SANGFOR

Guide to Identify Infected Files

Change Log

Date	Change Description
December 27, 2019	Version 1document release.

Contents

Understanding Malware Information 1

Judge with Threat Intelligence 2

Ransomware Engine Reports Maliciousness (Suspicious.Win32.Ransom.rsm) 5

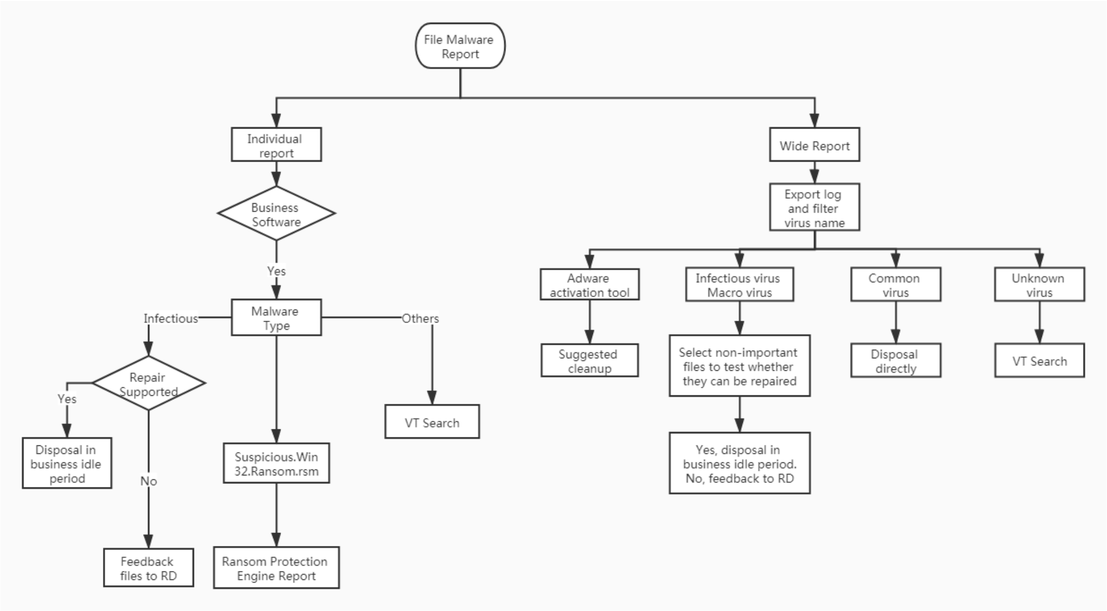
Infectious Virus 6
- Endpoint Secure Support Report Infectious Viruses (Common) 6
- Infectious virus Handling Step 6

Macro Virus 7
- Introduction 7
- Macro virus disposal ideas 7

Common Situation 8

Example 1: Eternal Blue related virus files 8

Example 2: File server reports a large number of viruses 8


File Malware Report
Individual report
Wide Report
Business Software
Yes
Export log and filter virus name
Adware activation tool
Infectious virus Macro virus
Common virus
Unknown virus
Infectious
Malware Type
Others
Suggested cleanup
Select non-important files to test whether they can be repaired
Disposal directly
VT Search
Repair Supported
Yes
VT Search
Disposal in business idle period
Suspicious.Win 32.Ransom.rsm
No
Yes, disposal in business idle period. No, feedback to RD
Feedback files to RD
Ransom Protection Engine Report

Note: Do not upload customer's files or folder to external web especially document file.

Understanding Malware Information

Malware Type	Description	Threat Degree
Trojan	Trojan	High
Backdoor	Backdoor	High
Virus	Virus (Generally infectious virus)	High
Worm	Worm (Including a part of infectious virus)	High
Ransom	Ransom	High
W97M/VBA/MSWord/X2000M	Macro Virus (All are Document Files)	High
Exploit	Exploit	High
ACAD/CAD	CAD Virus	High
HackTool	HackTool	Medium
Suspicious.Win32.Ransom.rsm	Ransomware engine reports poison	Subject to the file

Suspicious	Suspicious Files	Low
Adware	Adware	Low
Application/PUP/PUA	Application/PUP/PUA	Low

Judge with Threat Intelligence

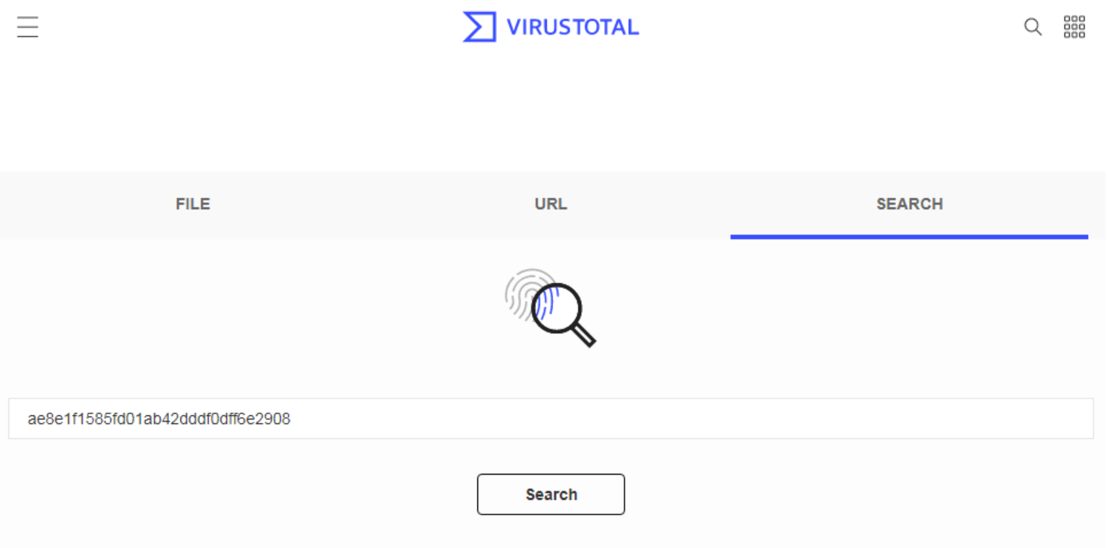
Search file threats: https://www.virustotal.com

Search traffic threats: https://x.threatbook.cn/

Online sandbox: https://habo.qq.com/ https://any.run/

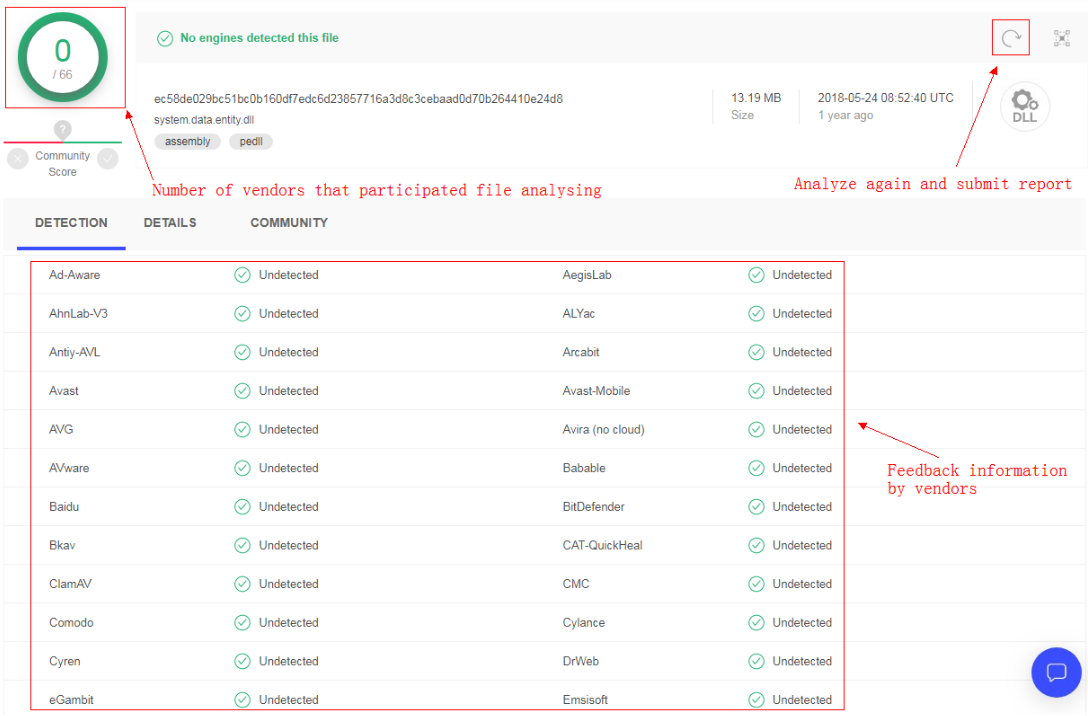
When customers' business service software and normal applications are reported as malware or virus. Visit https://www.virustotal.com to do checking.

1. Use the MD5 value to do checking in VT (https://www.virustotal.com), as figure shown below:



ae8e1f1585fd01ab42dddf0dff6e2908

2. You can get corresponding report after VT done checking.



✓ No engines detected this file

ec58de029bc51bc0b160df7edc6d23857716a3d8c3cebaad0d70b264410e24d8
system.data.entity.dll
assembly pedll

13.19 MB
Size

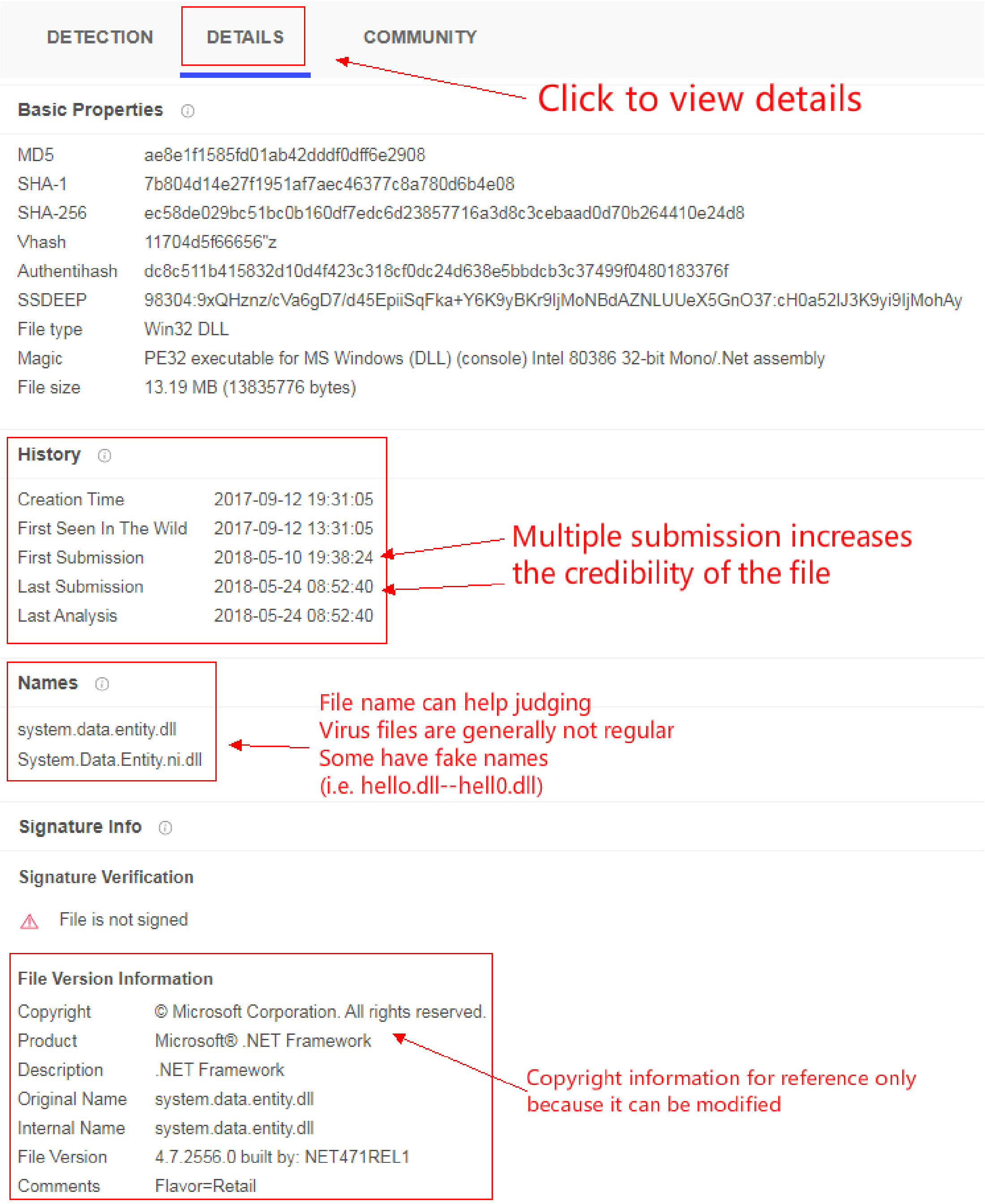
2018-05-24 08:52:40 UTC
1 year ago

Number of vendors that participated file analysing

Analyze again and submit report

Ad-Aware	✓ Undetected	AegisLab	✓ Undetected
AhnLab-V3	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	Avast-Mobile	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected
AVware	✓ Undetected	Babable	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
Bkav	✓ Undetected	CAT-QuickHeal	✓ Undetected
ClamAV	✓ Undetected	CMC	✓ Undetected
Comodo	✓ Undetected	Cylance	✓ Undetected
Cyren	✓ Undetected	DrWeb	✓ Undetected
eGambit	✓ Undetected	Emsisoft	✓ Undetected

Feedback information by vendors



Click to view details

Basic Properties

MD5	ae8e1f1585fd01ab42dddf0dff6e2908
SHA-1	7b804d14e27f1951af7aec46377c8a780d6b4e08
SHA-256	ec58de029bc51bc0b160df7edc6d23857716a3d8c3cebaad0d70b264410e24d8
Vhash	11704d5f66656"z
Authentihash	dc8c511b415832d10d4f423c318cf0dc24d638e5bbdcb3c37499f0480183376f
SSDEEP	98304:9xQHznz/cVa6gD7/d45EpiiSqFka+Y6K9yBKr9IjMoNBdAZNLUUeX5GnO37:cH0a52IJ3K9yi9IjMohAy
File type	Win32 DLL
Magic	PE32 executable for MS Windows (DLL) (console) Intel 80386 32-bit Mono/.Net assembly
File size	13.19 MB (13835776 bytes)

History

Creation Time	2017-09-12 19:31:05
First Seen In The Wild	2017-09-12 13:31:05
First Submission	2018-05-10 19:38:24
Last Submission	2018-05-24 08:52:40
Last Analysis	2018-05-24 08:52:40

Multiple submission increases the credibility of the file

Names

system.data.entity.dll
System.Data.Entity.ni.dll

File name can help judging
Virus files are generally not regular
Some have fake names
(i.e. hello.dll--hell0.dll)

Signature Info

Signature Verification

⚠ File is not signed

File Version Information

Copyright	© Microsoft Corporation. All rights reserved.
Product	Microsoft® .NET Framework
Description	.NET Framework
Original Name	system.data.entity.dll
Internal Name	system.data.entity.dll
File Version	4.7.2556.0 built by: NET471REL1
Comments	Flavor=Retail

Copyright information for reference only
because it can be modified

Whitelist file criteria can be obtained from the above information. (Below rules can as a reference to whitelist a file. It require to meet multiple rules in order to whitelist a file. In uncertain situation do not whitelist the file.)

1. Digitally signed, VT did not report malicious, can be directly judged as safe.

2. There is a digital signature, but the VT has a malicious report from the manufacturer. In this case, it should be judged whether it is a false positive report. Generally less than 5 reports, you need to

check the types of malicious reports and malicious families. Besides that, if those digital signed are from well-known companies, file can be judged as safe.

3. If there is an invalid digital signature and the signature from well known companies. The file can judge as safe.

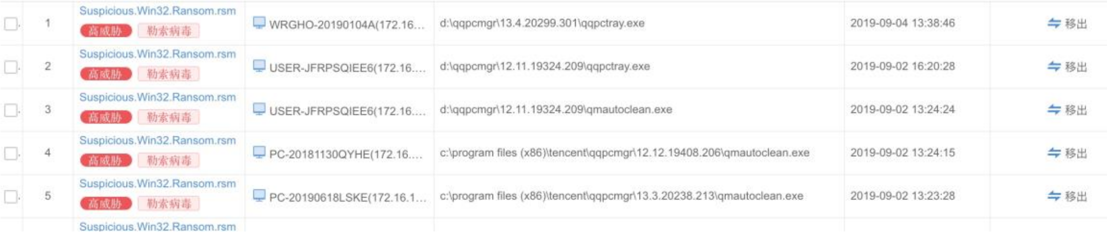
4. If there is an invalid digital signature, the first and last submission time are longer than 2 weeks. The file can judge as safe.

5. If there is no digital signature, VT does not reported the file as virus, and the last analysis date is more than 30 days from the current time. In this case can recognize as multiple submissions. (The meaning of multiple submissions: the time of the first submission and the last submission are not the same). If it is not multiple submissions, it is recommended to analyze and update the analysis report again to make a judgment. (Without a digital signature, no VT report virus. The file cannot be judge as safe.)

Ransomware Engine Reports Maliciousness (Suspicious.Win32.Ransom.rsm)

The reason is usually that the process wrote or deleted the ransomware bait file;

If you find reports of programs that have junk file cleaning functions such as 360 and Tencent Computer Manager (installation path is 360, tencent, qqpcmgr, etc.), you need to feedback the corresponding files to the RnD, and then ignore:



□	1	Suspicious.Win32.Ransom.rsm 高威胁 勒索病毒	WRGHO-20190104A(172.16...	d:\qqpcmgr\13.4.20299.301\qqpctray.exe	2019-09-04 13:38:46	⇋ 移出
□	2	Suspicious.Win32.Ransom.rsm 高威胁 勒索病毒	USER-JFRPSQIEE6(172.16....	d:\qqpcmgr\12.11.19324.209\qqpctray.exe	2019-09-02 16:20:28	⇋ 移出
□	3	Suspicious.Win32.Ransom.rsm 高威胁 勒索病毒	USER-JFRPSQIEE6(172.16....	d:\qqpcmgr\12.11.19324.209\qmautoclean.exe	2019-09-02 13:24:24	⇋ 移出
□	4	Suspicious.Win32.Ransom.rsm 高威胁 勒索病毒	PC-20181130QYHE(172.16....	c:\program files (x86)\tencent\qqpcmgr\12.12.19408.206\qmautoclean.exe	2019-09-02 13:24:15	⇋ 移出
□	5	Suspicious.Win32.Ransom.rsm 高威胁 勒索病毒	PC-20190618LSKE(172.16.1...	c:\program files (x86)\tencent\qqpcmgr\13.3.20238.213\qmautoclean.exe	2019-09-02 13:23:28	⇋ 移出
		Suspicious.Win32.Ransom.rsm				

At the same time, you need to take two files in the Endpoint Secure installation directory:

\Sangfor\EDR\agent\bin\frep\local_certificate\readme.txt

C:\ProgramData\Sangfor\EDR\log\ sfavsvc.log

Infectious Virus

Endpoint Secure Support Report Infectious Viruses (Common)

Almanahe
Chir
Expiro
Floxif
Jadtre
Neshta
Parite
Ramnit
Sality
Virut

Infectious virus Handling Step

1. Do a full scan in PC, check virus supported repair by Endpoint Secure (Eg Virus / Ramnit.a, Virus.Win32.Save.a are usually infectious viruses);

2. If it is in the repair list, perform one-click processing (The process corresponding to the file may be stopped during the repair, and this process should carry out during non business hour);

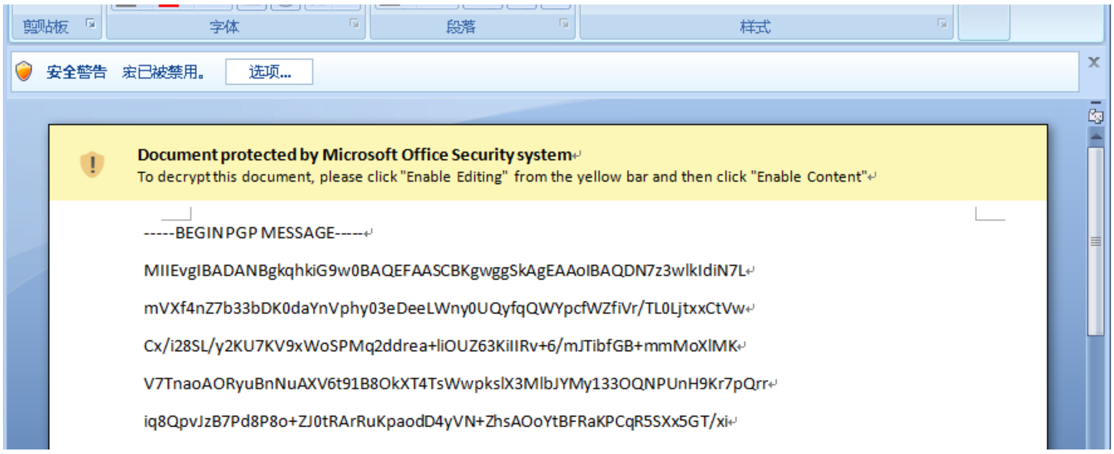
3. If it is not in the repair list, or the infection type reported by the SAVE engine does not have a family (such as Virus.Win32.Save.a), first select one of the two unimportant files for fix. Then see whether it is repaired or isolated. If it can be repaired then can proceed to one click process; if it is isolated, then select a part of the exe files, compress them with password, and feed back to the RnD together with the scan log;

4. If you want to scan the entire network, it is recommended to separate the business server from the ordinary office PC. You can first check the important servers individually and check whether the infection can be repaired.

Macro Virus

Introduction

A macro virus is a computer virus that resides in a macro of a document or template. Once the macro function is enabled for such a document, the macro code in it will be executed. Common macro viruses are currently divided into template macro viruses or download macro viruses. If a template macro virus is infected, all automatically saved documents on the host will be “infected” with this macro virus; download macro viruses are mainly used to download and execute other malicious files.



安全警告 宏已被禁用。

Document protected by Microsoft Office Security system

To decrypt this document, please click "Enable Editing" from the yellow bar and then click "Enable Content"

```
-----BEGIN PGP MESSAGE-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDN7z3wlkIdiN7L
mVXf4nZ7b33bDK0daYnVphy03eDeeLWny0UQyfqQWYpcfWZfiVr/TL0LjtxxCtVw
Cx/i28SL/y2KU7KV9xWoSPMq2ddrea+liOUZ63KiIIRv+6/mJTibfGB+mmMoXlMK
V7TnaoAORyuBnNuAXV6t91B8OkXT4TsWwpkslX3MlbJYMy133OQNPUnH9Kr7pQrr
iq8QpvJzB7Pd8P8o+ZJ0tRArRuKpaodD4yVN+ZhsAOoYtBFRaKPCqR5SXx5GT/xi
```

Macro virus disposal ideas

There are some macro viruses that can be repaired, especially template macro viruses. When Endpoint Secure detects and kills a large number of macro viruses:

1. One-click fix after backup. If the files can be repaired, they will be repaired, and those that cannot be repaired will be isolated;

2. Choose non business hour to do the repair process, if it is found that it cannot be repaired, you can recover from the quarantine area;

3. For the macro virus that cannot be repaired, you should feedback to RnD with the log and compress the file with password.

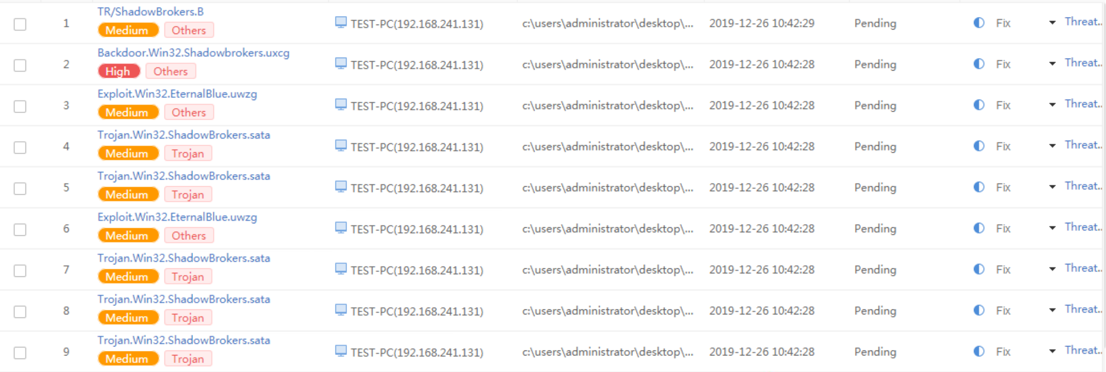
4. The macro virus repair scenarios is complicated. Due to the different repair technologies of each manufacturer, some repaired file still be reported by Endpoint Secure after repair by other manufacture, but because the complete macro code is damaged, it cannot be repaired. If you encounter such a situation, you can ignore or trust the files, product improvements will be made for these situations.

Common Situation

The host scans a large number of threat files and the threat names are all the same (Virus type), it may be infected virus or macro virus, please refer to the corresponding disposal ideas;

Example 1: Eternal Blue related virus files

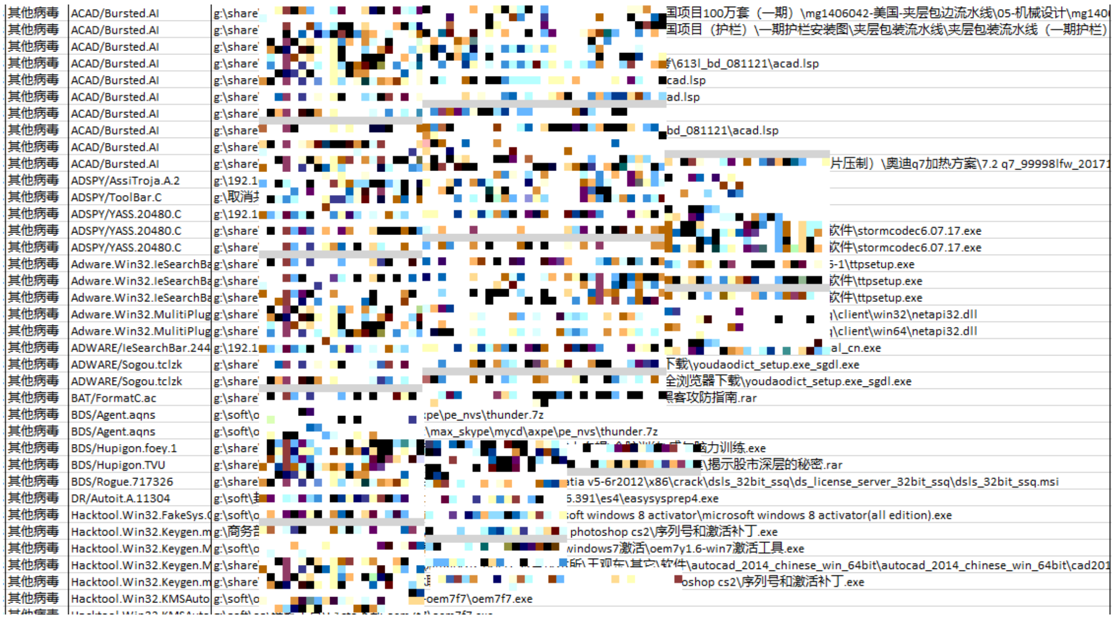
If there are hundreds of files with "EternalBlue" and "ShadowBrokers", it is an eternal blue exploit kit, indicating that the host may have a mining Trojan. You need to apply the corresponding patch first, and then check and kill:



□	1	TR/ShadowBrokers.B Medium Others	TEST-PC(192.168.241.131)	c:\users\administrator\desktop\...	2019-12-26 10:42:29	Pending	Fix	Threat..
□	2	Backdoor.Win32.Shadowbrokers.uxcg High Others	TEST-PC(192.168.241.131)	c:\users\administrator\desktop\...	2019-12-26 10:42:28	Pending	Fix	Threat..
□	3	Exploit.Win32.EternalBlue.uwzg Medium Others	TEST-PC(192.168.241.131)	c:\users\administrator\desktop\...	2019-12-26 10:42:28	Pending	Fix	Threat..
□	4	Trojan.Win32.ShadowBrokers.sata Medium Trojan	TEST-PC(192.168.241.131)	c:\users\administrator\desktop\...	2019-12-26 10:42:28	Pending	Fix	Threat..
□	5	Trojan.Win32.ShadowBrokers.sata Medium Trojan	TEST-PC(192.168.241.131)	c:\users\administrator\desktop\...	2019-12-26 10:42:28	Pending	Fix	Threat..
□	6	Exploit.Win32.EternalBlue.uwzg Medium Others	TEST-PC(192.168.241.131)	c:\users\administrator\desktop\...	2019-12-26 10:42:28	Pending	Fix	Threat..
□	7	Trojan.Win32.ShadowBrokers.sata Medium Trojan	TEST-PC(192.168.241.131)	c:\users\administrator\desktop\...	2019-12-26 10:42:28	Pending	Fix	Threat..
□	8	Trojan.Win32.ShadowBrokers.sata Medium Trojan	TEST-PC(192.168.241.131)	c:\users\administrator\desktop\...	2019-12-26 10:42:28	Pending	Fix	Threat..
□	9	Trojan.Win32.ShadowBrokers.sata Medium Trojan	TEST-PC(192.168.241.131)	c:\users\administrator\desktop\...	2019-12-26 10:42:28	Pending	Fix	Threat..

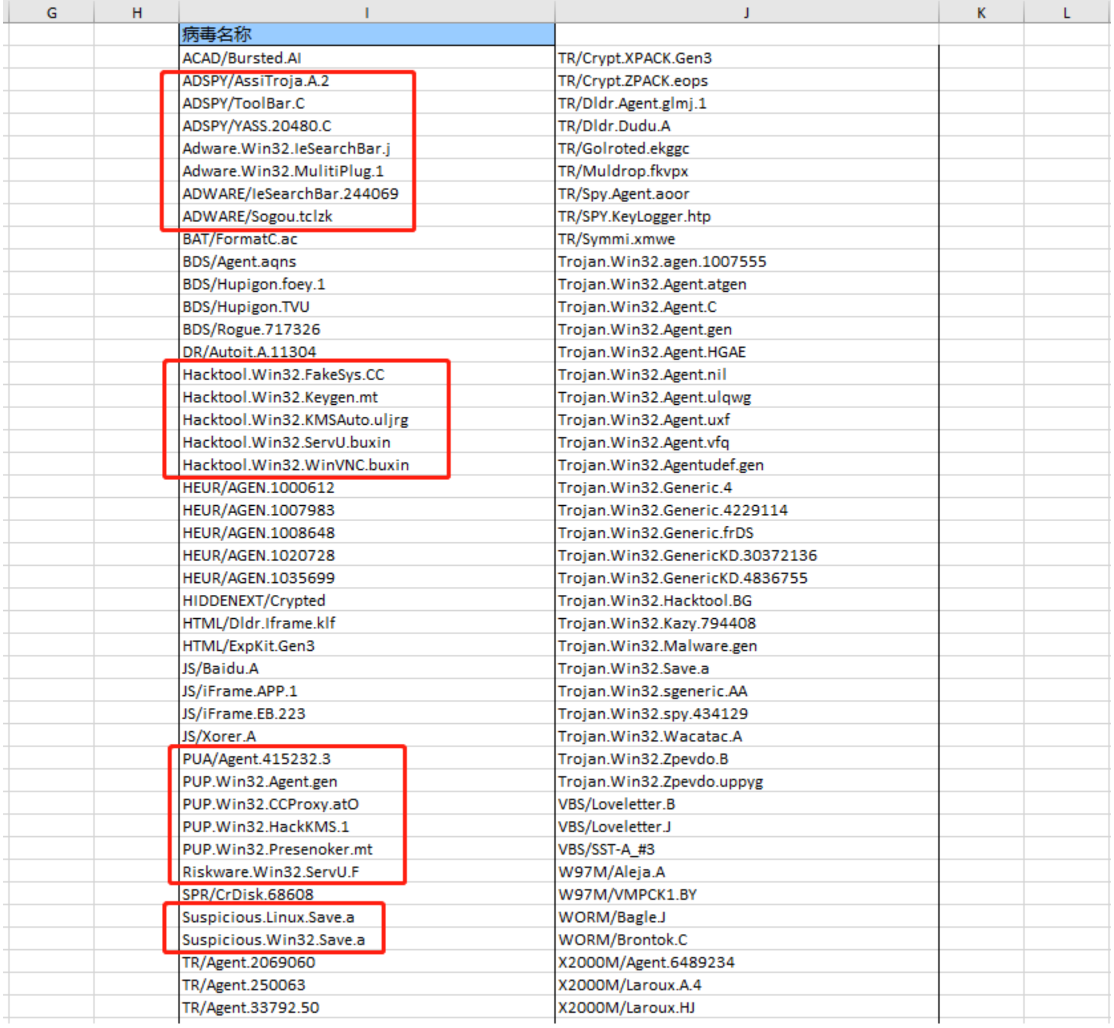
Example 2: File server reports a large number of viruses

The file server scanned for a large number of viruses:



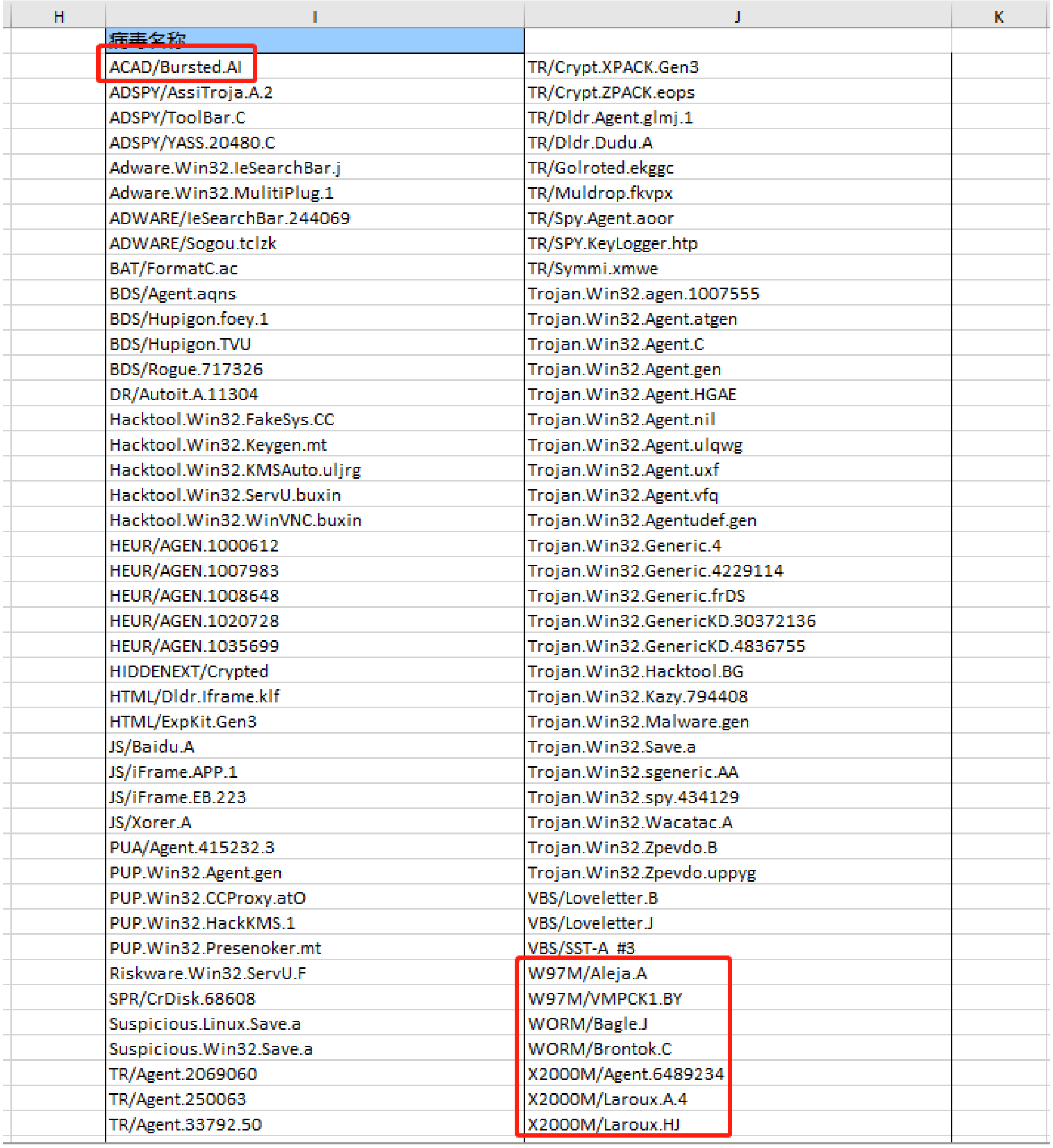
其他病毒	ACAD/Bursted.AI	g:\share [redacted] 国项目100万套（一期）\mg1406042-美国-夹层包边流水线\05-机械设计\mg140
其他病毒	ACAD/Bursted.AI	g:\share [redacted] 国项目（护栏）\一期护栏安装图\夹层包装流水线\夹层包装流水线（一期护栏）
其他病毒	ACAD/Bursted.AI	g:\share [redacted]
其他病毒	ACAD/Bursted.AI	g:\share [redacted] \613l_bd_081121\acad.lsp
其他病毒	ACAD/Bursted.AI	g:\share [redacted] cad.lsp
其他病毒	ACAD/Bursted.AI	g:\share [redacted] ad.lsp
其他病毒	ACAD/Bursted.AI	g:\share [redacted]
其他病毒	ACAD/Bursted.AI	g:\share [redacted] bd_081121\acad.lsp
其他病毒	ACAD/Bursted.AI	g:\share [redacted]
其他病毒	ACAD/Bursted.AI	g:\share [redacted] 片压制）\奥迪q7加热方案\7.2 q7_99998lfw_20171
其他病毒	ADSPY/AssiTroja.A.2	g:\192.1 [redacted]
其他病毒	ADSPY/ToolBar.C	g:\取消 [redacted]
其他病毒	ADSPY/YASS.20480.C	g:\192.1 [redacted]
其他病毒	ADSPY/YASS.20480.C	g:\share [redacted] 软件\stormcodec6.07.17.exe
其他病毒	ADSPY/YASS.20480.C	g:\share [redacted] 软件\stormcodec6.07.17.exe
其他病毒	Adware.Win32.IeSearchBa	g:\share [redacted] 5-1\ttpsetup.exe
其他病毒	Adware.Win32.IeSearchBa	g:\share [redacted] 软件\ttpsetup.exe
其他病毒	Adware.Win32.IeSearchBa	g:\share [redacted] 软件\ttpsetup.exe
其他病毒	Adware.Win32.MulitiPlug	g:\share [redacted] \client\win32\netapi32.dll
其他病毒	Adware.Win32.MulitiPlug	g:\share [redacted] \client\win64\netapi32.dll
其他病毒	ADWARE/IeSearchBar.244	g:\192.1 [redacted] al_cn.exe
其他病毒	ADWARE/Sogou.tclzk	g:\share [redacted] 下载\youdaodict_setup.exe_sgdl.exe
其他病毒	ADWARE/Sogou.tclzk	g:\share [redacted] 全浏览器下载\youdaodict_setup.exe_sgdl.exe
其他病毒	BAT/FormatC.ac	g:\share [redacted] 客攻防指南.rar
其他病毒	BDS/Agent.aqns	g:\soft\o [redacted] pe\pe_nvs\thunder.7z
其他病毒	BDS/Agent.aqns	g:\soft\o [redacted] \max_skype\mycd\axpe\pe_nvs\thunder.7z
其他病毒	BDS/Hupigon.foey.1	g:\share [redacted] 力训练.exe
其他病毒	BDS/Hupigon.TVU	g:\share [redacted] \揭示股市深层的秘密.rar
其他病毒	BDS/Rogue.717326	g:\share [redacted] atia v5-6r2012\x86\crack\dsls_32bit_ssq\ds_license_server_32bit_ssq\dsls_32bit_ssq.msi
其他病毒	DR/Autoit.A.11304	g:\soft\ [redacted] 5.391\es4\easysysprep4.exe
其他病毒	Hacktool.Win32.FakeSys.(	g:\soft\o [redacted] soft windows 8 activator\microsoft windows 8 activator(all edition).exe
其他病毒	Hacktool.Win32.Keygen.m	g:\商务部 [redacted] photoshop cs2\序列号和激活补丁.exe
其他病毒	Hacktool.Win32.Keygen.M	g:\soft\o [redacted] windows7激活\oem7y1.6-win7激活工具.exe
其他病毒	Hacktool.Win32.Keygen.M	g:\share [redacted] \autocad_2014_chinese_win_64bit\autocad_2014_chinese_win_64bit\cad201
其他病毒	Hacktool.Win32.Keygen.m	g:\share [redacted] oshop cs2\序列号和激活补丁.exe
其他病毒	Hacktool.Win32.KMSAuto	g:\soft\o [redacted] oem7f7\oem7f7.exe

First remove the virus name column separately and duplicate it. Then you can see the several types circled in the figure below. They are adware, installers, and hacking tools. If it is a useless file, it is recommended to isolate it. If it is needed Programs that can be ignored or trusted:



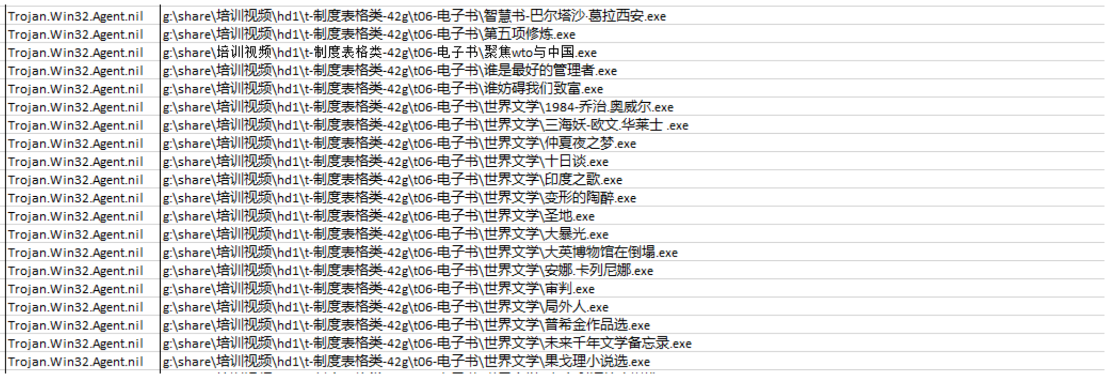
G	H	I	J	K	L
		病毒名称			
		ACAD/Bursted.AI	TR/Crypt.XPACK.Gen3		
		ADSPY/AssiTroja.A.2	TR/Crypt.ZPACK.eops		
		ADSPY/ToolBar.C	TR/Dldr.Agent.glmj.1		
		ADSPY/YASS.20480.C	TR/Dldr.Dudu.A		
		Adware.Win32.IeSearchBar.j	TR/Golroted.ekggc		
		Adware.Win32.MulitiPlug.1	TR/Muldrop.fkvpx		
		ADWARE/IeSearchBar.244069	TR/Spy.Agent.aoor		
		ADWARE/Sogou.tclzk	TR/SPY.KeyLogger.htp		
		BAT/FormatC.ac	TR/Symmi.xmwe		
		BDS/Agent.aqns	Trojan.Win32.agen.1007555		
		BDS/Hupigon.foey.1	Trojan.Win32.Agent.atgen		
		BDS/Hupigon.TVU	Trojan.Win32.Agent.C		
		BDS/Rogue.717326	Trojan.Win32.Agent.gen		
		DR/Autoit.A.11304	Trojan.Win32.Agent.HGAE		
		Hacktool.Win32.FakeSys.CC	Trojan.Win32.Agent.nil		
		Hacktool.Win32.Keygen.mt	Trojan.Win32.Agent.ulqwg		
		Hacktool.Win32.KMSAuto.uljrg	Trojan.Win32.Agent.uxf		
		Hacktool.Win32.ServU.buxin	Trojan.Win32.Agent.vfq		
		Hacktool.Win32.WinVNC.buxin	Trojan.Win32.Agentudef.gen		
		HEUR/AGEN.1000612	Trojan.Win32.Generic.4		
		HEUR/AGEN.1007983	Trojan.Win32.Generic.4229114		
		HEUR/AGEN.1008648	Trojan.Win32.Generic.frDS		
		HEUR/AGEN.1020728	Trojan.Win32.GenericKD.30372136		
		HEUR/AGEN.1035699	Trojan.Win32.GenericKD.4836755		
		HIDDENEXT/Crypted	Trojan.Win32.Hacktool.BG		
		HTML/Dldr.Iframe.klf	Trojan.Win32.Kazy.794408		
		HTML/ExpKit.Gen3	Trojan.Win32.Malware.gen		
		JS/Baidu.A	Trojan.Win32.Save.a		
		JS/iFrame.APP.1	Trojan.Win32.sgeneric.AA		
		JS/iFrame.EB.223	Trojan.Win32.spy.434129		
		JS/Xorer.A	Trojan.Win32.Wacatac.A		
		PUA/Agent.415232.3	Trojan.Win32.Zpevdo.B		
		PUP.Win32.Agent.gen	Trojan.Win32.Zpevdo.uppyg		
		PUP.Win32.CCProxy.atO	VBS/Loveletter.B		
		PUP.Win32.HackKMS.1	VBS/Loveletter.J		
		PUP.Win32.Presenoker.mt	VBS/SST-A_#3		
		Riskware.Win32.ServU.F	W97M/Aleja.A		
		SPR/CrDisk.68608	W97M/VMPCK1.BY		
		Suspicious.Linux.Save.a	WORM/Bagle.J		
		Suspicious.Win32.Save.a	WORM/Brontok.C		
		TR/Agent.2069060	X2000M/Agent.6489234		
		TR/Agent.250063	X2000M/Laroux.A.4		
		TR/Agent.33792.50	X2000M/Laroux.HJ		

As shown in the figure below, ACAD can be found in the virus information report form. It is a CAD virus. Usually it is not misreported and can be disposed directly. W97M and X2000M are disposed according to the macro virus disposal idea:



H	I	J	K
	病毒名称		
	ACAD/Bursted.AI	TR/Crypt.XPACK.Gen3	
	ADSPY/AssiTroja.A.2	TR/Crypt.ZPACK.eops	
	ADSPY/ToolBar.C	TR/Dldr.Agent.glmj.1	
	ADSPY/YASS.20480.C	TR/Dldr.Dudu.A	
	Adware.Win32.IeSearchBar.j	TR/Golroted.ekggc	
	Adware.Win32.MulitiPlug.1	TR/Muldrop.fkvpx	
	ADWARE/IeSearchBar.244069	TR/Spy.Agent.aoor	
	ADWARE/Sogou.tclzk	TR/SPY.KeyLogger.htp	
	BAT/FormatC.ac	TR/Symmi.xmwe	
	BDS/Agent.aqns	Trojan.Win32.agen.1007555	
	BDS/Hupigon.foey.1	Trojan.Win32.Agent.atgen	
	BDS/Hupigon.TVU	Trojan.Win32.Agent.C	
	BDS/Rogue.717326	Trojan.Win32.Agent.gen	
	DR/Autoit.A.11304	Trojan.Win32.Agent.HGAE	
	Hacktool.Win32.FakeSys.CC	Trojan.Win32.Agent.nil	
	Hacktool.Win32.Keygen.mt	Trojan.Win32.Agent.ulqwg	
	Hacktool.Win32.KMSAuto.uljrg	Trojan.Win32.Agent.uxf	
	Hacktool.Win32.ServU.buxin	Trojan.Win32.Agent.vfq	
	Hacktool.Win32.WinVNC.buxin	Trojan.Win32.Agentudef.gen	
	HEUR/AGEN.1000612	Trojan.Win32.Generic.4	
	HEUR/AGEN.1007983	Trojan.Win32.Generic.4229114	
	HEUR/AGEN.1008648	Trojan.Win32.Generic.frDS	
	HEUR/AGEN.1020728	Trojan.Win32.GenericKD.30372136	
	HEUR/AGEN.1035699	Trojan.Win32.GenericKD.4836755	
	HIDDENEXT/Crypted	Trojan.Win32.Hacktool.BG	
	HTML/Dldr.Iframe.klf	Trojan.Win32.Kazy.794408	
	HTML/ExpKit.Gen3	Trojan.Win32.Malware.gen	
	JS/Baidu.A	Trojan.Win32.Save.a	
	JS/iFrame.APP.1	Trojan.Win32.sgeneric.AA	
	JS/iFrame.EB.223	Trojan.Win32.spy.434129	
	JS/Xorer.A	Trojan.Win32.Wacatac.A	
	PUA/Agent.415232.3	Trojan.Win32.Zpevdo.B	
	PUP.Win32.Agent.gen	Trojan.Win32.Zpevdo.uppyg	
	PUP.Win32.CCProxy.atO	VBS/Loveletter.B	
	PUP.Win32.HackKMS.1	VBS/Loveletter.J	
	PUP.Win32.Presenoker.mt	VBS/SST-A #3	
	Riskware.Win32.ServU.F	W97M/Aleja.A	
	SPR/CrDisk.68608	W97M/VMPCK1.BY	
	Suspicious.Linux.Save.a	WORM/Bagle.J	
	Suspicious.Win32.Save.a	WORM/Brontok.C	
	TR/Agent.2069060	X2000M/Agent.6489234	
	TR/Agent.250063	X2000M/Laroux.A.4	
	TR/Agent.33792.50	X2000M/Laroux.HJ	

For some other virus names, it is hard to judge whether it is malicious according to the name. Therefore, observe the path. For example, most of the files corresponding to Trojan.Win32.Agent.nil appear to be stored by the user. For analysis, it is a non-standard exe program, and no signature causes a virus report. This type can be handled as needed:



Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\智慧书-巴尔塔沙·葛拉西安.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\第五项修炼.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\聚焦wto与中国.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\谁是最好的管理者.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\谁妨碍我们致富.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\1984-乔治.奥威尔.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\三海妖-欧文.华莱士 .exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\仲夏夜之梦.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\十日谈.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\印度之歌.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\变形的陶醉.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\圣地.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\大暴光.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\大英博物馆在倒塌.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\安娜.卡列尼娜.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\审判.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\局外人.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\普希金作品选.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\未来千年文学备忘录.exe
Trojan.Win32.Agent.nil	g:\share\培训视频\hd1\t-制度表格类-42g\t06-电子书\世界文学\果戈理小说选.exe

SANGFOR

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc