



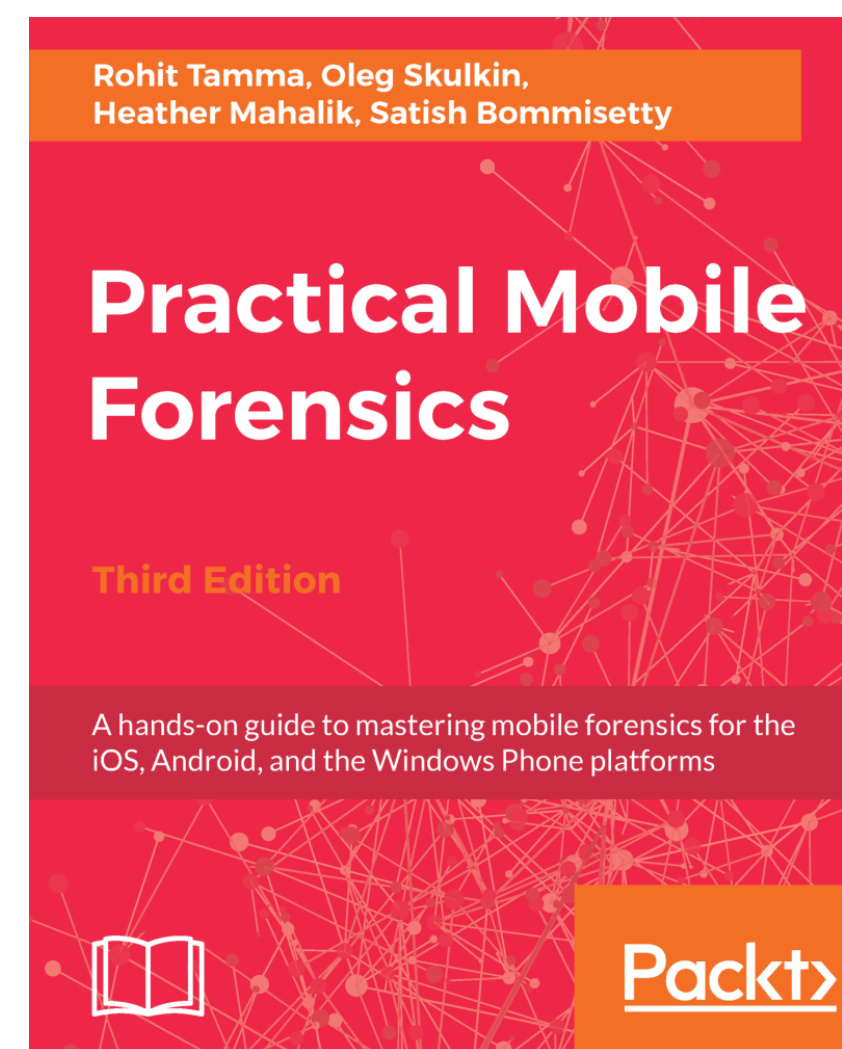
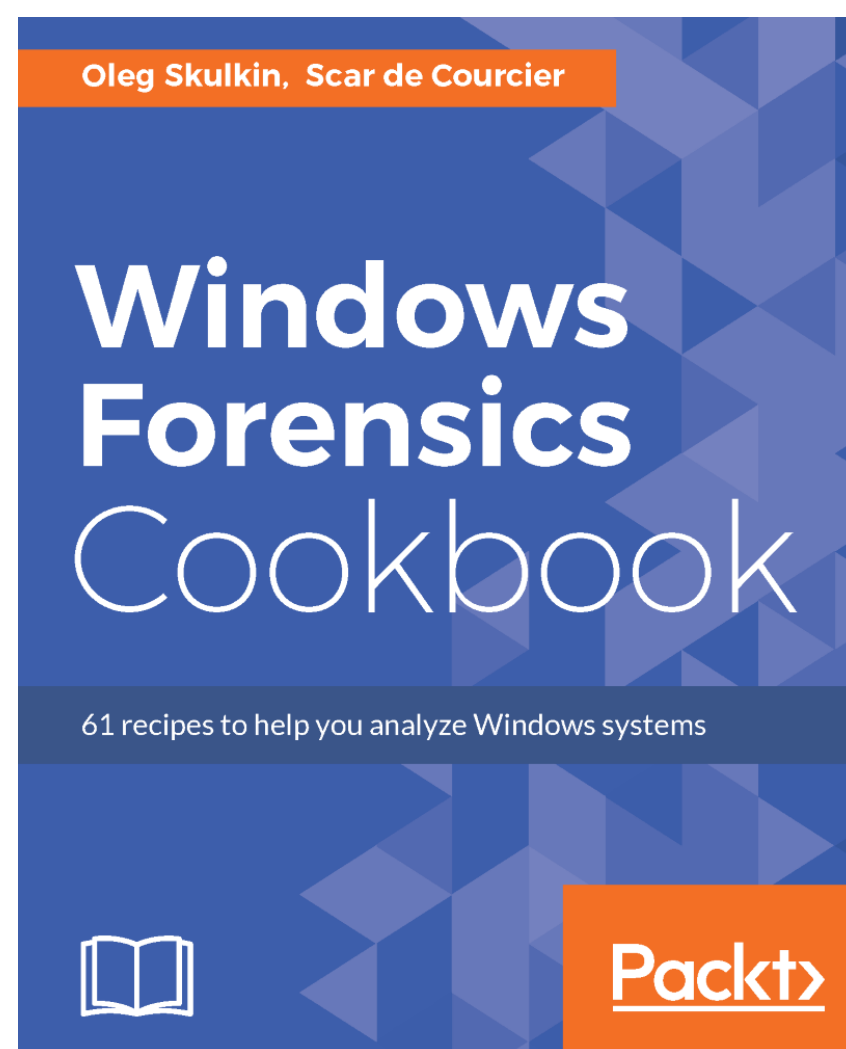
Обнаружение криминалистических артефактов функционирования ПО Metasploit в слепках оперативной памяти



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

```
Administrator: Command Prompt
DumpIt 3.0.20160920.99
Copyright (C) 2007 - 2016, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2016, Comae Technologies FZE <http://www.comae.io>

Destination path:      \??\C:\Users\msuiche\Desktop\Comae_Memory_Toolkit-3.0.20160920.99\DESKTOP-INDAR7N-20160920-140014.dmp

Computer name:         DESKTOP-INDAR7N

--> Proceed to the acquisition ? [y/n] y

[+] Information:
Dump Type:             Microsoft Crash Dump

[+] Machine Information:
Windows version:       10.0.14393
MachineId:             90CDE178-2BF3-4E2E-8DE1-E959F552B97A
TimeStamp:             131188536155983913
Cr3:                   0x1aa000
KdCopyDataBlock:      0xffffffff800c5bef098
KdDebuggerData:       0xffffffff800c5d0e500
KdpDataBlockEncoded:  0xffffffff800c5d5e110

Current date/time:     [2016-9-20 (YYYY-MM-DD) 14:0:15 (UTC)]
+ Processing... Done.

Acquisition finished at: [2016-09-20 (YYYY-MM-DD) 14:00:28 (UTC)]
Time elapsed:          0:13 minutes:seconds (13 secs)

Created file size:     1106833408 bytes ( 1055 Mb)

NtStatus (troubleshooting): 0x00000000
Total of written pages: 270221
Total of inaccessible pages: 0
Total of accessible pages: 270221

SHA-256: D1F7582882BE329DBF6DEC141E4430EFAD4AB6B26DAC55521D69A3DA6F3AD753
```



Вроде, получилось! Что дальше?

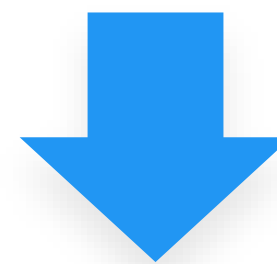


Чаты и веб-активность



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.

```
.....-
.hmMMMMMMMMMMNdddS\...//M\.../hdddmMMMMMMNo
:Nm-/MMMMMMMMMMMMM$NMMMMm&MMMMMMMMMMMMMMY
.sm/`-yMMMMMMMMMMMM$MMMMMMN&MMMMMMMMMMMMMMh`
-Nd` :MMMMMMMMMMMM$MMMMMMN&MMMMMMMMMMMMMMh`
-Nh` .yMMMMMMMMMMMM$MMMMMMN&MMMMMMMMMMMMMM/
.sNd :MMMMMMMMMMMM$MMMMMMN&MMMMMMMMMMMMM/
-mh :MMMMMMMMMMMM$MMMMMMN&MMMMMMMMMMMMM
: -o++++o000+:/o0000+:+o+++o0000++/
:///omh//dMMMMMMMMMMMMMMMMM/:::/+0000-//ydh//+s+0000000:--syN//os:
/MMMMMMMMMMMMMMMMMMM. /+--+y/...sydh/-+00--o//...oydh+
-hMMssddd+:dMMmNMMh. -+00 //^^^\\`+:+`0://^^^\\`::
.sMMmo. -dMd--:mN/` ||--X--|| ||--X--||
...../yddy/:...+hmo-...hdd:.....\\=v=//.....\\=v=//.....
+-----+
+-----| Session one died of dysentery. |-----+
+-----+
Press ENTER to size up the situation

% Date: April 25, 1848 %
% Weather: It's always cool in the lab %
% Health: Overweight %
% Caffeine: 12975 mg %
% Hacked: All the things %

Press SPACE BAR to continue

=[ metasploit v4.16.16-dev ]
+ -- --=[ 1702 exploits - 969 auxiliary - 299 post ]
+ -- --=[ 503 payloads - 40 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```



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



```
Командная строка
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit
-----
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x84ed1b98	System	4	0	82	491	-----	0	2018-03-10 10:16:31 UTC+0000	
0x85619b40	smss.exe	252	4	2	29	-----	0	2018-03-10 10:16:31 UTC+0000	
0x85b53d28	csrss.exe	320	312	9	352	0	0	2018-03-10 10:16:32 UTC+0000	
0x84f83a40	wininit.exe	368	312	3	77	0	0	2018-03-10 10:16:32 UTC+0000	
0x85b9f550	csrss.exe	380	360	7	253	1	0	2018-03-10 10:16:32 UTC+0000	
0x85b97728	winlogon.exe	420	360	3	110	1	0	2018-03-10 10:16:32 UTC+0000	
0x85c14268	services.exe	464	368	7	201	0	0	2018-03-10 10:16:32 UTC+0000	
0x85c1a030	lsass.exe	480	368	6	613	0	0	2018-03-10 10:16:32 UTC+0000	
0x85c1c030	lsm.exe	488	368	10	143	0	0	2018-03-10 10:16:32 UTC+0000	
0x85d28a40	svchost.exe	580	464	9	347	0	0	2018-03-10 10:16:32 UTC+0000	
0x85d58030	VBoxService.ex	640	464	11	117	0	0	2018-03-10 10:16:33 UTC+0000	
0x85d63b50	svchost.exe	692	464	8	242	0	0	2018-03-10 10:16:33 UTC+0000	
0x85d7e270	svchost.exe	748	464	18	405	0	0	2018-03-10 10:16:33 UTC+0000	
0x85da65c0	svchost.exe	864	464	16	369	0	0	2018-03-10 10:16:33 UTC+0000	
0x85dbdbb8	svchost.exe	904	464	15	330	0	0	2018-03-10 10:16:33 UTC+0000	
0x85d29a40	svchost.exe	928	464	28	830	0	0	2018-03-10 10:16:33 UTC+0000	
0x85dc3130	svchost.exe	992	464	5	115	0	0	2018-03-10 10:16:33 UTC+0000	
0x85df0030	svchost.exe	1124	464	16	367	0	0	2018-03-10 10:16:33 UTC+0000	
0x85e2b030	spoolsv.exe	1340	464	13	280	0	0	2018-03-10 10:16:33 UTC+0000	
0x85e44d28	taskhost.exe	1372	464	9	212	1	0	2018-03-10 10:16:34 UTC+0000	
0x85e55d28	svchost.exe	1408	464	20	295	0	0	2018-03-10 10:16:34 UTC+0000	
0x85ea0358	svchost.exe	1528	464	10	163	0	0	2018-03-10 10:16:34 UTC+0000	
0x85d88860	cygrunsrv.exe	1660	464	6	101	0	0	2018-03-10 10:16:34 UTC+0000	
0x85f21330	wlms.exe	1736	464	4	46	0	0	2018-03-10 10:16:34 UTC+0000	
0x84f4dd28	cygrunsrv.exe	1772	1660	0	-----	0	0	2018-03-10 10:16:34 UTC+0000	2018-03-10 10:16:34 UTC+0000
0x85f2ad28	conhost.exe	1788	320	2	33	0	0	2018-03-10 10:16:34 UTC+0000	
0x85f42300	sshd.exe	1808	1772	4	100	0	0	2018-03-10 10:16:34 UTC+0000	
0x84f9ad28	sppsvc.exe	1984	464	4	146	0	0	2018-03-10 10:16:35 UTC+0000	
0x85f81108	svchost.exe	280	464	5	91	0	0	2018-03-10 10:16:35 UTC+0000	
0x85f89030	dwm.exe	1564	864	3	70	1	0	2018-03-10 10:16:39 UTC+0000	
0x85b73030	explorer.exe	1556	1972	32	1013	1	0	2018-03-10 10:16:39 UTC+0000	
0x8602d7b8	VBoxTray.exe	1232	1556	13	151	1	0	2018-03-10 10:16:40 UTC+0000	
0x85f6c420	SearchIndexer.	924	464	12	657	0	0	2018-03-10 10:16:45 UTC+0000	
0x85ffb660	iexplore.exe	2568	1556	11	537	1	0	2018-03-10 10:17:52 UTC+0000	
0x860cbbf0	iexplore.exe	2640	2568	38	828	1	0	2018-03-10 10:17:52 UTC+0000	
0x85031d28	svchost.exe	3312	464	14	377	0	0	2018-03-10 10:18:33 UTC+0000	
0x85c011c8	WmiPrvSE.exe	1428	580	6	110	0	0	2018-03-10 10:20:32 UTC+0000	
0x85097030	antivirus_upda	3000	1556	0	-----	1	0	2018-03-10 10:21:17 UTC+0000	2018-03-10 10:21:59 UTC+0000
0x86149610	FTK Imager.exe	3784	1556	19	379	1	0	2018-03-10 10:25:54 UTC+0000	



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
0xdca8be0	UDPv4	0.0.0.0:5355	*:*		1124	svchost.exe	2018-03-10 10:19:19 UTC+0000
0xdccc8800	UDPv4	0.0.0.0:0	*:*		1124	svchost.exe	2018-03-10 10:19:19 UTC+0000
0xdccc8800	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
0xdcf9208	UDPv4	0.0.0.0:0	*:*		640	VBxService.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	
0xdf177c0	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



```
Командная строка
Process: svchost.exe Pid: 3312 Address: 0x600000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 49, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00600000 4d 5a e8 00 00 00 00 5b 52 45 55 89 e5 81 c3 64 MZ.....[REU....d
0x00600010 13 00 00 ff d3 81 c3 95 a4 02 00 89 3b 53 6a 04 .....;Sj].
0x00600020 50 ff d0 00 00 00 00 00 00 00 00 00 00 00 00 P.....
0x00600030 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 .....

0x00600000 4d          DEC EBP
0x00600001 5a          POP EDX
0x00600002 e800000000 CALL 0x600007
0x00600007 5b          POP EBX
0x00600008 52          PUSH EDX
0x00600009 45          INC EBP
0x0060000a 55          PUSH EBP
0x0060000b 89e5       MOV EBP, ESP
0x0060000d 81c364130000 ADD EBX, 0x1364
0x00600013 ffd3       CALL EBX
0x00600015 81c395a40200 ADD EBX, 0x2a495
0x0060001b 893b       MOV [EBX], EDI
0x0060001d 53          PUSH EBX
0x0060001e 6a04       PUSH 0x4
0x00600020 50          PUSH EAX
0x00600021 ffd0       CALL EAX
0x00600023 0000       ADD [EAX], AL
0x00600025 0000       ADD [EAX], AL
0x00600027 0000       ADD [EAX], AL
0x00600029 0000       ADD [EAX], AL
0x0060002b 0000       ADD [EAX], AL
0x0060002d 0000       ADD [EAX], AL
0x0060002f 0000       ADD [EAX], AL
0x00600031 0000       ADD [EAX], AL
0x00600033 0000       ADD [EAX], AL
0x00600035 0000       ADD [EAX], AL
0x00600037 0000       ADD [EAX], AL
0x00600039 0000       ADD [EAX], AL
0x0060003b 00f8       ADD AL, BH
0x0060003d 0000       ADD [EAX], AL
0x0060003f 00          DB 0x0
```



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



```
Командная строка
Rule: Oh_No_Its_Meterpreter
Owner: Process svchost.exe Pid 3312
0x01590240 73 74 64 61 70 69 5f 73 79 73 5f 70 6f 77 65 72 stdapi_sys_power
0x01590250 5f 65 78 69 74 77 69 6e 64 6f 77 73 00 00 00 00 _exitwindows...
0x01590260 77 65 62 63 61 6d 5f 6c 69 73 74 00 77 65 62 63 webcam_list.webc
0x01590270 61 6d 5f 73 74 61 72 74 00 00 00 00 77 65 62 63 am_start...webc
0x01590280 61 6d 5f 67 65 74 5f 66 72 61 6d 65 00 00 00 00 am_get_frame...
0x01590290 77 65 62 63 61 6d 5f 73 74 6f 70 00 77 65 62 63 webcam_stop.webc
0x015902a0 61 6d 5f 61 75 64 69 6f 5f 72 65 63 6f 72 64 00 am_audio_record.
0x015902b0 73 74 64 61 70 69 00 00 72 62 00 00 5c 00 00 00 stdapi..rb..\...
0x015902c0 25 73 00 00 25 73 5c 2a 00 00 00 00 25 73 5c 25 %s..%s\*...%s\%
0x015902d0 73 00 00 00 2e 00 62 00 61 00 74 00 00 00 00 00 s.....b.a.t.....
0x015902e0 2e 00 63 00 6d 00 64 00 00 00 00 00 2e 00 65 00 ..c.m.d.....e.
0x015902f0 78 00 65 00 00 00 00 00 2e 00 63 00 6f 00 6d 00 x.e.....c.o.m.
0x01590300 00 00 00 00 5f 6c 09 7d 08 ac 1f 4f be b7 5c 22 ...._l.}...0..\"
0x01590310 c5 17 ce 39 b0 cd 06 22 c1 19 d1 11 89 e0 00 c0 ...9...\".....
0x01590320 4f d7 a8 29 81 05 31 ab 80 ac d1 11 8d f3 00 c0 0..)..1.....
0x01590330 4f b6 ef 69 b1 cc 06 22 c1 19 d1 11 89 e0 00 c0 0..i...\".....
```



Откуда оно взялось!?



```
Командная строка
Volatility Foundation Volatility Framework 2.6
*****
Process: 2640 iexplore.exe
Cache type "DEST" at 0xe600005
Last modified: 2018-03-10 02:20:18 UTC+0000
Last accessed: 2018-03-10 10:20:18 UTC+0000
URL: IEUser@http://192.168.1.39/antivirus_update.exe
```



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·l·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



```
Командная строка
2010-11-20 12:17:31 UTC+0000 \\??\C:\Windows\system32\recdisc.exe
2016-12-14 11:47:34 UTC+0000 \\??\C:\xampp\xampp-control.exe
2012-11-23 02:48:41 UTC+0000 \\??\C:\Windows\system32\taskhost.exe
2017-11-14 01:37:24 UTC+0000 \\??\C:\Windows\System32\ieframe.dll
2017-10-12 00:25:47 UTC+0000 \\??\C:\Windows\system32\SearchFilterHost.exe
2017-10-12 00:26:07 UTC+0000 \\??\C:\Windows\system32\SearchProtocolHost.exe
2017-10-12 00:26:21 UTC+0000 \\??\C:\Windows\system32\SearchIndexer.exe
2018-03-10 09:42:21 UTC+0000 \\??\C:\Users\IEUser\Downloads\antivirus_update.exe
2009-07-14 01:14:51 UTC+0000 \\??\C:\Windows\system32\xpsrchvw.exe
2009-07-14 01:14:26 UTC+0000 \\??\C:\Windows\system32\mspaint.exe
2010-11-20 12:16:56 UTC+0000 \\??\C:\Windows\system32\calc.exe
2009-07-14 01:14:39 UTC+0000 \\??\C:\Windows\system32\SnippingTool.exe
2009-07-14 01:14:41 UTC+0000 \\??\C:\Windows\system32\StikyNot.exe
2013-10-01 22:34:12 UTC+0000 \\??\C:\Windows\system32\mstsc.exe
2009-07-14 01:14:18 UTC+0000 \\??\C:\Windows\system32\displayswitch.exe
```




Следы исполнения: UserAssist



```
Командная строка

REG_BINARY      C:\Users\IEUser\Downloads\antivirus_update.exe :
Count:          2
Focus Count:    0
Time Focused:   0:00:00.500000
Last updated:   2018-03-10 10:21:17 UTC+0000
Raw Data:
0x00000000  00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00  .....
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf  .....
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf  .....
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 20 b7 ba 86  .....
0x00000040  59 b8 d3 01 00 00 00 00  Y.....
```



Персистентность



```
Командная строка
Autoruns =====
Hive: \SystemRoot\System32\Config\SOFTWARE
  Microsoft\Windows\CurrentVersion\Run (Last modified: 2018-03-10 10:24:46 UTC+0000)
    VBoxTray           : C:\Windows\system32\VBoxTray.exe (PIDs: 1232)
    Antivirus Update   : C:\Users\IEUser\Downloads\antivirus_update.exe (PIDs: -)
    bginfo              : C:\BGinfo\Bginfo.exe /accepteula /ic:\bginfo\bgconfig.bgi /timer:0 (PIDs: -)
```



Вопросы?



Поговорить о цифровой криминалистике:

- на русском:

https://t.me/joinchat/ElgkbEvGmEvLN_zejp0Qig



- на английском:

<https://t.me/joinchat/ElgkbEOk4TRrGPFbyarEJw>



Предотвращаем и расследуем киберпреступления с 2003 года

www.group-ib.ru

blog.group-ib.ru

info@group-ib.ru

+7 495 984 33 64

twitter.com/groupib

facebook.com/group-ib