

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

The screenshot shows the VirusTotal interface for a file scan. The file is identified as 'tester.exe' with a size of 2.08 MB, scanned on 2019-12-20 at 08:39:32 UTC. A red banner indicates that 6 engines detected the file as malicious. A table below lists the detection results from various engines.

DETECTION	DETAILS	COMMUNITY
SecureAge APEX	Malicious	BitDefenderTheta, Gen.NN.ZelphiF.33556.fU0@a9D4bfi
eGambit	Unsafe.AL_Score_93%	FireEye, Generic.mg.98e68d0339c3155c
SentinelOne (Static ML)	DFI - Suspicious PE	VBA32, Adware.DealPly
Acronis	Undetected	Ad-Aware, Undetected
AegisLab	Undetected	AhnLab-V3, Undetected
Alibaba	Undetected	ALYac, Undetected
Antiy-AVL	Undetected	Arcabit, Undetected
Avast	Undetected	Avast-Mobile, Undetected
AVG	Undetected	Avira (no cloud), Undetected
Baidu	Undetected	BitDefender, Undetected

MetaDefender Opswat

Overview

- File Information Available
- Vulnerabilities
- Multiscanning 1
- Dynamic Analysis BETA
- Binary Reputation
- Scan History 1
- Community Feedback

Threats Found

ANALYZE AGAIN

tester.exe

SHA256 DE9DE8EE02E07A1044626964E18F533C6EEA2DD81C3C14659F625DC77F8C369C

THREAT NAME Adware/Unknown/Vh8FAbyp [Learn more](#)

MULTISCAN SCORE

1/39

[View full report](#)

VULNERABILITY SCORE

REPORT VULNERABILITY

No vulnerabilities reported!

CAST YOUR VOTE ON THIS FILE


0

0

[Check out our leaderboard](#)

You must be [Signed in](#) to vote

Jotti


















Jotti's malware scan Проверить файл Поиск хэша Язык ЧАВО (FAQ) Конфиденциальность Приложения API Свяжитесь с нами

testcon.exe

Имя: testcon.exe Размер: 968Кбайт (991 232 байт) Тип: PE32 executable (console) Intel 80386, for MS Windows Впервые замечен: 20 декабря 2019 г., 09:16:57 GMT+1 MD5: 2c50abca2d8a33657f9b69109715f878 SHA1: bb28597fed1901eed7e884b139aa6c10a0c3d64f

Статус: Проверка завершена. 0/15 антивирусов обнаружили вредоносный код. Дата проверки: 20 декабря 2019 г., 09:16:58 GMT+1

 20 дек. 2019 г. Ничего не найдено	 20 дек. 2019 г. Ничего не найдено	 19 дек. 2019 г. Ничего не найдено
 20 дек. 2019 г. Ничего не найдено	 20 дек. 2019 г. Ничего не найдено	 20 дек. 2019 г. Ничего не найдено
 20 дек. 2019 г. Ничего не найдено	 20 дек. 2019 г. Ничего не найдено	 19 дек. 2019 г. Ничего не найдено
 20 дек. 2019 г. Ничего не найдено	 19 дек. 2019 г. Ничего не найдено	 20 дек. 2019 г. Ничего не найдено
 20 дек. 2019 г. Ничего не найдено	 19 дек. 2019 г. Ничего не найдено	 19 дек. 2019 г. Ничего не найдено

© 2004-2019 Jotti

Hybrid-Analysis

HYBRID ANALYSIS Sandbox Quick Scans File Collections Resources Request Info

IP, Domain, Hash... More

Analysis Overview

Submission name: testcon.exe
Size: 968KiB
Type: [peexe](#) [executable](#)
Mime: application/x-dosexec
SHA256: 2fe67ccb537cedcead99b42849e97468e022544422a9fdfe06c668355242ed2
Operating System: Windows
Last Anti-Virus Scan: 12/20/2019 08:18:34 (UTC)
Last Sandbox Report: 12/20/2019 08:18:13 (UTC)

suspicious
Threat Score: 65/100

[Link](#) [Twitter](#) [E-Mail](#)

[Request Removal](#)

Analysis Overview

- Anti-Virus Scanner Results
- Falcon Sandbox Reports (1)
- Incident Response
- Community (0)

[Back to top](#)

Anti-Virus Results

[Refresh](#)

CrowdStrike Falcon	MetaDefender	VirusTotal
 CLEAN Static Analysis and ML Last Update: 12/20/2019 08:18:34 (UTC) View Details: N/A Visit Vendor: Visit Vendor	 CLEAN Multi Scan Analysis Last Update: 12/20/2019 08:18:34 (UTC) View Details: View Details Visit Vendor: Visit Vendor	 N/A Multi Scan Analysis Last Update: 12/20/2019 08:18:34 (UTC) View Details: N/A Visit Vendor: Visit Vendor

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

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_____\42563136363664306362642d3664643335632

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

pnrpns.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_ARCHITW6432=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

Виртуальные 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 анализа на виртуальных машина выше ос чем Windows 7 не используют.

Memory

Code:

127Mb
2047Mb

Виртуальные машины используют только 127 или 2047 Мб.

HDD

Code:

HDD:
IDE\DiskLULZHARDDISK_____1.0_____\42563136363664306362642d3664643335632
HDD:
IDE\DiskVBOX_HARDDISK_____1.0_____\42566332663737616134342d3038346339312

HDD:
IDE\DiskLULZHARDDISK_____1.0_____\42563136363664306362642d3664643335632
HDD:
IDE\DiskLULZHARDDISK_____1.0_____\42563136363664306362642d3664643335632
HDD:
IDE\DiskVBOX_HARDDISK_____1.0_____\42563437666164613164652d3532636366372

HDD:
IDE\DiskVBOX_HARDDISK_____1.0_____\42563437666164613164652d3532636366372

HDD:
IDE\DiskLULZHARDDISK_____1.0_____\42563136363664306362642d3664643335632
HDD:
IDE\DiskLULZHARDDISK_____1.0_____\42563136363664306362642d3664643335632
HDD:
IDE\DiskVBOX_HARDDISK_____1.0_____\42563735623738646362632d3032373130662

HDD:
IDE\DiskVBOX_HARDDISK_____1.0_____\42566332663737616134342d3038346339312

HDD:
IDE\DiskVBOX_HARDDISK_____1.0_____\42563735623738646362632d3032373130662

HDD:
IDE\DiskVBOX_HARDDISK_____1.0_____\42563539373231323339342d3232396639312

HDD: IDE\DiskVbt1M09q57d_____b85z49wmasoLEARKgMgsIr5F98Z
HDD: IDE\DiskFCS9sR15u0z_____JClA6893Hr0LUyJTU1bzWoJ8m52
HDD:
IDE\DiskLULZHARDDISK_____1.0_____\42563136363664306362642d3664643335632
HDD:
IDE\DiskVBOX_HARDDISK_____1.0_____\42563235396138333438372d3239323239642

Виртуальные машины в названии жесткого диска два варианта VBOX и LULZ

Process

Code:

frida-wininjector-helper-32.exe
frida-wininjector-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/#!4dxioYib!2uA7oPnfhgAo7welppoWUJnU4ACsmgySONZWD74gU4o>
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