HITB 2023, HACK IN THE BOX SECURITY CONFERENCE
Apr 17-21, 2023, AMSTERDAM, NL

All You Always Wanted to Know About AntiViruses

(and I had to hands-on to tell you!)

Marcus Botacin
Texas A&M University, USA
@MarcusBotacin

Publication

ELSEVIER

Computers & Security

Available online 12 October 2021, 102500

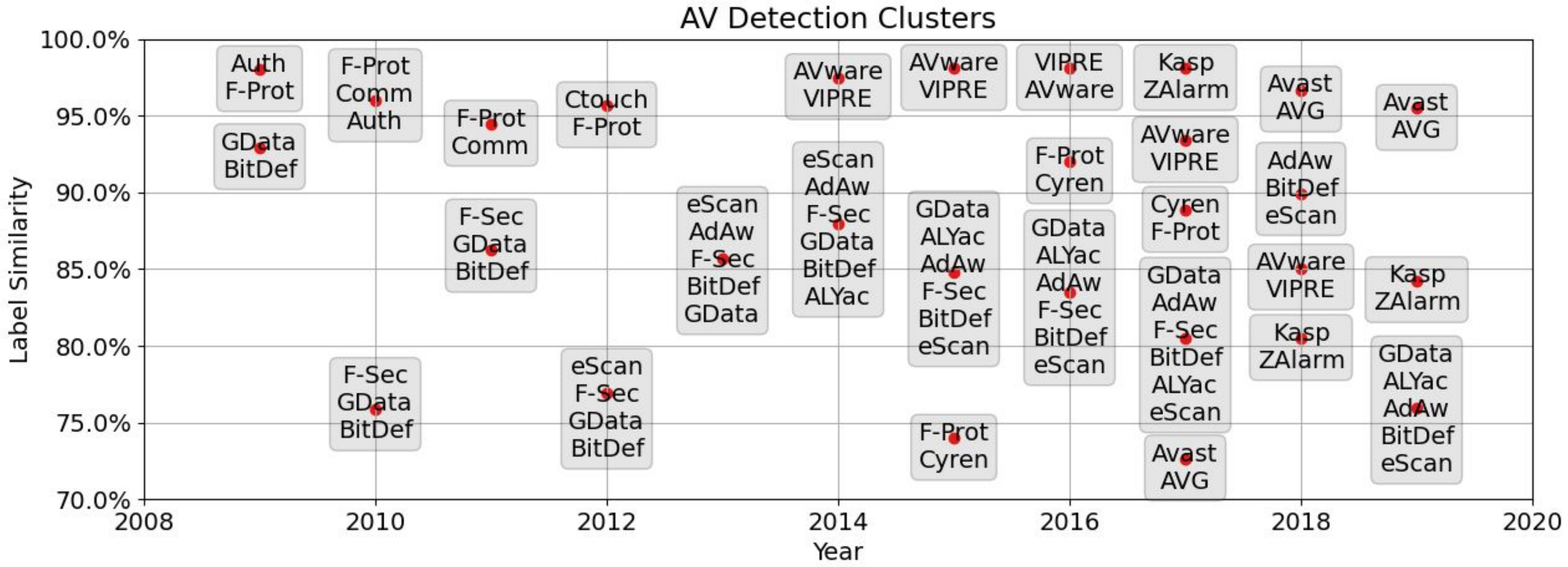
In Press, Journal Pre-proof ⓘ

AntiViruses under the Microscope: A Hands-On Perspective

Marcus Botacin [a] ✉, Felipe Duarte Domingues [b] ✉, Fabrício Ceschin [a] ✉, Raphael Machnicki [a] ✉, Marco Antonio Zanata Alves [a] ✉, Paulo Lício de Geus [b] ✉, André Grégio [a] ✉

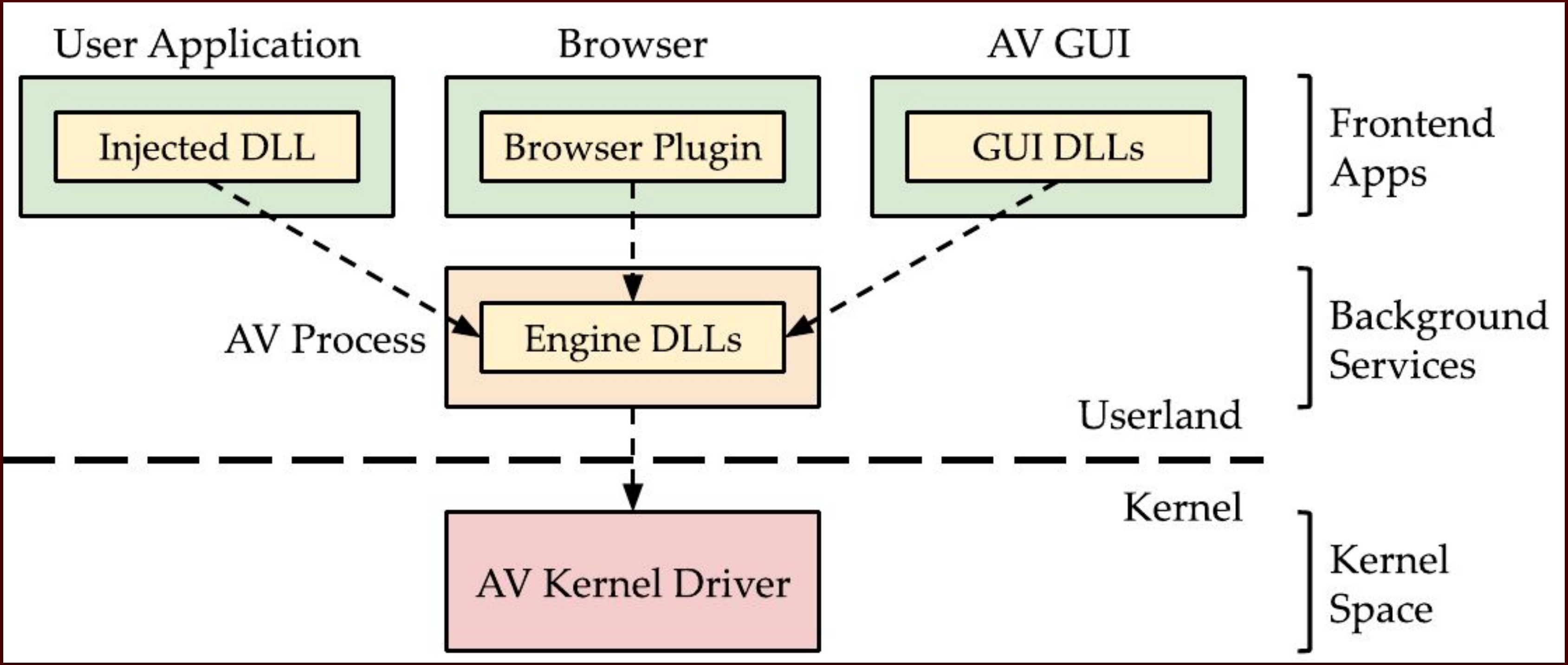
0x0. AV products are not the same as AV engines

Engine Sharing



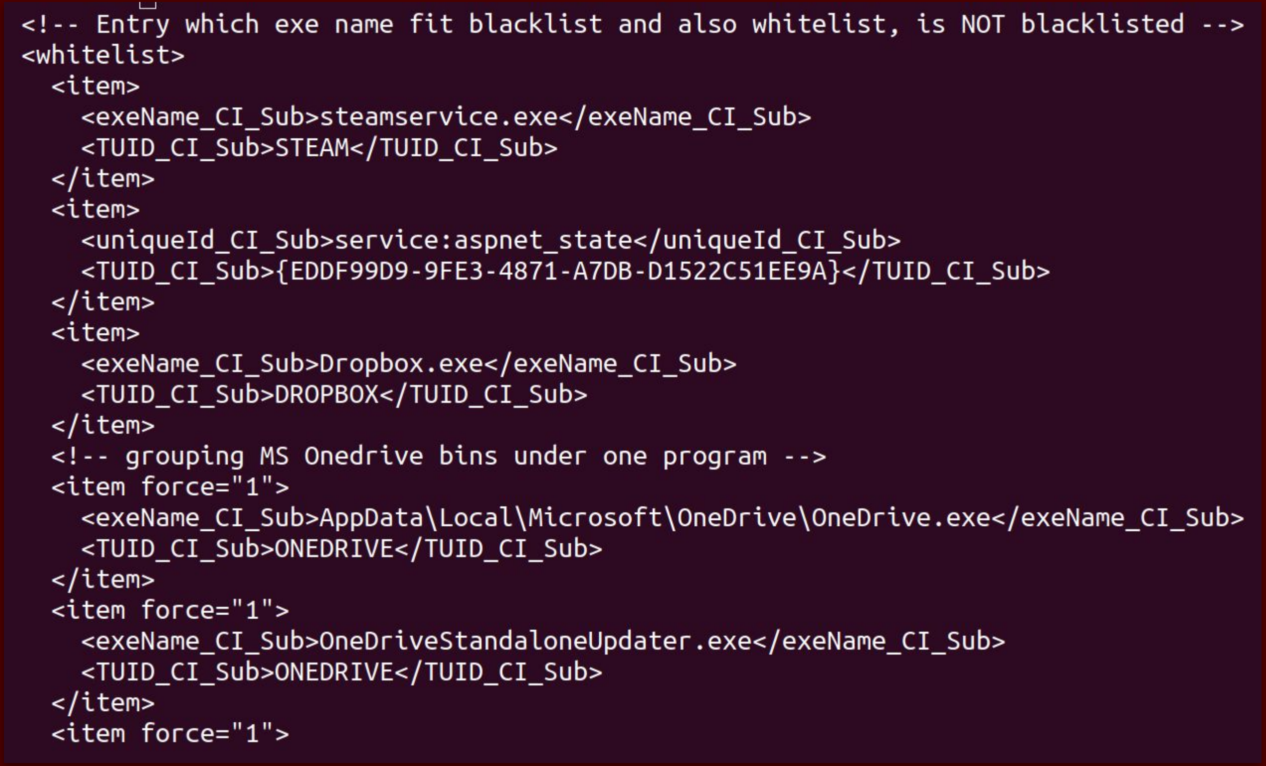
0x1. AVs have multiple components

AV Architecture



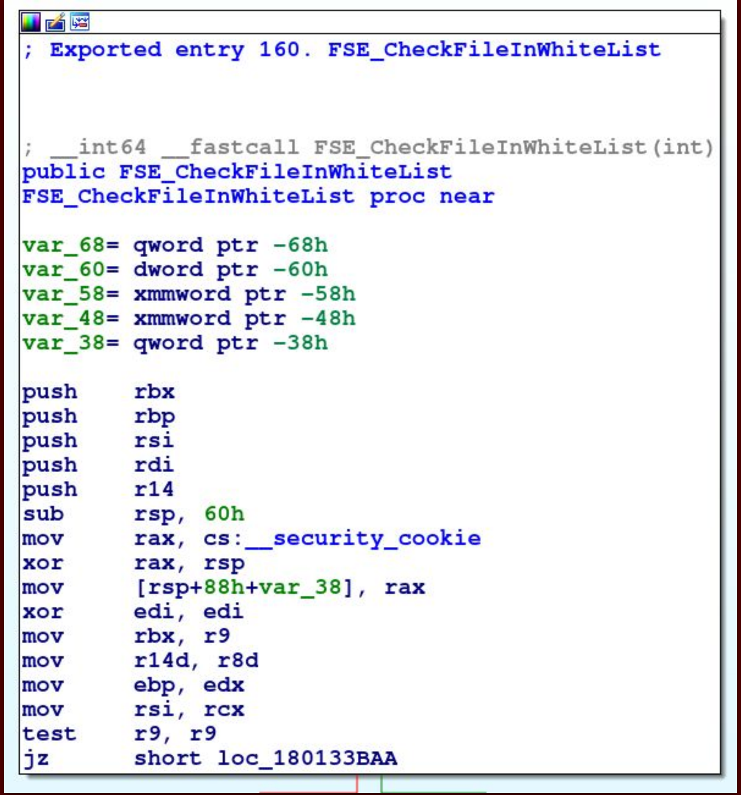
0x2. Whitelists are still widely used

Whitelisting



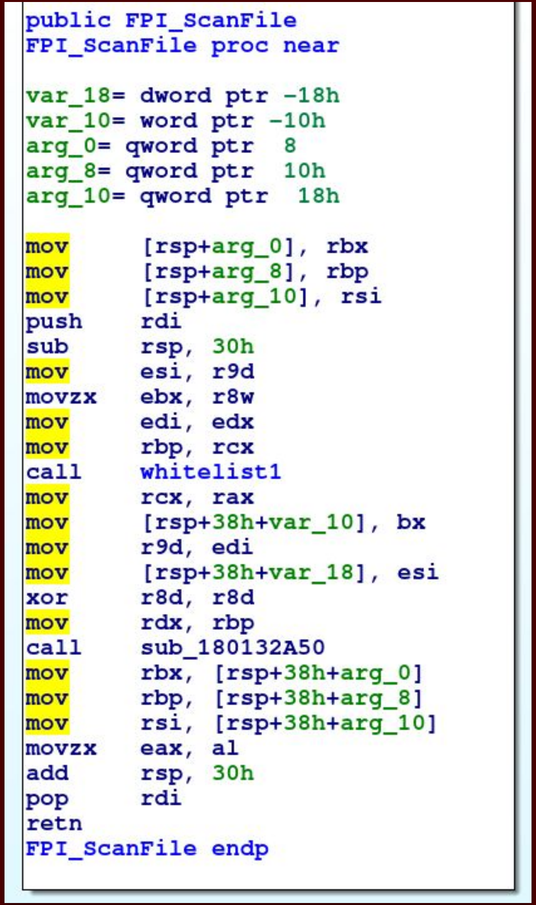
```
<!-- Entry which exe name fit blacklist and also whitelist, is NOT blacklisted -->
<whitelist>
  <item>
    <exeName_CI_Sub>steamservice.exe</exeName_CI_Sub>
    <TUID_CI_Sub>STEAM</TUID_CI_Sub>
  </item>
  <item>
    <uniqueId_CI_Sub>service:aspnet_state</uniqueId_CI_Sub>
    <TUID_CI_Sub>{EDDF99D9-9FE3-4871-A7DB-D1522C51EE9A}</TUID_CI_Sub>
  </item>
  <item>
    <exeName_CI_Sub>Dropbox.exe</exeName_CI_Sub>
    <TUID_CI_Sub>DROPBOX</TUID_CI_Sub>
  </item>
  <!-- grouping MS Onedrive bins under one program -->
  <item force="1">
    <exeName_CI_Sub>AppData\Local\Microsoft\OneDrive\OneDrive.exe</exeName_CI_Sub>
    <TUID_CI_Sub>ONEDRIVE</TUID_CI_Sub>
  </item>
  <item force="1">
    <exeName_CI_Sub>OneDriveStandaloneUpdater.exe</exeName_CI_Sub>
    <TUID_CI_Sub>ONEDRIVE</TUID_CI_Sub>
  </item>
  <item force="1">
```

Whitelisting



```
; Exported entry 160. FSE_CheckFileInWhiteList



; __int64 __fastcall FSE_CheckFileInWhiteList(int)
public FSE_CheckFileInWhiteList
FSE_CheckFileInWhiteList proc near

var_68= qword ptr -68h
var_60= dword ptr -60h
var_58= xmmword ptr -58h
var_48= xmmword ptr -48h
var_38= qword ptr -38h

push    rbx
push    rbp
push    rsi
push    rdi
push    r14
sub     rsp, 60h
mov     rax, cs:__security_cookie
xor     rax, rsp
mov     [rsp+88h+var_38], rax
xor     edi, edi
mov     rbx, r9
mov     r14d, r8d
mov     ebp, edx
mov     rsi, rcx
test    r9, r9
jz      short loc_180133BAA
```

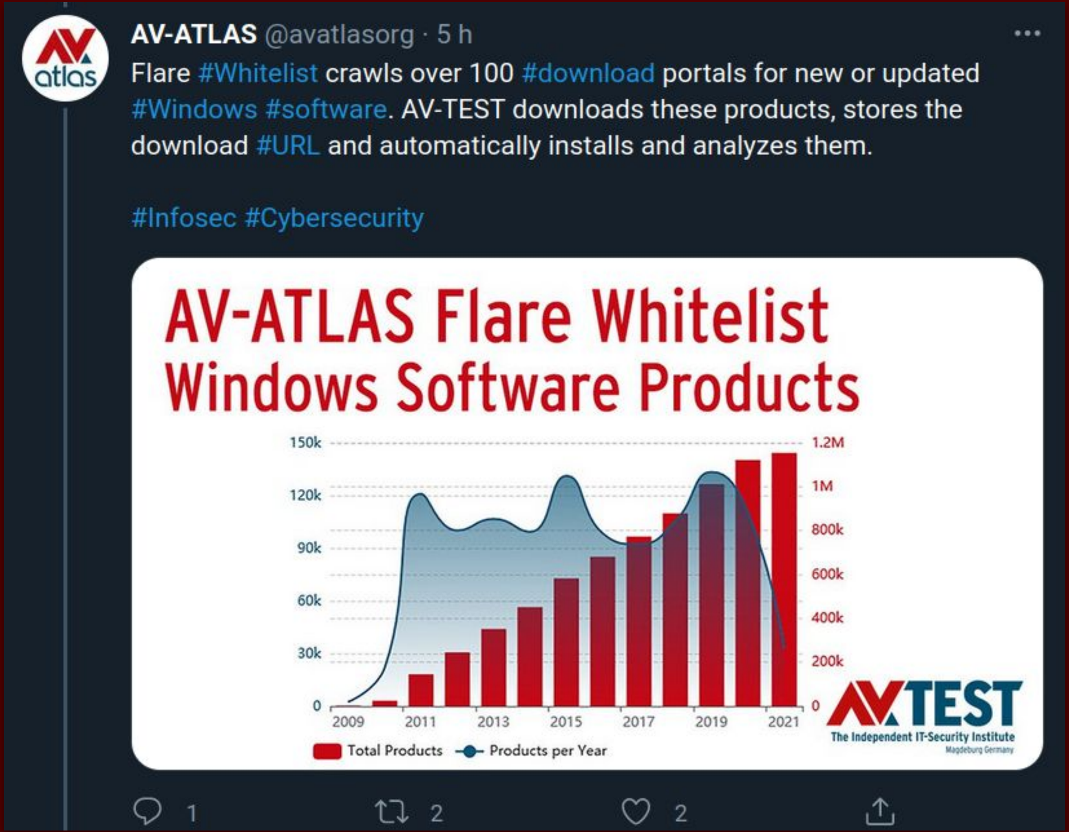
Whitelisting



```
public FPI_ScanFile
FPI_ScanFile proc near

var_18= dword ptr -18h
var_10= word ptr -10h
arg_0= qword ptr  8
arg_8= qword ptr  10h
arg_10= qword ptr  18h

mov     [rsp+arg_0], rbx
mov     [rsp+arg_8], rbp
mov     [rsp+arg_10], rsi
push    rdi
sub     rsp, 30h
mov     esi, r9d
movzx   ebx, r8w
mov     edi, edx
mov     rbp, rcx
call    whitelist1
mov     rcx, rax
mov     [rsp+38h+var_10], bx
mov     r9d, edi
mov     [rsp+38h+var_18], esi
xor     r8d, r8d
mov     rdx, rbp
call    sub_180132A50
mov     rbx, [rsp+38h+arg_0]
mov     rbp, [rsp+38h+arg_8]
mov     rsi, [rsp+38h+arg_10]
movzx   eax, al
add     rsp, 30h
pop     rdi
retn
FPI_ScanFile endp
```

0x3. Companies make money selling whitelisting data

Selling Whitelists

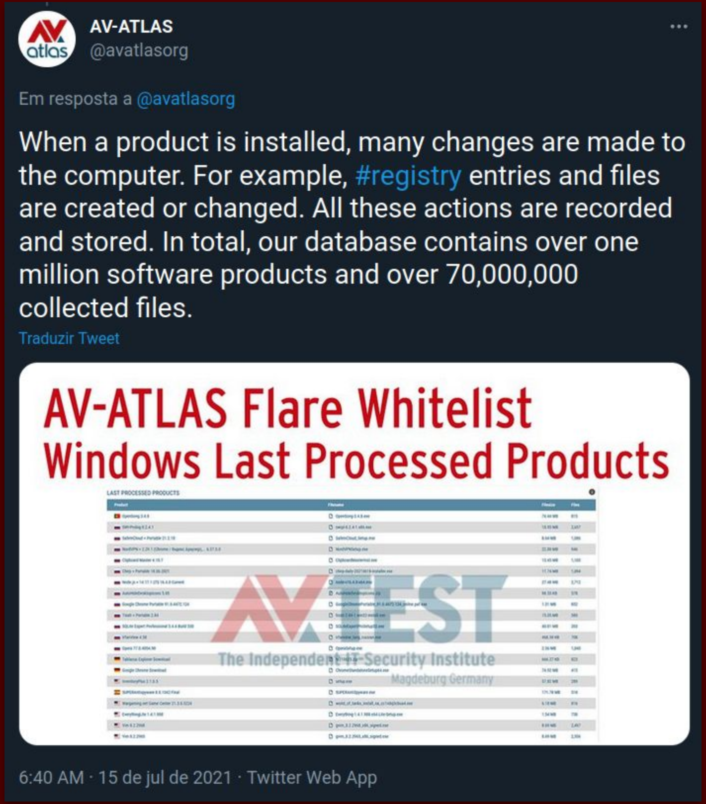


AV-ATLAS @avatlasorg · 5 h

Flare #Whitelist crawls over 100 #download portals for new or updated #Windows #software. AV-TEST downloads these products, stores the download #URL and automatically installs and analyzes them.

#Infosec #Cybersecurity

Selling Whitelists



AV-ATLAS
@avatlasorg

Em resposta a @avatlasorg

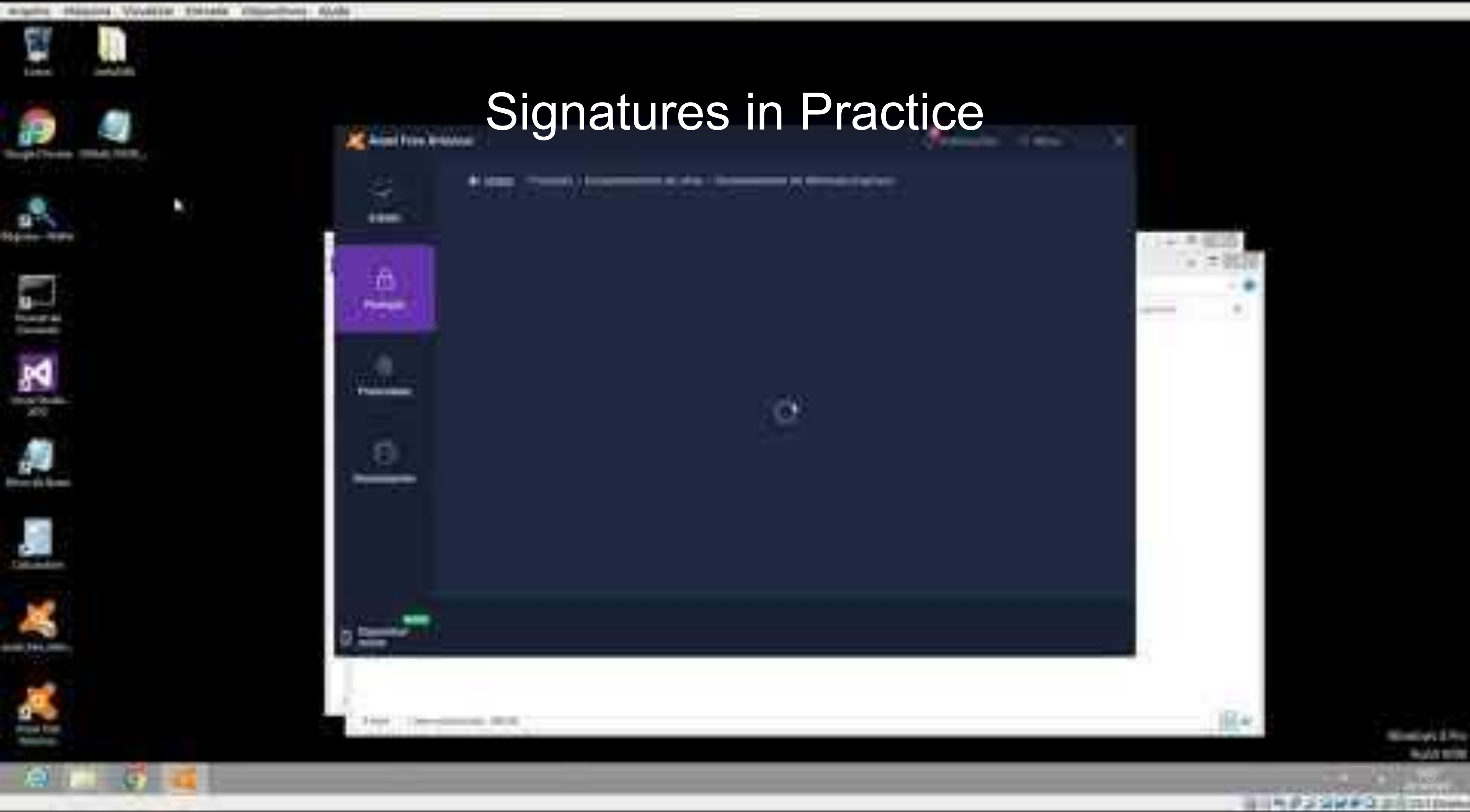
When a product is installed, many changes are made to the computer. For example, #registry entries and files are created or changed. All these actions are recorded and stored. In total, our database contains over one million software products and over 70,000,000 collected files.

Traduzir Tweet

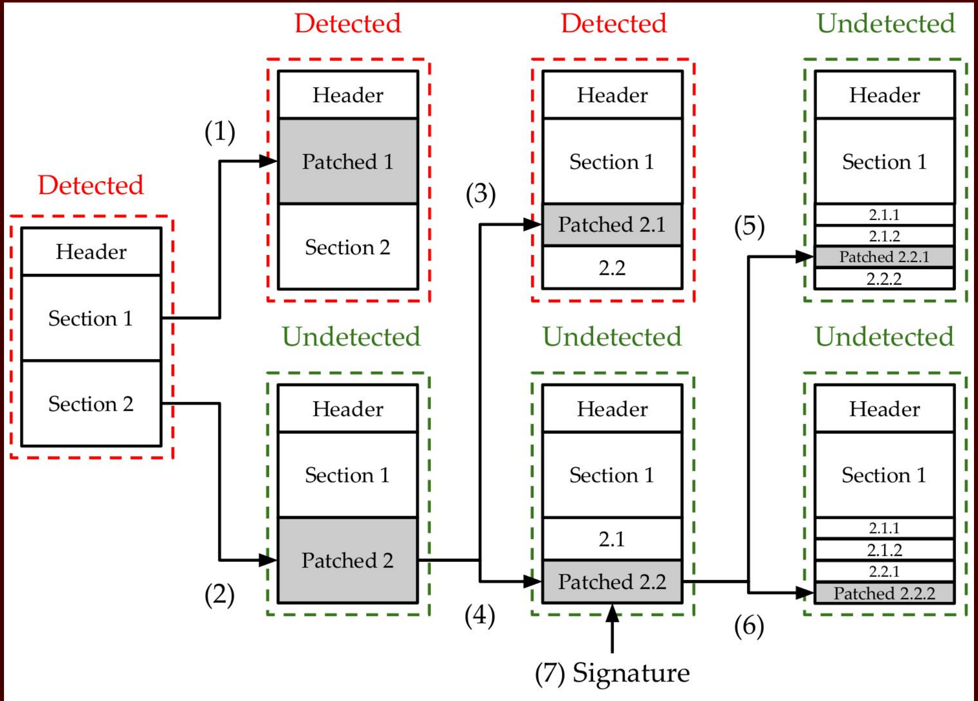
6:40 AM · 15 de jul de 2021 · Twitter Web App

0x4. Signatures are still widely used

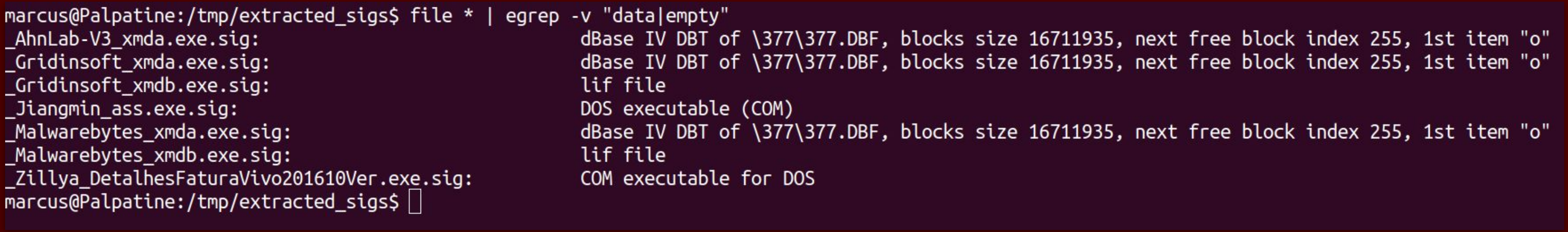
Signatures in Practice



Signature Extraction Algorithm

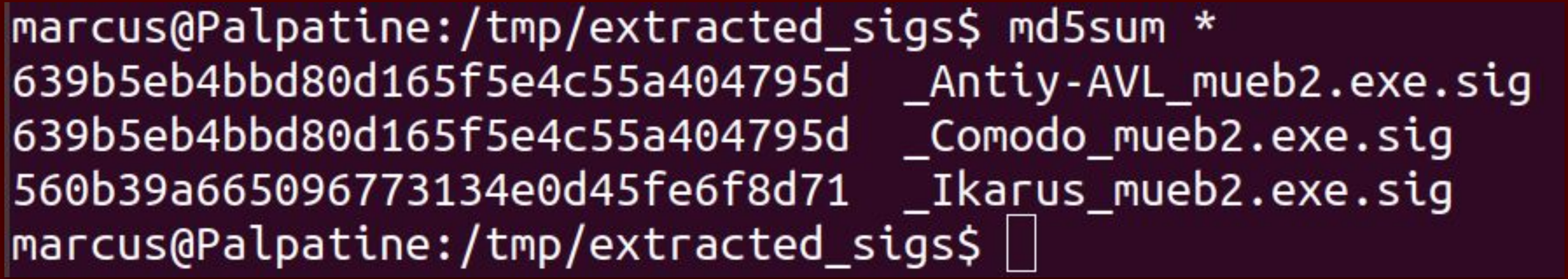


The extracted signatures



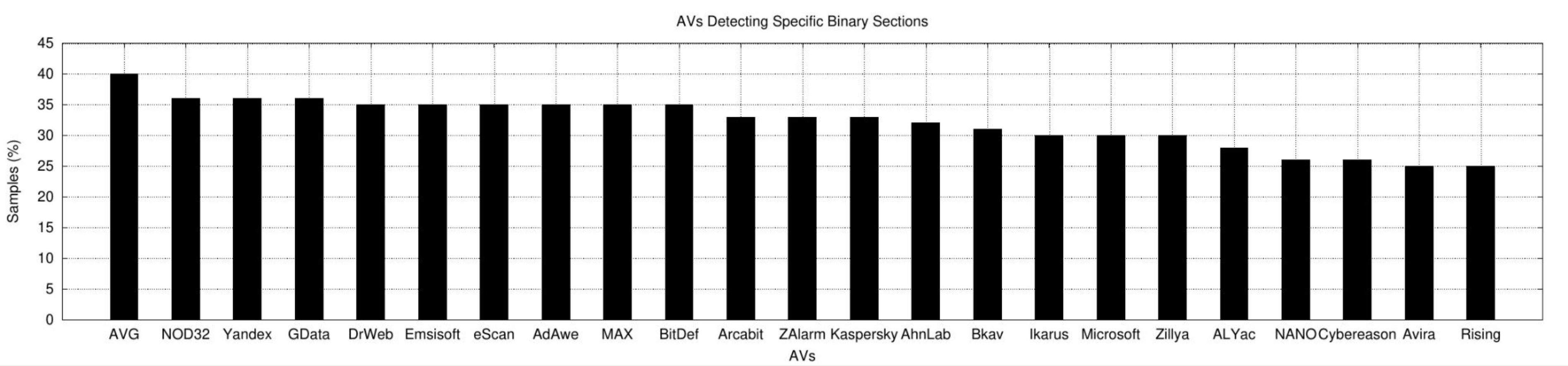
```
marcus@Palpatine:/tmp/extracted_sigs$ file * | egrep -v "data|empty"
_AhnLab-V3_xmda.exe.sig:                              dBase IV DBT of \377\377.DBF, blocks size 16711935, next free block index 255, 1st item "o"
_Gridinsoft_xmda.exe.sig:                             dBase IV DBT of \377\377.DBF, blocks size 16711935, next free block index 255, 1st item "o"
_Gridinsoft_xmdb.exe.sig:                             lif file
_Jiangmin_ass.exe.sig:                                DOS executable (COM)
_Malwarebytes_xmda.exe.sig:                           dBase IV DBT of \377\377.DBF, blocks size 16711935, next free block index 255, 1st item "o"
_Malwarebytes_xmdb.exe.sig:                           lif file
_Zillya_DetalhesFaturaVivo201610Ver.exe.sig:          COM executable for DOS
marcus@Palpatine:/tmp/extracted_sigs$ 
```

Signature Extraction Algorithm in Practice

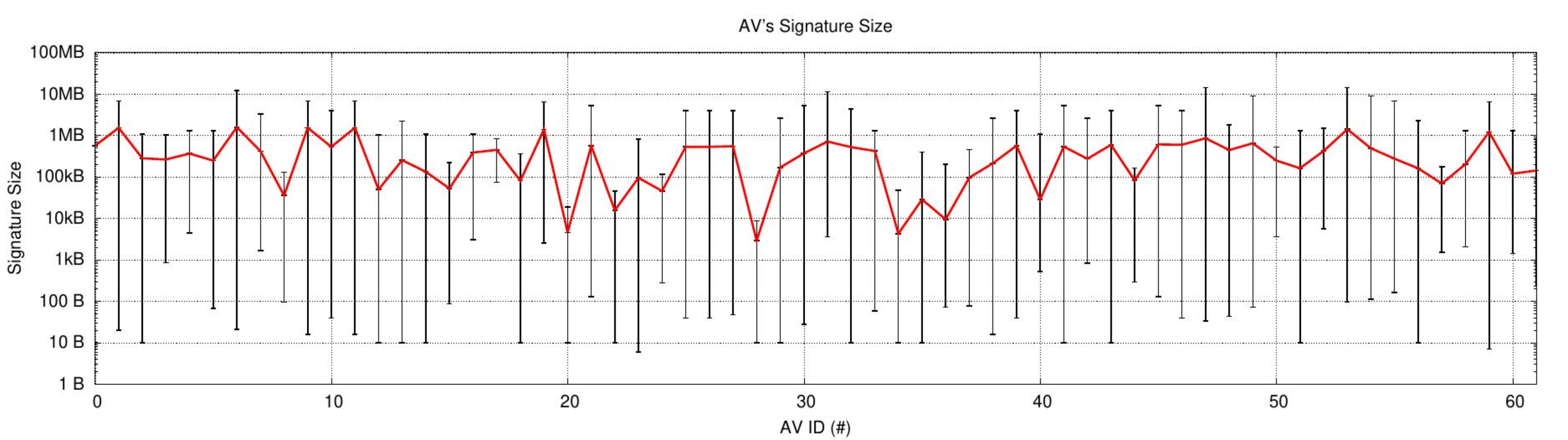


```
marcus@Palpatine:/tmp/extracted_sigs$ md5sum *
639b5eb4bbd80d165f5e4c55a404795d  _Antiy-AVL_mueb2.exe.sig
639b5eb4bbd80d165f5e4c55a404795d  _Comodo_mueb2.exe.sig
560b39a665096773134e0d45fe6f8d71  _Ikarus_mueb2.exe.sig
marcus@Palpatine:/tmp/extracted_sigs$ 
```

Signature Usage: Prevalence



Signature sizes



0x5. (Packed Malware) Detection is also a cost-benefit trade-off

Packers

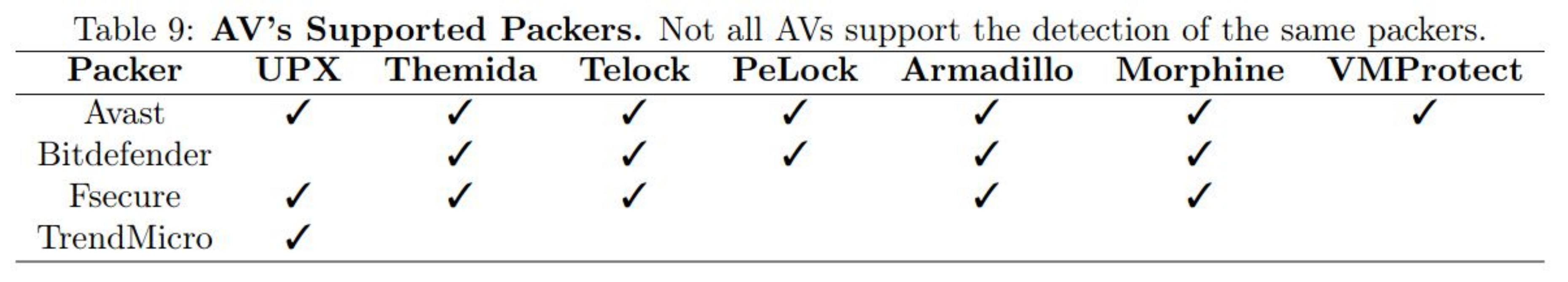
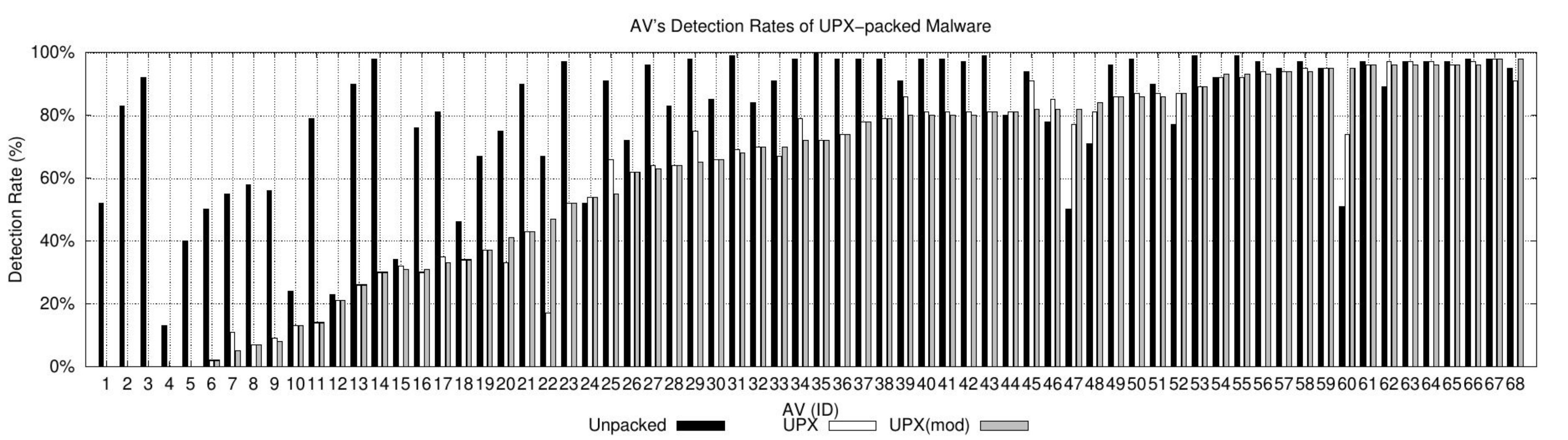


Table 9: **AV's Supported Packers.** Not all AVs support the detection of the same packers.

Packer	**UPX**	**Themida**	**Telock**	**PeLock**	**Armadillo**	**Morphine**	**VMProtect**
Avast	✓	✓	✓	✓	✓	✓	✓
Bitdefender		✓	✓	✓	✓	✓	
Fsecure	✓	✓	✓		✓	✓	
TrendMicro	✓						

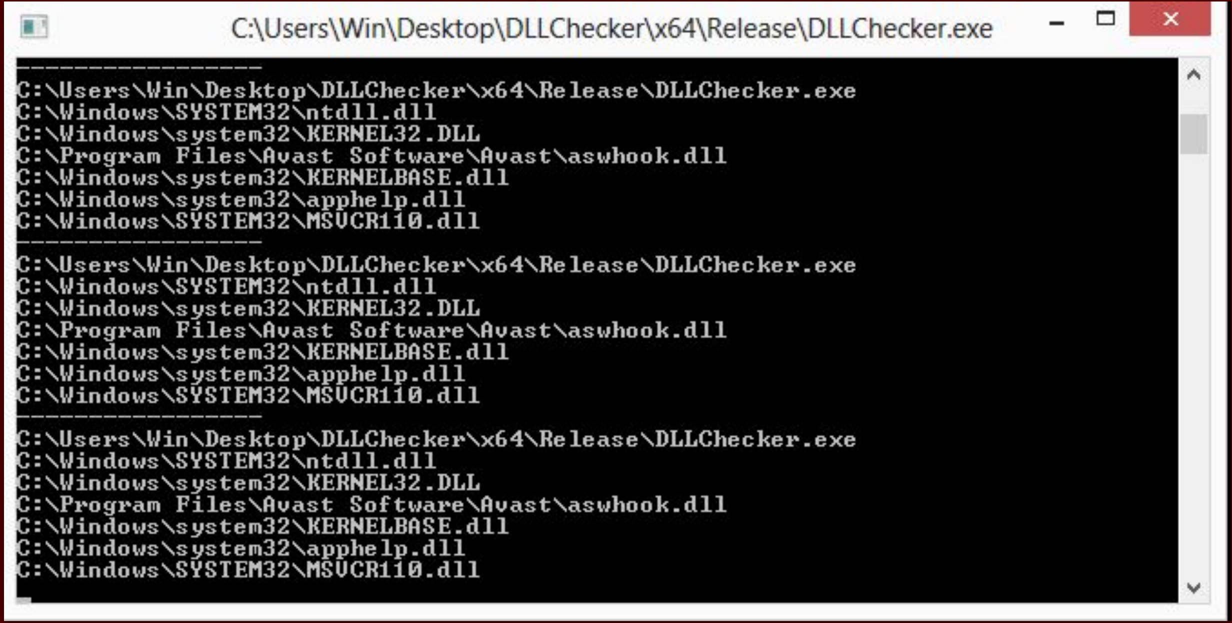
UPX support



AV's Detection Rates of UPX–packed Malware
Detection Rate (%)
100%
80%
60%
40%
20%
0%
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68
AV (ID)
Unpacked
UPX
UPX(mod)

0x6. AVs largely rely on userland hooking for data collection

Injected Libraries and hooks



```
------------------
C:\Users\Win\Desktop\DLLChecker\x64\Release\DLLChecker.exe
C:\Windows\SYSTEM32\ntdll.dll
C:\Windows\system32\KERNEL32.DLL
C:\Program Files\Avast Software\Avast\aswhook.dll
C:\Windows\system32\KERNELBASE.dll
C:\Windows\system32\apphelp.dll
C:\Windows\SYSTEM32\MSVCR110.dll
------------------
C:\Users\Win\Desktop\DLLChecker\x64\Release\DLLChecker.exe
C:\Windows\SYSTEM32\ntdll.dll
C:\Windows\system32\KERNEL32.DLL
C:\Program Files\Avast Software\Avast\aswhook.dll
C:\Windows\system32\KERNELBASE.dll
C:\Windows\system32\apphelp.dll
C:\Windows\SYSTEM32\MSVCR110.dll
------------------
C:\Users\Win\Desktop\DLLChecker\x64\Release\DLLChecker.exe
C:\Windows\SYSTEM32\ntdll.dll
C:\Windows\system32\KERNEL32.DLL
C:\Program Files\Avast Software\Avast\aswhook.dll
C:\Windows\system32\KERNELBASE.dll
C:\Windows\system32\apphelp.dll
C:\Windows\SYSTEM32\MSVCR110.dll
```

Try yourself!

Libs and Machine Learning: A Discussion

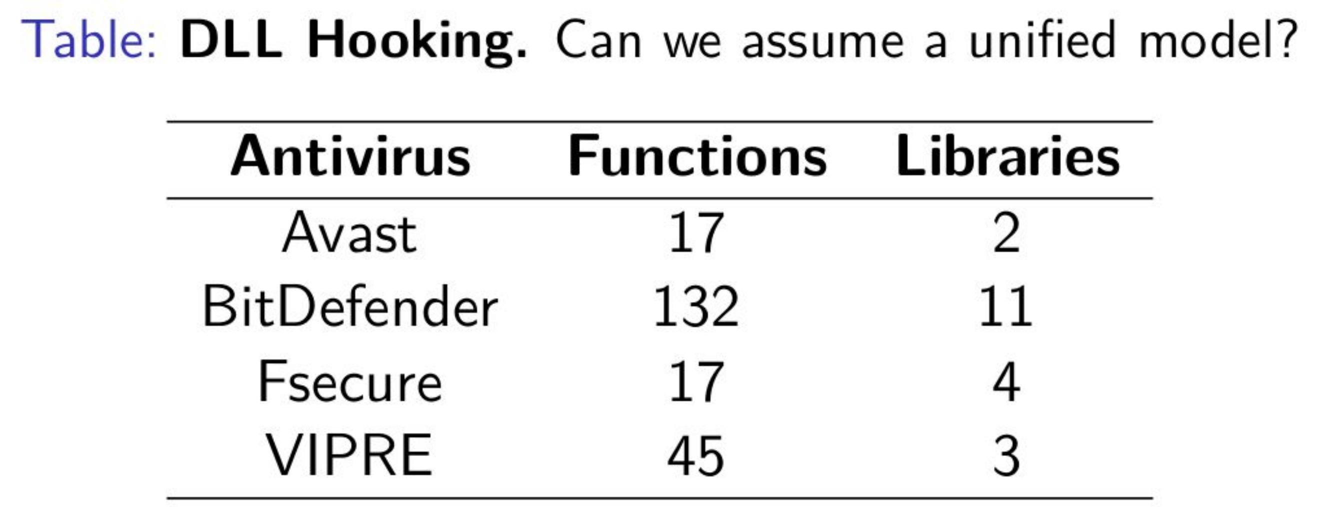


Table: **DLL Hooking.** Can we assume a unified model?

Antivirus	**Functions**	**Libraries**
Avast	17	2
BitDefender	132	11
Fsecure	17	4
VIPRE	45	3

0x7. AVs largely rely on kernel driver for self-protection

Kernel Filters and Callbacks

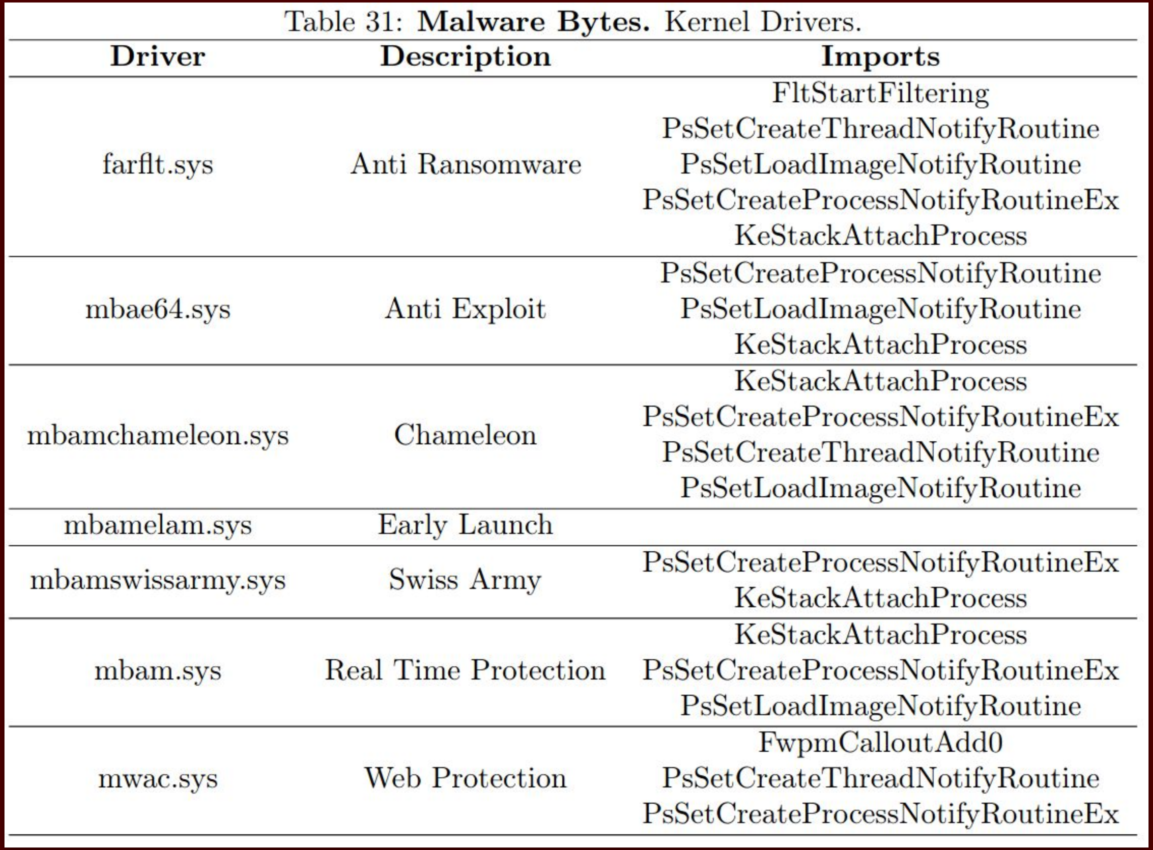


Table 31: **Malware Bytes.** Kernel Drivers.

Driver	Description	Imports
farflt.sys	Anti Ransomware	FltStartFiltering PsSetCreateThreadNotifyRoutine PsSetLoadImageNotifyRoutine PsSetCreateProcessNotifyRoutineEx KeStackAttachProcess
mbae64.sys	Anti Exploit	PsSetCreateProcessNotifyRoutine PsSetLoadImageNotifyRoutine KeStackAttachProcess
mbamchameleon.sys	Chameleon	KeStackAttachProcess PsSetCreateProcessNotifyRoutineEx PsSetCreateThreadNotifyRoutine PsSetLoadImageNotifyRoutine
mbamelam.sys	Early Launch	
mbamswissarmy.sys	Swiss Army	PsSetCreateProcessNotifyRoutineEx KeStackAttachProcess
mbam.sys	Real Time Protection	KeStackAttachProcess PsSetCreateProcessNotifyRoutineEx PsSetLoadImageNotifyRoutine
mwac.sys	Web Protection	FwpmCalloutAdd0 PsSetCreateThreadNotifyRoutine PsSetCreateProcessNotifyRoutineEx

Access Control

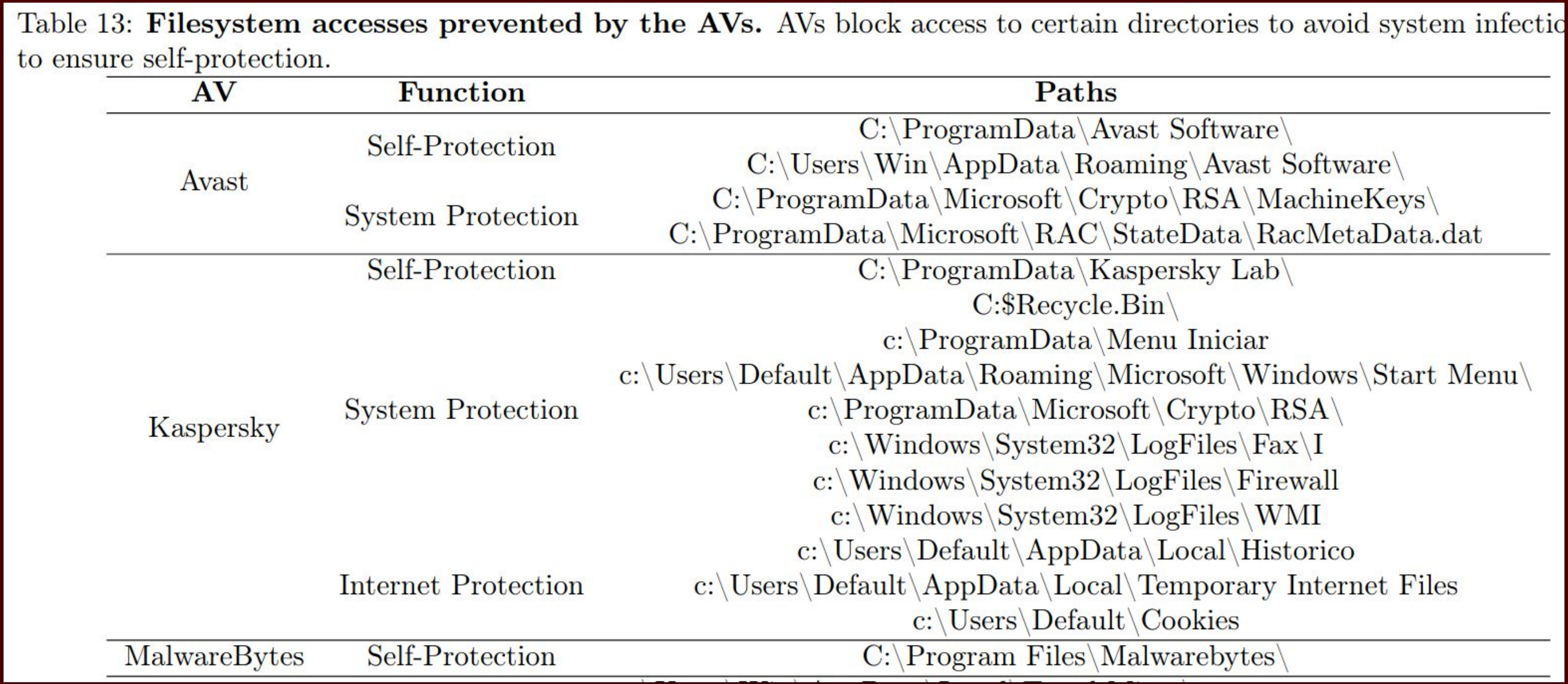
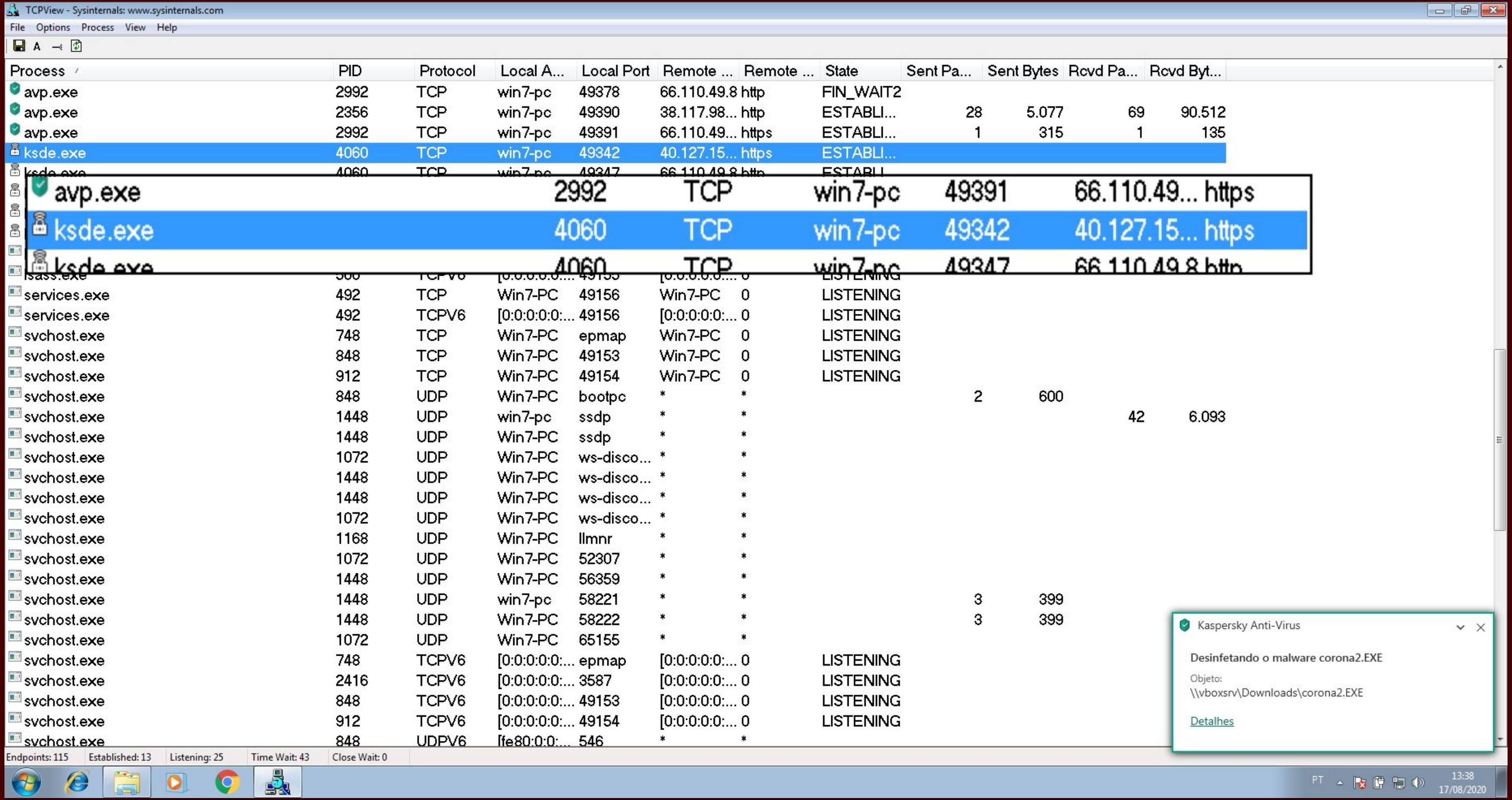


Table 13: **Filesystem accesses prevented by the AVs.** AVs block access to certain directories to avoid system infectio to ensure self-protection.

AV	Function	Paths
Avast	Self-Protection	C:\ProgramData\Avast Software\
		C:\Users\Win\AppData\Roaming\Avast Software\
	System Protection	C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\
		C:\ProgramData\Microsoft\RAC\StateData\RacMetaData.dat
Kaspersky	Self-Protection	C:\ProgramData\Kaspersky Lab\
	System Protection	C:$Recycle.Bin\
		c:\ProgramData\Menu Iniciar
		c:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\
		c:\ProgramData\Microsoft\Crypto\RSA\
		c:\Windows\System32\LogFiles\Fax\I
		c:\Windows\System32\LogFiles\Firewall
		c:\Windows\System32\LogFiles\WMI
	Internet Protection	c:\Users\Default\AppData\Local\Historico
		c:\Users\Default\AppData\Local\Temporary Internet Files
		c:\Users\Default\Cookies
MalwareBytes	Self-Protection	C:\Program Files\Malwarebytes\

0x8. AVs “spy” on your network traffic

Network Process: avp (Kaspersky)



TCPView - Sysinternals: www.sysinternals.com

Process	PID	Protocol	Local A...	Local Port	Remote ...	Remote ...	State	Sent Pa...	Sent Bytes	Rcvd Pa...	Rcvd Byt...
avp.exe	2992	TCP	win7-pc	49378	66.110.49.8	http	FIN_WAIT2				
avp.exe	2356	TCP	win7-pc	49390	38.117.98...	http	ESTABLI...	28	5.077	69	90.512
avp.exe	2992	TCP	win7-pc	49391	66.110.49...	https	ESTABLI...	1	315	1	135
ksde.exe	4060	TCP	win7-pc	49342	40.127.15...	https	ESTABLI...				
ksde.exe	4060	TCP	win7-pc	49347	66.110.49.8	http	ESTABLI...				
lsass.exe	500	TCPV6	[0:0:0:0:0:...	49155	[0:0:0:0:0:...	0	LISTENING				
services.exe	492	TCP	Win7-PC	49156	Win7-PC	0	LISTENING				
services.exe	492	TCPV6	[0:0:0:0:0:...	49156	[0:0:0:0:0:...	0	LISTENING				
svchost.exe	748	TCP	Win7-PC	epmap	Win7-PC	0	LISTENING				
svchost.exe	848	TCP	Win7-PC	49153	Win7-PC	0	LISTENING				
svchost.exe	912	TCP	Win7-PC	49154	Win7-PC	0	LISTENING				
svchost.exe	848	UDP	Win7-PC	bootpc	*	*		2	600		
svchost.exe	1448	UDP	win7-pc	ssdp	*	*				42	6.093
svchost.exe	1448	UDP	Win7-PC	ssdp	*	*					
svchost.exe	1072	UDP	Win7-PC	ws-disco...	*	*					
svchost.exe	1448	UDP	Win7-PC	ws-disco...	*	*					
svchost.exe	1448	UDP	Win7-PC	ws-disco...	*	*					
svchost.exe	1072	UDP	Win7-PC	ws-disco...	*	*					
svchost.exe	1168	UDP	Win7-PC	llmnr	*	*					
svchost.exe	1072	UDP	Win7-PC	52307	*	*					
svchost.exe	1448	UDP	Win7-PC	56359	*	*					
svchost.exe	1448	UDP	win7-pc	58221	*	*		3	399		
svchost.exe	1448	UDP	Win7-PC	58222	*	*		3	399		
svchost.exe	1072	UDP	Win7-PC	65155	*	*					
svchost.exe	748	TCPV6	[0:0:0:0:0:...	epmap	[0:0:0:0:0:...	0	LISTENING				
svchost.exe	2416	TCPV6	[0:0:0:0:0:...	3587	[0:0:0:0:0:...	0	LISTENING				
svchost.exe	848	TCPV6	[0:0:0:0:0:...	49153	[0:0:0:0:0:...	0	LISTENING				
svchost.exe	912	TCPV6	[0:0:0:0:0:...	49154	[0:0:0:0:0:...	0	LISTENING				
svchost.exe	848	UDPV6	[fe80:0:0:...	546	*	*					

avp.exe	2992	TCP	win7-pc	49391	66.110.49... https
ksde.exe	4060	TCP	win7-pc	49342	40.127.15... https
ksde.exe	4060	TCP	win7-pc	49347	66.110.49.8 http

Endpoints: 115 Established: 13 Listening: 25 Time Wait: 43 Close Wait: 0

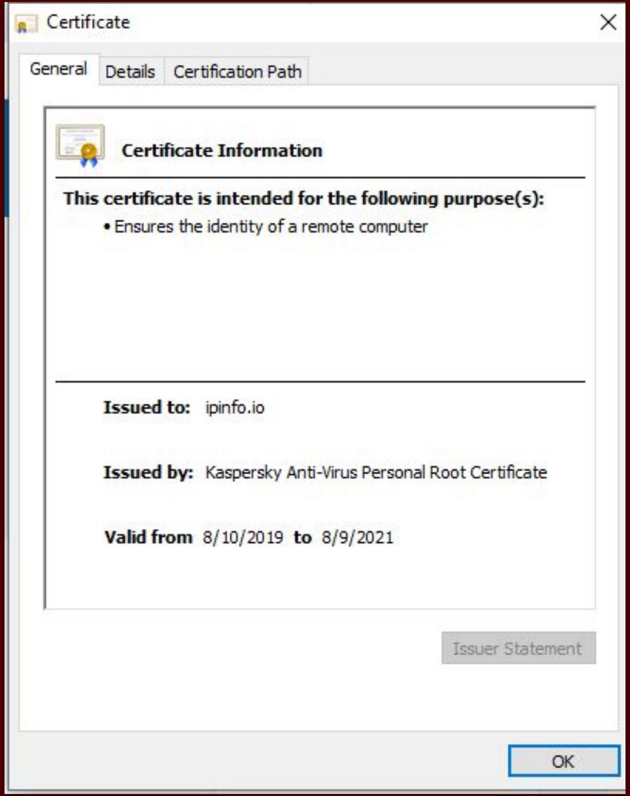
Kaspersky Anti-Virus

Desinfetando o malware corona2.EXE

Objeto:
\\vboxsrv\Downloads\corona2.EXE

Detalhes

Network Certificates



Certificate Information

This certificate is intended for the following purpose(s):

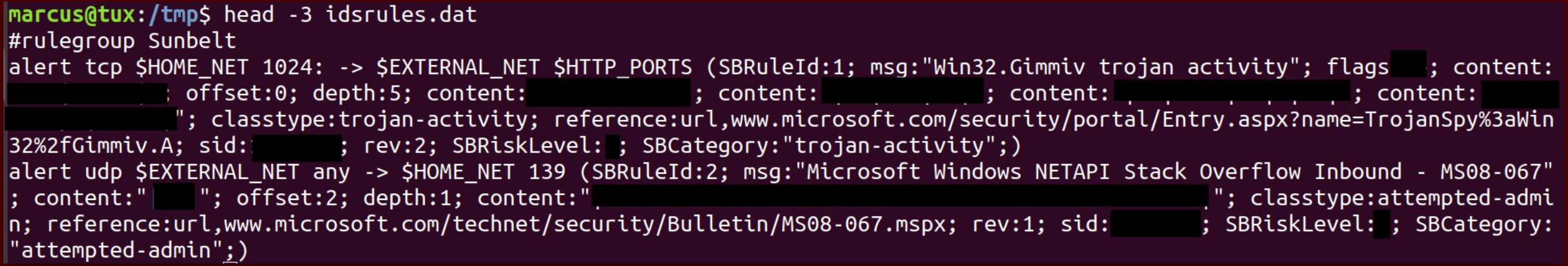
- Ensures the identity of a remote computer

Issued to: ipinfo.io

Issued by: Kaspersky Anti-Virus Personal Root Certificate

Valid from 8/10/2019 **to** 8/9/2021

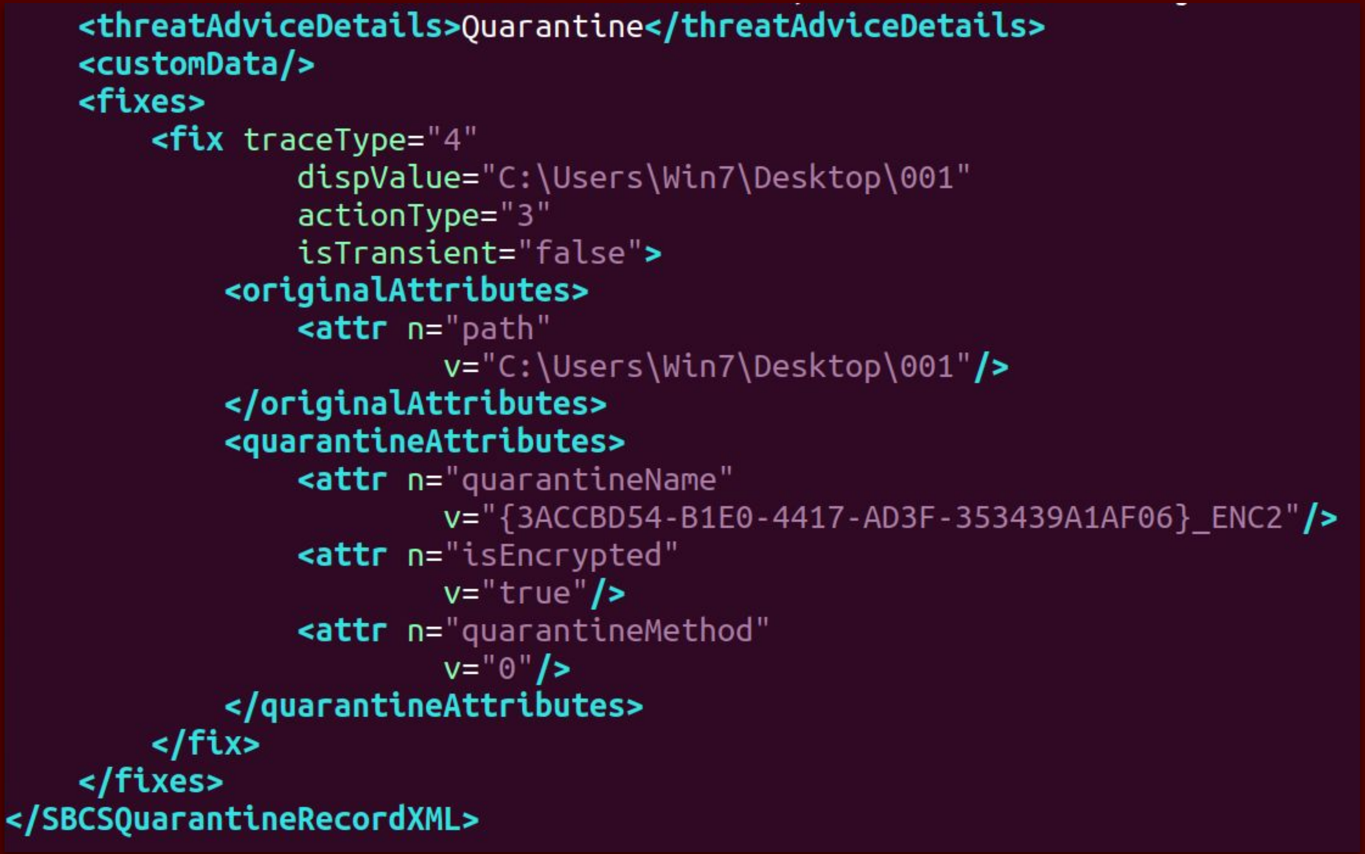
Snort Rules (VIPRE)



```
marcus@tux:/tmp$ head -3 idsrules.dat
#rulegroup Sunbelt
alert tcp $HOME_NET 1024: -> $EXTERNAL_NET $HTTP_PORTS (SBRuleId:1; msg:"Win32.Gimmiv trojan activity"; flags[redacted]; content:
[redacted]; offset:0; depth:5; content:[redacted]; content:[redacted]; content:[redacted]; content:[redacted]
[redacted]"; classtype:trojan-activity; reference:url,www.microsoft.com/security/portal/Entry.aspx?name=TrojanSpy%3aWin
32%2fGimmiv.A; sid:[redacted]; rev:2; SBRiskLevel:[redacted]; SBCategory:"trojan-activity";)
alert udp $EXTERNAL_NET any -> $HOME_NET 139 (SBRuleId:2; msg:"Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067"
; content:"[redacted]"; offset:2; depth:1; content:"[redacted]"; classtype:attempted-admi
n; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; rev:1; sid:[redacted]; SBRiskLevel:[redacted]; SBCategory:
"attempted-admin";)
```

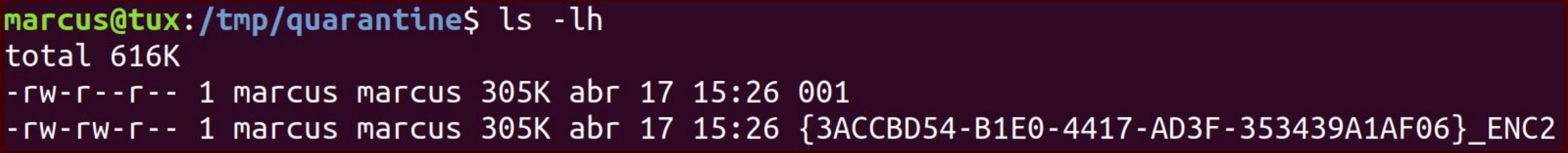
0x9. AVs store files in quarentines

Quarantine: Encoded File Information



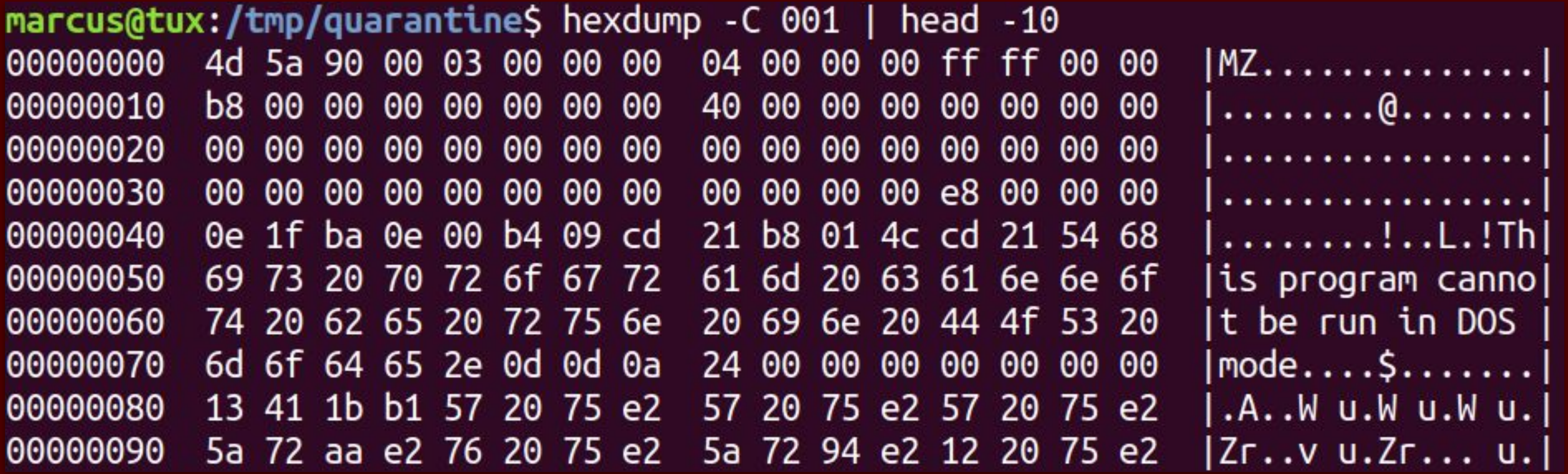
```
    <threatAdviceDetails>Quarantine</threatAdviceDetails>
    <customData/>
    <fixes>
        <fix traceType="4"
                dispValue="C:\Users\Win7\Desktop\001"
                actionType="3"
                isTransient="false">
            <originalAttributes>
                <attr n="path"
                        v="C:\Users\Win7\Desktop\001"/>
            </originalAttributes>
            <quarantineAttributes>
                <attr n="quarantineName"
                        v="{3ACCBD54-B1E0-4417-AD3F-353439A1AF06}_ENC2"/>
                <attr n="isEncrypted"
                        v="true"/>
                <attr n="quarantineMethod"
                        v="0"/>
            </quarantineAttributes>
        </fix>
    </fixes>
</SBCSQuarantineRecordXML>
```

Quarantine



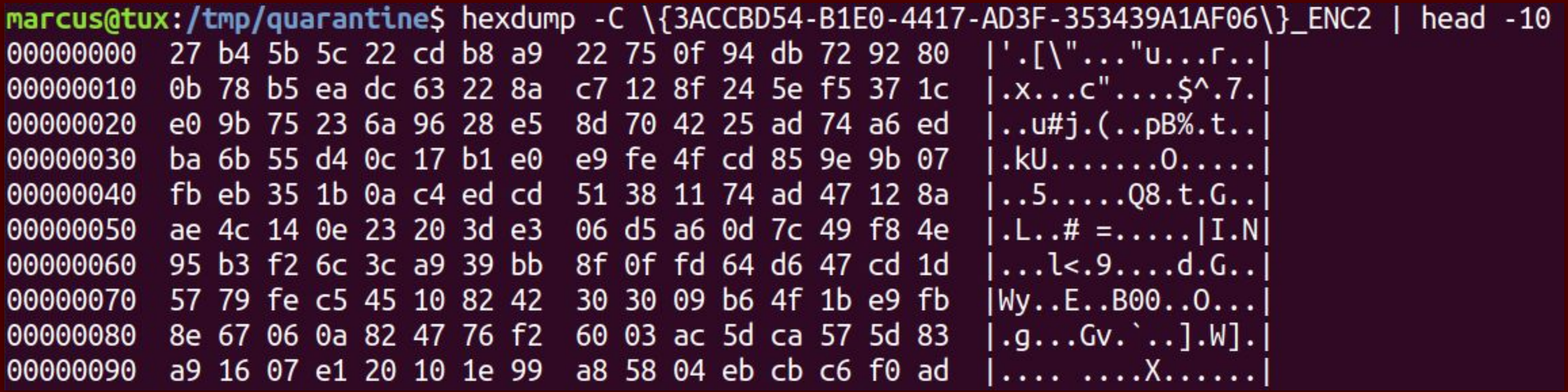
```
marcus@tux:/tmp/quarantine$ ls -lh
total 616K
-rw-r--r-- 1 marcus marcus 305K abr 17 15:26 001
-rw-rw-r-- 1 marcus marcus 305K abr 17 15:26 {3ACCBD54-B1E0-4417-AD3F-353439A1AF06}_ENC2
```

Quarantine: Original File



```
marcus@tux:/tmp/quarantine$ hexdump -C 001 | head -10
00000000  4d 5a 90 00 03 00 00 00  04 00 00 00 ff ff 00 00  |MZ..............|
00000010  b8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  |........@.......|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 e8 00 00 00  |................|
00000040  0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68  |........!..L.!Th|
00000050  69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f  |is program canno|
00000060  74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20  |t be run in DOS |
00000070  6d 6f 64 65 2e 0d 0d 0a  24 00 00 00 00 00 00 00  |mode....$.......|
00000080  13 41 1b b1 57 20 75 e2  57 20 75 e2 57 20 75 e2  |.A..W u.W u.W u.|
00000090  5a 72 aa e2 76 20 75 e2  5a 72 94 e2 12 20 75 e2  |Zr..v u.Zr... u.|
```

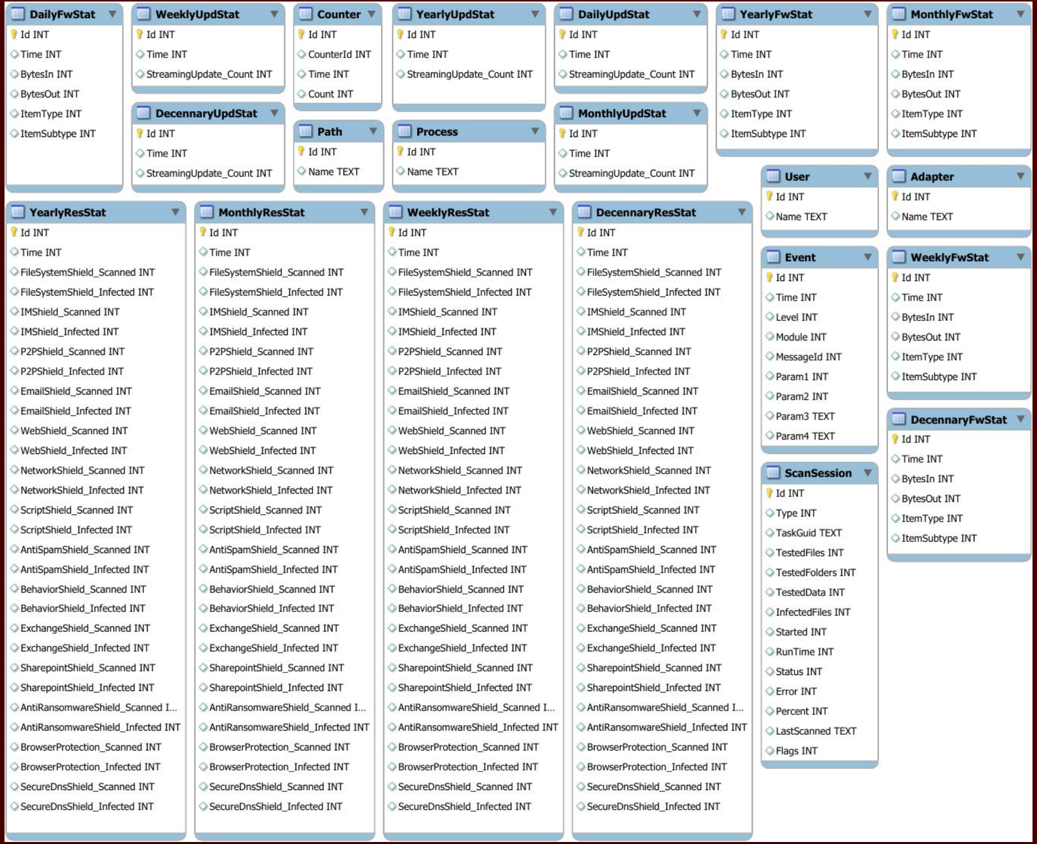
Quarantine: Encoded File



```
marcus@tux:/tmp/quarantine$ hexdump -C \{3ACCBD54-B1E0-4417-AD3F-353439A1AF06\}_ENC2 | head -10
00000000  27 b4 5b 5c 22 cd b8 a9  22 75 0f 94 db 72 92 80  |'.[\"..."u...r..|
00000010  0b 78 b5 ea dc 63 22 8a  c7 12 8f 24 5e f5 37 1c  |.x...c"....$^.7.|
00000020  e0 9b 75 23 6a 96 28 e5  8d 70 42 25 ad 74 a6 ed  |..u#j.(..pB%.t..|
00000030  ba 6b 55 d4 0c 17 b1 e0  e9 fe 4f cd 85 9e 9b 07  |.kU.......O.....|
00000040  fb eb 35 1b 0a c4 ed cd  51 38 11 74 ad 47 12 8a  |..5.....Q8.t.G..|
00000050  ae 4c 14 0e 23 20 3d e3  06 d5 a6 0d 7c 49 f8 4e  |.L..# =.....|I.N|
00000060  95 b3 f2 6c 3c a9 39 bb  8f 0f fd 64 d6 47 cd 1d  |...l<.9....d.G..|
00000070  57 79 fe c5 45 10 82 42  30 30 09 b6 4f 1b e9 fb  |Wy..E..B00..O...|
00000080  8e 67 06 0a 82 47 76 f2  60 03 ac 5d ca 57 5d 83  |.g...Gv.`..].W].|
00000090  a9 16 07 e1 20 10 1e 99  a8 58 04 eb cb c6 f0 ad  |.... ....X......|
```

0xA. AVs collect lots of data from you and about you

Databases and Logs



DailyFwStat
Id INT
Time INT
BytesIn INT
BytesOut INT
ItemType INT
ItemSubtype INT

WeeklyUpdStat
Id INT
Time INT
StreamingUpdate_Count INT

DecennaryUpdStat
Id INT
Time INT
StreamingUpdate_Count INT

Counter
Id INT
CounterId INT
Time INT
Count INT

Path
Id INT
Name TEXT

YearlyUpdStat
Id INT
Time INT
StreamingUpdate_Count INT

Process
Id INT
Name TEXT

DailyUpdStat
Id INT
Time INT
StreamingUpdate_Count INT

MonthlyUpdStat
Id INT
Time INT
StreamingUpdate_Count INT

YearlyFwStat
Id INT
Time INT
BytesIn INT
BytesOut INT
ItemType INT
ItemSubtype INT

MonthlyFwStat
Id INT
Time INT
BytesIn INT
BytesOut INT
ItemType INT
ItemSubtype INT

User
Id INT
Name TEXT

Adapter
Id INT
Name TEXT

YearlyResStat
Id INT
Time INT
FileSystemShield_Scanned INT
FileSystemShield_Infected INT
IMShield_Scanned INT
IMShield_Infected INT
P2PShield_Scanned INT
P2PShield_Infected INT
EmailShield_Scanned INT
EmailShield_Infected INT
WebShield_Scanned INT
WebShield_Infected INT
NetworkShield_Scanned INT
NetworkShield_Infected INT
ScriptShield_Scanned INT
ScriptShield_Infected INT
AntiSpamShield_Scanned INT
AntiSpamShield_Infected INT
BehaviorShield_Scanned INT
BehaviorShield_Infected INT
ExchangeShield_Scanned INT
ExchangeShield_Infected INT
SharepointShield_Scanned INT
SharepointShield_Infected INT
AntiRansomwareShield_Scanned I...
AntiRansomwareShield_Infected INT
BrowserProtection_Scanned INT
BrowserProtection_Infected INT
SecureDnsShield_Scanned INT
SecureDnsShield_Infected INT

MonthlyResStat
Id INT
Time INT
FileSystemShield_Scanned INT
FileSystemShield_Infected INT
IMShield_Scanned INT
IMShield_Infected INT
P2PShield_Scanned INT
P2PShield_Infected INT
EmailShield_Scanned INT
EmailShield_Infected INT
WebShield_Scanned INT
WebShield_Infected INT
NetworkShield_Scanned INT
NetworkShield_Infected INT
ScriptShield_Scanned INT
ScriptShield_Infected INT
AntiSpamShield_Scanned INT
AntiSpamShield_Infected INT
BehaviorShield_Scanned INT
BehaviorShield_Infected INT
ExchangeShield_Scanned INT
ExchangeShield_Infected INT
SharepointShield_Scanned INT
SharepointShield_Infected INT
AntiRansomwareShield_Scanned I...
AntiRansomwareShield_Infected INT
BrowserProtection_Scanned INT
BrowserProtection_Infected INT
SecureDnsShield_Scanned INT
SecureDnsShield_Infected INT

WeeklyResStat
Id INT
Time INT
FileSystemShield_Scanned INT
FileSystemShield_Infected INT
IMShield_Scanned INT
IMShield_Infected INT
P2PShield_Scanned INT
P2PShield_Infected INT
EmailShield_Scanned INT
EmailShield_Infected INT
WebShield_Scanned INT
WebShield_Infected INT
NetworkShield_Scanned INT
NetworkShield_Infected INT
ScriptShield_Scanned INT
ScriptShield_Infected INT
AntiSpamShield_Scanned INT
AntiSpamShield_Infected INT
BehaviorShield_Scanned INT
BehaviorShield_Infected INT
ExchangeShield_Scanned INT
ExchangeShield_Infected INT
SharepointShield_Scanned INT
SharepointShield_Infected INT
AntiRansomwareShield_Scanned I...
AntiRansomwareShield_Infected INT
BrowserProtection_Scanned INT
BrowserProtection_Infected INT
SecureDnsShield_Scanned INT
SecureDnsShield_Infected INT

DecennaryResStat
Id INT
Time INT
FileSystemShield_Scanned INT
FileSystemShield_Infected INT
IMShield_Scanned INT
IMShield_Infected INT
P2PShield_Scanned INT
P2PShield_Infected INT
EmailShield_Scanned INT
EmailShield_Infected INT
WebShield_Scanned INT
WebShield_Infected INT
NetworkShield_Scanned INT
NetworkShield_Infected INT
ScriptShield_Scanned INT
ScriptShield_Infected INT
AntiSpamShield_Scanned INT
AntiSpamShield_Infected INT
BehaviorShield_Scanned INT
BehaviorShield_Infected INT
ExchangeShield_Scanned INT
ExchangeShield_Infected INT
SharepointShield_Scanned INT
SharepointShield_Infected INT
AntiRansomwareShield_Scanned I...
AntiRansomwareShield_Infected INT
BrowserProtection_Scanned INT
BrowserProtection_Infected INT
SecureDnsShield_Scanned INT
SecureDnsShield_Infected INT

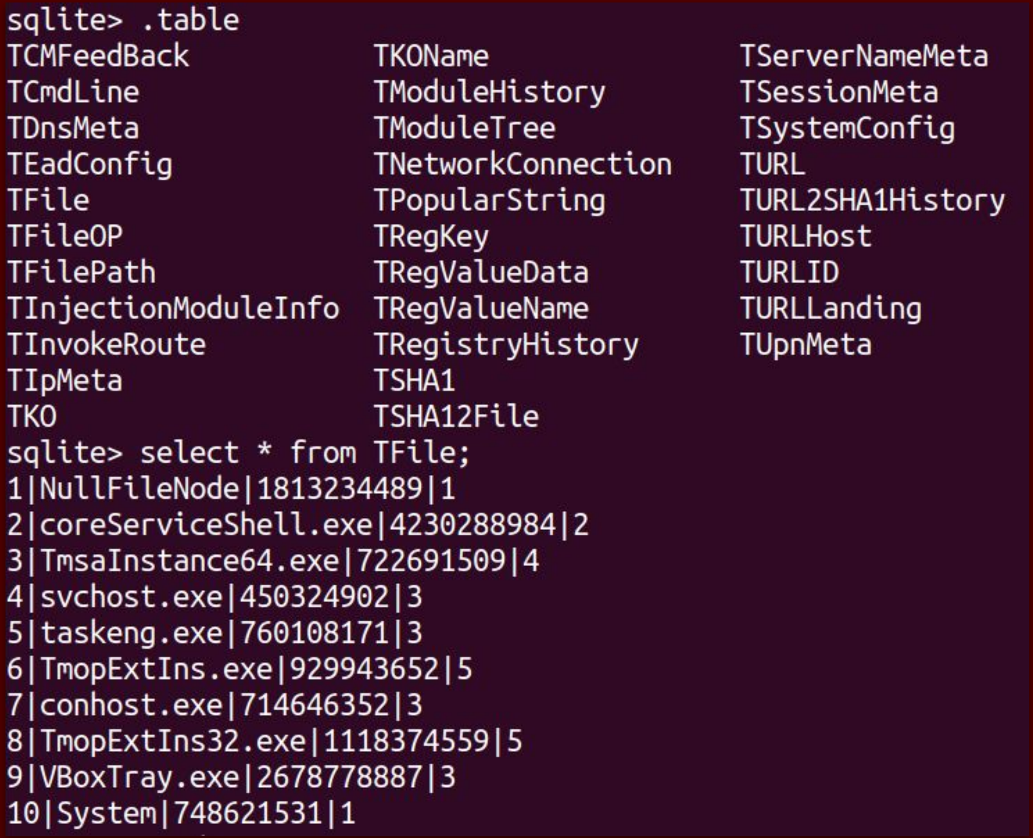
Event
Id INT
Time INT
Level INT
Module INT
MessageId INT
Param1 INT
Param2 INT
Param3 TEXT
Param4 TEXT

WeeklyFwStat
Id INT
Time INT
BytesIn INT
BytesOut INT
ItemType INT
ItemSubtype INT

ScanSession
Id INT
Type INT
TaskGuid TEXT
TestedFiles INT
TestedFolders INT
TestedData INT
InfectedFiles INT
Started INT
RunTime INT
Status INT
Error INT
Percent INT
LastScanned TEXT
Flags INT

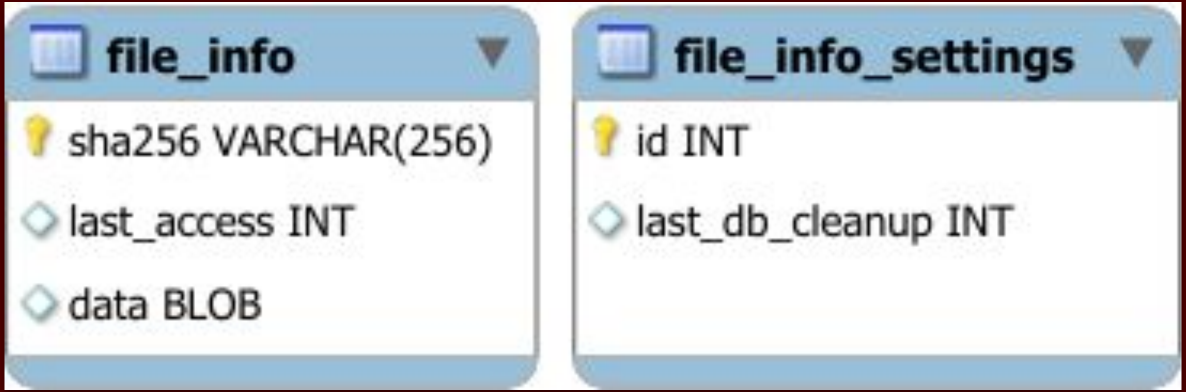
DecennaryFwStat
Id INT
Time INT
BytesIn INT
BytesOut INT
ItemType INT
ItemSubtype INT

AV Telemetry



```
sqlite> .table
TCMFeedBack           TKOName               TServerNameMeta
TCmdLine              TModuleHistory        TSessionMeta
TDnsMeta              TModuleTree           TSystemConfig
TEadConfig            TNetworkConnection    TURL
TFile                 TPopularString        TURL2SHA1History
TFileOP               TRegKey               TURLHost
TFilePath             TRegValueData         TURLID
TInjectionModuleInfo  TRegValueName         TURLLanding
TInvokeRoute          TRegistryHistory      TUpnMeta
TIpMeta               TSHA1
TKO                   TSHA12File
sqlite> select * from TFile;
1|NullFileNode|1813234489|1
2|coreServiceShell.exe|4230288984|2
3|TmsaInstance64.exe|722691509|4
4|svchost.exe|450324902|3
5|taskeng.exe|760108171|3
6|TmopExtIns.exe|929943652|5
7|conhost.exe|714646352|3
8|TmopExtIns32.exe|1118374559|5
9|VBoxTray.exe|2678778887|3
10|System|748621531|1
```

File Cache



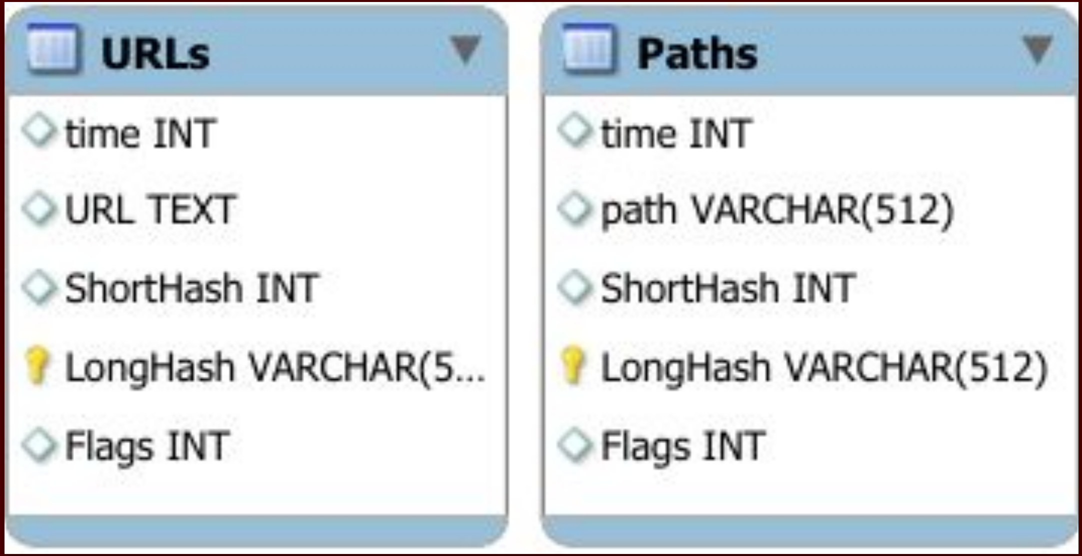
file_info

- sha256 VARCHAR(256)
- last_access INT
- data BLOB

file_info_settings

- id INT
- last_db_cleanup INT

URL cache



URLs

◇ time INT

◇ URL TEXT

◇ ShortHash INT

🔑 LongHash VARCHAR(5...

◇ Flags INT

Paths

◇ time INT

◇ path VARCHAR(512)

◇ ShortHash INT

🔑 LongHash VARCHAR(512)

◇ Flags INT

0xB. Caches can also be exploited

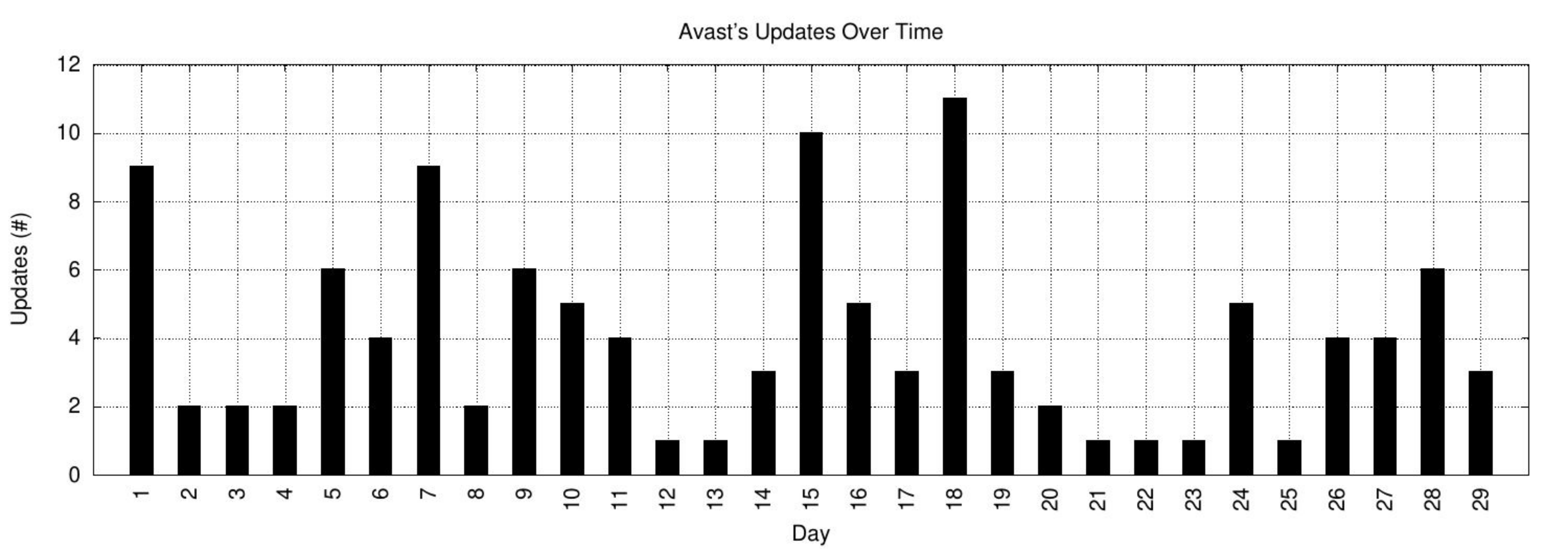
Attacks due to caching

Ameaça neutralizada

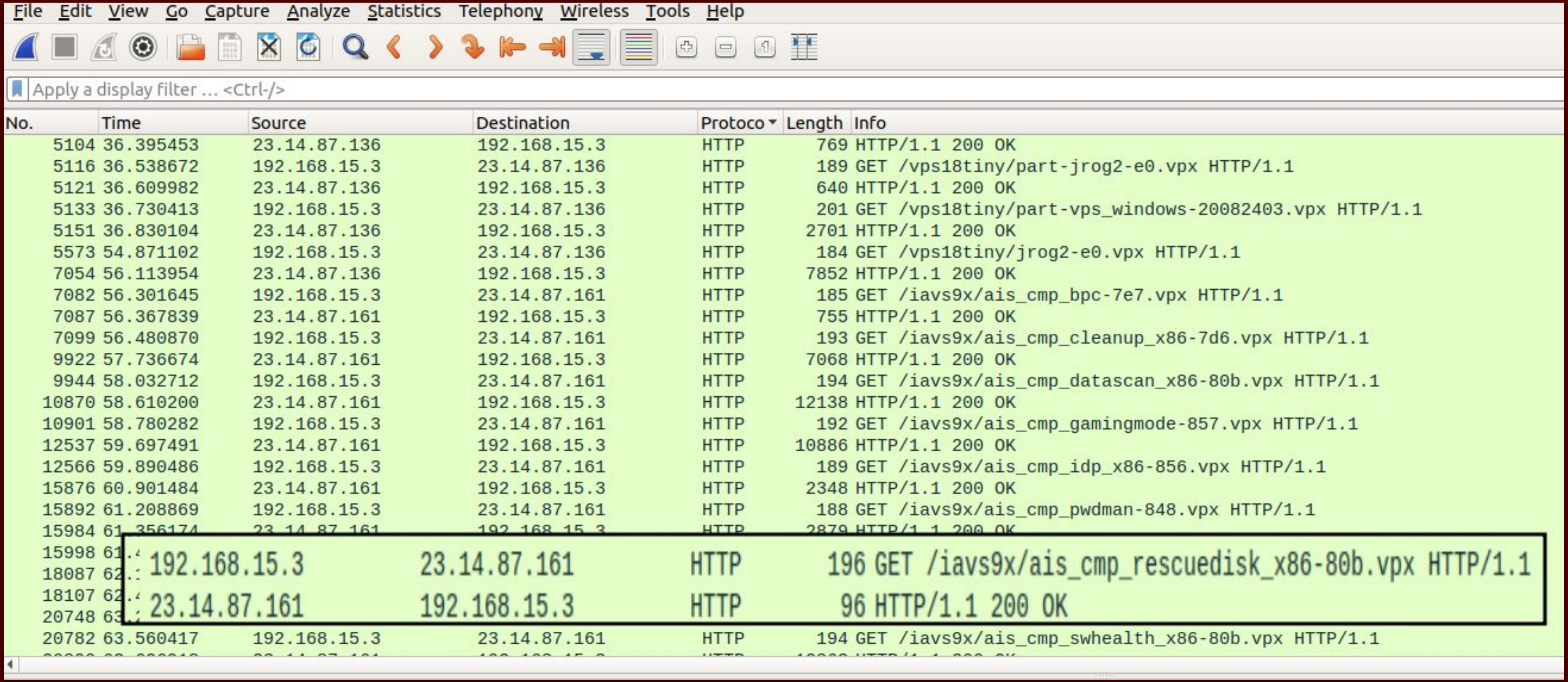
[illegible] reflective_dll.dll [illegible]

0xC. AVs updates definitions **AND** components

AV update in a month



Downloads in plain HTTP

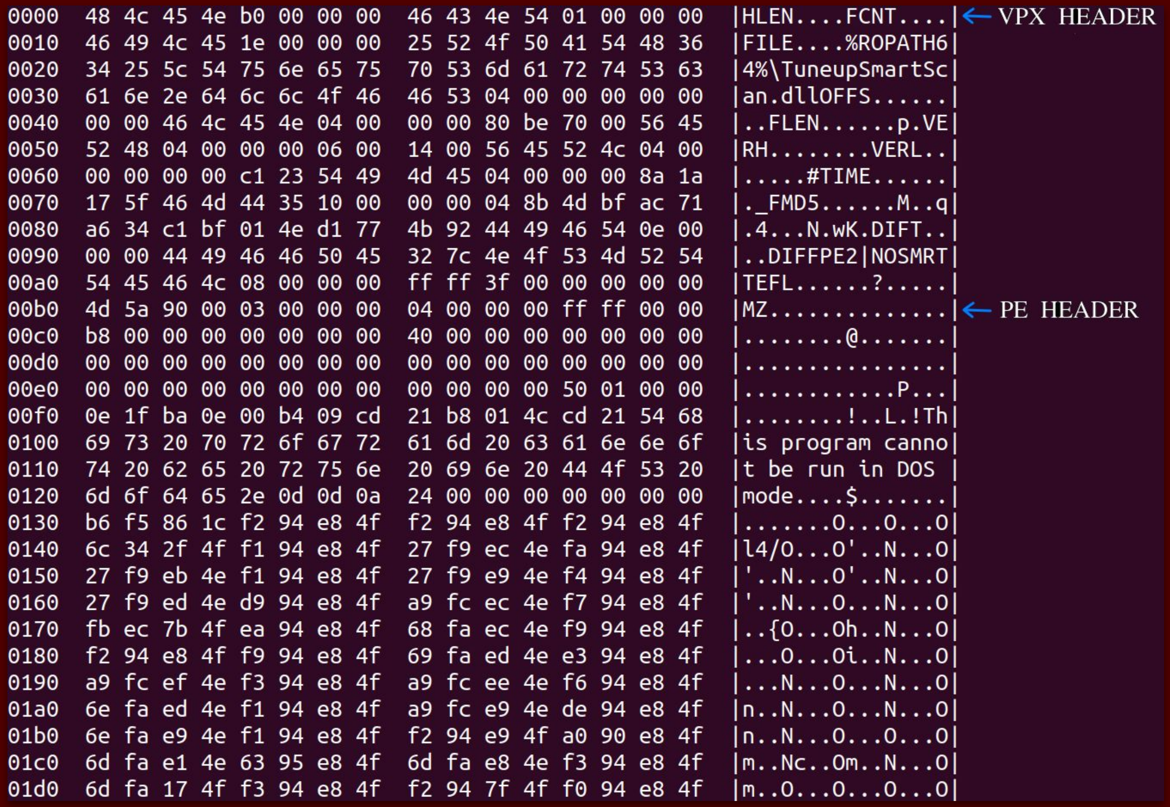


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.    Time       Source          Destination     Protoco Length Info
  5104 36.395453  23.14.87.136    192.168.15.3    HTTP      769 HTTP/1.1 200 OK
  5116 36.538672  192.168.15.3    23.14.87.136    HTTP      189 GET /vps18tiny/part-jrog2-e0.vpx HTTP/1.1
  5121 36.609982  23.14.87.136    192.168.15.3    HTTP      640 HTTP/1.1 200 OK
  5133 36.730413  192.168.15.3    23.14.87.136    HTTP      201 GET /vps18tiny/part-vps_windows-20082403.vpx HTTP/1.1
  5151 36.830104  23.14.87.136    192.168.15.3    HTTP     2701 HTTP/1.1 200 OK
  5573 54.871102  192.168.15.3    23.14.87.136    HTTP      184 GET /vps18tiny/jrog2-e0.vpx HTTP/1.1
  7054 56.113954  23.14.87.136    192.168.15.3    HTTP     7852 HTTP/1.1 200 OK
  7082 56.301645  192.168.15.3    23.14.87.161    HTTP      185 GET /iavs9x/ais_cmp_bpc-7e7.vpx HTTP/1.1
  7087 56.367839  23.14.87.161    192.168.15.3    HTTP      755 HTTP/1.1 200 OK
  7099 56.480870  192.168.15.3    23.14.87.161    HTTP      193 GET /iavs9x/ais_cmp_cleanup_x86-7d6.vpx HTTP/1.1
  9922 57.736674  23.14.87.161    192.168.15.3    HTTP     7068 HTTP/1.1 200 OK
  9944 58.032712  192.168.15.3    23.14.87.161    HTTP      194 GET /iavs9x/ais_cmp_datascan_x86-80b.vpx HTTP/1.1
 10870 58.610200  23.14.87.161    192.168.15.3    HTTP    12138 HTTP/1.1 200 OK
 10901 58.780282  192.168.15.3    23.14.87.161    HTTP      192 GET /iavs9x/ais_cmp_gamingmode-857.vpx HTTP/1.1
 12537 59.697491  23.14.87.161    192.168.15.3    HTTP    10886 HTTP/1.1 200 OK
 12566 59.890486  192.168.15.3    23.14.87.161    HTTP      189 GET /iavs9x/ais_cmp_idp_x86-856.vpx HTTP/1.1
 15876 60.901484  23.14.87.161    192.168.15.3    HTTP     2348 HTTP/1.1 200 OK
 15892 61.208869  192.168.15.3    23.14.87.161    HTTP      188 GET /iavs9x/ais_cmp_pwdman-848.vpx HTTP/1.1
 15984 61.356174  23.14.87.161    192.168.15.3    HTTP     2879 HTTP/1.1 200 OK
 15998 61.
 18087 62.
 18107 62.
 20748 63.
 20782 63.560417  192.168.15.3    23.14.87.161    HTTP      194 GET /iavs9x/ais_cmp_swhealth_x86-80b.vpx HTTP/1.1
```

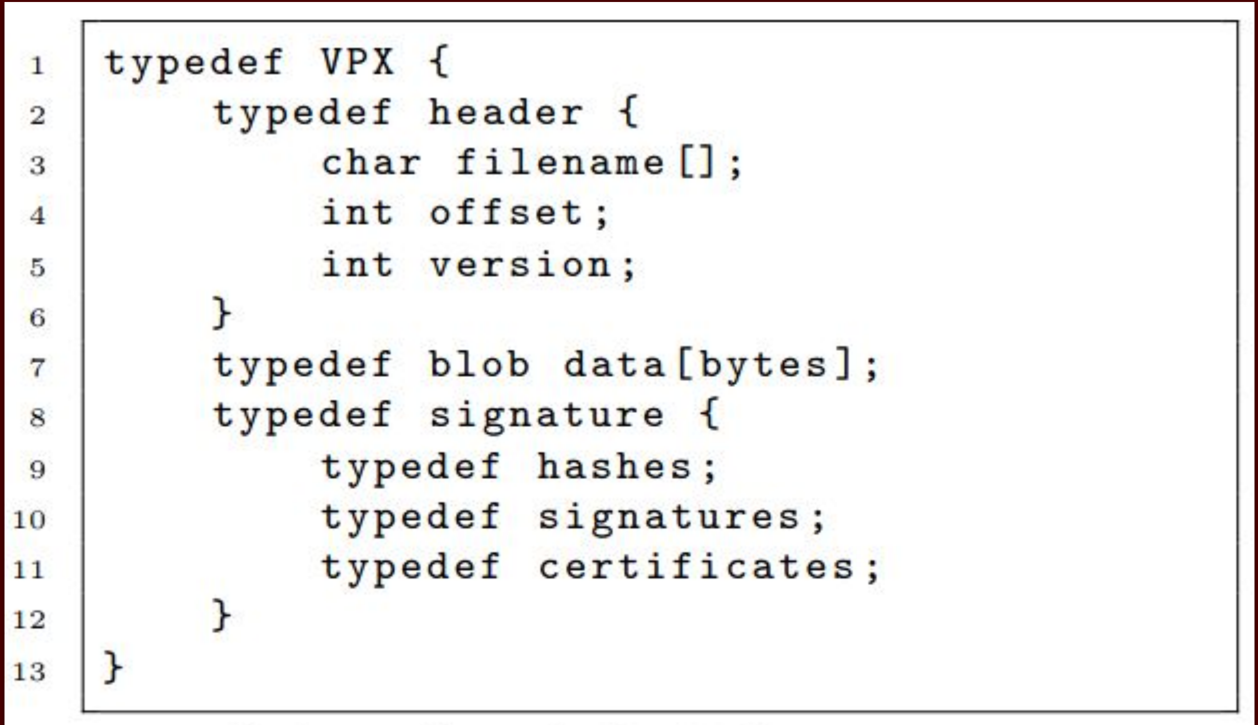
```
192.168.15.3    23.14.87.161    HTTP    196 GET /iavs9x/ais_cmp_rescuedisk_x86-80b.vpx HTTP/1.1
23.14.87.161    192.168.15.3    HTTP     96 HTTP/1.1 200 OK
```

VPX structure



```
0000  48 4c 45 4e b0 00 00 00  46 43 4e 54 01 00 00 00  |HLEN....FCNT....| ← VPX HEADER
0010  46 49 4c 45 1e 00 00 00  25 52 4f 50 41 54 48 36  |FILE....%ROPATH6|
0020  34 25 5c 54 75 6e 65 75  70 53 6d 61 72 74 53 63  |4%\TuneupSmartSc|
0030  61 6e 2e 64 6c 6c 4f 46  46 53 04 00 00 00 00 00  |an.dllOFFS......|
0040  00 00 46 4c 45 4e 04 00  00 00 80 be 70 00 56 45  |..FLEN......p.VE|
0050  52 48 04 00 00 00 06 00  14 00 56 45 52 4c 04 00  |RH........VERL..|
0060  00 00 00 00 c1 23 54 49  4d 45 04 00 00 00 8a 1a  |.....#TIME......|
0070  17 5f 46 4d 44 35 10 00  00 00 04 8b 4d bf ac 71  |._FMD5......M..q|
0080  a6 34 c1 bf 01 4e d1 77  4b 92 44 49 46 54 0e 00  |.4...N.wK.DIFT..|
0090  00 00 44 49 46 46 50 45  32 7c 4e 4f 53 4d 52 54  |..DIFFPE2|NOSMRT|
00a0  54 45 46 4c 08 00 00 00  ff ff 3f 00 00 00 00 00  |TEFL......?.....|
00b0  4d 5a 90 00 03 00 00 00  04 00 00 00 ff ff 00 00  |MZ..............| ← PE HEADER
00c0  b8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  |........@.......|
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00e0  00 00 00 00 00 00 00 00  00 00 00 00 50 01 00 00  |............P...|
00f0  0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68  |........!..L.!Th|
0100  69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f  |is program canno|
0110  74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20  |t be run in DOS |
0120  6d 6f 64 65 2e 0d 0d 0a  24 00 00 00 00 00 00 00  |mode....$.......|
0130  b6 f5 86 1c f2 94 e8 4f  f2 94 e8 4f f2 94 e8 4f  |.......O...O...O|
0140  6c 34 2f 4f f1 94 e8 4f  27 f9 ec 4e fa 94 e8 4f  |l4/O...O'..N...O|
0150  27 f9 eb 4e f1 94 e8 4f  27 f9 e9 4e f4 94 e8 4f  |'..N...O'..N...O|
0160  27 f9 ed 4e d9 94 e8 4f  a9 fc ec 4e f7 94 e8 4f  |'..N...O...N...O|
0170  fb ec 7b 4f ea 94 e8 4f  68 fa ec 4e f9 94 e8 4f  |..{O...Oh..N...O|
0180  f2 94 e8 4f f9 94 e8 4f  69 fa ed 4e e3 94 e8 4f  |...O...Oi..N...O|
0190  a9 fc ef 4e f3 94 e8 4f  a9 fc ee 4e f6 94 e8 4f  |...N...O...N...O|
01a0  6e fa ed 4e f1 94 e8 4f  a9 fc e9 4e de 94 e8 4f  |n..N...O...N...O|
01b0  6e fa e9 4e f1 94 e8 4f  f2 94 e9 4f a0 90 e8 4f  |n..N...O...O...O|
01c0  6d fa e1 4e 63 95 e8 4f  6d fa e8 4e f3 94 e8 4f  |m..Nc..Om..N...O|
01d0  6d fa 17 4f f3 94 e8 4f  f2 94 7f 4f f0 94 e8 4f  |m..O...O...O...O|
```

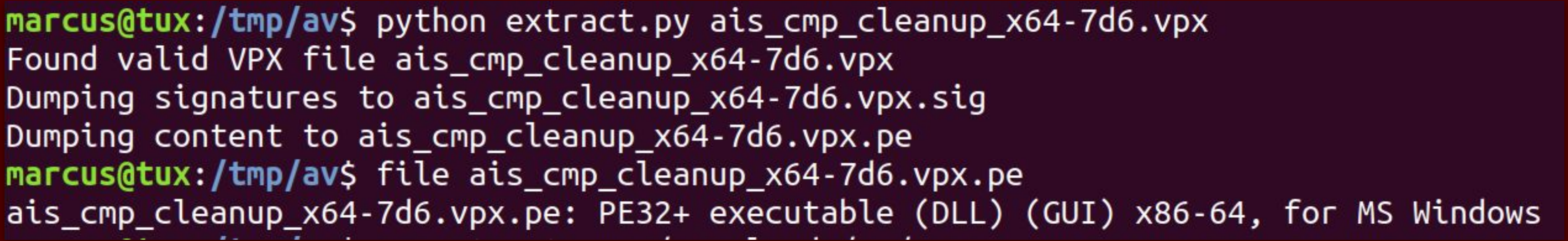
For Programmers



```
typedef VPX {
    typedef header {
        char filename[];
        int offset;
        int version;
    }
    typedef blob data[bytes];
    typedef signature {
        typedef hashes;
        typedef signatures;
        typedef certificates;
    }
}
```

Code 1: Avast's VPX file structure.

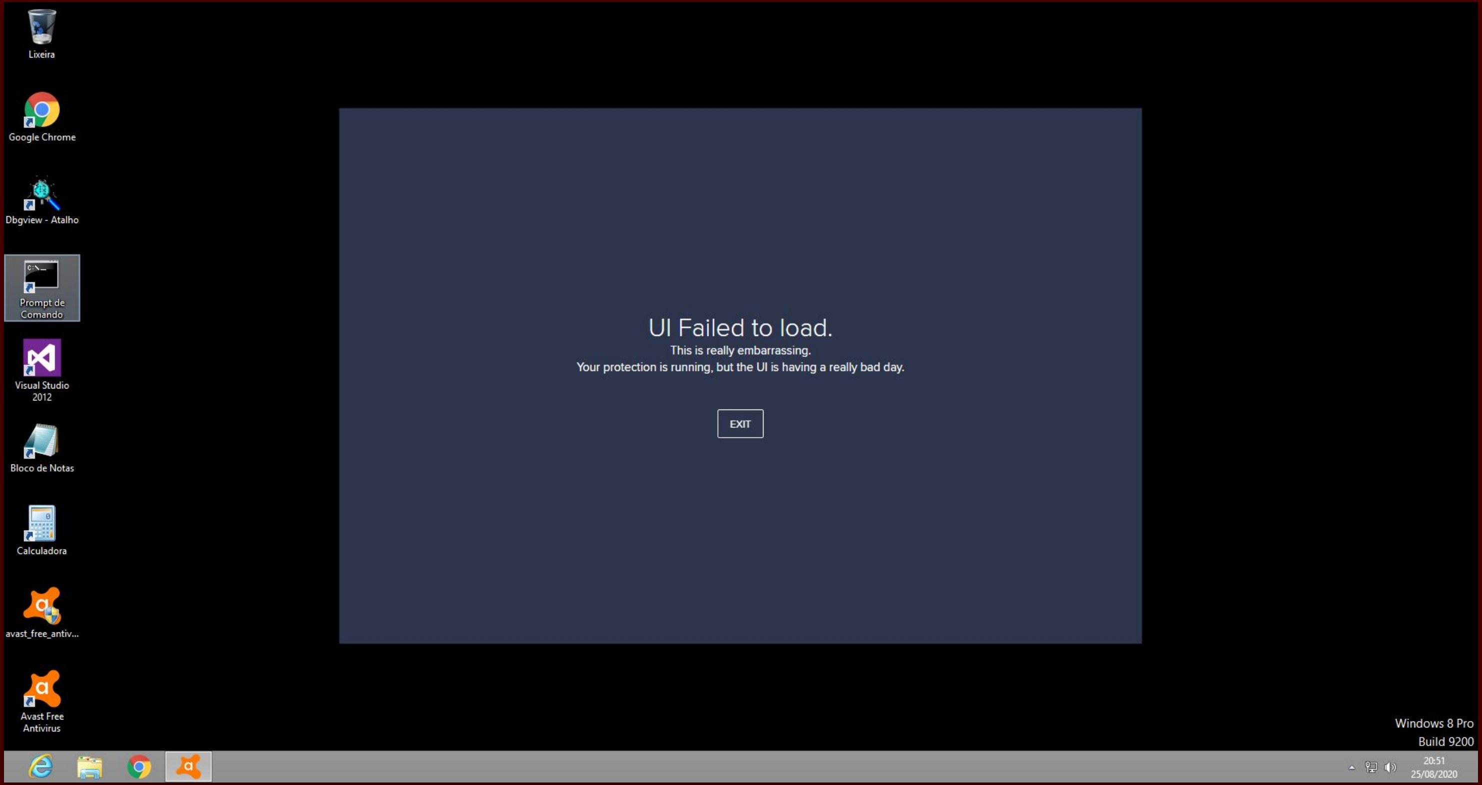
Extracting PE from VPX



```
marcus@tux:/tmp/av$ python extract.py ais_cmp_cleanup_x64-7d6.vpx
Found valid VPX file ais_cmp_cleanup_x64-7d6.vpx
Dumping signatures to ais_cmp_cleanup_x64-7d6.vpx.sig
Dumping content to ais_cmp_cleanup_x64-7d6.vpx.pe
marcus@tux:/tmp/av$ file ais_cmp_cleanup_x64-7d6.vpx.pe
ais_cmp_cleanup_x64-7d6.vpx.pe: PE32+ executable (DLL) (GUI) x86-64, for MS Windows
```

0xD. AVs security depends on their integrity

Patching in secure boot mode



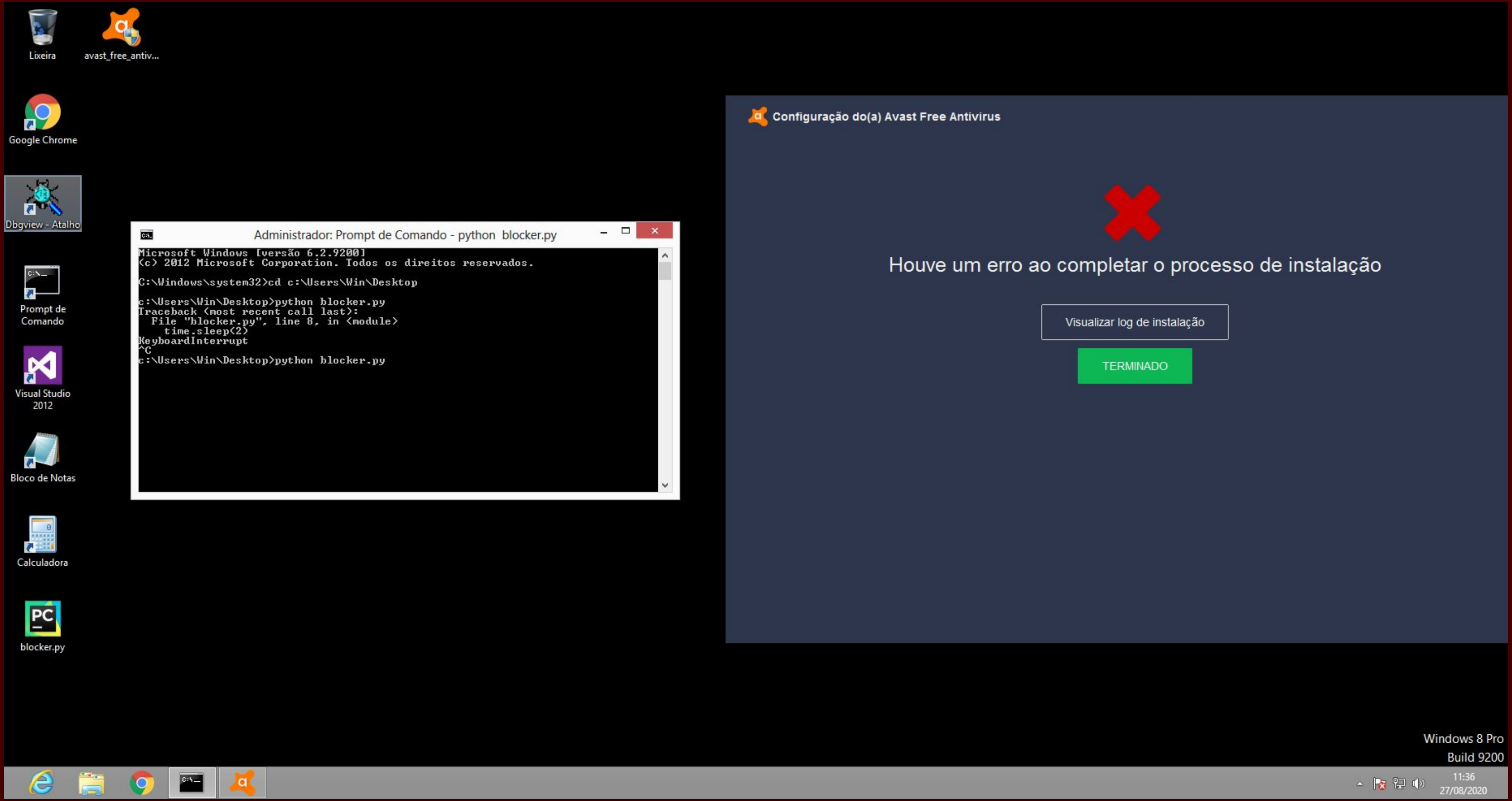
UI Failed to load.

This is really embarrassing.

Your protection is running, but the UI is having a really bad day.

0xE. AV’s security depends on pristine installations

Assume pristine installation

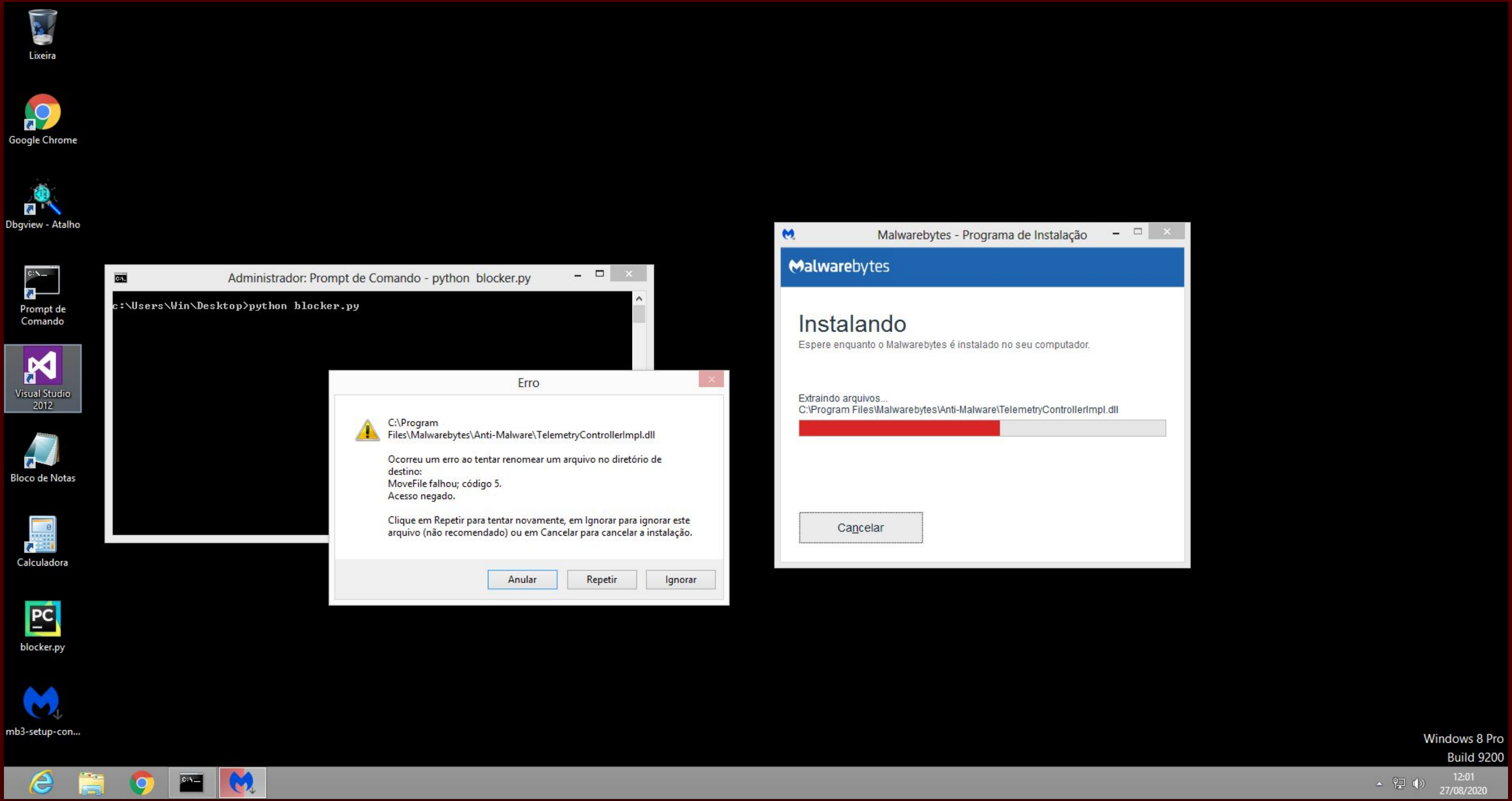


```
Microsoft Windows [versão 6.2.9200]
(c) 2012 Microsoft Corporation. Todos os direitos reservados.

C:\Windows\system32>cd c:\Users\Win\Desktop

c:\Users\Win\Desktop>python blocker.py
Traceback (most recent call last):
  File "blocker.py", line 8, in <module>
    time.sleep(2)
KeyboardInterrupt
^C
c:\Users\Win\Desktop>python blocker.py
```

Configuração do(a) Avast Free Antivirus

Houve um erro ao completar o processo de instalação

Pristine installation attempt



Administrador: Prompt de Comando - python blocker.py

```
c:\Users\Win\Desktop>python blocker.py
```

Erro

C:\Program Files\Malwarebytes\Anti-Malware\TelemetryControllerImpl.dll

Ocorreu um erro ao tentar renomear um arquivo no diretório de destino:
MoveFile falhou; código 5.
Acesso negado.

Clique em Repetir para tentar novamente, em Ignorar para ignorar este arquivo (não recomendado) ou em Cancelar para cancelar a instalação.

Malwarebytes - Programa de Instalação

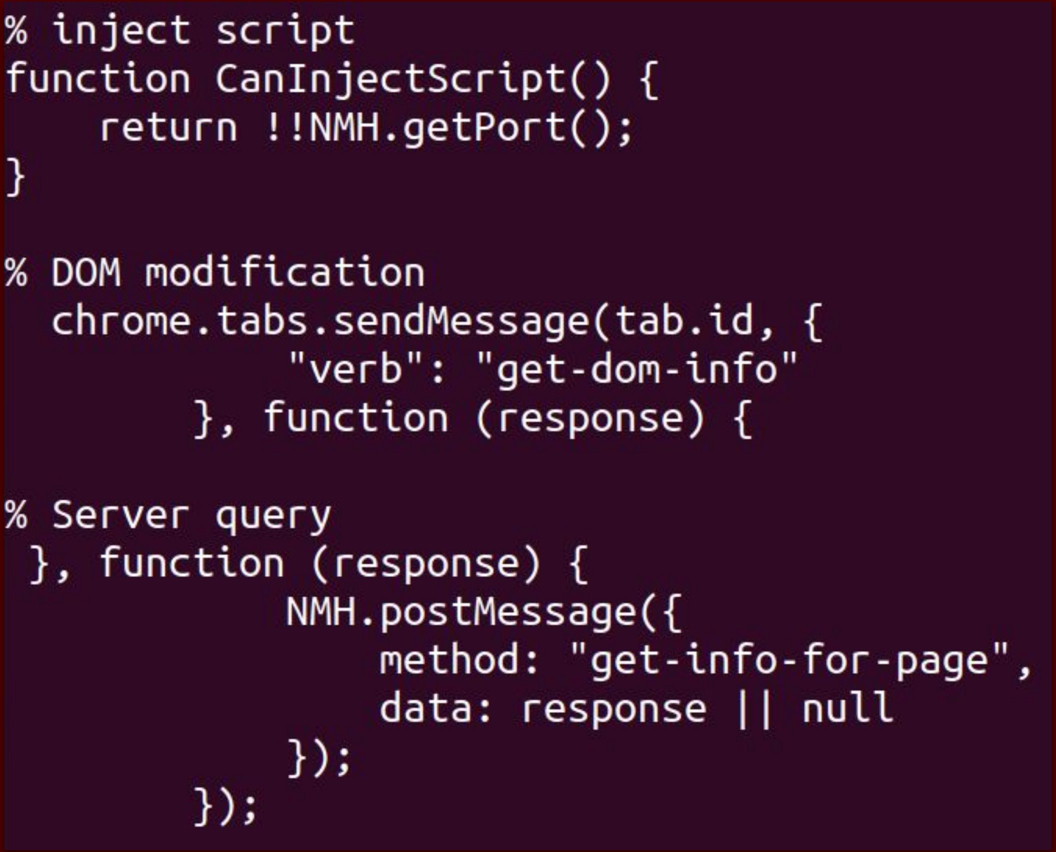
Instalando

Espere enquanto o Malwarebytes é instalado no seu computador.

Extraindo arquivos...
C:\Program Files\Malwarebytes\Anti-Malware\TelemetryControllerImpl.dll

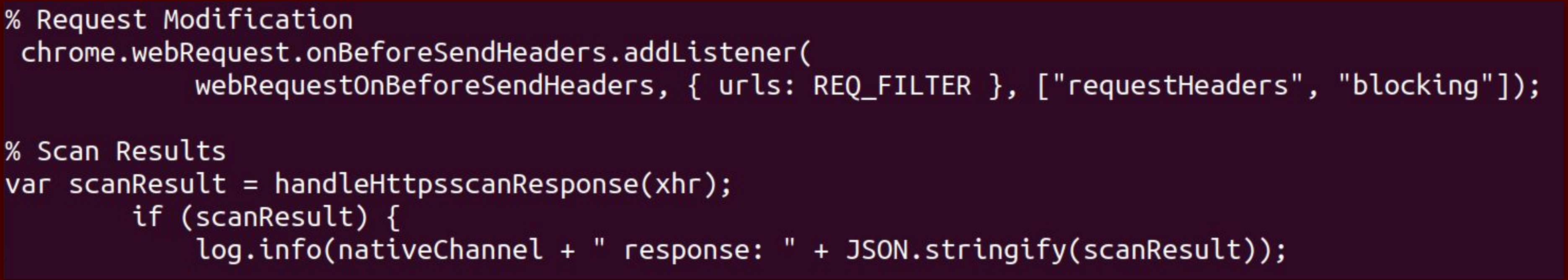
0xF. Browser extensions are AV clients

Javascript Injection



```
% inject script
function CanInjectScript() {
    return !!NMH.getPort();
}

% DOM modification
  chrome.tabs.sendMessage(tab.id, {
            "verb": "get-dom-info"
        }, function (response) {

% Server query
 }, function (response) {
            NMH.postMessage({
                method: "get-info-for-page",
                data: response || null
            });
        });
```

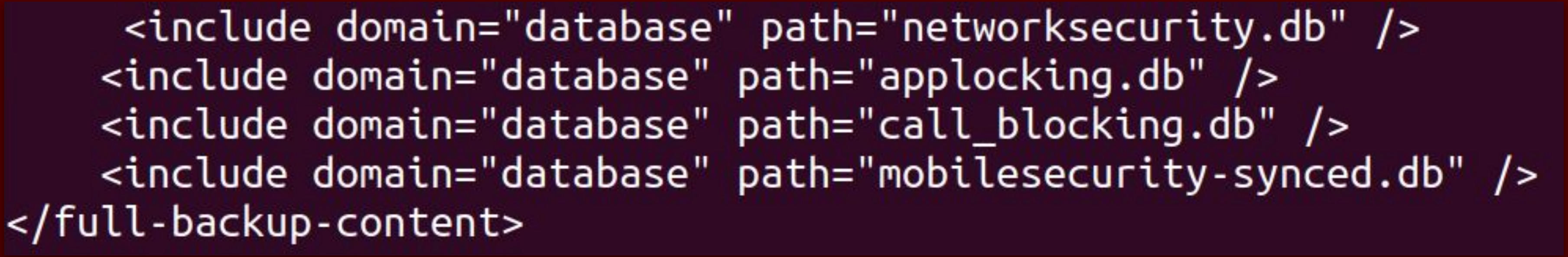
Content Modification



```
% Request Modification
 chrome.webRequest.onBeforeSendHeaders.addListener(
            webRequestOnBeforeSendHeaders, { urls: REQ_FILTER }, ["requestHeaders", "blocking"]);

% Scan Results
var scanResult = handleHttpsscanResponse(xhr);
        if (scanResult) {
            log.info(nativeChannel + " response: " + JSON.stringify(scanResult));
```

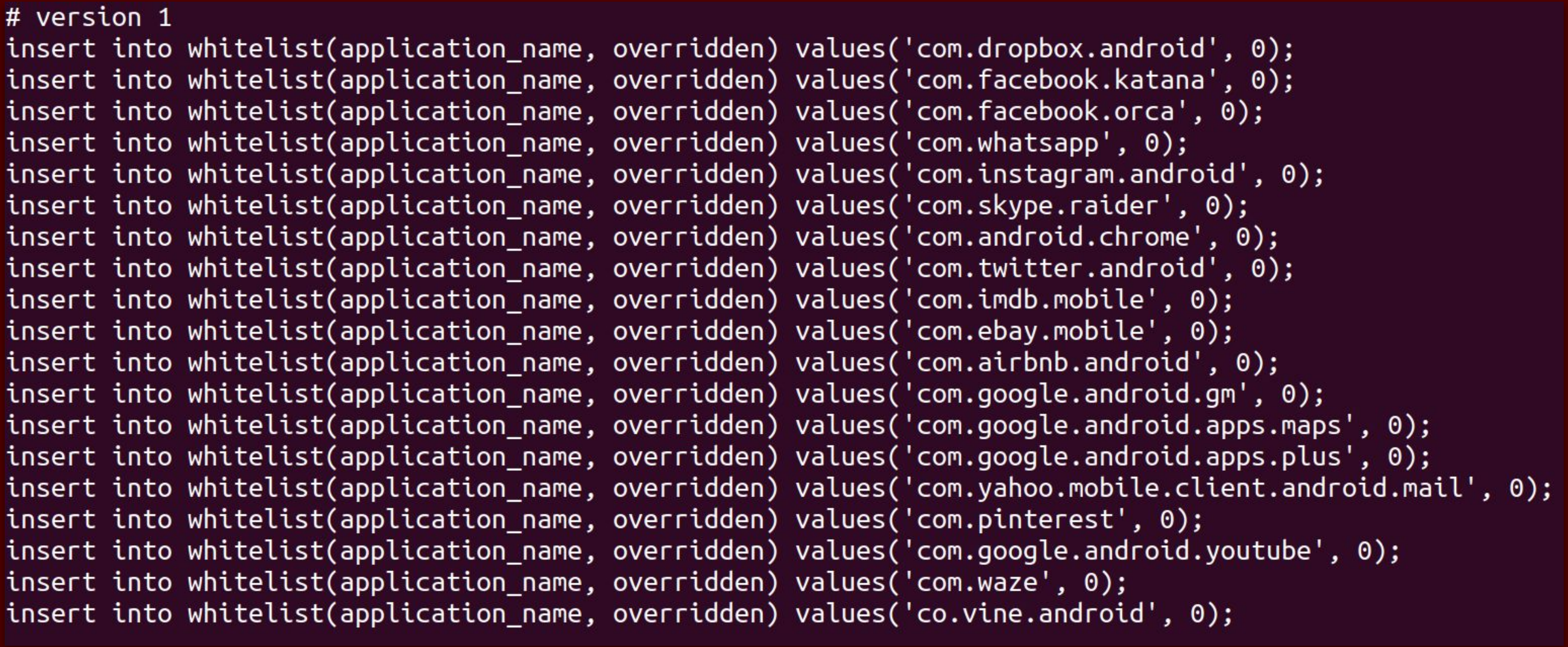
0x10. Android AVs are VERY weak

Android AVs: Static Filtering



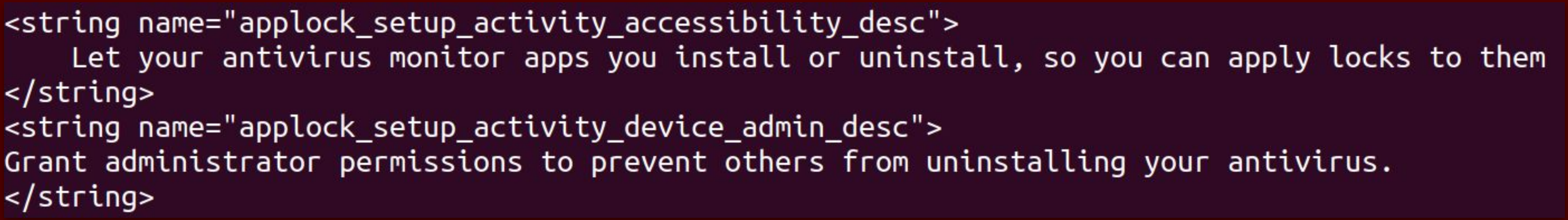
```
     <include domain="database" path="networksecurity.db" />
    <include domain="database" path="applocking.db" />
    <include domain="database" path="call_blocking.db" />
    <include domain="database" path="mobilesecurity-synced.db" />
</full-backup-content>
```

Android AVs: Whitelisting



```
# version 1
insert into whitelist(application_name, overridden) values('com.dropbox.android', 0);
insert into whitelist(application_name, overridden) values('com.facebook.katana', 0);
insert into whitelist(application_name, overridden) values('com.facebook.orca', 0);
insert into whitelist(application_name, overridden) values('com.whatsapp', 0);
insert into whitelist(application_name, overridden) values('com.instagram.android', 0);
insert into whitelist(application_name, overridden) values('com.skype.raider', 0);
insert into whitelist(application_name, overridden) values('com.android.chrome', 0);
insert into whitelist(application_name, overridden) values('com.twitter.android', 0);
insert into whitelist(application_name, overridden) values('com.imdb.mobile', 0);
insert into whitelist(application_name, overridden) values('com.ebay.mobile', 0);
insert into whitelist(application_name, overridden) values('com.airbnb.android', 0);
insert into whitelist(application_name, overridden) values('com.google.android.gm', 0);
insert into whitelist(application_name, overridden) values('com.google.android.apps.maps', 0);
insert into whitelist(application_name, overridden) values('com.google.android.apps.plus', 0);
insert into whitelist(application_name, overridden) values('com.yahoo.mobile.client.android.mail', 0);
insert into whitelist(application_name, overridden) values('com.pinterest', 0);
insert into whitelist(application_name, overridden) values('com.google.android.youtube', 0);
insert into whitelist(application_name, overridden) values('com.waze', 0);
insert into whitelist(application_name, overridden) values('co.vine.android', 0);
```

Android AVs: Exploiting accessibility services



```
<string name="applock_setup_activity_accessibility_desc">
    Let your antivirus monitor apps you install or uninstall, so you can apply locks to them
</string>
<string name="applock_setup_activity_device_admin_desc">
Grant administrator permissions to prevent others from uninstalling your antivirus.
</string>
```

Future Directions

What to do now?

- AV companies must be more transparent about their decisions.
- Researchers have many opportunities to be explored.
- AV evaluations should be multi-dimensional

What do we use this knowledge for?

Publications

Terminator: A Secure Coprocessor to Accelerate Real-Time AntiViruses Using Inspection Breakpoints

HEAVEN: A Hardware-Enhanced AntiVirus ENgine to accelerate real-time, signature-based malware detection

``VANILLA" malware: vanishing antiviruses by interleaving layers and layers of attacks

All You Always Wanted to Know About AntiViruses (and I had to hands-on to tell you!)

Thank you!

Contact: botacin@tamu.edu or @MarcusBotacin
My Website: marcusbotacin.github.io

Marcus Botacin
Texas A&M University, USA
@MarcusBotacin