

How to get automated Kill chain report of malware files from valkyrie

Kill Chain report is used for providing the full description of the malware file that is available on the network. Now the reports are also available for the users who are not holding the Valkyrie Dashboard functionality.

Step [1]: For login to the Valkyrie dashboard, Go to → valkyrie.comodo.com. Click ' Sign In → ' button it will navigate to a login page, provide the credentials of the c1 account. It will display all the malicious file entries since it has been enabled with the default option as " Your Recent Analysis Request ".We can able to view the account by choosing the particular account which has been provided under the filter options. This page will display the [malicious file](#) detail entry up to 25 entries as a default.

[SIGN IN](#)[SEARCH](#)

Valkyrie

Valkyrie is a file verdict system. Different from traditional signature based malware detection techniques Valkyrie conducts several analysis using run-time behavior and hundreds of features from a file and based on analysis results can warn users against malware undetected by classic Anti-Virus products.

[DOWNLOAD UNKNOWN FILE HUNTER](#)

LATEST FILE UPLOADS

SHA1	File Name	Source	Submit Date	Final Verdict	Human Expert Verdict	Human Expert Analysis Status
ae75ee2368ca988f21dd0985de798b54449f138	Kodi_1122057593.exe	Upload	2017-06-22 01:37:33	PUA	PUA	Completed
47069ac3ab836870ae341d844fd9fd5d56ae75a7	becdfbcbceafbebebeaefaedaa...	Upload	2017-06-22 19:58:58	Malware	Malware	Completed
de979720b8d5cb43080809b6c46c178cd2cb9b2	wannacry.exe	Upload	2017-06-22 19:26:57	Malware	Malware	Completed
d86a07191426484d9364d59fe912dc73e9145a	EmailAccessOnline.exe	Upload	2017-06-22 18:24:07	PUA	PUA	Completed
3a0d409a0c9aa7cfd8350d4c4ee03da978cb6b3	wannacry.exe	Upload	2017-06-22 18:14:58	Malware	Malware	Completed
4b24dedb7c8d56a4880d62d1ffad605cc5959eb1	sync.exe	Upload	2017-06-22 18:04:44	PUA	PUA	Completed
9f2a6d73d810247cec07c05112dbef1c2f8ae3f	mnp.exe	Upload	2017-06-22 17:51:36	Malware	Malware	Completed
ca0ed9801c1467b13b305f9b556dd9fd70bef891	bacteria-50.exe	Upload	2017-06-22 08:38:49	Malware	Malware	Completed
47c3821b235dca96a20cea76c95178b63f51fa9f	evsys-97.exe	Upload	2017-06-22 08:32:01	Malware	Malware	Completed
f2985c6ca13d9945156c433178d170f070c6b7	CheathappensTrainer1412.tmp	Upload	2017-06-22 07:50:08	PUA	PUA	Completed

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

[SIGN IN](#)

Welcome to Valkyrie

Login to your account

Login (Email or Username)

Password

☐ Remember Me

Don't have an account yet? [Create an account](#)

Forgot your password? [Click here](#)

[SIGN IN](#)

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



(Free User) (Enterprise)

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: 10 Total # of Clean: 3 Total # of Unknown: 0 Total # of Malware: 6 Total # of PUA: 1 Total # in Human Expert Analysis: 0

coyteewile@yahoo.com

[FILTER](#)

Show 25 entries

Search:

File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict	Human Expert Analysis Status	Actions
cpil.dll	Not Available	d3be9ebc42f164efb082...	2017-06-21 18:22:51	Malware			I D V T
fiddler4setup_2.exe	Not Available	a278cbba9ebb22701be2...	2017-06-21 17:16:09	Clean			I D V T
tserv.exe	Not Available	846c130e115589cf89720...	2017-06-21 14:49:46	Malware			I D V T F
ce2d63b3395071eb2e5357aa55...	Not Available	ce2d63b3395071eb2e53...	2017-06-12 11:55:41	Malware			I D V T F
Ghost.exe	Not Available	df3328f9944867c3c5e14...	2017-06-07 12:41:29	PUA	PUA	Analysis Completed	I D V T
cpil.exe	Not Available	795fe85537ec314f36670...	2017-06-07 12:41:16	Malware			I D V T F
cpil.exe	Not Available	795fe85537ec314f36670...	2017-06-07 12:41:16	Malware			I D V T F
pcflank.exe	Not Available	3437369e6b75021f57de...	2017-06-07 12:37:38	Malware			I D V T F
ProjectLibrary.dll	Not Available	9dc229e28467e9cdebb...	2017-06-07 12:37:05	Clean	Clean	Analysis Completed	I D V T
TrojanSimulator.exe	Not Available	85789749c0ec90c8246f...	2017-06-07 11:54:33	Malware			I D V T F
WAXA26.tmp	Not Available	9069e3b8e8ed76a2a0...	2017-06-07 11:53:09	Clean	Clean	Analysis Completed	I D V T

Showing 1 to 10 of 10 entries

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

Step [2]: For viewing the already existing malware file details, click below Kill Chain Report Button available on the at the right side of 'Actions' column.It will open the overall description for a [malware file](#) along with the option of Download Kill Chain Report.

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: 10 Total # of Clean: 3 Total # of Unknown: 0 Total # of Malware: 6 Total # of PUA: 1 Total # In Human Expert Analysis: 0

coyoteewile@yahoo.con

FILTER

Show 25 entries

Search:

File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict	Human Expert Analysis Status	Actions
cpil.dll	Not Available	d3be9ebc642f164efb082...	2017-06-21 18:22:51	Malware			i is VT is
fiddler4setup_2.exe	Not Available	a278cb9a6ebb22701be2...	2017-06-21 17:16:09	Clean			i is VT is
tserv.exe	Not Available	846c130e115589cf89720...	2017-06-21 14:49:46	Malware			i is VT is
ce2d63b3395071eb2e5357aa85b...	Not Available	ce2d63b3395071eb2e53...	2017-06-12 11:55:41	Malware			i is VT is
Ghost.exe	Not Available	df3328f9944867c3c5e14...	2017-06-07 12:41:29	PUA	PUA	Analysis Completed	i is VT is
cpil.exe	Not Available	795fe85537ec514f36670...	2017-06-07 12:41:16	Malware			i is VT is
pcflank.exe	Not Available	3437369e6b75021f57de...	2017-06-07 12:37:38	Malware			i is VT is
ProjectLibrary.dll	Not Available	9dc229e28467e9cdebba...	2017-06-07 12:37:05	Clean	Clean	Analysis Completed	i is VT is
TrojanSimulator.exe	Not Available	85789749ce0ec90c8246f...	2017-06-07 11:54:33	Malware			i is VT is
WAXA26.tmp	Not Available	9069e3b8ee8ed7b0a2e0...	2017-06-07 11:53:09	Clean	Clean	Analysis Completed	i is VT is

Showing 1 to 10 of 10 entries

< 1 >

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

[Summary](#)
[Activity Details](#)
[Behaviour Graph](#)
[Behaviour Summary](#)
[Detailed File Info](#)
[Network Behaviour](#)
[Screenshots](#)

File Name: cpil.dll

File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

SHA1: d3be9ebc642f164efb08270ee85116158ce7a8a

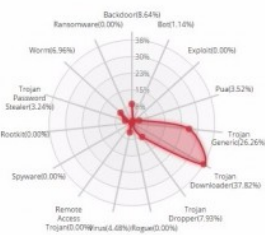
MD5: 5fb133a80a9bb9cdab3672cc1a0846d

[DOWNLOAD KILL CHAIN REPORT](#)

DETECTION SECTION



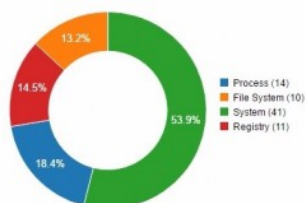
CLASSIFICATION



ACTIVITY OVERVIEW

Hooking and other Techniques for Hiding Protection 1 (100.00%)

HIGH LEVEL BEHAVIOR DISTRIBUTION



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

Step [3]: By clicking on the " Download Kill Chain Report " it will provide the entire file information as a Report on a pdf. For more analysis and description of the kill chain report you can refer the following topic <https://help.comodo.com/topic-397-1-...in-Report.html>

Step [4]: To View, the kill chain report of the new malware file click the 'Kill Chain Report' that has been prevailed on the right side of the 'Actions' column. Simultaneously, by selecting the ' View Info ' button it will navigate to next page. Select the ' Send to Kill Chain Analysis ' which was prevailing on the right side top of the 'Valkyrie Final Verdict'.

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: 10 Total # of Clean: 3 Total # of Unknown: 0 Total # of Malware: 6 Total # of PUA: 1 Total # in Human Expert Analysis: 0

coyoteewile@yahoo.con ▼

FILTER T

Show 25 entries

Search:

File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict	Human Expert Analysis Status	Actions
cpil.dll	Not Available	d3be9ebc642f164efb082...	2017-06-21 18:22:51	Malware			  
fiddler4setup_2.exe	Not Available	a278cbba6ebb22701be2...	2017-06-21 17:16:09	Clean			  
tserv.exe	Not Available	846c130e115589cf99720...	2017-06-21 14:49:46	Malware			  
ce2d63b3395071eb2e5357aa85b...	Not Available	ce2d63b3395071eb2e53...	2017-06-12 11:55:41	Malware			  
Ghost.exe	Not Available	df3328f9944867c3c5e14...	2017-06-07 12:41:29	PUA	PUA	Analysis Completed	  
cpil.exe	Not Available	795fe85537ec514f36670...	2017-06-07 12:41:16	Malware			  
cpil.exe	Not Available	795fe85537ec514f36670...	2017-06-07 12:41:16	Malware			  
pcflank.exe	Not Available	3437369e6b75021f57de...	2017-06-07 12:37:38	Malware			  
ProjectLibrary.dll	Not Available	9dc229e28467e9cdebba...	2017-06-07 12:37:05	Clean	Clean	Analysis Completed	  
TrojanSimulator.exe	Not Available	85789749ce0ec90c8246f...	2017-06-07 11:54:33	Malware			  
WAXA26.tmp	Not Available	9069e3b8ee8ed7b0a2e0...	2017-06-07 11:53:09	Clean	Clean	Analysis Completed	  

Showing 1 to 10 of 10 entries

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




Summary Static Analysis Dynamic Analysis Precise Detectors File Details

File Name: cpil.dll
 File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
 SHA1: d3be9ebc642f164efb082f70ee85116158ce7a8a
 MD5: 5fb133a80a9bb9cdab3672cc1a08e46d
 First Seen Date: 2016-08-22 12:00:58 (10 months ago)
 Number of Clients Seen: 2
 Last Analysis Date: 2016-08-23 10:44:00 (10 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

[Send to Kill Chain Analysis](#)

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2016-08-23 10:44:00	Malware 
Static Analysis Overall Verdict	2016-08-23 10:44:00	No Threat Found 
File Certificate Validation	2016-08-23 05:14:00	Not Applicable 

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


Step [5]: Once you clicked the analysis, a message will pop up like " Are you sure you want to send the file to Kill-Chain Analysis ? " select the send button.It will ensure you a report that will be generated automatically with a time span of 30 minutes after selecting the button.

Send to Kill Chain Analysis

Are you sure you want to send file to Kill-Chain Analysis ?

SEND

CANCEL



(Free User) (Enterprise)

Summary

Static Analysis

Dynamic Analysis

Precise Detectors

File Details

File Name: cpil.dll

File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

SHA1: d3be9ebc642f164efb082f70ee85116158ce7a8a

MD5: 5fb133a80a9bb9cdab3672cc1a08e46d


First Seen Date: 2016-08-22 12:00:58 (10 months ago)

Number of Clients Seen: 2

Last Analysis Date: 2016-08-23 10:44:00 (10 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

Kill Chain report is being created

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2016-08-23 10:44:00	Malware 
Static Analysis Overall Verdict	2016-08-23 10:44:00	No Threat Found 
File Certificate Validation	2016-08-23 05:14:00	Not Applicable 

Step [6]: By clicking on the "Download Kill Chain Report" you can able to get the entire description of the file on Summary, Activity Details, Behaviour Graph, Behaviour Summary, Network Behavior, Detailed File Info along with the Screenshots.

7

Summary Static Analysis Dynamic Analysis Precise Detectors File Details

File Name: cpil.dll
File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
SHA1: d3be9ebc642f164efb08270ee85116158ce7a8a
MD5: 5fb133a80a9bb9cdab3672cc1a08e46d
First Seen Date: 2016-08-22 12:00:58 (10 months ago)
Number of Clients Seen: 2
Last Analysis Date: 2016-08-23 10:44:00 (10 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

Click this report



Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2016-08-23 10:44:00	Malware
Static Analysis Overall Verdict	2016-08-23 10:44:00	No Threat Found
File Certificate Validation	2016-08-23 05:14:00	Not Applicable

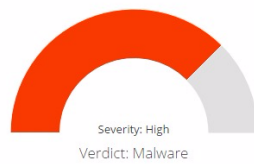
© Valkyrie, Comodo Group, Inc. 2017. All rights reserved. v1.17.0-ENT

Summary Activity Details Behaviour Graph Behaviour Summary Detailed File Info Network Behaviour Screenshots

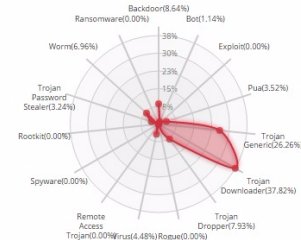
File Name: cpil.dll
File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
SHA1: d3be9ebc642f164efb08270ee85116158ce7a8a
MD5: 5fb133a80a9bb9cdab3672cc1a08e46d

DOWNLOAD KILL CHAIN REPORT

DETECTION SECTION



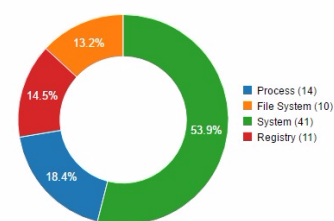
CLASSIFICATION



ACTIVITY OVERVIEW

Hooking and other Techniques for Hiding Protection 1 (100.00%)

HIGH LEVEL BEHAVIOR DISTRIBUTION



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