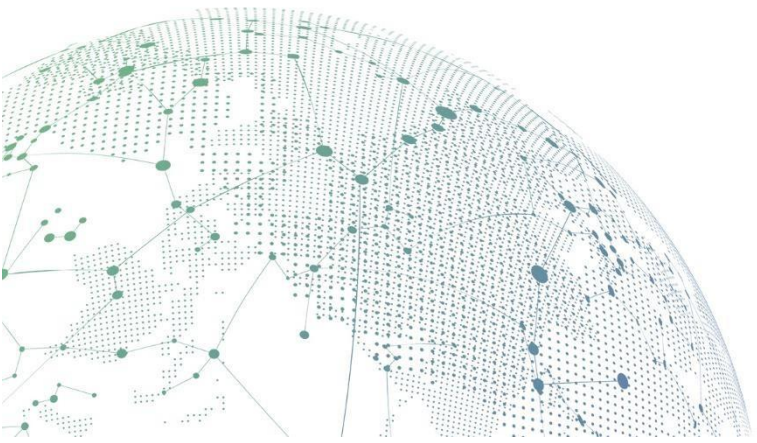
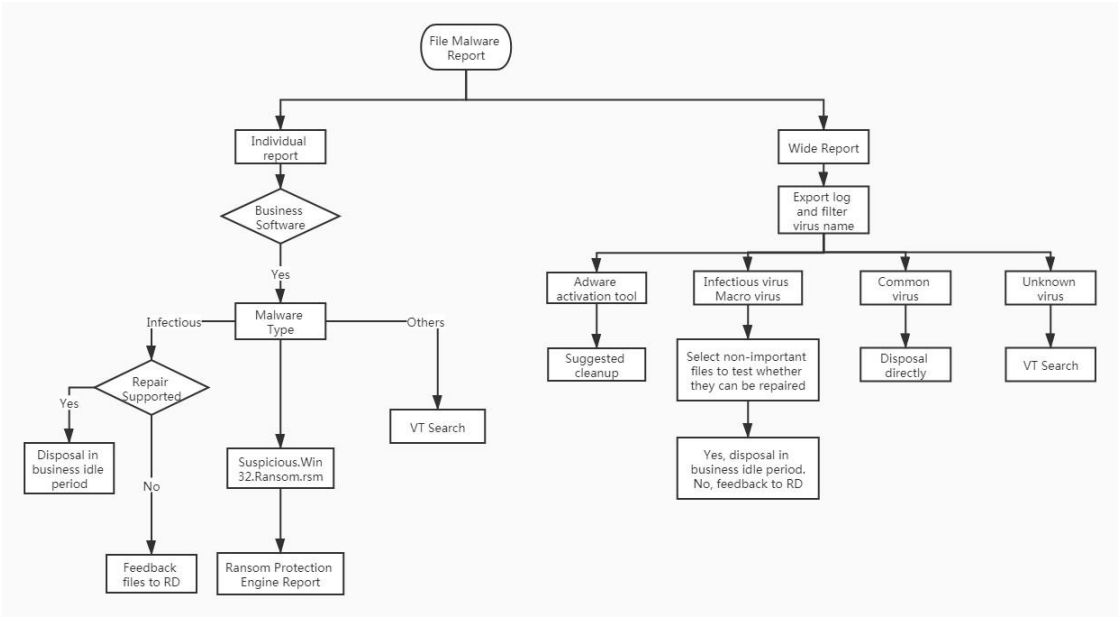
SANGFOR

Guide to Identify Infected File



Tanggal	Deskripsi Perubahan
27 Desember 2019	Dokumen versi 1 terbit

Daftar isi



Peringatan: Jangan mengunggah file atau folder pelanggan ke web eksternal terutama file dokumen.

Memahami Informasi Malware

Tipe Malware	**Deskripsi**	**Tingkatan Ancaman**
Trojan	Trojan	Tinggi
Backdoor	Backdoor	Tinggi
Virus	Virus (Generally infectious virus)	Tinggi
Worm	Worm (Including a part of infectious virus)	Tinggi
Ransom	Ransom	Tinggi
W97M/VBA/MSWord/X2000M	Macro Virus (All are Document Files)	Tinggi
Exploit	Exploit	Tinggi
ACAD/CAD	CAD Virus	Tinggi
HackTool	HackTool	Menengah
Suspicious.Win32.Ransom.rsm	Ransomware engine reports poison	Mengacuh pada file

Suspicious	Suspicious Files	Rendah
Adware	Adware	Rendah
Application/PUP/PUA	Application/PUP/PUA	Rendah

Menilai dengan Judge Threat Intelligence

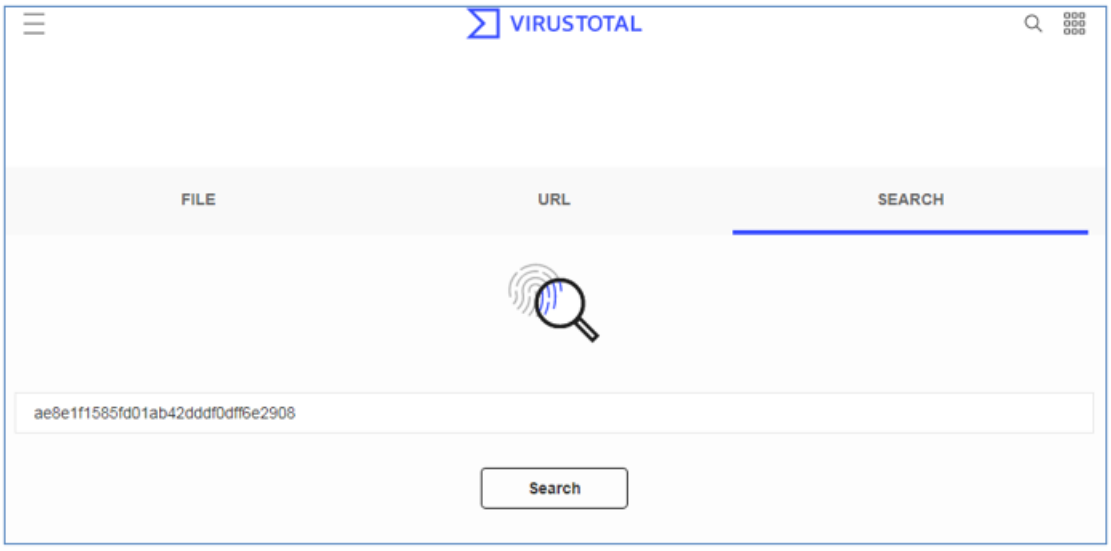
Temukan file ancaman: https://www.virustotal.com

Temukan traffic ancaman: https://x.threatbook.cn/

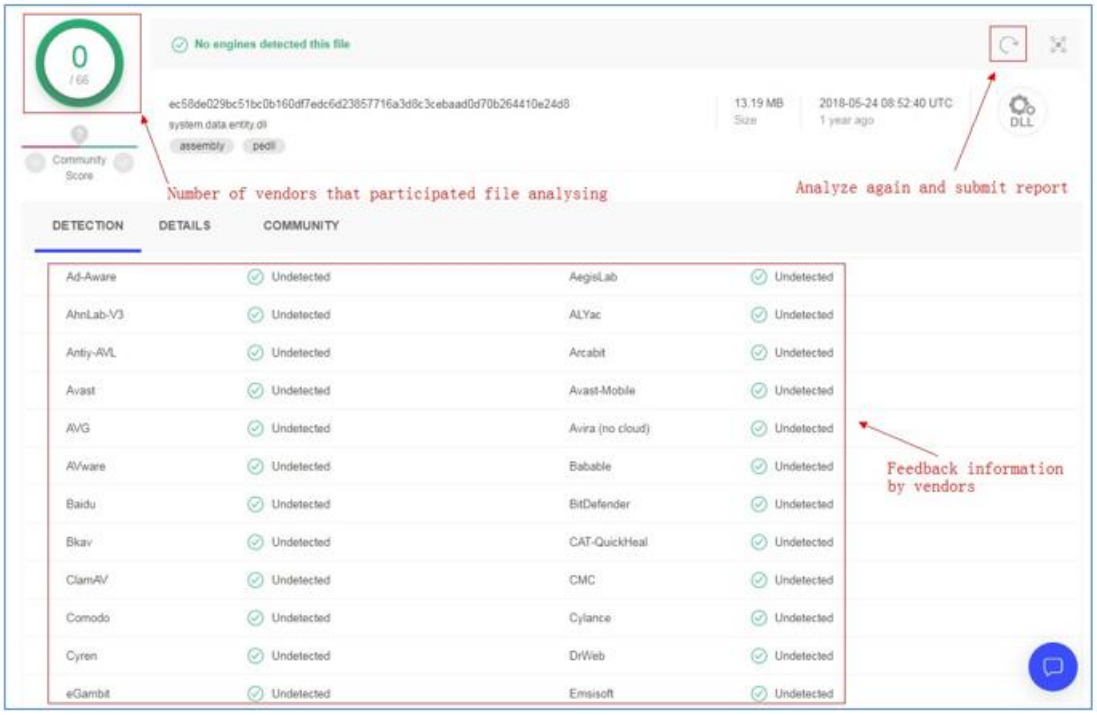
Online sandbox: https://habo.qq.com/ https://any.run/

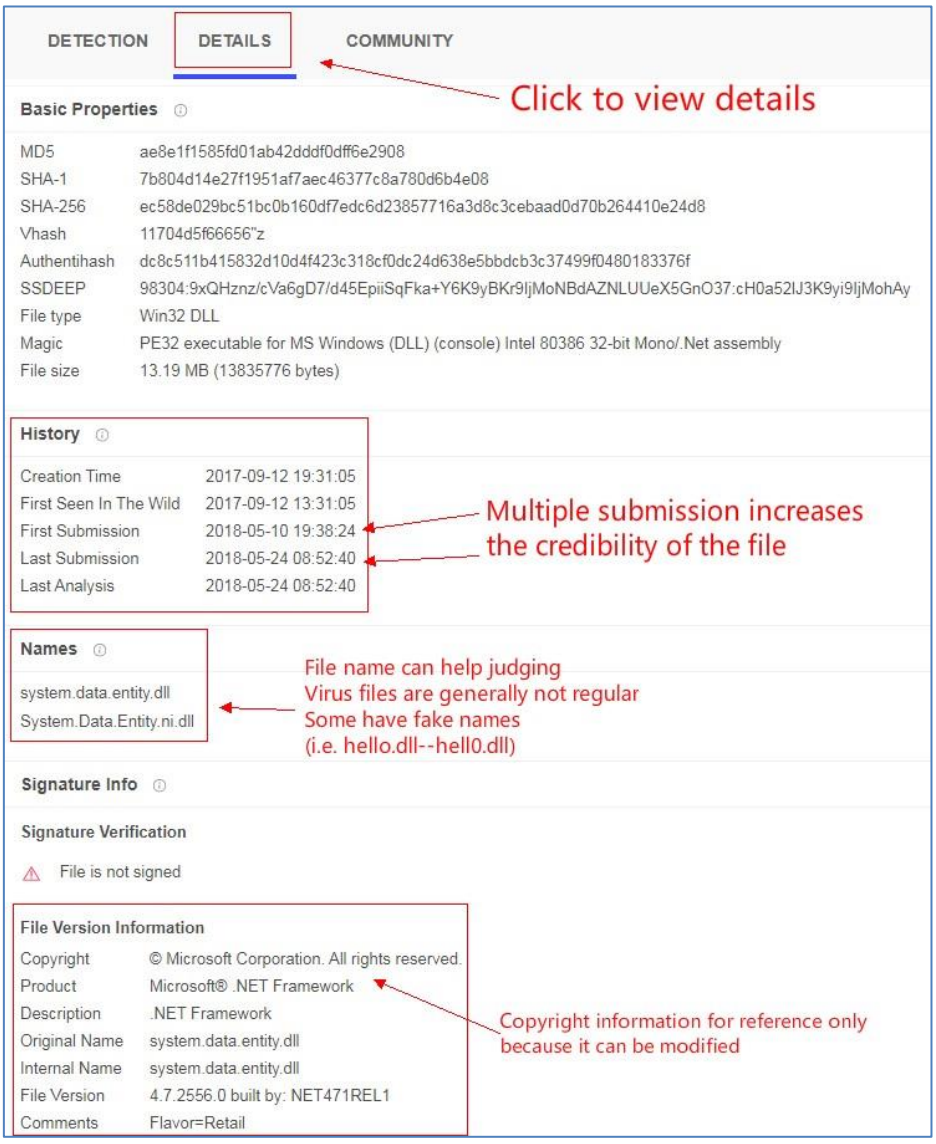
Ketika software dan aplikasi normal bisnis pelanggan dilaporkan sebagai malware atau virus. Kunjungi https://www.virustotal.com untuk melakukan pemeriksaan.

1. Gunakan enkripsi MD5 untuk melakukan pemeriksaan VT (https://www.virustotal.com), seperti tampilan figur dibawah:



2. Anda dapat laporan lengkap setelah VT selesai melakukan pemeriksaan.





Kriteria file Whitelist dapat dicapai dari informasi dibawah. (Dibawah ini adalah rules yang dapat dijadikan referensi untuk whitelist sebuah file. Membutuhkan memenuhi beberapa rule

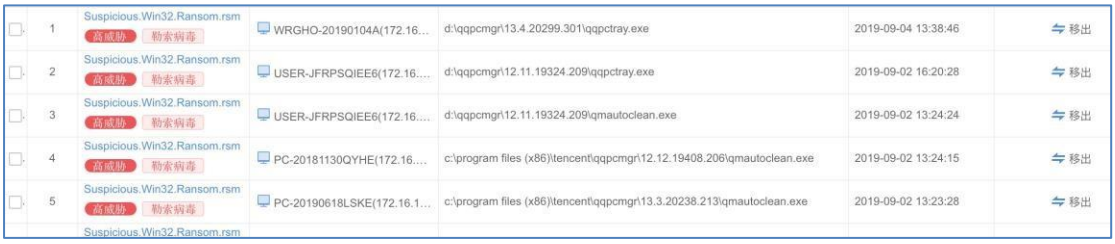
agar file dapat di whitelist. Dalam situasi yang tidak yakin jangan whitelist file)

1. Ditandatangani secara digital, VT tidak melaporkan mencurigakan, dapat secara langsung dinilai sebagai aman.
2. Memiliki tandatangan digital, namun VT memiliki laporan mencurigakan dari pembuat file, dalam kasus ini, ini harus dinilai sebagai laporan false positive. Biasanya kurang dari laporan, nada dapat memeriksa tipe dari laporan yang mencurigakan . Selain itu jika tanda tangan digital berasal dari perusahaan yang sangat terkenal, file dapat dinilai sebagai aman.
3. Jika ada tanda tangan digital yang sudah tidak berlaku dan tanda tersebut berasal dari perusahaan yang dikenal secara baik. File dapat dinyatakan aman.
4. Jika ada tanda tangan digital yang sudah tidak berlaku, tapi waktu pertama dan terakhir pengajuannya lebih dari 2 minggu, file dapat dikatakan aman.
5. Jika tidak ada tanda digital. VT tidak melaporkan sebagai file virus, dan analisa terakhir lebih dari 30 hari dari saat ini. Dalam kasus ini dapat dikenali sebagai pengajuan dalam jumlah banyak (pengertian dari pengajuan dalam jumlah banyak : waktu pertama kali pengajuandan pengajuan terakhir tidak sama)Jika ini bukan pengajuan yang banyak, direkomendasikan untuk menganalisa dan memperbaharui laporan analisa lagi untuk membuat penilaian. (Tanpa adanya tanda tangan digital.tanpa tanpa laporan virus, file tidak bisa dikatan aman)

Laporan Kejahatan Ransomware Engine

(Suspicious.Win32.Ransom.rsm)

\\Alasannya adalah biasanya proses mengubah dan menghapus file umpan ransomware;
Jika kamu menemukan program yang memiliki fungsi membersihkan seperti 360 dan Tencent Computer Manager (tempat instalasi adalah 360, tencent, qqpcmgr, dll.), anda butuh memberikan umpan balik kepada berupa file RnD, kemudian mengabaikannya:



Pada waktu yang bersamaan, anda butuh untuk mengambil 2 file di direktori instalasi Endpoint Secure;

\Sangfor\EDR\agent\bin\frep\local_certificate\rea
dme.txt C:\ProgramData\Sangfor\EDR\log\
sfavsvc.lo

Infeksi Virus

Laporan dukungan Endpoint Secure Pada Infeksi Virus (Umum)

Almanahe
Chir
Expiro
Floxif
Jadtre
Neshta
Parite
Ramnit
Sality
Virut

Langkah Menangani Infeksi Virus

1. Lakukan pemindaian penuh pada PC, periksa perbaikan virus pada Endpoint Secure (contoh Virus / Ramnit.a, Virus.Win32.biasanya menyimpan virus yang menginfeksi);

2. Jika virus ada di list perbaikan, lakukan proses sekali klik (Proses berhubungan dengan file akan terhenti selama perbaikan, dan proses ini seharusnya dilakukan diluar jam kerja);

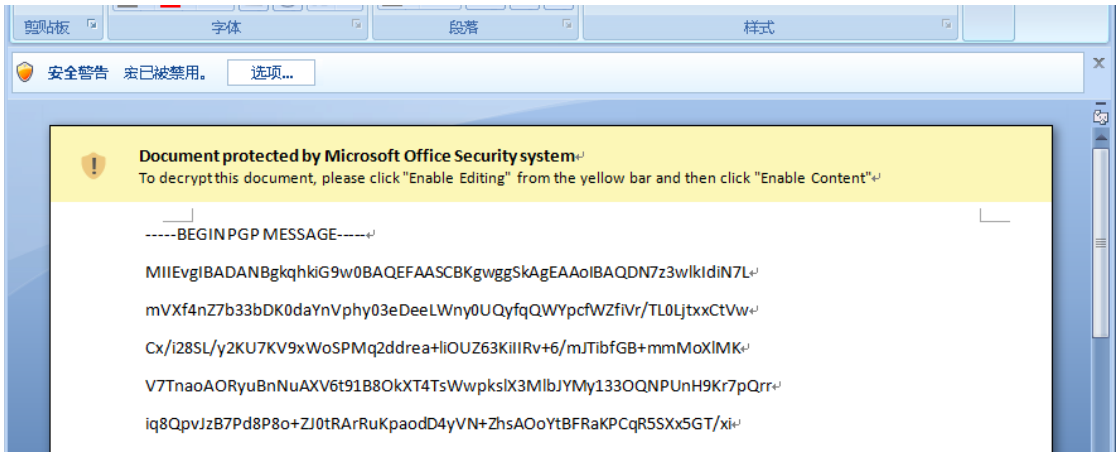
3. Jika virus tidak berada di dalam list perbaikan, atau jika tipe infeksi teleah dilaporakan oleh save engine bahwa tida memiliki tipe sejenenis (seperti Virus.Win32.Save.a), pertama pilih satu atau dua file yang tidak terlalu penting untuk diperbaiki. Lalu lihat apakah file nya benar atau terisolasi. Jika itu dapat diperbaiki lalu proses dapat dilakukan satu kali klik, jika teriskolasi, lalu pilih bagian dari file exe, kompresi dengan password lalu kirimkan ke tim RnD bersama dengan log pemindaian.

4. Jika ada ingin memindai seluruh jaringan, direkomendasikan untuk memisahkan server bisnis dengan pc kantor biasa, Anda dapat memeriksa server yang penting sendiri lalu periksa apakah infeksi dapat diperbaiki.

Makro Virus

Pengenalan

Makro virus adalah virus komputer yang menempati sebuah dokumen atau template. Begitu fungsi makro diaktifkan untuk seperti pada dokumen, kode makro akan dijalankan. Umumnya makro virus dibagi menjadi makro virus template atau makro virus download. Jika terinfeksi makro virus template, semua dokumen secara otomatis semua dokumen yang tersimpan di host akan ikut tersinfeksi; makrovirus download adalah virus yang digunakan untuk mendownload and menjalankan file kotor lainnya.



Ide Pembuangan Makro Virus

Ada beberapa makro virus yang dapat diperbaiki, terutama makro virus template, Ketika Endpoint Secure mendeteksi dan membunuh makro virus dalam jumlah besar:T

1. Satu kali klik perbaikan setelah backup. Jika file dapat diperbaiki, maka akan diperbaiki,dan yang tidak dapat diperbaiki akan diisolasi;

2. Pilih diluar jam kerja untuk proses perbaikan, Jika ditemukan tidak dapat diperbaiki, anda dapat memulihkan dari quarantine area;

3. Untuk makro virus yang tidak dapat diperbaiki, anda sebaiknya memberikan feed back kepada tim RnD dengan log dan kompresi file dengan password.

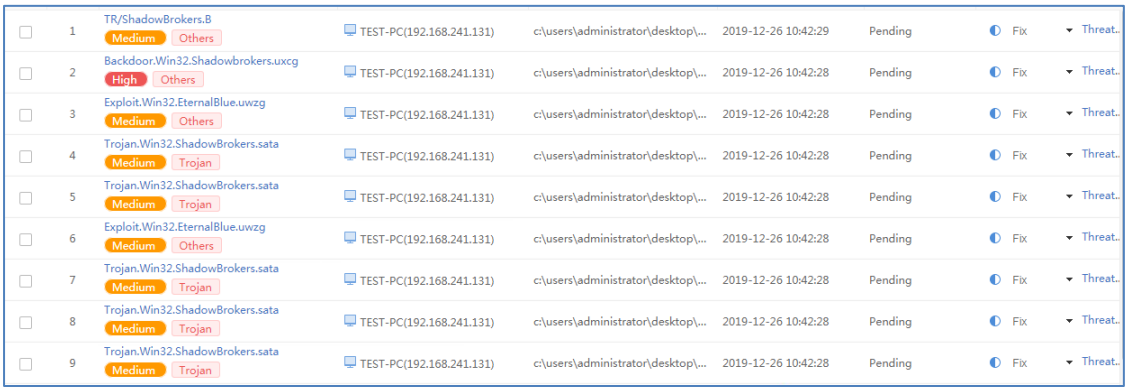
4. Skenario perbaikan makro virus itu rumit. Termasuk karena perbedaan perbaikan teknologi dari setiap pembuat, beberapa file masih dilaporkan oleh Endpoint Secure setelah diperbaiki oleh pembuatnya, tapi karena kode makro telah rusak, itu tidak dapat diperbaiki, jika terjadi situasi demikian, anda dapat mengabaikan atau mempercayai file tersebut, improvement produk akan dibuat untuk situasi ini.

Situasi Umum

Host memindai file yang mengancam dalam jumlah besar dan namanya biasanya sama (tipe virus), itu mungkin adalah virus yang menginfeksi atau makro virus, silahkan merujuk pada bagian ide pembuangan virus;

Contoh 1: File Virus yang Berelasi Eternal Blue

Jika ada 100 file dengan "EternalBlue" dan "ShadowBrokers", itu adalah eternal blue exploit kit, ini mengindikasikan bahwa host memiliki tambang trojan. Anda butuh mengalikasikan patch terkait dahulu, lalu periksa dan habiskan;



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..

Contoh 2: File server Melaporkan Virus dalam Jumlah Besar.

File Server memindai virus dalam jumlah besar:

其他病毒	ACAD/Bursted.AI	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.AI	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.AI	g:\share	
其他病毒	ACAD/Bursted.AI	g:\share	\613l_bd_081121\acad.lsp
其他病毒	ACAD/Bursted.AI	g:\share	cad.lsp
其他病毒	ACAD/Bursted.AI	g:\share	ad.lsp
其他病毒	ACAD/Bursted.AI	g:\share	
其他病毒	ACAD/Bursted.AI	g:\share	bd_081121\acad.lsp
其他病毒	ACAD/Bursted.AI	g:\share	
其他病毒	ACAD/Bursted.AI	g:\share	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	
其他病毒	ADSPY/ToolBar.C	g:\取消	
其他病毒	ADSPY/YASS.20480.C	g:\192.1	
其他病毒	ADSPY/YASS.20480.C	g:\share	欣件\stormcodec6.07.17.exe
其他病毒	ADSPY/YASS.20480.C	g:\share	欣件\stormcodec6.07.17.exe
其他病毒	Adware.Win32.IeSearchBa	g:\share	3-1\ttpsetup.exe
其他病毒	Adware.Win32.IeSearchBa	g:\share	欣件\ttpsetup.exe
其他病毒	Adware.Win32.IeSearchBa	g:\share	欣件\ttpsetup.exe
其他病毒	Adware.Win32.MulitiPlug	g:\share	i\client\win32\netapi32.dll
其他病毒	Adware.Win32.MulitiPlug	g:\share	i\client\win64\netapi32.dll
其他病毒	ADWARE/IeSearchBar.244	g:\192.1	al_cn.exe
其他病毒	ADWARE/Sogou.tclzk	g:\share	下载\youdaodict_setup.exe_sgdl.exe
其他病毒	ADWARE/Sogou.tclzk	g:\share	全浏览器下载\youdaodict_setup.exe_sgdl.exe
其他病毒	BAT/FormatC.ac	g:\share	客攻防指南.rar
其他病毒	BDS/Agent.aqns	g:\soft\o	:pe\pe_nvs\thunder.7z
其他病毒	BDS/Agent.aqns	g:\soft\o	\max_skype\mycd\axpe\pe_nvs\thunder.7z
其他病毒	BDS/Hupigon.foey.1	g:\share	力训练.exe
其他病毒	BDS/Hupigon.TVU	g:\share	\揭示股市深层的秘密.rar
其他病毒	BDS/Rogue.717326	g:\share	tia 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\	5.391\es4\easysysprep4.exe
其他病毒	Hacktool.Win32.FakeSys.(	g:\soft\o	oft windows 8 activator\microsoft windows 8 activator(all edition).exe
其他病毒	Hacktool.Win32.Keygen.m	g:\商务	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.Keygen.M	g:\share	软件\autocad_2014_chinese_win_64bit\autocad_2014_chinese_win_64bit\cad201
其他病毒	Hacktool.Win32.Keygen.m	g:\share	oshop cs2\序列号和激活补丁.exe
其他病毒	Hacktool.Win32.KMSAuto	g:\soft\o	oem7f7\oem7f7.exe

Pertama buang nama kolom virus dan duplikasikan. Lalu anda dapat melihat beberapa tipe dilingkaran seperti figur dibawah. Mereka adalah aplikasi iklan, penginstall, dan peralatan hack. Jika itu adalah file yang tdak berguna, direkomendasikan untuk diisolasi. Jika itu program maka dapat dibiarkan atau dipercaya;

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		

Seperti terlihat pada contoh dibawah, ACAD dapat ditemukan pada formulir laporan informasi virus. Itu adalah CAD virus. Biasanya itu tidak salah dilaporkan dan dapat dibuang langsung. W97M dan X2000M dibuang sesuai ide membuang makro virus.: