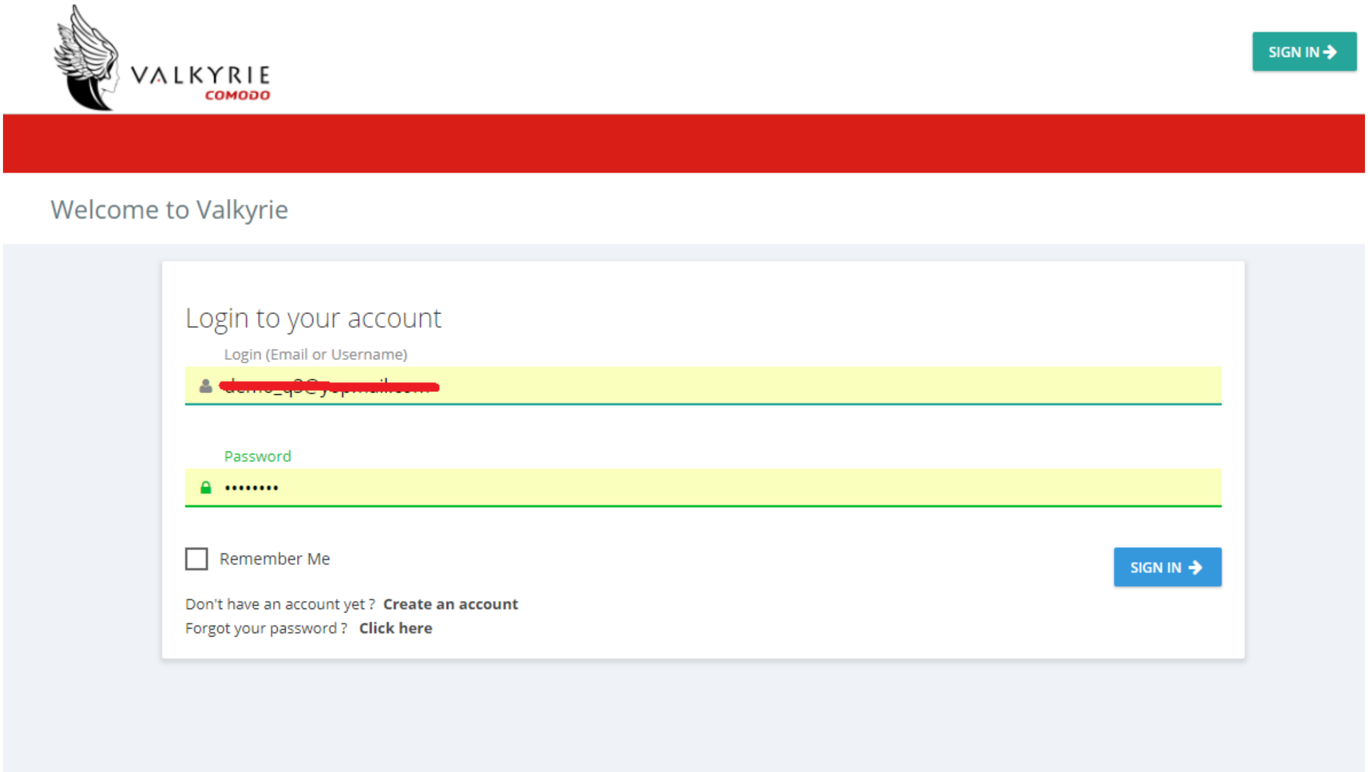
How to upload and analyze files in Valkyrie

Valkyrie is an online file verdict system that investigates unknown files to identify whether the files you have uploaded are malicious or not.

The Valkyrie console allows users to upload new files for analysis and to view scan results, virus total result and also you can download the virus report too.It can identify the file as four different types of clean, malware, no threat found, PUA.

By using this system you can also download the kill chain report and we can also send the unknown file for Human Expert Analysis.

STEP[1]: GO TO https://verdict.xcitium.com/login.Login with credentials.



Welcome to Valkyrie

Login to your account

Login (Email or Username)

[redacted]

Password

••••••••

□ Remember Me

Don't have an account yet ? **Create an account**

Forgot your password ? **Click here**

STEP[2] At the bottom right side as shown in below screenshot click upload button to upload file or URL or sha1; select the appropriate file and click on "Analyze".

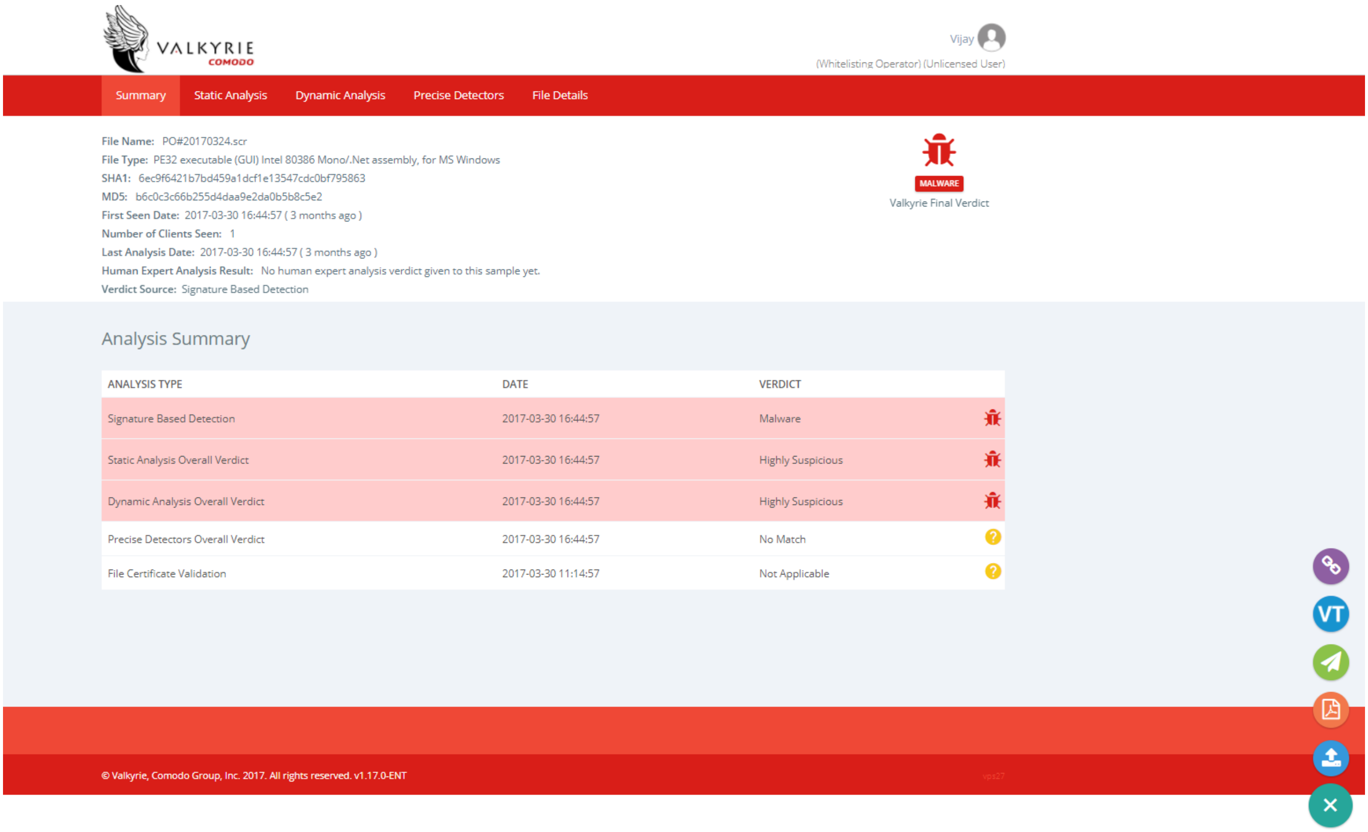
[NOTE:] **You can upload files size up to 150 MB.**

Step[3]: First it will analyze the file and then give the result of any of these stages, Initially there are four stages(Malware, Pua, Clean, Nothreatfound), If you upload any file.

For Example Malware File

1. If you uploaded any file then it gives the result as malware. with following tabs(Summary, Static Analysis, Dynamic Analysis, Precise Detectors, File Details) consists information about file result.

Summary:



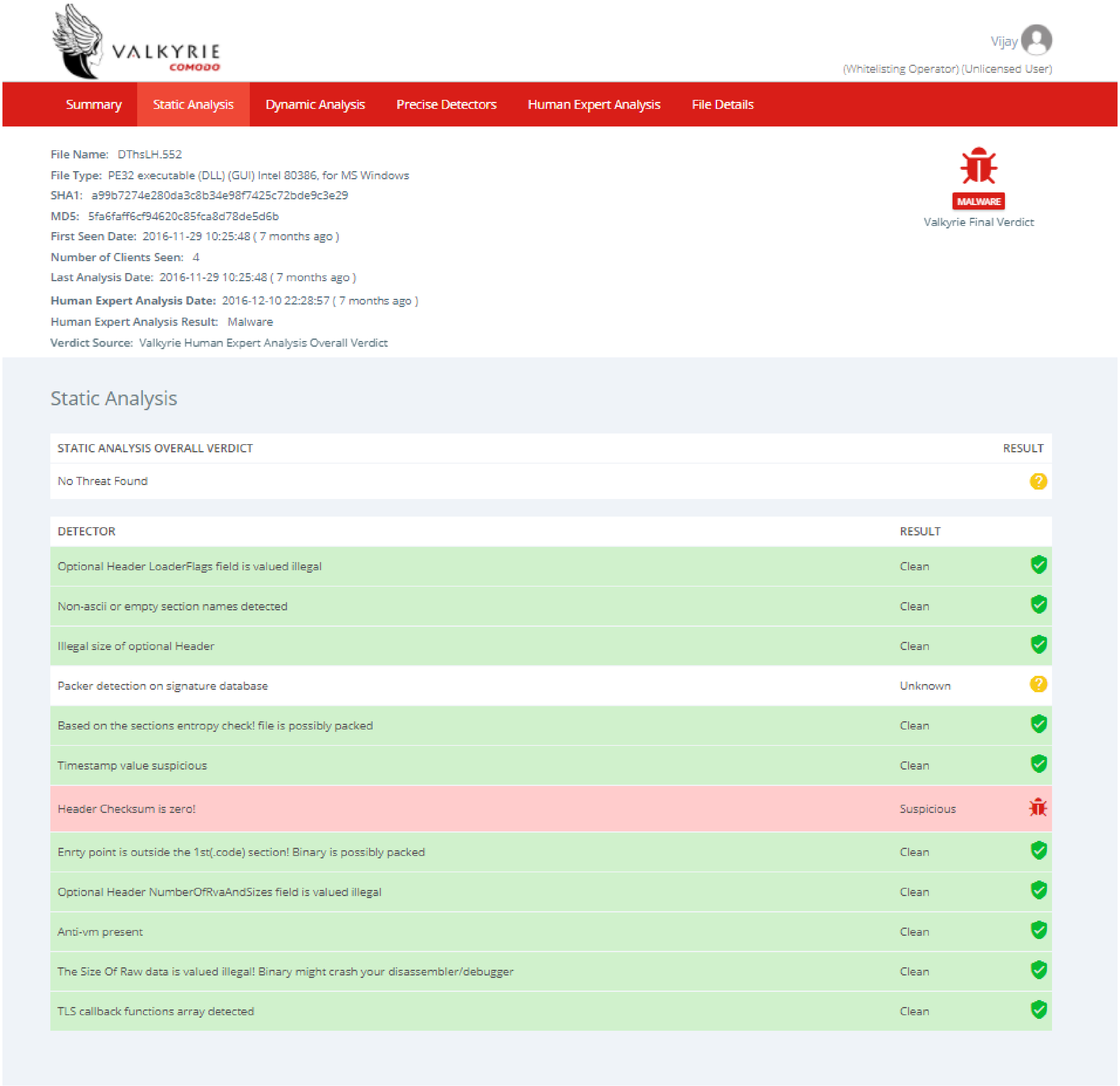
File Name: PO#20170324.scr
File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1: 6ec9f6421b7bd459a1dcf1e13547cdc0bf795863
MD5: b6c0c3c66b255d4daa9e2da0b5b8c5e2
First Seen Date: 2017-03-30 16:44:57 (3 months ago)
Number of Clients Seen: 1
Last Analysis Date: 2017-03-30 16:44:57 (3 months ago)
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2017-03-30 16:44:57	Malware
Static Analysis Overall Verdict	2017-03-30 16:44:57	Highly Suspicious
Dynamic Analysis Overall Verdict	2017-03-30 16:44:57	Highly Suspicious
Precise Detectors Overall Verdict	2017-03-30 16:44:57	No Match
File Certificate Validation	2017-03-30 11:14:57	Not Applicable

© Valkyrie, Comodo Group, Inc. 2017. All rights reserved. v1.17.0-ENT

Static Analysis:



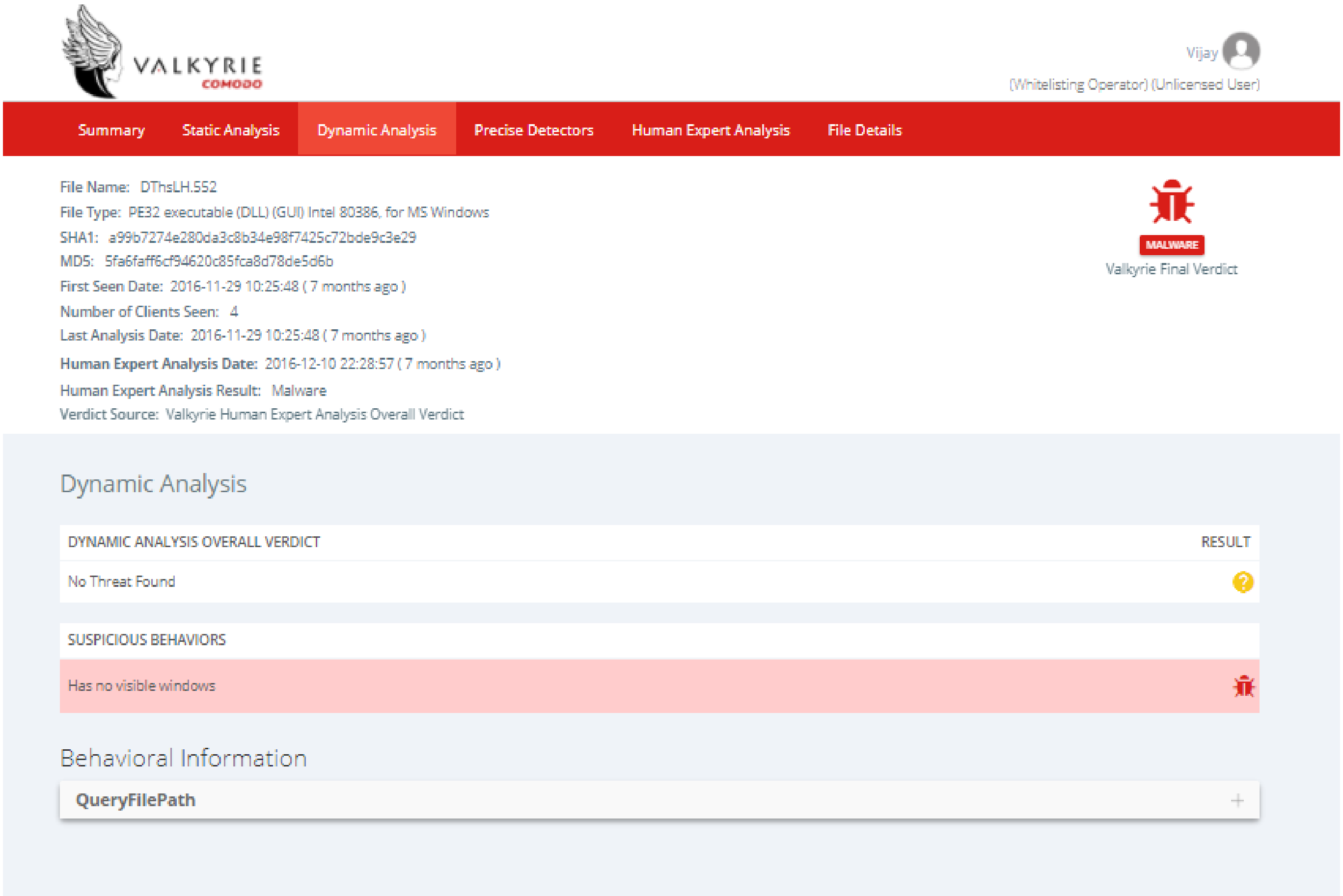
File Name: DThsLH.552
File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
SHA1: a99b7274e280da3c8b34e98f7425c72bde9c3e29
MD5: 5fa6faff6cf94620c85fca8d78de5d6b
First Seen Date: 2016-11-29 10:25:48 (7 months ago)
Number of Clients Seen: 4
Last Analysis Date: 2016-11-29 10:25:48 (7 months ago)
Human Expert Analysis Date: 2016-12-10 22:28:57 (7 months ago)
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	?

DETECTOR	RESULT	
Optional Header LoaderFlags field is valued illegal	Clean	✓
Non-ascii or empty section names detected	Clean	✓
Illegal size of optional Header	Clean	✓
Packer detection on signature database	Unknown	?
Based on the sections entropy check! file is possibly packed	Clean	✓
Timestamp value suspicious	Clean	✓
Header Checksum is zero!	Suspicious	🐞
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean	✓
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean	✓
Anti-vm present	Clean	✓
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean	✓
TLS callback functions array detected	Clean	✓

Dynamic Analysis:



File Name: DThsLH.552
File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
SHA1: a99b7274e280da3c8b34e98f7425c72bde9c3e29
MD5: 5fa6faff6cf94620c85fca8d78de5d6b
First Seen Date: 2016-11-29 10:25:48 (7 months ago)
Number of Clients Seen: 4
Last Analysis Date: 2016-11-29 10:25:48 (7 months ago)
Human Expert Analysis Date: 2016-12-10 22:28:57 (7 months ago)
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	?

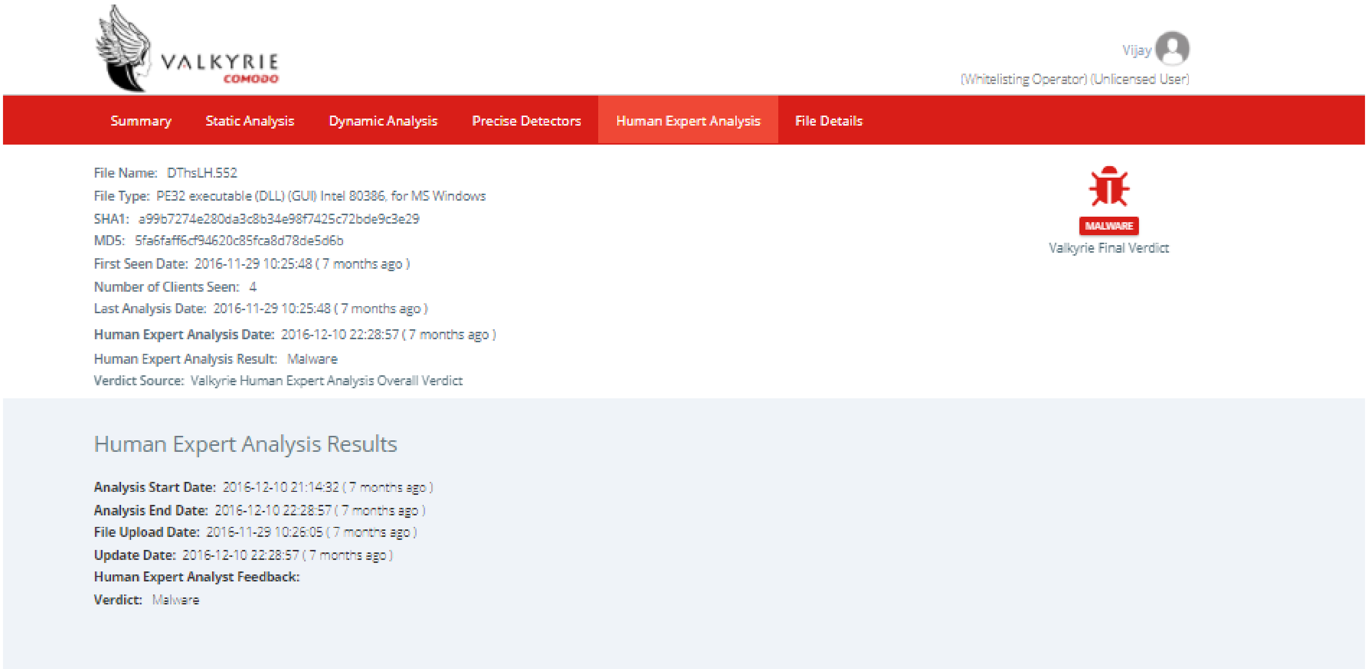
SUSPICIOUS BEHAVIORS
Has no visible windows

Behavioral Information

QueryFilePath +

Precise Detectors:

Human Expert Analysis:

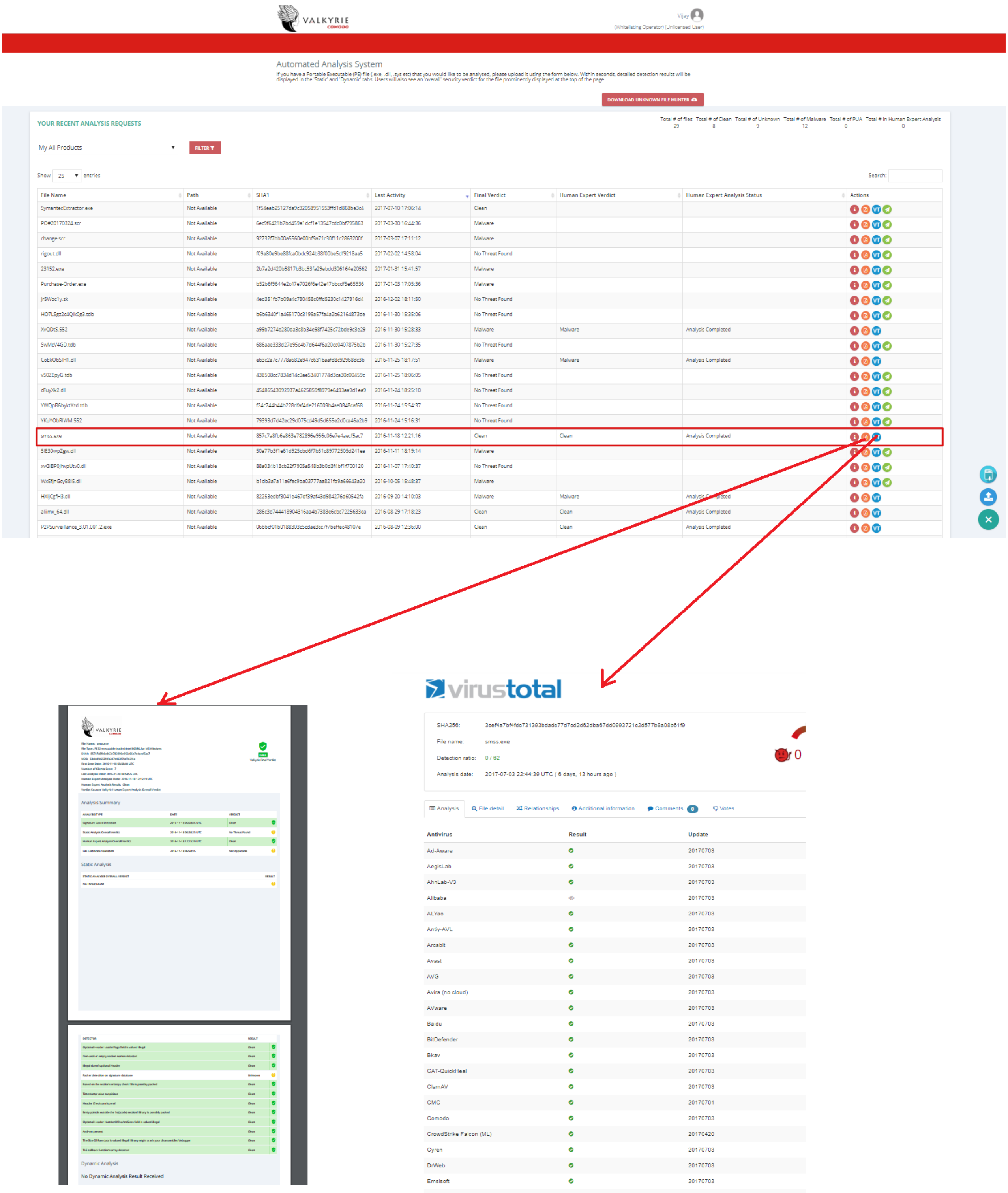


File Name: DThsLH.552
File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
SHA1: a99b7274e280da3c8b34e98f7425c72bde9c3e29
MD5: 5fa6faff6cf94620c85fca8d78de5d6b
First Seen Date: 2016-11-29 10:25:48 (7 months ago)
Number of Clients Seen: 4
Last Analysis Date: 2016-11-29 10:25:48 (7 months ago)
Human Expert Analysis Date: 2016-12-10 22:28:57 (7 months ago)
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Human Expert Analysis Results

Analysis Start Date: 2016-12-10 21:14:32 (7 months ago)
Analysis End Date: 2016-12-10 22:28:57 (7 months ago)
File Upload Date: 2016-11-29 10:26:05 (7 months ago)
Update Date: 2016-12-10 22:28:57 (7 months ago)
Human Expert Analyst Feedback:
Verdict: Malware

File Details:



VALKYRIE
COMODO
Vijay
(Whitelisting Operator) (Unlicensed User)

Automated Analysis System

If you have a Portable Executable (PE) file (.exe, .dll, .sys etc) that you would like to be analysed, please upload it using the form below. Within seconds, detailed detection results will be displayed in the 'Static' and 'Dynamic' tabs. Users will also see an 'overall' security verdict for the file prominently displayed at the top of the page.

DOWNLOAD UNKNOWN FILE HUNTER

YOUR RECENT ANALYSIS REQUESTS

Total # of files	Total # of Clean	Total # of Unknown	Total # of Malware	Total # of PUA	Total # In Human Expert Analysis
29	8	9	12	0	0

File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict	Human Expert Analysis Status	Actions
SymantecExtractor.exe	Not Available	1f54eab25127da9c32058951553ffd1d868be3c4	2017-07-10 17:06:14	Clean			● ● VT ●
PO#20170324.scr	Not Available	6ec9f6421b7bd459a1dcf1e13547cdc0bf795863	2017-03-30 16:44:36	Malware			● ● VT ●
change.scr	Not Available	92732f7bb00a5560e00bf9a71c30f11c2863200f	2017-03-07 17:11:12	Malware			● ● VT ●
rigout.dll	Not Available	f09a80e9be88fca0bdc924b38f00be5df9218aa5	2017-02-02 14:58:04	No Threat Found			● ● VT ●
23152.exe	Not Available	2b7a2d420b5817b3bc93fa29ebdd306164e20562	2017-01-31 15:41:57	Malware			● ● VT ●
Purchase-Order.exe	Not Available	b52b6f9644e2c47e7026f6e42e47bbcdf5e65936	2017-01-03 17:05:36	Malware			● ● VT ●
Jr5Woc1y.zk	Not Available	4ed351fb7b09a4c790458c0ffd5230c1427916d4	2016-12-02 18:11:50	No Threat Found			● ● VT ●
HO7LSgz2c4QIk0g3.tdb	Not Available	b6b6340f1a465170c3199a57fa4a2b62164873de	2016-11-30 15:35:06	No Threat Found			● ● VT ●
XvQDtS.552	Not Available	a99b7274e280da3c8b34e98f7425c72bde9c3e29	2016-11-30 15:28:33	Malware	Malware	Analysis Completed	● ● VT
SwMcV4GD.tdb	Not Available	686aae333d27e95c4b7d644f6a20cc0407875b2b	2016-11-30 15:27:35	No Threat Found			● ● VT ●
CoEkQbSIH1.dll	Not Available	eb3c2a7c7778a682e947c631baafd8c92968dc3b	2016-11-25 18:17:51	Malware	Malware	Analysis Completed	● ● VT
v50ZEpyG.tdb	Not Available	438508cc7834d14c0ae53401774d3ca30c00459c	2016-11-25 18:06:05	No Threat Found			● ● VT ●
cFuyXk2.dll	Not Available	45486543092937a4625859f8979e6493aa9d1ea9	2016-11-24 18:25:10	No Threat Found			● ● VT ●
YWQpB6byktXzd.tdb	Not Available	f24c744b44b228dfaf4de216009b4ae0848caf68	2016-11-24 15:54:37	No Threat Found			● ● VT ●
YKuYObRIWM.552	Not Available	79393d7d42ec29d075cd49d5d655e2d0ca46a2b9	2016-11-24 15:16:31	No Threat Found			● ● VT ●
smss.exe	Not Available	857c7a8fb6e863e782896e956c06e7e4aecf5ac7	2016-11-18 12:21:16	Clean	Clean	Analysis Completed	● ● VT
5IE30wpZgw.dll	Not Available	50a77b3f1e61d925cbd6f7b51c89772505d241ea	2016-11-11 18:19:14	Malware			● ● VT ●
xvGIBP0JhvpUtv0.dll	Not Available	88a034b13cb22f7905a548b3b0d3f4bf1f700120	2016-11-07 17:40:37	No Threat Found			● ● VT ●
WxEfjnGcyB8I5.dll	Not Available	b1db3a7a11a6fec9ba03777aa821fb9a66643a20	2016-10-05 15:48:37	Malware			● ● VT ●
HXIjCgfH3.dll	Not Available	82253edbf3041e467df39af43d984276d60542fa	2016-09-20 14:10:03	Malware	Malware	Analysis Completed	● ● VT
aliimx_64.dll	Not Available	286c3d744418904316aa4b7383e6cbc7225633ea	2016-08-29 17:18:23	Clean	Clean	Analysis Completed	● ● VT
P2PSurveillance_3.01.001.2.exe	Not Available	06bbcf01b0188303c5cdae3cc7f7beffec48107e	2016-08-09 12:36:00	Clean	Clean	Analysis Completed	● ● VT

File Name: smss.exe
File Type: PE32 executable (native) Intel 80386, for MS Windows
SHA1: 857c7a8fb6e863e782896e956c06e7e4aecf5ac7
MD5: 53dddfb653f4fa2d7e463f7faf7e2f4a
First Seen Date: 2016-11-18 05:58:04 UTC
Number of Clients Seen: 7
Last Analysis Date: 2016-11-18 06:58:25 UTC
Human Expert Analysis Date: 2016-11-18 12:15:19 UTC
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2016-11-18 06:58:25 UTC	Clean	✓
Static Analysis Overall Verdict	2016-11-18 06:58:25 UTC	No Threat Found	?
Human Expert Analysis Overall Verdict	2016-11-18 12:15:19 UTC	Clean	✓
File Certificate Validation	2016-11-18 06:58:25	Not Applicable	?

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	?

DETECTOR	RESULT	
Optional Header LoaderFlags field is valued illegal	Clean	✓
Non-ascii or empty section names detected	Clean	✓
Illegal size of optional Header	Clean	✓
Packer detection on signature database	Unknown	?
Based on the sections entropy check! file is possibly packed	Clean	✓
Timestamp value suspicious	Clean	✓
Header Checksum is zero!	Clean	✓
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean	✓
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean	✓
Anti-vm present	Clean	✓
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean	✓
TLS callback functions array detected	Clean	✓

Dynamic Analysis

No Dynamic Analysis Result Received

SHA256: 3cef4a7bf4fdc731393bdadc77d7cd2d62dba67dd0993721c2d577b8a08b61f9
File name: smss.exe
Detection ratio: 0 / 62
Analysis date: 2017-07-03 22:44:39 UTC (6 days, 13 hours ago)

Antivirus	Result	Update
Ad-Aware	✓	20170703
AegisLab	✓	20170703
AhnLab-V3	✓	20170703
Alibaba		20170703
ALYac	✓	20170703
Antiy-AVL	✓	20170703
Arcabit	✓	20170703
Avast	✓	20170703
AVG	✓	20170703
Avira (no cloud)	✓	20170703
AVware	✓	20170703
Baidu	✓	20170703
BitDefender	✓	20170703
Bkav	✓	20170703
CAT-QuickHeal	✓	20170703
ClamAV	✓	20170703
CMC	✓	20170701
Comodo	✓	20170703
CrowdStrike Falcon (ML)	✓	20170420
Cyren	✓	20170703
DrWeb	✓	20170703
Emsisoft	✓	20170703