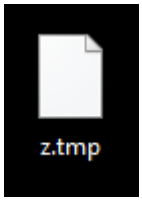
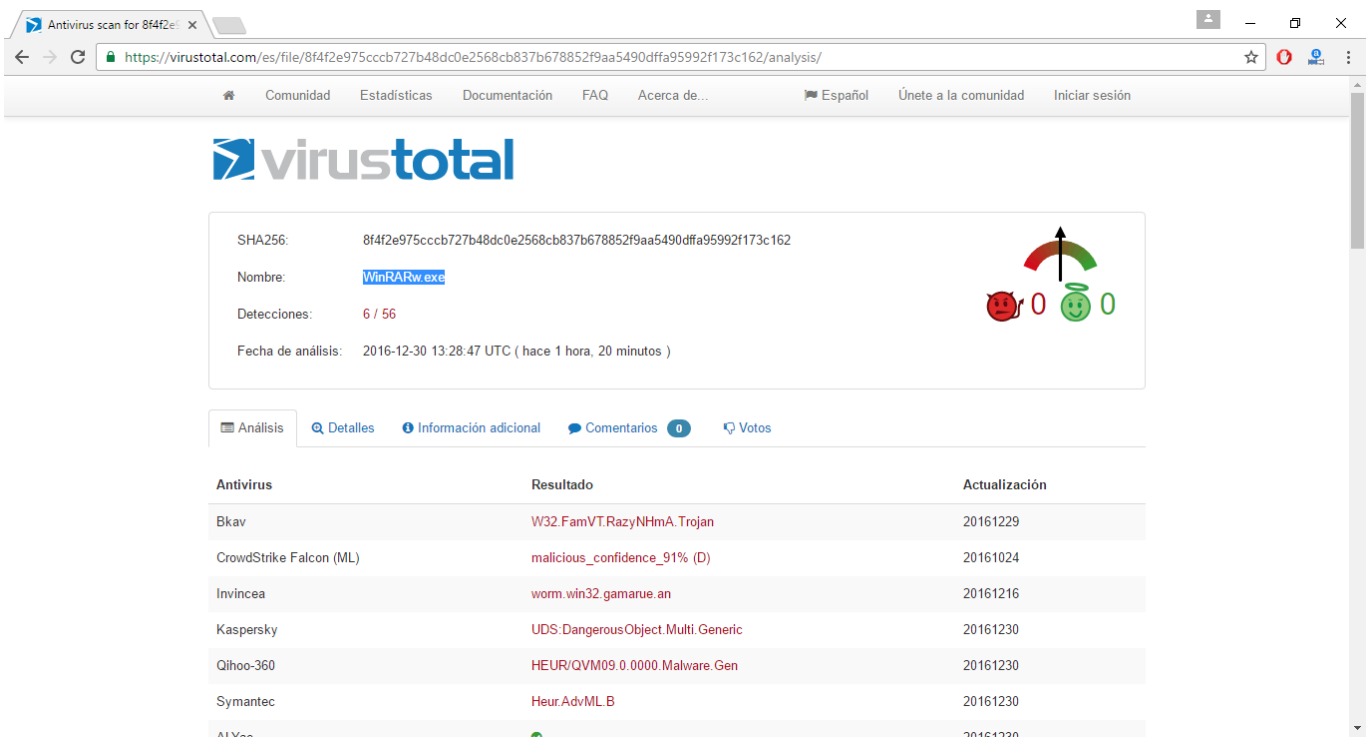
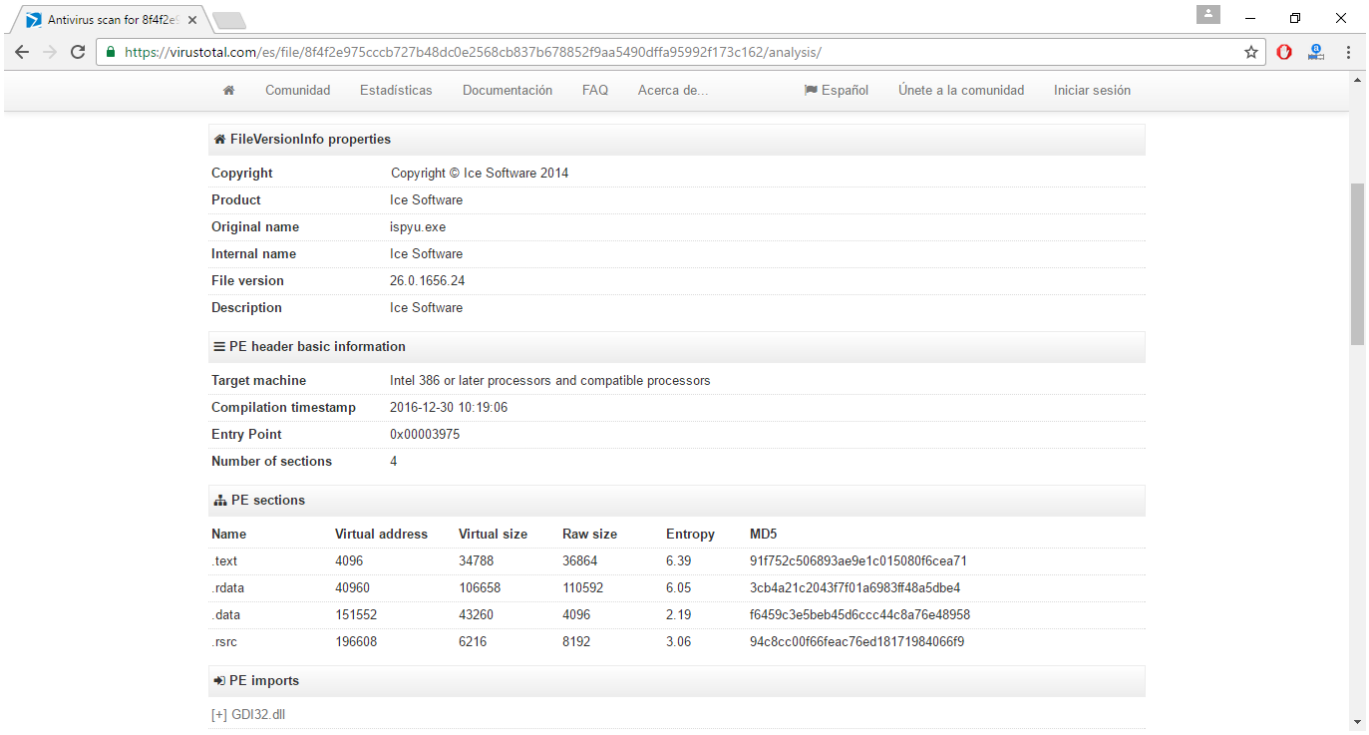
Virus WinRARw.exe – ispyu.exe – Ice Software



Antivirus	Resultado	Actualización
Bkav	W32.FamVT.RazyNHmA.Trojan	20161229
CrowdStrike Falcon (ML)	malicious_confidence_91% (D)	20161024
Invincea	worm.win32.gamarue.an	20161216
Kaspersky	UDS:DangerousObject.Multi.Generic	20161230
Qihoo-360	HEUR/QVM09.0.0000.Malware.Gen	20161230
Symantec	Heur.AdvML.B	20161230





FileVersionInfo properties

Copyright	Copyright © Ice Software 2014
Product	Ice Software
Original name	ispyu.exe
Internal name	Ice Software
File version	26.0.1656.24
Description	Ice Software

PE header basic information

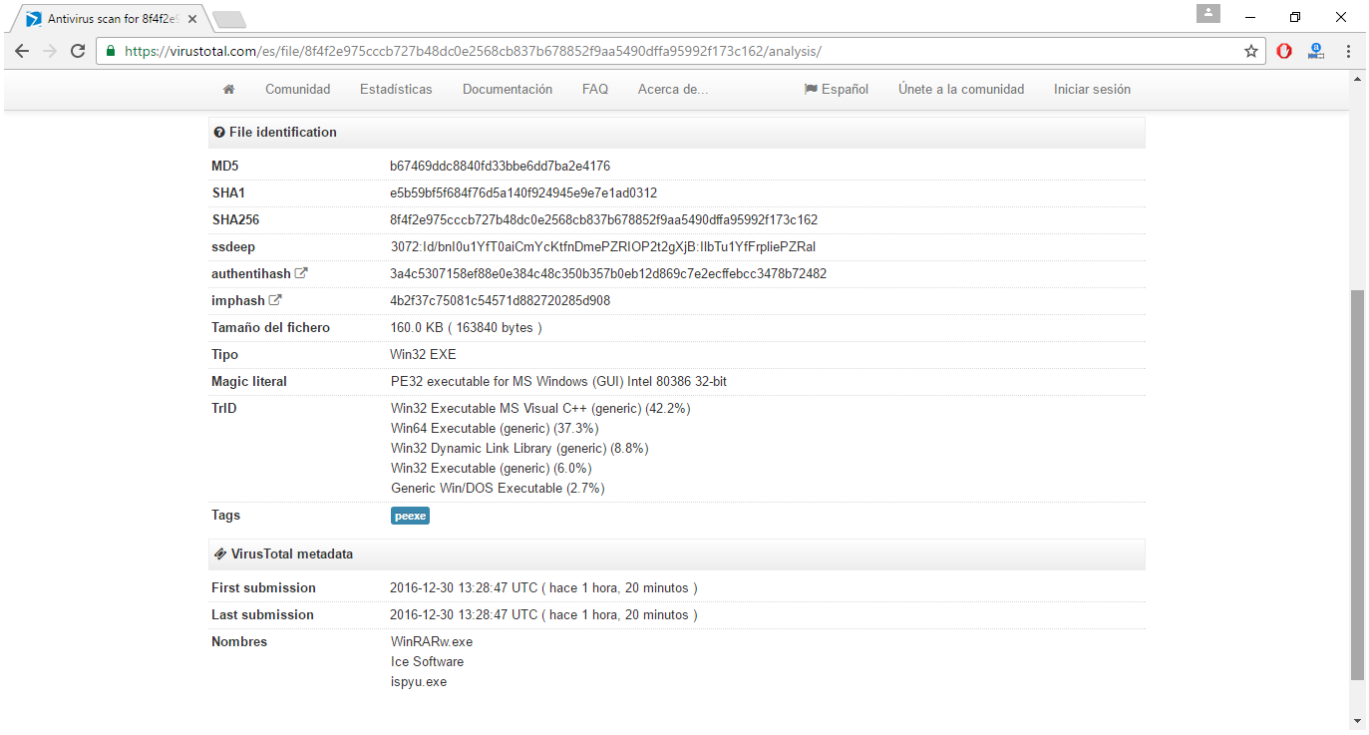
Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2016-12-30 10:19:06
Entry Point	0x00003975
Number of sections	4

PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	34788	36864	6.39	91f752c506893ae9e1c015080f6cea71
.rdata	40960	106658	110592	6.05	3cb4a21c2043f7f01a6983ff48a5dbe4
.data	151552	43260	4096	2.19	f6459c3e5beb45d6ccc44c8a76e48958
.rsrc	196608	6216	8192	3.06	94c8cc00f66feac76ed18171984066f9

PE imports

[+] GDI32.dll



File identification

MD5	b67469ddc8840fd33bbe6dd7ba2e4176
SHA1	e5b59bf5f684f76d5a140f924945e9e7e1ad0312
SHA256	8f4f2e975cccb727b48dc0e2568cb837b678852f9aa5490dffa95992f173c162
ssdeep	3072:ld/bnl0u1YfT0aiCmYcKtfnDmePZRIOP2t2gXjB:IlbTu1YfFrplePZRal
authentihash	3a4c5307158ef88e0e384c48c350b357b0eb12d869c7e2ecffebcc3478b72482
imphash	4b2f37c75081c54571d882720285d908
Tamaño del fichero	160.0 KB (163840 bytes)
Tipo	Win32 EXE
Magic literal	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (42.2%) Win64 Executable (generic) (37.3%) Win32 Dynamic Link Library (generic) (8.8%) Win32 Executable (generic) (6.0%) Generic Win/DOS Executable (2.7%)
Tags	peexe

VirusTotal metadata

First submission	2016-12-30 13:28:47 UTC (hace 1 hora, 20 minutos)
Last submission	2016-12-30 13:28:47 UTC (hace 1 hora, 20 minutos)
Nombres	WinRARw.exe Ice Software ispyu.exe