Статья Сбор данных с VM антивирусных компаний.

xss.is/threads/34080

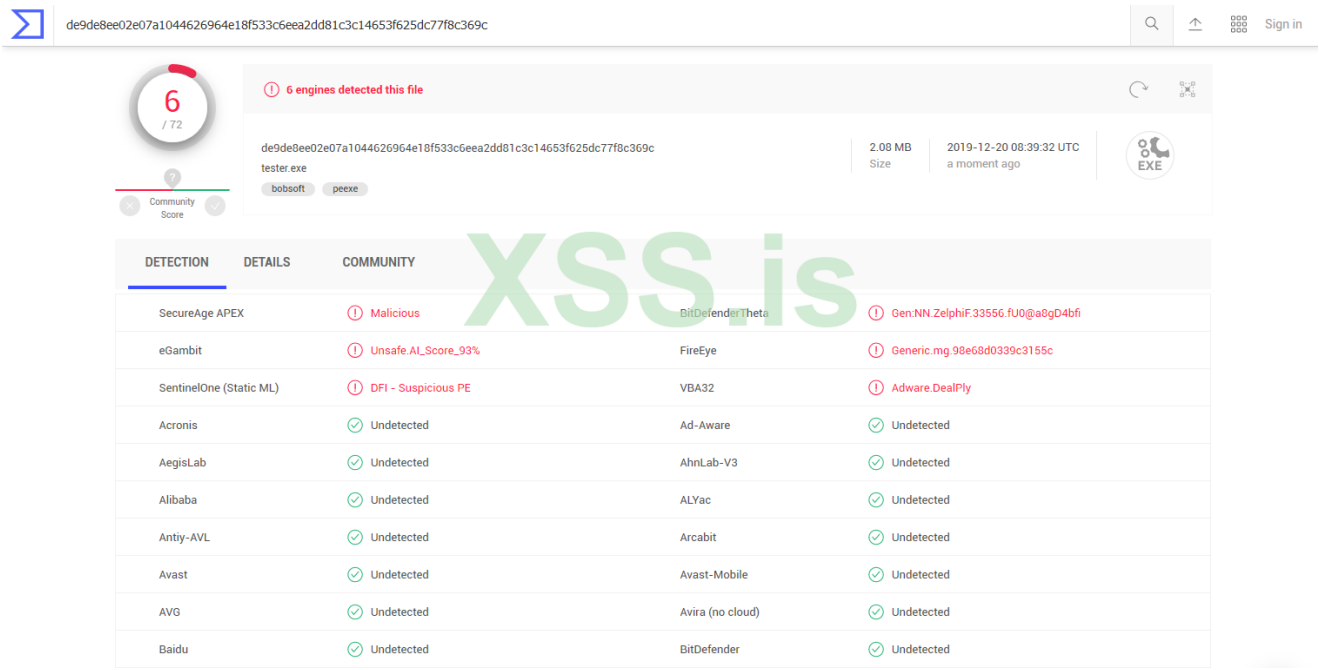
Сбор данных с VM антивирусных компаний.

Дело было к вечеру, делать было нечего. Тема анализа систем проверки файлов уже много раз поднималась, но я решил еще раз уделить внимание данной тематики и актуализировать ее.
Написал побыстрому софт который собирает информацию о виртуальной машине и отправляет на веб сервер.

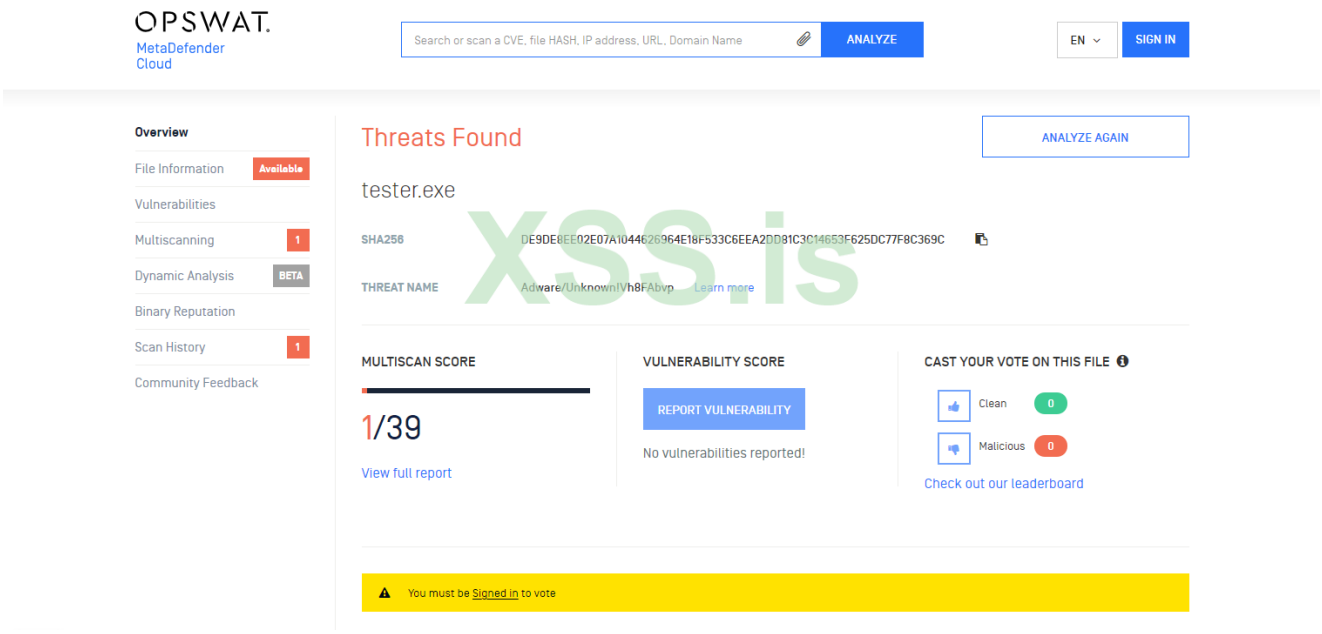
Что будем собирать:
IP, OS, Username, Computer, Group, Lang, DateTime, TimeZone,BIOS, CPU, Memory, Motherboard, HDD, Screen,GPU, AntiVirus, AntiSpyware, Firewall, Languages, Module Dll, Environment, Process, Soft

Собрал два проекта с интерфейсами console и gui. Компилировал под x32 (но можно и под x64).
Закинул на несколько систем проверки VirusTotal, Hybrid-Analysis, MetaDefender Opswat, Jotti

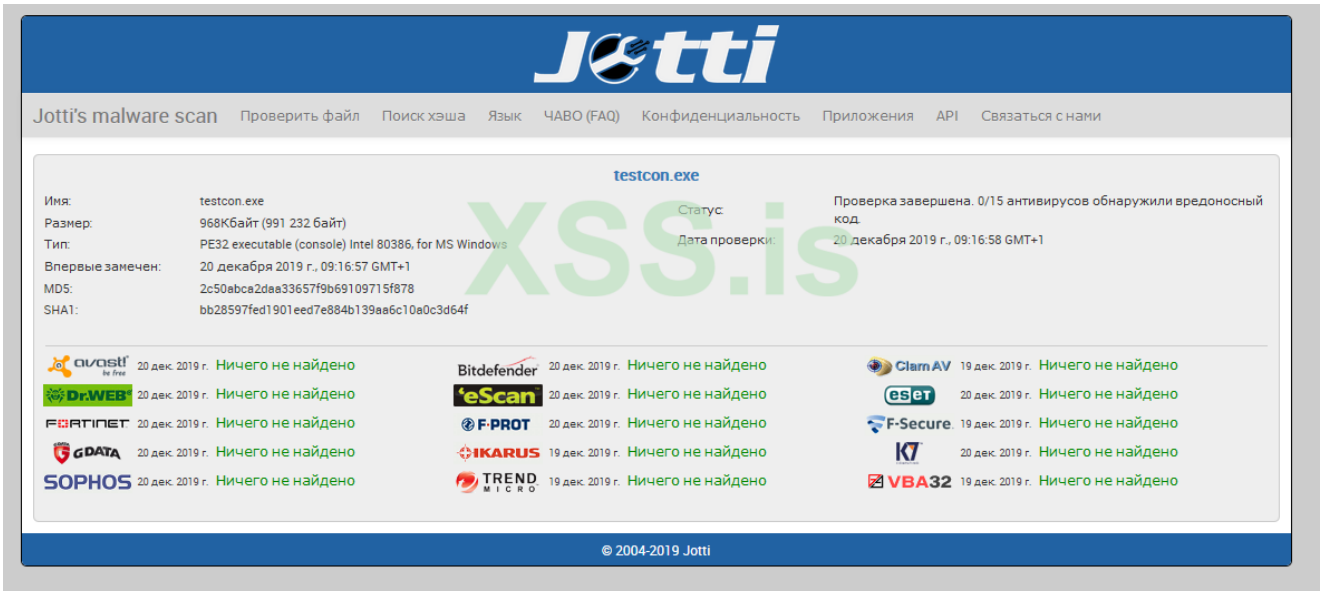
VirusTotal



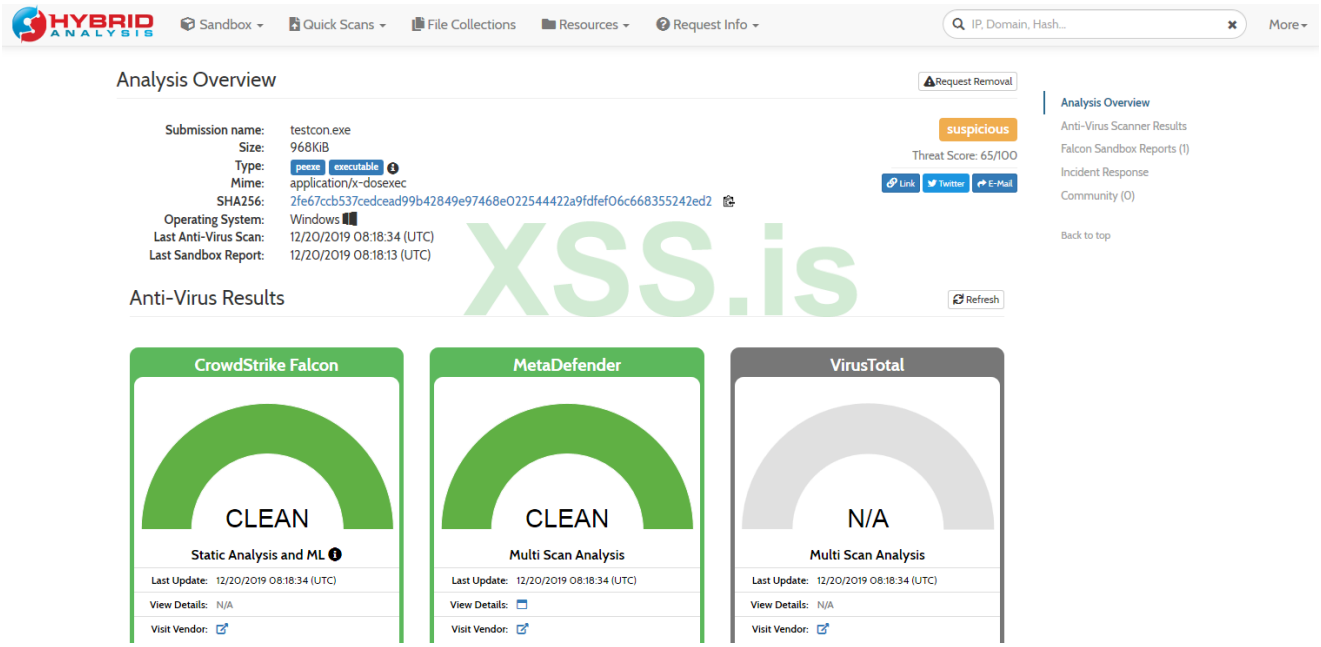
MetaDefender Opswat



Jotti



Hybrid-Analysis



В течении полу часа набрались отчеты. Я их приложил в архиве для тех кто хочет посомтреть.

Пример одного из ответов
Code:

IP: 51.75.62.81

Windows: Windows 7 x64 7601

Username: admin

Computer: USER-PC

Group: Admin

Lang: US

Time: 12/20/2019 6:06:25 AM

TimeZone: Romance Standard Time bias=-60 standardbias=0

BIOS:

CPU: Intel Core Processor (Broadwell, IBRS) cores 2

Memory: 2047Gb

Motherboard:

HDD:
IDE\DiskLULZHARDDISK_____1.0_____\4256313636366430636264 2d3664643335632

Screen: 800x600 32 bit

GPU:
Standard VGA Graphics Adapter
RDPDD Chained DD
RDP Encoder Mirror Driver
RDP Reflector Display Driver

AV:
AS:
displayName Windows Defender
instanceGuid {D68DDC3A-831F-4fae-9E44-DA132C1ACF46}
pathToSignedProductExe %ProgramFiles%\Windows Defender\MSASCui.exe
pathToSignedReportingExe %SystemRoot%\System32\svchost.exe
productState 393472

FW:
Languages:
English (United States)

Module:
tester.exe
ntdll.dll
kernel32.dll

KERNELBASE.dll
oleaut32.dll
ole32.dll
msvcrt.dll
GDI32.dll
USER32.dll
ADVAPI32.dll
sechost.dll
RPCRT4.dll
SspiCli.dll
CRYPTBASE.dll
LPK.dll
USP10.dll
version.dll
netapi32.dll
netutils.dll
srvcli.dll
wkscli.dll
comctl32.dll
SHLWAPI.dll
shell32.dll
wininet.dll
urlmon.dll
CRYPT32.dll
MSASN1.dll
iertutil.dll
winspool.drv
IMM32.DLL
MSCTF.dll
frida-agent-32.dll
DNSAPI.dll
WS2_32.dll
NSI.dll
IPHLPAPI.DLL
WINNSI.DLL
Secur32.dll
PSAPI.DLL
WINMM.dll
api-ms-win-core-synch-l1-2-0.DLL
wtsapi32.dll
WINSTA.dll
uxtheme.dll
CLBCatQ.DLL
wbemdisp.dll
wbemcomn.dll
wbemprox.dll
wbemcomn2.dll
SXS.DLL
wmiutils.dll
NLAapi.dll
napinsp.dll

```
pnrpnsp.dll
mswsock.dll
winrnr.dll
fwpuclnt.dll
rasadhlp.dll
CRYPTSP.dll
rsaenh.dll
RpcRtRemote.dll
wbemsvc.dll
fastprox.dll
NTDSAPI.dll

Environment:
=C:=C:\Users\admin\Downloads
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\admin\AppData\Roaming
CommonProgramFiles=C:\Program Files (x86)\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=USER-PC
ComSpec=C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Users\admin
LOCALAPPDATA=C:\Users\admin\AppData\Local
LOGONSERVER=\\USER-PC
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\Program Files (x86)\Common
Files\Oracle\Java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\
 Files\dotnet\;C:\Program Files
(x86)\dotnet\;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Users\admin\AppData\Local\Program

PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_ARCHITEW6432=AMD64
PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 1, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=3c01
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files (x86)
ProgramFiles(x86)=C:\Program Files (x86)
ProgramW6432=C:\Program Files
PSModulePath=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
PUBLIC=C:\Users\Public
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\admin\AppData\Local\Temp
TMP=C:\Users\admin\AppData\Local\Temp
USERDOMAIN=USER-PC
```

```
USERNAME=admin
USERPROFILE=C:\Users\admin
windir=C:\Windows
windows_tracing_flags=3
windows_tracing_logfile=C:\BVTBin\Tests\installpackage\csilogfile.log

Process:
[System Process]
System
smss.exe
csrss.exe
wininit.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
lsm.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
audiodg.exe
svchost.exe
svchost.exe
spoolsv.exe
svchost.exe
taskhost.exe
dwm.exe
explorer.exe
svchost.exe
svchost.exe
SearchIndexer.exe
wmpnetwk.exe
svchost.exe
WmiPrvSE.exe
sppsvc.exe
pyw.exe
pythonw.exe
SearchProtocolHost.exe
SearchFilterHost.exe
tester.exe
frida-winjector-helper-32.exe
conhost.exe
frida-winjector-helper-32.exe
frida-winjector-helper-64.exe

Soft:
Google Chrome
Mozilla Firefox 68.0 (x86 en-US)
Steam
```

```
Microsoft .NET Core Runtime - 2.2.6 (x86)
OpenOffice 4.1.6
Java 8 Update 221
Java Auto Updater
Microsoft .NET Core Runtime - 2.2.6 (x64)
Google Update Helper
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161
Microsoft .NET Core Host FX Resolver - 2.2.6 (x86)
Adobe Acrobat Reader DC
Microsoft .NET Core 2.2.6 - Windows Server Hosting
Microsoft ASP.NET Core 2.2.6 Shared Framework (x86)
Python Launcher
Microsoft .NET Core Host - 2.2.6 (x86)
Microsoft .NET Core Runtime - 2.2.6 (x86)
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.21.27702


Я немного оптимизировал подборку данных и разделил для более удобного анализа. И так начнем.

[b]CPU[/b]
[code]
Intel Core Processor (Broadwell, IBRS) cores 2
Intel(R) Xeon(R) CPU E5-1650 0 @ 3.20GHz cores 1
Intel Core Processor (Broadwell, IBRS) cores 2
Intel Core Processor (Broadwell, IBRS) cores 2
Intel(R) Xeon(R) CPU E5-1650 0 @ 3.20GHz cores 1
Intel(R) Xeon(R) CPU E5-1650 0 @ 3.20GHz cores 1
Intel Core Processor (Broadwell, IBRS) cores 2
Intel Core Processor (Broadwell, IBRS) cores 2
Intel(R) Xeon(R) CPU E3-1245 V2 @ 3.40GHz cores 1
Intel(R) Xeon(R) CPU E5-1650 0 @ 3.20GHz cores 1
Intel(R) Xeon(R) CPU E3-1245 V2 @ 3.40GHz cores 1
Intel(R) Xeon(R) CPU E3-1245 V2 @ 3.40GHz cores 1
Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz cores 2
Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz cores 2
Intel Core Processor (Broadwell, IBRS) cores 2
Intel(R) Xeon(R) CPU E3-1245 V2 @ 3.40GHz cores 1
```

Виртульные машины не используют более двух ядер.

OS
Code:

```
Windows 7 x64 7601
Windows XP x32 2600
Windows 7 x64 7601
Windows 7 x64 7601
Windows XP x32 2600
Windows XP x32 2600
Windows 7 x64 7601
Windows 7 x64 7601
Windows XP x32 2600
Windows XP x32 2600
Windows XP x32 2600
Windows XP x32 2600
Windows 7 x32 7601
Windows 7 x32 7601
Windows 7 x64 7601
Windows XP x32 2600
```

Можно заметить, что все системы аназа на виртуальных машина выше ос чем Windows 7 не используют.

Memory
Code:

```
127Mb
2047Mb
```

Виртульные машины используют только 127 или 2047 Мб.

HDD
Code:

```
HDD:
IDE\DiskLULZHARDDISK_____________________________1.0_____\4256313636366430636264 2d3664643335632
HDD:
IDE\DiskVBOX_HARDDISK_____________________________1.0_____\4256633266373761613434 2d3038346339312

HDD:
IDE\DiskLULZHARDDISK_____________________________1.0_____\4256313636366430636264 2d3664643335632
HDD:
IDE\DiskLULZHARDDISK_____________________________1.0_____\4256313636366430636264 2d3664643335632
HDD:
IDE\DiskVBOX_HARDDISK_____________________________1.0_____\4256343766616461316465 2d3532636366372

HDD:
IDE\DiskVBOX_HARDDISK_____________________________1.0_____\4256343766616461316465 2d3532636366372

HDD:
IDE\DiskLULZHARDDISK_____________________________1.0_____\4256313636366430636264 2d3664643335632
HDD:
IDE\DiskLULZHARDDISK_____________________________1.0_____\4256313636366430636264 2d3664643335632
HDD:
IDE\DiskVBOX_HARDDISK_____________________________1.0_____\4256373562373864636263 2d3032373130662

HDD:
IDE\DiskVBOX_HARDDISK_____________________________1.0_____\4256633266373761613434 2d3038346339312

HDD:
IDE\DiskVBOX_HARDDISK_____________________________1.0_____\4256373562373864636263 2d3032373130662

HDD:
IDE\DiskVBOX_HARDDISK_____________________________1.0_____\4256353937323132333934 2d3232396639312

HDD: IDE\DiskVbt1M09q57d_____________________________b85z49wmasoLEARKgMgsIr5F98Z
HDD: IDE\DiskFCS9sR15u0z_____________________________JCla6893Hr0LUyJTu1bzWoJ8m52
HDD:
IDE\DiskLULZHARDDISK_____________________________1.0_____\4256313636366430636264 2d3664643335632
HDD:
IDE\DiskVBOX_HARDDISK_____________________________1.0_____\4256323539613833343837 2d3239323239642
```

Виртульные машины в названии жесткого диска два варианта VBOX и LULZ

Process

Code:

```
frida-winjector-helper-32.exe
frida-winjector-helper-64.exe
pyw.exe
pythonw.exe
python.exe
```

Выше список приложений который были запущены на VM, я выделил только те, кто поддерживают работу системы аналитики.

Dll
Code:

```
frida-agent-32.dll
frida-agent-64.dll
```

Dll системы аналитики которые были добавлены к приложению.

GPU
Code:

```
Standard VGA Graphics Adapter
RDPDD Chained DD
RDP Encoder Mirror Driver
RDP Reflector Display Driver
VirtualBox Graphics Adapter
NetMeeting driver
RDPDD Chained DD
```

Видео карты - стандартные для VM

Исходники софта с библиотекой сбора информации и отчеты:
Link:
https://mega.nz/#!4dxi0Yib!2uA70PnfhgA07welpp0WUJnU4ACsmgySONZWD74gU40
Pass: exploit.in

Что нам это дает?
По вышеизложенным данным можно создать систему которая будет детектировать систему анализа построенную на виртуальной машине и обходить ее или не давать запускаться.
Это в свою очередь даст более долгий процесс не попадаться в базы данных антивирусных компаний.

PS: всем спасибо кто дочитал до конца

Дополню логами которые пришли через 10 часов. Эти логи показывают, что после автоматизированных систем анализа файл ушел реверсерам для ручного анализа и

подтверждения. Заметил еще, что к полноценным GUI системы более лояльно относятся.

Link: https://mega.nz/#!cV4BXYiK!IApNwnMT5Py_eMpCq21H4IyaFI-2oVgKC_G9z3_GDTU
Pass: exploit.in
(L1) cache