

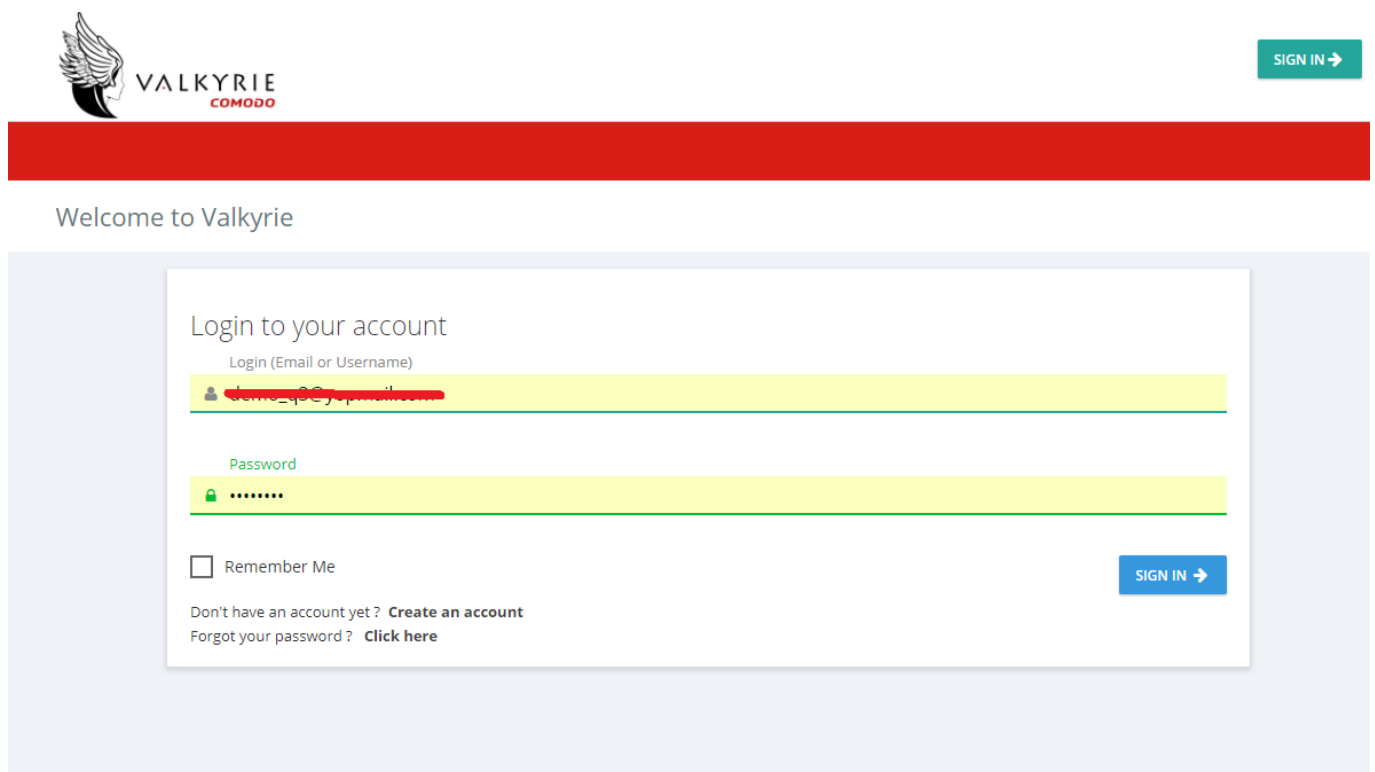
How to upload and analyze files in Valkyrie

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: 6ec9f6421b7bd459a1dcf1e13547cdc0b795863
 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



MALWARE
Valkyrie Final Verdict

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:

File Name: DThsLH.552
 File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
 SHA1: a99b7274e280da3c8b34e98f7425c72bde9c3e29
 MD5: 5fa6faff6c94620c85fca8d78de5d6b
 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: 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:

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



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), you can upload it 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 HEADER](#)

YOUR RECENT ANALYSIS REQUESTS

Total # of Files: 29 Total # of Clean: 8 Total # of Unknown: 9 Total # of Malware: 12 Total # of PUJ: 0 Total # in Human Expert Analysis: 0

My All Products FILTER ▼

Show 25 entries

File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict	Human Expert Analysis Status	Actions
SymantecScrtorator.exe	Not Available	1646b231275a8d320589153761c869a3d4	2017-07-10 17:06:14	Clean			
P0420170321.scr	Not Available	6e096421070a659f1edf4135470e009795663	2017-08-30 16:44:36	Malware			
change.scr	Not Available	9273a70e05a5650a009a7e71c0911c2883200f	2017-08-07 17:11:12	Malware			
ngout.dll	Not Available	09a80e0889a050c040a389000e0e0f218ad	2017-02-02 14:58:04	No Threat Found			
2f182.exe	Not Available	207a2d2058817b30c9f9a29e0c006164a20562	2017-01-31 15:41:37	Malware			
Purchase-Order.exe	Not Available	0520894462a7470298a4244700c95465836	2017-01-03 17:05:36	Malware			
J59hac7y.uk	Not Available	4ae031070a04c7905d80f65330c142791664	2016-12-02 18:11:50	No Threat Found			
H071gpaQdHg3.sbs	Not Available	8e063a0f1a485170a2199a794a2a621648730a	2016-11-30 15:35:06	No Threat Found			
XQ0D5.SB2	Not Available	499072744200a03d03a48974432720e0c3e29	2016-11-30 15:28:33	Malware	Malware	Analysis Completed	
SuM014QD.sbs	Not Available	686aa833027f96c0708449f5d0c04079752d3	2016-11-30 15:27:35	No Threat Found			
Cd8Q05ml.dll	Not Available	4032a7c7778a82674831aa0f5c529630c3d	2016-11-25 18:17:51	Malware	Malware	Analysis Completed	
v028y2.sbs	Not Available	438808c783411c0e4f3a01774c3a30c0c0459a	2016-11-25 18:06:05	No Threat Found			
dfyWk2.dll	Not Available	4548645292937a62389989796493a9f1ea9	2016-11-24 18:25:10	No Threat Found			
YWQ88y1c702.sbs	Not Available	1547444402387040e216009a4e0848ca98	2016-11-24 15:54:37	No Threat Found			
YKUC0uRMM.SB2	Not Available	793937842a2c307f5c08b5a855a20ca46a209	2016-11-24 15:16:31	No Threat Found			
smss.exe	Not Available	857c7a9f6a83a782396a956a744ae75a7	2016-11-18 12:21:16	Clean	Clean	Analysis Completed	
SEB02p2n.dll	Not Available	88077a7e1a9230a0f7051c897728505241ea	2016-11-11 18:19:14	Malware			
wg8p1mp03o.dll	Not Available	50a73a0130c217905a640c30c39a07f700120	2016-11-07 17:40:37	No Threat Found			
Ww8f5g8B8.dll	Not Available	010a3a7a1a8f9c08777aa821709a66643a20	2016-10-25 15:48:37	Malware			
H0jCpH3.dll	Not Available	8223a48f705148f7938438082761605429a	2016-09-20 14:10:03	Malware	Malware	Analysis Completed	
xiW1_64.dll	Not Available	206c374418940734a4b738346c72283394	2016-08-29 17:18:23	Clean	Clean	Analysis Completed	
P0P5urvellance_3_01.001.2.exe	Not Available	060cc70107183030c30693c770efcc48107e	2016-08-09 12:36:00	Clean	Clean	Analysis Completed	

Analysis Summary

Tool Name	SHA1	Verdict
Signature Scan (ClamAV)	2016-11-18-08:04:37	Clean
Static Analysis (Valkyrie)	2016-11-18-08:04:37	No Threat Found
Dynamic Analysis (Valkyrie)	2016-11-18-08:04:37	No Threat Found

Static Analysis

Tool Name	Verdict
Signature Scan (ClamAV)	Clean
Static Analysis (Valkyrie)	No Threat Found
Dynamic Analysis (Valkyrie)	No Threat Found

Dynamic Analysis

No Dynamic Analysis Result Received



SHA1: 857c7a9f6a83a782396a956a744ae75a7

File name: smss.exe

Deletion ratio: 0 / 62

Analysis date: 2017-07-02 22:44:39 UTC (6 days, 13 hours ago)

Antivirus	Result	Update
Ad-Aware		20170703
Avast		20170703
AVG		20170703
Avira (no cloud)		20170703
Avira		20170703
BitDefender		20170703
BKAV		20170703
CAT-QuickHeal		20170703
ClamAV		20170703
CMC		20170701
Comodo		20170703
CrowdStrike Falcon (ML)		20170420
Cyren		20170703
DrWeb		20170703
Emsisoft		20170703