

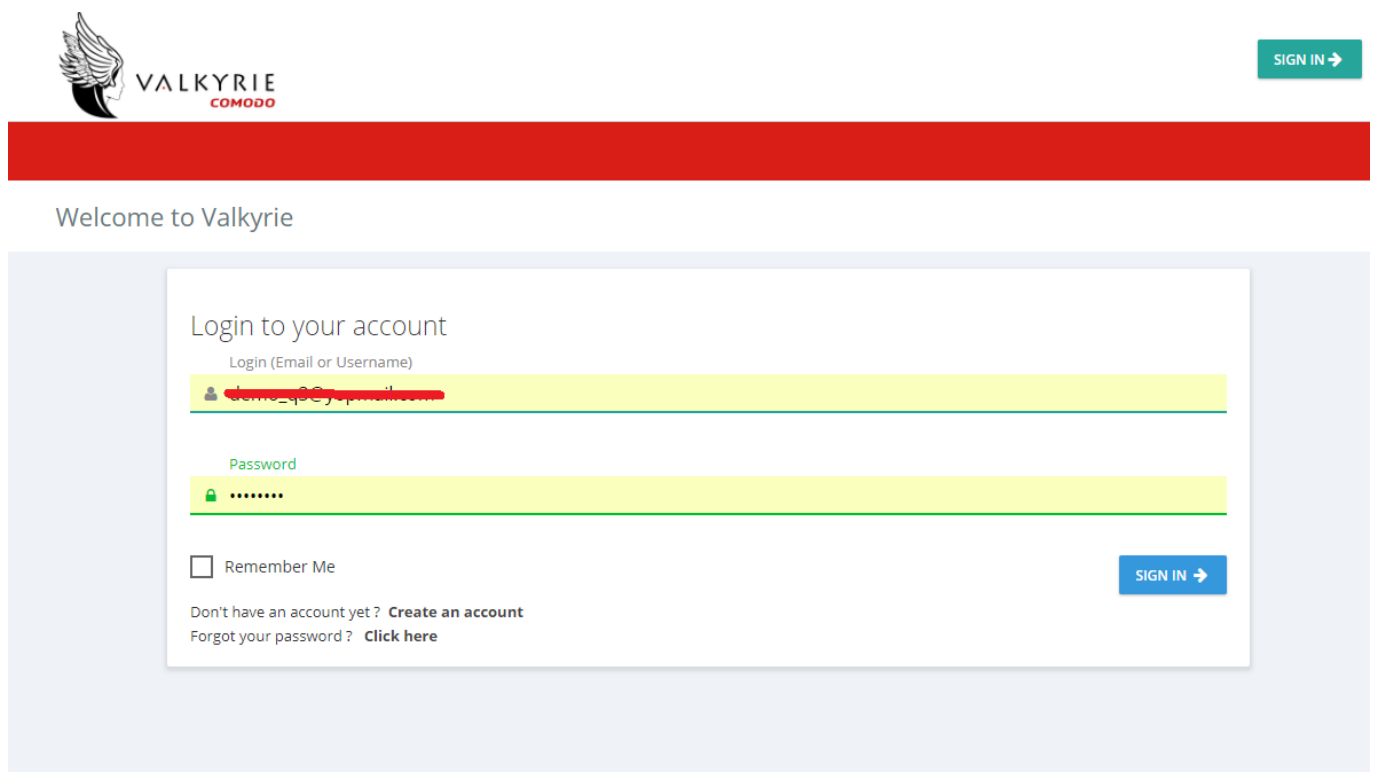
How to upload and analyze files in Valkyrie.

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



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

You have a Portable Executable (PE) file etc. all, just add 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 HEADER](#)

YOUR RECENT ANALYSIS REQUESTS

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

My All Products ▼ [FILTER ▼](#)

Show 25 entries

Search:

File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict	Human Expert Analysis Status	Actions
SymantecScorator.exe	Not Available	1546b231275a8d320589153791c869ba3d4	2017-07-10 17:06:14	Clean			📄 🔍 👤
P0420170321.scr	Not Available	6e3956210786195f1e0f4135470e0c0795663	2017-03-30 16:44:36	Malware			📄 🔍 👤
change.scr	Not Available	9273d78e05d65604098e71c3911c2883200f	2017-03-07 17:11:12	Malware			📄 🔍 👤
ngout.dll	Not Available	49840e89878a00c0a4a389000e0e0f9218aa3	2017-02-02 14:58:04	No Threat Found			📄 🔍 👤
23152.exe	Not Available	2b7a2d2618817b3c0939423e0c036164420562	2017-01-31 15:41:37	Malware			📄 🔍 👤
Purchase-Order.exe	Not Available	952b894462a4742029642447b00d95468936	2017-01-03 17:05:36	Malware			📄 🔍 👤
J9HnXcy.uk	Not Available	4ae8310707094c7905b0d9f533c142791664	2016-12-02 18:11:50	No Threat Found			📄 🔍 👤
H071gpc2d3q3.sbs	Not Available	8e6340f1a46317045199437944266216487304	2016-11-30 15:35:06	No Threat Found			📄 🔍 👤
XQD5.SB2	Not Available	499072744200a3d3a38974437220e0c3e29	2016-11-30 15:28:33	Malware	Malware	Analysis Completed	📄 🔍 👤
SixM14QD.sbs	Not Available	686aa833279f95c0708449f5d0c04079792b3	2016-11-30 15:27:35	No Threat Found			📄 🔍 👤
CdE0Q5m1.dll	Not Available	4b32a7c7738a8247631aa10f5c296363d3	2016-11-25 18:17:51	Malware	Malware	Analysis Completed	📄 🔍 👤
45023y2.sbs	Not Available	438808c7834f1c0c4e3401774c3a30c0c04594	2016-11-25 18:06:55	No Threat Found			📄 🔍 👤
dfyW2.dll	Not Available	4548645292937a6238939979e493a9f1ea39	2016-11-24 18:25:10	No Threat Found			📄 🔍 👤
YWQ88y47c02.sbs	Not Available	4547444402387040e2160094ae0848c493	2016-11-24 15:54:37	No Threat Found			📄 🔍 👤
YKUY0uRMM.SB2	Not Available	793937842ac2807f5cd8b5e85562c046a2628	2016-11-24 15:16:31	No Threat Found			📄 🔍 👤
smss.exe	Not Available	957c7a9f6483a7823964956a744ae75a7	2016-11-18 12:21:16	Clean	Clean	Analysis Completed	📄 🔍 👤
SEB3023n2.dll	Not Available	88e77071e10303e0d7051c897728505241e4	2016-11-11 18:19:14	Malware			📄 🔍 👤
mgB8f0p3c0c0.dll	Not Available	50a734013cc2f790564b03c0c39af7f700120	2016-11-07 17:40:37	No Threat Found			📄 🔍 👤
Ww8f05g.B8S.dll	Not Available	010a3a711a8f9c8d3777aa217b9466643a20	2016-10-25 15:48:37	Malware			📄 🔍 👤
H05cYd3.dll	Not Available	82234e0f70414d7f938438b8227616054294	2016-09-20 14:10:03	Malware	Malware	Analysis Completed	📄 🔍 👤
4f1m1_64.dll	Not Available	266d37441894037464b73834fc0c72263394	2016-08-29 17:18:23	Clean	Clean	Analysis Completed	📄 🔍 👤
P05uVnHlance_3_01.001.2.exe	Not Available	06bc05107183030c30c770e0c48107e	2016-08-09 12:36:00	Clean	Clean	Analysis Completed	📄 🔍 👤



VALKYRIE

Analysis Summary

Analysis Type	SHA1	Verdict
Signature based detection	957c7a9f6483a7823964956a744ae75a7	Clean
Static analysis (heuristics)	957c7a9f6483a7823964956a744ae75a7	No Threat Found
Dynamic analysis (sandbox)	957c7a9f6483a7823964956a744ae75a7	No Threat Found

Static Analysis

SHA1: 957c7a9f6483a7823964956a744ae75a7

File Name: smss.exe

Dynamic Analysis

No Dynamic Analysis Result Received



SHA256: 3ee847d9160781392bd4d07747c02d82b2a87e00903721c2d977b5a080b19

File name: smss.exe

Detection ratio: 0 / 62

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

Analysis

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