

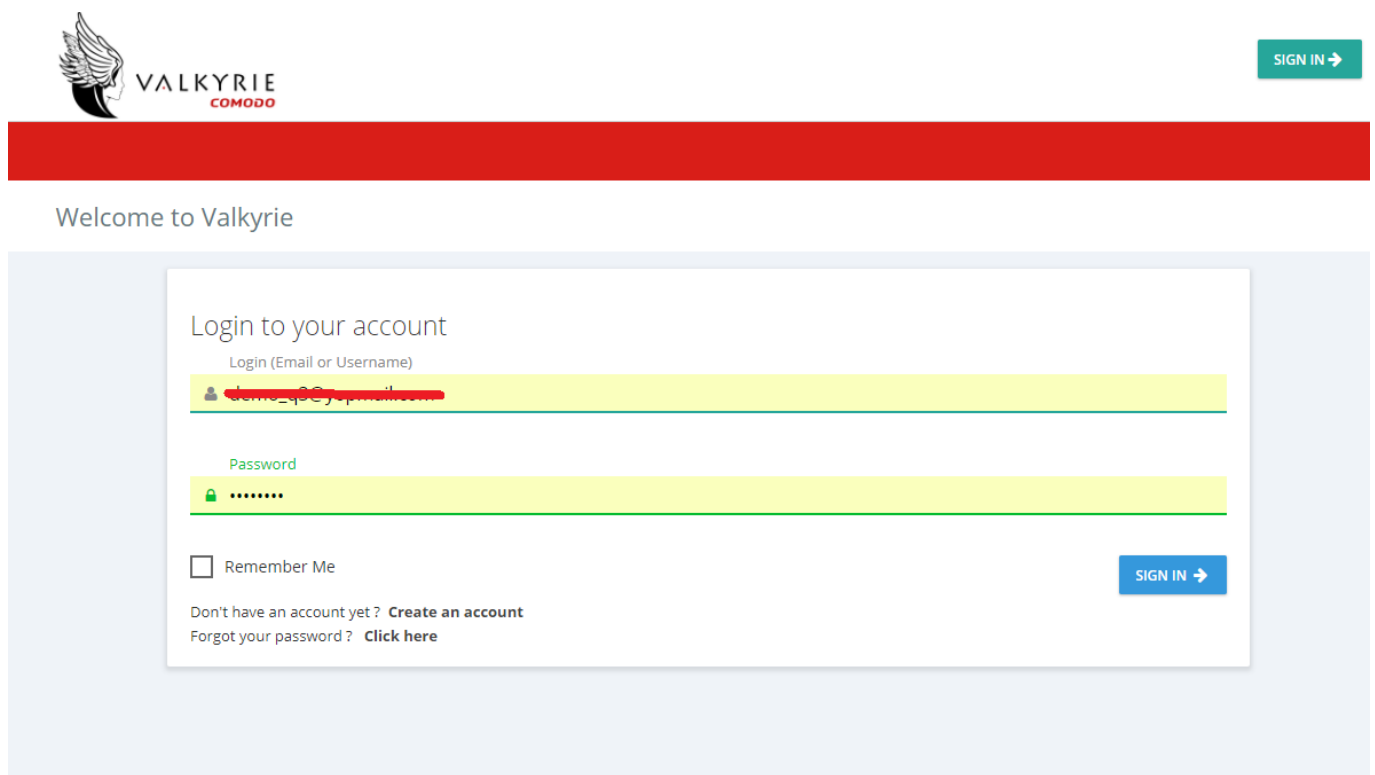
How to upload and analyze files in Valkyrie

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:

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 



Static Analysis:

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



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	⚠
Entry 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:

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: 5fa6fa96cf94620c85fca8d78de5d6b
 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:

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: 5fa6fa96cf94620c85fca8d78de5d6b
 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:

Automated Analysis System

If you have a Portable Executable (PE) file (.exe, .dll, .sys etc) that you would like to be analyzed, 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



































































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

YOUR RECENT ANALYSIS REQUESTS

[My All Products](#)

FILTER

Search

File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict	Human Expert Analysis Status	Actions
Symantec\tracore.exe	Not Available	154ea025127ca8c22088915320f1c880ba3c4	2017-07-10 17:08:14	Clean			  
POW20170324.scr	Not Available	6ac9f642170d589a0f441354f03c0f95863	2017-03-30 16:44:36	Malware			  
changes.exe	Not Available	927327b0c0a560c0a09f9f1c30f1c1863200f	2017-03-07 17:11:12	Malware			  
rgout.dll	Not Available	419e18e78ff8a0c0c3d3a38f050edf92128e5	2017-02-02 14:58:04	No Threat Found			  
23f32.exe	Not Available	207a24205881793bd39f9a29e0d506164c2562	2017-01-31 15:41:57	Malware			  
Purchase-Order.exe	Not Available	b32da9f64a4c2c470230f6a47b0c056f836	2017-01-03 17:03:36	Malware			  
j5Wcty.js	Not Available	4dc051b767009ac7904380b0f6230c14279164	2016-12-30 18:11:50	No Threat Found			  
HO7L3gc2c4Qkq3.tsb	Not Available	b3d6f4091448170d3739f39f76a2c626164873ee	2016-11-30 15:35:06	No Threat Found			  
XVOTL583	Not Available	a9997274a02058d30d39f497432c720e9f2a28	2016-11-30 15:28:33	Malware	Malware	Analysis Completed	  
SwM1400.tsb	Not Available	688aee336219f95cd70849fa25cd3287879c28	2016-11-30 15:27:35	No Threat Found			  
CatExQbDHL.dll	Not Available	e03Ca70777881Ea8c37d315ae0f8329863c0b	2016-11-28 18:17:51	Malware	Malware	Analysis Completed	  
v502EyG.tsb	Not Available	438f08c78334f1c45ea1347174a33a30c0a489e	2016-11-28 18:06:05	No Threat Found			  
dFuyK2.dll	Not Available	4540843092937a4c288998f947d433a9d1eap	2016-11-24 18:25:10	No Threat Found			  
VWQ86y6x0ctz.tsb	Not Available	724c4a4a0c238af94c4760095a46c8d49f68	2016-11-24 15:54:37	No Threat Found			  
VWQ86y6x0ctz.S32	Not Available	7939397034ac259075cc938f650582a5ca6a29	2016-11-24 15:56:31	No Threat Found			  
Itms.exe	Not Available	857c0d9d6483a73228a596506a7eade5ac7	2016-11-18 12:21:16	Clean	Clean	Analysis Completed	  
SEIOx2gw.dll	Not Available	50a7793f1ef1d3c0e0f93d187723305c15ee	2016-11-18 18:19:14	Malware			  
v5B9F0v0v0v.dll	Not Available	89a34013cc2579564630c039ca07f00120	2016-11-07 17:40:37	No Threat Found			  
WlExF0y8B5.dll	Not Available	810d3a7a1f6fd9c0a03777ae021b9a6663a27	2016-10-26 15:48:37	Malware			  
HQYqH3.dll	Not Available	82233e0350a74e47978f9d0394276805a20a	2016-09-20 14:10:03	Malware	Malware	Analysis Completed	  
elims_64.dll	Not Available	286c3f444189043f6a6d7383a6c0c725833ee	2016-08-29 17:18:23	Clean	Clean	Analysis Completed	  
RPSJmellence_3.01.001.2.exe	Not Available	0b0c07f00188303d3039f706f04d4010e	2016-08-02 12:36:00	Clean	Clean	Analysis Completed	  

[illegible]

virustotal

↗

SHA256: 3ee4e7b64fe371393bdade77d7ec20c20bae76cd093721c20577b8a0bb10

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 5
 Votes

Antivirus	Result	Update
Ad-Aware		2017/07/03
AegisLab		2017/07/03
AhnLab-V3		2017/07/03
Alibaba		2017/07/03
ALYac		2017/07/03
Anity-AVL		2017/07/03
Avast		2017/07/03
Avira		2017/07/03
AVG		2017/07/03
Avira (he cloud)		2017/07/03
AVware		2017/07/03
Baidu		2017/07/03
BioDefender		2017/07/03
Blav		2017/07/03
CAT-QuickHeal		2017/07/03
ClamAV		2017/07/03
CMC		2017/07/01
Comodo		2017/07/03
CrowStrike Falcon (ML)		2017/04/20
Cyren		2017/07/03
DrWeb		2017/07/03
Emsisoft		2017/07/03