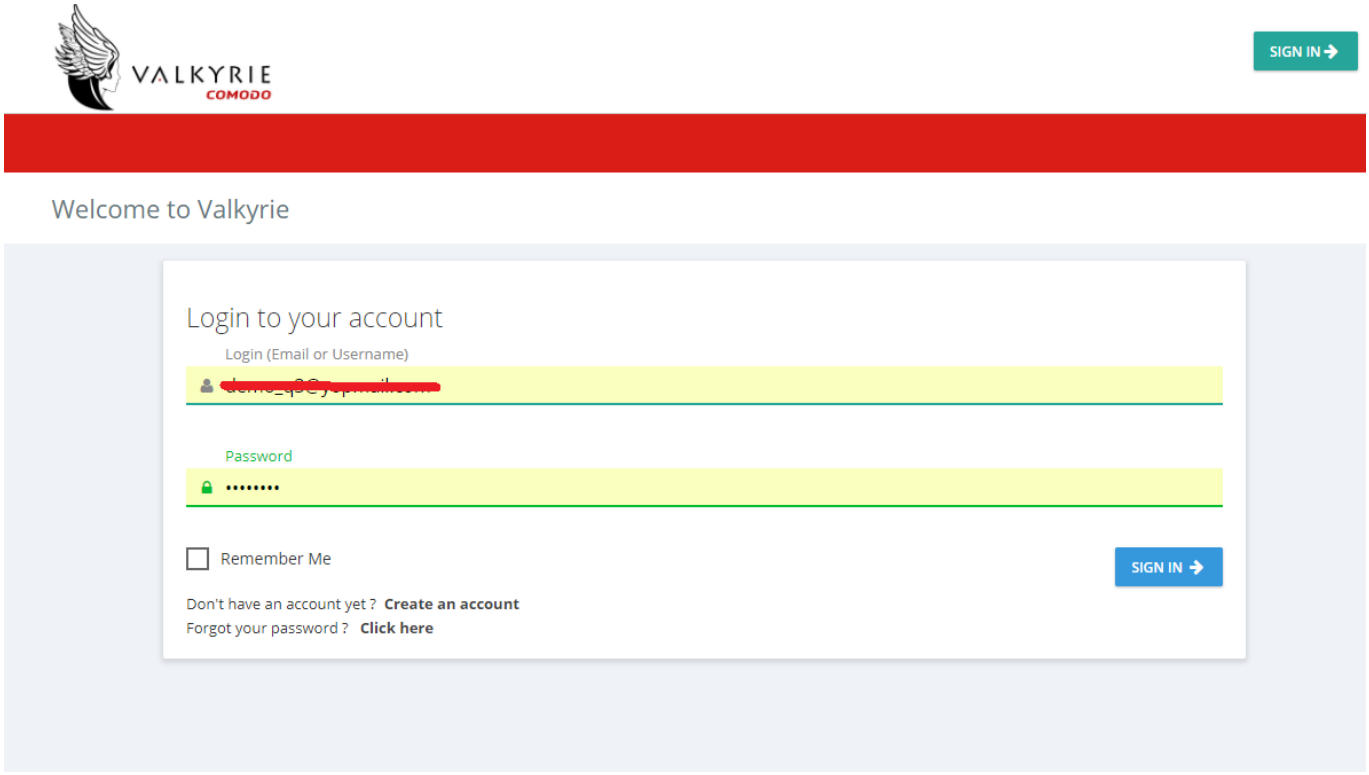
How to upload and analyze files in Valkyrie

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.



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".

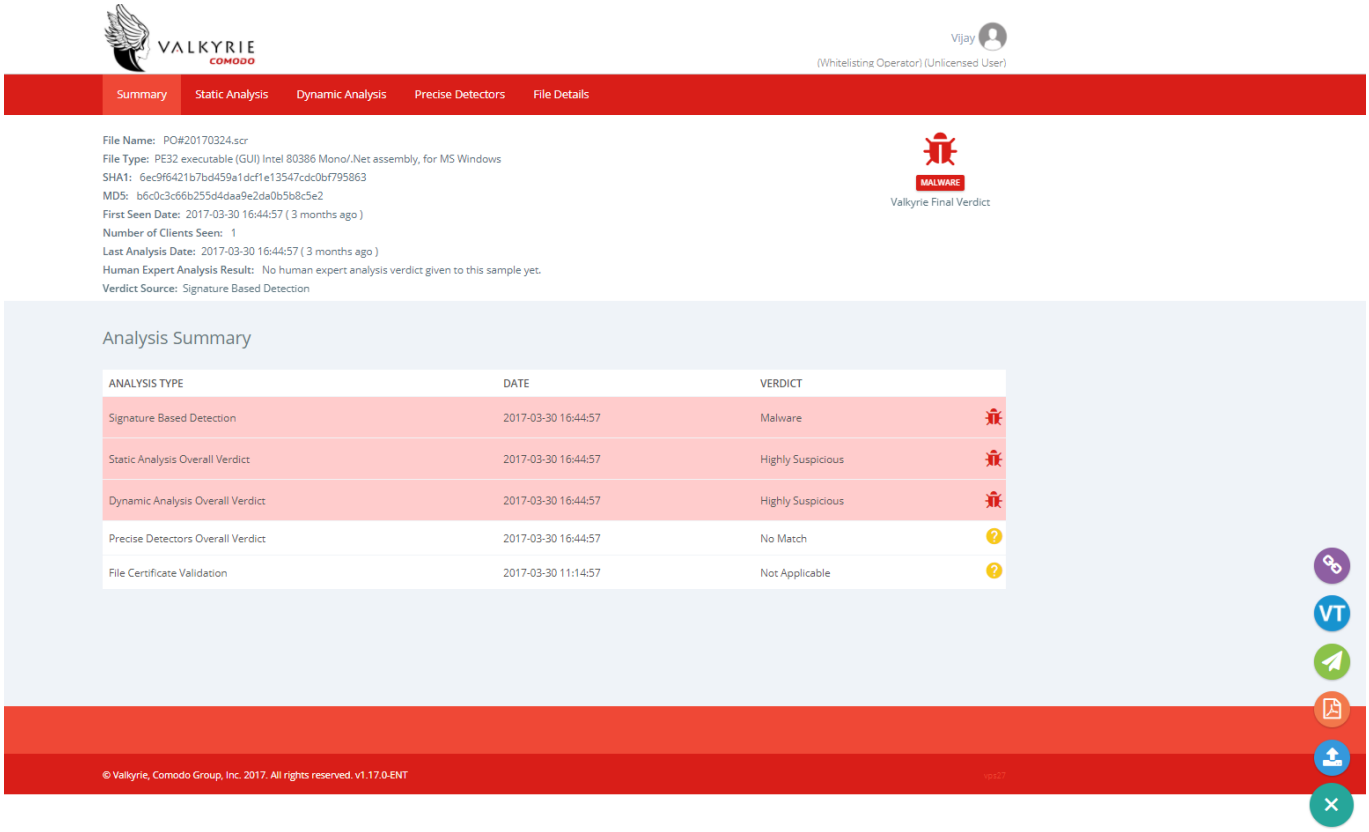
[NOTE:] **You can upload files size up to 150 MB.**

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:



Static Analysis:

VALKYRIE COMODO

Vijay
(Whitelisting Operator) (Unlicensed User)

Summary | Static Analysis | Dynamic Analysis | Precise Detectors | Human Expert Analysis | File Details

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

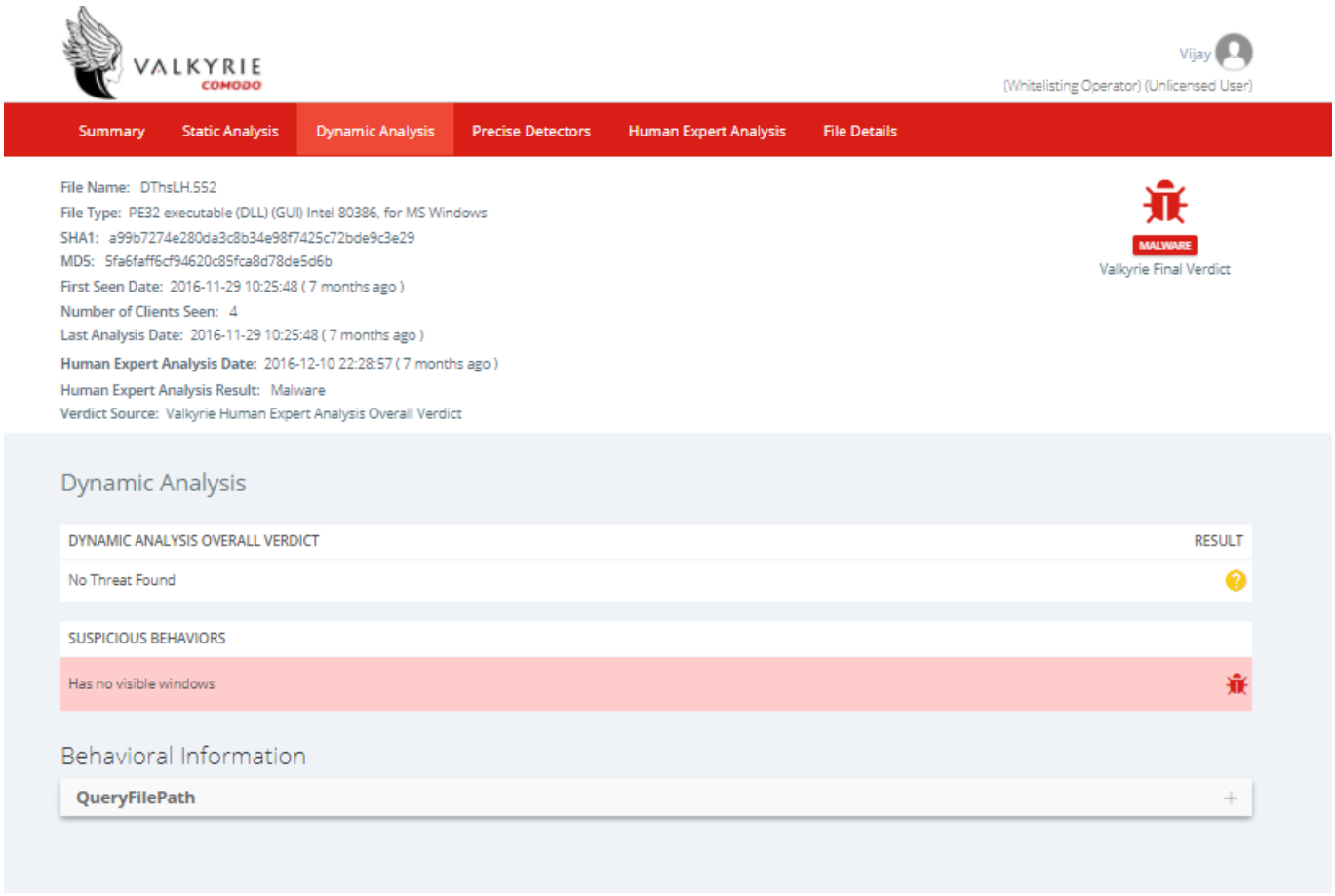
MALWARE
Valkyrie Final Verdict

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

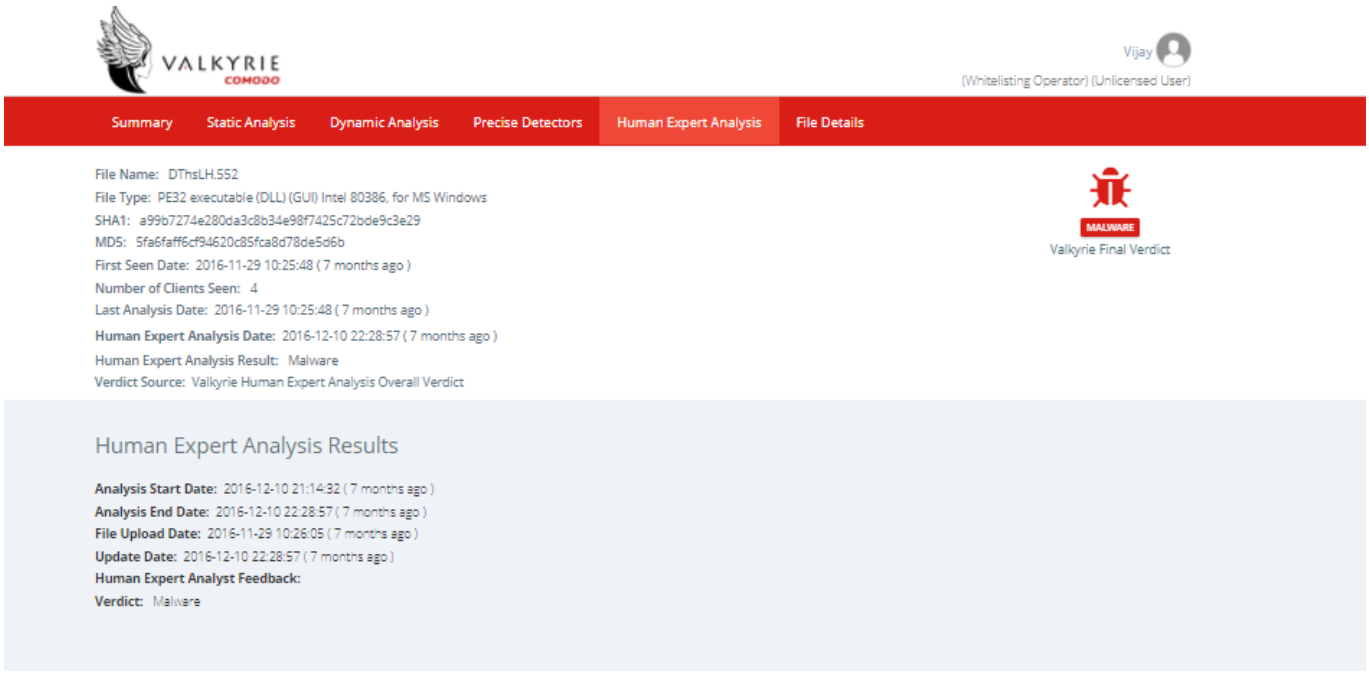
DETECTOR	RESULT
Optional Header LoaderFlags field is valued illegal	Clean
Non-ascii or empty section names detected	Clean
Illegal size of optional Header	Clean
Packer detection on signature database	Unknown
Based on the sections entropy check! file is possibly packed	Clean
Timestamp value suspicious	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:

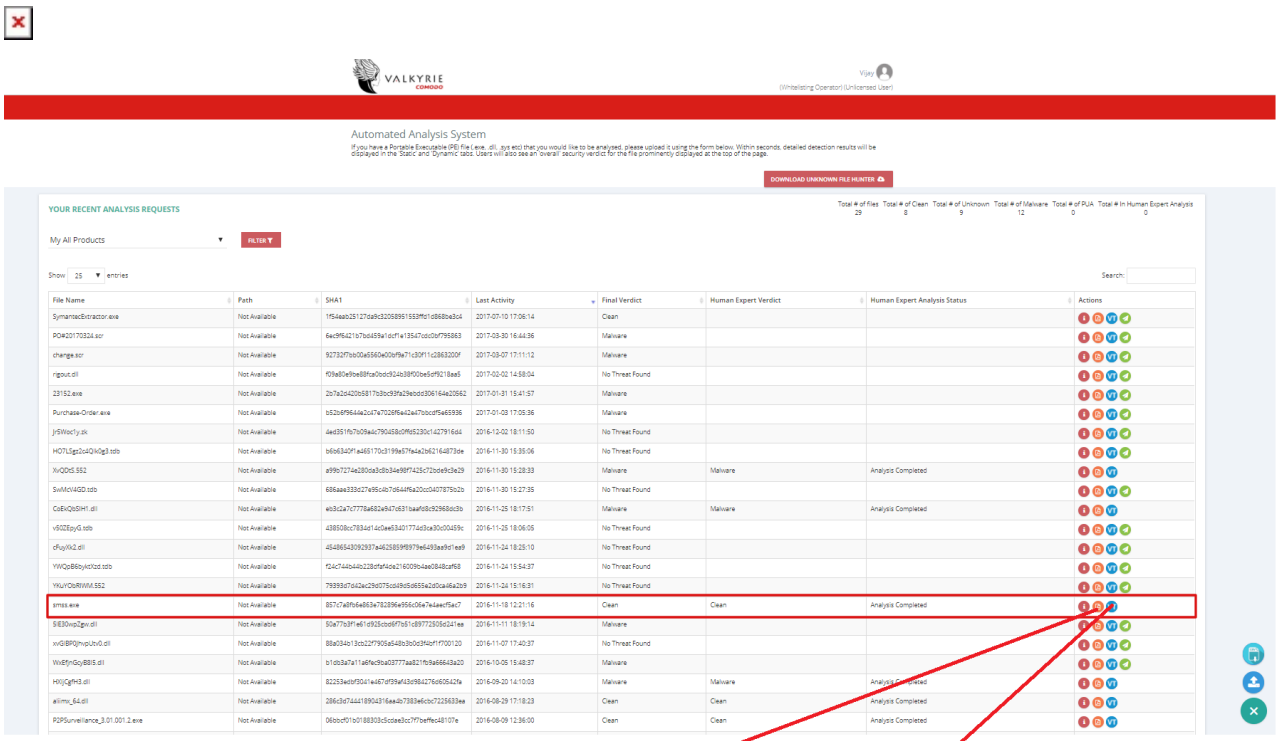


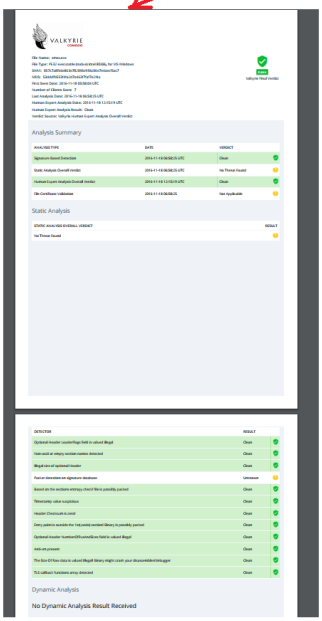
Precise Detectors:

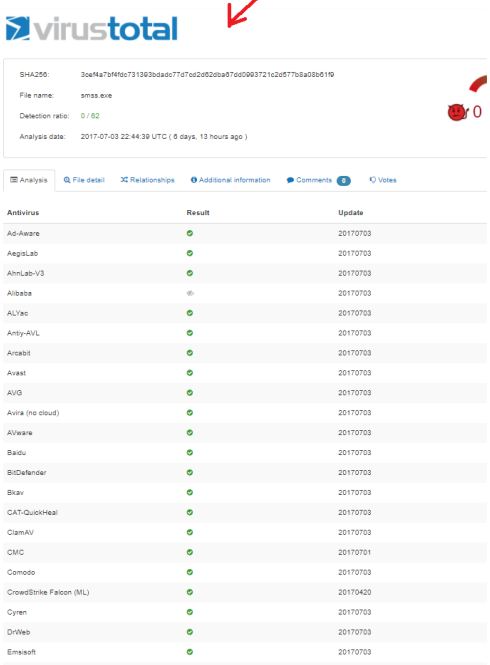
Human Expert Analysis:



File Details:


VALKYRIE
COMODO
Automated Analysis System
DOWNLOAD UNKNOWN FILE HUNTER
YOUR RECENT ANALYSIS REQUESTS




virustotal
SHA256: 3oef4a7bf4fdc731393bdade77d7cd2d62dba67dd0993721c2d577b8a08b61f9
File name: smss.exe
Detection ratio: 0 / 62
Analysis date: 2017-07-03 22:44:39 UTC (6 days, 13 hours ago)
Analysis
File detail
Relationships
Additional information
Comments 0
Votes
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