Files Framework

Motivation

- In 2.1 and prior, "file" handling...
  - is inconsistent
  - causes performance problems
  - is not extensible
  - not cool

Talking about file handling

- Charles Smutz and his Ruminate-IDS project
  - File reassembly
  - Passing files to other tools and parsers

Realizations

- A "file" is a single flow byte stream
  - *Hint: a connection is bidirectional so it's a dual flow bytestream*
  - Bro can have file analyzers that work incrementally like our protocol analyzers
  - How many file types would you like to be able to parse?

Realizations (cont'd.)

- A "file" is another base abstraction in Bro
  - `files.log` and `conn.log` have a lot of similarities
- Files have unique IDs just like connections

Files are source agnostic

- Files out of files
- Files out of any unencrypted file protocol
- Input framework

Implementation

- Keep file data out of script land
- No reassembly yet, but design decisions were made to support it in a future release
- File manager is a completely new internal component of Bro that accepts file data from anywhere it can be acquired

Forensic Logging - `conn.log`

ts	1232039481.41058
uid	**wd5Gv4mDKY**
id	10.0.0.245 1066 78.109.18.210 80
proto	tcp
service	http
duration	1.492474
orig_bytes	66
resp_bytes	49337
conn_state	RSTO
missed_bytes	0
history	ShADadfR

Forensic Logging - `http.log`

ts	1232039481.56861
uid	**wd5Gv4mDKY**
id	10.0.0.245 1066 78.109.18.210 80
trans_depth	1
method	GET
host	78.109.18.210
uri	/lprx.php
referrer	-
user_agent	-
request_body_len	0
response_body_len	49152
resp_fuids	**hVkwqId1J1h**
resp_mime_types	application/x-dosexec

Forensic Logging - `files.log`

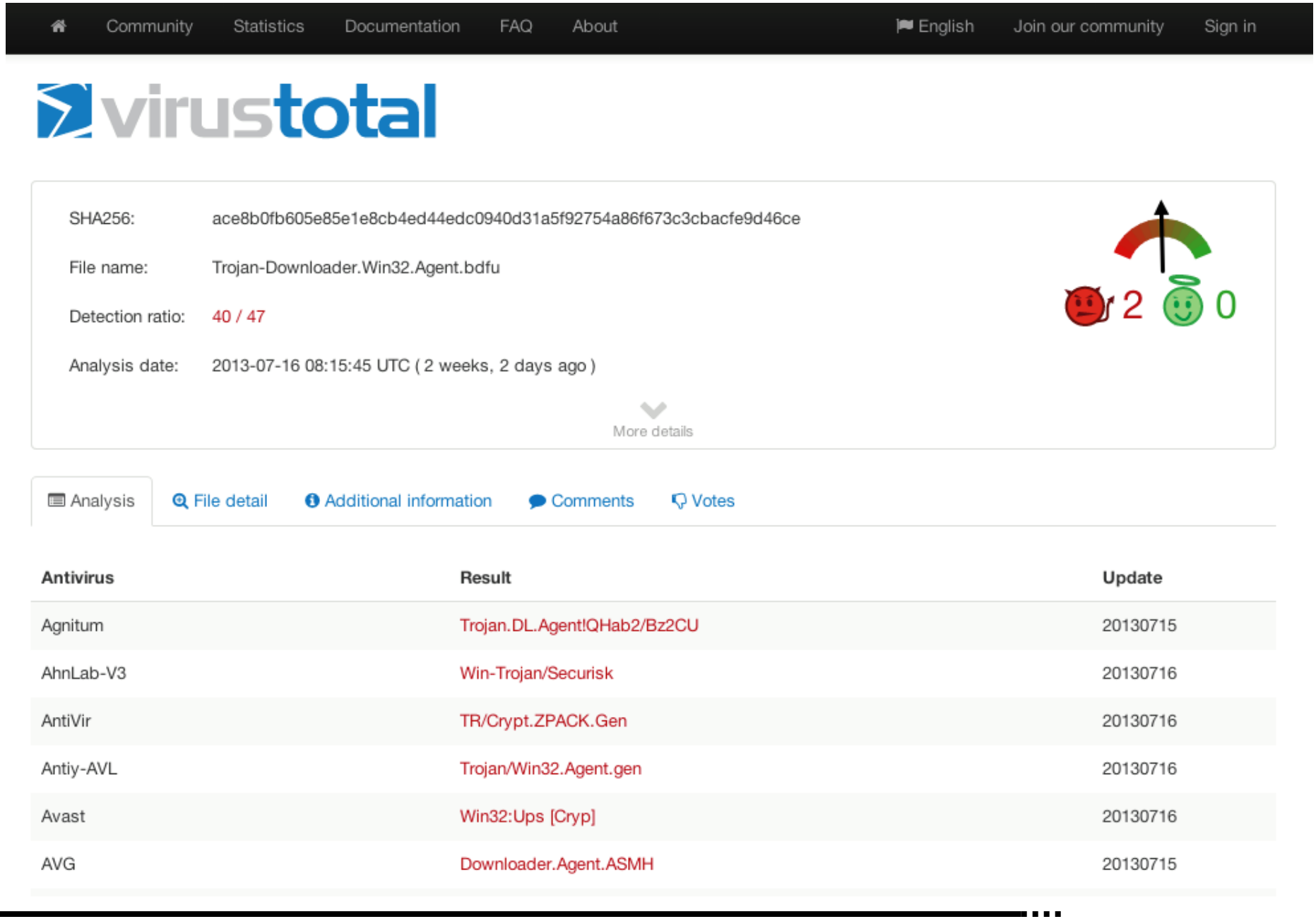
ts	1232039481.72727
fuid	**hVkwqId1J1h**
tx_hosts	78.109.18.210
rx_hosts	10.0.0.245
conn_uids	**wd5Gv4mDKY**
source	HTTP
depth	0
analyzers	SHA1, MD5, PE
mime_type	application/x-dosexec
duration	1.151308
is_orig	F
seen_bytes	49152
total_bytes	49152
md5	1d016184387937e2f81da268dace5758
sha1	9fba10c34168496486cd4205cb7c9cda41abf8b9
extracted	-

Forensic Logging - `pe.log`

ts	1232039481.72727
fuid	**hVkwqId1J1h**
machine	I386
compile_ts	1200557518
os	Windows NT 4.0
subsystem	WINDOWS_GUI
characteristics	32BIT_MACHINE,RELOCS_STRIPPED,EXECUTABLE_IMAGE,LOCAL_SYMS_STRIPPED,LINE_NUMS_STRIPPED
section_names	.text,.data,.rdata,.INIT,.edata

Forensic Logging - `notice.log`

ts	1232039482.87858
uid	**wd5Gv4mDKY**
id	10.0.0.245 1066 78.109.18.210 80
fuid	**hVkwqId1J1h**
file_mime_type	application/x-dosexec
file_desc	http://78.109.18.210/lprx.php
note	TeamCymruMalwareHashRegistry::Match
msg	Malware Hash Registry Detection rate: 11% Last seen: 2009-01-12 14:01:04
sub	https://www.virustotal.com/en/file/9fba10c34168496486cd4205cb7c9cda41abf8b9/analysis/


Community
Statistics
Documentation
FAQ
About
English
Join our community
Sign in
virustotal
SHA256: ace8b0fb605e85e1e8cb4ed44edc0940d31a5f92754a86f673c3cbacfe9d46ce
File name: Trojan-Downloader.Win32.Agent.bdfu
Detection ratio: 40 / 47
Analysis date: 2013-07-16 08:15:45 UTC (2 weeks, 2 days ago)
2
0
More details
Analysis
File detail
Additional information
Comments
Votes
Antivirus
Result
Update
Agnitum
Trojan.DL.Agent!QHab2/Bz2CU
20130715
AhnLab-V3
Win-Trojan/Securisk
20130716
AntiVir
TR/Crypt.ZPACK.Gen
20130716
Antiy-AVL
Trojan/Win32.Agent.gen
20130716
Avast
Win32:Ups [Cryp]
20130716
AVG
Downloader.Agent.ASMH
20130715

Included File analyzers

- Extraction
- Hashing
  - MD5, SHA-1, SHA-256
- Entropy - Not in preview release
- Data
  - Make file data available in scriptland
- PE - Windows executables, still in development

Exercises