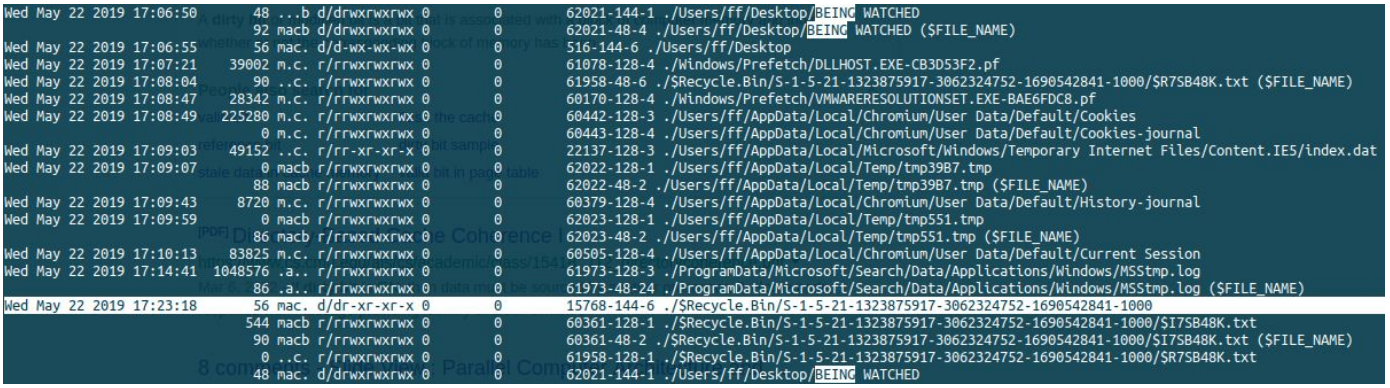
Summer Internship Protocol. Draft

Сделал образ диска через ftk imager, потом спарсил $mft через analyzeMFT, но таблица оч большая. Поэтому я сделал то же самое, только с ntfs флешкой — единственное, там корзины нет. После удаления запись осталась, только с пометкой deleted. Вот так запись для файла something.txt выглядит в таблице (до удаления мимо корзины и после) – ссылка

Что за временные метки в таблице? (NTFS file timestamps)

FN_CTime_2 file creation time
FN_ATime_2 file modified time
FN_MTime_2 mft entry modified time
FN_RTime_2 file last access time

Таймлайны fls+mactime и MFT сравнение



```
Wed May 22 2019 17:06:50      48 ...b d/drwxrwxrwx 0        0        62021-144-1 ./Users/ff/Desktop/BEING WATCHED
                              92 macb d/drwxrwxrwx 0        0        62021-48-4 ./Users/ff/Desktop/BEING WATCHED ($FILE_NAME)
Wed May 22 2019 17:06:55      56 mac. d/d-wx-wx-wx 0        0        516-144-6 ./Users/ff/Desktop
Wed May 22 2019 17:07:21   39002 m.c. r/rrwxrwxrwx 0        0        61078-128-4 ./Windows/Prefetch/DLLHOST.EXE-CB3D53F2.pf
Wed May 22 2019 17:08:04      90 ..c. r/rrwxrwxrwx 0        0        61958-48-6 ./$Recycle.Bin/S-1-5-21-1323875917-3062324752-1690542841-1000/$R7SB48K.txt ($FILE_NAME)
Wed May 22 2019 17:08:47   28342 m.c. r/rrwxrwxrwx 0        0        60170-128-4 ./Windows/Prefetch/VMWARERESOLUTIONSET.EXE-BAE6FDC8.pf
Wed May 22 2019 17:08:49  225280 m.c. r/rrwxrwxrwx 0        0        60442-128-3 ./Users/ff/AppData/Local/Chromium/User Data/Default/Cookies
                              0 m.c. r/rrwxrwxrwx 0        0        60443-128-4 ./Users/ff/AppData/Local/Chromium/User Data/Default/Cookies-journal
Wed May 22 2019 17:09:03   49152 ..c. r/rr-xr-xr-x 0        0        22137-128-3 ./Users/ff/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/index.dat
Wed May 22 2019 17:09:07      0 macb r/rrwxrwxrwx 0        0        62022-128-1 ./Users/ff/AppData/Local/Temp/tmp39B7.tmp
                             88 macb r/rrwxrwxrwx 0        0        62022-48-2 ./Users/ff/AppData/Local/Temp/tmp39B7.tmp ($FILE_NAME)
Wed May 22 2019 17:09:43   8720 m.c. r/rrwxrwxrwx 0        0        60379-128-4 ./Users/ff/AppData/Local/Chromium/User Data/Default/History-journal
Wed May 22 2019 17:09:59      0 macb r/rrwxrwxrwx 0        0        62023-128-1 ./Users/ff/AppData/Local/Temp/tmp551.tmp
                             86 macb r/rrwxrwxrwx 0        0        62023-48-2 ./Users/ff/AppData/Local/Temp/tmp551.tmp ($FILE_NAME)
Wed May 22 2019 17:10:13   83825 m.c. r/rrwxrwxrwx 0        0        60505-128-4 ./Users/ff/AppData/Local/Chromium/User Data/Default/Current Session
Wed May 22 2019 17:14:41 1048576 .a.. r/rrwxrwxrwx 0        0        61973-128-3 ./ProgramData/Microsoft/Search/Data/Applications/Windows/MSStmp.log
                             86 .a.. r/rrwxrwxrwx 0        0        61973-48-24 ./ProgramData/Microsoft/Search/Data/Applications/Windows/MSStmp.log ($FILE_NAME)
Wed May 22 2019 17:23:18      56 mac. d/dr-xr-xr-x 0        0        15768-144-6 ./$Recycle.Bin/S-1-5-21-1323875917-3062324752-1690542841-1000
                            544 macb r/rrwxrwxrwx 0        0        60361-128-1 ./$Recycle.Bin/S-1-5-21-1323875917-3062324752-1690542841-1000/$I7SB48K.txt
                             90 macb r/rrwxrwxrwx 0        0        60361-48-2 ./$Recycle.Bin/S-1-5-21-1323875917-3062324752-1690542841-1000/$I7SB48K.txt ($FILE_NAME)
                              0 ..c. r/rrwxrwxrwx 0        0        61958-128-1 ./$Recycle.Bin/S-1-5-21-1323875917-3062324752-1690542841-1000/$R7SB48K.txt
                             48 mac. d/drwxrwxrwx 0        0        62021-144-1 ./Users/ff/Desktop/BEING WATCHED
```

Сгенерировали таймлайн: на 6й минуте создали папку, на 23й удалили файл – важный кусок

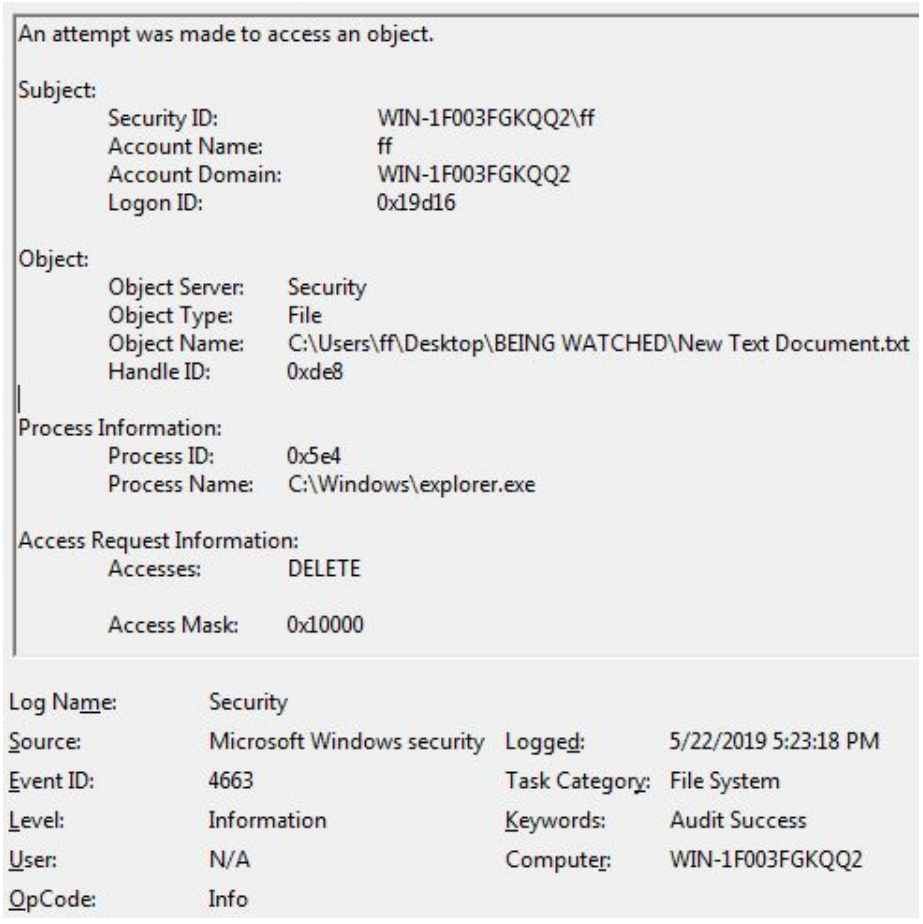
MFT entry для нашего файла до и после удаления – ссылка. У них разные имена, но offset таблице одинаковый

Реестр

Сделали [diff двух дампов реестра]: до и после удаления. RegShot автоматически показал, какие файлы были удалены

```
----------------------------------
Files deleted: 3
----------------------------------
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS00010.log
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\MSS00010.log
C:\Users\ff\Desktop\BEING WATCHED\New Text Document.txt
```

Event viewer



Запись в логе показывает, что 0xde8 – handle для файла `New Text Document.txt`, который мы планируем удалить

An object was deleted.

Subject:

Security ID:	WIN-1F003FGKQQ2\ff
Account Name:	ff
Account Domain:	WIN-1F003FGKQQ2
Logon ID:	0x19d16

Object:

Object Server:	Security
Handle ID:	0xde8

Process Information:

Process ID:	0x5e4
Process Name:	C:\Windows\explorer.exe
Transaction ID:	{00000000-0000-0000-0000-000000000000}

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	5/22/2019 5:23:18 PM
Event ID:	4660	Task Category:	File System
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN-1F003FGKQQ2
OpCode:	Info		

Удалили файл через windows explorer в корзину (handle – 0xde8)

An attempt was made to access an object.

Subject:

Security ID:	WIN-1F003FGKQQ2\ff
Account Name:	ff
Account Domain:	WIN-1F003FGKQQ2
Logon ID:	0x19d16

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\$Recycle.Bin\S-1-5-21-1323875917-3062324752-1690542841-1000\$R7SB48K.txt
Handle ID:	0xde8

Process Information:

Process ID:	0x5e4
Process Name:	C:\Windows\explorer.exe

Access Request Information:

Accesses:	ReadAttributes
Access Mask:	0x80

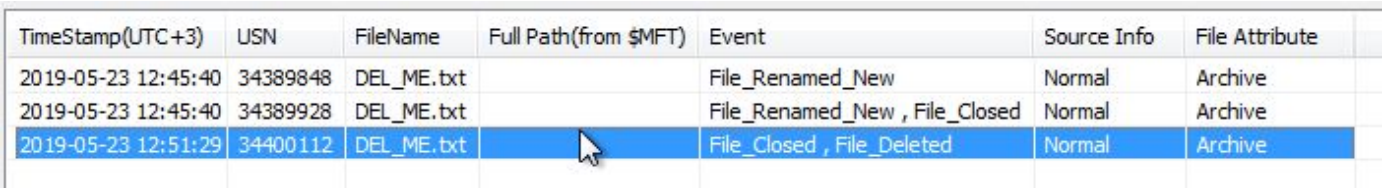
Log Name:	Security		
Source:	Microsoft Windows security	Logged:	5/22/2019 5:23:18 PM
Event ID:	4663	Task Category:	File System
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN-1F003FGKQQ2
OpCode:	Info		

После удаления наш файл (узнаем его по handle) был перемещен в корзину

NTFS Log Tracker

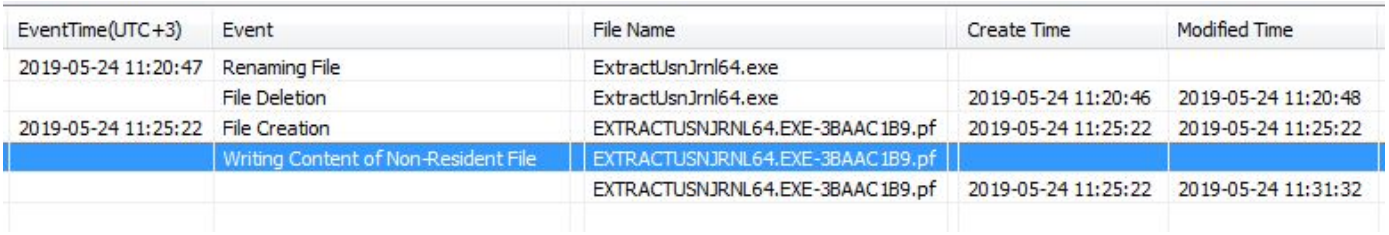
Спарсили $UsnJrnl_$J.bin и нашли удаленный файл. До этого сдампли с живого диска с помощью

```
> .\ExtractUsnJrnl64.exe /DevicePath:c: /OutputPath:c:\temp
```



TimeStamp(UTC+3)	USN	FileName	Full Path(from $MFT)	Event	Source Info	File Attribute
2019-05-23 12:45:40	34389848	DEL_ME.txt		File_Renamed_New	Normal	Archive
2019-05-23 12:45:40	34389928	DEL_ME.txt		File_Renamed_New , File_Closed	Normal	Archive
2019-05-23 12:51:29	34400112	DEL_ME.txt		File_Closed , File_Deleted	Normal	Archive

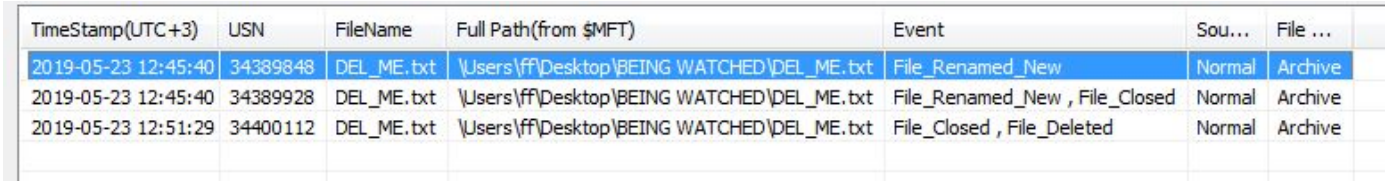
$LogFile не содержал информации о DEL_ME.txt и о записях старше вчерашнего вечера. На скриншоте виден момент удаления одного из файлов, с которым мы работали этим утром



EventTime(UTC+3)	Event	File Name	Create Time	Modified Time
2019-05-24 11:20:47	Renaming File	ExtractUsnJrnl64.exe		
	File Deletion	ExtractUsnJrnl64.exe	2019-05-24 11:20:46	2019-05-24 11:20:48
2019-05-24 11:25:22	File Creation	EXTRACTUSNJRNL64.EXE-3BAAC1B9.pf	2019-05-24 11:25:22	2019-05-24 11:25:22
	Writing Content of Non-Resident File	EXTRACTUSNJRNL64.EXE-3BAAC1B9.pf		
		EXTRACTUSNJRNL64.EXE-3BAAC1B9.pf	2019-05-24 11:25:22	2019-05-24 11:31:32

$UsnJrnl_$J.bin был взят с живого диска, $LogFile был взят с образа взятого этим утром

$UsnJrnl:$J с образа выглядит также



TimeStamp(UTC+3)	USN	FileName	Full Path(from $MFT)	Event	Sou...	File ...
2019-05-23 12:45:40	34389848	DEL_ME.txt	\Users\ff\Desktop\BEING WATCHED\DEL_ME.txt	File_Renamed_New	Normal	Archive
2019-05-23 12:45:40	34389928	DEL_ME.txt	\Users\ff\Desktop\BEING WATCHED\DEL_ME.txt	File_Renamed_New , File_Closed	Normal	Archive
2019-05-23 12:51:29	34400112	DEL_ME.txt	\Users\ff\Desktop\BEING WATCHED\DEL_ME.txt	File_Closed , File_Deleted	Normal	Archive

Разбор временных меток в ntfs через fls+mactime

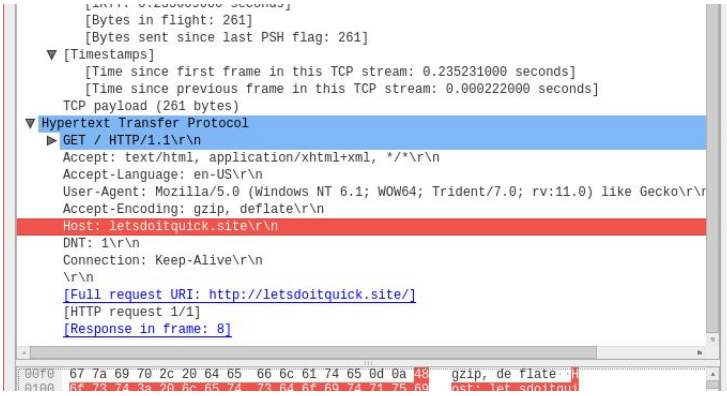
Таймлайн с нашими пояснениями

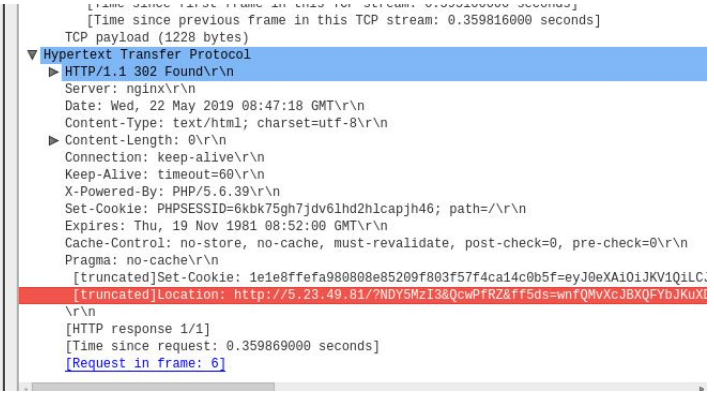
Разбор временных меток в ext4 через fls+mactime

Timeline

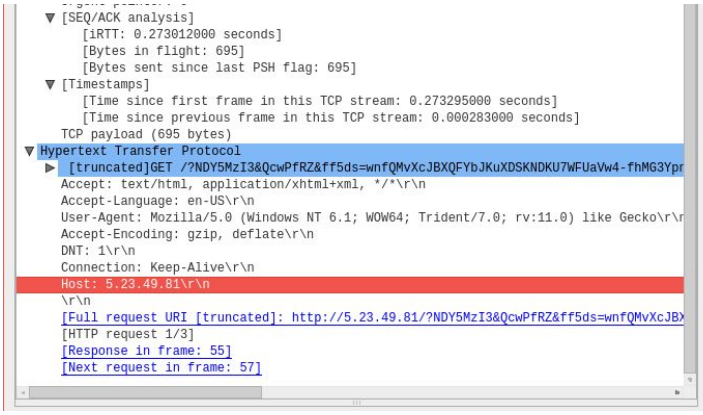
GandCrab pcap

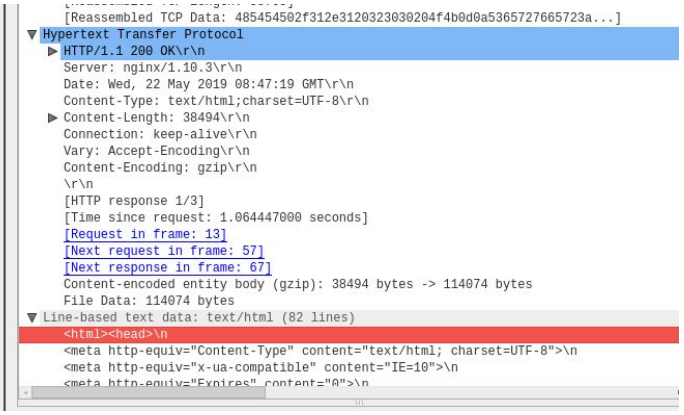
	Time	Source	Destination	Protoc	Lengtl	Info
6	0.316525	10.5.22.101	letsdoitquick.site	HTTP	315	GET / HTTP/1.1
8	0.676394	letsdoitquick.site	10.5.22.101	HTTP	1282	HTTP/1.1 302 Found
13	0.959634	10.5.22.101	vds-cq75232.timeweb.ru	HTTP	749	GET /?NDY5MzI3&QcwPfRZ&ff5ds=wnfQMvXcJBXQFYbJKuX
55	2.024081	vds-cq75232.timeweb.ru	10.5.22.101	HTTP	1481	HTTP/1.1 200 OK (text/html)
57	2.264106	10.5.22.101	vds-cq75232.timeweb.ru	HTTP	969	GET /?MzU0Mjkx&vngMJqX&fhzLaqwjkdLBeR=strategy&l
67	2.598844	vds-cq75232.timeweb.ru	10.5.22.101	HTTP	658	HTTP/1.1 200 OK (application/x-shockwave-flash)
69	3.227370	10.5.22.101	vds-cq75232.timeweb.ru	HTTP	260	GET /favicon.ico HTTP/1.1
71	3.540263	vds-cq75232.timeweb.ru	10.5.22.101	HTTP	291	HTTP/1.1 200 OK
76	4.013968	10.5.22.101	vds-cq75232.timeweb.ru	HTTP	731	GET /?MjE4MzEz&RrznwCQ&hFIyROkAlmigb=wrapped&UPF
774	8.031512	vds-cq75232.timeweb.ru	10.5.22.101	HTTP	536	HTTP/1.1 200 OK (application/x-msdownload)



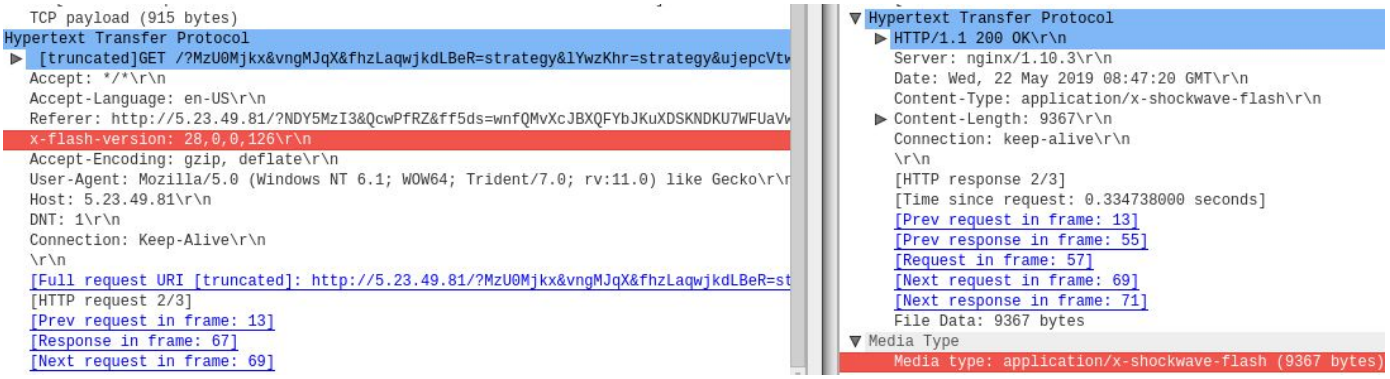


1. Посещается сайт letsdoitquick.site, который моментально редиректит на 5.23.49.81/?NDY5M...

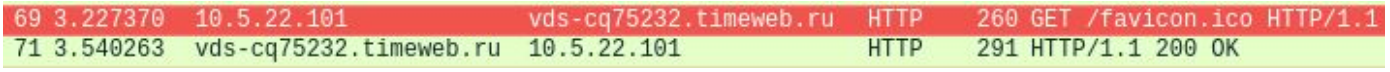




2. 5.23.49.81/?NDY5M… возвращает html страницу с 4 обфусцированными js скриптами.



3. Один из скриптов скачивает swf файл с CVE-2018-4878 эксплоитом.



4. В следующем пакете просто скачивается favicon.ico

5. Один из обфусцированных js скриптов выполняет vbs скрипт, который эксплуатирует CVE-2016-0189 скачивая зашифрованный exe файл шифровальщика.

Подробнее про 4 обфусцированных js скрипта

1. obf1.js сильно обфусцированный файл, который эксплуатирует CVE-2015-2419 для запуска шеллкода, который пытается подключиться к 5.23.49.81/?MjU5Nz… Не сработал т.к. Этого пакета в pcap файле нет.
2. obf2.js встраивает в страницу flash player и скачивает swf файл с CVE-2018-4878 эксплоитом из 5.23.49.81/?MzU0M...
3. obf3.js запускает payload1.vbs и вызывает функцию ProtectMe из vbs скрипта с другой функцией (hedfsdf) из этого vbs скрипта в аргументе.
4. obf4.js запускает payload2.vbs

Подробнее про payload1.vbs

1. ProtectMe является CVE-2016-0189 эксплойтом, который запускает функцию fire
2. fire скачивает с 5.23.49.81/?MjE4MzE… исполняемый файл шифровальщика зашифрованный алгоритмом RC4 с ключём cvytEL5a.

3. Потом во временное папке создаёт папку System32 и в неё кладёт файл shell32.dll (payload._dll)
4. После этого сохраняет расшифрованный исполняемый файл шифровальщика во временную папку с именем из 8ми случайных символов.
5. Меняет переменную окружения SystemRoot и создает объект CreateObject("Shell.Application") чтобы заставить текущий процесс импортировать фейковый shell32.dll
6. shell.dll предположительно запускает исполняемый файл шифровальщика функцией CreateProcessAsUserW

Подробнее про payload2.vbs

1. Сильно обфусцированный vbs скрипт. Похоже, что пытается эксплуатировать какую-то уязвимость. Содержит тот же шеллкод, что и obf1.js. В коде упоминается url 5.23.49.81/?MTY0MTk… Похоже этот скрипт не сработал т.к. В pcap файле этот url не упоминается.

Подробнее про шеллкод (shellcode.bin)

```
.data:00000000   eb12                jmp loc_00000014
.data:00000002   58                  pop %eax
.data:00000003   31c9                xor %ecx,%ecx
.data:00000005   66b96d05            mov $0x56d,%cx
.data:00000009
.data:00000009                   loc_00000009:
.data:00000009   49                  dec %ecx
.data:0000000a   80340884            xorb $0x84,(%eax,%ecx,1)
.data:0000000e   85c9                test %ecx,%ecx
.data:00000010   75f7                jne loc_00000009
.data:00000012   ffe0                jmp *%eax
.data:00000014
.data:00000014                   loc_00000014:
.data:00000014   e8e9ffffff          call
.data:00000019   d10d61074028        rorl 0x28400761
.data:0000001f   d7                  xlat %ds:(%ebx)
.data:00000020   d5d3                aad $0xd3
.data:00000022   b544                mov $0x44,%ch
.data:00000024   e00f                loopne 0x00000035
.data:00000026   c4b40fc4880fc4      les -0x3bf0773c(%edi,%ecx,1),%esi
.data:0000002d   880f                mov %cl,(%edi)
.data:0000002f   840f                test %cl,(%edi)
.data:00000031   840f                test %cl,(%edi)
.data:00000033   dc9c0d5c87c4b8      fcompl -0x473b78a4(%ebp,%ecx,1)
.data:0000003a   0fd4fc              paddq %mm4,%mm7
.data:0000003d   855e0f              test %ebx,0xf(%esi)
.data:00000040   fe                  db feh
```

Встречается в двух RCE эксплоитах (в obf1.js и payload2.vbs). Ни один из этих эксплоитов не сработал. Похоже большая часть шеллкода зашифрована (xor с 0x84) подробнее здесь и здесь.

Всё файлы собранные из файла pcap зд
есь.