов событий;
- много чего еще!

Как мне сделать слепок оперативной памяти?

Существует целый ряд инструментов, которые позволяют это сделать, вот некоторые из них:

- DumpIt
- WinPMEM
- Belkasoft Live RAM Capturer
- AccessData FTK Imager



Вроде, получилось! Что дальше?

Чаты и веб-активность

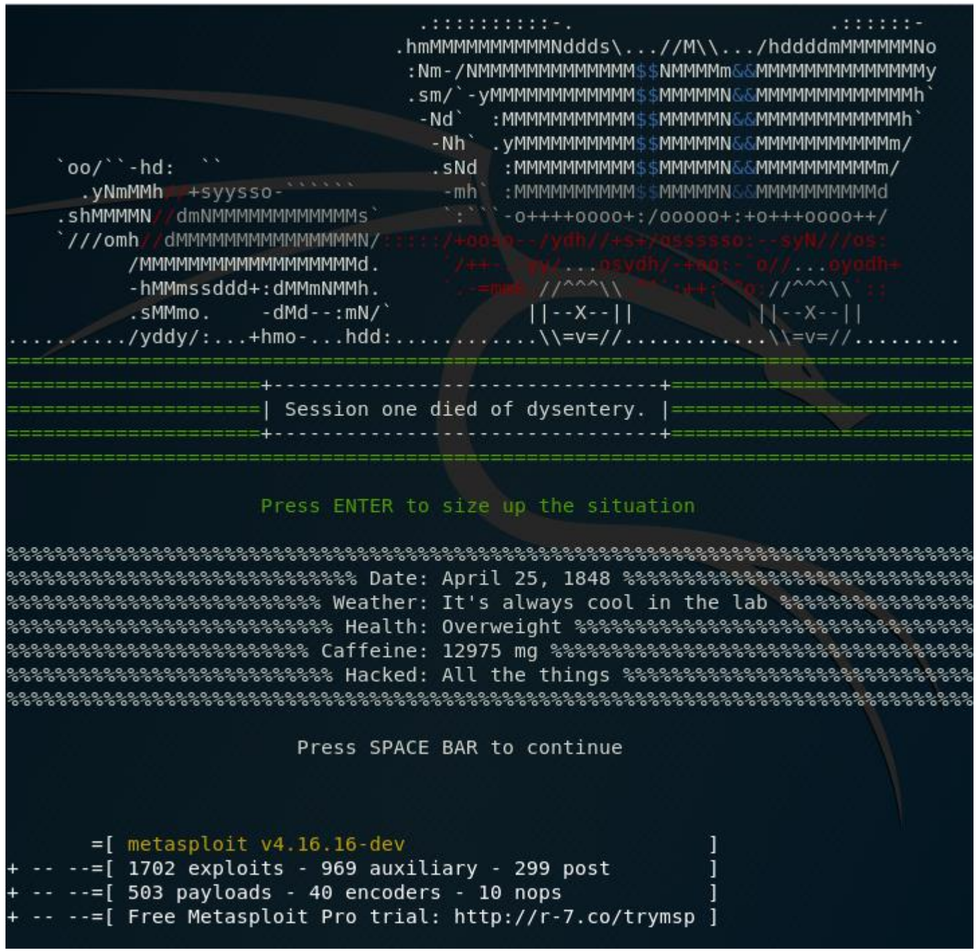
Belkasoft Evidence Center
Magnet AXIOM
BlackBag BlackLight

Вредоносная активность

Redline
Volatility Framework
Rekall Memory Forensic Framework

Meta-что?

Фреймворк, предназначенный для проведения тестов на проникновение.
Но, как показывает практика, инструкцию прочитали далеко не все.

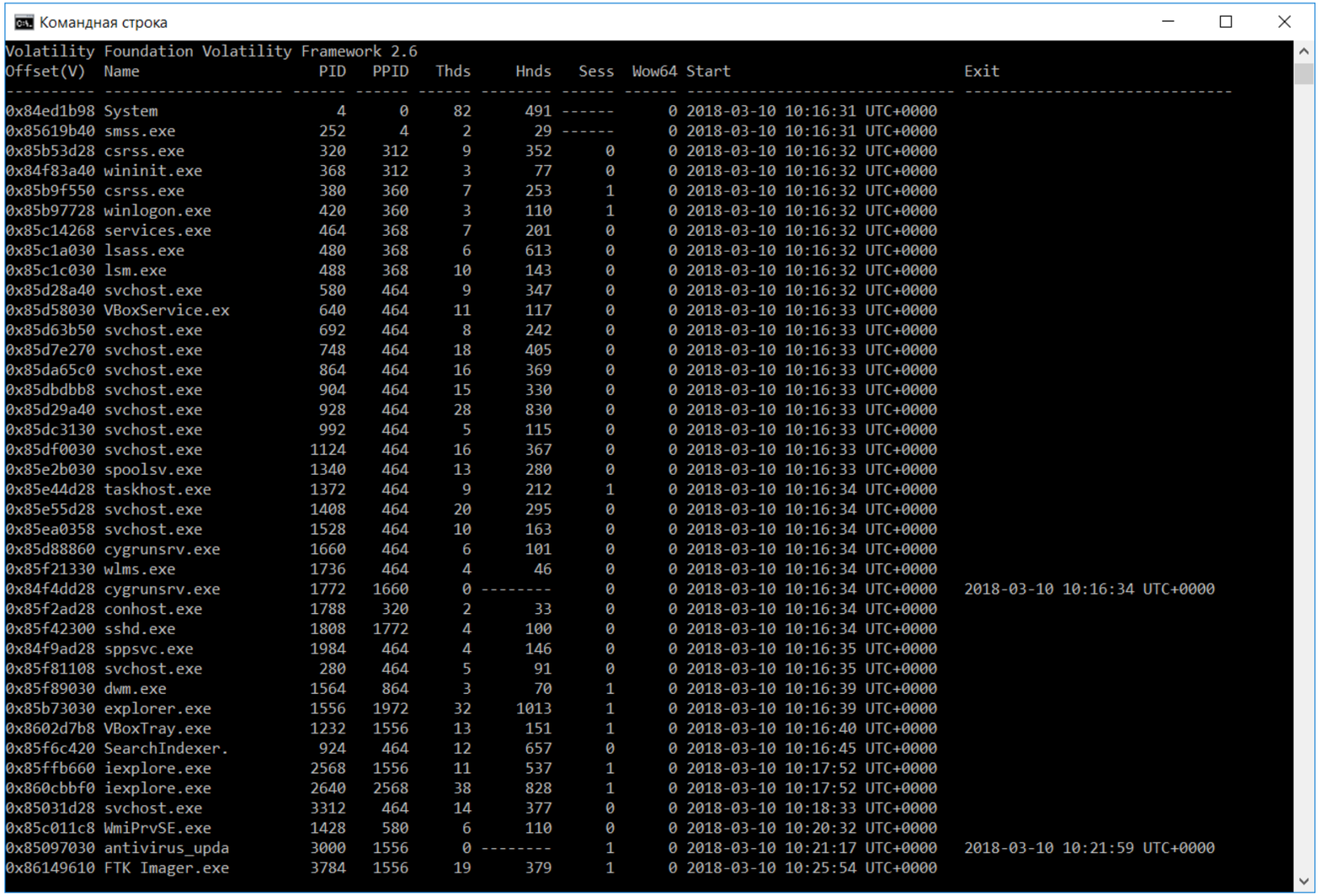


Соберем информацию о слепке

Командная строка

```
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\0136\Desktop\Share\meterpreter.mem)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x8276dc78L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x8276ed00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2018-03-10 10:26:18 UTC+0000
     Image local date and time : 2018-03-10 02:26:18 -0800
```

Ищем подозрительные процессы

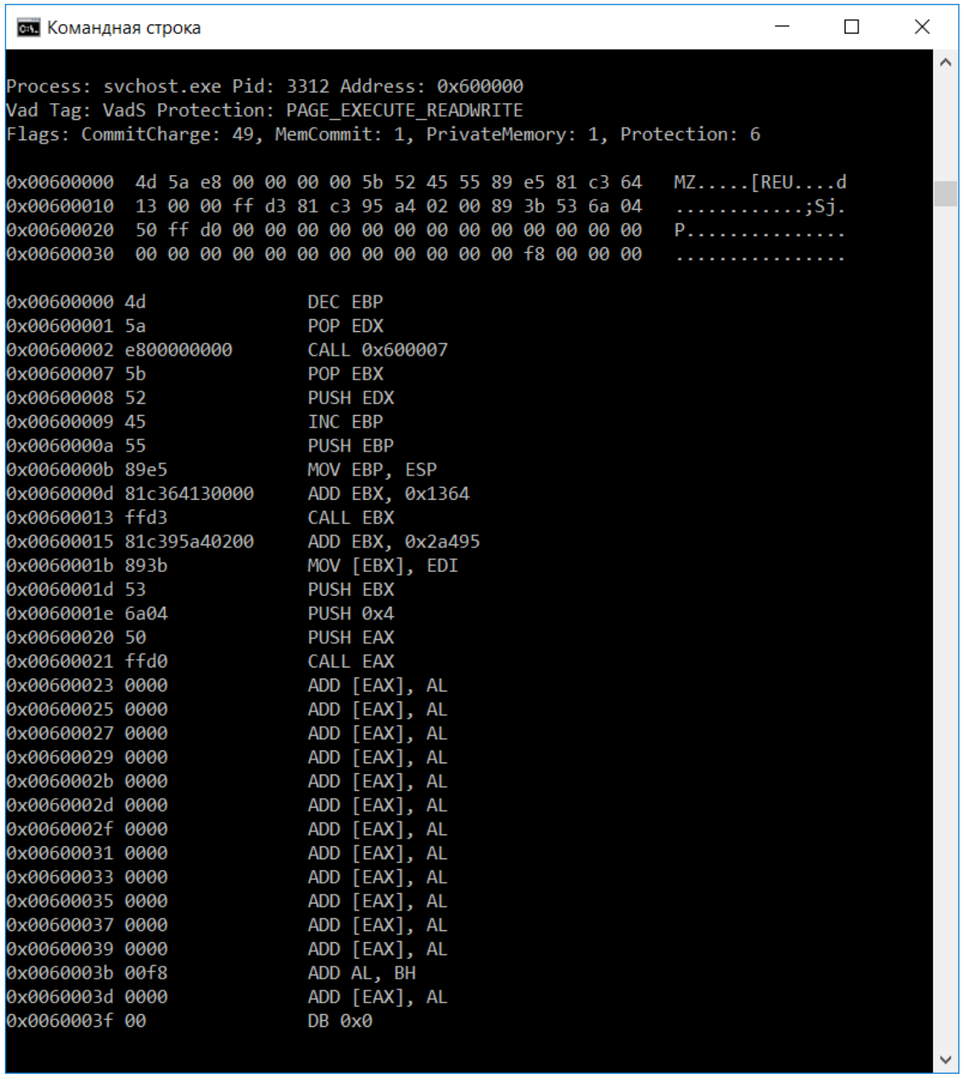


Посмотрим на сетевые соединения

Командная строка

```
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State          Pid      Owner          Created
0xdec8d610         UDPv4    0.0.0.0:56341                  *:*                                 1124     svchost.exe    2018-03-10 10:22:33 UTC+0000
0xdeca8be0         UDPv4    0.0.0.0:5355                   *:*                                 1124     svchost.exe    2018-03-10 10:19:19 UTC+0000
0xdecc8800         UDPv4    0.0.0.0:0                      *:*                                 1124     svchost.exe    2018-03-10 10:19:19 UTC+0000
0xdecc8800         UDPv6    :::0                           *:*                                 1124     svchost.exe    2018-03-10 10:19:19 UTC+0000
0xdece6260         UDPv4    0.0.0.0:60667                  *:*                                 1124     svchost.exe    2018-03-10 10:26:33 UTC+0000
0xdecf9208         UDPv4    0.0.0.0:0                      *:*                                 640      VBoxService.ex 2018-03-10 10:26:37 UTC+0000
0xded40d80         UDPv4    0.0.0.0:2096                   *:*                                 1124     svchost.exe    2018-03-10 10:17:56 UTC+0000
0xded83778         UDPv4    0.0.0.0:0                      *:*                                 2640     iexplore.exe   2018-03-10 10:23:01 UTC+0000
0xded83778         UDPv6    :::0                           *:*                                 2640     iexplore.exe   2018-03-10 10:23:01 UTC+0000
0xded86268         UDPv4    0.0.0.0:61424                  *:*                                 1124     svchost.exe    2018-03-10 10:26:27 UTC+0000
0xded880c8         UDPv4    0.0.0.0:0                      *:*                                 2640     iexplore.exe   2018-03-10 10:22:45 UTC+0000
0xded880c8         UDPv6    :::0                           *:*                                 2640     iexplore.exe   2018-03-10 10:22:45 UTC+0000
0xded884b8         UDPv4    0.0.0.0:55653                  *:*                                 1124     svchost.exe    2018-03-10 10:22:04 UTC+0000
0xdef30138         UDPv4    0.0.0.0:0                      *:*                                 280      svchost.exe    2018-03-10 10:16:35 UTC+0000
0xdef30138         UDPv6    :::0                           *:*                                 280      svchost.exe    2018-03-10 10:16:35 UTC+0000
0xdef3c298         UDPv4    0.0.0.0:0                      *:*                                 280      svchost.exe    2018-03-10 10:16:35 UTC+0000
0xdef9cd90         UDPv4    0.0.0.0:50497                  *:*                                 1124     svchost.exe    2018-03-10 10:26:33 UTC+0000
0xdefac6f0         UDPv4    192.168.1.89:137               *:*                                 4        System         2018-03-10 10:19:19 UTC+0000
0xdefb0d50         UDPv4    192.168.1.89:138               *:*                                 4        System         2018-03-10 10:19:19 UTC+0000
0xdec4d310         TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING      480      lsass.exe
0xdee276f0         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING      928      svchost.exe
0xdee276f0         TCPv6    :::49154                       :::0                 LISTENING      928      svchost.exe
0xdee28290         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING      928      svchost.exe
0xdee71410         TCPv4    0.0.0.0:22                     0.0.0.0:0            LISTENING      1808     sshd.exe
0xdee71410         TCPv6    :::22                          :::0                 LISTENING      1808     sshd.exe
0xdef138f0         TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING      480      lsass.exe
0xdef138f0         TCPv6    :::49156                       :::0                 LISTENING      480      lsass.exe
0xdef56248         TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING      4        System
0xdef56248         TCPv6    :::445                         :::0                 LISTENING      4        System
0xdef7e3b0         TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING      464      services.exe
0xdef7e3b0         TCPv6    :::49155                       :::0                 LISTENING      464      services.exe
0xdef7ff58         TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING      464      services.exe
0xdefb9c70         TCPv4    192.168.1.89:139               0.0.0.0:0            LISTENING      4        System
0xdf1709f0         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING      692      svchost.exe
0xdf172910         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING      692      svchost.exe
0xdf172910         TCPv6    :::135                         :::0                 LISTENING      692      svchost.exe
0xdf177228         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING      368      wininit.exe
0xdf177228         TCPv6    :::49152                       :::0                 LISTENING      368      wininit.exe
0xdf1777c0         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING      368      wininit.exe
0xdf19f8d8         TCPv4    0.0.0.0:22                     0.0.0.0:0            LISTENING      1808     sshd.exe
0xdf1a34f8         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING      748      svchost.exe
0xdf1a34f8         TCPv6    :::49153                       :::0                 LISTENING      748      svchost.exe
0xdf1a5f58         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING      748      svchost.exe
0xdec373a0         TCPv4    192.168.1.89:49424             192.168.1.39:4444    ESTABLISHED    -1
0xdfc9c8f8         UDPv4    0.0.0.0:60478                  *:*                                 1124     svchost.exe    2018-03-10 10:23:14 UTC+0000
```

Ищем внедренный код



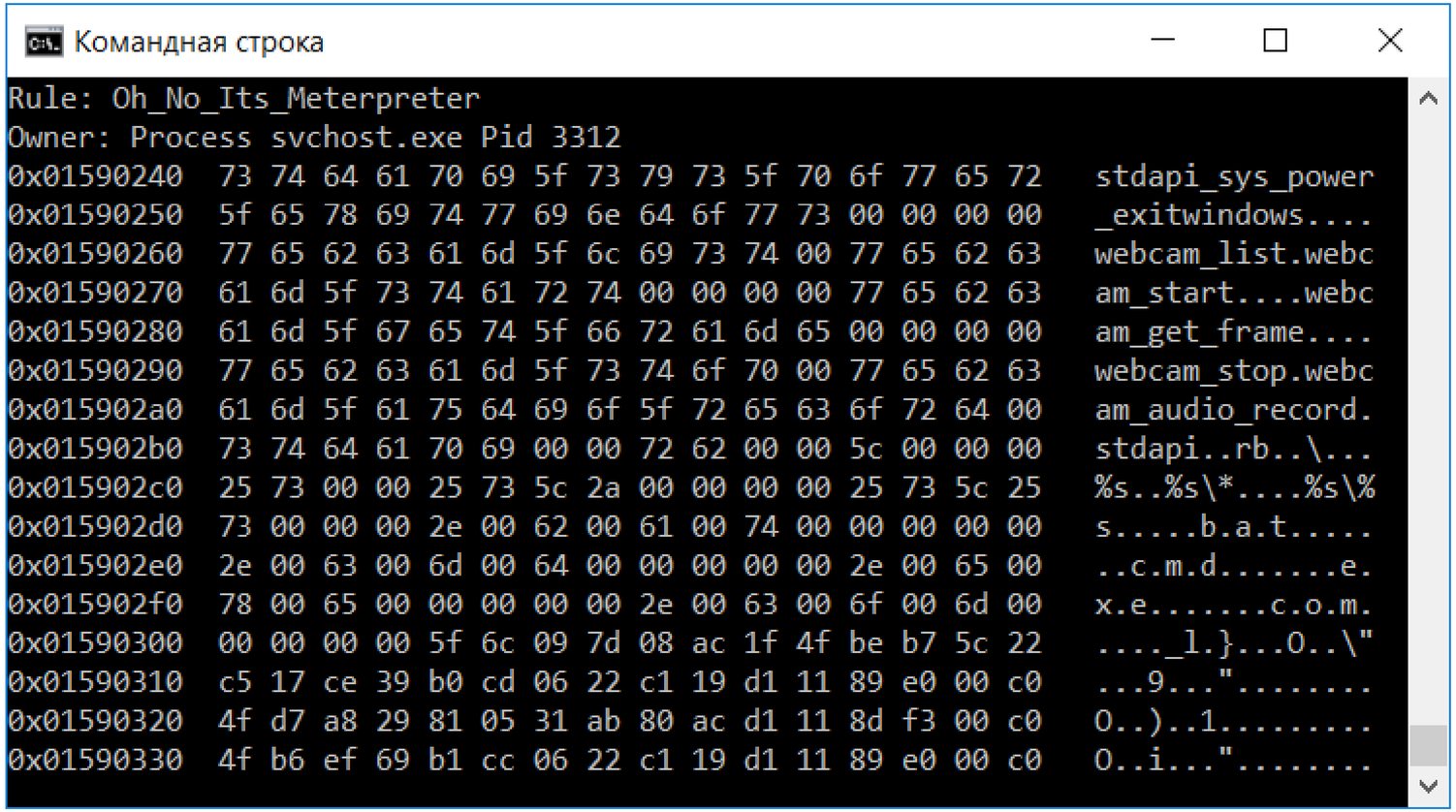
Кажется, все в порядке

AhnLab-V3	Clean	Antiy-AVL	Clean
Avast	Clean	Avast Mobile Security	Clean
AVG	Clean	Avira	Clean
AVware	Clean	Bkav	Clean
CAT-QuickHeal	Clean	CMC	Clean
Comodo	Clean	Cyren	Clean
DrWeb	Clean	ESET-NOD32	Clean
F-Prot	Clean	Fortinet	Clean
Jiangmin	Clean	K7AntiVirus	Clean
K7GW	Clean	Kingsoft	Clean
Malwarebytes	Clean	McAfee	Clean
McAfee-GW-Edition	Clean	NANO-Antivirus	Clean
nProtect	Clean	Palo Alto Networks	Clean
Panda	Clean	Qihoo-360	Clean

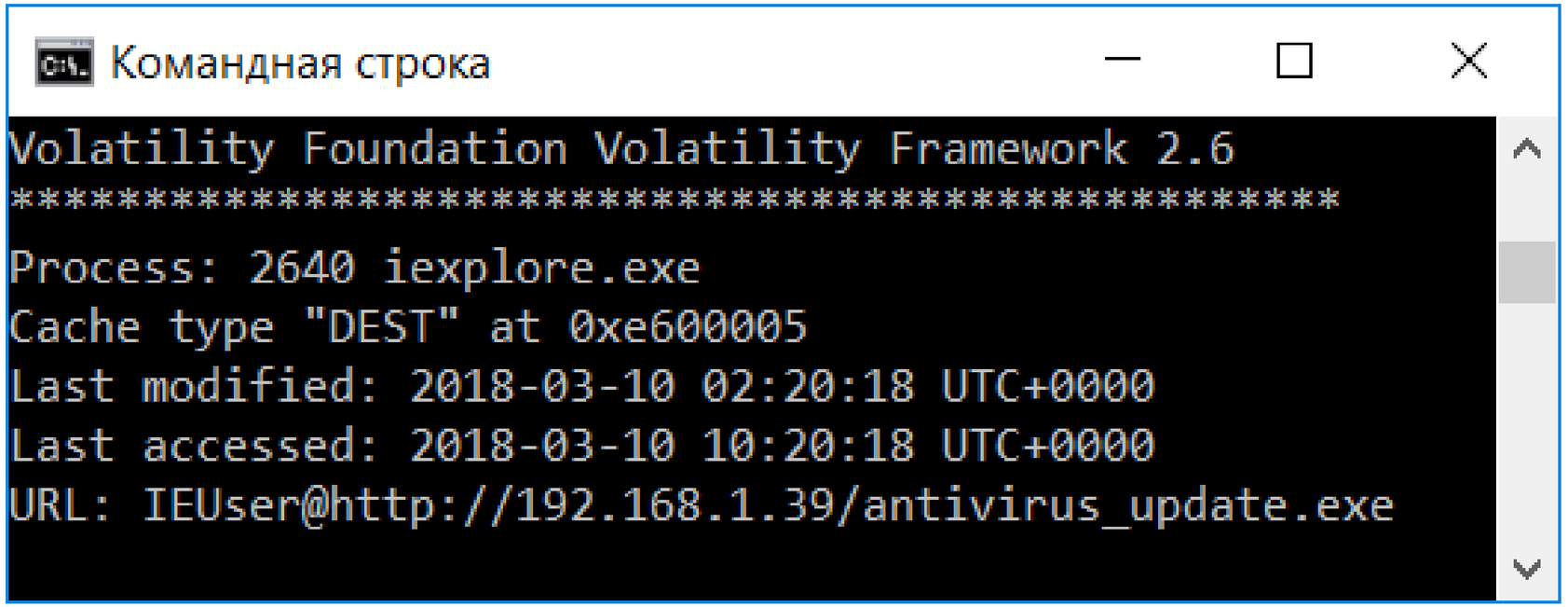
На самом деле нет

Ad-Aware	Gen:HackTool.MeterPreter.1	ALYac	Gen:HackTool.MeterPreter.1
Arcabit	Gen:HackTool.MeterPreter.1	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Gen:HackTool.MeterPreter.1	ClamAV	Win.Tool.MeterPreter-6294292-0
CrowdStrike Falcon	malicious_confidence_100% (D)	Cylance	Unsafe
eGambit	Trojan.Generic	Emsisoft	Gen:HackTool.MeterPreter.1 (B)
Endgame	malicious (moderate confidence)	eScan	Gen:HackTool.MeterPreter.1
F-Secure	Gen:HackTool.MeterPreter.1	GData	Gen:HackTool.MeterPreter.1
Ikarus	Trojan.Win64.Meterpreter	Kaspersky	HEUR:Trojan.Win32.Generic
MAX	malware (ai score=81)	Microsoft	Trojan:Win64/Meterpreter.A
Rising	HackTool.Swrort!1.6477 (CLASSIC)	Sophos ML	heuristic

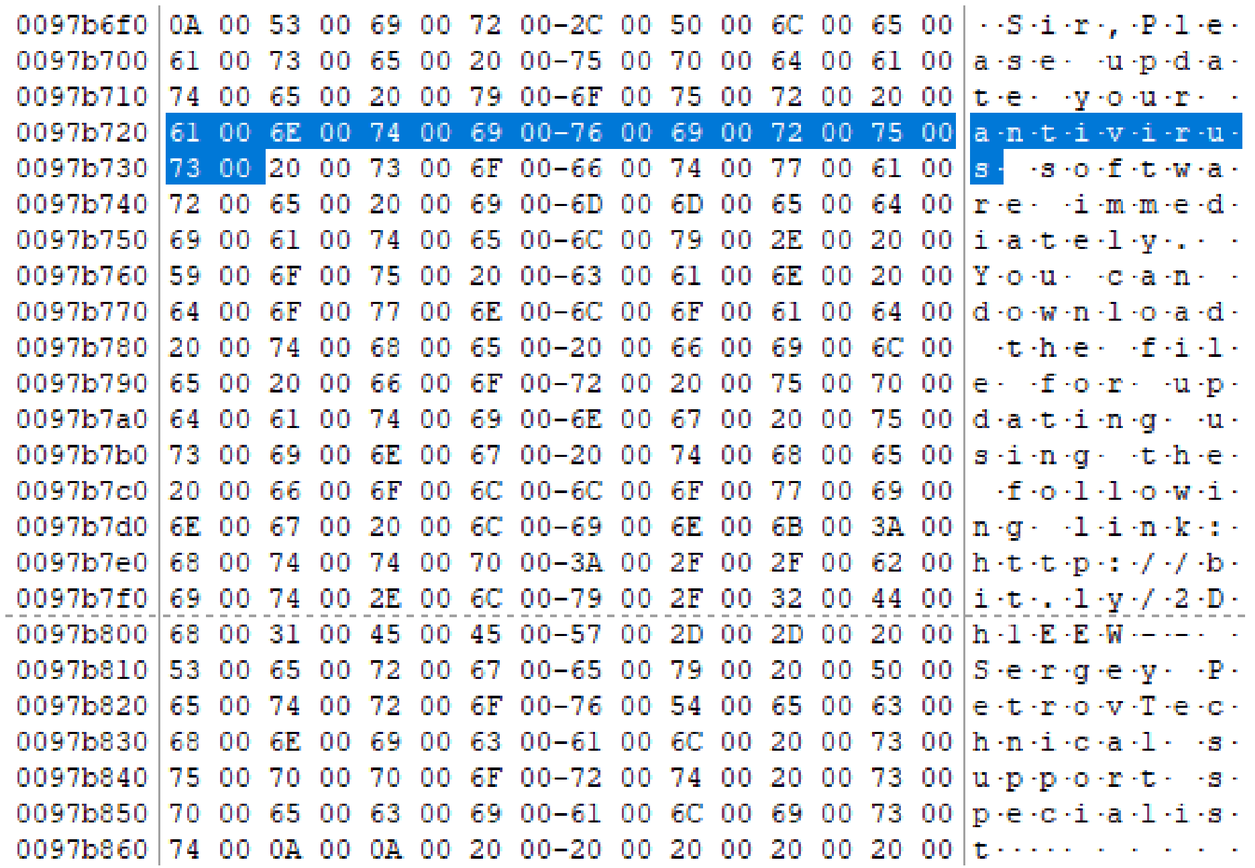
Можно еще быстрее



Откуда оно взялось!?

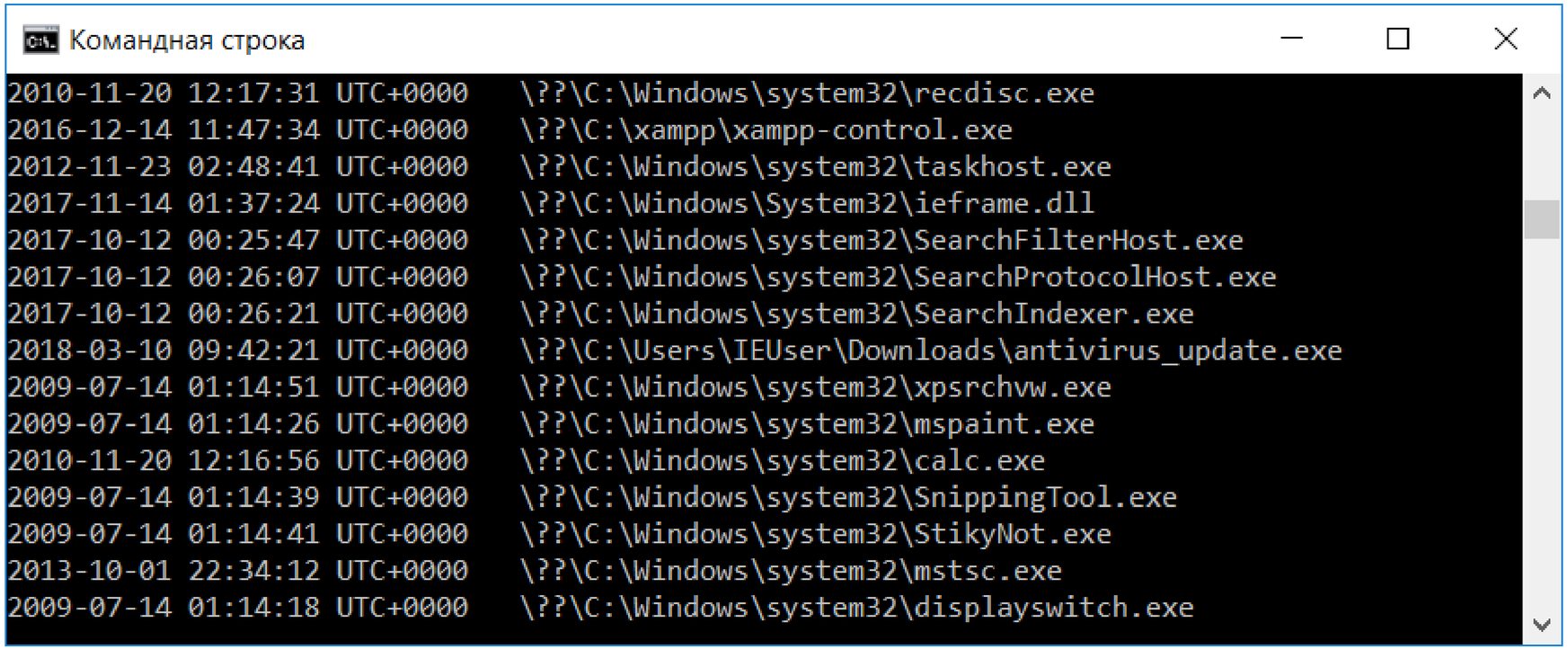


Копнем глубже!

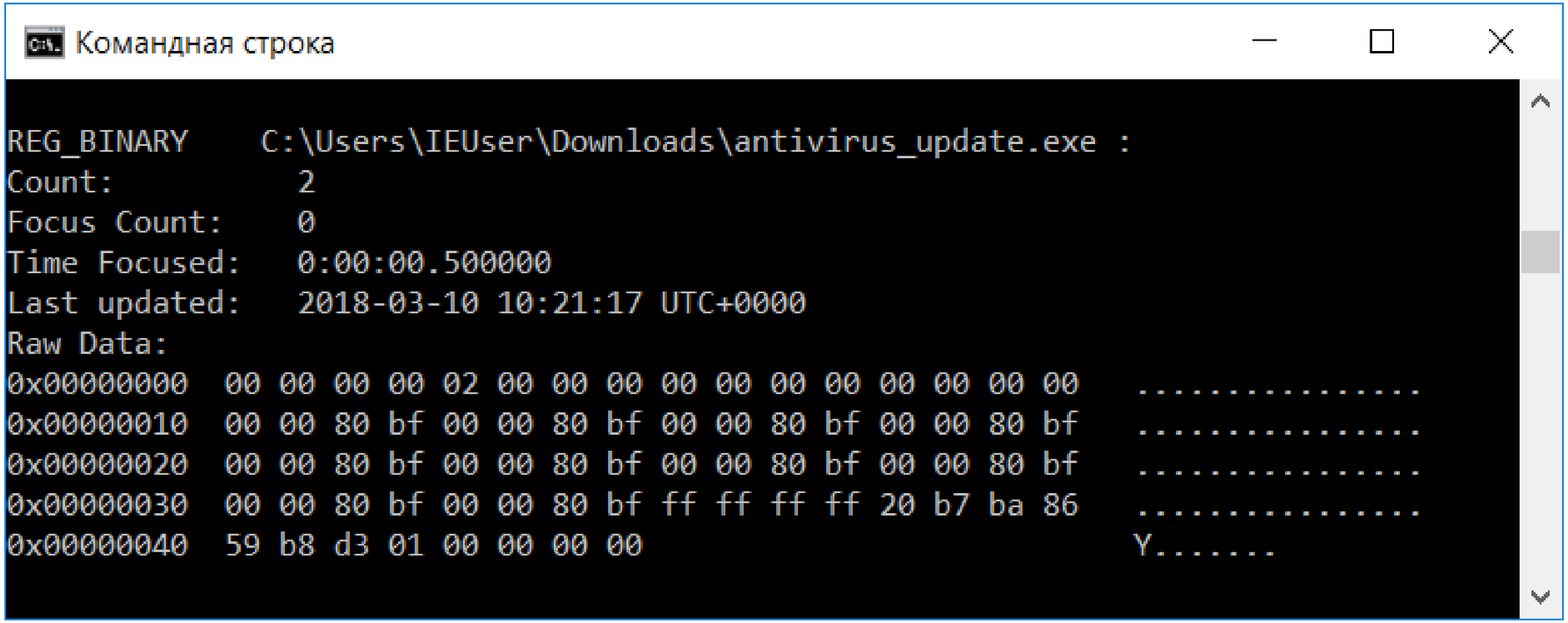


```
0097b6f0 0A 00 53 00 69 00 72 00-2C 00 50 00 6C 00 65 00  ··S·i·r·,·P·l·e·
0097b700 61 00 73 00 65 00 20 00-75 00 70 00 64 00 61 00  a·s·e· ·u·p·d·a·
0097b710 74 00 65 00 20 00 79 00-6F 00 75 00 72 00 20 00  t·e· ·y·o·u·r· ·
0097b720 61 00 6E 00 74 00 69 00-76 00 69 00 72 00 75 00  a·n·t·i·v·i·r·u·
0097b730 73 00 20 00 73 00 6F 00-66 00 74 00 77 00 61 00  s· ·s·o·f·t·w·a·
0097b740 72 00 65 00 20 00 69 00-6D 00 6D 00 65 00 64 00  r·e· ·i·m·m·e·d·
0097b750 69 00 61 00 74 00 65 00-6C 00 79 00 2E 00 20 00  i·a·t·e·l·y·.· ·
0097b760 59 00 6F 00 75 00 20 00-63 00 61 00 6E 00 20 00  Y·o·u· ·c·a·n· ·
0097b770 64 00 6F 00 77 00 6E 00-6C 00 6F 00 61 00 64 00  d·o·w·n·l·o·a·d·
0097b780 20 00 74 00 68 00 65 00-20 00 66 00 69 00 6C 00   ·t·h·e· ·f·i·l·
0097b790 65 00 20 00 66 00 6F 00-72 00 20 00 75 00 70 00  e· ·f·o·r· ·u·p·
0097b7a0 64 00 61 00 74 00 69 00-6E 00 67 00 20 00 75 00  d·a·t·i·n·g· ·u·
0097b7b0 73 00 69 00 6E 00 67 00-20 00 74 00 68 00 65 00  s·i·n·g· ·t·h·e·
0097b7c0 20 00 66 00 6F 00 6C 00-6C 00 6F 00 77 00 69 00   ·f·o·l·l·o·w·i·
0097b7d0 6E 00 67 00 20 00 6C 00-69 00 6E 00 6B 00 3A 00  n·g· ·l·i·n·k·:·
0097b7e0 68 00 74 00 74 00 70 00-3A 00 2F 00 2F 00 62 00  h·t·t·p·:·/·/·b·
0097b7f0 69 00 74 00 2E 00 6C 00-79 00 2F 00 32 00 44 00  i·t·.·l·y·/·2·D·
0097b800 68 00 31 00 45 00 45 00-57 00 2D 00 2D 00 20 00  h·1·E·E·W·-·-· ·
0097b810 53 00 65 00 72 00 67 00-65 00 79 00 20 00 50 00  S·e·r·g·e·y· ·P·
0097b820 65 00 74 00 72 00 6F 00-76 00 54 00 65 00 63 00  e·t·r·o·v·T·e·c·
0097b830 68 00 6E 00 69 00 63 00-61 00 6C 00 20 00 73 00  h·n·i·c·a·l· ·s·
0097b840 75 00 70 00 70 00 6F 00-72 00 74 00 20 00 73 00  u·p·p·o·r·t· ·s·
0097b850 70 00 65 00 63 00 69 00-61 00 6C 00 69 00 73 00  p·e·c·i·a·l·i·s·
0097b860 74 00 0A 00 0A 00 20 00-20 00 20 00 20 00 20 00  t·····  ·  ·  ·  ·
```

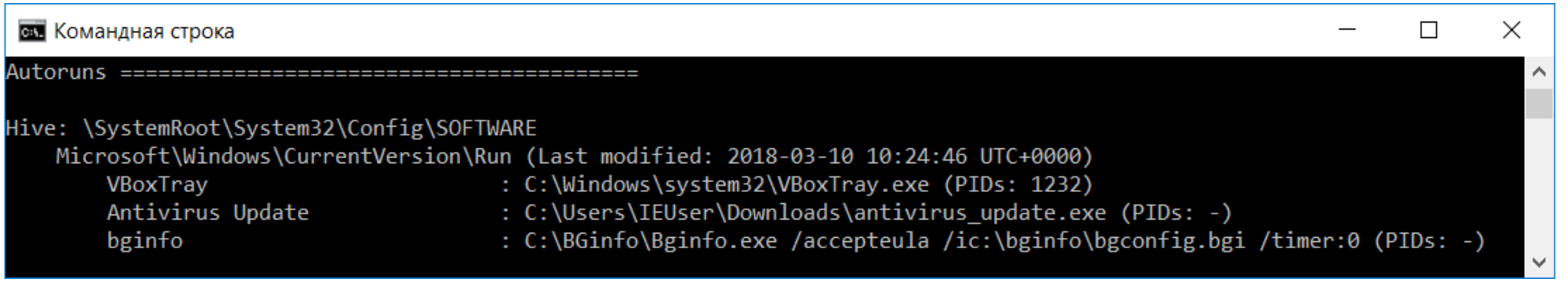
Следы исполнения: Shimcache



Следы исполнения: UserAssist



Персистентность



Вопросы?

Поговорить о цифровой криминалистике:

- на русском:

https://t.me/joinchat/EIgkbEvGmEvLN_zejp0Qig

- на английском:

https://t.me/joinchat/EIgkbEOk4TRrGPFbyarEJw

Предотвращаем и расследуем киберпреступления с 2003 года

www.group-ib.ru
info@group-ib.ru
twitter.com/groupib
blog.group-ib.ru
+7 495 984 33 64
facebook.com/group-ib