

УДК 004.056.57

РАССЛЕДОВАНИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ VOLATILITY FRAMEWORK

Алексеев Д.М.*Научный руководитель: к.т.н., доцент кафедры БИТ Тумоян Е.П.**Южный федеральный университет, Институт компьютерных технологий и информационной безопасности, Таганрог, e-mail: alekseev_1994dima@mail.ru*

В рамках данной работы рассмотрен теоретический материал по расследованию инцидентов информационной безопасности, проведен анализ возможностей инструмента Volatility Framework в области расследования инцидентов. В ходе исследований выполнен анализ тестовой операционной системы посредством применения возможностей инструмента Volatility Framework, представлен и описан процесс расследования конкретного инцидента информационной безопасности – воздействие вредоносной троянской программы Stuxnet. В результате использования программы при анализе тестового образа памяти установлено, что червь установил в систему два драйвера, один из которых является драйвером-фильтром файловой системы, скрывающим наличие компонентов вредоносной программы на съемном носителе. Второй драйвер используется для внедрения зашифрованной динамической библиотеки в системные процессы и содержит в себе специализированное ПО для выполнения основной задачи.

Ключевые слова: информационная безопасность, инциденты информационной безопасности, Volatility Framework, менеджмент инцидентов информационной безопасности, вредоносное программное обеспечение, компьютерный вирус, Stuxnet, расследование инцидентов информационной безопасности

INVESTIGATION OF THE INFORMATION SECURITY INCIDENT WITH THE USE OF VOLATILITY FRAMEWORK

Alekseev D.M.*Scientific advisor: Candidate of Technical Sciences, Associate professor Tumoyan E.P.**Southern Federal University, Institute of Computer Technologies and Information Security, Taganrog, e-mail: alekseev_1994dima@mail.ru*

In this work, theoretical material on the investigation of incidents of information security is considered, an analysis of the capabilities of the Volatility Framework in the field of incident investigation is carried out. During the research, the test operating system was analyzed using the capabilities of the Volatility Framework tool, the process of investigating a particular information security incident – the impact of the malicious Trouxnet Trojan program – was presented and described. As a result of using the program when analyzing the test image of the memory, it is established that the worm installed two drivers into the system, one of which is a file system filter driver that hides the components of the malicious program on removable media. The second driver is used to implement the encrypted dynamic library in the system processes and contains specialized software to perform the main task.

Keywords: Information security, incidents of information security, Volatility Framework, management of information security incidents, malicious software, computer virus, Stuxnet, investigation of information security incidents

Отличительным признаком современного мира является стремительное развитие информационного общества, проявление и широкое распространение технологий мультимедиа, электронных информационных ресурсов, сетевых технологий. Применение информационных технологий требует повышенного внимания к вопросам информационной безопасности.

Информационная безопасность – это защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений [1].

В настоящее время выделяются различные направления деятельности по обеспечению информационной безопасности: составление модели угроз и нарушителей ИБ; оценка рисков нарушений ИБ; внедрение и совершенствование защитных мер; создание службы ИБ; менеджмент ИБ; менеджмент инцидентов ИБ; защита персональных данных и другие.

Вопрос менеджмента инцидентов информационной безопасности является достаточно **актуальным**. Именно во время расследования и реагирования на инцидент проявляются конкретные уязвимости информационной системы, обнаруживаются следы атак и вторжений, проверяется работа защитных механизмов, качество архитектуры системы ИБ и ее управления.

```
C:\Users\ДНС\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe
-f C:\Users\ДНС\Desktop\volatility_2.5.win.standalone\task3.vmem imageinfo
Volatility Foundation Volatility Framework 2.5
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with Win
XPSP2x86)
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (C:\Users\ДНС\Desktop\volatili
ty_2.5.win.standalone\task3.vmem)
PAE type : PAE
DTB : 0x319000L
KDBG : 0x80545ae0L
Number of Processors : 1
Image Type (Service Pack) : 3
KPCR for CPU 0 : 0xffdf000L
KUSER_SHARED_DATA : 0xffdf000L
Image date and time : 2011-06-03 04:31:36 UTC+0000
Image local date and time : 2011-06-03 00:31:36 -0400
```

Рис. 1. Первичная информация о тестовом образе памяти

Целью работы является анализ тестовой операционной системы посредством применения возможностей инструмента Volatility Framework.

Инцидент информационной безопасности – одно или серия нежелательных или неожиданных событий в системе информационной безопасности, которые имеют большой шанс скомпрометировать деловые операции и поставить под угрозу защиту информации [2].

Volatility Framework – программа для исследования копий (образов) оперативной памяти. Фрэймворк с полностью открытым кодом, представляющий собой набор Python – инструментов для извлечения цифровых артефактов из энергонезависимой памяти (RAM). Эта утилита может быть полезна при расследовании инцидентов информационной безопасности или просто при исследовании работы программы с критичными данными.

Самой последней версией Volatility Framework является версия 2.5, выпущенная в октябре 2015 года. Более поздние версии также доступны в разделе Releases на официальном сайте Volatility Framework [3]. Некоторые параметры командной строки, опции и плагины могут незначительно отличаться от версии к версии. С полным списком команд Volatility Framework можно ознакомиться в [4].

Volatility Framework распространяется как в виде открытого исходного кода, так

и в виде исполняемого файла (только для Windows).

На сегодняшний день программа поддерживает следующие платформы: Windows, Linux, OS X. Volatility Framework является одним из самых многофункциональных пакетов для исследования памяти. В его **возможности** входит извлечение информации о: списке запущенных процессов; списке открытых сетевых соединений; списке открытых сетевых сокетов; списке загруженных динамических библиотек (DLL) для каждого процесса; именах открытых файлов для каждого процесса; адресуемую память; открытых записей реестра; извлечение образов процессов.

Как было описано выше, целью данной работы является анализ тестовой операционной системы посредством применения возможностей инструмента Volatility Framework.

Результаты работы и их анализ

В ходе выполнения работы была получена первичная информация об образе памяти, представленная на рис. 1.

Анализ первичной информации позволяет выяснить дату и время получения данного образа памяти, а также тип операционной системы: Windows XP Service Pack 3 (x86).

В первую очередь, после получения первичной общей информации об образе памяти, был проанализирован список процессов:

```
C:\Users\ДНС\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe
--profile=WinXPSP3x86 -f C:\Users\ДНС\Desktop\volatility_2.5.win.standalone\tas
k3.vmem pslist
Volatility Foundation Volatility Framework 2.5
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Star
```

t	Exit					

0x823c8830 System	4	0	59	403	-----	0
0x820df020 smss.exe	376	4	3	19	-----	0 2010
-10-29 17:08:53 UTC+0000						
0x821a2da0 csrss.exe	600	376	11	395	0	0 2010
-10-29 17:08:54 UTC+0000						
0x81da5650 winlogon.exe	624	376	19	570	0	0 2010
-10-29 17:08:54 UTC+0000						
0x82073020 services.exe	668	624	21	431	0	0 2010
-10-29 17:08:54 UTC+0000						
0x81e70020 lsass.exe	680	624	19	342	0	0 2010
-10-29 17:08:54 UTC+0000						
0x823315d8 vmacthlp.exe	844	668	1	25	0	0 2010
-10-29 17:08:55 UTC+0000						
0x81db8da0 svchost.exe	856	668	17	193	0	0 2010
-10-29 17:08:55 UTC+0000						
0x81e61da0 svchost.exe	940	668	13	312	0	0 2010
-10-29 17:08:55 UTC+0000						
0x822843e8 svchost.exe	1032	668	61	1169	0	0 2010
-10-29 17:08:55 UTC+0000						
0x81e18b28 svchost.exe	1080	668	5	80	0	0 2010
-10-29 17:08:55 UTC+0000						
0x81ff7020 svchost.exe	1200	668	14	197	0	0 2010
-10-29 17:08:55 UTC+0000						
0x81fee8b0 spoolsv.exe	1412	668	10	118	0	0 2010
-10-29 17:08:56 UTC+0000						
0x81e0eda0 jqs.exe	1580	668	5	148	0	0 2010
-10-29 17:09:05 UTC+0000						
0x81fe52d0 vmtoolsd.exe	1664	668	5	284	0	0 2010
-10-29 17:09:05 UTC+0000						
0x821a0568 VMUpgradeHelper	1816	668	3	96	0	0 2010
-10-29 17:09:08 UTC+0000						
0x8205ada0 alg.exe	188	668	6	107	0	0 2010
-10-29 17:09:09 UTC+0000						
0x820ec7e8 explorer.exe	1196	1728	16	582	0	0 2010
-10-29 17:11:49 UTC+0000						
0x820ecc10 wscntfy.exe	2040	1032	1	28	0	0 2010
-10-29 17:11:49 UTC+0000						
0x81e86978 TSVNCache.exe	324	1196	7	54	0	0 2010
-10-29 17:11:49 UTC+0000						
0x81fc5da0 VMwareTray.exe	1912	1196	1	50	0	0 2010
-10-29 17:11:50 UTC+0000						
0x81e6b660 VMwareUser.exe	1356	1196	9	251	0	0 2010
-10-29 17:11:50 UTC+0000						
0x8210d478 jusched.exe	1712	1196	1	26	0	0 2010
-10-29 17:11:50 UTC+0000						
0x82279998 imapi.exe	756	668	4	116	0	0 2010
-10-29 17:11:54 UTC+0000						
0x822b9a10 wuauc1t.exe	976	1032	3	133	0	0 2010
-10-29 17:12:03 UTC+0000						
0x81c543a0 Procmon.exe	660	1196	13	189	0	0 2011
-06-03 04:25:56 UTC+0000						
0x81fa5390 wmiprvse.exe	1872	856	5	134	0	0 2011
-06-03 04:25:58 UTC+0000						
0x81c498c8 lsass.exe	868	668	2	23	0	0 2011
-06-03 04:26:55 UTC+0000						
0x81c47c00 lsass.exe	1928	668	4	65	0	0 2011
-06-03 04:26:55 UTC+0000						
0x81c0cda0 cmd.exe	968	1664	0	-----	0	0 2011
-06-03 04:31:35 UTC+0000	2011-06-03 04:31:36 UTC+0000					
0x81f14938 ipconfig.exe	304	968	0	-----	0	0 2011
-06-03 04:31:35 UTC+0000	2011-06-03 04:31:36 UTC+0000					

Полученный список процессов был проанализирован. Большинство из процессов являются системными, остальные связаны с работой программы VMware. В сети Интернет выполнен поиск описания по каждому из процессов. В ходе анализа была найдена информация о том, что один из процессов **lsass.exe** – необходимый системный процесс, отвечающий за работу локального сервера проверки подлинности, политику безопасности и авторизацию пользователей. Взаимодействует со службой Winlogon. Однако, **lsass.exe** может также быть процессом, известным как троянский вирус. Эта троянская программа позволяет злоумышленникам получать доступ к вашему ПК, похищать пароли и персональные данные. Под именем lsass.exe известен также downloader – программа, загружающая данные (в том числе вирусы) из Интернета на ПК пользователя без их ведома [5].

В ходе более детального исследования процесса **lsass.exe** было отмечено его неоднократный старт, причем с ощутимой разницей во времени старта. Более того, процесс **lsass.exe** находится в числе «первых» загружаемых при загрузке. В силу этого значение идентификатора этого процесса является небольшим. Однако подозрительные процессы с PID = 868 и PID = 1928 имеют более высокое значение идентификатора, нежели процесс с PID = 680.

Также можно заметить, что процесс с PID = 680 был порожден процессом с PID = 624 (а именно, процессом **winlogon.exe**). Это является правильным поведением процесса **lsass.exe**, так как он взаимодействует со службой Winlogon. В случае процессов с PID = 1928 и PID = 868 такого взаимодействия не наблюдается. В этом можно наглядно убедиться, построив дерево процессов:

```
C:\Users\ДНЦ\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe
--profile=WinXPSP3x86 -f C:\Users\ДНЦ\Desktop\volatility_2.5.win.standalone\task3.vmem pstree
```

Volatility Foundation Volatility Framework 2.5

Name	Pid	PPid	Thds	Hnds	T
0x81da5650:winlogon.exe	624	376	19	570	2
010-10-29 17:08:54 UTC+0000					
... 0x82073020:services.exe	668	624	21	431	2
010-10-29 17:08:54 UTC+0000					
.... 0x81c47c00:lsass.exe	1928	668	4	65	2
011-06-03 04:26:55 UTC+0000					
.... 0x81c498c8:lsass.exe	868	668	2	23	2
011-06-03 04:26:55 UTC+0000					
... 0x81e70020:lsass.exe	680	624	19	342	2
010-10-29 17:08:54 UTC+0000					

В ходе дальнейшего исследования были проанализированы список открытых сетевых соединений и список открытых сетевых сокетов. Было установлено, что на момент получения образа памяти никаких сетевых соединений не было установлено (рис. 2).

Анализ списка открытых сетевых сокетов (рис. 3) дает еще одно основание полагать, что

процесс с **PID = 680** является безопасным процессом с характерным для него поведением. Дело в том, что назначение процесса **lsass.exe** предполагает, как правило прослушивание портов (в данном случае, это порты 500 и 4500. В то же время, анализ сокетов дает еще один аргумент в пользу подозрительности процессов с **PID = 868** и **PID = 1928**.

```
C:\Users\ДНЦ\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe
--profile=WinXPSP3x86 -f C:\Users\ДНЦ\Desktop\volatility_2.5.win.standalone\task3.vmem connections
Volatility Foundation Volatility Framework 2.5
Offset(U) Local Address Remote Address Pid
```

Рис. 2. Список открытых сетевых соединений

```
C:\Users\ДНЦ\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe
--profile=WinXPSP3x86 -f C:\Users\ДНЦ\Desktop\volatility_2.5.win.standalone\tas
k3.vmem sockets
Volatility Foundation Volatility Framework 2.5
```

Offset(U)	PID	Port	Proto	Protocol	Address	Create Time
0x81dc2008	680	500	17	UDP	0.0.0.0	2010-10-29 17:
09:05 UTC+0000						
0x82061c08	4	445	6	TCP	0.0.0.0	2010-10-29 17:
08:53 UTC+0000						
0x82294aa8	940	135	6	TCP	0.0.0.0	2010-10-29 17:
08:55 UTC+0000						
0x821a5008	188	1025	6	TCP	127.0.0.1	2010-10-29 17:
09:09 UTC+0000						
0x81cb3d70	1080	1141	17	UDP	0.0.0.0	2010-10-31 16:
06:16 UTC+0000						
0x81da4d18	680	0	255	Reserved	0.0.0.0	2010-10-29 17:
09:05 UTC+0000						
0x81fdba98	1032	123	17	UDP	127.0.0.1	2011-06-03 04:
25:47 UTC+0000						
0x81c79778	1080	1142	17	UDP	0.0.0.0	2010-10-31 16:
06:16 UTC+0000						
0x81c20898	1200	1900	17	UDP	127.0.0.1	2011-06-03 04:
25:47 UTC+0000						
0x82060008	680	4500	17	UDP	0.0.0.0	2010-10-29 17:
09:05 UTC+0000						
0x81cb9e98	1580	5152	6	TCP	127.0.0.1	2010-10-29 17:
09:05 UTC+0000						
0x81da54b0	4	445	17	UDP	0.0.0.0	2010-10-29 17:
08:53 UTC+0000						

Рис. 3. Список открытых сетевых сокетов

Затем для каждого из процессов с PID = 680, 868, 1928 был получен **список загруженных библиотек**. Их анализ позволил выявить небольшое количество DLL для подозрительных про-

цессов с PID = 868, 1928 по сравнению с PID = 680 (в четыре и два раза меньшее количество DLL соответственно). Ниже представлен список DLL для процесса с PID = 868:

```
C:\Users\ДНЦ\Desktop\volatility_2.5.win.standalone>volatility-
2.5.standalone.exe
--profile=WinXPSP3x86 -f C:\Users\ДНЦ\Desktop\volatility_2.5.win.standalone\
tas
k3.vmem dlllist -p 868
Volatility Foundation Volatility Framework 2.5
*****
lsass.exe pid:      868
Command line : «C:\WINDOWS\system32\lsass.exe»
Service Pack 3
```

Base	Size	LoadCount	Path
-----	-----	-----	----
0x01000000	0x6000	0xffff	C:\WINDOWS\system32\lsass.exe
0x7c900000	0xaf000	0xffff	C:\WINDOWS\system32\ntdll.dll
0x7c800000	0xf6000	0xffff	C:\WINDOWS\system32\kernel32.dll
0x77dd0000	0x9b000	0xffff	C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000	0x92000	0xffff	C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000	0x11000	0xffff	C:\WINDOWS\system32\Secur32.dll
0x7e410000	0x91000	0xffff	C:\WINDOWS\system32\USER32.dll
0x77f10000	0x49000	0xffff	C:\WINDOWS\system32\GDI32.dll

Далее, используя ключ `-malfind`, был выполнен поиск скрытых DLL для подозрительных процессов. Для подозрительных процессов были получены Crash Dump Files:

```
C:\Users\ДНЦ\Desktop\volatility_2.5.win.standalone>volatility-
2.5.standalone.exe
--profile=WinXPSP3x86 -f C:\Users\ДНЦ\Desktop\volatility_2.5.win.standalone\tas
k3.vmem malfind -p 868 -D C:\Users\ДНЦ\Desktop\volatility_2.5.win.standalone\
Але
ксеев1
Volatility Foundation Volatility Framework 2.5
```


Process: lsass.exe Pid: 868 Address: 0x80000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

```
0x00080000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x00080010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 .....@.....
0x00080020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00080030 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 .....

```



Проводится анализ файла.

SHA256: 2b2945f7cc7cf5b30ccdf37e2adbb236594208e409133bcd56f577c009ffe6d

Имя файла: process.0x81c47c00.0x80000.dmp

Показатель выявления: 49 / 55

Анализ | **Дополнительные сведения** | Комментарии | Голосование

Антивирус	Результат	Дата обновления
ALYac	Backdoor.Generic.577628	20160603
AVG	Hider.IRJ	20160603
AVware	Trojan.Win32.Generic!BT	20160603
Ad-Aware	Backdoor.Generic.577628	20160603
AegisLab	W32.W.Stuxnet.ad!c	20160603
AhnLab-V3	Worm/Win32.Stuxnet	20160603
Antiy-AVL	Worm/Win32.Stuxnet	20160603

Рис. 4. Результат анализа файлов

```
C:\Users\ДНЧ\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe
--profile=WinXPSP3x86 -f C:\Users\ДНЧ\Desktop\volatility_2.5.win.standalone\tas
k3.vmem modscan
Volatility Foundation Volatility Framework 2.5
Offset(P)      Name          Base          Size File
-----
0x00000000001e2a530 mrxnet.sys    0xb21d8000    0x3000 \??\C:\WINDOWS\sys
tem32\Drivers\mrxnet.sys
```

Рис. 5. Список драйверов

Для дальнейшего анализа файлы были загружены на **VirusTotal**. Каждый из файлов был распознан большинством антивирусов как троянская программа – **Stuxnet** (рис. 4).

Затем был проанализирован список драйверов (рис. 5) с помощью команды **modscan** (позволяет получить список ранее выгруженных драйверов и драйверов, которые были скрыты). Попытка поиска в сети Интернет имени первого же драйвера из списка принесла результат: Первая модификация червя **Stuxnet**, созданная в 2009 году, использовала только один файл драйвера –

mrxcsl.sys, – и в нем отсутствовала цифровая подпись. В 2010 году авторы создали второй драйвер **mrxnet.sys** (его целью было сокрытие файлов червя на USB-дисках) и снабдили **mrxnet.sys** и драйвер **mrxcsl.sys** цифровыми сертификатами компании **Realtek** [6].

В ходе проведенного исследования тестового образа памяти **Task3.vmem** было обнаружено действие **вредоносной троянской программы – Stuxnet**. **Win32/Stuxnet** – компьютерный червь, поражающий компьютеры под управлением операционной системы **Microsoft Windows**. Дан-

ный вирус использует четыре уязвимости системы Microsoft Windows (уязвимость «нулевого дня» (zero-day) и три ранее неизвестные уязвимости), позволяющие ему распространяться при помощи USB-flash накопителей.

В ходе работы установлено, что **червь установил в систему два драйвера**, один из которых является драйвером-фильтром файловой системы, скрывающим наличие компонентов вредоносной программы на съемном носителе. Второй драйвер используется для внедрения зашифрованной динамической библиотеки в системные процессы и содержит в себе специализированное ПО для выполнения основной задачи. Драйверы, которые троян устанавливает в систему, снабжены цифровыми подписями, украденными у производителей легального программного обеспечения. Злоумышленники используют цифровую подпись для «тихой» установки драйверов руткита в целевую систему. В системах безопасности многих производителей файлы, подписанные известными фирмами, заведомо считаются безопасными, и наличие подписи дает возможность

беспрепятственно, не выдавая себя, производить действия в системе. Кроме того, червь располагает механизмами контроля количества заражений, самоликвидации и дистанционного управления.

Подводя итог, стоит отметить, что управление инцидентами информационной безопасности является важной частью системы ИБ в любой современной организации. В связи с этим, велика роль инструментов и средств расследования инцидентов информационной безопасности.

Список литературы

1. Информационная безопасность [Электронный ресурс]: – Режим доступа: https://ru.wikipedia.org/wiki/Информационная_безопасность.
2. Инцидент информационной безопасности [Электронный ресурс]: – Режим доступа: http://www.wikisec.ru/index.php?title=Инцидент_информационной_безопасности
3. Volatility Framework [Электронный ресурс]: Режим доступа: <http://www.volatilityfoundation.org/>
4. Volatility Framework – Command Reference [Электронный ресурс]: Режим доступа: <https://code.google.com/archive/p/volatility/wikis/CommandReference.wiki>.
5. Программы, сервисы, процессы в Windows XP [Электронный ресурс]: Режим доступа: <http://articles.org.ru/cn/showdetail.php?cid=5721>.
6. Stuxnet/Duqu: эволюция драйверов XP [Электронный ресурс]: Режим доступа: <https://securelist.ru/analysis/obzor/81/stuxnetduqu-e-volyutsiya-drajverov/>