



SANGFOR



Panduan untuk mengidentifikasi file yang terinfeksi



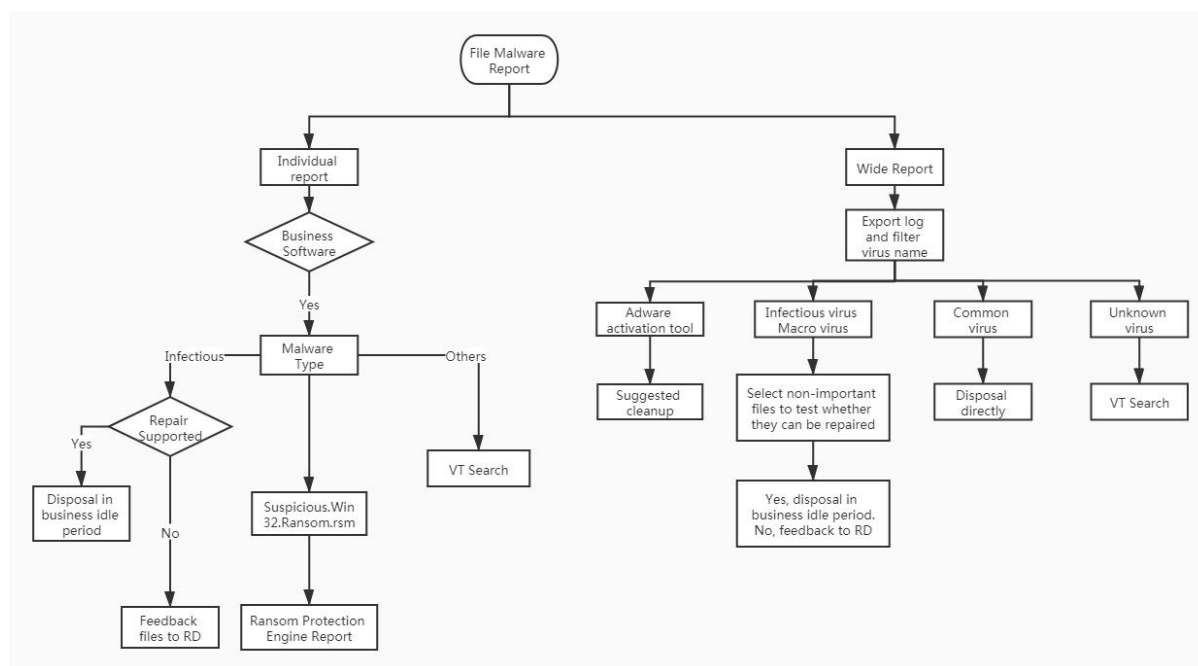
Perubahan Catatan

Tanggal	Deskripsi Perubahan
27 Desember, 2019	Versi 1 dokumen lolos.

Daftar Isi

Bab 1 Memahami Informasi Malware.....	1
Bab 2 Menilai Dengan Threat Intelligence.....	2
Bab 3 Mesin Ransomware Melaporkan Kejahatan (Suspicious.Win32.Ransom.rsm).....	3
Bab 4 Virus Menular.....	4
4.1 Laporan Dukungan Endpoint Secure Pada Virus Menular (Umum).....	4
4.2 Langkah Penanganan Infeksi Virus.....	4
Bab 5 Virus Makro.....	5
5.1 Pendahuluan.....	5
5.2 Ide pembuangan virus makro.....	5
Bab 6 Situasi Umum.....	5
6.1 Contoh 1: File Virus terkait Eternal Blue.....	5
6.2 Contoh 2: Server file melaporkan virus berjumlah besar.....	6

Panduan untuk mengidentifikasi file yang terinfeksi



Catatan: Jangan mengupload file atau folder pelanggan ke web eksternal terutama file dokumen.

Bab 1 Memahami Informasi Malware

Tipe Malware	Deskripsi	Tingkat Ancaman
Trojan	Trojan	Tinggi
Backdoor	Backdoor	Tinggi
Virus	Virus (umumnya menular)	Tinggi
Worm	Worm (Termasuk bagian dari virus menular)	Tinggi
Ransom	Ransom	Tinggi
W97M/VBA/MSWord/X2000M	Macro Virus (Semua adalah File Dokumen)	Tinggi
Exploit	Exploit	Tinggi
ACAD/CAD	CAD Virus	Tinggi
HackTool	HackTool	Sedang
Suspicious.Win32.Ransom.rsm	Mesin ransomware melaporkan racun	Subject to the file
Suspicious	File yang mencurigakan	Rendah
Adware	Adware	Rendah
Application/PUP/PUA	Application/PUP/PUA	Rendah

Bab 2 Menilai Dengan Threat Intelligence

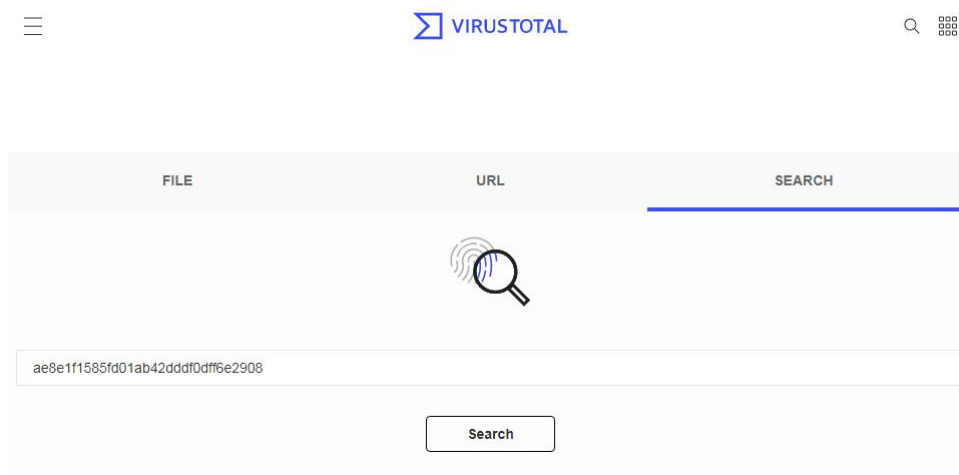
Cari threat/ancaman: <https://www.virustotal.com>

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

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

Apabila software layanan bisnis pelanggan dan aplikasi yang normal dilaporkan sebagai malware atau virus. Kunjungi <https://www.virustotal.com> untuk melakukan pengecekan.

1. Gunakan nilai MD5 untuk melakukan check-in VT (<https://www.virustotal.com>), seperti gambar dibawah ini:



2. Anda bisa mendapatkan laporan yang sesuai setelah VT selesai diperiksa.

Number of vendors that participated file analysing

Analyze again and submit report

Feedback information by vendors

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

Panduan untuk mengidentifikasi file yang terinfeksi

DETECTION **DETAILS** COMMUNITY

Click to view details

Basic Properties

MD5	ae8e1f1585fd01ab42ddd0dff6e2908
SHA-1	7b804d14e27f1951af7aec46377c8a780d6b4e08
SHA-256	ec58de029bc51bc0b160df7edc6d23857716a3d8c3cebaad0d70b264410e24d8
Vhash	11704d5f66656z
Authentihash	dc8e511b415832d10d4f423c318cf0dc24d638e5bbdcb3c37499f0480183376f
SSDEEP	98304:9xQHznz/cVa6gD7/d45EpiiSqFka+Y6K9yBKr9ijMoNBdAZNLUUeX5GnO37:cH0a52lJ3K9y9lJlMohAy
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

Kriteria file daftar putih didapat dari informasi di atas. (Aturan di bawah ini dapat menjadi referensi untuk memasukkan file ke daftar putih. Kriteria harus memenuhi beberapa aturan untuk memasukkan file ke daftar putih. Jika situasi tidak pasti, jangan masukan file ke daftar putih.)

1. Ditandatangani secara digital, VT tidak melaporkan bahaya, dapat langsung dinilai aman.
2. Ada tanda tangan digital, tetapi VT memiliki laporan berbahaya dari pabrik. Dalam kasus ini, harus dinilai apakah itu laporan benar-benar palsu. Umumnya kurang dari 5 laporan, anda harus cek jenis laporan berbahaya. Selain itu, jika tanda tangan digital tersebut berasal dari perusahaan ternama, maka file dinilai aman.
3. Jika ada tanda tangan digital yang tidak valid dan tanda tangan dari perusahaan terkenal. File tersebut dapat dinilai aman.
4. Jika ada tanda tangan digital yang tidak valid, waktu pengiriman pertama dan terakhir lebih dari 2 minggu. File tersebut dapat dinilai aman.
5. Jika tidak ada tanda tangan digital, VT tidak melaporkan file sebagai virus, dan tanggal analisis terakhir adalah lebih dari 30 hari dari waktu saat ini. Dalam hal ini dapat dikenali sebagai beberapa kiriman. (Arti dari beberapa kiriman: waktu kiriman pertama dan kiriman terakhir tidak sama). Jika tidak banyak pengiriman, disarankan untuk menganalisis dan memperbarui laporan analisis lagi untuk membuat penilaian) (Tanpa tanda tangan digital, tidak ada virus laporan VT. File tersebut tidak dapat dianggap aman.)

Bab 3 Mesin Ransomware Melaporkan Kejahatan (Suspicious.Win32.Ransom.rsm)

Alasannya biasanya karena proses tersebut menulis atau menghapus file umpan ransomware;

Panduan untuk mengidentifikasi file yang terinfeksi

Jika Anda menemukan laporan program yang memiliki fungsi pembersihan file sampah seperti 360 dan Tencent Computer Manager (jalur penginstalan 360, tencent, qqpcmgr, dll.), Anda perlu memberi umpan balik file terkait ke RnD, dan kemudian mengabaikan:

No	Deteksi	Identifikasi	File	Waktu	Aksi
1	Suspicious.Win32.Ransom.rsm 高威胁 勒索病毒	WRGHO-20190104A(172.16...	d:\qqpcmgr\13.4.20299.301\qqctray.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\qqctray.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

Pada saat yang sama, Anda perlu mengambil dua file di direktori instalasi Endpoint Secure:

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

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

Bab 4 Virus Menular

4.1 Laporan Dukungan Endpoint Secure Pada Virus Menular (Umum)

Almanah
Chir
Expiro
Floxif
Jadtre
Neshta
Parite
Ramnit
Sality
Virut

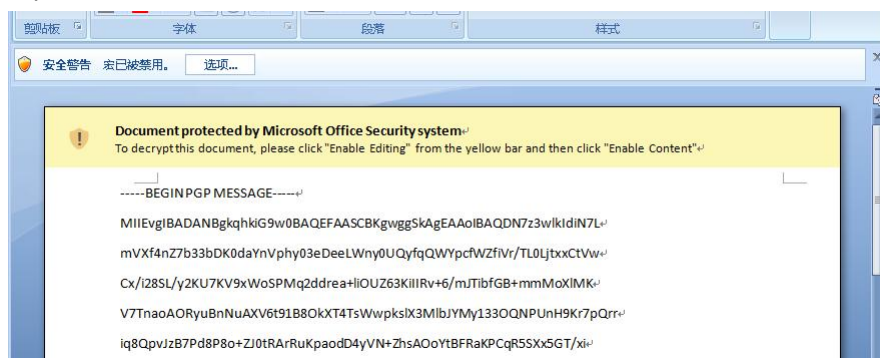
4.2 Langkah Penanganan Infeksi Virus

1. Lakukan pemindaian penuh di PC, periksa perbaikan yang didukung virus oleh Endpoint Secure (Eg Virus / Ramnit.a, Virus.Win32.Save.a yang biasanya merupakan infeksi virus);
2. Jika ada dalam daftar perbaikan, lakukan pemrosesan satu-klik (Proses yang sesuai dengan file mungkin berhenti selama perbaikan, dan proses ini harus dilakukan selama bukan jam kerja);
3. Jika tidak ada dalam daftar perbaikan, atau jenis infeksi yang dilaporkan oleh mesin SAVE tidak memiliki kelompok (seperti Virus.Win32.Save.a), pertama pilih salah satu dari dua file yang tidak penting untuk diperbaiki. Kemudian lihat apakah itu diperbaiki atau diisolasi. Jika dapat diperbaiki maka dapat melanjutkan ke proses satu klik; jika diisolasi, pilih bagian dari file exe, kompres dengan kata sandi, dan masukkan kembali ke RnD bersama dengan log pemindaian;
4. Jika Anda ingin memindai seluruh jaringan, disarankan untuk memisahkan server bisnis dari PC kantor biasa. Pertama Anda dapat memeriksa server penting satu per satu dan memeriksa apakah infeksi dapat diperbaiki.

Bab 5 Virus Makro

5.1 Pendahuluan

Virus makro adalah virus komputer yang berada di makro dari dokumen atau templat. Setelah fungsi makro diaktifkan untuk dokumen semacam itu, kode makro di dalamnya akan dieksekusi. Virus makro umum saat ini dibagi menjadi virus makro template atau virus makro download. Jika template virus makro terinfeksi, semua dokumen yang disimpan secara otomatis di host akan "terinfeksi" dengan virus makro ini; mengunduh virus makro terutama digunakan untuk mengunduh dan menjalankan file berbahaya lainnya.



5.2 Ide pembuangan virus makro

Ada beberapa virus makro yang dapat diperbaiki, terutama virus makro template. Saat Endpoint Secure mendeteksi dan membunuh sejumlah besar virus makro:

1. Perbaiki sekali klik setelah pencadangan. Jika file dapat diperbaiki, mereka akan diperbaiki, dan file yang tidak dapat diperbaiki akan diisolasi;
2. Pilih bukan jam kerja untuk melakukan proses perbaikan, jika ternyata tidak dapat diperbaiki, Anda dapat memulihkan dari area karantina;
3. Untuk virus makro yang tidak dapat diperbaiki, Anda harus memberi umpan balik ke RnD dengan log dan kompres file dengan kata sandi.
4. Skenario perbaikan virus makro rumit. Karena teknologi perbaikan yang berbeda dari setiap pabrikan, beberapa file yang diperbaiki masih dilaporkan oleh Endpoint Secure setelah diperbaiki oleh pabrikan lain, tetapi karena kode makro lengkap rusak, itu tidak dapat diperbaiki. Jika Anda mengalami situasi seperti itu, Anda dapat mengabaikan atau mempercayai file, perbaikan dari sisi produk akan dilakukan untuk situasi ini.

Bab 6 Situasi Umum

Tuan rumah memindai sejumlah besar file ancaman dan nama ancaman semuanya sama (jenis Virus), mungkin saja virus yang terinfeksi atau virus makro, silakan merujuk ke ide pembuangan yang sesuai;

6.1 Contoh 1: File Virus terkait Eternal Blue

Jika ada ratusan file dengan "EternalBlue" dan "ShadowBrokers", itu adalah salah satu exploit dari eternal blue, yang menunjukkan bahwa host mungkin memiliki penambahan Trojan. Anda perlu menerapkan patch yang sesuai terlebih dahulu, lalu periksa dan matikan prosesnya:

Panduan untuk mengidentifikasi file yang terinfeksi

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..

6.2 Contoh 2: Server file melaporkan virus berjumlah besar

Server file memindai virus berjumlah besar:

其他病毒	ACAD/Bursted.Al	g:\share	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.Al	g:\share	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.Al	g:\share	f\613_bd_081121\acad.lsp
其他病毒	ACAD/Bursted.Al	g:\share	acad.lsp
其他病毒	ACAD/Bursted.Al	g:\share	ad.lsp
其他病毒	ACAD/Bursted.Al	g:\share	bd_081121\acad.lsp
其他病毒	ACAD/Bursted.Al	g:\share	bd_081121\acad.lsp
其他病毒	ADSPY/AssiTroja.A.2	g:\192.1	片压制)\奥迪q7加热方案\7.2 q7_99998\fw_2017
其他病毒	ADSPY/ToolBar.C	g:\取消消	
其他病毒	ADSPY/YASS.20480.C	g:\192.1	
其他病毒	ADSPY/YASS.20480.C	g:\share	软件\stormcodec6.07.17.exe
其他病毒	ADSPY/YASS.20480.C	g:\share	软件\stormcodec6.07.17.exe
其他病毒	ADware.Win32.IeSearchB	g:\share	5-1\tpsetup.exe
其他病毒	ADware.Win32.IeSearchB	g:\share	软件\tpsetup.exe
其他病毒	ADware.Win32.MulitiPlug	g:\share	软件\tpsetup.exe
其他病毒	ADware.Win32.MulitiPlug	g:\share	\client\win32\netapi32.dll
其他病毒	ADWARE/IeSearchBar.244	g:\192.1	\client\win64\netapi32.dll
其他病毒	ADWARE/Sogou.tclzk	g:\share	al_cn.exe
其他病毒	ADWARE/Sogou.tclzk	g:\share	下载\youdaodict_setup.exe_sgdl.exe
其他病毒	BAT/FormatC.ac	g:\share	全浏览器下载\youdaodict_setup.exe_sgdl.exe
其他病毒	BDS/Agent.aqns	g:\soft\o	病毒攻防指南.rar
其他病毒	BDS/Agent.aqns	g:\soft\o	pe\pe_nvs\thunder.7z
其他病毒	BDS/Hupigon.foey.1	g:\share	\max_skype\mycd\axpe\pe_nvs\thunder.7z
其他病毒	BDS/Hupigon.TVU	g:\share	磁力训练.exe
其他病毒	BDS/Rogue.717326	g:\share	揭示股市深层的秘密.rar
其他病毒	DR/AutoIt.A.11304	g:\soft\3	stia v5-6r2012\X86\crack\dsls_32bit_ssq\ds_license_server_32bit_ssq\dsls_32bit_ssq.msi
其他病毒	Hacktool.Win32.FakeSysC	g:\soft\3	5.391\es4\easyssysprep4.exe
其他病毒	Hacktool.Win32.Keygen.M	g:\soft\o	soft windows 8 activator\microsoft windows 8 activator(all edition).exe
其他病毒	Hacktool.Win32.Keygen.M	g:\soft\o	photoshop cs2\序列号和激活补丁.exe
其他病毒	Hacktool.Win32.Keygen.M	g:\soft\o	windows7激活\oem7y1.6-win7激活工具.exe
其他病毒	Hacktool.Win32.KMSAuto	g:\soft\o	激活于任何正版软件\autocad_2014_chinese_win_64bit\autocad_2014_chinese_win_64bit\cad20
其他病毒	Hacktool.Win32.KMSAuto	g:\soft\o	oshop cs2\序列号和激活补丁.exe

Pertama, hapus kolom nama virus secara terpisah dan duplikat. Kemudian Anda dapat melihat beberapa jenis yang dilingkari pada gambar di bawah ini. Mereka adalah adware, installer, dan alat hacking. Jika ini adalah file yang tidak berguna, disarankan untuk mengisolasi. Jika diperlukan Program yang dapat diabaikan atau dipercaya:

Panduan untuk mengidentifikasi file yang terinfeksi

G	H	I	J	K	L
		病毒名称			
		ACAD/Bursted.AI	TR/CryptXPACK.Gen3		
		ADSPY/AssiTroja.A.2	TR/CryptZPACK.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.MultiPlug.1	TR/Muldrop.fkvp		
		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		

Seperti yang ditunjukkan pada gambar di bawah ini, ACAD dapat ditemukan dalam formulir laporan informasi virus. Itu adalah virus CAD. Biasanya tidak salah pelaporan dan dapat dibuang secara langsung. W97M dan X2000M dibuang sesuai dengan gagasan pembuangan virus makro:

H	I	J	K
	病毒名称		
	ACAD/Bursted.AI	TR/CryptXPACK.Gen3	
	ADSPY/AssiTroja.A.2	TR/CryptZPACK.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.MultiPlug.1	TR/Muldrop.fkvp	
	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	

Untuk beberapa nama virus lainnya, sulit untuk menilai apakah itu berbahaya menurut namanya. Oleh karena itu, amati alurnya. Misalnya, sebagian besar file yang terkait dengan Trojan.Win32.Agent.nil tampaknya disimpan oleh pengguna. Untuk analisis, ini adalah program exe non-standar, dan tidak ada tanda yang menyebabkan laporan virus. Jenis ini dapat ditangani sesuai kebutuhan:

Panduan untuk mengidentifikasi file yang terinfeksi

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·亨利.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\大曝光.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



Hak cipta (c) Sangfor Technologoes Inc. Hak cipta dilindungi oleh undang-undang. Dilarang menyebarkan atau memproduksi ulang sebagian dari atau seluruh dokumen ini tanpa persetujuan tertulis dari Sangfor Technologies Inc. SANGFOR adalah merek dagang dari Sangfor Technologies Inc. Semua merek dagang dan nama dagang lain yang disebutkan dalam dokumen ini adalah milik dari pemegangnya masing-masing. Segala upaya telah dilakukan dalam mempersiapkan dokumen ini untuk memastikan keakuratan konten, namun semua pernyataan, informasi, dan rekomendasi dalam dokumen ini bukan merupakan jaminan dalam bentuk apa pun, tersurat maupun tersirat. Informasi dalam dokumen ini dapat berubah tanpa pemberitahuan. Untuk mendapatkan versi terbaru, hubungi pusat layanan internasional SANGFOR Technologies Inc.