



Comodo Unknown File Hunter

Software Version 2.1

Administrator Guide

Guide Version 2.1.061118

Comodo Security Solutions 1255 Broad Street Clifton, NJ 07013

Table of Contents

1 Introduction to Comodo Unknown File Hunter	3
2 Run Unknown File Hunter	4
2.1 The Main Interface	5
3 Scan Computers	7
3.1 Scan Computers using Active Directory	8
3.2 Scan Computers using Workgroup	14
3.3 Scan Computers by Network Addresses	20
3.4 Scan Local Computer	24
3.5 Analyze Files with Valkyrie	31
4 Scan Results	34
4.1 Comodo Unknown File Hunter Scan Results	35
4.2 Valkyrie Analysis Results	39
5 Reports	53
5.1 Executive Report	53
5.2 Device Report	55
5.3 Program Report	55
6 About Comodo Unknown File Hunter	56
7 Agent Requirements	57
About Comodo Security Solutions	59

COMODO Creating Trust Online

1 Introduction to Comodo Unknown File Hunter

It is estimated that traditional antivirus software can only catch 40% of all malware in the world today. The other 60% are 'unknown'. An advanced persistent threat (APT) is an 'Unknown' piece of malware that is so well disguised it can be months before a traditional anti-virus catches up to it. During this time, these malicious files continue to reside on the victim's computer, executing their payloads all the while.

Comodo Unknown File Hunter (UFH) is a lightweight scanner which identifies unknown, and potentially malicious files, residing on your network. After scanning your systems, it will classify all audited files as 'Safe', 'Malicious' or 'Unknown'. While 'Safe' files are OK and 'Malicious' files should be deleted immediately, it is in the category of 'Unknown' that most zero-day threats are to be found. The UFH scanner allows you to upload these files to our Valkyrie servers where they will undergo a battery of run-time tests designed to reveal whether or not they are harmful. You can view the results of these tests in the UFH interface.

COMODO Creating Trust Online Unknown File Hunter	_ 🗆 ×
🕑 Start Scan 🥒 Analyze with Valkyrie 💿 Stop Scan 🌰 Reports - 🍥 Options 👔 Help - 🖌	Search
Scan results Valkyrie analysis results Group by Computers	Group by Files
Name	▼ Size
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1472. Unknown files: 1. Malicious files: 0.	aan aa ahaa ahaa ahaa ahaa ahaa ahaa ah
C\program files\freedownloadmanager.org\free download manager\qt5qml.dll	2 MB
C:\Program Files (x86)\OpenOffice 4\program\unopkg.exe	11 KB
c:\program files\freedownloadmanager.org\free download manager.common.dll	416 KB
🔘 c:\program files\freedownloadmanager.org\free download manager\imageformats\qjpeg.dll	234 KB
🔘 c:\program files\freedownloadmanager.org\free download manager\libcetdll	62 MB
c:\program files:\freedownloadmanager.org:\free download manager.swscale-4.dll	647 KB
⑦ c:\program files\freedownloadmanager.org\free download manager\avfilter-5.dll	2 MB
c.\program files\freedownloadmanager.org\free download manager\winwfpmonitor.exe	829 KB
C:\program files:\freedownloadmanager.org\free download manager\sqldrivers\qsqlite.dll	866 KB
Please click here to see the detailed results	
1 Unknown files, 0 Malicious files (1 of 1 Computers scanned)	

Features

- No installation required, just run the portable application on any computer in the network
- · Capable of scanning computers from Active Directory, Work Group and by Network Addressees
- Unknown files can be automatically uploaded to Comodo Valkyrie and tested for malicious behavior
- · Comprehensive reports provide granular details about the trust level of files on your endpoints

This guide is intended to take you through the use of Comodo UFH and is broken down into the following main sections.

Introduction

COMODO Creating Trust Online*

- Running Unknown File Hunter
- Scanning Computers
 - Scanning Computers using Active Directory
 - Scanning Computers using Workgroup
 - Scanning Computers by Network Addressees
 - Scanning Local Computer
 - Analyzing Files with Valkyrie
- Scan Results
 - Unknown File Hunter Tool Scan Results
 - Valkyrie Analysis Results
- Reports
 - Executive Report
 - Device Report
 - Program Report

2 Run Unknown File Hunter

Comodo Unknown File Hunter can be downloaded from https://valkyrie.comodo.com/apt_tool/download/UnknownFileHunter.exe.

After saving the application to your computer, you can launch the tool by double-clicking on the application icon:

🔄 UnknownFileHunter

The Main Interface will be displayed.

COMODO Creating Trust Online*



Refer to the next section 'The Main Interface' for more details about the features.

2.1 The Main Interface

The main interface of the tool allows you to configure and run scans, view results and generate risk reports.

COMODO Creating Trust Online

Title Bar	Mer	nu Bar	
COMODO Creating Trust Online Unknown File Hu	nter		_ 🗆 ×
💽 Start Scan 🧳 Analyze with Valk	yrie 🔳 Stop Scan 🏼 🙆 R	eports - 🍥 Options 🕧 F	rleip - 👂 Search
Scan results Valkyrie analysis results Name		Group by Size Verdict	Computers Group by Files Trusted Vendor
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 5. Unknown files	: 1. Malicious files: 0. Trusted/Clean files: 4.		
	Main Display View the details endpoints and resu and Valkyrie Ar	Area of scanned ilts of UFH tool nalysis	
1 Unknown files, 0 Malicious files (1 of 2 Comput	<u>Please click here to see the</u> ers scanned)	e detailed results	
	Notificatio	n Area	

Main Functional Areas

- **Title Bar** Displays the scanning progress. You can also minimize, maximize and close the application by using the controls at the far right.
- Menu Bar Contains the controls for using the application.
 - Start Scan Scan target computers to identify unknown files. You can add computers via Active Directory, Workgroup or Network Addresses. Refer to the section 'Scanning Computers' for more details.
 - Stop Scan Allows you to cancel the scanning process.
 - **Options** Displays the port numbers that CUFH uses to communicate with our file lookup service (FLS). The FLS is used to deliver real-time verdicts on the trust status of unknown files. Admins should leave these ports at the default.

COMODO Creating Trust Online*

Options				×
	FLS TCP Port	80		
	FLS UDP Part	53		
	G	ncel	Save	

- **Reports** Allows administrators to view reports generated by the UFH tool and Valkyrie. Refer to the section '**Reports**' for more details.
- Help The 'About' menu entry shows product and version information. Refer to 'About Comodo Unknown File Hunter for more details. The 'Agent Requirements' menu entry contains troubleshooting advice if you experience problems connecting to your target computer.
- Search Allows administrators to search for listed endpoints by name.
- Main Display Area Displays the details of scanned endpoints and the results from UFH and Valkyrie. Refer to the sections 'Scanning Computers' and 'Scan Results' for more details.
- Notification Area Displays real-time information about unknown and malicious files detected, and number of endpoints scanned.

3 Scan Computers

The Comodo UFH tool allows administrators to add computers for scanning in multiple ways. The scanning will be performed by the UFH tool and results displayed. If you want further analysis of the detected files, then you can submit the results to Valkyrie.

- Active Directory Suitable for a corporate environment where a large number of endpoints need to be scanned within a network.
- Workgroup Allows you to add computers that belong to work group for scanning
- Network Address Specify host names, IP addresses or IP ranges of computers which need to be scanned.
- This Computer Allows you to run a scan on your local device.

COMODO Creating Trust Online*



Refer to the following sections for more details:

- Scan Computers using Active Directory
- Scan Computers using Workgroup
- Scan Computers by Network Addresses
- Scan Computers by Custom Scan

3.1 Scan Computers using Active Directory

The Active Directory method of adding computers allows administrators to include a number of endpoints in a domain for scanning.

• To open the 'Start Scan Wizard', click the 'Start Scan' button at top-left or the 'Scan Now!' link in the main display area.

COMODO Creating Trust Online



• Select 'Active Directory' to open the AD configuration screen:

Start Scan Wiza	ard		×
	Active Directory Creden	tials	
	Domain Name	Enter Domain Name	
	Domain Administrator	Enter Domain Administrator	
	Password	Enter Password	\$
Back			Next

• Enter the domain name and administrator details of your Active Directory.

COMODO Creating Trust Online*

Start Scan Wiz	ard	×
	Select Computers	
Back		Next

After successful authentication of the domain details, the 'Select Computers' screen will be displayed.

Start Scan Wiza	ard		×	<
	Scan Credentials			
	Login	Administrator		
	Password	•••••	<i>•</i>	
Back		Quick Scan	Full Scan	

COMODO Creating Trust Online*

Select the endpoints that you want to scan and choose one of the following scan types:

Quick Scan: Scans critical and commonly infected areas of target endpoints

Full Scan: Scans all files and folders on target endpoints.

•

COMODO Creating Trust Online Unknown File Hunter (S	tarting scan)				_ 🗆 ×
🕟 Start Scan 🏾 🍼 Analyze with Valkyrie	Stop Scan	i Reports +	Options	(i) Help -	Search
Scan results Valkyrie analysis results					
Name					▼ Size
DESKTOP-TTPO9PR (10.108.51.100) Enumerating autoruns: 993					
WIN-EV5S84NSROI (10.108.51.242) Connecting to the target computer					
					G
0 Unknown files, 0 Malicious files (0 of 2 Computers scann	ed)				

The progress of the scan will be displayed for each computer on the respective rows and the total scanning progress on the title bar.

• Click the 'Stop Scan' button to discontinue the scanning process and confirm it in the 'Stop Scan' dialog.

The notification bar at the bottom displays the number of unknown and malware programs detected including the number of endpoints being scanned. After the scanning process is completed, the results will be displayed including the option to analyze the results with Valkyrie.

COMODO Creating Trust Online*

COMODO Creating Trust Online Unknown File Hunter	_ 🗆 ×
Start Scan	O Search
Scan results Valkyrie analysis results Group by Computers	Group by Files
Name	▼ Size
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1541. Unknown files: 5. Malicious files: 0.	
WIN-EV5584NSROI (10.108.51.242) Login problem: invalid username or bad password.	
Please click here to see the detailed results	
1 Unknown files, 0 Malicious files (1 of 2 Computers scanned)	

The details of results will be displayed in the respective endpoint rows, providing information such as the number of unknown files, number of malware found, the accessibility to the computers, scan progress and more.

There are results will be displayed in two ways:

Group by Computer: The scan results will display total number of computers scanned and the number of unknown files found in those computers.

Group by File: The scan results will display the name and number of instances of unknown files identified. The option dialog to analyze the results with Valkyrie will also be displayed:

COMODO Creating Trust Online

Scan F	Results	×
()	Scan Complete Do you want to an Valkyrie?	ed! nalyze unknown files with
	Scan Summary: 2 Total Scan Attemp - 1 Successful Scans - 1 Failed Scans	ts
	Threat Detection Sur 5 Total Threats Foun - 5 Unknown Files	nmary: d*
	* 5 files have unique Yes	hash values No

Valkyrie is an online file verdict service which analyzes the behavior of unknown files with a range of static and dynamic tests. Clicking 'OK' opens the 'Activate Valkyrie' screen. Existing users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Get Valkyrie' to create a free account.



You can also Click 'Analyze with Valkyrie' button to submit to Valkyrie for further analysis.

Submit to Valkyrie	×
Please sign in with Comodo License Account credentials to analyze files with Valkyrie	Please sign up to Valkyrie if you don't have a Valkyrie account yet
Enter User Name	<u>Valkyrie</u> is a cloud-based file analysis service for submitted known and unknown files with a range of static and dynamic detectors including file lookup,
	heuristics and real-time behaviour analysis
The State State State Activity and State	
ОК	Sign Up

Valkyrie results will be displayed in the Unknown File Hunter interface and, in more detail, in the Valkyrie portal:

lkyrie is a file verdict system. Different f lkyrie conducts several analysis using ru	rom traditional signature un-time behavior and hun	based n dreds of	halware of features	detection s from a f	techniqu file and b	ies ased on
alysis results can warn users against m	alwares undetected by cla	assic Anti	i-Virus pr	oducts.		
			DOWNL	OAD UNKNI	UWN HILE HU	JNTER 🖎
LATEST FILE UPLOADS						
SHA1	File Name	Source	Submit Date	Final Verdict	Human Expert Verdict	Human Expert Analysis Status
545e3297ed5f6324f261921bb5f007767c7bf6bc	VLC_Media_Player_Setup.exe	Upload	2016- 12-19 18:48:35	PUA	PUA	Complete
4476e9dc1b397f89fa2e1ec5256fced6dcaff686	be25	Upload	2016- 12-19 12:48:16	Malware	Malware	Complete
bc46a374f8215e5a0b35ff0ce11af1ed8a292e9b	Driver_9291.exe	Upload	2016- 12-19 11:29:00	PUA	PUA	Complete
c23d29666c5e67b90a5782d71729edffcc43991b	8550bd85bd1f774ab87cb86	Upload	2016- 12-19 11:24:58	PUA	PUA	Complete
60904de5d6f45714fd9d8d1dc91528b04448d7d1	Adobe_Flash_Player_xetapp	Upload	2016- 12-19 11:24:27	Malware	Malware	Complete

Refer to the section 'Analyzing Files with Valkyrie' and 'Scan Results' for more details.

3.2 Scan Computers using Workgroup

The Comodo UFH tool allows administrators to run a scan on computers that are available within a Workgroup.

To open the 'Start Scan Wizard' screen, click the 'Start Scan' button at the top-left or the 'Scan Now!' link in the main display area.

COMODO Creating Trust Online*



 Click 'Workgroup' and select the available workgroups or enter the domain name of your existing Workgroup

Start Scan Wizard	d		×
	Specify Workgroup		
	Search Available Workgroups (m	ay take some time)	
	 Use Known Workgroup Name 	Enter Workgroup Name	
Back			Next

Select the endpoints that you want to scan and choose one of the following scan types:
 Quick Scan: Scans critical and commonly infected areas of target endpoints
 Full Scan: Scans all files and folders on target endpoints.

COMODO Creating Trust Online

Start Scan Wiza	ard	×
	Select Computers	
	 C1TEST COMODO TEST WORKGROUP 	
Back		Next

• Enter the system's unique administrator username/password.

Start Scan Wiza	ard			×
	Scan Credentials			
	Login	Enter Login		
	Password	Enter Password	~	
Back		Quick Scan	Full Scan	

COMODO Creating Trust Online*



· Click the 'Stop Scan' button to discontinue the scanning process and confirm it in the 'Stop Scan' dialog.

The notification bar at the bottom displays the number of unknown and malware programs detected, the number of endpoints scanned, the accessibility to the computers, scan progress details and more. Full results will be displayed after the scan finishes. You will also be given the opportunity to analyze unknown files with Valkyrie:

COMODO Creating Trust Online*

COMODO Creating Trust Online Unknown File Hunter	_ 🗆 ×
Start Scan	O Search
Scan results Valkyrie analysis results Group by Computers	Group by Files
Name	▼ Size
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1541. Unknown files: 5. Malicious files: 0.	
WIN-EV5584NSROI (10.108.51.242) Login problem: invalid username or bad password.	
Please click here to see the detailed results	
1 Unknown files, 0 Malicious files (1 of 2 Computers scanned)	

For each endpoint that was successfully scanned, you'll see total number of files scanned and the number of unknown and malware files found. Results can be viewed in two ways:

Group by Computer: Shows the total number of computers scanned and the number of unknown files found in those computers.

Group by File: Shows the name and quantity of each unknown file.

The option to analyze the results with Valkyrie will also be displayed:

COMODO Creating Trust Online

Scan I	Scan Results X					
(Scan Complete Do you want to an Valkyrie? Scan Summary: 2 Total Scan Attemp - 1 Successful Scans - 1 Failed Scans	ed! nalyze unknown files ts	with			
	Threat Detection Su 5 Total Threats Foun - 5 Unknown Files * 5 files have unique	mmary: d* hash values				
	Yes	No				

Tap 'Yes' to open the 'Submit to Valkyrie' dialog:

Submit to Valkyrie	×
Please sign in with Comodo License Account credentials to analyze files with Valkyrie	Please sign up to Valkyrie if you don't have a Valkyrie account yet
Enter User Name	Valkyrie is a cloud-based file analysis service for submitted known and unknown files with a range of static and dynamic detectors including file lookup,
Enter Password	heuristics and real-time behaviour analysis
or	
The Science And Science St. The art Manual	
ОК	Sign Up

Existing users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.

You can also find your license key by logging in at https://accounts.comodo.com/.and visiting https://accounts.comodo.com/valkyrie/management

Please note that you will be able to view results in 'Valkyrie analysis results' only after the tool provides a verdict on scan results.

COMODO Creating Trust Online Unknown File Hunter		_ 🗆 ×
🕟 Start Scan 🥤 Analyze with Valkyrie 📧 Stop Scan	Reports - 🛞 Options (1) Help - 🔎	earch
Scan results Valkyrie analysis results	Group by Computers	Group by Files
Bibcef.dll (Chromium Embedded Framework (CEF) Dynamic Link Library) Instance.	62 MB Not Analyzed (Exceed size li	No
▷ Swscale-4.dll 1 instance.	647 KB Clean	No
 avfilter-6.dll 1 instance. 	2 MB Clean	No
 winunivappfeatures.dll (winunivappfeatures) 1 instance. 	97 KB No Threat Found	No
 avformat-57.dll 1 instance. 	2 MB Clean	No
Please click here to	o see the detailed results	
1 Unknown files, 0 Malicious files (1 of 2 Computers scanned)		

Refer to the section 'Analyzing Files with Valkyrie' and 'Scan Results' for more details.

3.3 Scan Computers by Network Addresses

Comodo UFH allows administrators to scan computers by specifying their IP address or hostname.

COMODO Creating Trust Online*

COMODO Creating Trust Online	Unknown File Hunter					C	
Start Scan	Analyze with Valkyrie	Stop Scan	(d) Reports *	Options	(i) Help *	O Search	
				Start Scar Select Scar	n Wizard n Targets		×
				· · ·	+ Activ	e Directory	 Network Addresses
		No scans hav	e heen nerformed ist		scar selecti	ng them from ve Directory	scan computers by specifying IP addresses or endpoint names
			Scan Now	+ ["		nelon tou an	This Computer
					Scan selection W	computers by ng them from lorkgroup	Scan this computer
							Cancel
	This product	s just one part of Como	odo ONE productivity	and revenue genera	tion		
	engine. To g	et more AWESOME pro	ducts for FREE, please	visit one.comodo.co	m		

To open the 'Start Scan Wizard', click the 'Start Scan' button at the top-left or the 'Scan Now!' link in the main display area.

Click 'Network Addresses'

Start Scan Wizar	d	×
	Network Addresses	
	5	Add
	10.108.51.100	Remove
		Remove All
Back		Next



- Network Address: Enter the IP address, IP range or host name as shown below:
 - IP 10.0.0.1
 - IP Range 10.0.0.1-10.0.0.5
 - IP Subnet 10.0.0.0/24 or 10.0.0.0/255.255.255.0
 - Computer Name Home Computer
- Click the 'Add' button

The specified item will be added and displayed. Repeat the process to add more endpoints. To delete an item from the list, click the 'Remove' button beside it.

Click 'Next' to continue.

•

- Login to the target device using either use the existing administrator credentials, or with custom credentials.
- Next, click either the 'Quick Scan' or 'Full Scan' button to start the scan.
 - · Quick Scan: Scans critical and commonly infected areas of target endpoints
 - Full Scan: Scans all files and folders on target endpoints.

COMODO Creating Trust Online	Unknown File Hunter	(Starting scan))			_ 🗆 ×
● Start Scan	🌈 Analyze with Valkyrie	Stop Scan	🕪 Reports •	Options	(i) Help +	Search
Scan results Val	kyrie analysis results					
Name						▼ Size
DESKTOP-TTPO Enumerating auto	9PR (10.108.51.100) oruns: 1005					
						N
						6
0 Unknown files, 0 Mal	licious files (0 of 1 Computers sca	nned)				

The scan will begin after UFH successfully connects to the device.

Click the 'Stop Scan' button if you want to discontinue the scanning process.

The notification bar at the bottom displays the number of unknown and malware programs detected, the number of endpoints scanned, the accessibility to the computers, scan progress details and more. Full results will be displayed after the scan finishes.

COMODO Creating Trust Online*

COMODO Creating Trust Online Unknown File Hunter	_ 🗆 ×
🕟 Start Scan 🥒 Analyze with Valkyrie 💿 Stop Scan 🌰 Reports - 🎯 Options 🕧 Help - 🔎	Search 🕻
Scan results Valkyrie analysis results Group by Computers Name	Group by Files
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1472. Unknown files: 1. Malicious files: 0.	
⑦ c:\program files\freedownloadmanager.org\free download manager\qt5qml.dll	2 MB
C∴Program Files (x86)\OpenOffice 4\program\unopkg.exe	11 KB
c:\program files\freedownloadmanagecorg\free download manager\common.dll	416 KB
c:\program files\freedownloadmanager.org\free download manager\imageformats\ojpeg.dll	234 KB
c.\program files\freedownloadmanager.org\free download manager\libcetdll	62 MB
c:\program files\freedownloadmanager.org\free download manager\swscale-4.dll	647 KB
C.\program files\freedownloadmanager.org\free download manager\avfilter-5.dll	2 MB
C\program files\freedownloadmanager.org\free download manager\winwfpmonitor.exe	829 KB
c:\program files\freedownloadmanager.org\free download manager\sqldrivers\qsqlite.dll	866 KB
Please click here to see the detailed results 1 Unknown files, 0 Malicious files (1 of 1 Computers scanned)	

You will also be given the opportunity to analyze unknown files with Valkyrie.

COMODO Creating Trust Online Unknown File Hunter					_ 🗆 ×
🕟 Start Scan 🍼 Analyze with Valkyrie	💿 Stop Scan	🐽 Reports - 🌘	Options (i) Help -	₽ Search
Scan results Valkyrie analysis results		Size	Grou Verdict	up by Computers	Group by Files Trusted Vendor
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 4. Unknown files: 1. Mai	licious files: 0. Trusted/Clea	n files: 3.			
					2
	Please click here to	see the detailed res	sults		
1 Unknown files, 0 Malicious files (1 of 1 Computers sca	anned)				

For each endpoint that was successfully scanned, you'll see total number of files scanned and the number of unknown and malware files found. Results can be viewed in two ways:

Group by Computer: Shows the total number of computers scanned and the number of unknown files found in those computers.

Group by File: Shows the name and quantity of each unknown file.

The option to analyze the results with Valkyrie will also be displayed:

Scan I	Results		\times
(Scan Complet Do you want to a Valkyrie? Scan Summary: 1 Total Scan Attemp - 1 Successful Scan Threat Detection Sc 12 Total Threats Fo - 4 Unknown Files - 8 Lookup in Progr * 12 files have uniq	ted! analyze unknown files ots s ummary: und* ress ue hash values	with
	Yes	No	

Click 'Yes' to open the Valkyrie options dialog.

Existing users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.

You can also find your license key by logging in at https://accounts.comodo.com/ .and visiting https://accounts.comodo.com/valkyrie/management

Refer to the section 'Analyzing Files with Valkyrie' and 'Scan Results' for more details.

3.4 Scan Local Computer

Comodo UFH allows you to scan your local device for unknown files. You can scan your device with a quick scan, full scan or custom scan.

COMODO Creating Trust Online



To open the 'Start Scan Wizard', click the 'Start Scan' button at the top-left or the 'Scan Now!' link in the main display area.

Click 'This Computer'

Start Scan Wizard			×
Select Scan Targets			
+ + And Sc sel	ctive Directory an computers by	Network Addresses Scan computers by specifying IP addresses or endpoint names	
+ : Sc sel	Workgroup an computers by ecting them from Workgroup	This Computer Scan this computer	
		Cancel	

The three scan types will open.

COMODO Creating Trust Online



• Select the endpoints that you want to scan and choose one of the following scan types:

Quick Scan: Scans critical and commonly infected areas of target endpoints

Full Scan: Scans all files and folders on target endpoints.

Custom Scan: Scans selected files or folders.

If you choose the 'Quick' or 'Full Scan' options then the scan will begin immediately. If you select 'Custom Scan', then you should next choose the directories and files you wish to scan in the 'Select Directories' screen:

COMODO Creating Trust Online

Start Scan Wiz	ard	×
	Select Directories	
	 \$WINDOWS.~BT Documents and Settings inetpub OpenSSL-Win32 PerfLogs Program Files Program Files (x86) ProgramData 	
Back	Recovery Scan critical areas of computer which are most often targeted by malware Scan	

- Select 'Scan critical areas...' to scan frequently targeted areas of your computer in addition to the items in your custom scan.
- Click 'Scan' to begin the scan.

COMODO Creating Trust Online*

COMODO Creating Trust Online	Unknown File Hunter	(Starting scan))			_ 🗆 ×
● Start Scan	🌈 Analyze with Valkyrie	Stop Scan	🐽 Reports •	Options	(i) Help +	Search
Scan results Val	lkyrie analysis results					
Name						▼ Size
DESKTOP-TTPO Enumerating aut	9PR (10.108-51.100) Joruns: 1005					
						Ν
						ν <u>σ</u>
0 Unknown files, 0 Ma	licious files (0 of 1 Computers sca	nned)				

- The scanning of endpoint(s) will start.
- Click the 'Stop Scan' button to discontinue the scanning process and confirm it in the 'Stop Scan' dialog.
- The notification bar at the bottom displays the number of unknown and malware programs detected, the number of endpoints scanned, the accessibility to the computers, scan progress and more. Full results will be displayed after the scan finishes. You will also be given the opportunity to analyze unknown files with Valkyrie.

COMODO Creating Trust Online*

COMODO Creating Trust Online Unknown File Hunter	_ 🗆 ×
▶ Start Scan 🧳 Analyze with Valkyrie 💿 Stop Scan 🌰 Reports 🔹 🎯 Options (i) Help •	🔎 Search
Scan results Valkyrie analysis results Group by Computers	Group by Files
Name	▼ Size
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1541. Unknown files: 5. Malicious files: 0.	
WIN-EV5SB4NSROI (10.108.51.242) Login problem: invalid username or bad password.	
Please click here to see the detailed results	
1 Unknown files, 0 Malicious files (1 of 2 Computers scanned)	

The details of results will be displayed in the respective endpoint rows, providing information such as the total number of programs scanned, number of unknown files, number of malware found and number of files that are failed to analyzed. There are results will be displayed in two ways:

For each endpoint that was successfully scanned, you'll see total number of files scanned and the number of unknown and malware files found. Results can be viewed in two ways:

Group by Computer: Shows the total number of computers scanned and the number of unknown files found in those computers.

Group by File: Shows the name and quantity of each unknown file.

The option to analyze the results with Valkyrie will also be displayed:

COMODO Creating Trust Online*

Scan Results X		
(Scan Completed! Do you want to analyze Valkyrie? Scan Summary: 2 Total Scan Attempts - 1 Successful Scans - 1 Failed Scans	unknown files with
	Threat Detection Summary: 5 Total Threats Found* - 5 Unknown Files * 5 files have unique hash v	alues
	Yes	No

Existing users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.

COMODO Creating Trust Online*

COMODO Creating Trust Online Unknown File Hunter			_ 🗆 ×		
🕟 Start Scan 🏾 🍼 Analyze with Valkyrie 💿 Stop	Scan 🐽 Reports - 🛞 C	Options 🧻 Help - 🔎	Search		
Scan results Valkyrie analysis results		Group by Computers	Group by Files		
Name	Size	Verdict	Trusted Vendor		
b libcef.dll (Chromium Embedded Framework (CEF) Dynamic Link Li 1 instance.	brary) 62 MB	Not Analyzed (Exceed size li	No		
 Swscale-4.dll 1 instance. 	647 KB	Clean	No		
 Instance, 	2 MB	Clean	No		
 winunivappfeatures.dll (winunivappfeatures) 1 instance. 	97 KB	No Threat Found	No		
 I instance. 	2 MB	Clean	No		
Please click	Please click here to see the detailed results				
1 Unknown files, 0 Malicious files (1 of 2 Computers scanned)					

You can also find your license key by logging in at https://accounts.comodo.com/ and visiting https://accounts.comodo.com/valkyrie/management

3.5 Analyze Files with Valkyrie

Valkyrie is a cloud based file analysis system that is completely different from the conventional signature based malware detection technique. The uploaded files are analyzed dynamically and statically. The dynamic process includes the run-time behavior and static process includes analyzing the file's binary properties extracted from it such as its sections, entropy , packer type and many more. Any deviation from the expected values in these features provides the clue about the nature of the file.

The UFH uses the Comodo's file look up service to identify files with its huge database of blacklisted and whitelisted files. If the files analyzed by the UFH tool is not available in either of these blacklist or whitelist, then they are categorized as 'Unknowns'. The administrator then has the option to submit the UFH tool detected unknown files with Valkyrie for an in-depth analysis including run-time behavior of the submitted files.

To submit the UFH tool detected unknown files with Valkyrie for analysis, click 'Yes' in the 'Scan Completed! Do you want to analyze files Valkyrie?'. This dialog appears after a scan is completed and displays the details of the scan including the number of malware and unknown files detected.

COMODO Creating Trust Online*

Scan Results X			
(!)	Scan Completed!		
Ŭ	Do you want to analyze unknown files with Valkyrie?		
	Scan Summary:		
	1 Total Scan Attempts		
	- 1 Successful Scans		
	Threat Detection Summary:		
	42 Total Threats Found*		
	- 0 Unknown Files		
	- 42 Lookup in Progress		
	* 42 files have unique hash values		
	Ves No		

The detected files will be submitted to Valkyrie for an in-depth analysis and the progress will be displayed. The main interface will now have two tabs - one showing the results of UFH tool analysis and the the other for Valkyrie.

After the analysis is completed the results are displayed under the 'Valkyrie analysis results' tab.

COMODO Creating Trust Online*

COMODO Creating Trust Online Unknown File Hunter	_ 🗆 ×
🕟 Start Scan 🥑 Analyze with Valkyrie 💿 Stop Scan 🌰 Reports - 🎯 Options (1) Help - 🔎	Search
Scan results Valkyrie analysis results Group by Computers Name	Group by Files T Size
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1472. Unknown files: 1. Malicious files: 0.	
Please click here to see the detailed results	
1 Unknown files, 0 Malicious files (1 of 1 Computers scanned)	

Both results can be displayed in two ways:

Group by Computer: Shows the total number of computers scanned and the number of unknown files found in those computers.

Group by File: Shows the name and quantity of each unknown file.

COMODO Creating Trust Online*

COMODO Creating Trust Online Unknown File Hunter		_ 🗆 X
🕟 Start Scan 🧳 Analyze with Valkyrie 🔳 Sto	o Scan 🍓 Reports 🔹 🍥 Options	(i) Help * P Search
Scan results Valkyrie analysis results Name	Size Verdi	Group by Computers Group by Files
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1. Unknown files: 1. Malicious files: 0.		
Diana di	k have to ease the datailed results	
1 Unknown files, 0 Malicious files (1 of 1 Computers scanned)	k here to see the detailed results	

The results displays the details such as the name of the file, its size, the scanning verdict and more. Refer to the section 'Valkyrie Analysis Results' for more details.

4 Scan Results

After the scanning process is completed, the results will be displayed in the main interface. The unknown files detected by the UFH tool are displayed under the 'Scanning results' tab. If the files are submitted to Valkyrie, then its results will be displayed under the 'Valkyrie analysis results' tab.

COMODO Creating Trust Online*

COMODO Creating Trust Online Unknown File Hunter	_ 🗆 ×
💽 Start Scan 🧳 Analyze with Valkyrie 💿 Stop Scan 👜 Reports - 🎯 Options 👔 Help - 🖌	Search
Scan results Valkyrie analysis results Group by Computers Name	Group by Files T Size
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1472. Unknown files: 1. Malicious files: 0.	
⑦ c\program files\freedownloadmanager.org\free download manager.qtSqml.dll	2 MB
C1/Program Files (x85)\OpenOffice 4\program\unopkg.exe	11 KB
c:\program files\freedownloadmanage.org\free download manager\common.dll	416 KB
c:\program files\freedownloadmanage.org\free download manager\imageformats\qjpeg.dll	234 KB
c:\program files\freedownloadmanager.org\free download manager\libcefdll	62 MB
c:\program files\freedownloadmanager.org\free download manager\swscale-4.dll	647 KB
© c:\program files\freedownloadmanager.org\free download manager\avfilter=5.dll	2 MB
c:\program files\freedownloadmanager.org\free download manager\winwfpmonitor.exe	829 KB
c:\program files\freedownloadmanager.org\free download manager\sqldrivers\qsqlite.dll	866 KB
Please click here to see the detailed results	
Fondowr mes, o wantous mes (For F computers scanned)	

Refer to the following sections for more details:

- Comodo Unknown File Hunter Scan Results
- Valkyrie Analysis Results

4.1 Comodo Unknown File Hunter Scan Results

The results of the Comodo UFH tool scan will be displayed in the 'Scanning results' tab in the main display area. The scan results are provided for each computer that the UFH tool has scanned including the name of the computer and the name of the detected files in them.

To view the UFH tool scan results, click the 'Scanning files' tab

COMODO Creating Trust Online*

COMODO Creating Trust Online Unknown File Hunter	_ 🗆 ×
🕟 Start Scan 🥑 Analyze with Valkyrie 💿 Stop Scan 🌰 Reports - 🎯 Options (1) Help - 🔎	Search
Scan results Valkyrie analysis results Group by Computers Name	Group by Files T Size
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1472. Unknown files: 1. Malicious files: 0.	
Please click here to see the detailed results	
1 Unknown files, 0 Malicious files (1 of 1 Computers scanned)	

• Click on the arrow beside each endpoint to expand and view the details of detected files in it such as the location, its name and so on.

COMODO Creating Trust Online*

COMODO Creating Trust Online Unknown File Hunter	_ 🗆 ×
Start Scan Analyze with Valkyrie Stop Scan Reports Scan results Valkyrie analysis results Name	Group by Files
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1472, Unknown files: 1. Malicious files: 0.	
c:\program files\freedownloadmanager.org\free download manager\qt5qml.dll	2 MB
C:\Program Files (x86)\OpenOffice 4\program\unopkg.exe	11 KB
c:\program files\freedownloadmanager.org\free download manager\common.dll	416 KB
c:\program files\freedownloadmanager.org\free download manager/imageformats\qjpeg.dll	234 KB
c:\program files\freedownloadmanager.org\free download manager\libcetdll	62 MB
c:\program files\freedownloadmanager.org\free download manager\swscale-4.dll	647 KB
c:\program files\freedownloadmanager.org\free download manager\avfilter-6.dll	2 MB
c:\program files\freedownloadmanager.org\free download manager\winwfpmonitor.exe	829 KB
c:\program files\freedownloadmanager.org\free download manager\sqldrivers\qsqlite.dll	866 KB
Please click here to see the detailed results	
1 Unknown files, 0 Malicious files (1 of 1 Computers scanned)	

Searching, sorting and filtering Options

Searching Option

• To search for a particular endpoint, enter its name or IP address partially or fully in the 'Search' box at the top right

The items that match the search criteria will be displayed.

COMODO Creating Trust Online Unknown File Hunter	_ 🗆 ×
💽 Start Scan 🧳 Analyze with Valkyrie 💿 Stop Scan 🌰 Reports - 🚳 Option	s (j) Help · Pttp ×
Scan results Valkyrie analysis results Name	Group by Computers Group by Files
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1472. Unknown files: 1. Malicious files: 0.	
Please click here to see the detailed results	
1 Unknown files, 0 Malicious files (1 of 1 Computers scanned)	

• To display all the endpoints again, clear the search box.

Sorting Option

· Click on the 'Name' column header to sort the endpoints in ascending/descending order

COMODO Creating Trust Online*

• To sort the files in ascending/descending order according to its name and size, expand the endpoints to display the detected files and click on the 'Name' and 'Size' column headers

Filtering Option

• Click the funnel icon 🗵 at the end of 'Name' column

۲	Size
In Progres	55
Canceled	
Complete	d
Failed	
Offline	
	Clear Filter

- Select the filter criteria from the options
 - In Progress Displays the endpoints in which the scanning is in progress
 - Canceled Displays the endpoints for which the scanning was canceled
 - Completed Displays the endpoints for which the scanning was completed
 - · Failed Displays the endpoints for which the scanning failed
 - Offline Displays the endpoints that have gone offline during the scanning process
- If the filter icon is in blue color 🔰 , it indicates filter(s) are applied
- To display all the endpoints again, click 'Clear Filter'

To view the details of file, double click on the file from the list.

COMODO Creating Trust Online*

COMODO Creating Trust Online Unkr	nown File Hunter		_ 🗆 X
Start Scan An Scan results Valkyrie analy Name	alyze with Valkyrie 💿 Stop Scan	Reports • (6) Options (1)	Help • Pttp X avy Computers Group by Files T Size
DESKTOP-TTPO9PR (10.10 Completed: Total files scanne Comprogram files\freedownlo	8.51.100) ed: 1472. Unknown files: 1. Malicious files: 0. admanager.org/,free/download/manager/.qtSqml.d	1	2 MB
© Details			×
© c qt5q	ml.dll		В
File Nar Verdict:	ne: qt5qml.dll Clean	Hash (SHA1): B70C854D19AB Signer: n/a	16F50B4DD5F5771F B
Created Modifie	 10/13/2016 1:50:29 PM 3/3/2016 7:26:46 PM 	Version: 5.6.0.0 Copyright: Copyright (C) 20	115 The Qt Company
© c Accesse	d: 10/13/2016 1:50:29 PM	Product: Qt5	8
1 Unknown files, 0 Malicious file	Please click here to s (1 of 1 Computers scanned)) see the detailed results	Close

The details of the file include SHA1 hash value, file name, its size, version no and so on.

• Click the 'Close' button to return to the scan results screen.

4.2 Valkyrie Analysis Results

The 'Valkyrie analysis results' tab will be available only if the administrator has opted to submit unknown files to Valkyrie for in-depth analysis. Refer to the sections 'Scanning Computers' and 'Analyzing Files with Valkyrie' for more details about scanning endpoints and about Valkyrie.

To view the Valkyrie scan results, click the 'Valkyrie analysis results' tab.

COMODO Creating Trust Online*

COMODO Creating Trust Online Unknown File Hunter					_ 🗆 X
🕟 Start Scan 🍼 Analyze with Valkyrie	Stop Scan	leports +	Options	(i) Help *	₽ Search
Scan results Valkyrie analysis results Name		Si	ze Verdict	Group by Computers	Group by Files Trusted Vendor
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1. Unknown files: 1. Malicio	ous files: 0.				
<u>PI</u>	lease click here to	o see the detailed	results		
1 Unknown files, 0 Malicious files (1 of 1 Computers scann	ned)				

Sorting option

· Click on a column header to sort the results in ascending/descending order

The details of computer(s) that is affected by a file and its location can be viewed by clicking the arrow beside each file.

COMODO Creating Trust Online*

COMODO Greating Trust Online Unknown File Hunter			_ 🗆 ×
Start Scan Analyze with Valkyrie Stop Scan	👜 Reports - 🍥 Oj	ptions (i) Help • P	ttp X Group by Files
Name	Size	Verdict	Trusted Vendor
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1. Unknown files: 1. Malicious files: 0.			
C\program files\freedownloadmanager.org\free download manager\winuniv	appfeature 97 KB	No Threat Found	No
Please click here to s	ee the detailed results		
1 Unknown files, 0 Malicious files (1 of 1 Computers scanned)			

Valkyrie Analysis Results - Table of Column Descriptions					
Column Header	Description				
Name	The name of the file. The icon ¹ beside a file indicates a malware file.				
Size	The size of the analyzed file				
Verdict	The result of Valkyrie analysis of a file. Indicates if the file is a malware or safe.				
Status	The file has been successfully analyzed by Valkyrie				
White Listed	Indicates whether the file has been whitelisted after the manual review. Even if a program is marked as whitelisted, it will be detected again during the next scan but shown as whitelisted.				

The bottom of the Valkyrie results page shows a short summary of the unknown programs and malware discovered by the scan. It also shows the number of computers scanned.

The 'Valkyrie' website at https://valkyrie.comodo.com provides detailed results for the scans that are run and includes the following options:

- Submit the files for manual analysis
- View detailed information about each file
- Download the result for each in PDF format
- View detailed information about each detected file from VirusTotal.com website

To view the detailed results, click the 'Please click here to see the detailed results' link at the bottom of the results

COMODO Creating Trust Online

interface.

Please click here to see the detailed results
1 Unknown files, 0 Malicious files (1 of 1 Computers scanned)

You will be navigated to the Valkyrie website login page at https://valkyrie.comodo.com

VALKYRIE	IGN IN 🔿
Welcome to Valkyrie	
Login to your account Login (Email or Username) Password Remember Me Don't have an account yet ? Greate an account Forgot your password ? Click here	
® Valkata Comodo Group Joc 2016. All cipher researed	

- If you do not have an account, click the 'Create an account' link, provide the required details and sign up for an account, which is free.
- If you already have an Valkyrie account, enter the credentials and click the 'Sign In' button.

The 'Dashboard' page will be displayed by default.

ES VA	LKYRIF					John None	0	
	соморо					(Unlicemas)	d Liser)	
Automate	d Analysis Sys	tem						
If you have a Port	table Executable (PE) file	(.exedll, .ays etc) that you would	d like to be analysed, p	lease upload it usin	ng the form below. Within secon	ids, detailed detection results will be		
displayed in the '	Static' and 'Dynamic' tab	is. Users will also see an 'overall' s	ecurity verdict for the	file prominently dis	splayed at the top of the page.			
						DOWNLOAD VALKYRIE HUNTER	•	
YOUR RECENT ANALYSIS R	EQUESTS			Total # of files 22	s Total#ofClean Total#ofU 10 7	nknown Total#ofMalware Total#in 5	Human Expert An 0	alysis
My All Products	FILTER T							
My All Products	FILTER T							
My All Products	FILTER T					Search:		
My All Products Show 25 • entries	HLTER T					Search:		
My All Products • Show 25 • entries File Name :	RLTER T	6 SHAT 0	Last Activity 💡	Final Verdict	8 Human Expert Verdict 6	Search: Human Expert Analysis Status :	Actions	
My All Products • Show 25 • entries File Name 9 N56N5c10.104.84.21W5ceN3eN5.	Path	6 SHA1 6 e801005700375611aaad	Last Activity y 2015-12-24 06:19:51	Final Verdict d	Human Expert Verdict Clean	Search: Human Expert Analysis Status & Analysis Completed	Actions	
My All Products Show 25 • entries File Name MScHSct0.10L68.21WScH0.3485. Setup-VideoBox-3.0exe	HLTER Y	6 SHA1 6 +9610057603764d1xaad 4e3115624635e0b70cd6	Last Activity ¥ 2015-12-24 09:19:51 2015-12-24 09:19:19	Final Verdict Clean Oean	E Human Expert Verdict & Clean	Search: Human Expert Analysis Status - Analysis Completed Analysis Completed	Actions	
My All Products Show 25 antrias File Name MscHoct0.104.09.21MSceH3aHS. Setup-Vide080x-3.0exe MscHoct0.104.69.21MSccH3aHS.	Path	5 SHA1 0 #601005790375631aaad 4e31156246296b70cd6 3e5644c734182296344a	Last Activity v 2015-12-24 08:19:51 2015-12-24 08:19:07 2015-12-24 08:19:07	Final Verdict d Gean Gean	Human Expert Verdict Clean Clean Clean Clean	Search: Human Expert Analysis Status 1 Analysis Completed Analysis Completed Analysis Completed	Actions	
My All Products • Show 25 • entries File Name StockSct0.104.85.2145ccH3a45. Setup-VideoBox-3.0exe Wi5CkSct0.104.68.2145ccH3a45. WinSCR.axe	Path	b SHA1 0 e6010057003756d1aaad 4e3115624639ebb70cd6 3e56467934187296344a ie073dfbcbe42526e073e e6073dfbcbe42526e073e 6073dfbcbe42526e073e	Last Activity v 2015-12-24 68:19:51 2015-12-24 68:19:19 2015-12-24 69:19:67 2015-12-24 69:19:67	Final Verdict of Clean Clean Clean Clean	Human Expert Verdict Clean Oean Olan	Search: Human Expert Analysis Status : Analysis Completed Analysis Completed Analysis Completed	Actions 8 2 9 3 9 3 9 3 8 3 8 3 8 3 8 3 8 3 8 3 8 3 8	
My All Products Show 25 • entries File Name MScHSct0.10L68.21WSccH3#MS. Setup-VideoBox-3.0exe MScKSct0.10L68.21WSccH3#MS. WHSCP.ase cst_installer_st&Lexe	Path	6 SHA1 6 w6010057003754d1aaand 4e3115624435eb070cd6 3e5644ef334187265344a x6973d1bcba425256073a b234b700d10ba8ts22saat b244b700d10ba8ts22saat	Last Artivity 2015-12-24 68:19:51 2015-12-24 68:19:19 2015-12-24 69:19:07 2015-12-23 15:45:55 2015-12-23 15:45:55	Final Verdict of Clean Oean Oean Clean Clean	Human Expert Verdict () Clean Oean Clean	Search: Human Expert Analysis Status i Analysis Completed Analysis Completed Analysis Completed	Actions 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	

Comodo Unknown File Hunter Admin Guide | © 2018 Comodo Security Solutions Inc. | All rights reserved.

COMODO Creating Trust Online

You can navigate to different pages of the website by clicking your account name on the top right side of the page.



- My Dashboard Provides details of each file that was submitted to Valkyrie for analysis, including its SHA1 signature, submitted date and more. Refer to the section 'Dashboard' for more details.
- My Stats Provides the summary of files analyzed by Valkyrie for your account. Refer to the section 'Valkyrie Usage Statistics' for more details.
- Activity Logs Provides the Valkyrie account usage details such as date and time of login, the source IP of the computer used to login and more. Refer to the section 'Activity Logs' for more details.
- My APT Scans The scan start and end date, number of files scanned, queried files, uploaded files, cleaned files and malware files and the actions that can be performed for each scan information.
- Unparalleled Protection Provides statistics with monthly details of total number of malware files that were
 not detected by previous vendor and AV industry.
- Weekly Unknown Stats Provides graphical representation of Malware and unknown files.
- Settings This option displays the details of the user and portal.
- Log Out Allows you to log out of your account.

Dashboard

The 'Dashboard' page of Valkyrie displays the details of analysis for the files submitted. From this page, you can view the download auto analysis report, view details of static analysis, view details of dynamic analysis and more.

Click 'My Dashboard'

The details of each analyzed file will be displayed in the table. The number of items to be displayed on each page can be selected from the 'Show entries' option on the left.

COMODO Creating Trust Online*

VA 💕	LKYRIE					John None Dinitemes	(User)
Automated	d Analysis Svs	tem					
If you have a Portu displayed in the 'S	able Executable (PE) file tatic' and 'Dynamic' tab	e (.exedll, .zys etc) that you would is. Users will also see an 'overall' s	d like to be analyzed, p ecurity verdict for the f	lease upload it usin lie prominently dis;	g the form below. Within secon played at the top of the page.	ds, detailed detection results will be	
						DOWNLOAD VALKYRIE HUNTER	•
YOUR RECENT ANALYSIS RE	QUESTS			Total # of files	Total#of Gean Total#of Un	iknown Total#ofMalware Total#in 5	Human Expert Analysis
My All Products •	FILTER T					Search:	
My All Products Show 25 entries File Name	FILTER T Path	ó SHAT ⇒	Last Activity 💡	Final Verdict	Human Expert Verdict 🗄	Search: Human Expert Analysis Status :	Actions
My All Products Show 25 entries File Name Strokestro.106.49.2145cce43.2445	RLTER Y	6 SHA1 6 +961005/7603/Md1aaad	Last Activity ¥ 2015-12-24 06:19:51	Final Verdict d	Human Expert Verdict \diamond Clean	Search: Human Expert Analysis Status : Analysis Completed	Actions O
My All Products • Show 25 • entries File Name 0 %56%510.104.69.21%55cr%12%54. Sebup-VideoBox-3.0.exe	RLTER Y	6 SHA1 6 +6610057603766d1aaad 4e3115624635e0b70cd6	Last Activity ¥ 2015-12-24 08:19-51 2015-12-24 08:19:19	Final Verdict d	Human Expert Verdict & Clean Osan	Search: Human Expert Analysis Status - Analysis Completed Analysis Completed	Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Act
My All Products • Show 25 • entries File Name 0 %5c%5c10.104.69.21%5cc%3a%5 5 Setup-VideoBox-3.0.exe %5c%5c10.104.69.21%5cc%3a%5	PLTER T	5 SHA1 0 #601005700375631641aaad 4e31156246290b70006 3e5644073418296344a	Last Activity v 2015-12-24 08:19:51 2015-12-24 08:19:19 2015-12-24 08:19:07	Final Verdict d Gean Gean	Human Expert Verdict () Clean Clean Osan	Search: Human Expert Analysis Status 1 Analysis Completed Analysis Completed Analysis Completed	Actions 8 0 9 0 8 0 8 0
My All Products Show 25 • entries File Name StochSc10.104.69.2145cc43.345 Setup-VideoBo+3.0ese %Sc465c10.104.69.2145cc43.3455 WinSC4P.axe	Path	5 SHA1 8 #601005760375631aaad 4e3115624629ebb70od6 3e5644934187296344a 6073dfbcbe425266073e 6073dfbcbe425266073e 6073dfbcbe425266073e	Last Activity 2013-12-34 98:19:51 2015-12-34 98:19:19 2015-12-34 98:19:07 2015-12-24 98:19:07 2015-12-23 15:46:56	Final Verdict d Clean Clean Clean Clean	Human Expert Verdict 0 Clean Clean Clean	Search: Human Expert Analysis Status 1 Analysis Completed Analysis Completed Analysis Completed	Actions
My All Products Show 25 • entries File Name MS5085c10.104.69.21055c93.305. Setup-VideoBor-3.0.exe WS5085c10.104.69.21055c93.305. WinS5085c10.104.69.21055c93.305. WinS5085c10.104.69.21055c93.305.	Path	5 SHA1 8 e601005760375631aaad 4e3115624639eb070cd6 3e5644ef3341872963443 e8730fbcbe42525e6073a 5234b70od10688c523a6 5234b70od10688c523a6	Last Activity v 2015-12-24 08:19:51 2015-12-24 08:19:19 2015-12-24 09:19:07 2015-12-23 15:49:50 2015-12-23 15:49:50	Final Verdict d Clean Clean Clean Clean Clean	Human Expert Verdict © Clean Clean Clean	Search: Human Expert Analysis Status I Analysis Completed Analysis Completed Analysis Completed	Actions

The summary of analysis requests and results are displayed at the top of the table.

Sort and search options

Sorting the entries

• You can sort the items in ascending/descending order by clicking on the column headers.

Searching for particular item(s)

- Enter the details partially or fully in the search field on the top right side. You can search for items based on all columns except the 'Actions' column.
- To display all the entries again, clear the search field.

	Valkyrie Detailed Analysis Results - Table of Column Descriptions
Column Header	Description
File Name	The name of the submitted file
Path	The IP of the endpoint and the file's path details
SHA1	The SHA1 hash value of the file.
Last Activity	The date and time the last activity of analysis was performed.
Final Verdict	 The Valkyrie dynamic and static analysis results for the file. The results available are: Clean - The file is 99.9% safe to run No Threat Found - No malware found in the file, but cannot say it is safe to run Malware - The file is a malware and should not be run
Human Expert Verdict	 The results of the file after Human expert analysis: Clean - File is safe to run Malware - The file is a malware file Potentially Unwanted Application (PUA) - Applications such as Adware, Spyware and so on No Threat Found - No malware found in the file, but cannot say it is safe to run

	 Not Ready - Indicates manual analysis of the file is in progress
Human Expert Analysis Status	Indicates the status of files submitted for Human Expert analysis. The statuses are: In Queue - The analysis has not started
	 In Progress - The analysis has started and in progress
	 Analysis Completed - The analysis is completed and verdict displayed under the 'Manual Verdict' column
	• Objected - Indicates the user wants a re-analysis of the file. If the user thinks that the initial manual verdict for the file is wrong, he/she can submit it again for another manual analysis.
	Objection Completed - Indicates the manual re-analysis is completed.
Actions	The available actions are:
	• View Info - You can view the complete details of the results for the file such as summary, static analysis, dynamic analysis and file details. Refer to 'File Analysis Results' for more details.
	- Download Automatic Analysis Report - Allows you to download the report in PDF format. Refer to 'Download Automatic Analysis Report' for more details.
	- View Virus Total Result - Takes you to the Virus Total website that displays its results for the file. Refer to 'View Virus Total Results for the File' for more details.
	- Send to Manual Analysis - Allows you to submit the file for manual analysis by Comodo technicians. Refer to 'Send the File for Manual Analysis' for more details.

File Analysis Results

Click the 'View Info' icon
 under the 'Actions' column for a file to view its detailed results

A new web page will open displaying the detailed results for the file.

Click the 'Summary' tab

COMODO Creating Trust Online*

Summer Soliti Analysis Dimenic Analysis Numan Depent Analysis Hie Details File Name: gent Analysis (big Dig intel B0566 Monol.Nac assembly, for MS Windows summer / pert P12 2056/101 // Dimentio B0200 Monol.Nac assembly, for MS Windows summer // P12 2056/101 // Dimentio B0200 Monol.Nac assembly, for MS Windows Subtra - end B05093334-451614498537722006/117 End Solitie (DUI) intel B0506 Monol.Nac assembly, for MS Windows summer // P12 2056/101 // Dimentio B0200 Monol.Nac assembly, for MS Windows Subtra - end B05093334-451614498537722006/117 End Solitie (DUI) intel B0500 Monol.Nac assembly, for MS Windows summer // P12 2056/101 // Dimentio B0200 Monol.Nac assembly, for MS Windows Marke - Mark -	VALKYRIE		1	ohn None	
File Name: agent/uwatcherserviewase issues of table (0007) Intel #0006 Monor. Naet assembly. For MS Windows: issues of table (0007) Mast hased (16007) Monor. Naet assembly. For MS Windows: issues of table (0007) Mast hased (16007) Monor. Naet assembly. For MS Windows: issues of table (0007) Mast hased (16007) Monor. Naet assembly. For MS Windows: issues of table (0007) Mast hased (16007) Monor. Naet assembly. For MS Windows: issues of table (0007) Mast hased (16007) Monor. Naet assembly. For MS Windows: issues of table (0007) Mast hased (16007) Monor. Naet assembly. For MS Windows: issues of table (0007) Mast hased (16007) Monor. Naet assembly. For MS Windows: issues of table (0007) Mast hased (16007) Monor. Naet assembly. For MS Windows: issues of table (0007) Mast hased (16007) Monor. Naet assembly. For MS Windows: issues of table (0007) Mast hased (16007) Monor. Naet assembly. For MS Windows: issues of table (0007) Mast hased (16007) Monor. Naet assembly. For MS Windows: issues of table (0007) Mast hased (16007) Mast hased	Summary Static Analysis Dynamic Analysis Hu	uman Expert Analysis File Details			
ANALYSIS TWPE DATE VERDHCT Signature Based Detection 2015-09-17 20:59:10 No Match 0 Static Analysis Overall Verdict 2015-09-17 20:59:10 Highly Suspicious m Human Expert Analysis Overall Verdict 2015-09-17 20:59:10 Clean 0 File Certificator Validation 2015-09-17 20:59:10 Not Applicable 0	File Name: agentz-swatcherservice.exe File Type: FE32 encoutable (0UT) Intel 80386 Monor.Net assembly. for SHA1: e981866798578d1aaadc16a3c702ed5bd03b4cb MD5: be50278384a5161da055572205fa12f First Seen Date: 2015-09-12 2656c10 (7 months ago.) Number of Clients Seen: 7 Last Analysis Date: 2015-09-12 2656c10 (7 months ago.) Human Depert Analysis Date: 2015-12-24 10;4021 (3 months ago.) Human Depert Analysis Date: 2015-12-24 10;4021 (3 months ago.) Human Depert Analysis Date: 2016-12-24 10;4021 (3 months ago.) Human Depert Analysis Date: 2016-12-24 10;4021 (3 months ago.)	MS Windows	Valige	CRAAN Per Final Verdict	
ANALYSIS TYPE DATE VERDICT Signature Basied Detection 2015-09-17 20:06:10 No Match Image: Control	Analysis Summary				
Signature Based Detection 2015-09-17 20:09:10 No Match 20 Static Analysis Overall Verdict 2015-09-17 20:09:10 Highly Suspicious Image: Comparison of Compar	ANALYSIS TYPE	DATE	VERDICT		
Static Analysis Overall Verdict 2015-09-17 2058:10 Highly Suspicious # Human Expert Analysis Overall Verdict 2015-09-17 2058:10 Clean Image: Clean	Signature Based Detection	2015-09-17 20:56:10	No Match	0	%
Human Expert Analysis Overall Veralict 2015-09-17 2056:10 Clean File Certificate Validation 2016-04-04 17:30:33 Not Applicable	Static Analysis Overall Verdict	2015-09-17 20:56:10	Highly Suspicious	兼	
File Certificate Validation 2016-04-04 17:32:33 Not Applicable 🥹	Human Expert Analysis Overall Verdict	2015-09-17.20:56:10	Clean	۲	õ
	File Certificate Validation	2016-04-04 17:38:33	Not Applicable	0	
					×

Summary - The top section shows file details such as name, file type, and more. At the top right, the 'Valkyrie Final Verdict' is displayed. The details under 'Analysis Summary' displays the summary of the file analysis such as signature based detected, static analysis overall verdict and dynamic overall verdict for the file.

• To view the detailed results of static analysis of the file, click the 'Static Analysis' tab

VALKYRIE	Jahn Q	
Summary Static Analysis Dynamic Analysis Human Expert Analysis File Details		
File Name: agent_rvwatcherservice.exe File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows SHA1: e98186b798574d1aaadc16a3c762ed5b003b4cb MD5: be50979384a5161da0955772205fa12f First-Seen Date: 2015-09-17 2056:10 (7 months ago) Number of Clients Seen: 7 Last Analysis Date: 2015-09-17 2056:10 (7 months ago) Human Expert Analysis Date: 2015-12-24 18:40:21 (3 months ago) Human Expert Analysis Result: Clean Verdict Source: Valkyrie Human Expert Analysis Overall Verdict	Queen Valkyme Anal Verdict	
Static Analysis		
STATIC ANALYSIS OVERALL VERDICT	RESULT	
Highly Suspicious	*	8
DETECTOR	RESULT	B
Optional Header LoaderFlags field is valued illegal	Clean 🥑	•
Non-ascii or empty section names detected	Clean 🦁	
Illegal size of optional Header	Clean 🥑	

Static Analysis - Static process includes analyzing the file's binary properties extracted from it such as its sections, entropy , packer type and many more. Any deviation from the expected values in these features provides the clue about the nature of the file.

Scroll down the page to view static analysis overall verdict for the file as well as detailed result for each of the parameter checked for the file.

• To view the detailed results of dynamic analysis of the file, click the 'Dynamic Analysis' tab

COMODO Creating Trust Online*

Summary Static A	nalysis Dynamic Analysis	File Details	
Manual Analysis Result: N Aerdict Source: Valkyrie Au	io manual analysis verdict given itomatic Analysis	to this sample yet.	
Dynamic Analysi	s		
DYNAMIC ANALYSIS OVER	RALL VERDICT		RESULT
No Threat Found			0
SUSPICIOUS BEHAVIORS			
Has no visible windows			÷.
Behavioral Infori	mation		
QueryProcessAddr	ess		+
QueryFilePath			+
LoadLibrary			+

Dynamic Analysis - The dynamic process includes the run-time behavior of the file in an test environment. The page provides the dynamic analysis overall verdict and behavioral information for the file. Scroll down the page to view the detailed behavioral information for the file.

· To view the more details about the file, click the 'File Details' tab

Summary	Static Analysis	Dynamic Analysis	File Details		
le Name: libeay	32.dll			9	
le Type: PE32+ e	executable (DLL) (o	onsole) x86-64, for MS W	Andows		•
HA1: 946820b88	6ae2f1b62680417	3782df8c2f6ec74a		NO THREAT	FOUND
1D5: 1b934ad14l	bae56fd019c60dd0	66fadc1		Valkyrie Fina	al Verdict
rst Seen Date: 2	015-10-14 12:06:04	(5 days ago)			
umber of Clients	Seen: 1				
ast Analysis Date	: 2015-10-14 12:00	i:04 (5 days ago)			
lanual Analysis R	lesult: No manual	analysis verdict given to	this sample yet.		
erunce adulteer ve	ingrie Automatic A	110/3310			
dditional	File Inform	ation			
dditional PE Header	File Informa s	ation			
Additional @ PE Header ■ File Paths	File Informa	ation			+++++++++++++++++++++++++++++++++++++++
PE Header	File Informa s	ation	SEEN COUNT		+
Additional PE Header File Paths File Path on CL %56%5c10.108.17 (x88)%5cvmware	File Informa s JENT 7.106%Scc%3a%Sc; MScrmware+playe	ation rogram+files+ %5cx64%5clibeay32.dll	SEEN COUNT		+
dditional I PE Header File Paths File Path on CLI M5cW5c10.108.17 X80M5cvmware A PE Section	File Informa s JENT 7.106%Scc%3a%Sc MScrmware+playe	ation rogram+files+ %5cx54%5clibeay32.dll	SEEN COUNT		+ + +
Additional I PE Header File Paths File Path on CL N5cNSc10.108.17 X80/M5cvmware A PE Section A PE Import:	File Informa s IENT 7.100MSccW3aWScc MScrmware+playe	ation rogram+files+ %Scx64%Sclibeay32.dll	SEEN COUNT		+ + +

File Details - Provides additional file information such as the file path on the client machine, PE headers, PE sections and more. Scroll down the page to view the details file information.

Download Automatic Analysis Report

 Click the 'Download Automatic Analysis Report' icon the report in PDF format under the 'Actions' column for a file to download

COMODO Creating Trust Online

A new web page will open displaying the detailed results for the file.

VALKYRIE						
File Name: agent.rv.watcherservice.exe File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows SHA1: e98186b79857f4d1aaadc16a3c762ed5bd03b4cb MD5: be50979384a5161da0955772205fa12f First Seen Date: 2015-09-17 15:26:10 UTC Number of Clients Seen: 5 Last Analysis Date: 2015-09-17 15:26:10 UTC Manual Analysis Result: No manual analysis verdict given to this sample yet.						
Analysis Summary						
ANALYSIS TYPE	DATE	VERDICT				
Signature Based Detection	2015-09-17 15:26:10 UTC	No Match	0			
Static Analysis Overall Verdict	2015-09-17 15:26:10 UTC	Malware	₩			
Dynamic Analysis Overall Verdict	2015-09-17 15:26:10 UTC	No Threat Found	?			
Static Analysis						
STATIC ANALYSIS OVERALL VERDICT			RESULT			
Malware			- Ř			
DETECTOR		RESULT				
Optional Header LoaderFlags field is valued illegal		Clean	0			
Non-ascii or empty section names detected		Clean	0			
Illegal size of optional Header		Clean	0			
Packer detection on signature database		Unknown	0			
Based on the sections entropy check! file is possibly pa	acked	Clean	0			

The report contains the compiled results of the automatic analysis explained in the **File Analysis Results** section. Scroll down the page to view the full report and save it.

View Virus Total Results for the File

•

Virus Total, a subsidiary of Google, is a information aggregation website and one of its function is to aggregate output data of different antivirus engines, website scanners and so on. Valkyrie allows to get the details of the file from this website.

Click the 'View Virus Total Results' icon V under the 'Actions' column for a file to view the Virus Total analysis results for the file

The 'Virus Total' web page for the selected file will be displayed with its results.

COMODO Creating Trust Online

0	https://www.virustotal.com/en/file/199fa222bffd6	5989f5be16c19472f321217f85d94170171407689699a19cebe	c/analysis/
	 Community Statistics Documental 	tion FAQ About PEnglish	Join our community Sign in
		n burkisti ni hodo a newni ni dolar newnol o'w donaf gww.dewn s bronnin 1517 eu al o o deal un few down y ddwr	
	Virustotal	l	
	614.352 1006-3735-#400804Eb-s10-104	17791311317486.40.41701714076806500-10-shor	
	5194250. 155142220105505050505150416C154	121321211100004110111401003033813Celose	
	File name: TSServ.exe		a 3 a 2
	Detection ratio: 33 / 55		9 9 2
	Analysis date: 2015-07-09 00:28:02 UTC (3	months, 1 week ago)	
	□ Analysis Q File detail ≭ Relationships	Additional information P Comments Q Q Votes	
	C Analysis Q File detail 74 Relationships	Additional information P Comments Q Votes	
	I Analysis Q File detail ≭ Relationships Antivirus	Additional information P Comments Q Votes Result	Update
	I Analysis Q File detail ≭ Relationships Antivirus AVG	Additional information Comments O O Votes Result Tool F	Update 20150708
	Antivirus Avg Avg Avvare	Additional information Comments Q Q Votes Result Tool F Trajan Win32: Generic IBT	Update 20150708 20150709
	Antivirus	Additional information Comments Q Q Votes Result Tool.F Trojan Win32. Generic (BT Application. TrojanSimulator	Update 20150708 20150709 20150708
	Analysis Antivirus AVG AVware Ad-Aware AhnLab-V3	Additional information Comments Q Votes Result Tool.F Trojan.Win32.Generic18T Application.TrojanSimulator Win-AppCare/Trojansimulator	Update 20150708 20150709 20150708 20150708
	Analysis Analysis File detail Relationships AvG AVG AVware Ad-Aware AhnLab-V3 Activ_AVI	Additional information Comments O Votes Result Tool F Trojan Win32, Generic (BT Application, TrojanSimulator Win-AppCare/TrojanSimulator Win-AppCare/Trojansimulator Bit/Ware/Downloader rot-avging HE/H2000/221100	Update 20150708 20150709 20150708 20150708 20150708
	Antivirus Antivirus Avvare Ad-Aware AhnLab-V3 Antiv-AVL	Additional information Comments O Votes Result Tool.F Trojan.Win32: Generic:IBT Application.TrojanSimulator Win-AppCare/TrojanSimulator Win-AppCare/TrojanSimulator SkWare[Downloader.not-a-virus.HEUR]/Win32:LMN	Update 20150708 20150709 20150708 20150708 20150709
	Antivirus Avvare Ad-Aware Antukab-V3 Anty-AVL Arcabit	Additional information Comments O Votes Result Tool.F Trojan.Win32: Generic:IBT Application.TrojanSimulator Win-AppCare/TrojanSimulator Win-AppCare/TrojanSimulator RiskWare[Downloader.not-a-virus,HEUR]/Win32:LMN Application.TrojanSimulator	Update 20150708 20150709 20150708 20150708 20150709 20150709

Scroll down the page to view the results for the file from different antivirus engines.

Send the File for Manual Analysis

You can also send a file for manual analysis by Comodo malware specialists for more comprehensive inspection in addition to the automated process. This is premium service and users should subscribe for the same.

Click the 'Send to Manual Analysis' icon under the 'Actions' column to submit a file for manual analysis by Comodo engineers

A confirmation dialog will be displayed.



Click 'OK' to confirm

After the file is submitted for manual analysis, it will show as 'In Queue' under the 'Status' column and 'Unknown' under 'Manual Verdict'. The 'Send to Manual Analysis' icon also will not be available indicating the file is already submitted.

YOUR RECENT ANALYSIS REQU	IESTS			Total # of files Total 18	# of Clean Total # o 3	f Unknown Total # o 10	f Malware To 5	tal # In Manual Analy 0
Show 10 entries							Search:	
File Name	Path 🔅	SHA1 0	Source 🔅	Submit Date 💡	Auto Verdict	Manual Verdict	Status (Actions
JZipShell.dll	%5c%5 (x86)%	74e2e	Upload	2015-10-15 11:04:56	Clean	Unknown	In Queue	105
tsserv.exe	%5c%5	846c1	Upload	2015-10-14 12:48:51	Malware	Unknown	In Queue	100
ocsinventory-deploy-tool.exe	965c965 (x86)96 deploy-	e3fabf	Upload	2015-10-14 12:06:21	No Threat Found			

COMODO Creating Trust Online*

Valkyrie Usage Statistics

The 'My Valkyrie Usage Statistics' page of Valkyrie displays how many files are submitted for your account and displays the details for:

- Today Details of files submitted today
- This Week Details of files submitted for this week
- · This Month Details of files submitted for month
- All Time Total number of files submitted since account creation

To view your Valkyrie account usage statistics, click the 'My Stats' link



The usage statistics page will be displayed.

/ Portal	RIE USAGE S	TATIST	ICS						
Date	Total Files	Clean	Malware	Undetected	Automatic Analysis	Human Expert Analysis	Basic Info Req.	Full Info Req.	UI Get Info Req.
Today	1	1	0	0	0 (0)	0 (0)	0 (0)	0 (0)	1 (1)
This Week	1	1	0	0	0 (0)	0 (0)	0 (0)	0 (0)	2 (1)
This Month	1	1	0	0	0 (0)	0 (0)	0 (0)	0 (0)	2 (1)
All Time	22	10	5	7	19 (18)	6 (6)	234 (18)	0 (0)	23 (8)
Values inside	paranthesis rej	presents (unique numb	er of files in that	category.				

	My Valkyrie Usage Statistics - Table of Column Descriptions				
Column Header	Description				
Date	Indicates the period of usage				
Total Files	Number of files submitted for the period				
Clean	Number of files found to be clean				
Malware	Number of files found to be malware files submitted				
Undetected	Indicates the number of files in which no threat was found				
Automatic Analysis	Number of files submitted for automatic analysis				
Human Expert Analysis	Number of files submitted for manual analysis				
Basic Info Reg.	Indicates the number of times the user has used Valkyrie REST API named fvs_basic_info, requesting basic analysis results from Valkyrie database such as if the file is uploaded before, verdict of last analysis, last analysis date, first analysis date, is the file whitelisted and so on.				
Full Info Req.	This is same as Basic Info Req. but requested for greater detail. Indicates the number of times the user has used REST API named fvs_full_info, which is used to retrieve last analysis results from Valkyrie database in greater detail such as static, dynamic and manual results including behavioral and file information.				
UI Get Info Req.	Indicates the number of times the user opened the detailed analysis results page from the Dashboard screen by pressing the button or doing a search by SHA1 of a file.				

Activity Logs

The 'Activity Logs' page provides the records of activities carried out in the Valkyrie account such as the activity date, user name, activity type and more.

To view your Valkyrie Activity Logs, click the 'Activity Logs' link

	John Smith	
۵	My Dashboard	
▦	My Stats	
B	Activity Logs	
÷	Log Out	

The activity logs page will be displayed. The number of logs to be displayed on each page can be selected from the 'Show entries' option on the left.

COMODO Creating Trust Online

V ~	LKYRIE COMODO				(U	John 💽
Activity Lo	gs					
_	-					
YOUR RECENT ACTIVITIES					:	search:
Activity Date	User Name 0	Email 4	Activity Type	Source IP	API Key ‡	SHA1 4
2016-04-05 13:12:21	John		See MyStats	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d	
2010-04-05 13:01:44	John		Get Info	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d	e98186b79857f4d1aaadc16a
2016-04-05 13:01:07	John.		View Dashboard	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d	
2016-04-05 12:50:34	John		View Dashboard	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d	
2016-04-05 12:46:48	John		View Dashboard	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d	
2016-04-05 12:45:36	John		View Dashboard	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d	
2016-04-05 12:45:35	John		Log In	10.108.51.61		
2016-04-04 17:52:15	John		Download Auto Analysis Report	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d	e98186b79857f4d1aaadc16a
2016-04-04 17:36:33	John		Get Info	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d	e98186b79857f4d1aaadc16a
2016-04-04 16:14:30	John		View Dashboard	10.108.51.61	ee9ca32f-acf3-4b6c-8513-7d	
2016-04-04 16:14:29	John		Log In	10.108.51.61		
2016 01 14 102605	isha		Maw Backboard	10 100 17 104	water \$10 with their \$500 Tel	

Sort and search options

Sorting the entries

• You can sort the items in ascending/descending order by clicking on the column headers.

Searching for particular item(s)

- Enter the details partially or fully in the search field on the top right side. You can search for logs based on all the columns.
- To display all the logs again, clear the search field.

Activity Logs - Table of Column Descriptions			
Column Header	Description		
Activity Date	The date and time of using the Valkyrie account for a particular activity type		
User Name	The logged user name for the account		
Email	The email id of the Valkyrie account.		
Activity Type	The name of the activity that was recorded.		
Source IP	The IP of the computer from which the Valkyrie account was logged in and used		
API Key	The private key of the user to use REST API		
SHA1	If a file is the subject of activity then its SHA1 hash details will be displayed here.		

5 Reports

After each scan is completed, the administrators can view the reports for the scan results. The reports are divided into three categories - Executive Report, Per Device Report and Per Program Report. The Executive Report is a summary of the scan providing details such as number of devices scanned, number of unknown programs found and so on. The Per Device Report is a summary of scan results providing details for each device scanned. The Per Program Report is a summary of scan results providing details of each unknown / malicious program, the devices affected by it and so on.

If the unknown files are submitted to Valkyrie for further analysis, the results reports for these scans also will also be available from the Reports drop-down as 'Executive Valkyrie, 'Per Device Valkyrie' and 'Per Program Valkyrie'. Please note that if you have note scanned with Valkyrie you can view only Executive, Per Device and Per Program Device reports and once you have scanned the files using Valkyrie analysis, you will be able to view only Valkyrie results.

COMODO Greating Trust Online Unknown File Hunter			_ 🗆 ×	
🕟 Start Scan 🏾 🍼 Analyze with Valkyrie 🔳 Stop Scan	🐽 Reports • 🍥	Options (i) Help -	Pttp ×	
Scan results Valkyrie analysis results	Executive Valkyrie	Group by Computers	Group by Files	
Name	Per Device Valkyrie	Verdict	Trusted Vendor	
DESKTOP-TTPO9PR (10.108.51.100) Completed: Total files scanned: 1. Unknown files: 1. Malicious files: 0.	Per Program Valkyrie			
Completed: Total files scanned: T. Unknown files: T. Malicious files: U. Per Program Valkyre Or Coprogram files freedownloadmanager.org free download manager winunivappfeature 97 KB No Threat Found No				
Please click here to see the detailed results				
1 Unknown files, 0 Malicious files (1 of 1 Computers scanned)				

Refer to the following for more details:

- Executive Report
- Device Report
- Program Report

5.1 Executive Report

The executive report is a summary of the scan results which provides details such as when the scan was started and finished, number of devices scanned and so on. The programs rating on the scanned devices and scanned devices rating are also available in pie chart. If a Valkyrie scan is run, then the programs Valkyrie rating over the scanned devices is also displayed in pie chart.

To generate an 'Executive' report results, click 'Reports' and then 'Executive' or 'Executive Valkyrie'.

The report will be generated and displayed:

COMODO Creating Trust Online



Executive Valkyr	ie Report			\times
🐸 🖬 😹 🕆 🧍	1 /2		Search	
<u>C</u>	одомо		12/19/2016 10:23:00 PM	
A	PT Assessment	Scan	VALKYRIE	
Re	eport Summary			
	Device Source: Scan Started: Scan Finished: Inaccessible Devices: Scan Attempts: Successful Scans: Failed Scans: Total Files Scanned: Trusted Files Found: Unknown Files Found: Malicious Files Found: Lookup in Progress:	Network Addresses (10.108.51.100) 12/19/2016 8:36:19 PM 12/19/2016 8:40:04 PM 0 1 1 0 1472 1472 1471 1 0 0		₽

Scroll down to view the full report. The report in PDF format is saved in a temporary folder and will not be available after the application is closed. To save the report, click the folder icon on the top left side, copy the report file and save in another location.

- Report Summary Provides the details of the scan such as number of devices scanned, date and time of the scan, number of malware found and so on.
- Summary Charts Provides the details of programs found on the scanned devices and the rating of the scanned devices.
 - Programs Rating Over Scanned Devices Results displayed in pie chart of the programs that were scanned on the devices. Provides the percentage of trusted programs, unknown programs and malware.
 - Scanned Devices Rating The statuses of the scanned devices in pie chart providing the percentage of devices that are found safe, infected and at risk.
 - **Programs Valkyrie Rating Over Scanned Devices** This is will be available in 'Executive Valkyrie' report only. Provides details of the Valkyrie rating of unknown files that were scanned.

5.2 Device Report

The 'Per Device Report' is a summary of scan results for a particular device. It includes details of malware found on each device, unknown files found and the path of the files. If a Valkyrie scan is run, then the Valkyrie verdict is also provided for the unknown files at the end of the report.

To generate a 'Per Device' report, click 'Reports' and then 'Per Device' or 'Per Device Valkyrie'.

The report will be generated and displayed:

1/3		🔎 Search
сомодо		12/19/2016 10:33:42 PM
APT Assessmer	nt Scan	
Report Summary		
Device Source: Scan Started: Scan Finished: Inaccessible Devices: Scan Attempts: Successful Scans: Failed Scans:	Network Addresses (10.108.51.100) 12/19/2016 8:36:19 PM 12/19/2016 8:40:04 PM 0 1 1 1 0	
Total Files Scanned: Trusted Files Found: Unknown Files Found: Malicious Files Found: Lookup in Progress:	1472 1471 1 0 0	

Scroll down to view the full report. The report in PDF format is saved in a temporary folder and will not be available after the application is closed. To save the report, click the folder icon on the top left side, copy the report file and save in another location.

- **Report Summary** Provides the details of the scan such as number of devices scanned, date and time of the scan, number of malware found and so on.
- **Summary Chart** Provides the details in bar graph the top 10 endpoints that are detected with unknown/malware files.
- **Details per Device** The details of each device including the name of the device, number of malware/unknown files in them, the path of each malware/unknown files in the affected device and more.
- Valkyrie This is will be available in 'Per Device Valkyrie' report only. Provides the details of the scan report of each of the unknown file.

5.3 Program Report

The 'Per Program Report' provides scan results on a per program basis. It includes details of each malware/unknown file found, the devices on which they were found, the path of the files on the device and more. If a Valkyrie scan is run, then the Valkyrie verdict is also provided for each of the malware/unknown file.

COMODO Creating Trust Online

To generate a 'Per Program' report, click 'Reports' and then 'Per Device' or 'Per Program Valkyrie'.

The report will be generated and displayed:



Scroll down to view the full report. The report in PDF format is saved in a temporary folder and will not be available after the application is closed. To save the report, click the folder icon on the top left side, copy the report file and save in another location.

- **Report Summary** Provides the details of the scan such as number of devices scanned, date and time of the scan, number of malware/unknown files found and so on.
- Summary Chart Provides the details of the top 10 unknown/malicious programs in bar graph.
- Details per Program The details of each file including the name(s) of the device(s) it was found on, IP addresses of the devices and more. In the 'Per Program Valkyrie' report, the verdict of the Valkyrie analysis will also be provided for each program.

6 About Comodo Unknown File Hunter

The 'About' dialog provides the details of the product and its version number.

• To view the product details and its version number, click 'About' from the 'Help' in menu.

COMODO Creating Trust Online*

COMODO Creating Trust Online Unknown File Hunt	er			_ 🗆 ×
Start Scan 🥑 Analyze with Valkyr	e 💽 Stop Scan	A Reports * (Option	ns 🚺 Help •	P Search
Scan results Valkyrie analysis results			About	
Name			Agent Requirem	nents ⁷ Size
			~	
About 🧲			X	C.
	COMOD C Creating Trust Onlin)		
	Product Name:	Unknown File Hunter		
	Product Version:	2.1.21203.140		
© 2016 Comodo Securit	y Solutions, Inc. All Rig	ghts Reserved.	Close	

- Product Name The full name of the product
- Product Version The version number of the product
- Click the 'Close' button to return to the application.

7 Agent Requirements

The 'Agent requirements' item in the help menu provides configuration advice to help you run scans successfully:

COMODO Creating Trust Online*

COMODO Creating Trust Online Unknown File Hunter -	
🕟 Start Scan 🦿 Analyze with Valkyrie 💿 Stop Scan 🌰 Reports - 🍥 Options 🚺 Help -	h
Scan results Valkyrie analysis results About	
Name Agent Requirements	Size
Agent Requirements < X Check whether a target computer is turned on and connected to the network.	1
Check whether firewall on a target computer is turned Off.	
Check whether IP address of a target computer is correct.	
In the Network Neighbourhood run Network Wizard, enable file sharing.	
Make sure Administrator password is not blank and correct.	
Check whether 'Forceguest' option on target computer is disabled: HKLM\\SYSTEM\ \CurrentControlSet\\Control\\Lsa 'forceguest' dword is 0.	
If the account is not a built-in Administrator, check whether: HKLM\\SOFTWARE\\Microsoft\ \Windows\\CurrentVersion\\Policies\\System 'LocalAccountTokenFilterPolicy' dword is 1.	
Close	

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street Clifton, NJ 07013 United States Tel : +1.888.266.636 Tel : +1.703.581.6361 https://www.comodo.com Email: EnterpriseSolutions@Comodo.com