COMODO
Creating Trust Online®

Comodo Valkyrie

Software Version 1.42

User Guide

Guide Version 1.42.010620

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

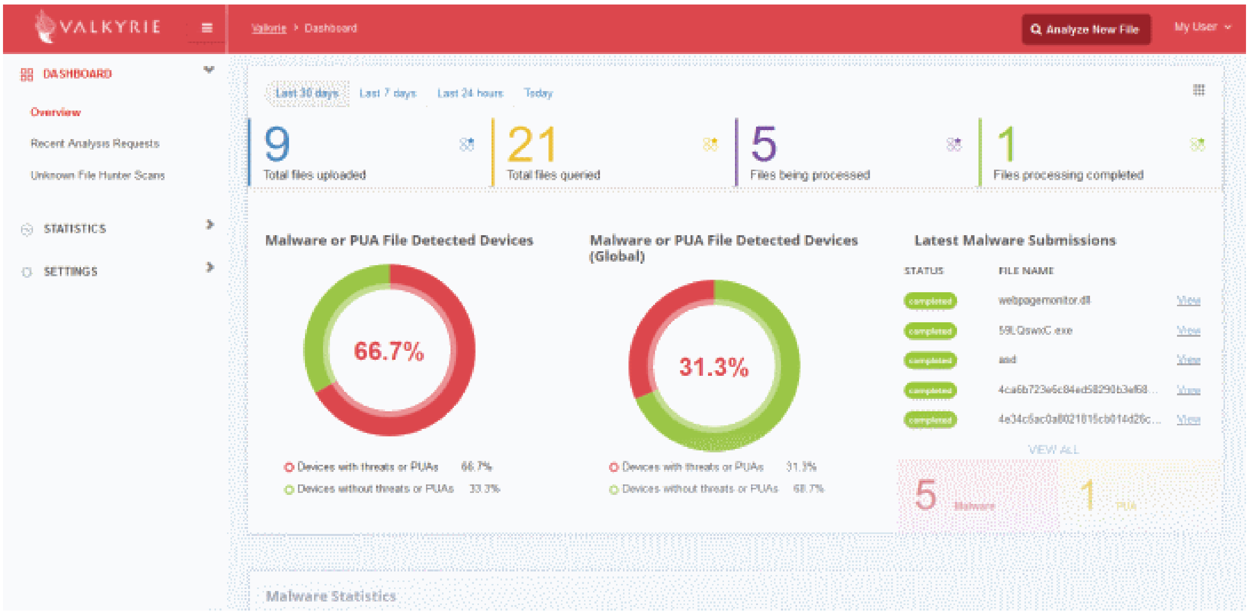
1 Introduction to Comodo Valkyrie....3
2 Create a Valkyrie Account....5
2.1 Log into Valkyrie....8
3 Upload Files for Analysis 11
4 Valkyrie Analysis Results....13
4.1 Valkyrie Dashboard....16
4.2 Recent Analysis Requests....23
4.3 Kill Chain Report....35
4.4 My Analysis Statistics....43
4.5 Unknown File Hunter Scans....45
4.6 Unparalleled Protection Statistics....49
4.7 Unknown File Statistics....51
4.8 Configure Valkyrie Account Settings 55
4.8.1 Account Configuration....56
4.8.2 Antivirus Vendors....57
5 Unknown File Hunter Tool....59
About Comodo Security Solutions....65

1 Introduction to Comodo Valkyrie

Valkyrie is an online file verdict system that tests unknown files with a range of static and behavioral checks in order to identify those that are malicious. Because Valkyrie analyzes the entire run-time behavior of a file, it is more effective at detecting zero-day threats missed by the signature-based detection systems of classic antivirus products.

The Valkyrie console allows users to upload new files for analysis and to view scan results in a range of dashboards and reports. Users also have the option to forward files Comodo Labs for in-depth, human expert checks. The Comodo Unknown File Hunter tool allows users to locally scan entire networks for unknown files then upload them to Valkyrie for analysis.

- The results of your most recent analysis requests are shown by default
- Click your user-icon at top-right to navigate to the dashboard and other important areas



9 Total files uploaded

21 Total files queried

5 Files being processed

1 Files processing completed

Malware or PUA File Detected Devices

○ Devices with threats or PUAs 66.7%

○ Devices without threats or PUAs 33.3%

Malware or PUA File Detected Devices (Global)

○ Devices with threats or PUAs 31.3%

○ Devices without threats or PUAs 68.7%

Latest Malware Submissions

STATUS	FILE NAME	
completed	webpagemonitor.dll	View
completed	59LQswxC.exe	View
completed	asd	View
completed	4ca6b723e6c84ed58290b3ef68...	View
completed	4e34c6ac0a8021815cb014d26c...	View

5 Malware

1 PUA

Malware Statistics

Features

- No installation required, just upload files for analysis
- Automated and human expert analysis (optional) of submitted files
- Comprehensive reporting and dashboards

Overview of the Technologies

Valkyrie analysis systems consist of multiple techniques to ensure each and every file submitted is analyzed thoroughly before providing the verdict. In order to do that Valkyrie deploys two types of technologies - Automatic analysis and Human Expert analysis. The techniques used for automatic analysis include **Static Analysis**, Dynamic Analysis, Valkyrie Plugins and Embedded Detectors, Signature Based Detection, Trusted Vendor and Certificate Validation, Reputation System and Big Data VirusScope Analysis System.

Static Analysis

This technique involves extraction and analysis of various binary features and static behavioral inferences of an executable such as API headers, referred DLLs, PE sections and more such resources. Any deviation from the expected results are listed in the static analysis results and the verdict given accordingly.

Dynamic Analysis

The dynamic analysis technique include studying the run time behavior of a file to identify malware patterns that cannot be be identified through static analysis.

Valkyrie Plugins and Embedded Detectors

Valkyrie plugins utilizes the different malware analysis techniques developed by various communities and educational institutions and deployed by them on their systems as RESTful Web Services. Valkyrie includes these results also to compute a final overall verdict.

Embedded detectors in Valkyrie uses new methods of malware detection developed by Comodo AV laboratory to compute an overall final verdict of a file.

Signature Based Detection

Valkyrie uses different signature based detection sources in order to detect a given sample in the first place. Signature based detection simply checks SHA1 hash of files from signature sources to determine if there is any match in database.

Trusted Vendor and Certificate Validation

Valkyrie checks vendor details of a file with Trusted Vendor database that are continuously updated. If the vendor is white listed, then certificate validation is done to ensure that certificate chain is valid and not revoked or expired.

Reputation System

Reputation data of files that are collected from millions of endpoints through Comodo network and products are evaluated on a big data platform and converted to intelligence form to be used by Valkyrie.

Big Data VirusScope Analysis System

VirusScope, a part of Comodo Security products, is a dynamic application analyzer system that detects malicious behavior of a file, blocks and reverses those actions when necessary. The detected malware are reported to Comodo servers and this data is also used by Valkyrie.

Human Expert Analysis

Valkyrie system includes submission of files by users for manual analysis. Comodo expert analysis, which consists of the most sophisticated analysis of a file and provides the ultimate verdict of the file.

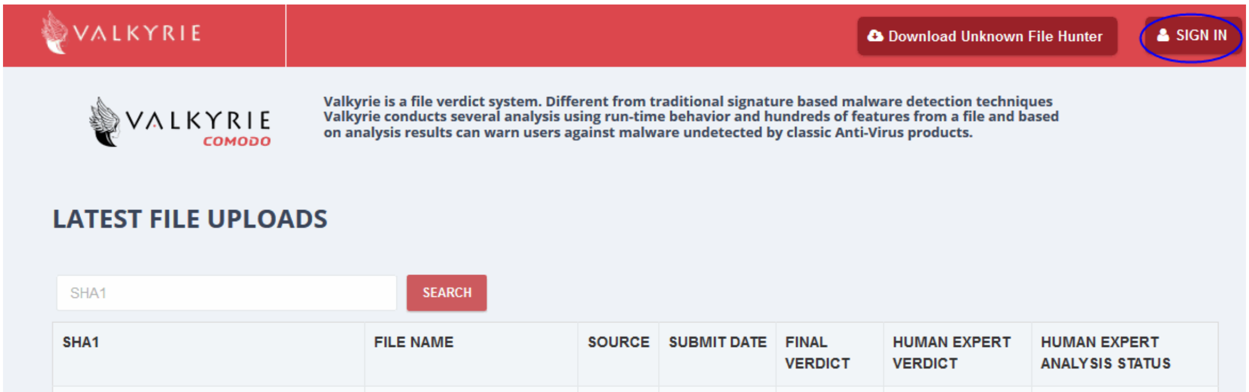
Guide Structure

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

- Introduction
- Create a Valkyrie Account
  - Log into Valkyrie
- Upload Files for Analysis
- Valkyrie Analysis Results
  - Valkyrie Dashboard
  - Recent Analysis Requests
  - Kill Chain Report
  - My Analysis Statistics
  - Unknown File Hunter Scans
  - Unparalleled Protection Statistics
  - Unknown File Statistics
  - Configure Valkyrie Account Settings
    - Account Configuration
    - Antivirus Vendors
- Unknown File Hunter Tool

2 Create a Valkyrie Account

Creating a Valkyrie account is very simple and can be done within a few minutes. Enter https://valkyrie.comodo.com into the address bar of any browser and click the 'Sign In' button at the top right of the screen.

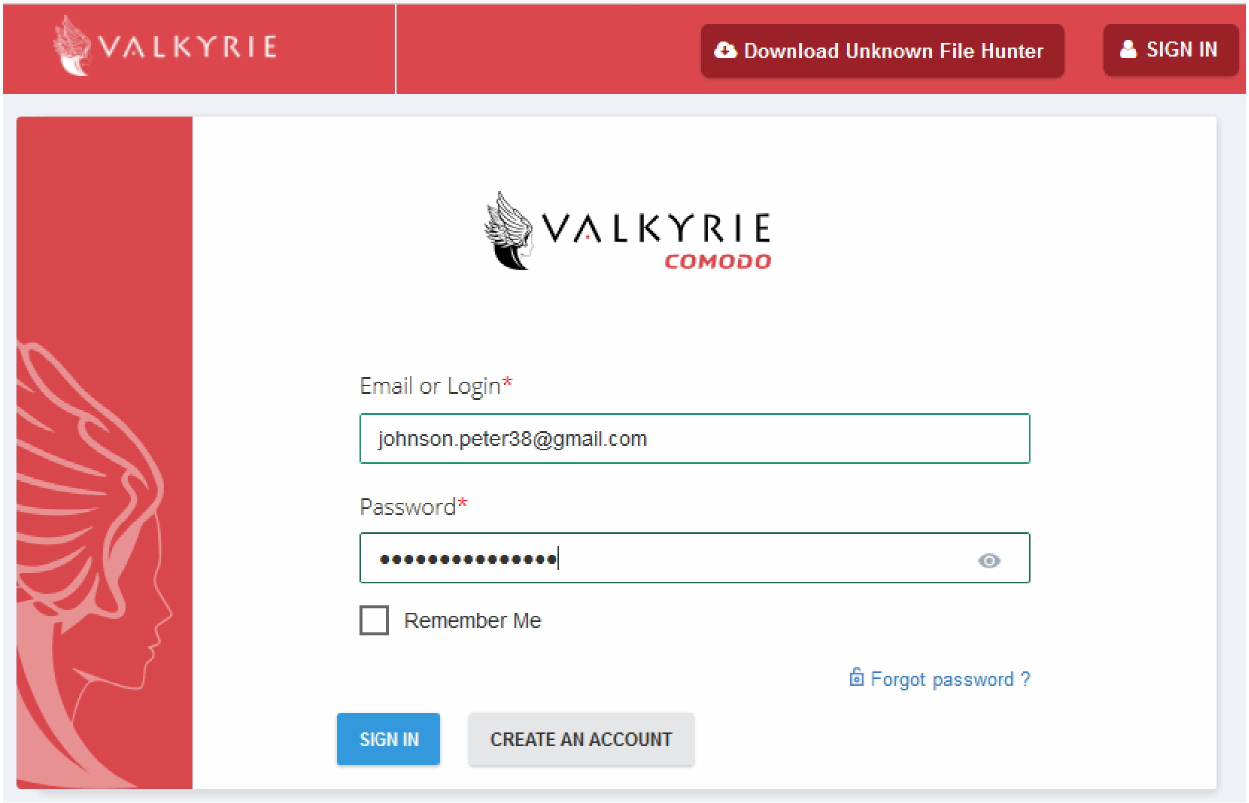


Valkyrie is a file verdict system. Different from traditional signature based malware detection techniques Valkyrie conducts several analysis using run-time behavior and hundreds of features from a file and based on analysis results can warn users against malware undetected by classic Anti-Virus products.

LATEST FILE UPLOADS

SHA1	FILE NAME	SOURCE	SUBMIT DATE	FINAL VERDICT	HUMAN EXPERT VERDICT	HUMAN EXPERT ANALYSIS STATUS

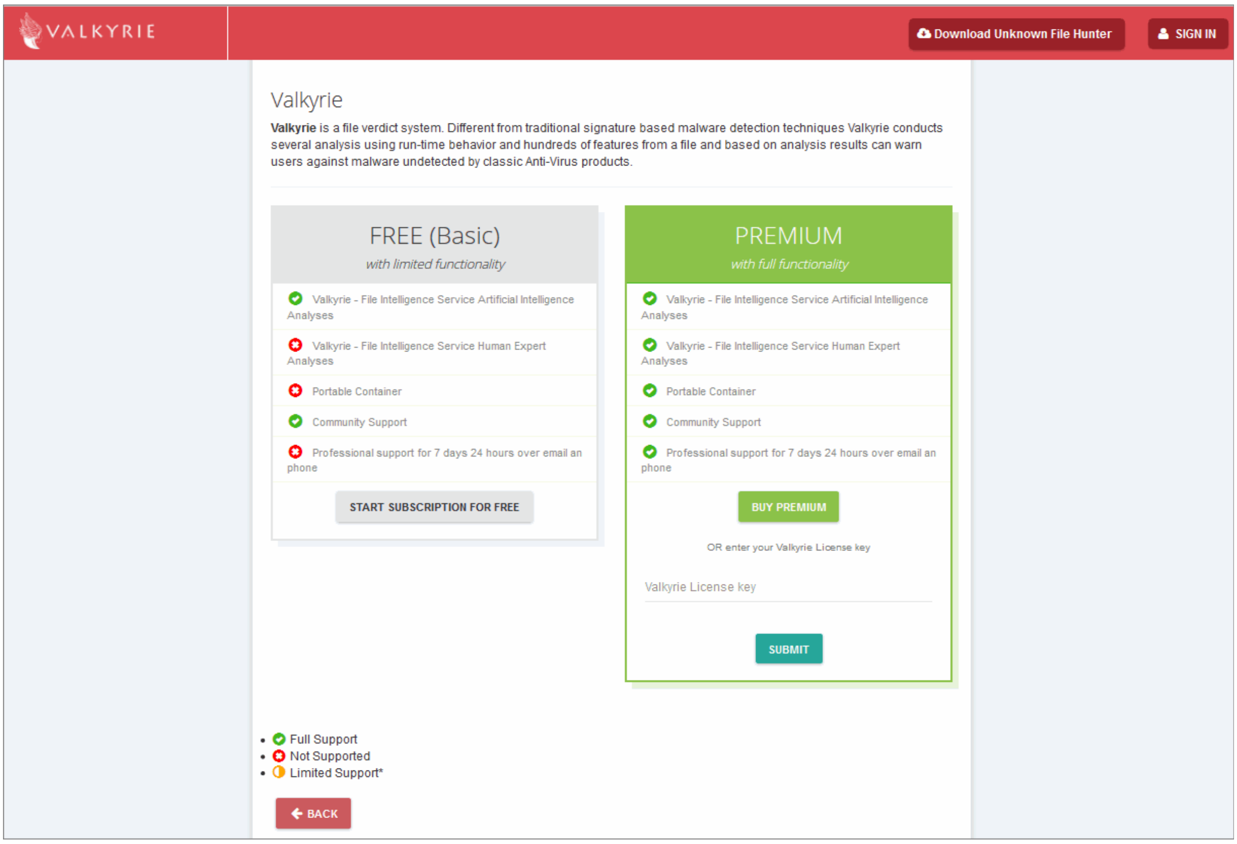
The 'Comodo Valkyrie' login screen will be displayed.



Email or Login*
johnson.peter38@gmail.com
Password*
•••••••••••••••
□ Remember Me

- Click the 'Create an account' link

You will be taken to the Valkyrie subscription form.



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.

FREE (Basic) *with limited functionality*	PREMIUM *with full functionality*
✓ Valkyrie - File Intelligence Service Artificial Intelligence Analyses	✓ Valkyrie - File Intelligence Service Artificial Intelligence Analyses
☒ Valkyrie - File Intelligence Service Human Expert Analyses	✓ Valkyrie - File Intelligence Service Human Expert Analyses
☒ Portable Container	✓ Portable Container
✓ Community Support	✓ Community Support
☒ Professional support for 7 days 24 hours over email an phone	✓ Professional support for 7 days 24 hours over email an phone
START SUBSCRIPTION FOR FREE	BUY PREMIUM OR enter your Valkyrie License key Valkyrie License key SUBMIT

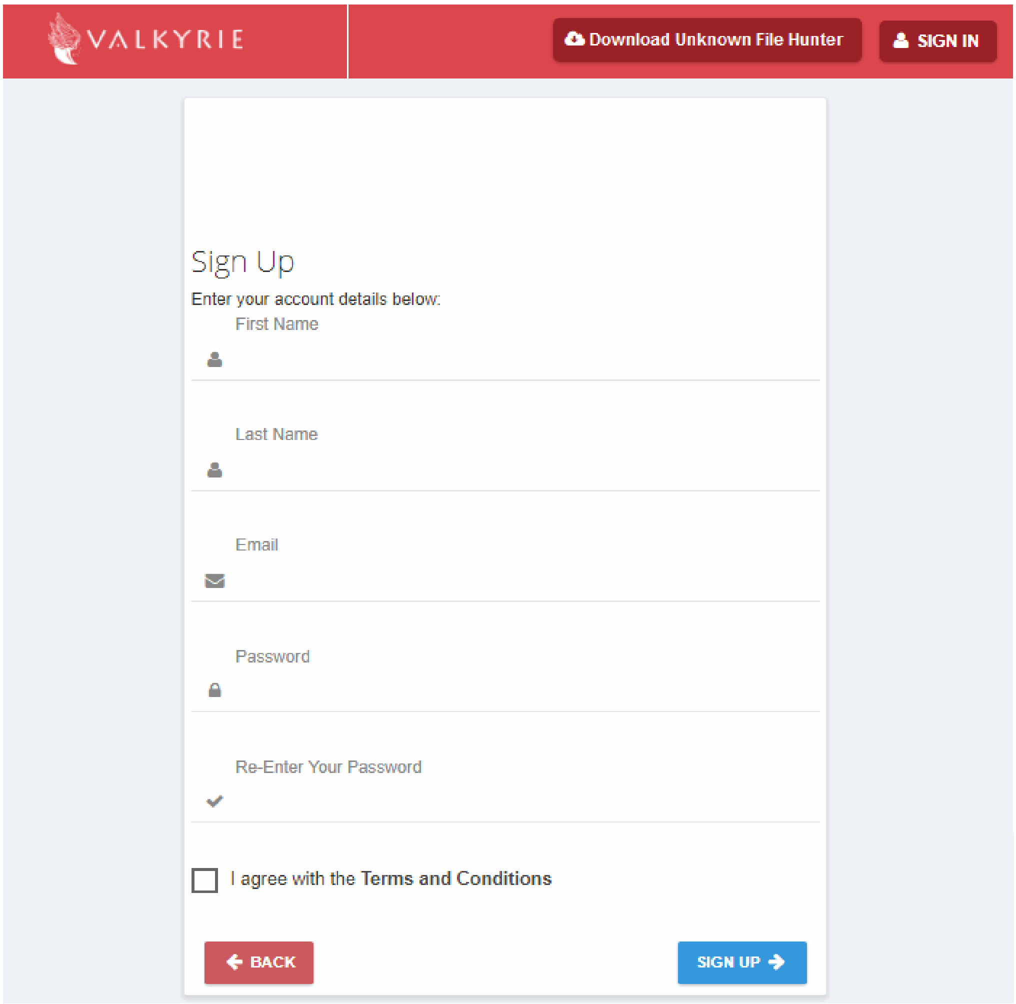
- ✓ Full Support
- ☒ Not Supported
- ◐ Limited Support*

- Click 'BUY PREMIUM' or 'START SUBSCRIPTION FOR FREE' to be taken to Comodo Valkyrie sign-up page. Enter your User Details and Contact Information in the respective sections. You will receive a confirmation email.

  OR

- Enter a valid Valkyrie license key and click 'SUBMIT' to log straight into the interface

If you need to sign-up, please complete the following form:



Sign Up

Enter your account details below:

First Name

Last Name

Email

Password

Re-Enter Your Password

□ I agree with the Terms and Conditions

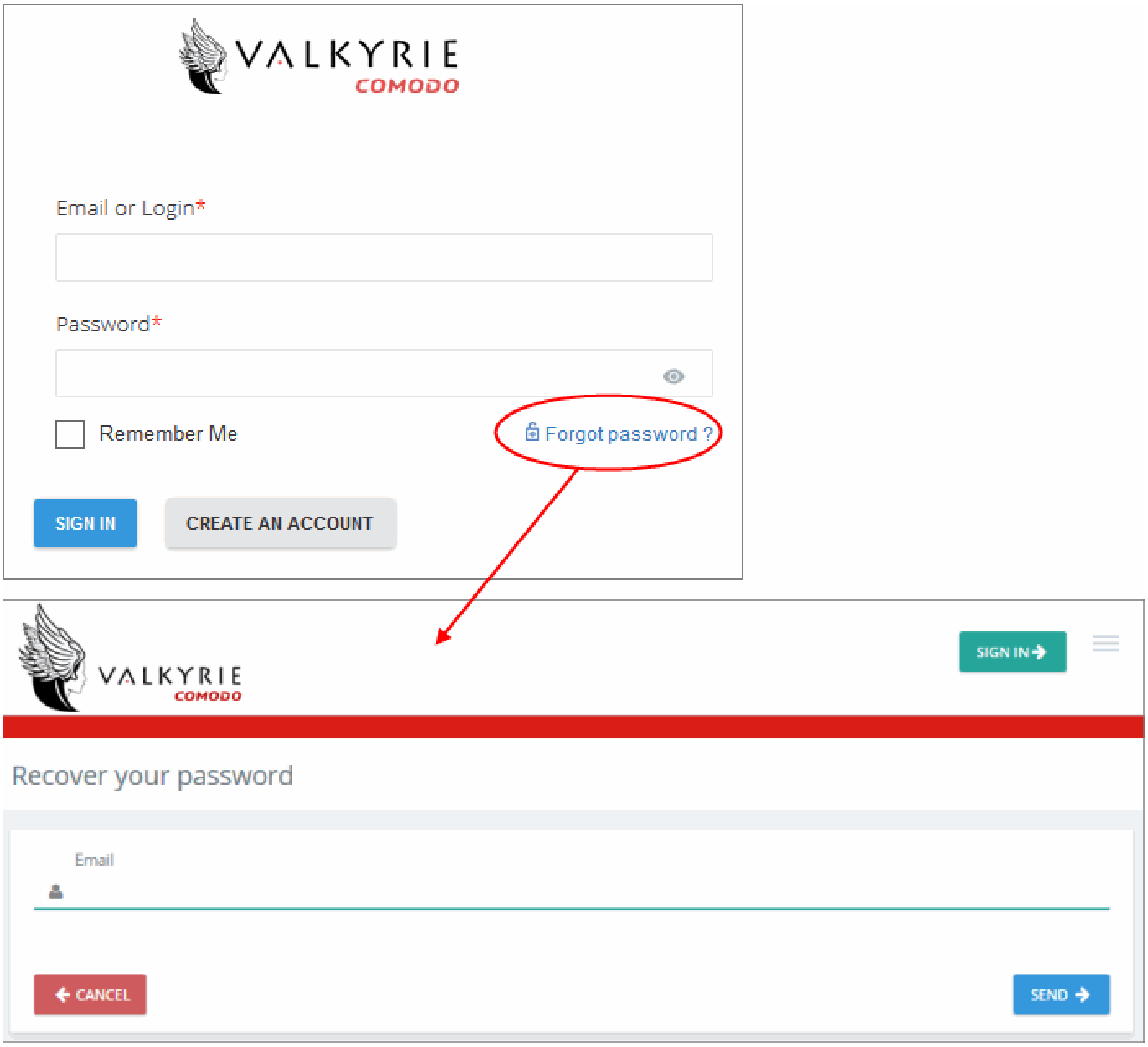
- First Name / Last Name - Enter your account first and last names. These will be displayed in the interface after logging in.
- Email - Enter a valid email that will be used for logging into your account.
- Password - Enter the password for logging into your account and confirm it in the next field.
- Click 'Terms and Conditions', read the 'Comodo Terms and Conditions' fully, select the check box beside 'I agree with the Terms and Conditions' and click the 'Sign Up' button.

That's it. Your Valkyrie account will be created and the 'Dashboard' screen will be displayed.

If you have forgotten your password, it can be reset as follows:

- From the 'Welcome to Valkyrie' screen, click the link 'Click here' beside 'Forgot your password?

The 'Recover your password' screen will be displayed:



- Enter the email address to which the password should be sent in the 'Email' field and click the 'Send' button.

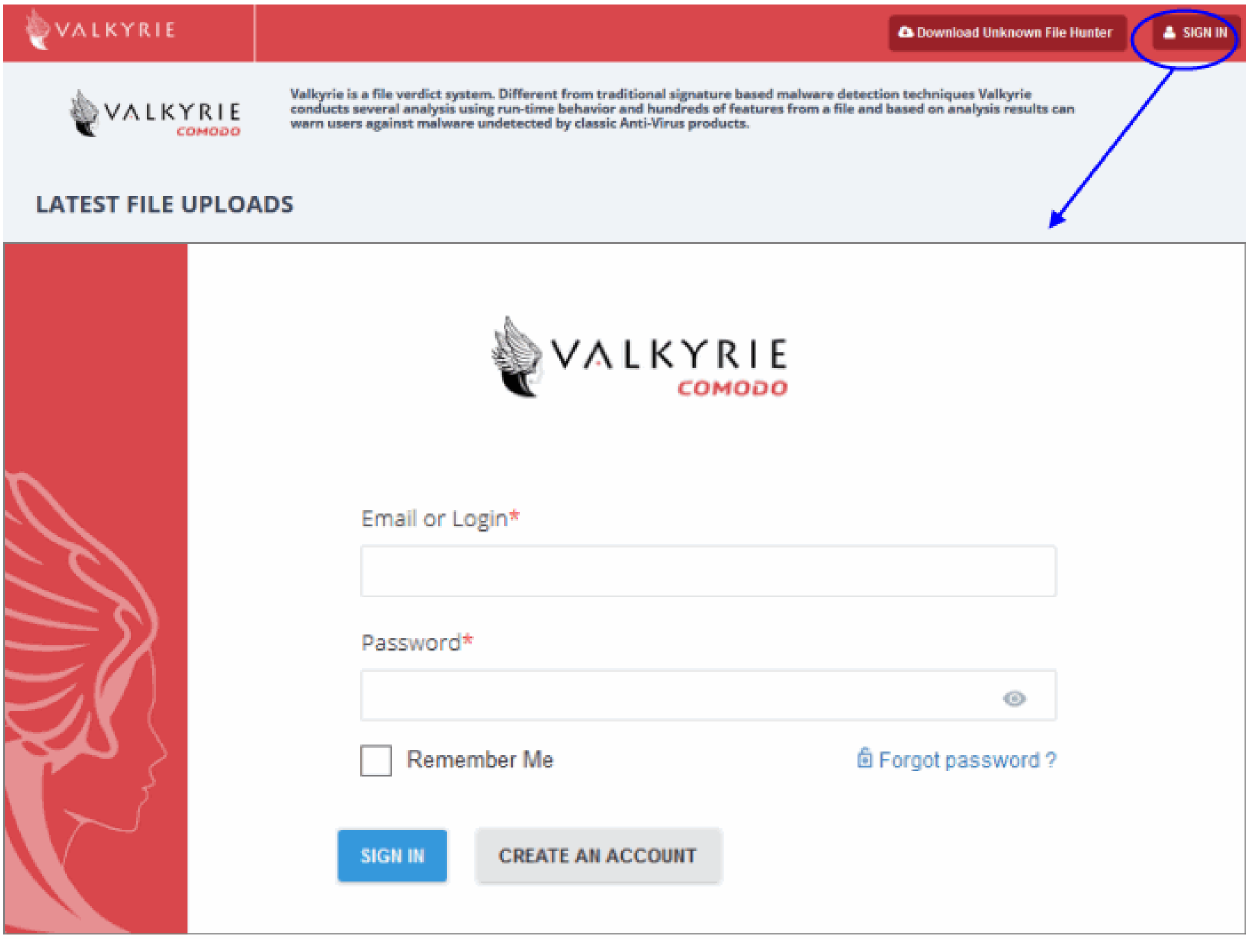
You will receive the reset password to the specified mail above. Now you can login to the account using the new password. Please note that you can also reset the current password from the 'Settings' screen. See '**Configure Valkyrie Account Settings**' for more details.

2.1 Log into Valkyrie

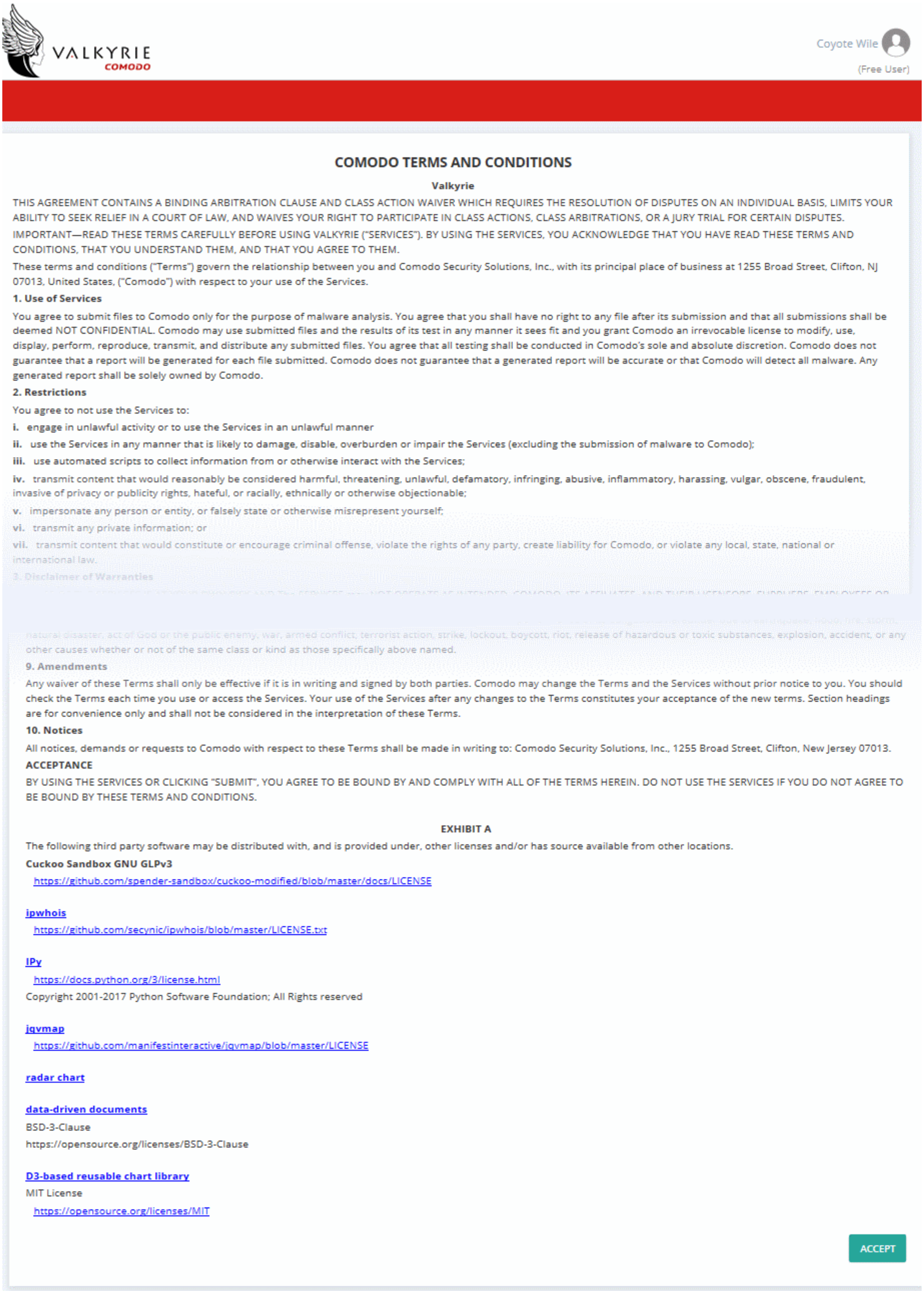
You can login to your Valkyrie account using any internet browser.

- Enter 'https://valkyrie.comodo.com' in the address bar then click 'Enter'

The home page appears:


VALKYRIE
Download Unknown File Hunter
SIGN IN
VALKYRIE COMODO
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.
LATEST FILE UPLOADS
VALKYRIE COMODO
Email or Login*
Password*
□ Remember Me
Forgot password ?
SIGN IN
CREATE AN ACCOUNT

- Click the 'Sign In' button at the top right. The Login page will be displayed.
- Enter your Comodo username and password. Comodo One / ITarian users can use their C1/ ITarian username and password.
- If you select the 'Remember Me' you will be logged into your account automatically each time you visit.
- If you have a premium license you need to accept the terms and conditions after your first login.


Coyote Wile
(Free User)

COMODO TERMS AND CONDITIONS

Valkyrie

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE AND CLASS ACTION WAIVER WHICH REQUIRES THE RESOLUTION OF DISPUTES ON AN INDIVIDUAL BASIS, LIMITS YOUR ABILITY TO SEEK RELIEF IN A COURT OF LAW, AND WAIVES YOUR RIGHT TO PARTICIPATE IN CLASS ACTIONS, CLASS ARBITRATIONS, OR A JURY TRIAL FOR CERTAIN DISPUTES.

IMPORTANT—READ THESE TERMS CAREFULLY BEFORE USING VALKYRIE ("SERVICES"). BY USING THE SERVICES, YOU ACKNOWLEDGE THAT YOU HAVE READ THESE TERMS AND CONDITIONS, THAT YOU UNDERSTAND THEM, AND THAT YOU AGREE TO THEM.

These terms and conditions ("Terms") govern the relationship between you and Comodo Security Solutions, Inc., with its principal place of business at 1255 Broad Street, Clifton, NJ 07013, United States, ("Comodo") with respect to your use of the Services.

1. Use of Services

You agree to submit files to Comodo only for the purpose of malware analysis. You agree that you shall have no right to any file after its submission and that all submissions shall be deemed NOT CONFIDENTIAL. Comodo may use submitted files and the results of its test in any manner it sees fit and you grant Comodo an irrevocable license to modify, use, display, perform, reproduce, transmit, and distribute any submitted files. You agree that all testing shall be conducted in Comodo's sole and absolute discretion. Comodo does not guarantee that a report will be generated for each file submitted. Comodo does not guarantee that a generated report will be accurate or that Comodo will detect all malware. Any generated report shall be solely owned by Comodo.

2. Restrictions

You agree to not use the Services to:

i. engage in unlawful activity or to use the Services in an unlawful manner

ii. use the Services in any manner that is likely to damage, disable, overburden or impair the Services (excluding the submission of malware to Comodo);

iii. use automated scripts to collect information from or otherwise interact with the Services;

iv. transmit content that would reasonably be considered harmful, threatening, unlawful, defamatory, infringing, abusive, inflammatory, harassing, vulgar, obscene, fraudulent, invasive of privacy or publicity rights, hateful, or racially, ethnically or otherwise objectionable;

v. impersonate any person or entity, or falsely state or otherwise misrepresent yourself;

vi. transmit any private information; or

vii. transmit content that would constitute or encourage criminal offense, violate the rights of any party, create liability for Comodo, or violate any local, state, national or international law.

3. Disclaimer of Warranties

natural disaster, act of God or the public enemy, war, armed conflict, terrorist action, strike, lockout, boycott, riot, release of hazardous or toxic substances, explosion, accident, or any other causes whether or not of the same class or kind as those specifically above named.

9. Amendments

Any waiver of these Terms shall only be effective if it is in writing and signed by both parties. Comodo may change the Terms and the Services without prior notice to you. You should check the Terms each time you use or access the Services. Your use of the Services after any changes to the Terms constitutes your acceptance of the new terms. Section headings are for convenience only and shall not be considered in the interpretation of these Terms.

10. Notices

All notices, demands or requests to Comodo with respect to these Terms shall be made in writing to: Comodo Security Solutions, Inc., 1255 Broad Street, Clifton, New Jersey 07013.

ACCEPTANCE

BY USING THE SERVICES OR CLICKING "SUBMIT", YOU AGREE TO BE BOUND BY AND COMPLY WITH ALL OF THE TERMS HEREIN. DO NOT USE THE SERVICES IF YOU DO NOT AGREE TO BE BOUND BY THESE TERMS AND CONDITIONS.

EXHIBIT A

The following third party software may be distributed with, and is provided under, other licenses and/or has source available from other locations.

Cuckoo Sandbox GNU GLPv3
https://github.com/spender-sandbox/cuckoo-modified/blob/master/docs/LICENSE

ipwhois
https://github.com/secynic/ipwhois/blob/master/LICENSE.txt

IPy
https://docs.python.org/3/license.html
Copyright 2001-2017 Python Software Foundation; All Rights reserved

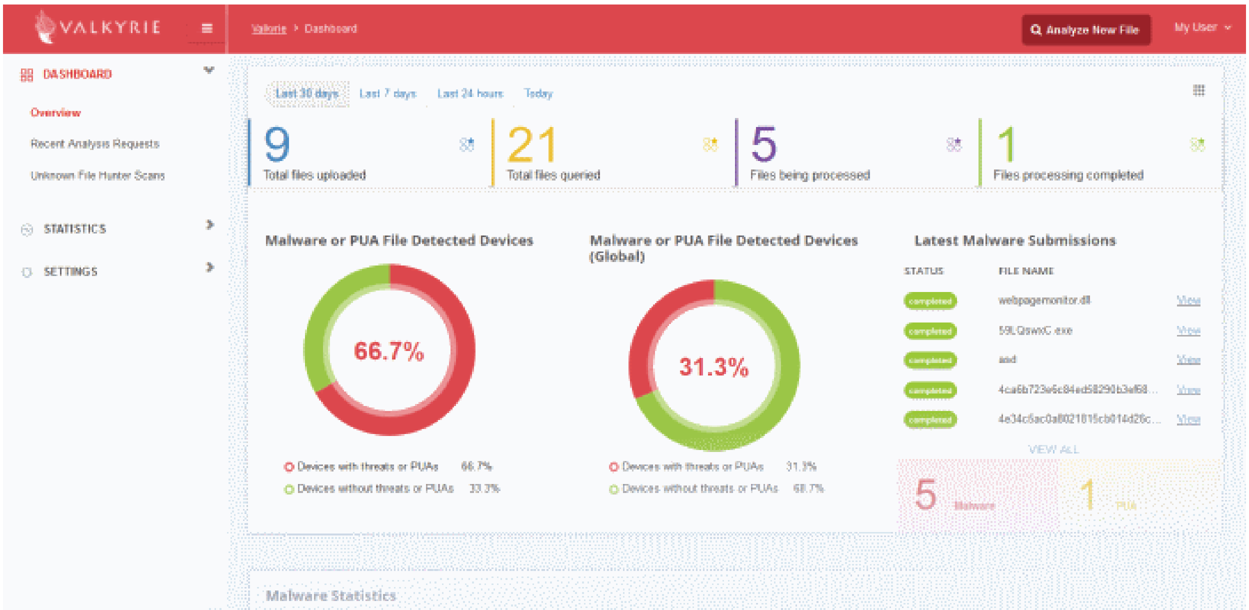
jqvmap
https://github.com/manifestinteractive/jqvmap/blob/master/LICENSE

radar chart

data-driven documents
BSD-3-Clause
https://opensource.org/licenses/BSD-3-Clause

D3-based reusable chart library
MIT License
https://opensource.org/licenses/MIT

The 'Dashboard' page is shown by default after successful sign in. See '**Valkyrie Dashboard**' for more details.


VALKYRIE
Valkyrie > Dashboard
Analyze New File
My User
DASHBOARD
Overview
Recent Analysis Requests
Unknown File Hunter Scans
STATISTICS
SETTINGS
Last 30 days
Last 7 days
Last 24 hours
Today
9
Total files uploaded
21
Total files queried
5
Files being processed
1
Files processing completed
Malware or PUA File Detected Devices
66.7%
Devices with threats or PUAs 66.7%
Devices without threats or PUAs 33.3%
Malware or PUA File Detected Devices (Global)
31.3%
Devices with threats or PUAs 31.3%
Devices without threats or PUAs 68.7%
Latest Malware Submissions
VIEW ALL
5 Malware
1 PUA
Malware Statistics

STATUS	FILE NAME	
completed	webpagemonitor.dll	View
completed	59LQswxC.exe	View
completed	asd	View
completed	4ca6b723e6c84ed58290b3ef68...	View
completed	4e34c6ac0a8021815cb014d26c...	View

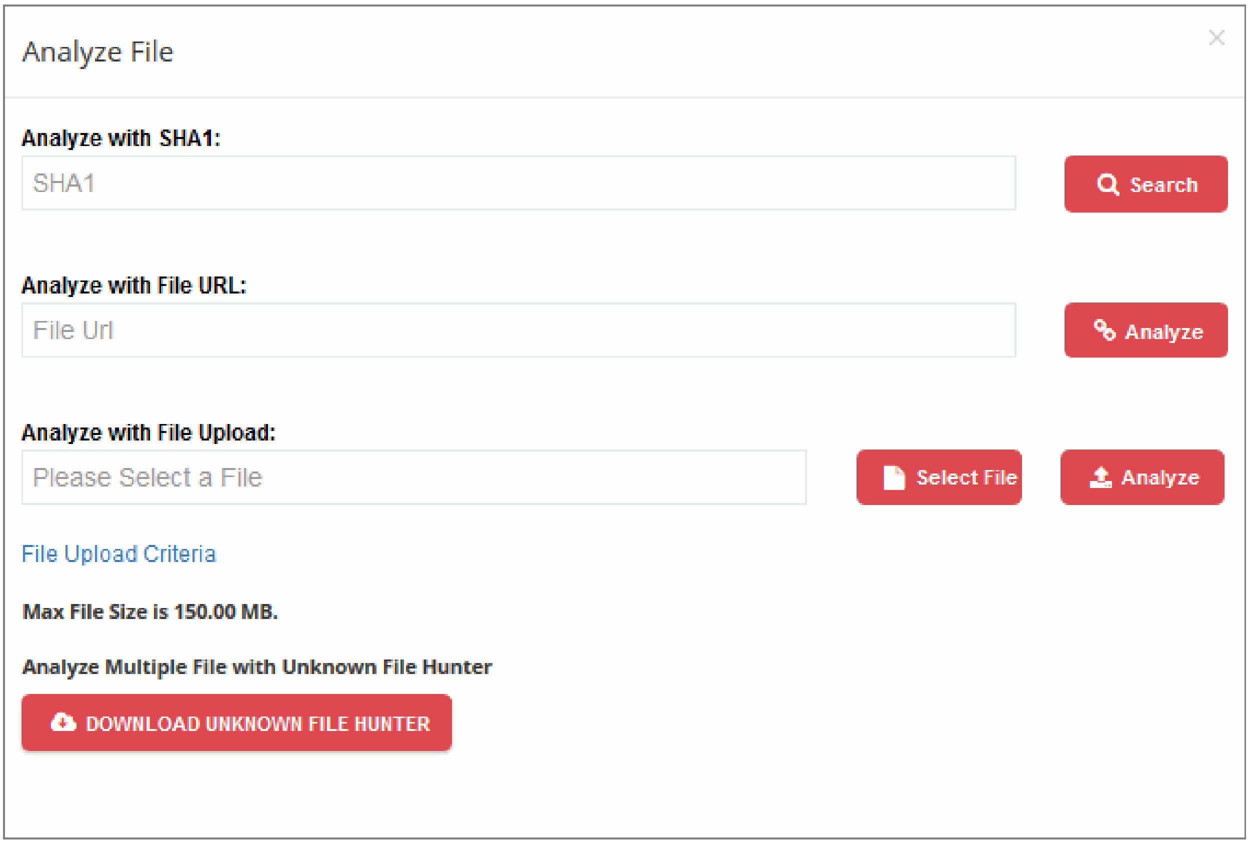
Next - '**Upload Files for Analysis**' .

3 Upload Files for Analysis

Files uploaded to Valkyrie are analyzed with a wide range of dynamic and static tests in order to reach a verdict on their trustworthiness.

- Click 'Analyze New File' **Analyze New File** to upload files for scanning. This button is located at the top right corner of the dashboard.

The file upload and analyze form will open:



Analyze File

Analyze with SHA1:

SHA1

Analyze with File URL:

File Url

Analyze with File Upload:

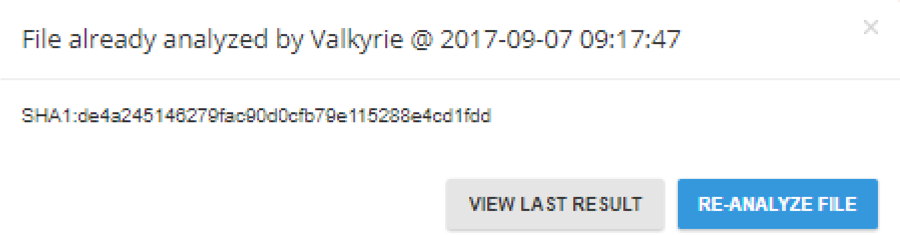
Please Select a File

File Upload Criteria

Max File Size is 150.00 MB.

Analyze Multiple File with Unknown File Hunter

- **Analyze with SHA1** - Enter the SHA1 hash value of the file you wish to investigate and click 'Search'. Valkyrie will search its databases to see if it has a record of the file and display results accordingly. If no record is found then use 'Analyze with File Upload' to submit the file for testing.
- **Analyze with File URL** - Enter the URL of a file and click the 'Analyze' button. Valkyrie will test the file and provide a verdict in a few minutes.
- **Analyze with File Upload** – Directly submit files for Valkyrie analysis. Click 'Select File', choose the file you wish to submit then click the 'Analyze' button. The following message will be displayed if the file has already been analyzed:

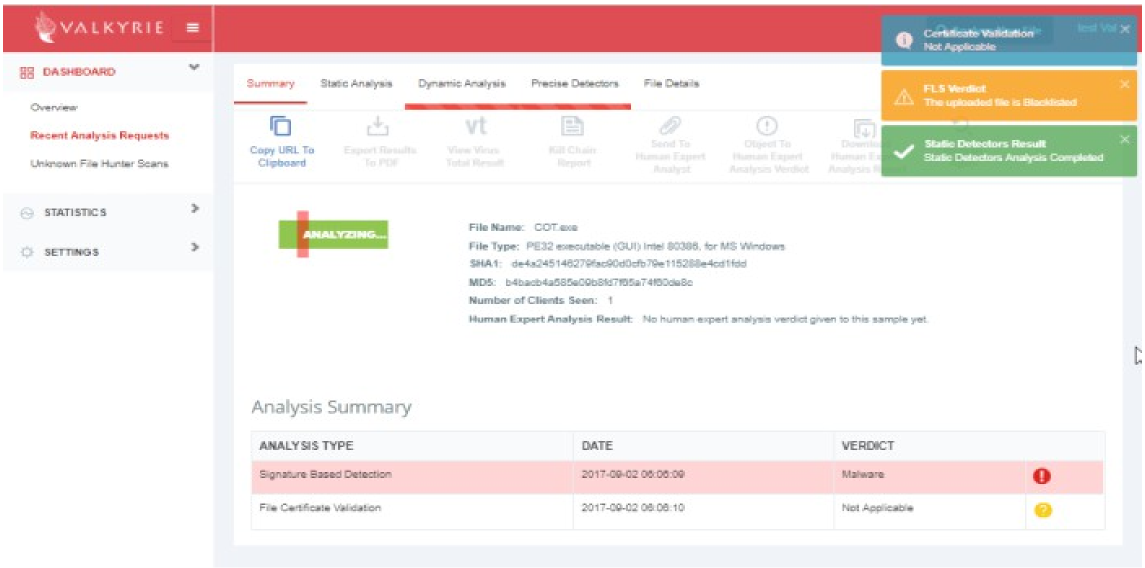


File already analyzed by Valkyrie @ 2017-09-07 09:17:47

SHA1:de4a245146279fac90d0cfb79e115288e4cd1fdd

- **Download Unknown File Hunter** - Comodo Unknown File Hunter is a utility which lets you scan local and network endpoints for unknown files. These files can then be uploaded to Valkyrie for analysis.
  - Click 'View Last Result' to view the most recently completed analysis. Click 'Re-Analyze File' to test the file again.
  - Click 'Re-analyze File' to resubmit the file for another round of dynamic and static tests to get a verdict on its trustworthiness.

The analysis progress will be shown as follows:



Certificate Validation
Not Applicable

FLS Verdict
The uploaded file is Blacklisted

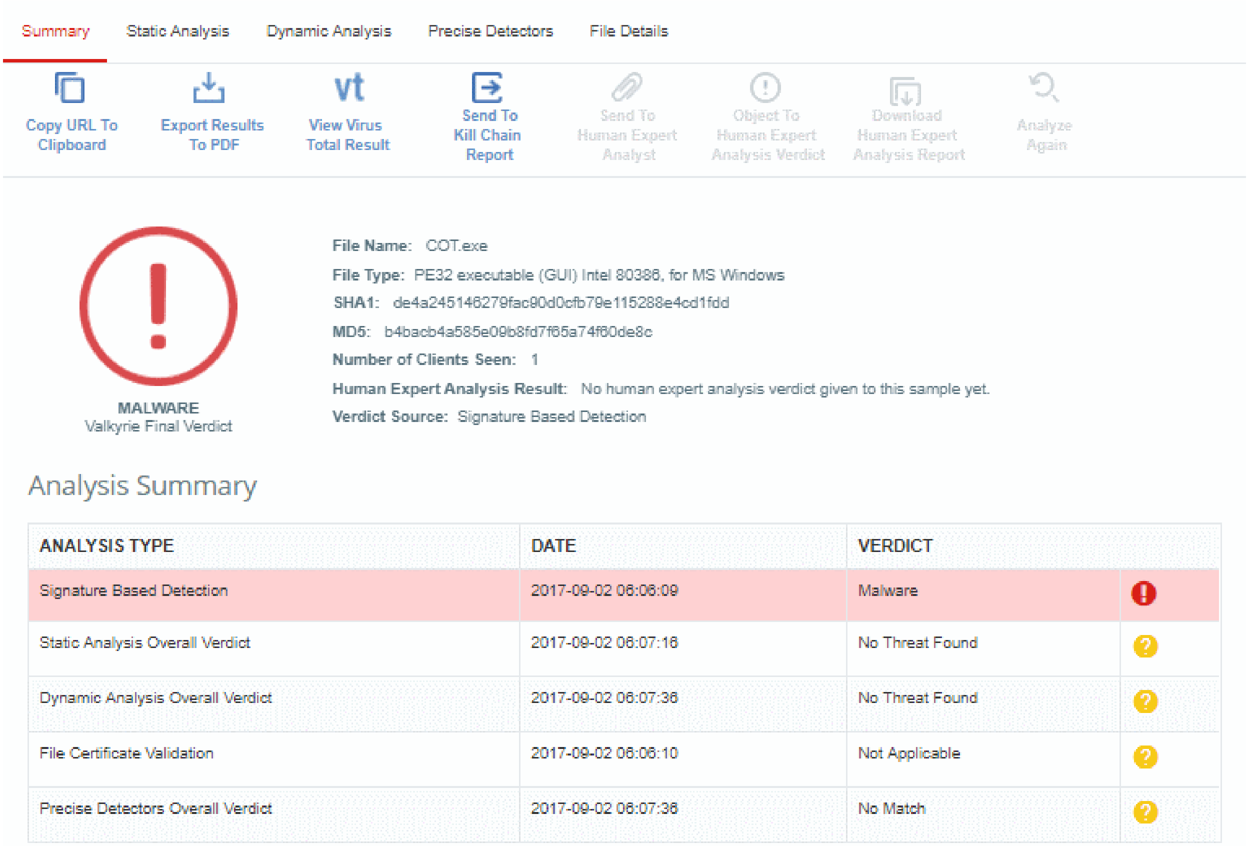
Static Detectors Result
Static Detectors Analysis Completed

File Name: COT.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: de4a245146279fac90d0cfb79e115288e4cd1fdd
MD5: b4bacb4a585e09b8fd7f65a74f60de8c
Number of Clients Seen: 1
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2017-09-02 06:06:09	Malware	!
File Certificate Validation	2017-09-02 06:06:10	Not Applicable	?

Results is shown once the analysis is complete:



File Name: COT.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: de4a245146279fac90d0cfb79e115288e4cd1fdd
MD5: b4bacb4a585e09b8fd7f65a74f60de8c
Number of Clients Seen: 1
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

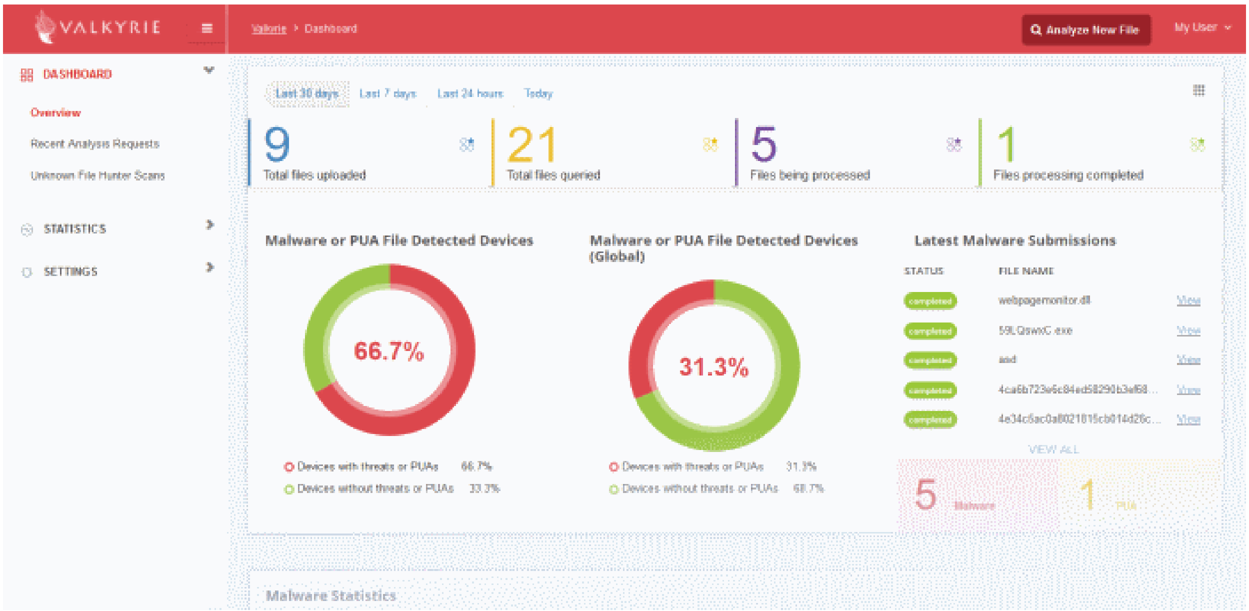
Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2017-09-02 06:06:09	Malware	!
Static Analysis Overall Verdict	2017-09-02 06:07:16	No Threat Found	?
Dynamic Analysis Overall Verdict	2017-09-02 06:07:36	No Threat Found	?
File Certificate Validation	2017-09-02 06:06:10	Not Applicable	?
Precise Detectors Overall Verdict	2017-09-02 06:07:36	No Match	?

See '**Valkyrie Analysis Results**' to understand the results.

4 Valkyrie Analysis Results

The Valkyrie homepage shows verdicts on your most recently submitted files:

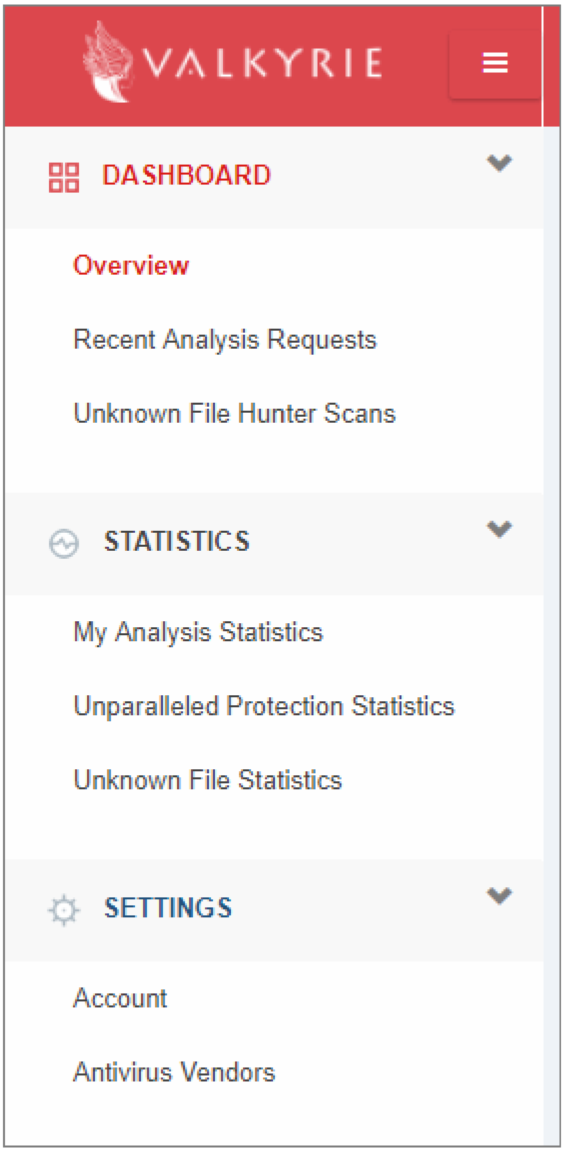

VALKYRIE
Valkyrie › Dashboard
Analyze New File
My User
DASHBOARD
Overview
Recent Analysis Requests
Unknown File Hunter Scans
STATISTICS
SETTINGS
Last 30 days
Last 7 days
Last 24 hours
Today
9
Total files uploaded
21
Total files queried
5
Files being processed
1
Files processing completed
Malware or PUA File Detected Devices
66.7%
Devices with threats or PUAs 66.7%
Devices without threats or PUAs 33.3%
Malware or PUA File Detected Devices (Global)
31.3%
Devices with threats or PUAs 31.3%
Devices without threats or PUAs 68.7%
VIEW ALL
5 Malware
1 PUA
Malware Statistics

Latest Malware Submissions

STATUS	FILE NAME	
completed	webpagemonitor.dll	View
completed	59LQswxC.exe	View
completed	aaa	View
completed	4ca6b723e6c84ed58290b3ef68...	View
completed	4e34c8ac0a8021815cb014d26c...	View

Click the hamburger button at the top-left of the page to open the navigation menu. It has the following items:

- **Dashboard** - Details about each file that was submitted to Valkyrie for analysis. This includes the file's SHA1 signature, submitted date, verdicts and more. See '**Valkyrie Dashboard**' for more details.
  - **Overview** - Overall statistics about the files you have submitted to Valkyrie. Data includes total files uploaded, malware detected per device, most contacted external addresses and unparalleled protection statistics. See '**Valkyrie Dashboard**' for more details.
    - **Recent Analysis Requests** - Shows verdicts on the files you most recently uploaded. See **Recent Analysis Requests** for more details.
    - **Unknown File Hunter Scans** - Verdicts on files uploaded using 'Comodo Unknown File Hunter' (CUFH). CUFH is a free utility capable of scanning your entire network for unknown files. These files can then be uploaded to Valkyrie for analysis. CUFH can be downloaded from **https://valkyrie.comodo.com/**.



- **Statistics**
  - **My Analysis Statistics -** Aggregated verdicts on all files submitted by your account over time. Includes total files submitted, total number of clean/malware files and total number of unknown files. See '**My Analysis Statistics**' to find out more.
  - **Unparalleled Protection Statistics -** Lists unknown files you submitted which Valkyrie identified as malicious before any other antivirus company. See '**Unparalleled Protection Statistics**' to find out more.
  - **Unknown File Statistics -** A graphical summary of unknown files that are white-listed / determined to be malware, and the number of unknown files that are under analysis. See '**Unknown File Statistics**' to find out more.
- **Settings** - Configure your Valkyrie account details. Allows you to update your account details and antivirus vendors. See '**Configre Valkyrie Account Settings**' for more details.
  - **My Account -** Allows you to update account details such as name, current password and more. See **Account configuration** to find out more.
  - **Antivirus Vendors** - Choose which AV software you have used in the past or are currently using. Valkyrie uses this data to dynamically compare it's performance with that of competing solutions. For example, the 'Undetected by your previous vendor' column in the 'Unparalleled Protection' section is determined by the vendor you choose here. See **Antivirus Vendors** to find out more.

4.1 Valkyrie Dashboard

The Valkyrie dashboard shows a top-level summary of Valkyrie results on files that you have submitted.

This lets you quickly view the total number of files uploaded, queried, processed and in progress.

To view your dashboard

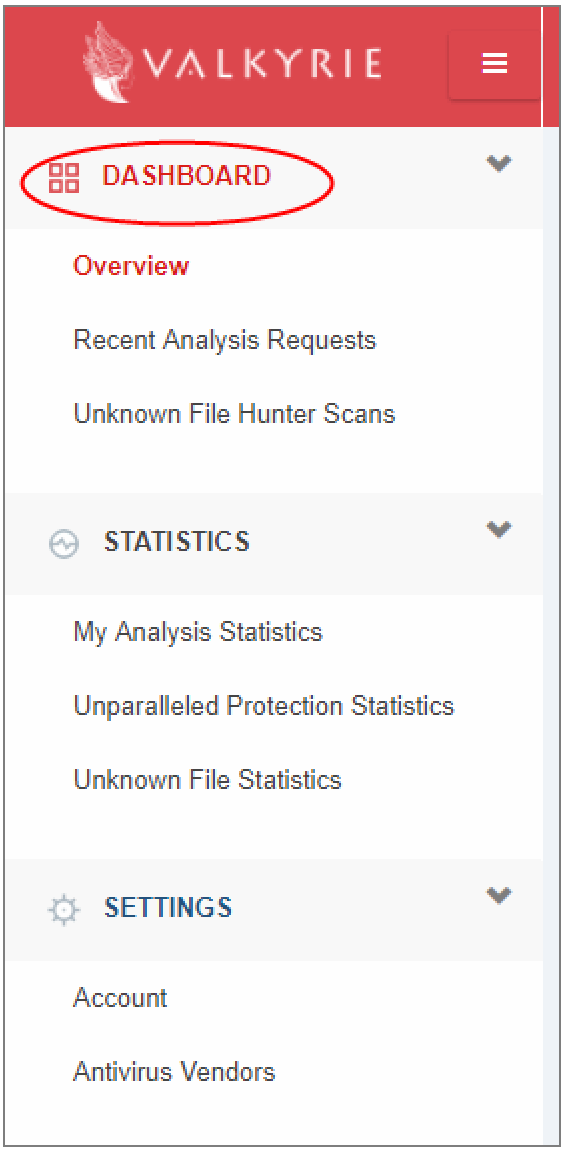
- Click your account name at the top-right and then 'Dashboard' from the left-hand menu

  OR
- Click the hamburger icon at top-left then 'Dashboard'
- **Note:** The charts in the dashboard are a historical record of malware that was found on your devices at a given time. They do not necessarily mean you have active malware on your devices right now, especially if you have security software installed to clean the threats.

  For example, the 'Today' stats might show that malware was detected on your devices.

  However, your security software may already have handled those threats.

  The 'Today' figure will return to zero at 00.00 AM the next day if the threats are no longer active.



The dashboard has three sections:

- **Overview -** Real-time charts and graphs showing key data about unknown files and threats on devices in your network. See **Overview** for more details.

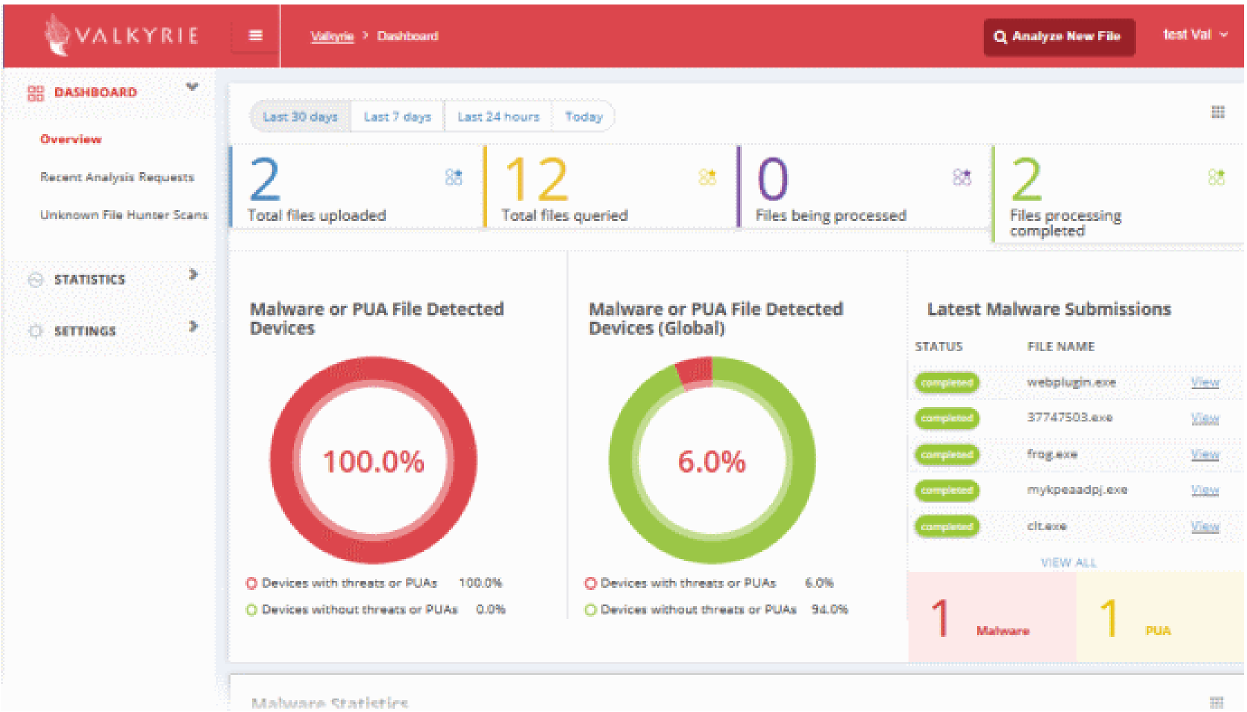
- **Recent Analysis Requests -** Shows trust verdicts on files which you have recently uploaded to Valkyrie for analysis. You can download reports on each file, submit a file for testing on Virus Total and submit a file for human analysis. See **Recent Analysis Requests** for more details.
- **Unknown File Hunter Scans -** Valkyrie verdicts on files discovered and submitted by Comodo's Unknown File Hunter (UFH) tool. Comodo UFH is a lightweight scanner designed to find all unknown files on your network. You then have the option to upload these files to Valkyrie for analysis. See **Unknown File Hunter Scans** to find out more.

Overview

The overview contains charts, graphs and statistics about Valkyrie results on unknown files in your network.

To open the overview:

- Click the hamburger button at the top-left
- Click 'Dashboard' > 'Overview' on the left-menu

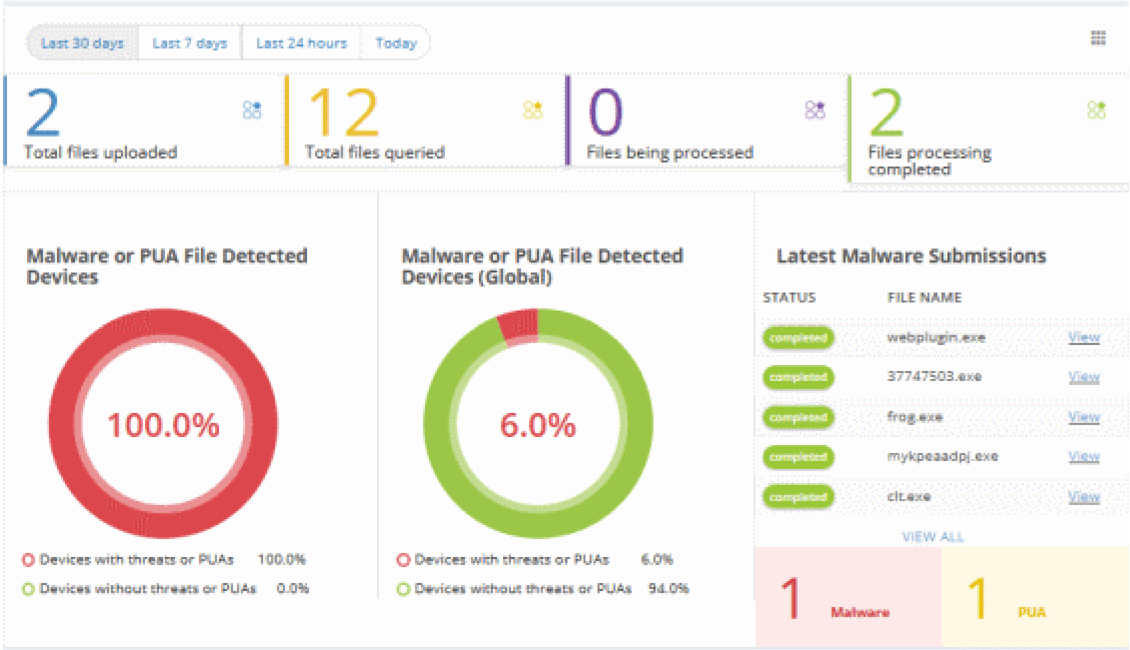

VALKYRIE
Valkyrie > Dashboard
Analyze New File
test Val
DASHBOARD
Overview
Recent Analysis Requests
Unknown File Hunter Scans
STATISTICS
SETTINGS
Last 30 days
Last 7 days
Last 24 hours
Today
2
Total files uploaded
12
Total files queried
0
Files being processed
2
Files processing completed
Malware or PUA File Detected Devices
100.0%
Devices with threats or PUAs 100.0%
Devices without threats or PUAs 0.0%
Malware or PUA File Detected Devices (Global)
6.0%
Devices with threats or PUAs 6.0%
Devices without threats or PUAs 94.0%
Latest Malware Submissions
VIEW ALL
1 Malware
1 PUA
Malware Statistics

STATUS	FILE NAME	
completed	webplugin.exe	View
completed	37747503.exe	View
completed	frog.exe	View
completed	mykpeaadpj.exe	View
completed	clt.exe	View

'Overview' contains the following items:

File Statistics

An overall summary of file totals:


Last 30 days
Last 7 days
Last 24 hours
Today
2
Total files uploaded
12
Total files queried
0
Files being processed
2
Files processing completed
Malware or PUA File Detected Devices
100.0%
Devices with threats or PUAs 100.0%
Devices without threats or PUAs 0.0%
Malware or PUA File Detected Devices (Global)
6.0%
Devices with threats or PUAs 6.0%
Devices without threats or PUAs 94.0%
Latest Malware Submissions
VIEW ALL
1 Malware
1 PUA

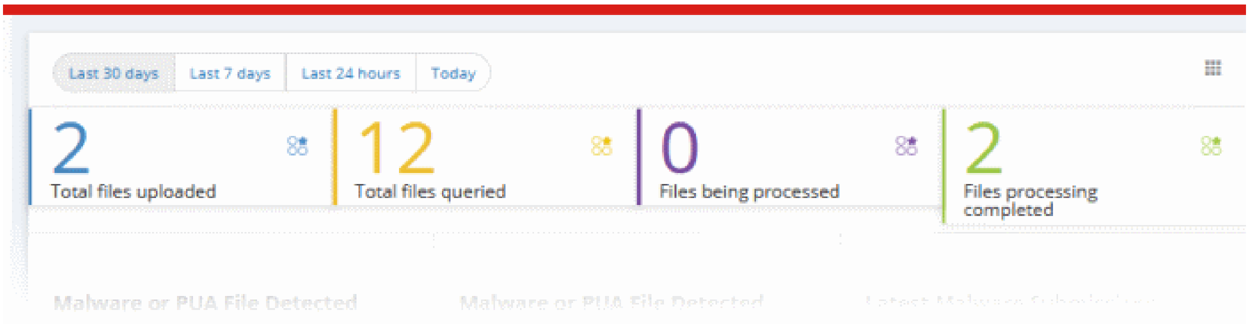
STATUS	FILE NAME	
completed	webplugin.exe	View
completed	37747503.exe	View
completed	frog.exe	View
completed	mykpeaadpj.exe	View
completed	clt.exe	View

Total files uploaded - Number of files you have submitted using the Valkyrie web interface (direct upload).

Total files queried - Total number of files submitted by your account. This figure incorporates files submitted by direct upload and those submitted by Comodo software and services like Unknown File Hunter, Forensic Analysis Tool, Comodo Client Security and Comodo Cloud Antivirus.

Files being processed - Number of files currently being analyzed by Valkyrie

Files processing completed - Number of files which have been successfully analyzed



You can view data on files submitted within the last 30 days / 7 days / 24 hours / today by clicking the appropriate link at the top of the interface.

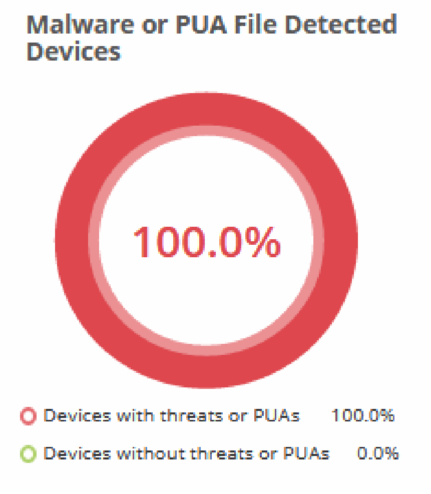
Malware or PUA File Detected Devices

Shows how many of your devices contain or contained malware/PUAs versus those that are clean.

The chart is a history of malware found on your devices rather than a concrete indicator of currently active malware. For example, your security software may already have removed the malware shown in the 'Today' statistics. The statistics for 'Today' will reset at 00.00 AM.

Place your mouse cursor over items in the legend to change the information displayed in the chart.

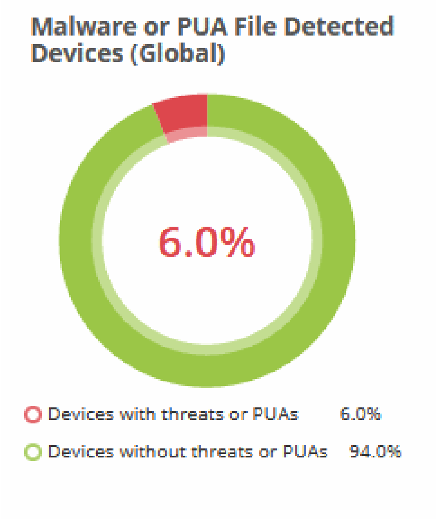
PUA stands for 'Potentially Unwanted Application'. While not strictly speaking malware, these applications are often bundled with legitimate software and might have been installed without a user's knowledge. Often they have unclear objectives. An example is a browser toolbar which purports to offer weather advice, but which also serves adverts or tracks internet usage.



Malware or PUA File Detected Devices(Global)

The 'Global' charts show aggregated data for all Valkyrie customers. This chart shows how many devices contain malware versus those that are clean across the entire Valkyrie user-base.

Place your mouse cursor over items in the legend to change the information displayed in the chart.

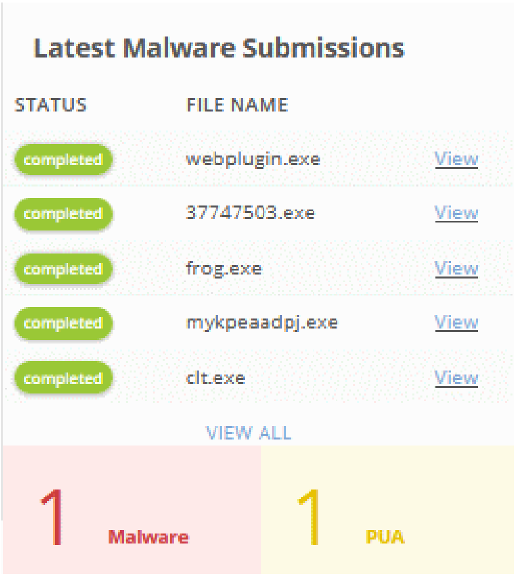


Latest Malware Submissions

Shows the files you have most-recently submitted for analysis.

Click 'View' to open a detailed report on an individual file.

Click 'View All' to see a list of verdicts and other information on all submitted files.



Latest Malware Submissions

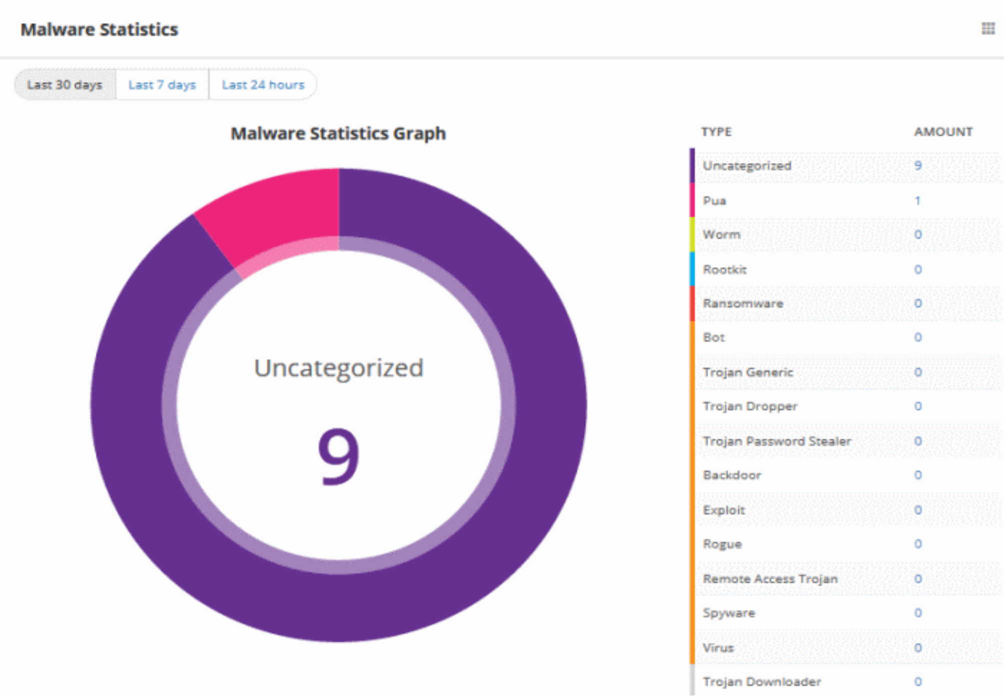
STATUS	FILE NAME	
completed	webplugin.exe	View
completed	37747503.exe	View
completed	frog.exe	View
completed	mykpeaadpj.exe	View
completed	clt.exe	View

Malware Statistics

Shows the quantity of various malware types discovered on your devices. Example malware types include worms, rootkits, ransomware, and password stealers.

Place your mouse cursor over items in the legend to change the information displayed in the chart.

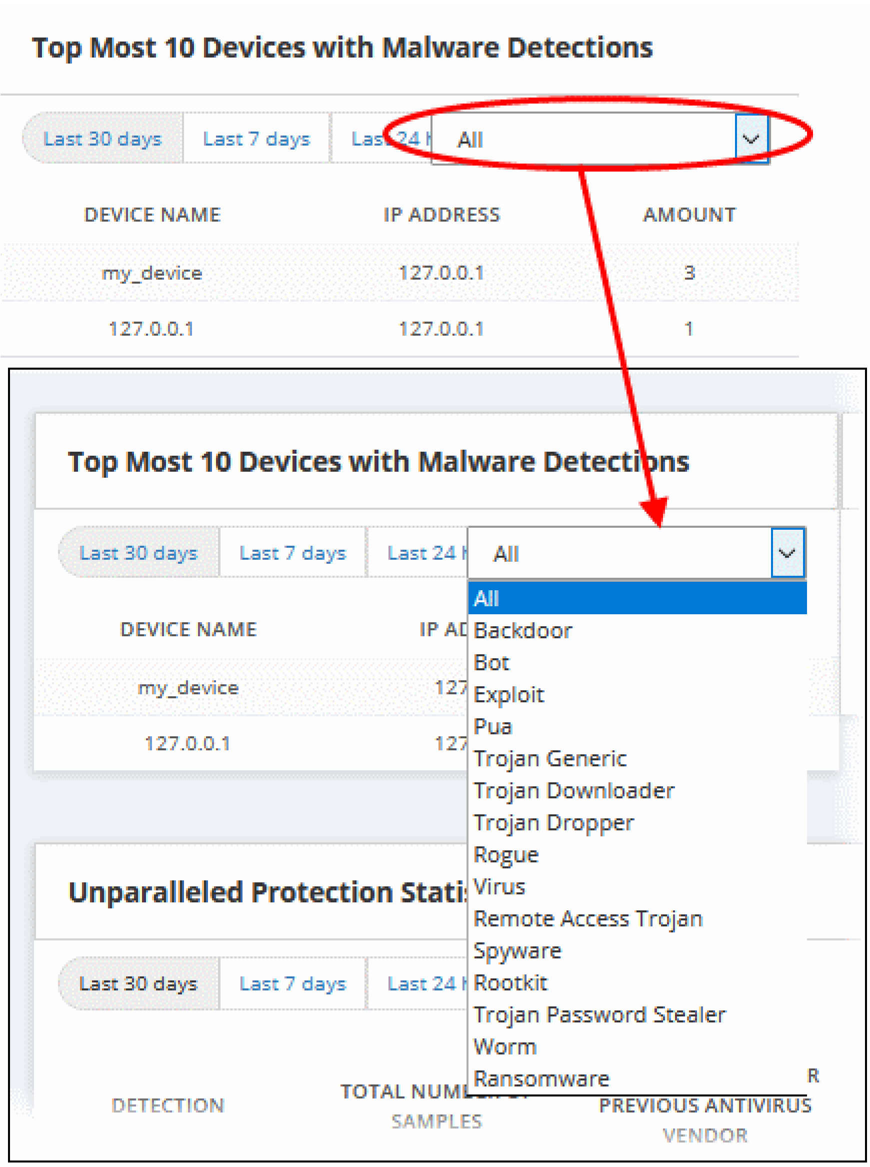
You can view data on malware found within the last 30 days / 7 days / 24 hours / today by clicking the appropriate link at the top of the interface.



TYPE	AMOUNT
Uncategorized	9
Pua	1
Worm	0
Rootkit	0
Ransomware	0
Bot	0
Trojan Generic	0
Trojan Dropper	0
Trojan Password Stealer	0
Backdoor	0
Exploit	0
Rogue	0
Remote Access Trojan	0
Spyware	0
Virus	0
Trojan Downloader	0

Top Most 10 Devices with Malware Detection

The 10 devices upon which most malware was found. The chart shows 'All' types of malware by default. You can choose specific types of malware using the drop-down to the right.



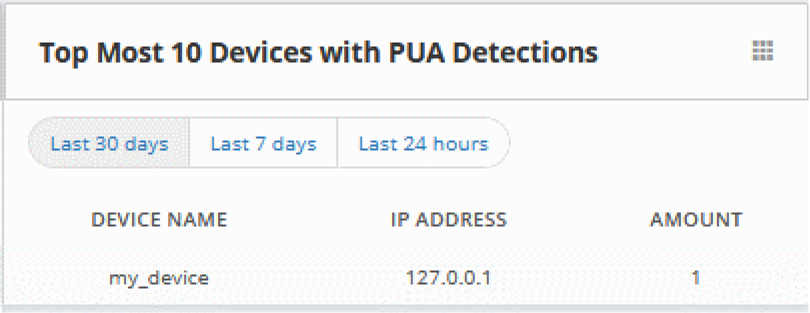
Top Most 10 Devices with Malware Detections

DEVICE NAME	IP ADDRESS	AMOUNT
my_device	127.0.0.1	3
127.0.0.1	127.0.0.1	1

Top Most 10 Devices with PUA Detections

The 10 devices upon which most Potential Unwanted Applications were found.

PUA stands for 'Potentially Unwanted Application'. While not strictly speaking malware, these applications are often bundled with legitimate software and might have been installed without a user's knowledge. Often they have unclear objectives. An example is a browser toolbar which purports to offer weather advice, but which also serves adverts or tracks internet usage.



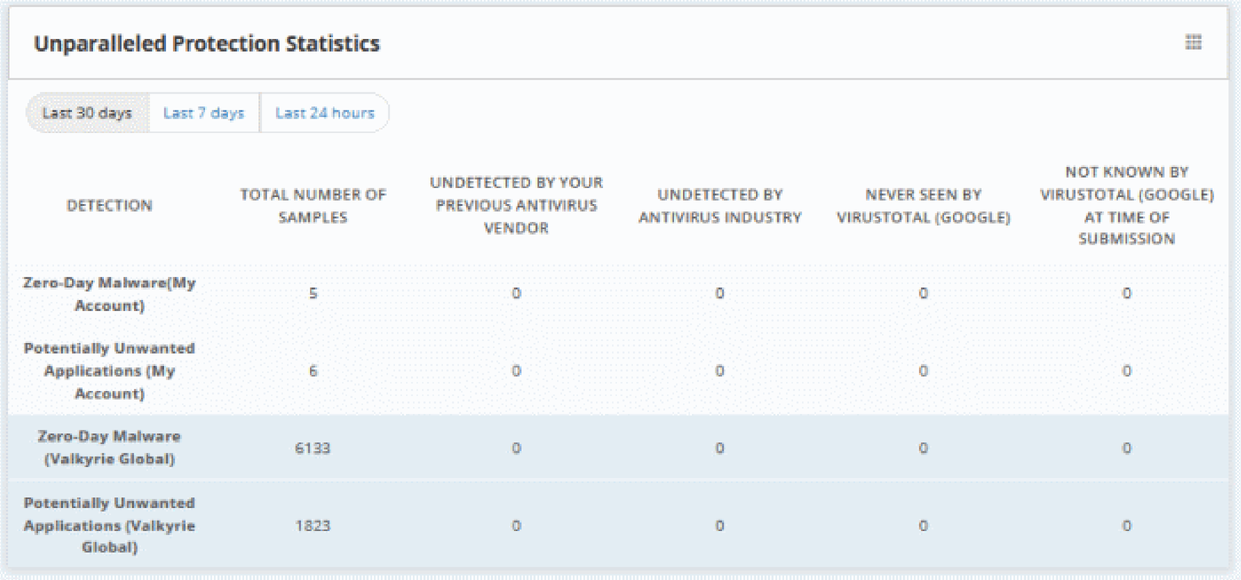
Top Most 10 Devices with PUA Detections

DEVICE NAME	IP ADDRESS	AMOUNT
my_device	127.0.0.1	1

You can view data within the last 30 days / 7 days / 24 hours / today by clicking the appropriate link at the top of the interface.

Unparalleled Protection Statistics

Unparalleled protection shows files which Valkyrie found to be malware before any other vendor in the antivirus industry. The table shows data for zero-day malware and zero-day PUA's for both your account and for all Valkyrie users (global).



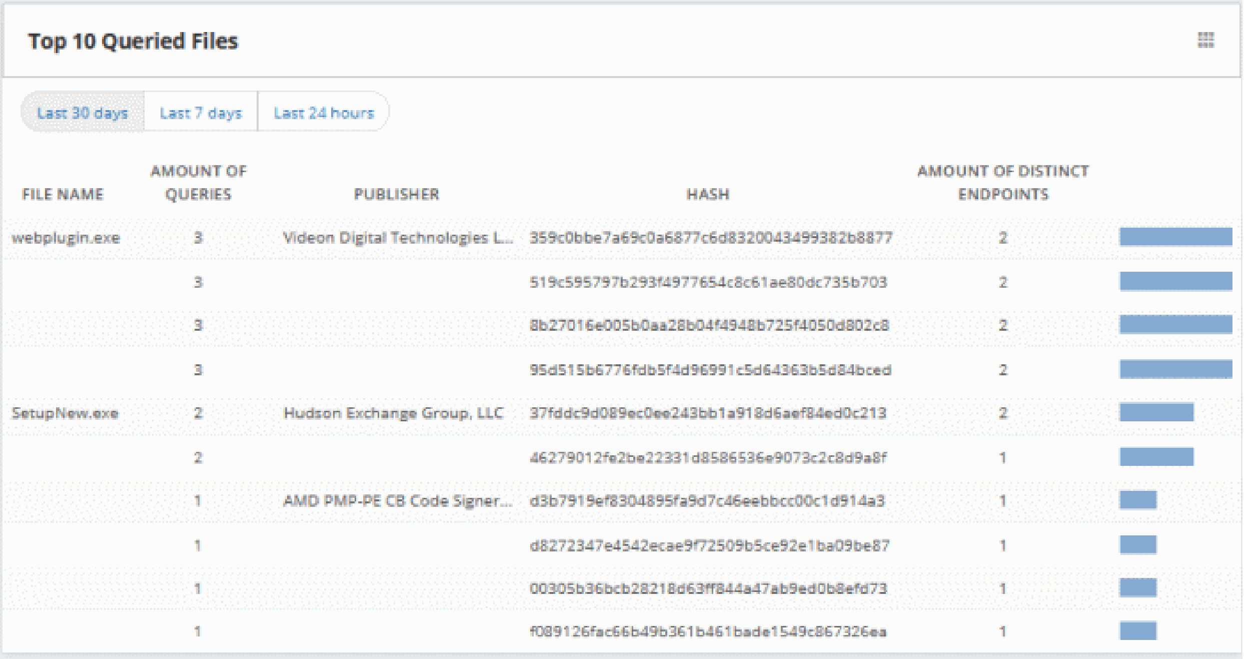
Unparalleled Protection Statistics

DETECTION	TOTAL NUMBER OF SAMPLES	UNDETECTED BY YOUR PREVIOUS ANTIVIRUS VENDOR	UNDETECTED BY ANTIVIRUS INDUSTRY	NEVER SEEN BY VIRUSTOTAL (GOOGLE)	NOT KNOWN BY VIRUSTOTAL (GOOGLE) AT TIME OF SUBMISSION
Zero-Day Malware(My Account)	5	0	0	0	0
Potentially Unwanted Applications (My Account)	6	0	0	0	0
Zero-Day Malware (Valkyrie Global)	6133	0	0	0	0
Potentially Unwanted Applications (Valkyrie Global)	1823	0	0	0	0

You can view data within the last 30 days / 7 days / 24 hours / today by clicking the appropriate link at the top of the interface.

Top 10 Queried Files

Shows the 10 files which have been most often submitted for analysis. The table shows the file name, the number of queries and the number of endpoints on which the file was found.



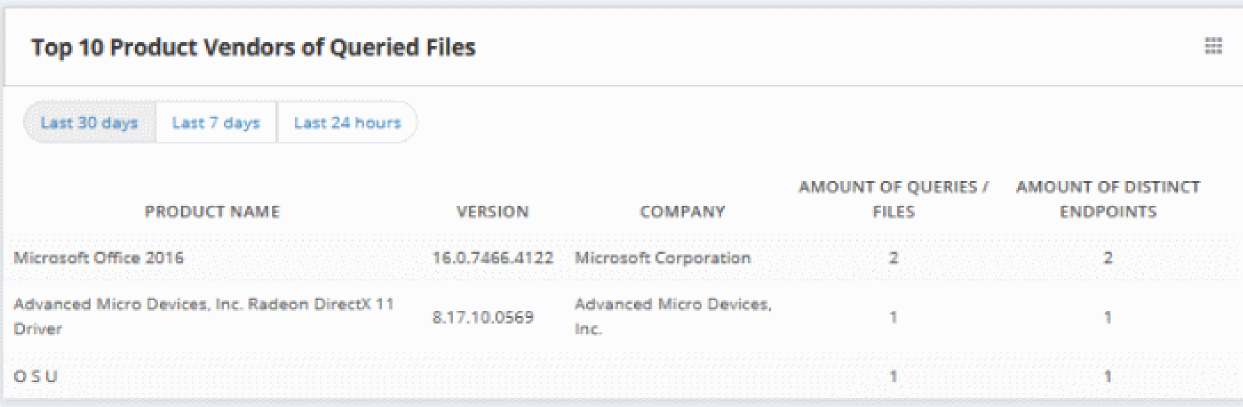
Top 10 Queried Files

FILE NAME	AMOUNT OF QUERIES	PUBLISHER	HASH	AMOUNT OF DISTINCT ENDPOINTS
webplugin.exe	3	Videon Digital Technologies L...	359c0bbe7a69c0a6877c6d8320043499382b8877	2
	3		519c595797b293f4977654c8c61ae80dc735b703	2
	3		8b27016e005b0aa28b04f4948b725f4050d802c8	2
	3		95d515b6776fdb5f4d96991c5d64363b5d84bced	2
SetupNew.exe	2	Hudson Exchange Group, LLC	37fddc9d089ec0ee243bb1a918d6aef84ed0c213	2
	2		46279012fe2be22331d8586536e9073c2c8d9a8f	1
	1	AMD PMP-PE CB Code Signer...	d3b7919ef8304895fa9d7c46eebbcc00c1d914a3	1
	1		d8272347e4542ecae9f72509b5ce92e1ba09be87	1
	1		00305b36bcb28218d63ff844a47ab9ed0b8efd73	1
	1		f089126fac66b49b361b461bade1549c867326ea	1

You can view data within the last 30 days / 7 days / 24 hours / today by clicking the appropriate link at the top of the interface.

Top 10 Product Vendors of Queried files

Shows the 10 software publishers who are responsible for most file queries. A single vendor may be the publisher of multiple individual files.



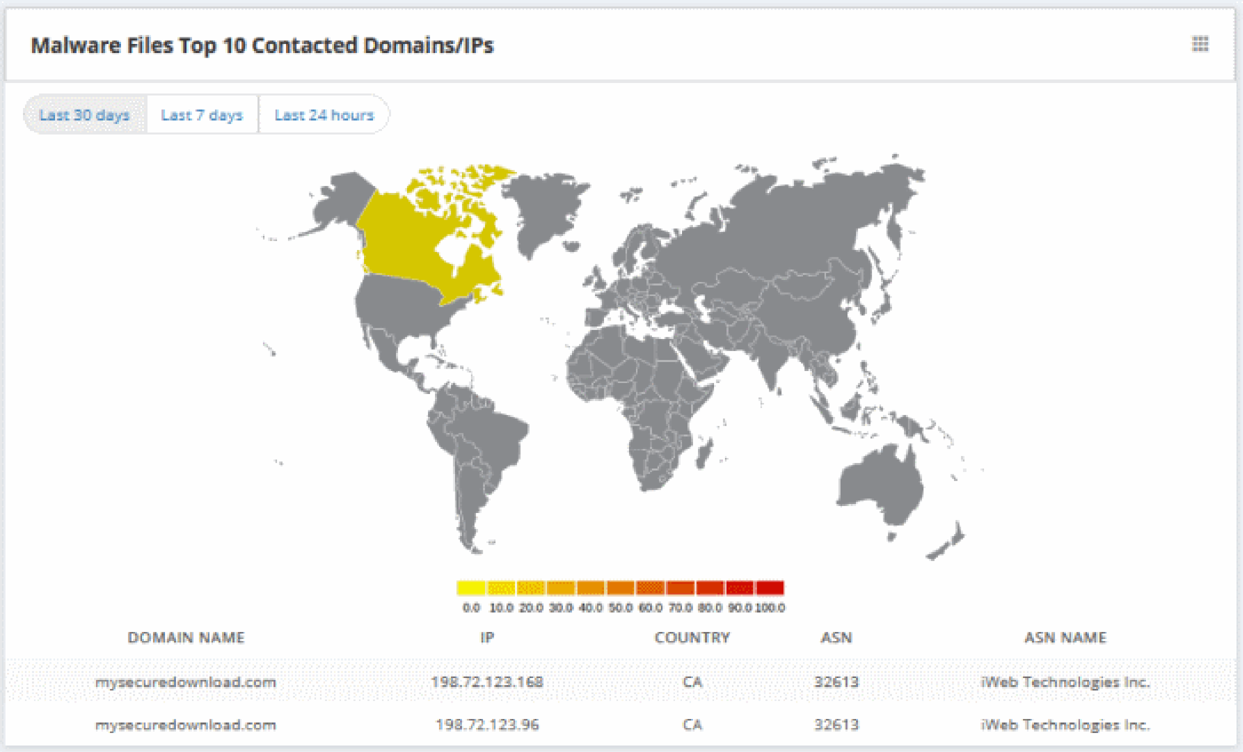
Top 10 Product Vendors of Queried Files

PRODUCT NAME	VERSION	COMPANY	AMOUNT OF QUERIES / FILES	AMOUNT OF DISTINCT ENDPOINTS
Microsoft Office 2016	16.0.7466.4122	Microsoft Corporation	2	2
Advanced Micro Devices, Inc. Radeon DirectX 11 Driver	8.17.10.0569	Advanced Micro Devices, Inc.	1	1
O S U			1	1

You can view data within the last 30 days / 7 days / 24 hours / today by clicking the appropriate link at the top of the interface.

Malware Files top 10 Contacted Domains/IPs

The 10 IP addresses and domains which were most contacted by malware found on your devices. The table lists the addresses which were contacted and the regional internet registry that controls these addresses (ASN name). The map shows the physical locations of the addresses.



Malware Files Top 10 Contacted Domains/IPs

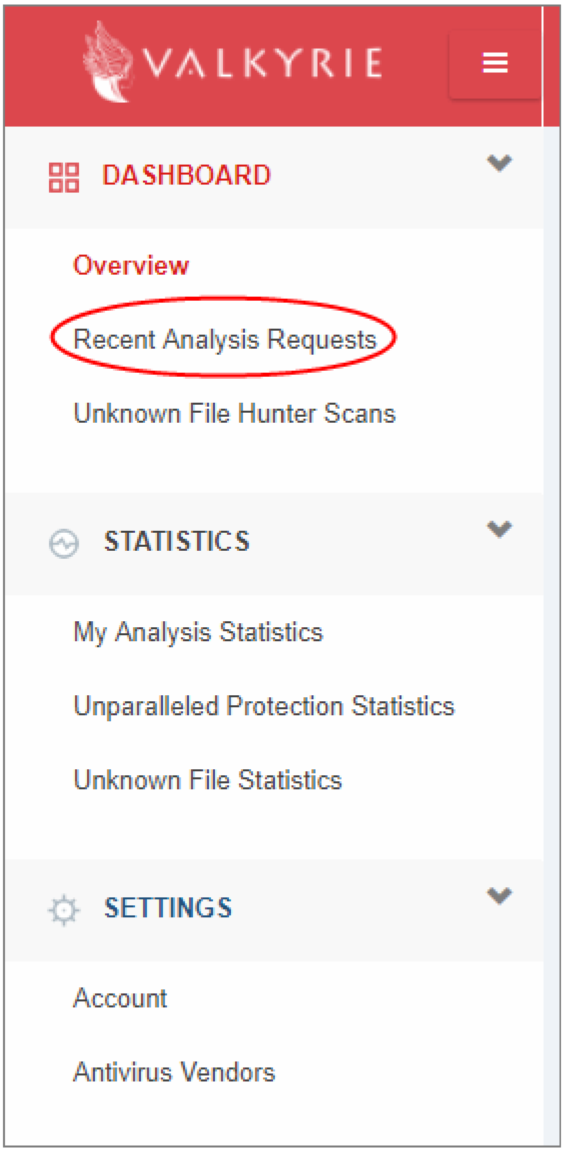
DOMAIN NAME	IP	COUNTRY	ASN	ASN NAME
mysecuredownload.com	198.72.123.168	CA	32613	iWeb Technologies Inc.
mysecuredownload.com	198.72.123.96	CA	32613	iWeb Technologies Inc.

You can view data within the last 30 days / 7 days / 24 hours / today by clicking the appropriate link at the top of the interface.

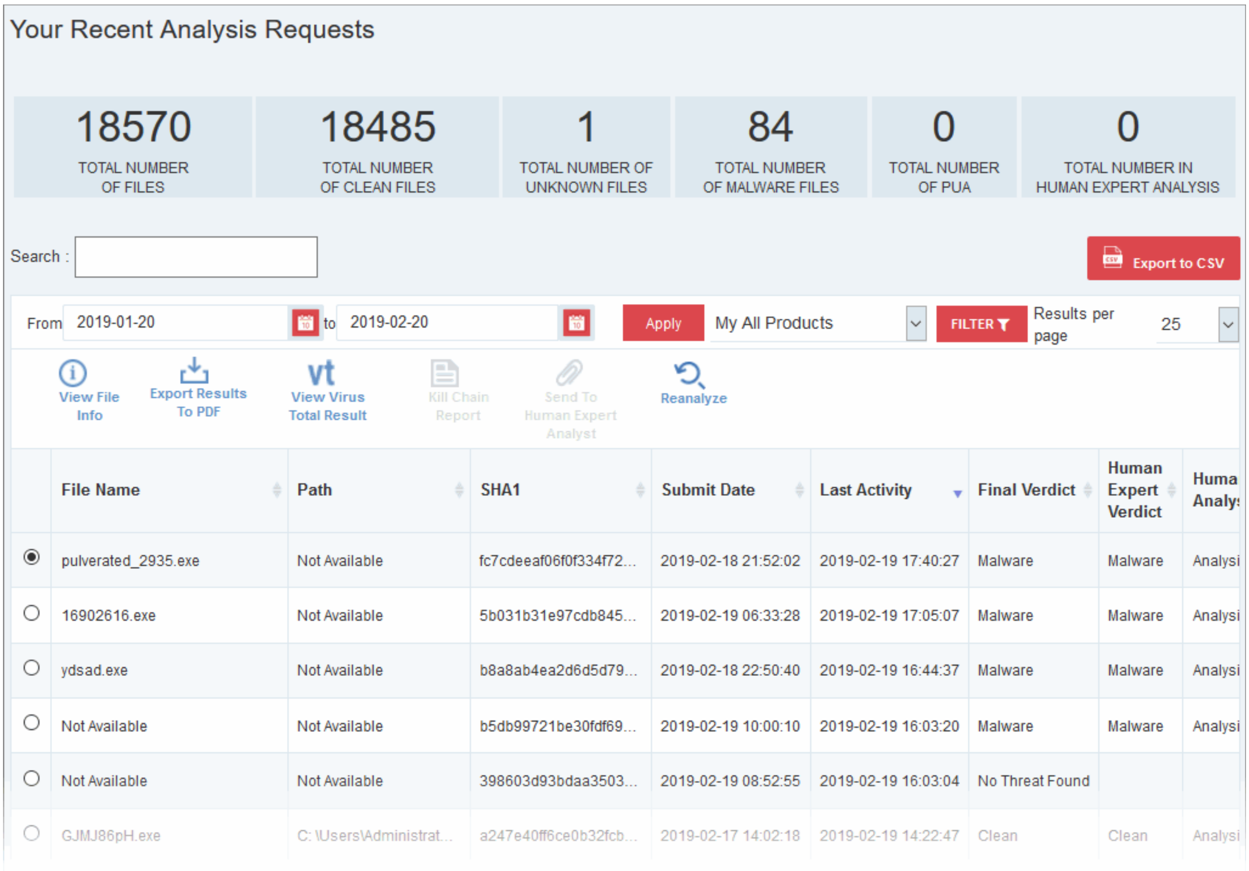
4.2 Recent Analysis Requests

To view recently analyzed files:

- Click the hamburger icon at top-left
- Click 'Dashboard' > 'Recent Analysis Requests'



The recent analysis screen shows the Valkyrie verdicts on files you have submitted (most recent first):



Your Recent Analysis Requests

18570	18485	1	84	0	0
TOTAL NUMBER OF FILES	TOTAL NUMBER OF CLEAN FILES	TOTAL NUMBER OF UNKNOWN FILES	TOTAL NUMBER OF MALWARE FILES	TOTAL NUMBER OF PUA	TOTAL NUMBER IN HUMAN EXPERT ANALYSIS

Search :

From 2019-01-20 to 2019-02-20

	File Name	Path	SHA1	Submit Date	Last Activity	Final Verdict	Human Expert Verdict	Huma Analy
●	pulverated_2935.exe	Not Available	fc7cdeeaf06f0f334f72...	2019-02-18 21:52:02	2019-02-19 17:40:27	Malware	Malware	Analysi
○	16902616.exe	Not Available	5b031b31e97cdb845...	2019-02-19 06:33:28	2019-02-19 17:05:07	Malware	Malware	Analysi
○	ydsad.exe	Not Available	b8a8ab4ea2d6d5d79...	2019-02-18 22:50:40	2019-02-19 16:44:37	Malware	Malware	Analysi
○	Not Available	Not Available	b5db99721be30fdf69...	2019-02-19 10:00:10	2019-02-19 16:03:20	Malware	Malware	Analysi
○	Not Available	Not Available	398603d93bdaa3503...	2019-02-19 08:52:55	2019-02-19 16:03:04	No Threat Found		
○	GJMJ86pH.exe	C: \Users\Administrat...	a247e40ff6ce0b32fcb...	2019-02-17 14:02:18	2019-02-19 14:22:47	Clean	Clean	Analysi

Your Recent Analysis Requests - Table of Column Descriptions	
Column Header	**Description**
File Name	Name of the submitted file.
Path	IP of the endpoint and the file path.
SHA1	SHA1 hash value of the file. Hash values, or signatures, as used to describe the file in whitelists and blacklists.
Submit Date	Date and time you uploaded the file to Valkyrie.
Last Activity	Date and time the file was submitted for analysis.
Final Verdict	The trust rating assigned to the file after Valkyrie's dynamic and static tests. Possible verdicts are: • Clean - The file is safe to run • No Threat Found - No malware found in the file, but cannot say it is safe to run • Malware - The file is harmful and should not be run
Human Expert Verdict	The trust rating assigned to the file after analysis by human experts: • Clean - File is safe to run • Malware - The file is harmful and should not be run • Potentially Unwanted Application (PUA) - Applications such as adware, spyware and browser toolbars. PUAs are not malicious per se, but may execute actions of which the user is unaware. For example, a weather toolbar may have code which tracks a user's activity on the internet

	• No Threat Found - No malware found in the file, but cannot say it is safe to run • Not Ready - Indicates human epert analysis of the file is in progress
Human Expert Analysis Status	The current status of files submitted for in-depth analysis by Comodo experts. The statuses are: • In Queue - The analysis has not yet started • In Progress - The analysis is currently underway • Analysis Completed - The analysis has finished. Verdicts are displayed in the 'Human Expert Verdict'. • Objected - Indicates the user has requested another analysis on the file. Users can re-submit files for testing if they think the verdict is incorrect. • Objection Completed - Indicates the manual re-analysis has finished.
Available Actions	Perform additional file activities: **Download** – Save a local copy of the file **Reanalyze** – Send the file back to Valkyrie for another round of automated tests **Send to human expert analysis** – Submit the file to Comodo technicians for manual testing

- Use the radio buttons on the left to select a file. This will activate the following options:

ⓘ View File Info - View File Info - Opens detailed information about the file. This includes the file type, file hash values, the number on endpoints on which it was found, the file's final trust rating and the results of individual tests. See '**File Analysis Results**' for more details.

Export Results To PDF - Export Results to PDF - Save a copy of the report in PDF format. See '**Download Automatic Analysis Report**' for more details.

vt View Virus Total Result - View Virus Total Result - Opens the Virus Total results page for the file. Virus Total is a meta-analysis website which reports verdicts on the file from multiple antivirus vendors. Note - Virus Total may not have results available if the file is 'Unknown'. See '**View Virus Total Results for the File**' for more details.

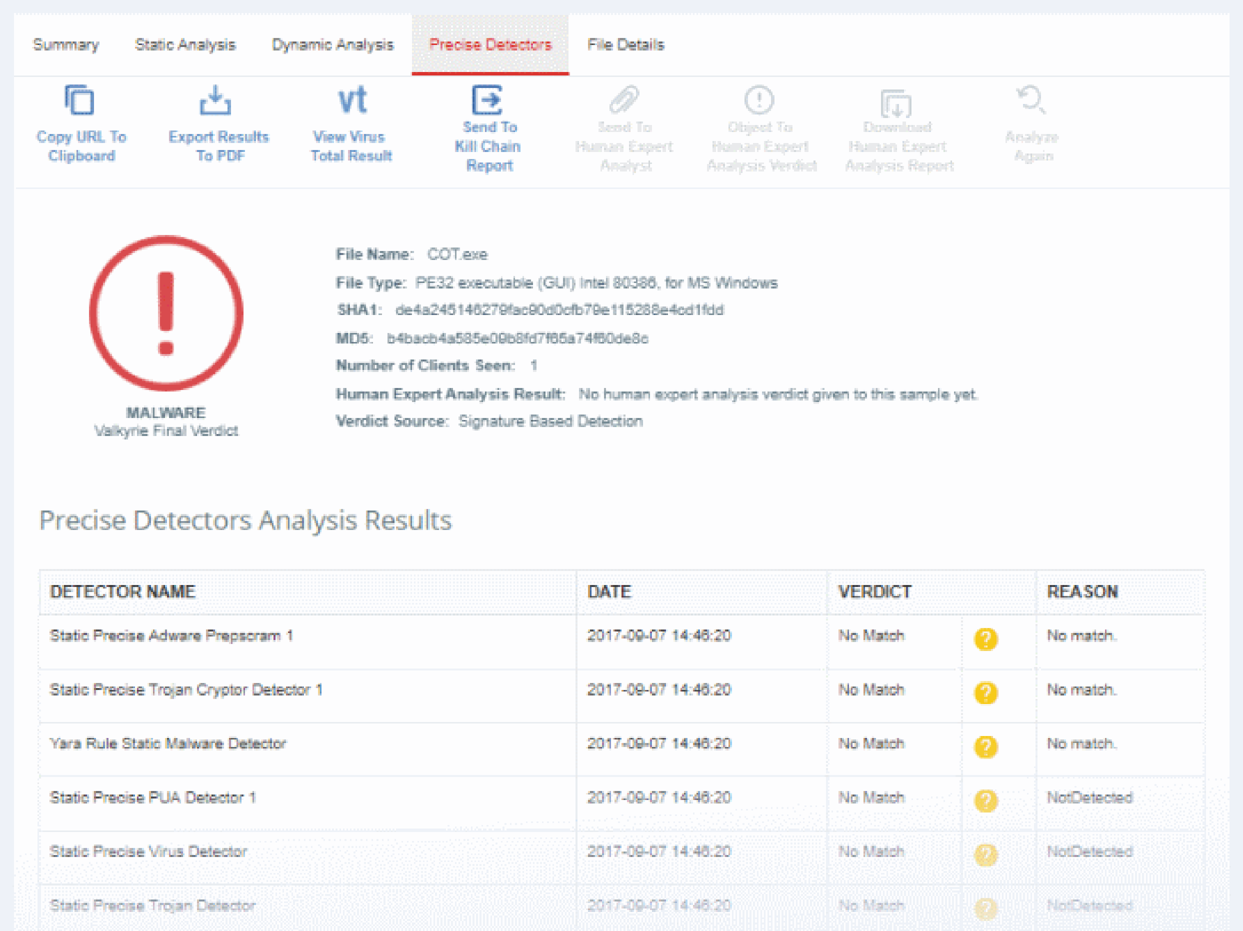
Send To Human Expert Analyst - Send to Human Expert Analysis (Premium and Consumer Premium licenses only) - Allows you to submit the file for inspection by Comodo technicians. See '**Send the File for Manual Analysis**' for more details.

Kill Chain Report - Kill Chain Report - View a granular analysis on the activities and threats posed by the file. See '**Kill Chain Report**' for more details.

Reanalyze - Reanalyze – Resubmit the file to Valkyrie for another round of dynamic and static tests.

File Analysis Results

- Click the 'View File Info' icon View File Info above the results table to view detailed file information:



File Name: COT.exe

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

SHA1: de4a245146279fac90d0cfb79e115288e4cd1fdd

MD5: b4bacb4a585e09b8fd7f65a74f60de8c

Number of Clients Seen: 1

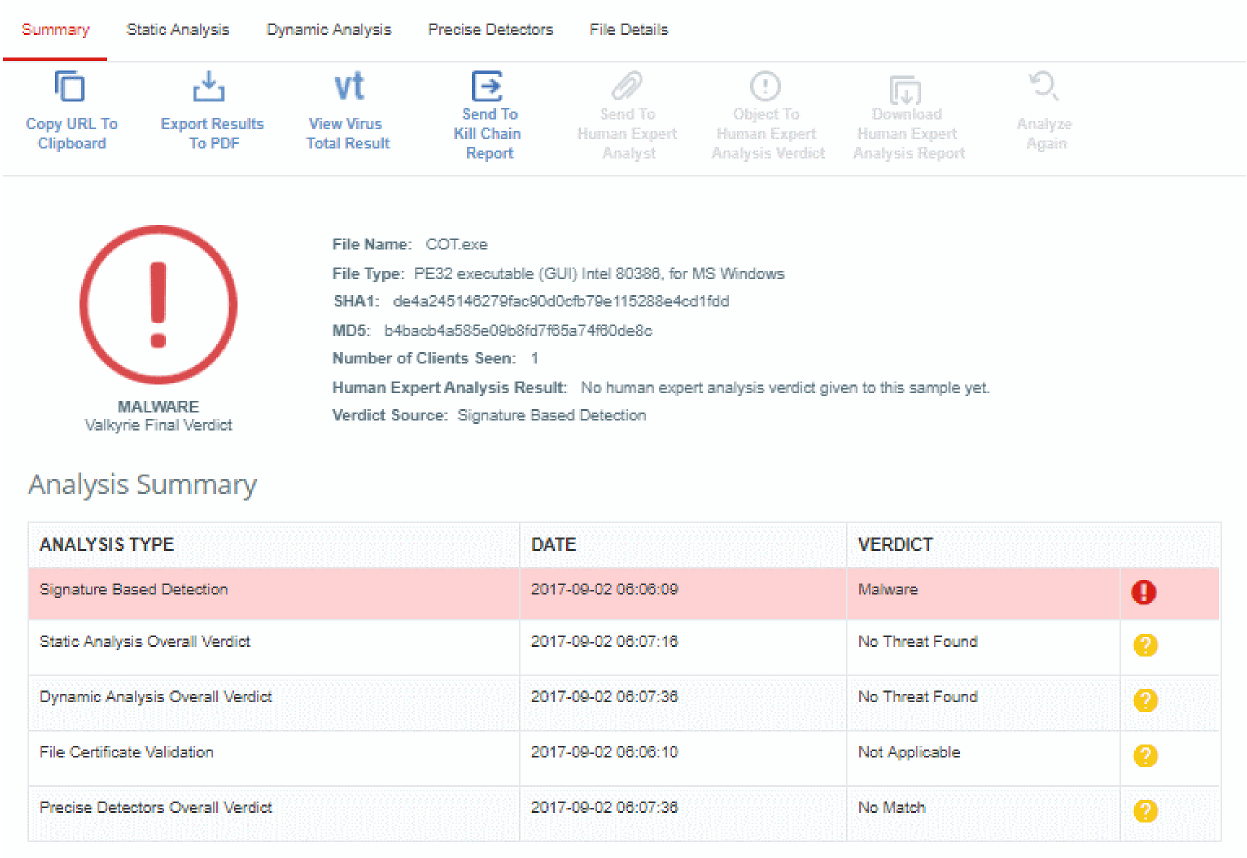
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.

Verdict Source: Signature Based Detection

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise Adware Prepscram 1	2017-09-07 14:46:20	No Match	?	No match.
Static Precise Trojan Cryptor Detector 1	2017-09-07 14:46:20	No Match	?	No match.
Yara Rule Static Malware Detector	2017-09-07 14:46:20	No Match	?	No match.
Static Precise PUA Detector 1	2017-09-07 14:46:20	No Match	?	NotDetected
Static Precise Virus Detector	2017-09-07 14:46:20	No Match	?	NotDetected
Static Precise Trojan Detector	2017-09-07 14:46:20	No Match	?	NotDetected

Summary – Contains general file details and the results of individual tests on the file:



File Name: COT.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: de4a245146279fac90d0cfb79e115288e4cd1fdd
MD5: b4bacb4a585e09b8fd7f65a74f60de8c
Number of Clients Seen: 1
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

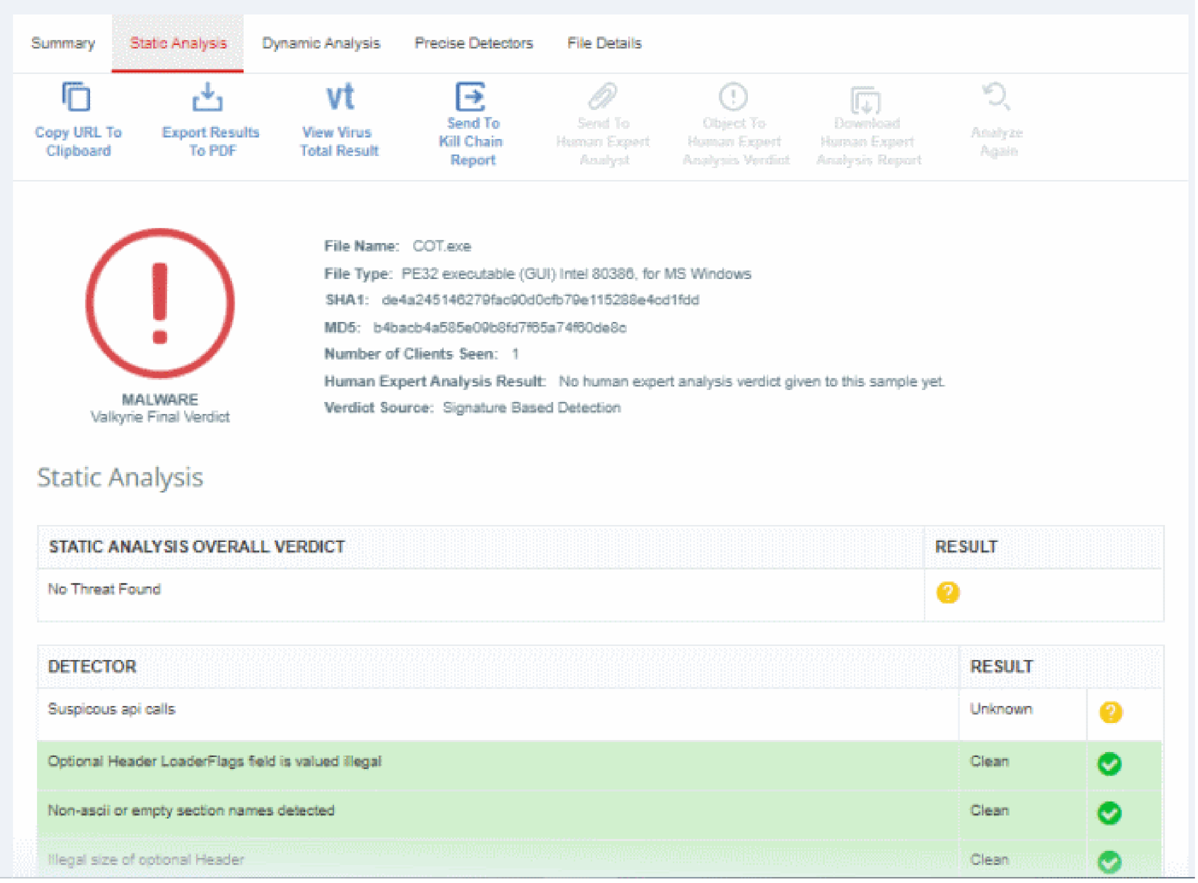
Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2017-09-02 06:06:09	Malware	!
Static Analysis Overall Verdict	2017-09-02 06:07:16	No Threat Found	?
Dynamic Analysis Overall Verdict	2017-09-02 06:07:36	No Threat Found	?
File Certificate Validation	2017-09-02 06:06:10	Not Applicable	?
Precise Detectors Overall Verdict	2017-09-02 06:07:36	No Match	?

Static Analysis - Static tests include analyzing the file's binary properties, entropy, packer type and more. Any deviation from expected values provides clues 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 static analysis of the file, click the 'Static Analysis' tab



File Name: COT.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: de4a245146279fac90d0cfb79e115288e4cd1fdd
MD5: b4bacb4a585e09b8fd7f65a74f60de8c
Number of Clients Seen: 1
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

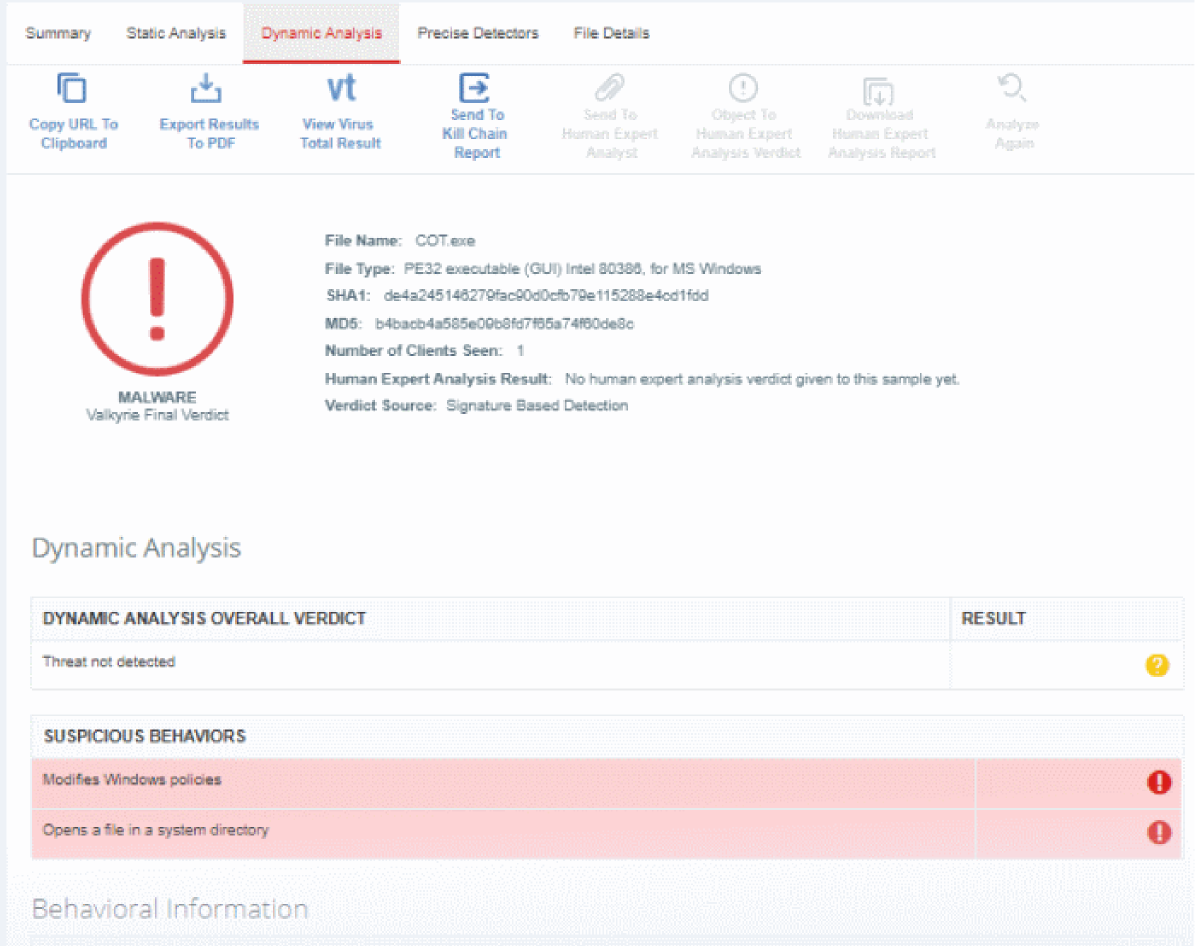
Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	?

DETECTOR	RESULT	
Suspicous api calls	Unknown	?
Optional Header LoaderFlags field is valued illegal	Clean	✓
Non-ascii or empty section names detected	Clean	✓
Illegal size of optional Header	Clean	✓

Dynamic Analysis – Dynamic tests cover the run-time behavior of the file in the test environment. The page provides a overall dynamic-test verdict and behavioral information about the file. Scroll down the page to view more detailed information.

- To view the dynamic analysis of the submitted files, click the 'Dynamic Analysis' tab



File Name: COT.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: de4a245146279fac90d0cfb79e115288e4cd1fdd
MD5: b4bacb4a585e09b8fd7f65a74f60de8c
Number of Clients Seen: 1
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Dynamic Analysis

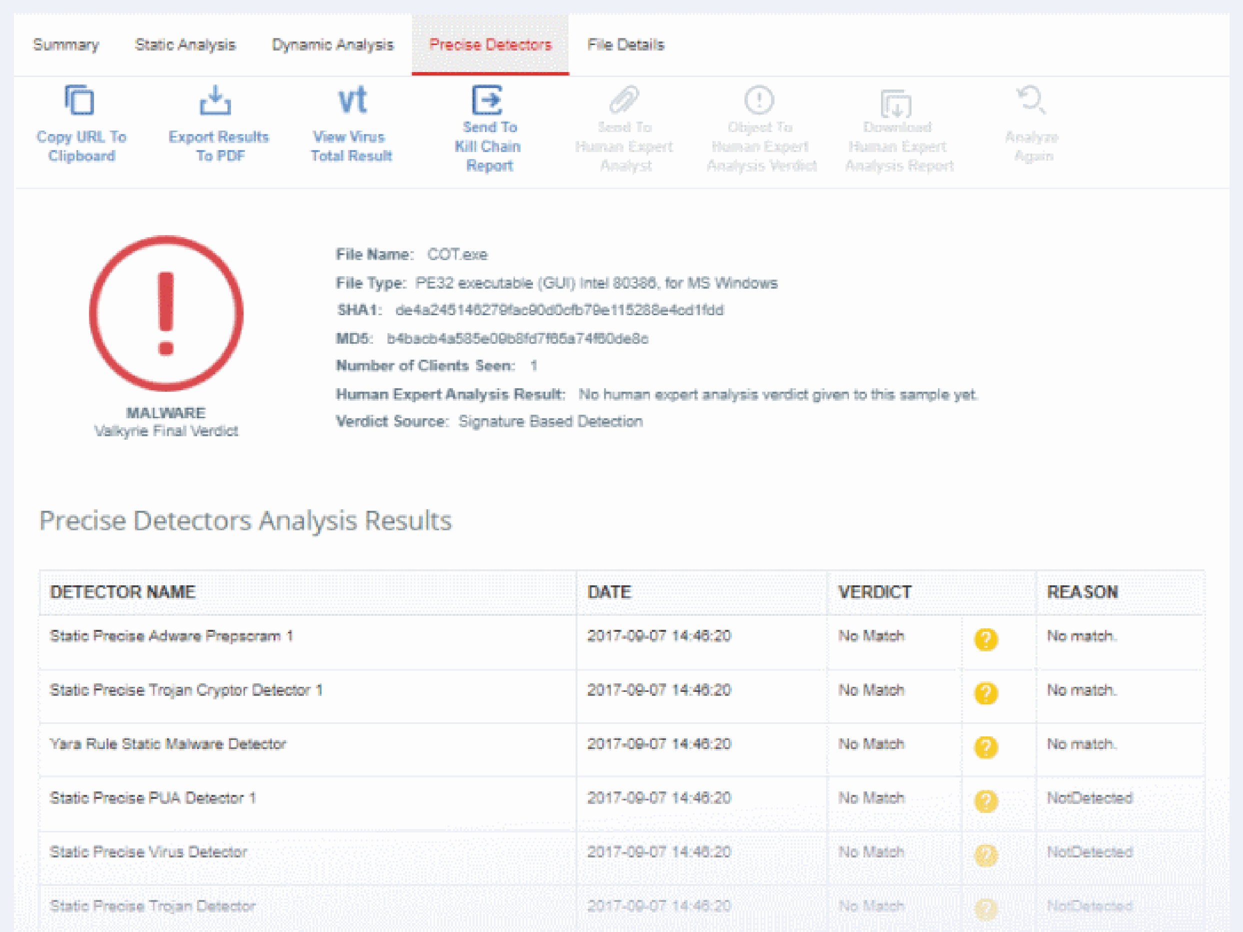
DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
Threat not detected	?

SUSPICIOUS BEHAVIORS	
Modifies Windows policies	!
Opens a file in a system directory	!

Behavioral Information

Precise Detectors - Shows how the malware file fared against individual tests.

- To view this section, click the 'Precise Detectors' tab



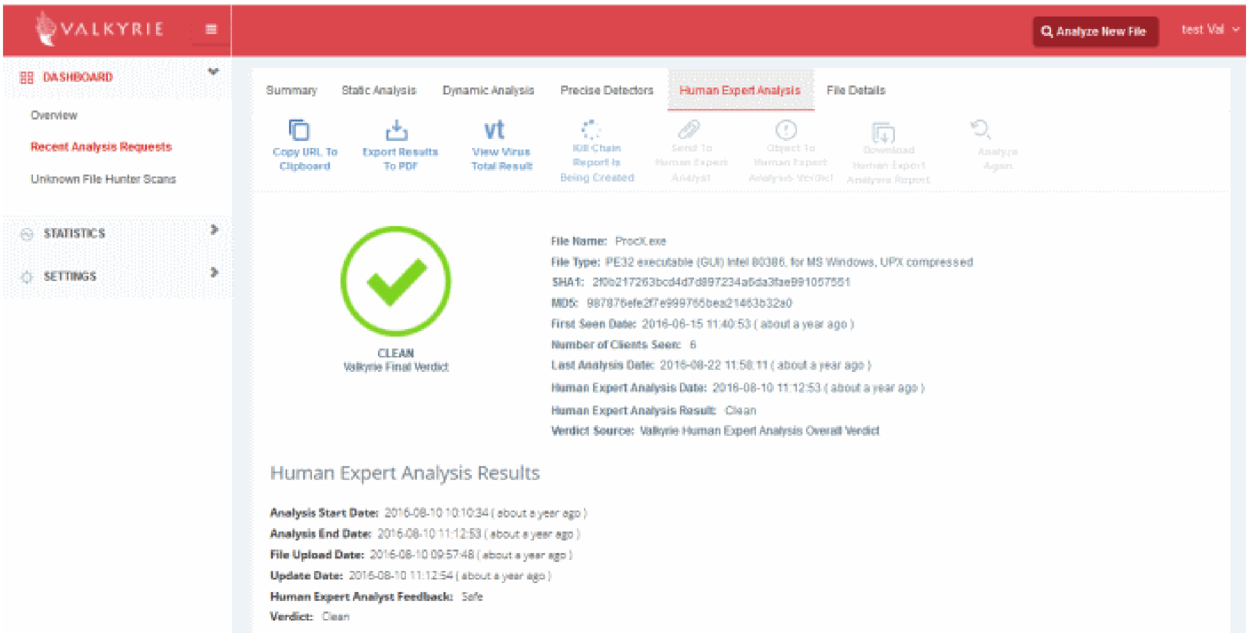
File Name: COT.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: de4a245146279fac90d0cfb79e115288e4cd1fdd
MD5: b4bacb4a585e09b8fd7f65a74f60de8c
Number of Clients Seen: 1
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise Adware Prepscram 1	2017-09-07 14:46:20	No Match	?	No match.
Static Precise Trojan Cryptor Detector 1	2017-09-07 14:46:20	No Match	?	No match.
Yara Rule Static Malware Detector	2017-09-07 14:46:20	No Match	?	No match.
Static Precise PUA Detector 1	2017-09-07 14:46:20	No Match	?	NotDetected
Static Precise Virus Detector	2017-09-07 14:46:20	No Match	?	NotDetected
Static Precise Trojan Detector	2017-09-07 14:46:20	No Match	?	NotDetected

Human Expert Analysis - Unknown files submitted for human analysis will receive in-depth inspection from Comodo's dedicated team of threat research analysts. Human Analysis can help to identify zero-day threats faster and more accurately than purely automated systems.

- To view this section, click the 'Human Expert Analysis' tab:



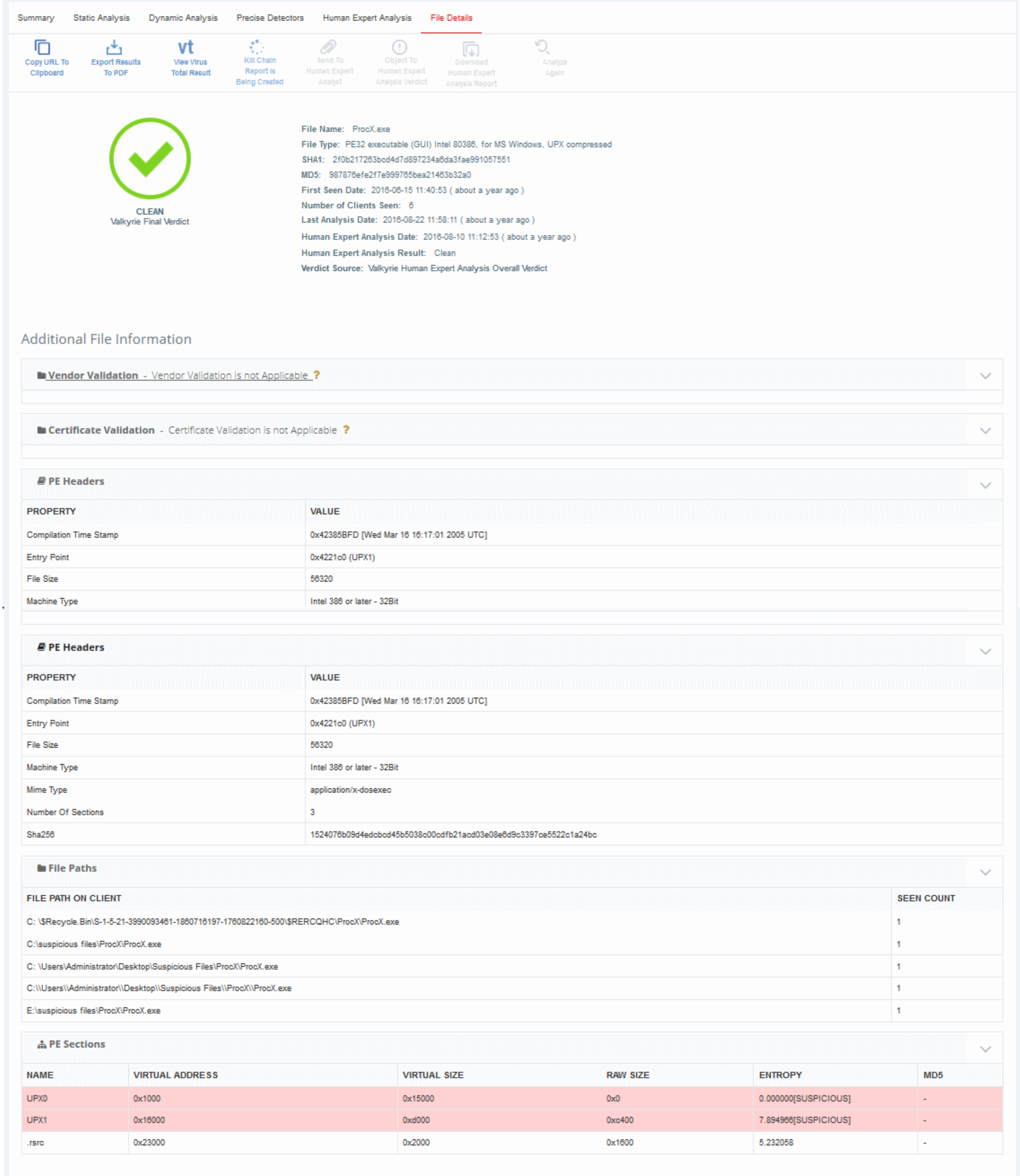
File Name: ProcX.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 2f0b217263bcd4d7d897234a6da3fae991057551
MD5: 987876efe2f7e999765bea21463b32a0
First Seen Date: 2016-06-15 11:40:53 (about a year ago)
Number of Clients Seen: 6
Last Analysis Date: 2016-08-22 11:58:11 (about a year ago)
Human Expert Analysis Date: 2016-08-10 11:12:53 (about a year ago)
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Human Expert Analysis Results

Analysis Start Date: 2016-08-10 10:10:34 (about a year ago)
Analysis End Date: 2016-08-10 11:12:53 (about a year ago)
File Upload Date: 2016-08-10 09:57:48 (about a year ago)
Update Date: 2016-08-10 11:12:54 (about a year ago)
Human Expert Analyst Feedback: Safe
Verdict: Clean

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 of the file.

- To view this section, click the 'File Details' tab:



File Name: ProcX.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 2f0b217263bcd4d7d897234a6da3fae991057551
MD5: 987876efe2f7e999765bea21463b32a0
First Seen Date: 2016-06-15 11:40:53 (about a year ago)
Number of Clients Seen: 6
Last Analysis Date: 2016-08-22 11:58:11 (about a year ago)
Human Expert Analysis Date: 2016-08-10 11:12:53 (about a year ago)
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x42385BFD [Wed Mar 16 16:17:01 2005 UTC]
Entry Point	0x4221c0 (UPX1)
File Size	56320
Machine Type	Intel 386 or later - 32Bit

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x42385BFD [Wed Mar 16 16:17:01 2005 UTC]
Entry Point	0x4221c0 (UPX1)
File Size	56320
Machine Type	Intel 386 or later - 32Bit
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	1524076b09d4edcbcd45b5038c00cdfb21acd03e08e6d9c3397ce5522c1a24bc

File Paths

FILE PATH ON CLIENT	SEEN COUNT
C: \$Recycle.Bin\S-1-5-21-3990093461-1860716197-1760822160-500\$RERCQHC\ProcX\ProcX.exe	1
C:\suspicious files\ProcX\ProcX.exe	1
C: \Users\Administrator\Desktop\Suspicious Files\ProcX\ProcX.exe	1
C:\\Users\\Administrator\\Desktop\\Suspicious Files\\ProcX\\ProcX.exe	1
E:\suspicious files\ProcX\ProcX.exe	1

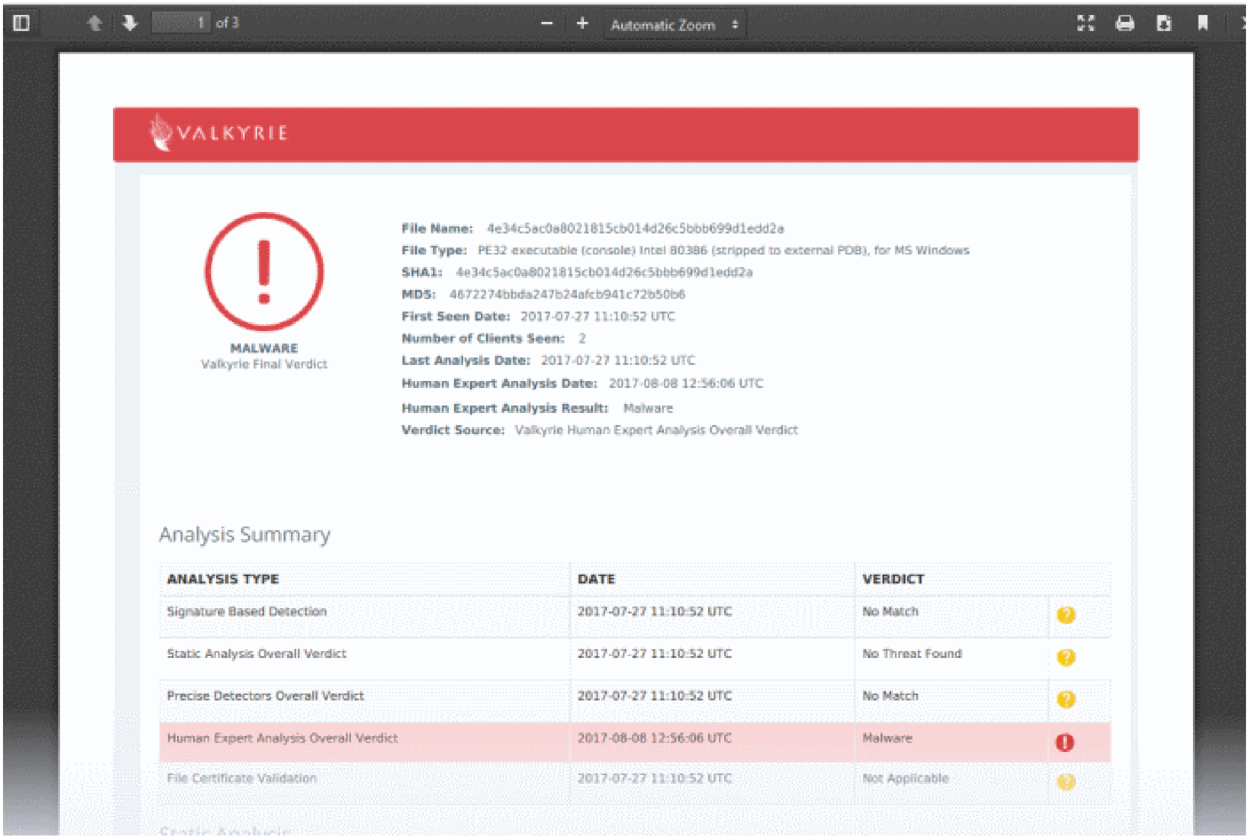
PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0x15000	0x0	0.000000[SUSPICIOUS]	-
UPX1	0x16000	0xd000	0xc400	7.894966[SUSPICIOUS]	-
.rsrc	0x23000	0x2000	0x1600	5.232058	-

Download Human Expert Analysis Report

- Click the 'Download Human Expert Analysis Report' icon to download the report in PDF format

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



MALWARE
Valkyrie Final Verdict

File Name: 4e34c5ac0a8021815cb014d26c5bbb699d1edd2a
File Type: PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows
SHA1: 4e34c5ac0a8021815cb014d26c5bbb699d1edd2a
MD5: 4672274bbda247b24afcb941c72b50b6
First Seen Date: 2017-07-27 11:10:52 UTC
Number of Clients Seen: 2
Last Analysis Date: 2017-07-27 11:10:52 UTC
Human Expert Analysis Date: 2017-08-08 12:56:06 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2017-07-27 11:10:52 UTC	No Match	?
Static Analysis Overall Verdict	2017-07-27 11:10:52 UTC	No Threat Found	?
Precise Detectors Overall Verdict	2017-07-27 11:10:52 UTC	No Match	?
Human Expert Analysis Overall Verdict	2017-08-08 12:56:06 UTC	Malware	!
File Certificate Validation	2017-07-27 11:10:52 UTC	Not Applicable	?

Static Analysis

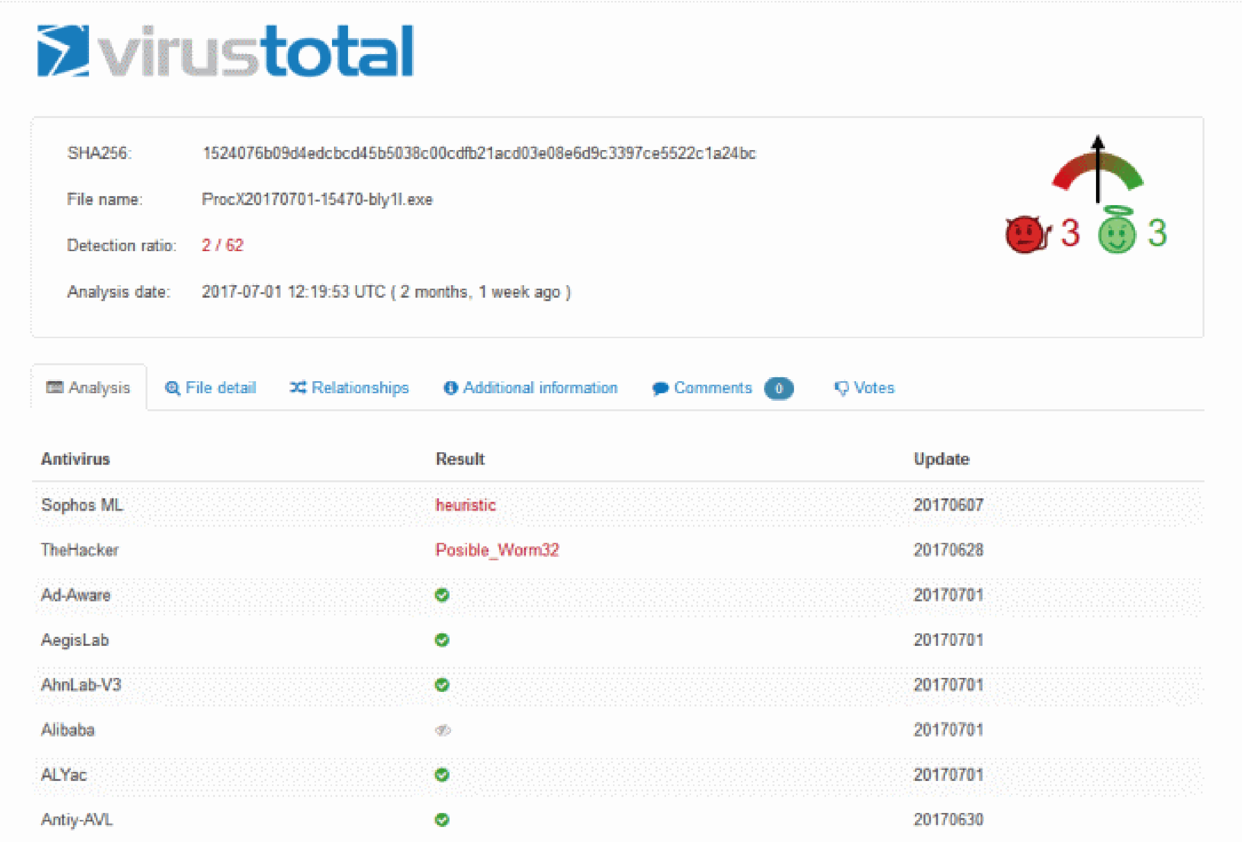
The report contains the compiled results of the automatic analysis explained in the **File Analysis Results** section. Scroll down the page to view the full report and save it.

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 Result' icon to view the Virus Total results for a file. Virus Total shows the verdicts on a particular file from a wide range of AV and security software vendors.

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



virustotal

SHA256: 1524076b09d4edcbcd45b5038c00cdfb21acd03e08e6d9c3397ce5522c1a24bc

File name: ProcX20170701-15470-bly1l.exe

Detection ratio: 2 / 62

Analysis date: 2017-07-01 12:19:53 UTC (2 months, 1 week ago)

Antivirus	Result	Update
Sophos ML	heuristic	20170607
TheHacker	Posible_Worm32	20170628
Ad-Aware	✓	20170701
AegisLab	✓	20170701
AhnLab-V3	✓	20170701
Alibaba		20170701
ALYac	✓	20170701
Antiy-AVL	✓	20170630

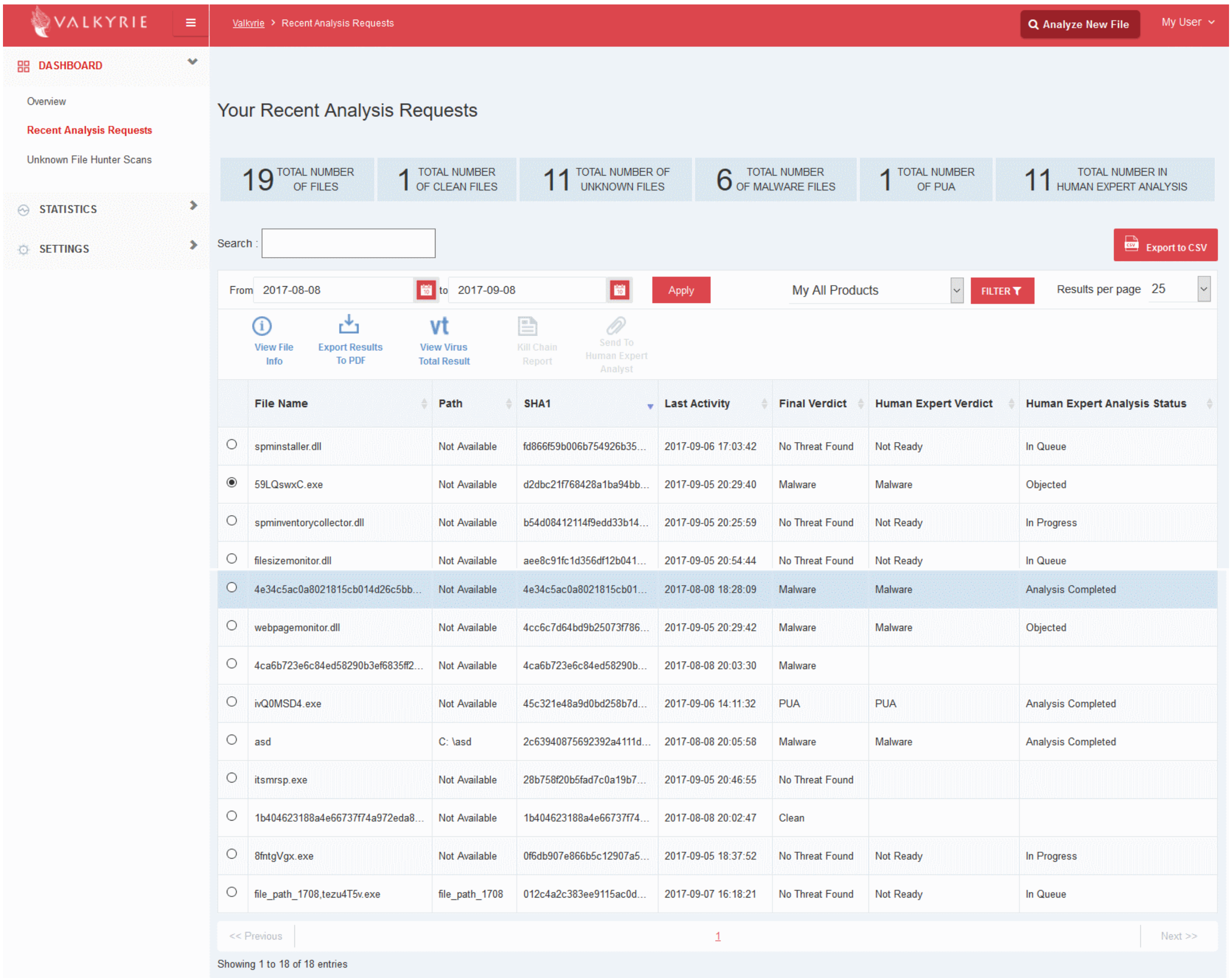
Scroll down the page to view the results for the file from different antivirus engines.

Send the File for Human Expert Analysis

You can also send a file for human expert analysis by Comodo malware specialists for more comprehensive inspection in addition to the automated process. This is a premium service and requires a subscription.

- Click the 'Send to Human Expert Analysis' icon Send To Human Expert Analyst on top of the tabular results to submit a file for manual analysis by Comodo engineers

After submitting, the file status will show as 'In Queue' in the 'Human Expert Analysis Status' column. If you have questioned the result, the status will change to 'Objected'.



Your Recent Analysis Requests

19 TOTAL NUMBER OF FILES | 1 TOTAL NUMBER OF CLEAN FILES | 11 TOTAL NUMBER OF UNKNOWN FILES | 6 TOTAL NUMBER OF MALWARE FILES | 1 TOTAL NUMBER OF PUA | 11 TOTAL NUMBER IN HUMAN EXPERT ANALYSIS

Search :

From 2017-08-08 to 2017-09-08

My All Products

Results per page 25

	File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict	Human Expert Analysis Status
○	spminstaller.dll	Not Available	fd866f59b006b754926b35...	2017-09-06 17:03:42	No Threat Found	Not Ready	In Queue
●	59LQswxC.exe	Not Available	d2dbc21f768428a1ba94bb...	2017-09-05 20:29:40	Malware	Malware	Objected
○	spminventorycollector.dll	Not Available	b54d08412114f9edd33b14...	2017-09-05 20:25:59	No Threat Found	Not Ready	In Progress
○	filesizemonitor.dll	Not Available	aee8c91fc1d356df12b041...	2017-09-05 20:54:44	No Threat Found	Not Ready	In Queue
○	4e34c5ac0a8021815cb014d26c5bb...	Not Available	4e34c5ac0a8021815cb01...	2017-08-08 18:28:09	Malware	Malware	Analysis Completed
○	webpagemonitor.dll	Not Available	4cc6c7d64bd9b25073f786...	2017-09-05 20:29:42	Malware	Malware	Objected
○	4ca6b723e6c84ed58290b3ef6835ff2...	Not Available	4ca6b723e6c84ed58290b...	2017-08-08 20:03:30	Malware		
○	ivQ0MSD4.exe	Not Available	45c321e48a9d0bd258b7d...	2017-09-06 14:11:32	PUA	PUA	Analysis Completed
○	asd	C: \asd	2c63940875692392a4111d...	2017-08-08 20:05:58	Malware	Malware	Analysis Completed
○	itsmrsp.exe	Not Available	28b758f20b5fad7c0a19b7...	2017-09-05 20:46:55	No Threat Found		
○	1b404623188a4e66737f74a972eda8...	Not Available	1b404623188a4e66737f74...	2017-08-08 20:02:47	Clean		
○	8fntgVgx.exe	Not Available	0f6db907e866b5c12907a5...	2017-09-05 18:37:52	No Threat Found	Not Ready	In Progress
○	file_path_1708,tezu4T5v.exe	file_path_1708	012c4a2c383ee9115ac0d...	2017-09-07 16:18:21	No Threat Found	Not Ready	In Queue

Showing 1 to 18 of 18 entries

The results of the analysis will be shown in the 'Human Expert Verdict' column.

Filter, sort and search options

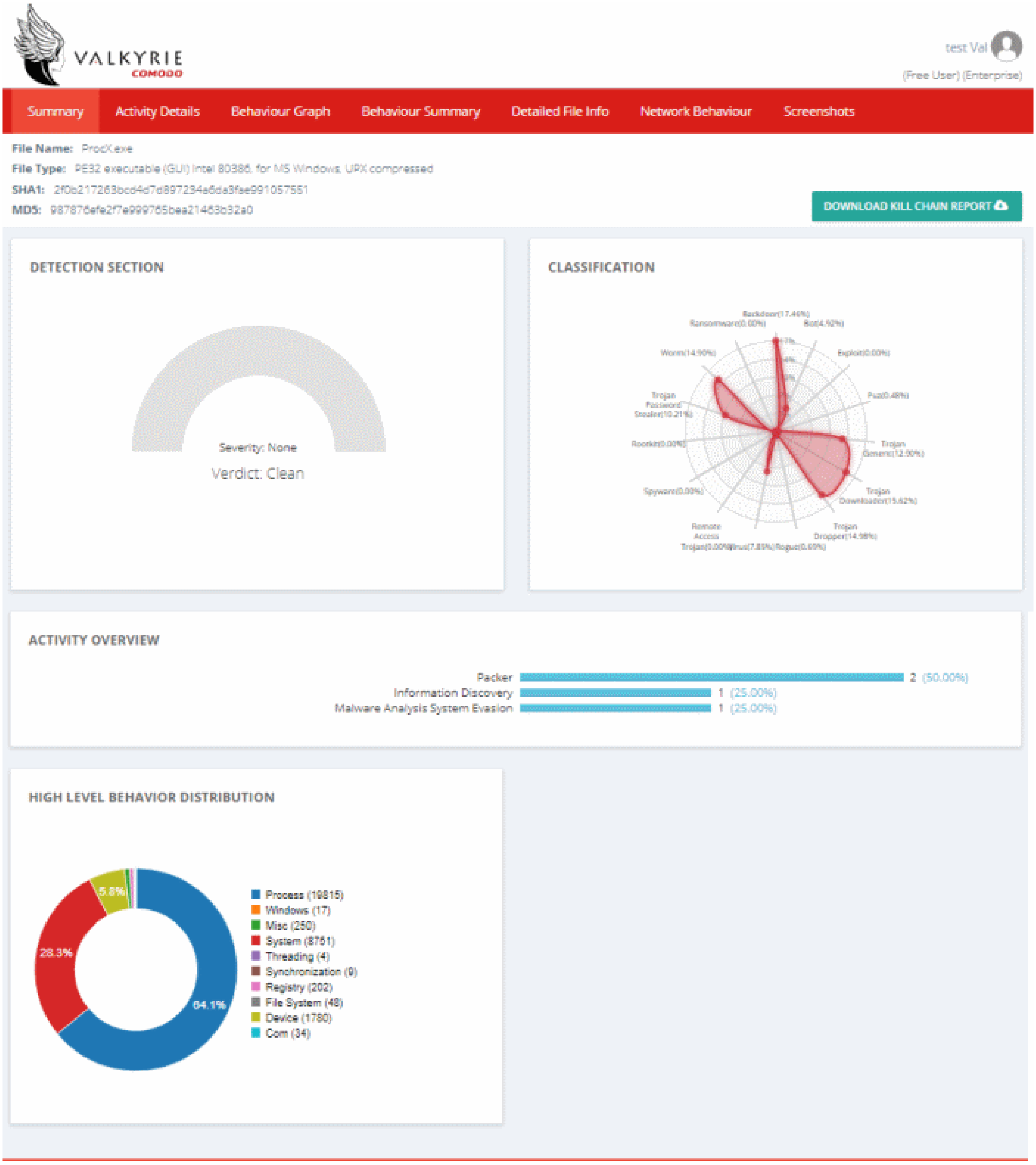
- To filter for a specific file, click the arrow next to 'Filter', select 'My All Products' or 'Other' and click 'Apply'.
- By default Valkyrie returns 25 results per page when you perform a search. Click the drop down next to Filter button to increase / decrease the number of results shown.
- Enter the details partially or fully in the search field on the top right side. You can search for items based on all columns.
- To display all the entries again, clear the search field.
- You can sort the items in ascending/descending order by clicking on the column headers.

4.3 Kill Chain Report

- Kill Chain reports are a highly detailed analysis of a specific piece of malware that was discovered on your network. Each report helps you gain a better understanding of your network's threat landscape by detailing each files malware attributes, file activity, network activity, suspicious behavior and more.
- Existing Kill Chain reports can be viewed in the web portal by all users.
- Premium license holders and Comodo One / ITarian users who have a 30-day trial can request new Kill Chain reports.

To view 'Kill Chain' report

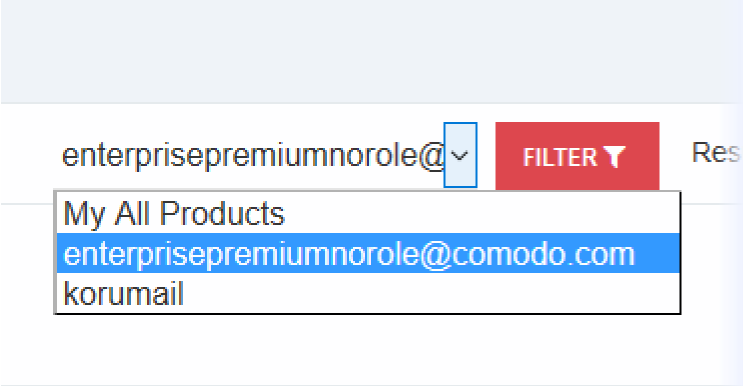
- Click the hamburger button top-left
- Click 'Recent Analysis Requests'



File Name: ProcX.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 2f0b217263bcd4d7d897234a6da3fae991057551
MD5: 987876efe2f7e999765bea21463b32a0

- Click the 'Send to Kill Chain Report' icon Send To Kill Chain Report to generate a Kill Chain report for the selected file.
- It will take up to 30 minutes to generate the report. Once the report is ready, click the 'Kill Chain Report' icon Kill Chain Report to download it.
- You can view files that belong to your Comodo One / ITarian account by choosing your login name from the

'Recent Analysis Requests'



Summary

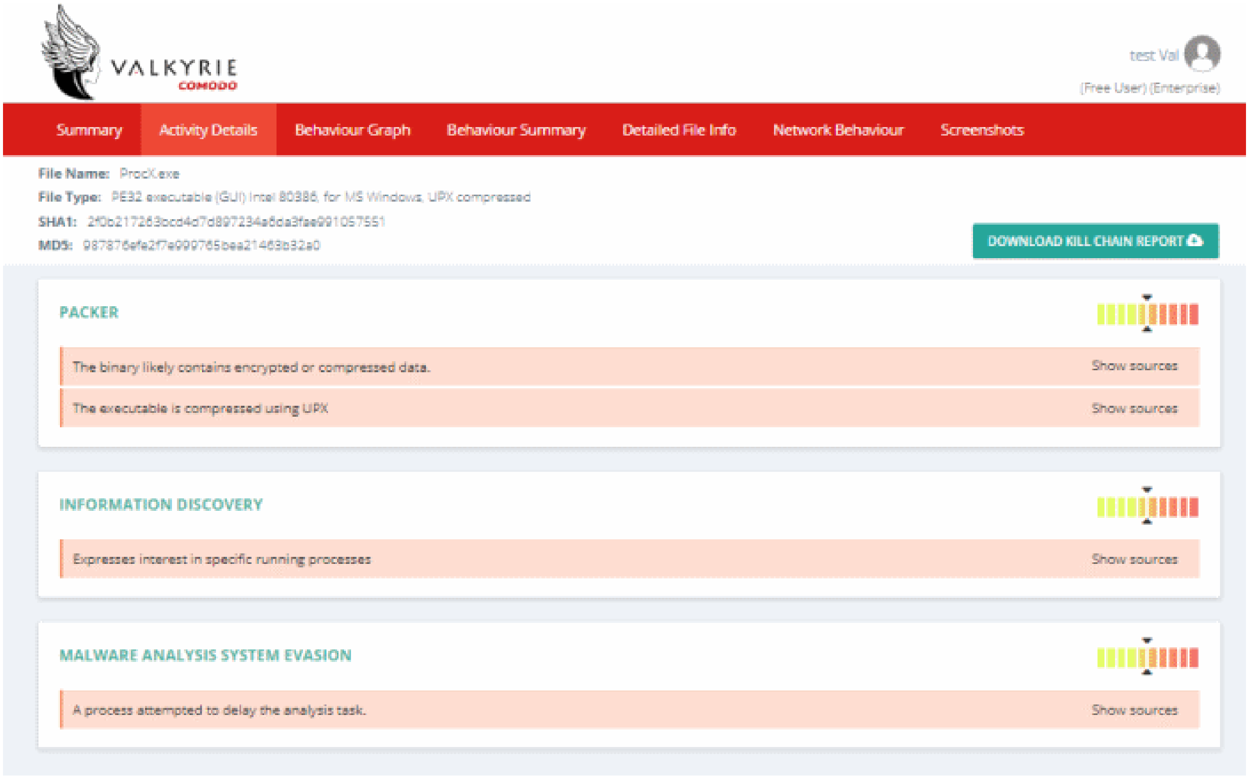
The summary area displays basic file details such as name, type and SHA1/MD5 values, along with the malware's classification and overall behavior.

- **Detection Section -** Shows the malware's overall severity level. The levels are Low, Moderate, High and Severe.
- **Classification -** An attribute matrix which shows the types of malicious behavior exhibited by the malware, and the percentage each behavior contributed to the file's total activity. This allows you to see the threat profile of the file by mapping its observed actions to those of well-known malware types.
- **Activity Overview -** Shows the broad attack categories used by the malware and the number of specific actions within each category. The 'Activity Details' section further down the report expands upon this information.
- **High Level Behavior Distribution -** Shows how the malware's behavior was spread across various operating system and network activities.

Activity Details

The activity details section displays the attack types exhibited by the malware. The information in this section is an expansion of that shown in the 'Activity Overview' bar-chart.

- Click the 'Activity Details' tab to open this section.
- Each item consists of a broad attack category followed by specific actions which fall into that category. The aggregate threat rating for all actions in a category is shown on the right.
- The category names illustrate the goal of the attack. Actions are the techniques used to achieve the goal.
- A single piece of malware may have multiple goals and may attempt multiple actions to achieve them.



File Name: ProcX.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 2f0b217263bcd4d7d897234a6da3fae991057551
MD5: 987876efe2f7e999765bea21463b32a0

PACKER

The binary likely contains encrypted or compressed data. Show sources

The executable is compressed using UPX Show sources

INFORMATION DISCOVERY

Expresses interest in specific running processes Show sources

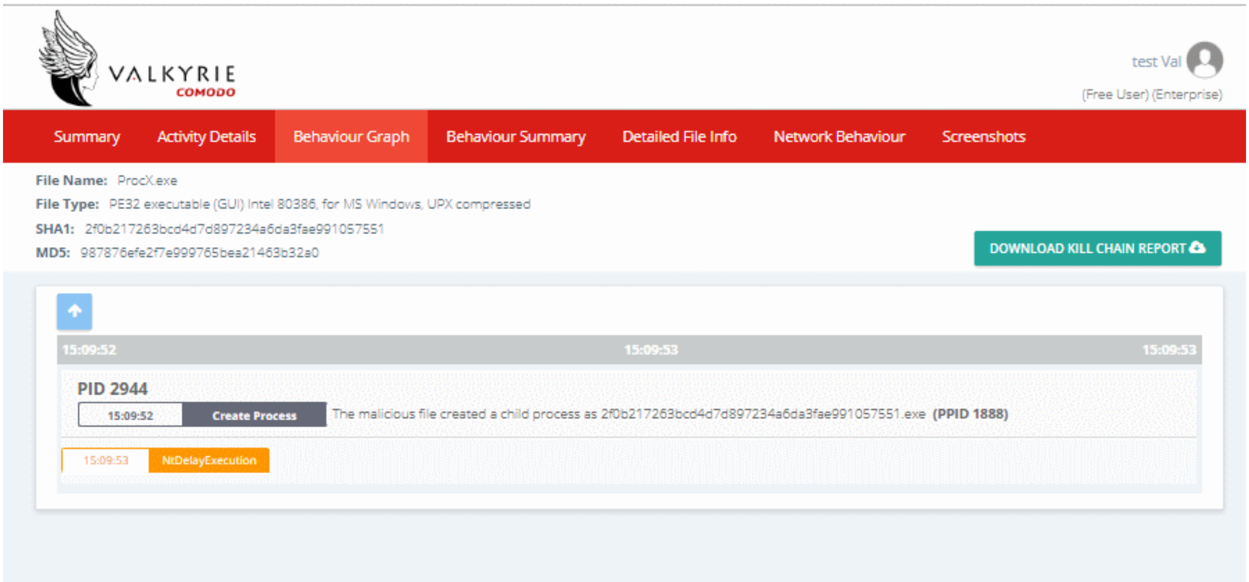
MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task. Show sources

- Click the 'Show sources' link to expand a section.

Behavior Graph

The behavior graph section displays all activities executed by the malware as a timeline. Each activity is time-stamped and color-coded according to severity level.



File Name: ProcX.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 2f0b217263bcd4d7d897234a6da3fae991057551
MD5: 987876efe2f7e999765bea21463b32a0

PID 2944

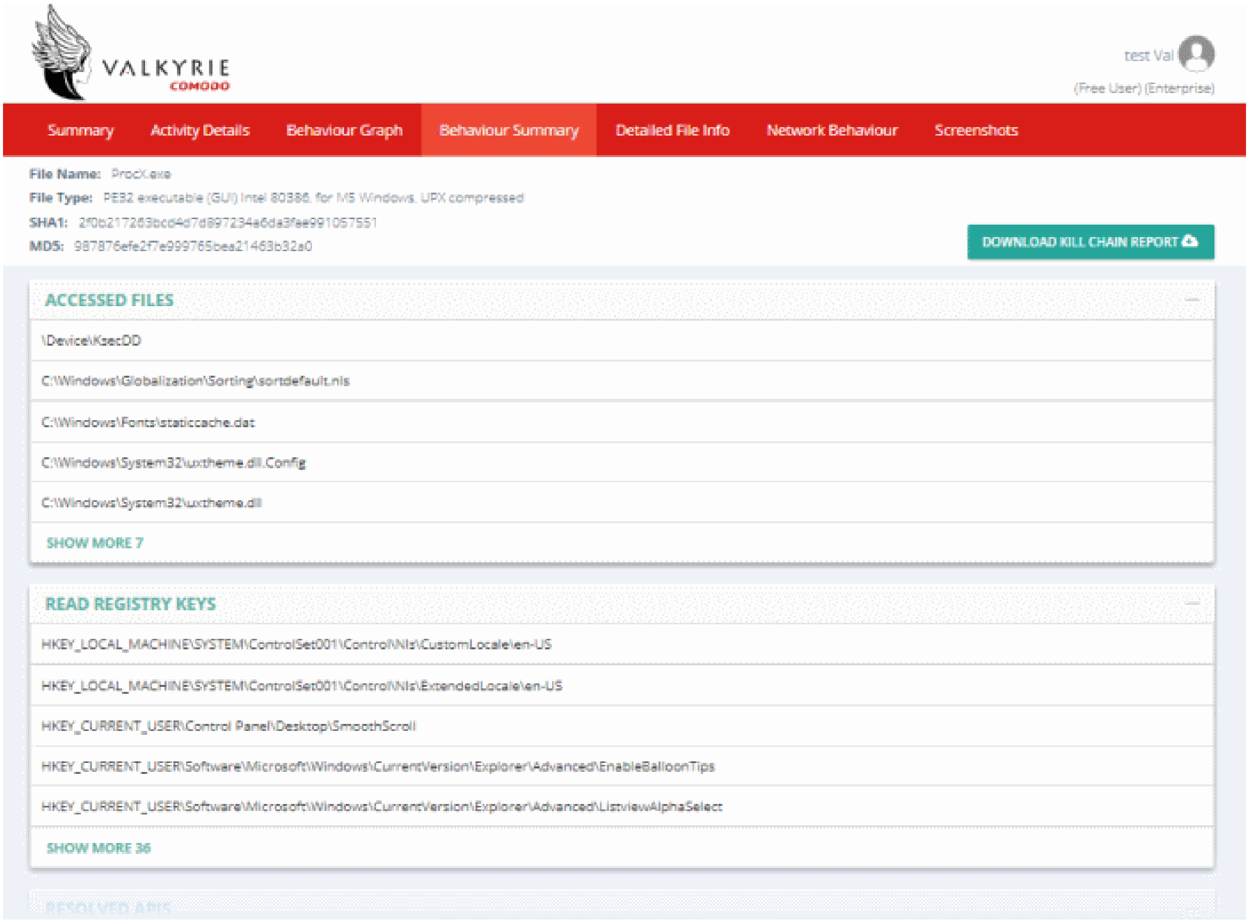
15:09:52 Create Process The malicious file created a child process as 2f0b217263bcd4d7d897234a6da3fae991057551.exe **(PPID 1888)**

15:09:53 NtDelayExecution

- Place your mouse over the graph to view detailed descriptions about a particular activity.
- Click the arrow on the top left to expand or collapse any section.

Behavior Summary

Condenses the activities of the malignant file. This includes the files and registry keys it accessed, resolved APIs and deleted files.



File Name: ProcX.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 2f0b217263bcd4d7d897234a6da3fae991057551
MD5: 987876efe2f7e999765bea21463b32a0

ACCESSED FILES

\Device\KsecDD
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_CURRENT_USER\Control Panel\Desktop\SmoothScroll
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\EnableBalloonTips
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewAlphaSelect

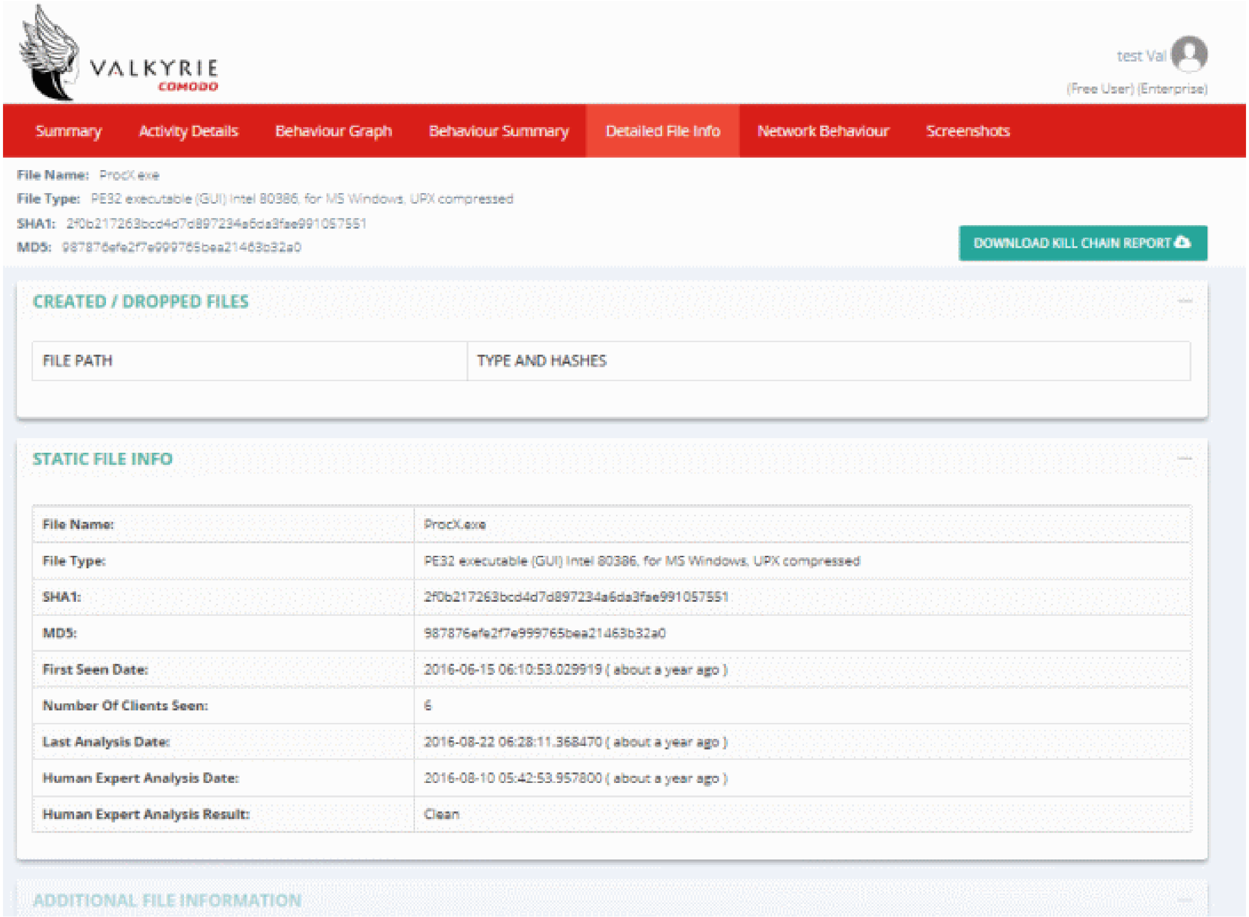
- Click '+' to expand any section

Detailed File Info

Provides detailed information about the malware and its footprint. This includes:

- The location, type and hash of all files created by the malware
- An overall summary of malware details, including name, type, hashes and trust verdict after human analysis
- Additional file information - A detailed list of PE headers, sections and imports

Click 'Detailed File Info' in the Valkyrie interface to view this section:



File Name: ProcX.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 2f0b217263bcd4d7d897234a6da3fae991057551
MD5: 987876efe2f7e999765bea21463b32a0

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

STATIC FILE INFO

File Name:	ProcX.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1:	2f0b217263bcd4d7d897234a6da3fae991057551
MD5:	987876efe2f7e999765bea21463b32a0
First Seen Date:	2016-06-15 06:10:53.029919 (about a year ago)
Number Of Clients Seen:	6
Last Analysis Date:	2016-08-22 06:28:11.368470 (about a year ago)
Human Expert Analysis Date:	2016-08-10 05:42:53.957800 (about a year ago)
Human Expert Analysis Result:	Clean

ADDITIONAL FILE INFORMATION

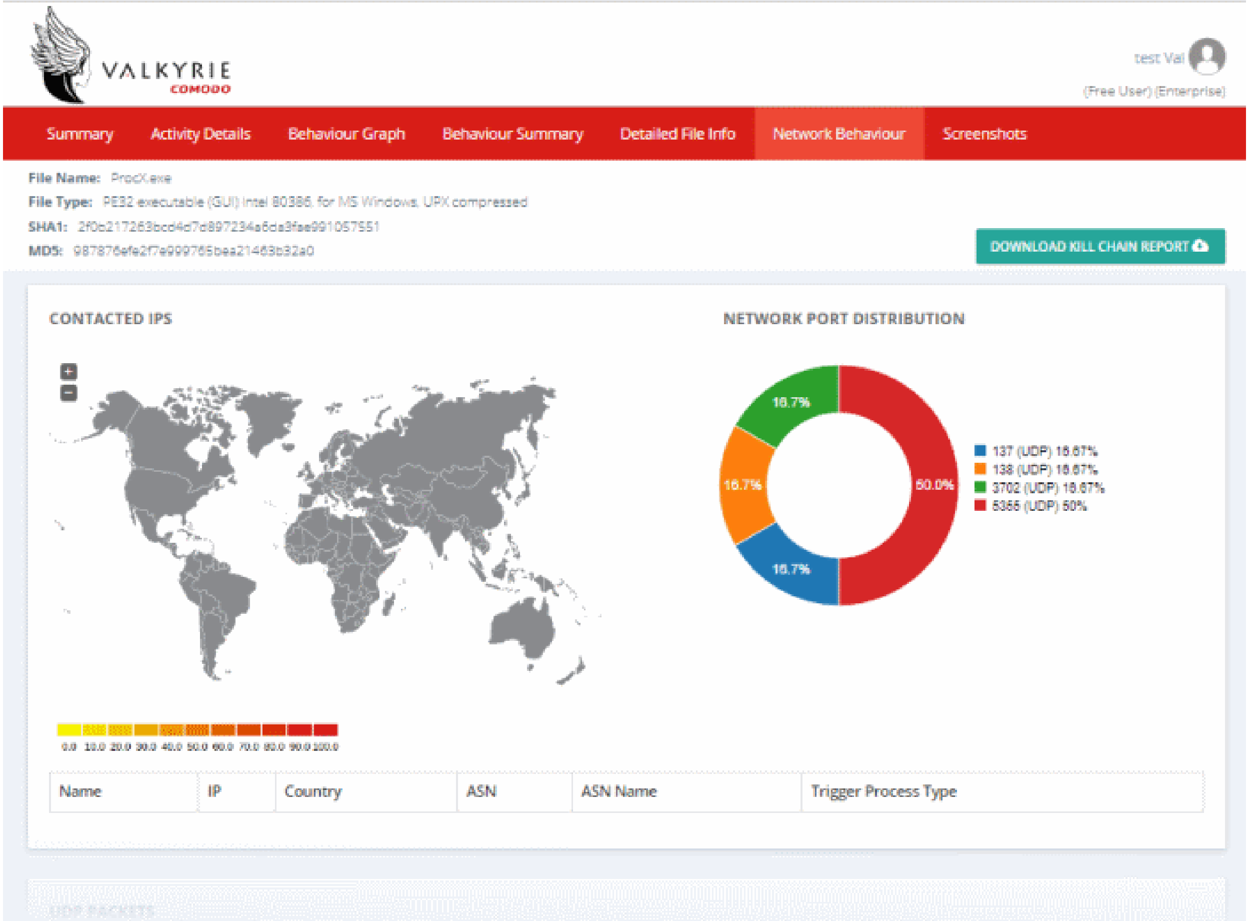
- Click '+' to expand any section

Network Behavior

Provides detailed information about the malware's activities across your network.

Note: It is possible that some queries you see in this section were made by native Windows services. The Valkyrie server tests files on a machine running only Windows and the executable being tested.

- Click the 'Network Behavior' tab to open this section:



File Name: ProcX.exe

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

SHA1: 2f0c217263bcd4d7d897234a6da3fae991057551

MD5: 987876efe2f7e999765bea21463b32a0

- 🟦 137 (UDP) 16.67%
- 🟧 138 (UDP) 16.67%
- 🟩 3702 (UDP) 16.67%
- 🟥 5355 (UDP) 50%

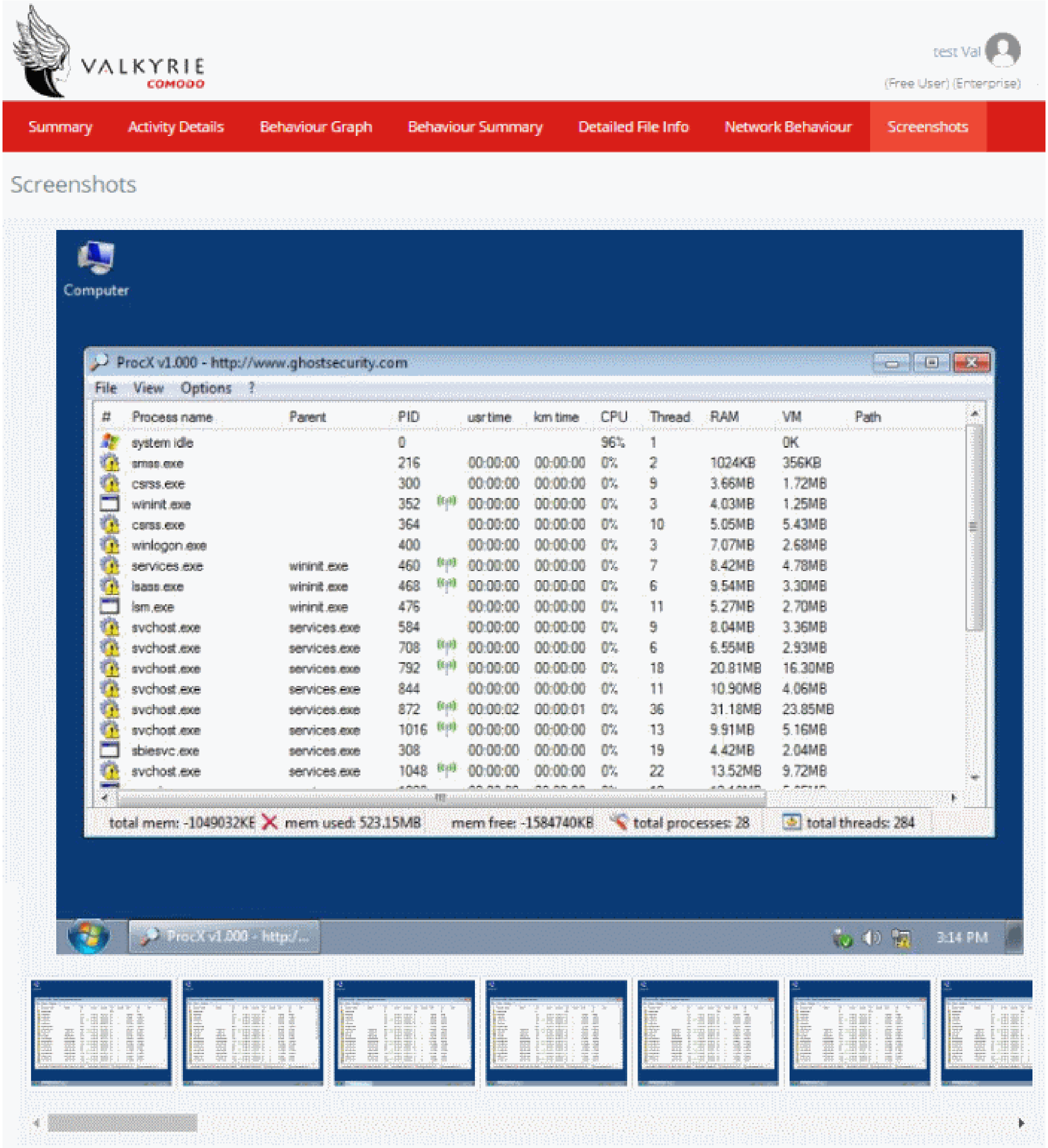
Name	IP	Country	ASN	ASN Name	Trigger Process Type

The section contains the following areas:

- **Contacted Ips -** Lists all domains and the IP addresses that were contacted during the testing process. Each row also contains the autonomous system number (ASN) and ASN name to which the IP address belongs.
- **Network Port Distribution -** Graph which shows the port numbers and protocols used for communication during the testing process. The percentages show much traffic was sent through a particular port as a percentage of the malware's total traffic.
- **HTTP Packets** - Shows all communications using HTTP packets during the testing period. A large number of connections could show the malware is involved in a denial of service attack.
- **DNS Queries/Answers** - Shows all domains for which DNS requests or answers were made during the testing period.
- **TCP Packets** - Shows all communications using TCP packets during the testing period. A large number of connections could show the malware is involved in a denial of service attack.
- **UDP Packets -** Shows all communications using UDP packets during the testing period. A large number of connections could show the malware is involved in a denial of service attack.

Screenshots

Shows screenshots of suspicious actions taken by the malware when it was running on the Valkyrie test servers.

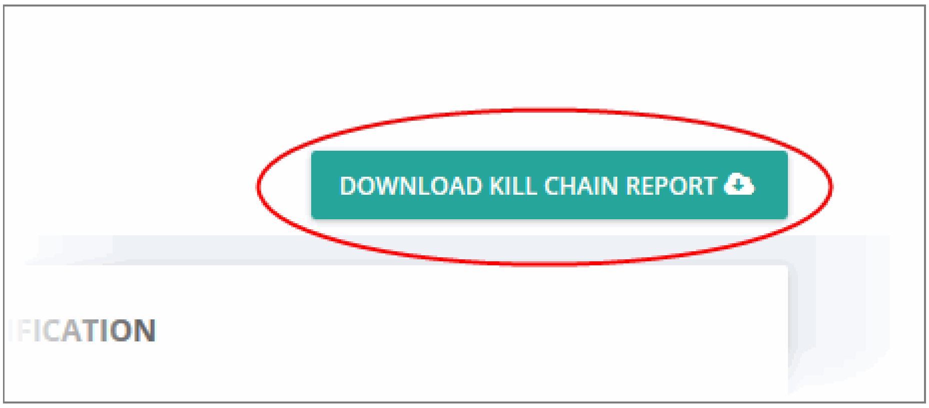


#	Process name	Parent	PID	usr time	km time	CPU	Thread	RAM	VM	Path
	system idle		0			96%	1		0K	
	smss.exe		216	00:00:00	00:00:00	0%	2	1024KB	356KB	
	csrss.exe		300	00:00:00	00:00:00	0%	9	3.66MB	1.72MB	
	wininit.exe		352	00:00:00	00:00:00	0%	3	4.03MB	1.25MB	
	csrss.exe		364	00:00:00	00:00:00	0%	10	5.05MB	5.43MB	
	winlogon.exe		400	00:00:00	00:00:00	0%	3	7.07MB	2.68MB	
	services.exe	wininit.exe	460	00:00:00	00:00:00	0%	7	8.42MB	4.78MB	
	lsass.exe	wininit.exe	468	00:00:00	00:00:00	0%	6	9.54MB	3.30MB	
	lsm.exe	wininit.exe	476	00:00:00	00:00:00	0%	11	5.27MB	2.70MB	
	svchost.exe	services.exe	584	00:00:00	00:00:00	0%	9	8.04MB	3.36MB	
	svchost.exe	services.exe	708	00:00:00	00:00:00	0%	6	6.55MB	2.93MB	
	svchost.exe	services.exe	792	00:00:00	00:00:00	0%	18	20.81MB	16.30MB	
	svchost.exe	services.exe	844	00:00:00	00:00:00	0%	11	10.90MB	4.06MB	
	svchost.exe	services.exe	872	00:00:02	00:00:01	0%	36	31.18MB	23.85MB	
	svchost.exe	services.exe	1016	00:00:00	00:00:00	0%	13	9.91MB	5.16MB	
	sbiesvc.exe	services.exe	308	00:00:00	00:00:00	0%	19	4.42MB	2.04MB	
	svchost.exe	services.exe	1048	00:00:00	00:00:00	0%	22	13.52MB	9.72MB	

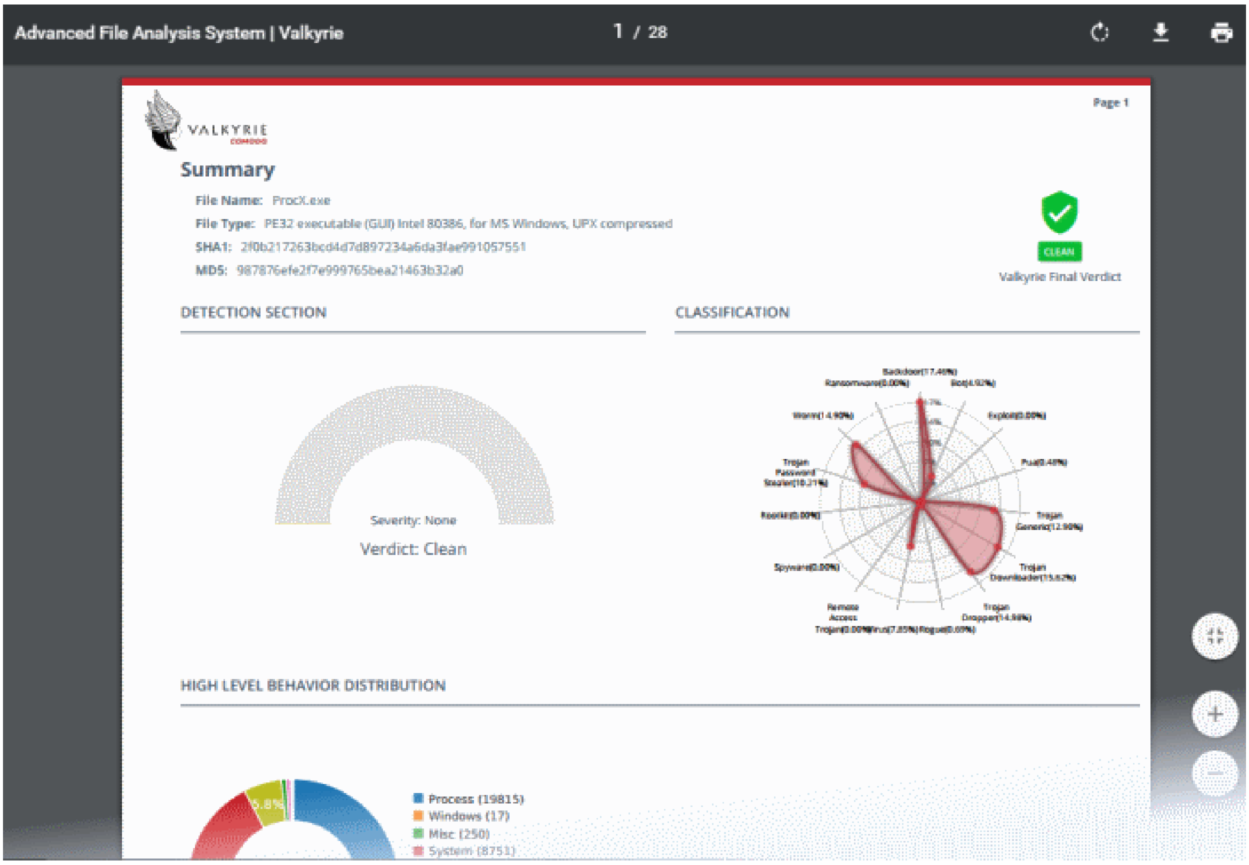
total mem: -1049032KE ✗ mem used: 523.15MB mem free: -1584740KB total processes: 28 total threads: 284

Download the Kill Chain report

Click 'Download Kill Chain Report' to get a pdf version of the report:



It will open the PDF file in a new window.



Summary

File Name: ProcX.exe

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

SHA1: 2f0b217263bcd4d7d897234a6da3fae991057551

MD5: 987876efe2f7e999765bea21463b32a0

Valkyrie Final Verdict

DETECTION SECTION

Verdict: Clean

CLASSIFICATION

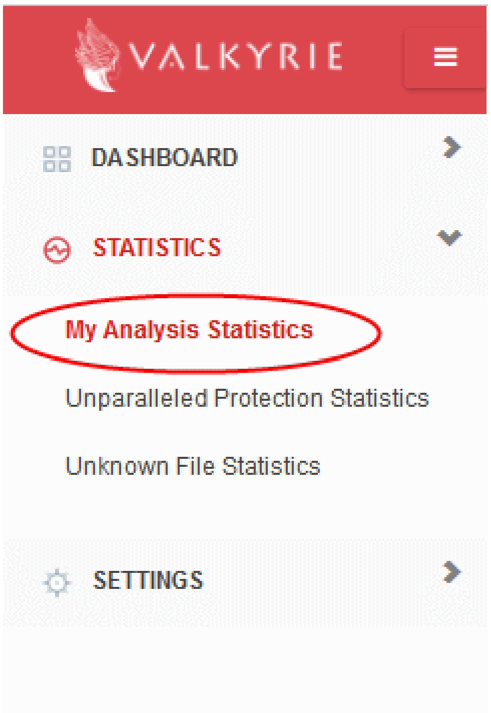
HIGH LEVEL BEHAVIOR DISTRIBUTION

4.4 My Analysis Statistics

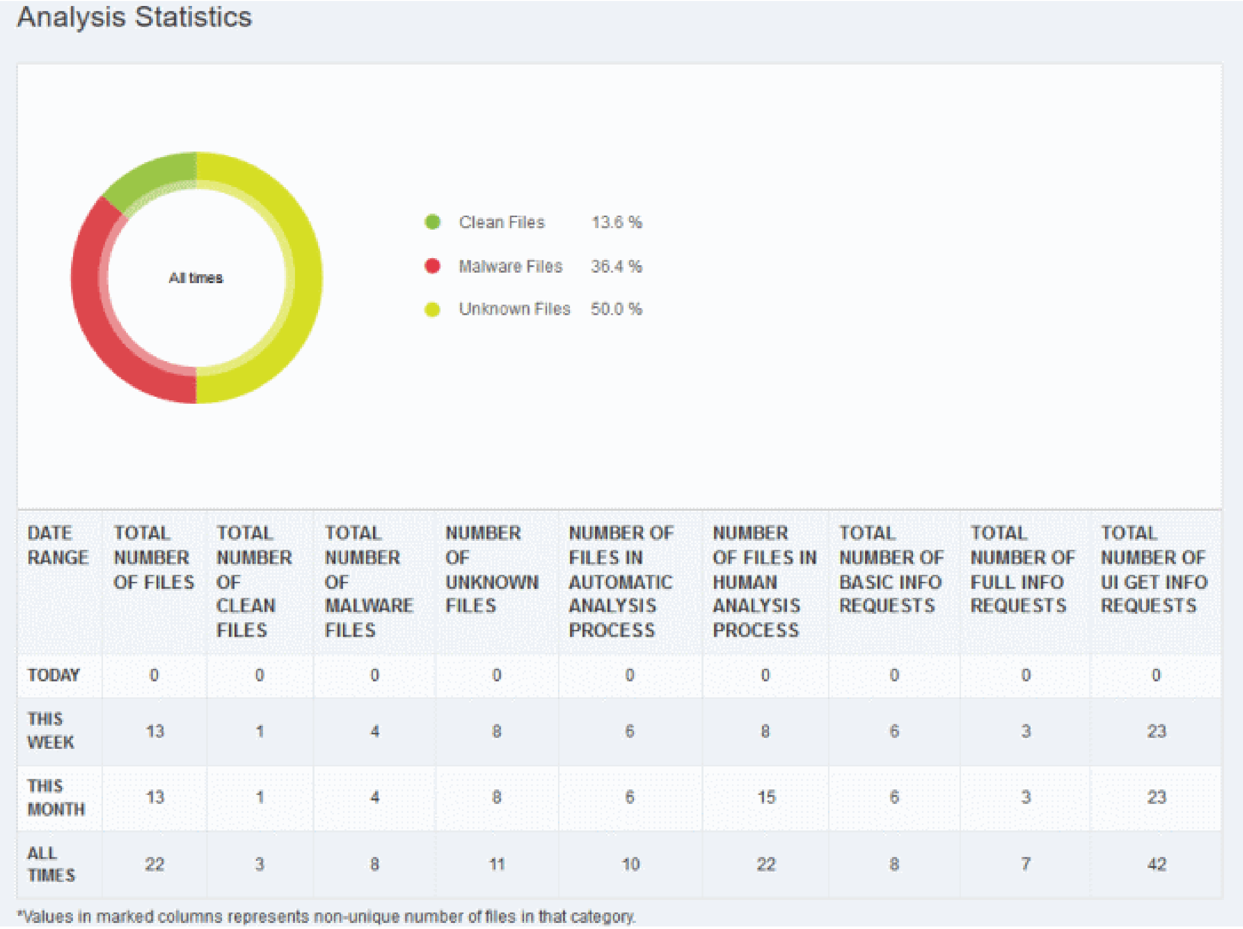
The 'My Analysis Statistics' page displays how many files have been submitted for your account.

To view your Valkyrie account statistics:

- Click the hamburger menu button top-left
- Click 'Dashboard' > 'My Analysis Statistics' link on the user menu



The 'Analysis Statistics' page will open:


Analysis Statistics

DATE RANGE	TOTAL NUMBER OF FILES	TOTAL NUMBER OF CLEAN FILES	TOTAL NUMBER OF MALWARE FILES	NUMBER OF UNKNOWN FILES	NUMBER OF FILES IN AUTOMATIC ANALYSIS PROCESS	NUMBER OF FILES IN HUMAN ANALYSIS PROCESS	TOTAL NUMBER OF BASIC INFO REQUESTS	TOTAL NUMBER OF FULL INFO REQUESTS	TOTAL NUMBER OF UI GET INFO REQUESTS
TODAY	0	0	0	0	0	0	0	0	0
THIS WEEK	13	1	4	8	6	8	6	3	23
THIS MONTH	13	1	4	8	6	15	6	3	23
ALL TIMES	22	3	8	11	10	22	8	7	42

*Values in marked columns represents non-unique number of files in that category.

It shows the following details:

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

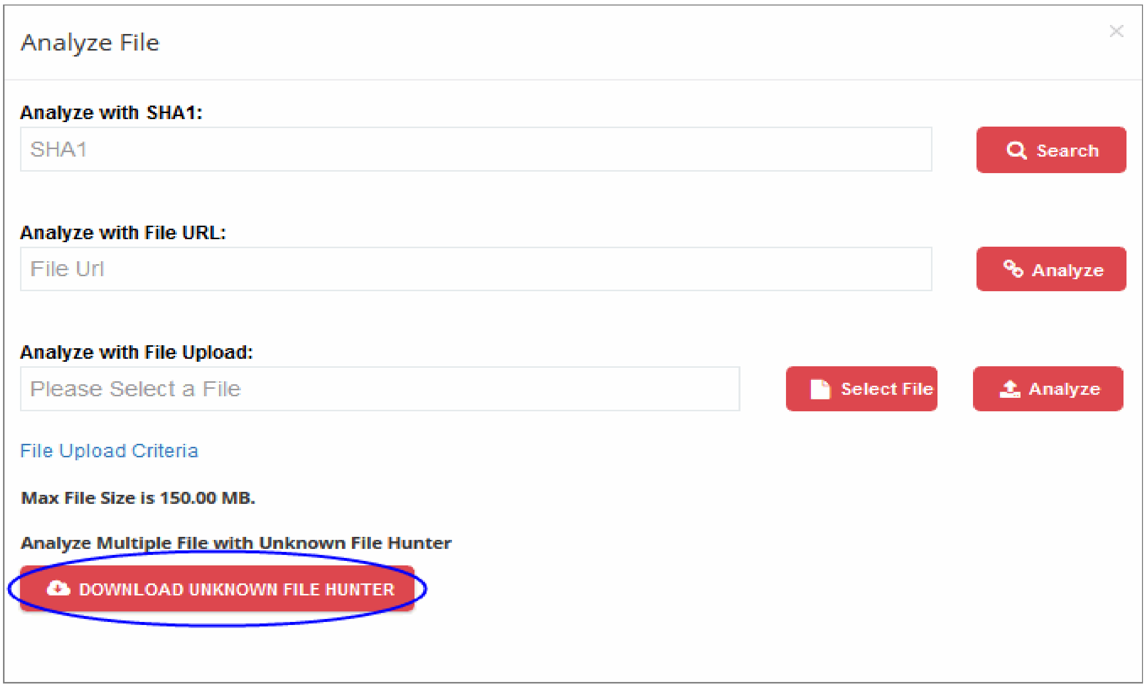
Analysis Statistics - Table of Column Descriptions	
Column Header	**Description**
Date Range	Indicates the period of usage.
Total Number of Files	Total number of files submitted for the period.
Total Number of Clean Files	Total number of files found to be clean.
Total Number of Malware Files	Total number of files found to be malware files submitted.
Number of Unknown Files	Indicates the number of files that cannot be classified as definitely safe or definitely malware after analysis.
Number of Files in Automatic Analysis Process	Number of files submitted for automatic analysis
Number of Files in Human Expert Analysis Process	Number of files submitted for human expert analysis.
Total Number of Basic Info Requests	The number of times the user has used the Valkyrie REST API (fvs_basic_info) to request basic analysis results from the Valkyrie database. Basic information includes whether the file has been previously uploaded, the verdict of the last analysis, the last and first analysis dates, and whether or not the file is white-listed.
Total Number of Full Info Requests.	This is similar to a basic info request (above) but shows greater detail. It shows the number of times the user has used the REST API (fvs_full_info) to request results from Valkyrie. The greater detail includes static, dynamic and human expert results, including behavioral and file information.
Total Number of UI Get Info Requests.	The number of times the user has requested analysis results via the dashboard. This can be done by clicking the 'View File Info' ⓘ View File Info button or by searching the SHA1 hash of a file.

- The values in parentheses represent the unique number of files for which information was requested. For example, '15 (5)' means you made 15 total requests spread across 5 different files.

4.5 Unknown File Hunter Scans

- Unknown File Hunter (UFH) is a free tool which lets you quickly and accurately identify all unknown files on your network.
- The 'Unknown File Hunter Scans' area lets you view the results of scans run with this tool.
- You can download and run UFH from the Valkyrie dashboard:
  - Click the 'Download Unknown File Hunter' button on the dashboard

    OR
  - Click 'Analyze New File' > 'Download Unknown File Hunter'



Analyze File

Analyze with SHA1:

SHA1

Analyze with File URL:

File Url

Analyze with File Upload:

Please Select a File

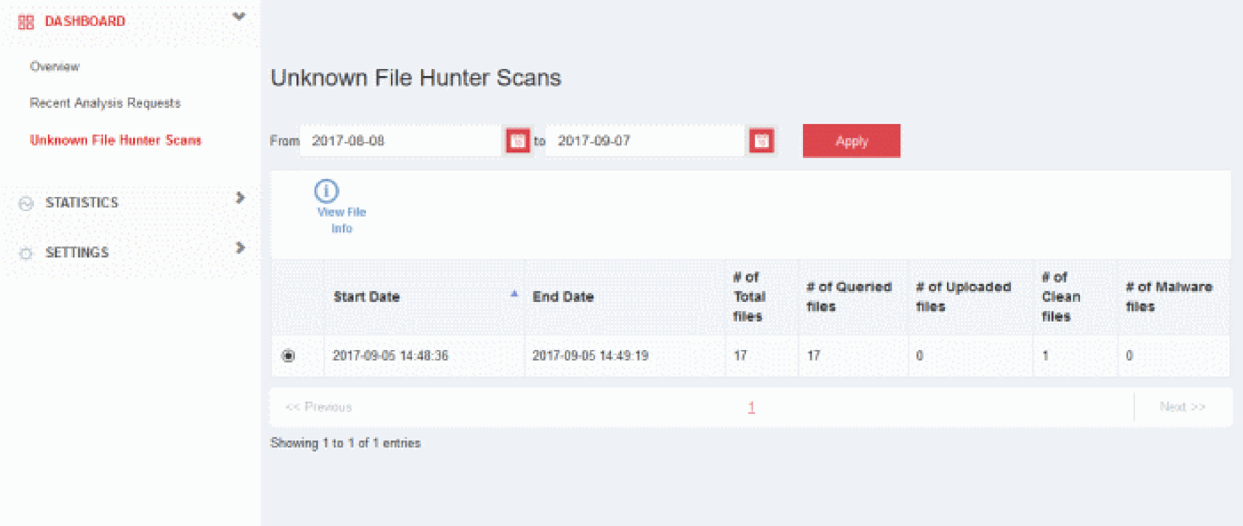
File Upload Criteria

Max File Size is 150.00 MB.

Analyze Multiple File with Unknown File Hunter

After running a UFH scan on your network, you can view results in the 'Unknown File Hunter Scans' area:

- Click 'Dashboard' > 'Overview' > 'Unknown File Hunter Scans'



Unknown File Hunter Scans

From 2017-08-08 to 2017-09-07

	Start Date	End Date	# of Total files	# of Queried files	# of Uploaded files	# of Clean files	# of Malware files
●	2017-09-05 14:48:36	2017-09-05 14:49:19	17	17	0	1	0

Showing 1 to 1 of 1 entries

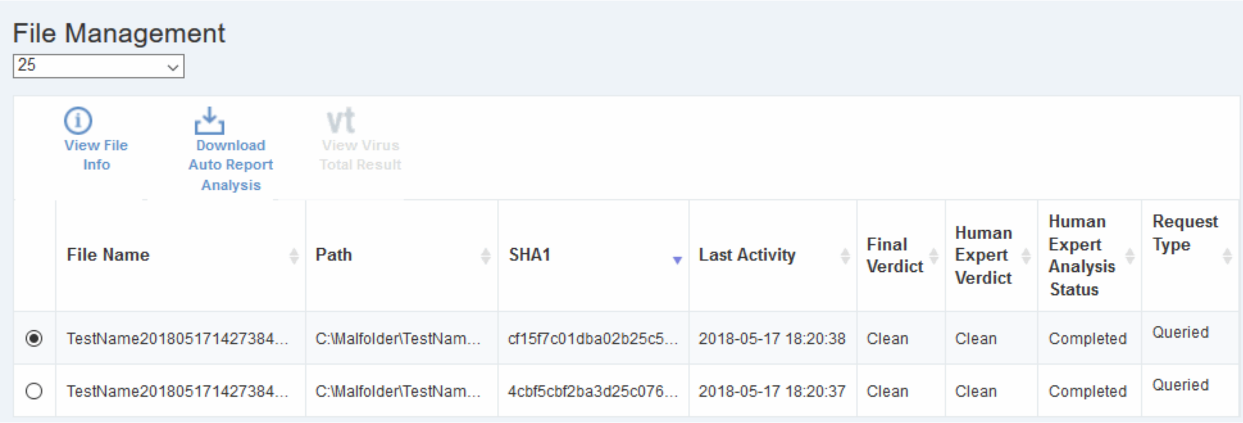
Click a scan row to view all files included in the scan.

View the details of a file:

- Click the 'View File Info' icon View File Info above the results table. A new web page opens with detailed results for the file.

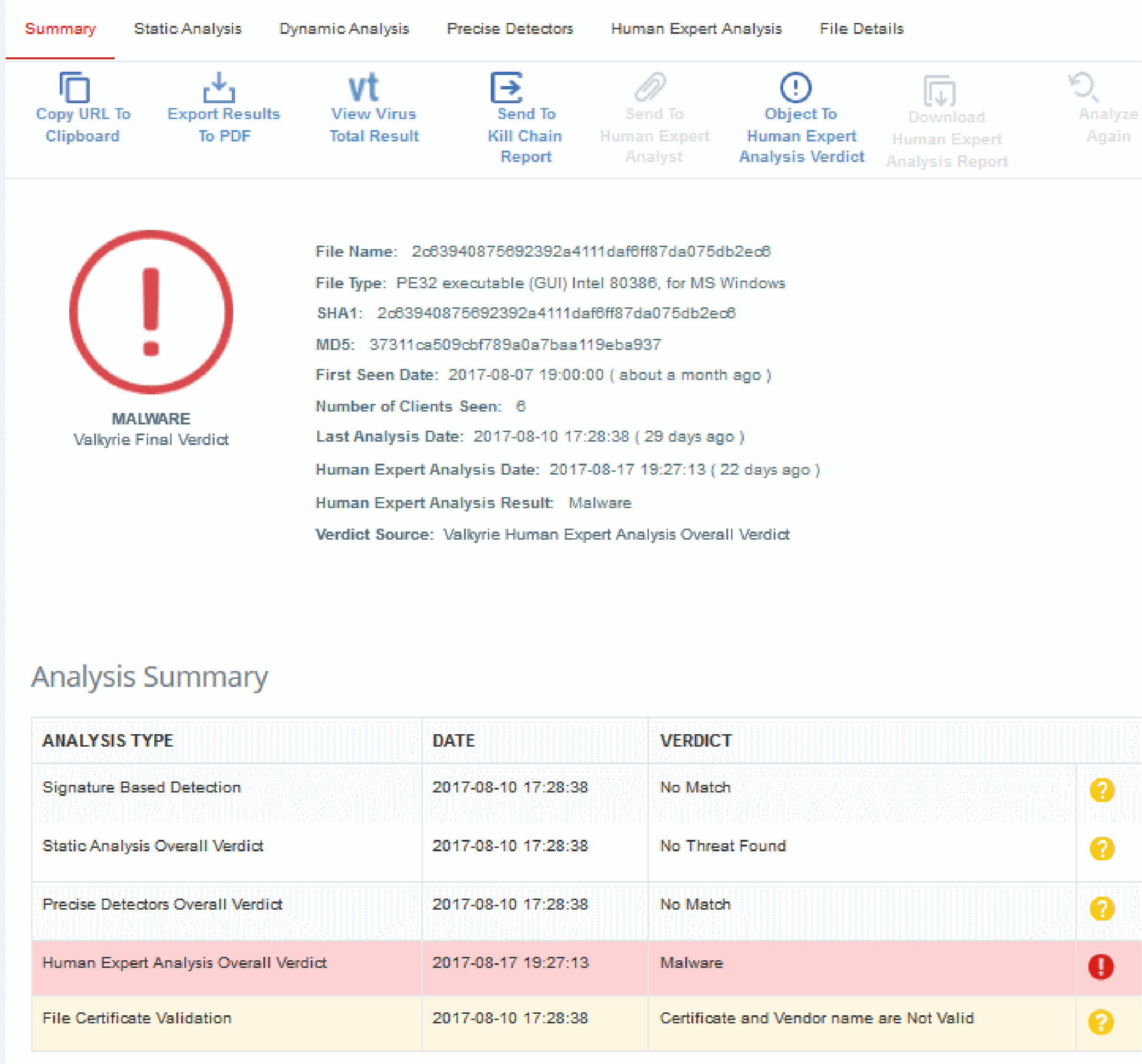
Unknown File Hunter Scans - Table of Column Descriptions	
Column Header	**Description**
Start Date	Scan start date and time
End Date	Scan end date and time

# of Total files	Number of files uploaded / verified by Valkyrie web interface within UFH tool
# of Queried files	Number of files verified by Valkyrie within UFH Number of files uploaded manually to Valkyrie within Unknown File Hunter Scan session
# of Uploaded files	Number of files uploaded manually to Valkyrie within Unknown File Hunter Scan session
# of Clean files	Number of files declared virus-free by UFH scans.
# of Malware files	Number of infected files identified by UFH scans



	File Name	Path	SHA1	Last Activity	Final Verdict	Human Expert Verdict	Human Expert Analysis Status	Request Type
●	TestName201805171427384...	C:\Malfolder\TestNam...	cf15f7c01dba02b25c5...	2018-05-17 18:20:38	Clean	Clean	Completed	Queried
○	TestName201805171427384...	C:\Malfolder\TestNam...	4cbf5cbf2ba3d25c076...	2018-05-17 18:20:37	Clean	Clean	Completed	Queried

- Click on any executable file in the 'File Management' page to view Valkyrie analysis results.
- Click the 'View File Info' icon ⓘ View File Info above the table of executable files. A new web page opens with detailed information about the file.



File Name: 2c63940875692392a4111daf6ff87da075db2ec6
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 2c63940875692392a4111daf6ff87da075db2ec6
MD5: 37311ca509cbf789a0a7baa119eba937
First Seen Date: 2017-08-07 19:00:00 (about a month ago)
Number of Clients Seen: 6
Last Analysis Date: 2017-08-10 17:28:38 (29 days ago)
Human Expert Analysis Date: 2017-08-17 19:27:13 (22 days ago)
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2017-08-10 17:28:38	No Match	?
Static Analysis Overall Verdict	2017-08-10 17:28:38	No Threat Found	?
Precise Detectors Overall Verdict	2017-08-10 17:28:38	No Match	?
Human Expert Analysis Overall Verdict	2017-08-17 19:27:13	Malware	!
File Certificate Validation	2017-08-10 17:28:38	Certificate and Vendor name are Not Valid	?

The 'Valkyrie analysis summary' screen will be displayed. See **Valkyrie Summary report** to find out more.

- Click 'Download Auto Report Analysis' icon Download Auto Report Analysis to view the Valkyrie analysis summary. See **Download Human Expert Analysis Report** for more details.

- Click the 'View Virus Total Result' icon vt View Virus Total Result above the table of executable files to see Virus Total meta-results on a particular file. See **Virus Total Results** for more details.

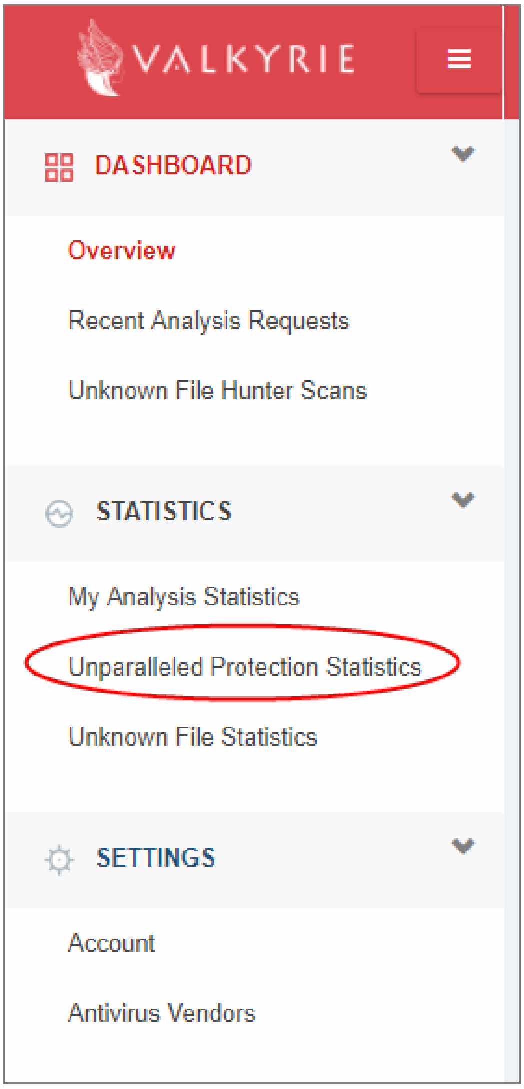
4.6 Unparalleled Protection Statistics

The 'Unparalleled Protection' page displays unknown files found on your computer or network that were subsequently identified as malware by Comodo Valkyrie - before any other antivirus company detected them as such.

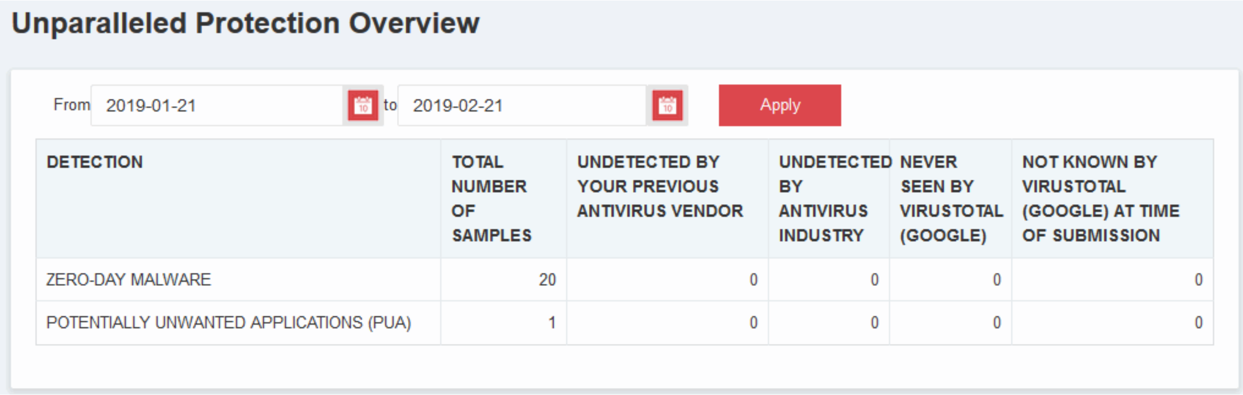
This is 'unparalleled' protection because traditional antivirus solutions would have allowed this malware to run. Fortunately, Comodo's Containment and Valkyrie technologies are on hand to protect you throughout. Containment keeps the files locked away in a secure sandbox environment where they could do no harm while Valkyrie analysis identifies the file as malware before anybody else.

View 'Unparalleled Protection statistics' details

- Click the hamburger menu button on the top-left
- Click 'Statistics' > 'Unparalleled Protection Statistics' link on the user menu



The 'Unparalleled Protection Overview' page opens:



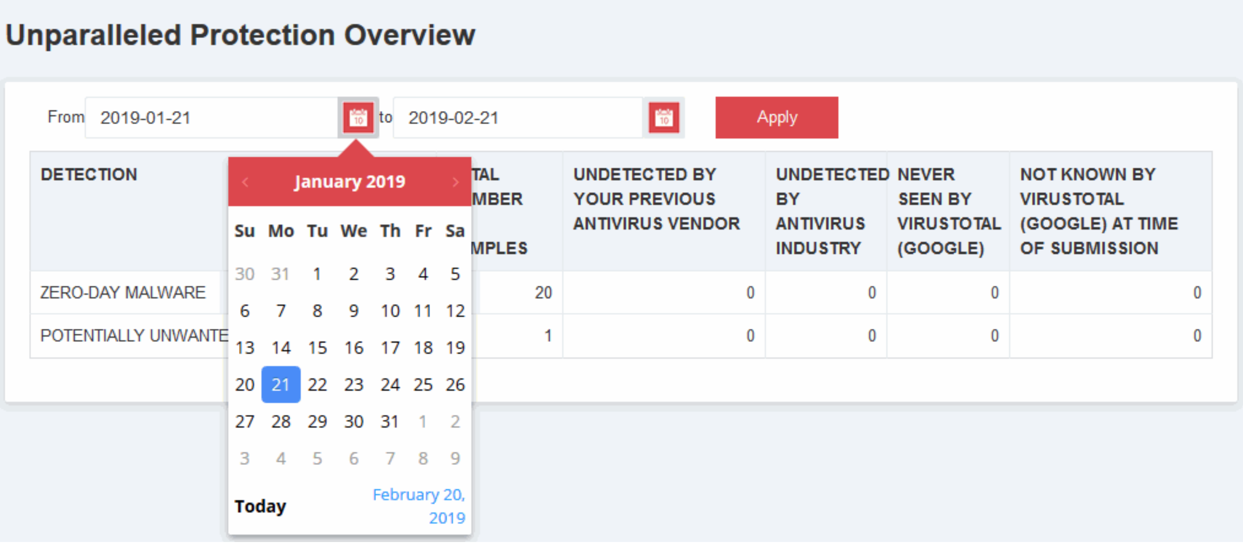
Unparalleled Protection Overview

From 2019-01-21 to 2019-02-21 Apply

DETECTION	TOTAL NUMBER OF SAMPLES	UNDETECTED BY YOUR PREVIOUS ANTIVIRUS VENDOR	UNDETECTED BY ANTIVIRUS INDUSTRY	NEVER SEEN BY VIRUSTOTAL (GOOGLE)	NOT KNOWN BY VIRUSTOTAL (GOOGLE) AT TIME OF SUBMISSION
ZERO-DAY MALWARE	20	0	0	0	0
POTENTIALLY UNWANTED APPLICATIONS (PUA)	1	0	0	0	0

By default, the filter will be for today's date. You can change the report dates using the date fields beside the 'Apply' button.

- Click the date field, select / enter the date from the calendar and click the 'Apply' button.



Unparalleled Protection Overview
From 2019-01-21 to 2019-02-21 Apply
DETECTION
TAL
MBER
MPLES
UNDETECTED BY YOUR PREVIOUS ANTIVIRUS VENDOR
UNDETECTED BY ANTIVIRUS INDUSTRY
NEVER SEEN BY VIRUSTOTAL (GOOGLE)
NOT KNOWN BY VIRUSTOTAL (GOOGLE) AT TIME OF SUBMISSION
ZERO-DAY MALWARE 20 0 0 0 0
POTENTIALLY UNWANTE 1 0 0 0 0
January 2019
Su Mo Tu We Th Fr Sa
30 31 1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31 1 2
3 4 5 6 7 8 9
Today
February 20, 2019

The first table provides the details for the selected period. The second table provides the details from the date of account creation up to a day before the selected 'From' date.

Unparalleled Protection Statistics - Table of Column Descriptions	
Column Header	**Description**
Detection	The type of threat detected by Valkyrie.
Total Number of Samples	Total number of files detected as malware by Valkyrie.
Undetected by Your Previous Antivirus Vendor	Number of threats that were not detected by your previous AV vendors. You can select your AV vendors from the settings screen. Refer to the section 'Configuring Valkyrie Account Settings' for more details.
Undetected by Antivirus Industry	Number of threats that were not detected by the entire AV industry. This potentially means you were the first person to encounter this threat in the world.
Never Seen by VirusTotal (Google)	Number of discovered threats that were not found by VirusTotal.
Not known by	Number of discovered threats that were not found by VirusTotal at the time they were

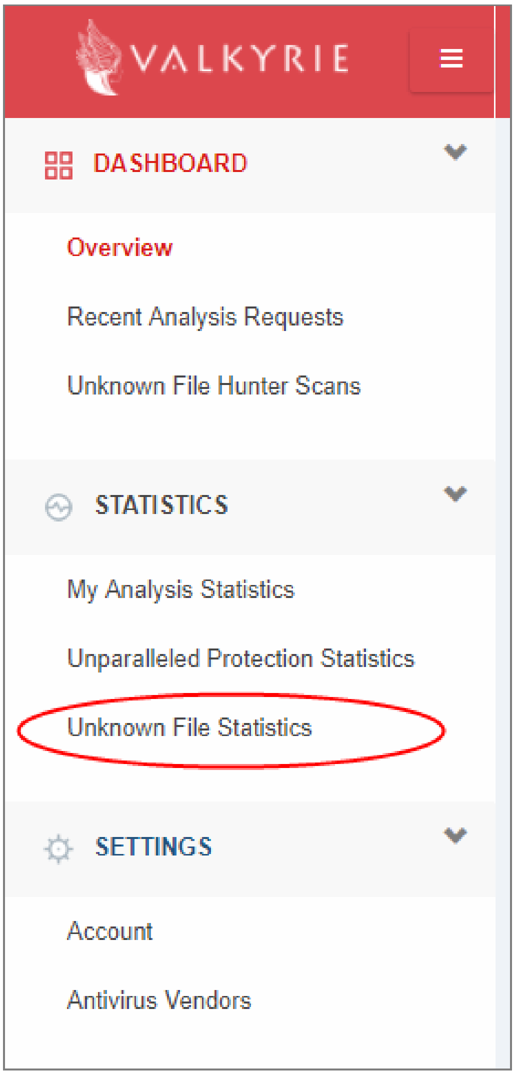
Virustotal (Google) at Time of Submission	submitted to Valkyrie.

4.7 Unknown File Statistics

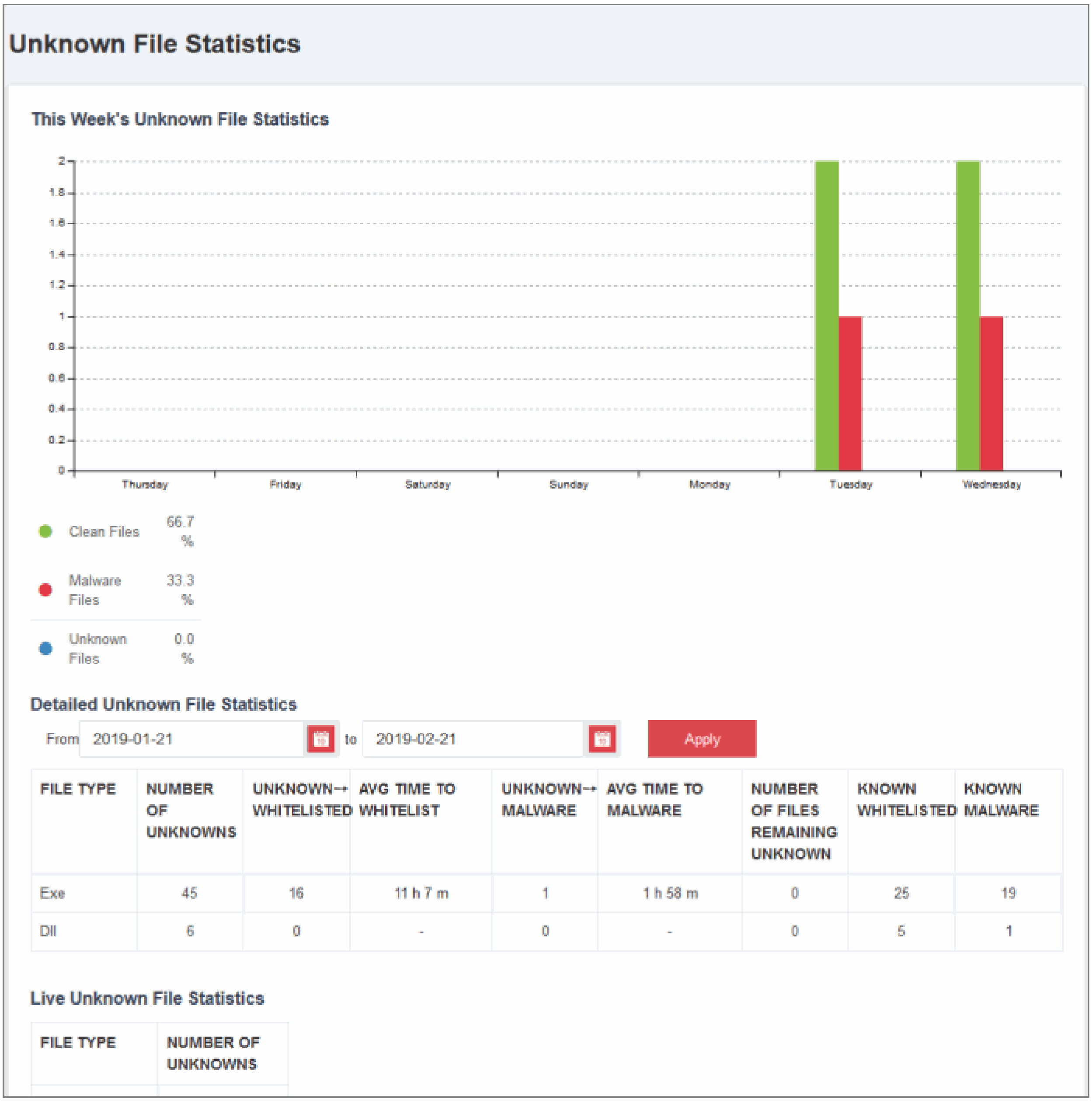
- Files that Valkyrie's initial analysis cannot classify as definitely safe nor definitely malware are given a status of 'Unknown'.
- Unknown files undergo further analysis to determine whether they are safe or malicious.
- The 'Unknown File Statistics' page shows details of file verdict changes and the average period taken to declare unknown files as either clean or malicious.
- 'This Week's Unknown File Statistics' is a graphical summary of your unknown files. It shows unknown files that were eventually deemed safe and whitelisted, unknown files that were found to be malware, and the number of unknown files that are still under analysis.

View your unknown file stats

- Click the hamburger menu button at top-left
- Click 'Dashboard' > 'Unknown File Statistics'



The 'Unknown File Statistics' page opens:



Unknown File Statistics

This Week's Unknown File Statistics

●	Clean Files	66.7 %
●	Malware Files	33.3 %
●	Unknown Files	0.0 %

Detailed Unknown File Statistics

From 2019-01-21 to 2019-02-21 Apply

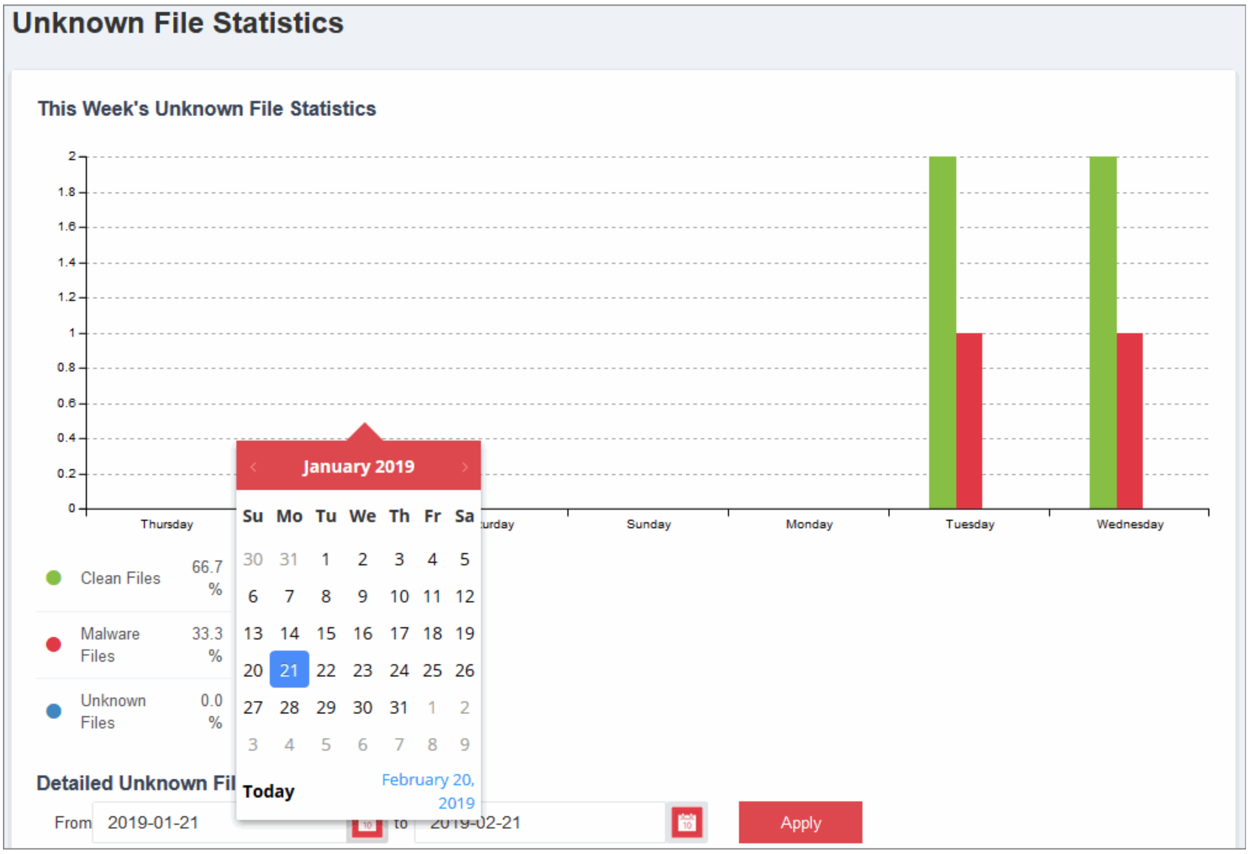
FILE TYPE	NUMBER OF UNKNOWNS	UNKNOWN→ WHITELISTED	AVG TIME TO WHITELIST	UNKNOWN→ MALWARE	AVG TIME TO MALWARE	NUMBER OF FILES REMAINING UNKNOWN	KNOWN WHITELISTED	KNOWN MALWARE
Exe	45	16	11 h 7 m	1	1 h 58 m	0	25	19
Dll	6	0	-	0	-	0	5	1

Live Unknown File Statistics

FILE TYPE	NUMBER OF UNKNOWNS

The default view is today's statistics. You can change the report dates using the date fields beside the 'Apply' button.

- Click the date field, select / enter the date from the calendar and click the 'Apply' button.



Unknown File Statistics

This Week's Unknown File Statistics

●	Clean Files	66.7 %
●	Malware Files	33.3 %
●	Unknown Files	0.0 %

‹ January 2019 ›

Su	Mo	Tu	We	Th	Fr	Sa
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

Today February 20, 2019

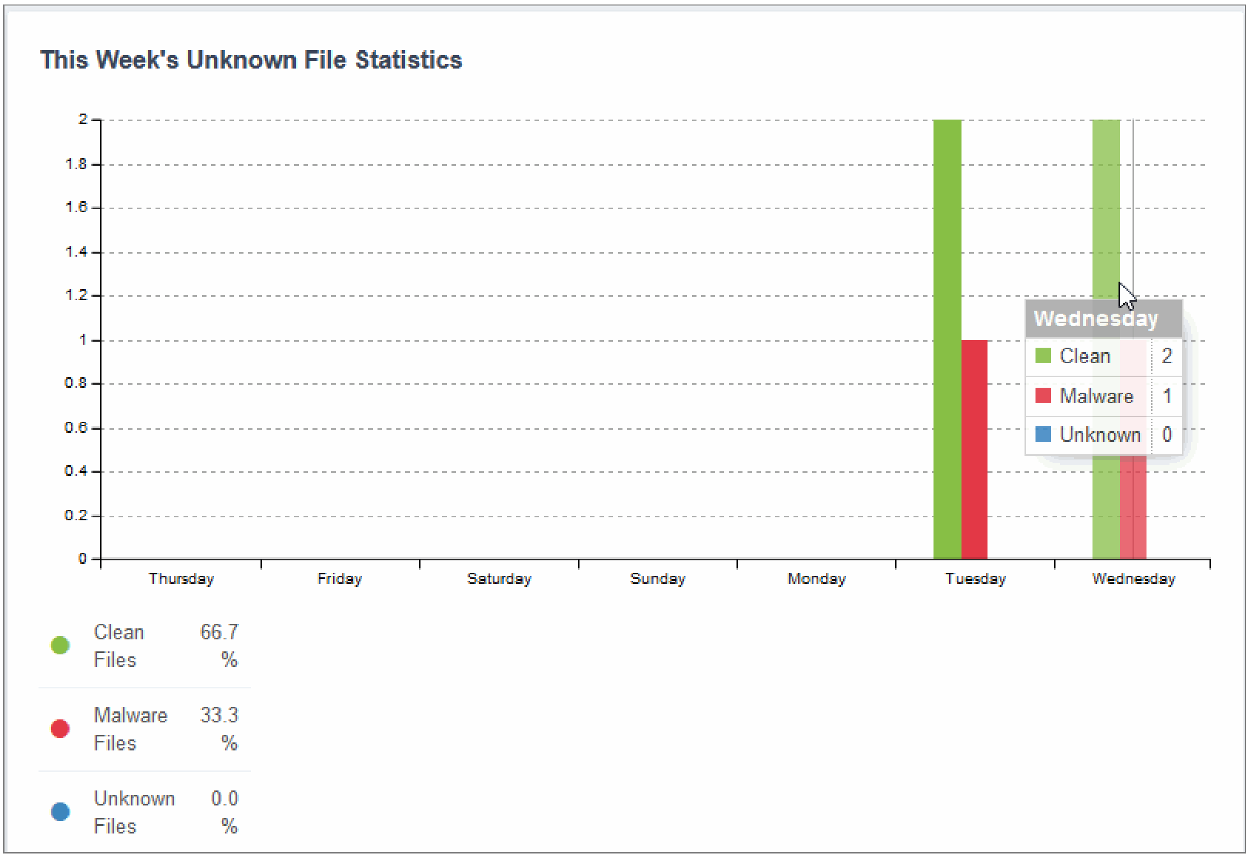
Detailed Unknown Fil

From 2019-01-21 to 2019-02-21

The graph will show details for the selected period. The X-axis represents the data for the last 7 days and the Y-axis represents the number of files.

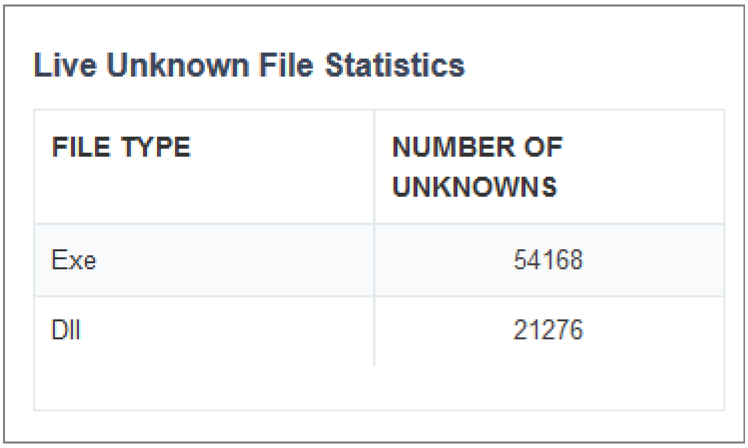
- Unknown - Files that were determined as unknown at first analysis
- Unknown > Whitelist - Unknown files that were white-listed after further analysis
- Unknown > Malware - Unknown files that were determined to be malware after further analysis
- Total Remaining Unknown - Cumulative value of the unknown files for the last 7 days

Place your mouse cursor over a point in the graph to view details for the respective day.



Unknown File Statistics - Table of Column Descriptions	
Column Header	**Description**
File Type	The type of file submitted for analysis and remains as unknown.
# of Unknowns	Number of unknown files for the selected period.
Unknown →Whitelisted	Number of unknown files that are whitelisted after further analysis.
Avg. time to Whitelist	The average time taken to analyze and give whitelist status for the unknown files.
Unknown →Malware	Number of unknown files that are determined as malware after further analysis.
Avg. time to Malware	The average time taken to analyze and determine as malware for the unknown files.
# of Files Remaining Unknown	Number of unknown files remaining to be analyzed further for the selected period.
Known Whitelisted	The total number files submitted during the selected period and found to be whitelisted in the Valkyrie database.
Known Malware	The total number of files submitted during the selected period and determined as malware by Valkyrie.

The table at the end of the page provides the details of files that are unknown and under analysis as of now.



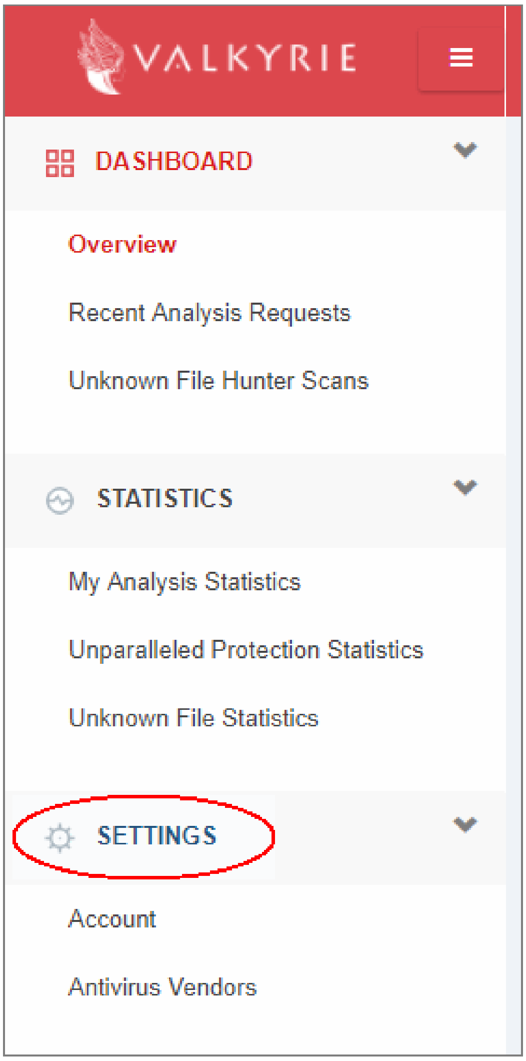
Live Unknown File Statistics

FILE TYPE	NUMBER OF UNKNOWNS
Exe	54168
Dll	21276

4.8 Configure Valkyrie Account Settings

The 'Settings' interface lets you change your current password, select your current antivirus vendor, view global statistics and more.

- Click the hamburger menu button top-left
- Click 'Settings' link on the left-hand



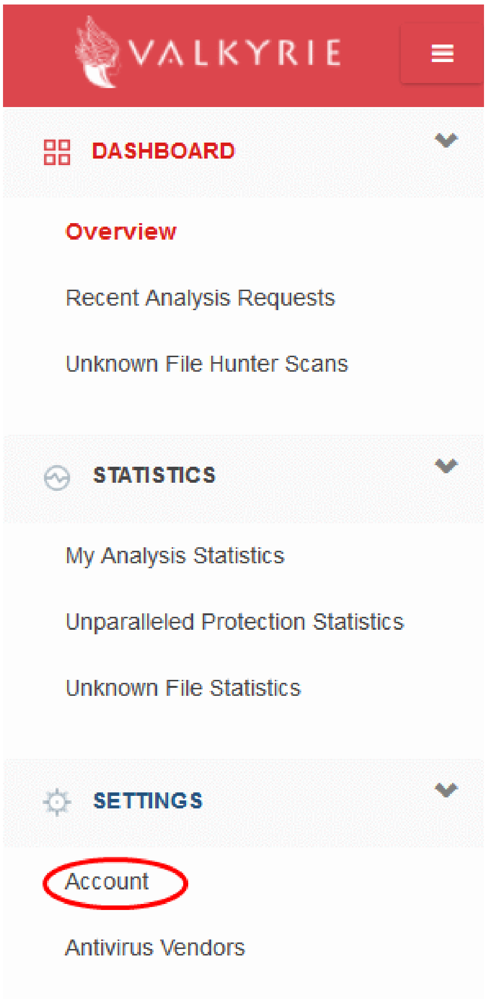
The dashboard has the following areas:

- **Account**
- **Antivirus Vendors**

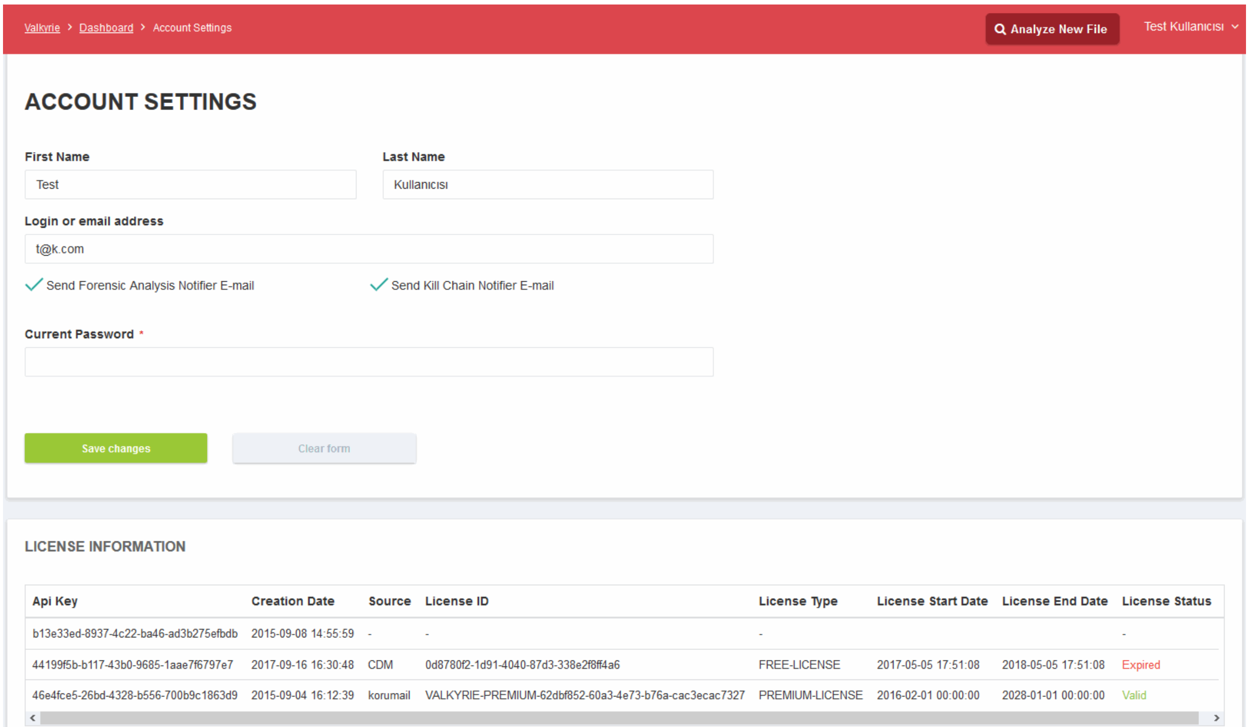
4.8.1 Account Configuration

- Click the hamburger menu button top-left
- Click 'Settings' > 'Account' in the left-hand menu

  OR
- Click your username at top-right then 'Settings'



The 'Accounts' screen will open:



ACCOUNT SETTINGS

First Name: Test

Last Name: Kullanıcısı

Login or email address: t@k.com

✓ Send Forensic Analysis Notifier E-mail

✓ Send Kill Chain Notifier E-mail

Current Password *

LICENSE INFORMATION

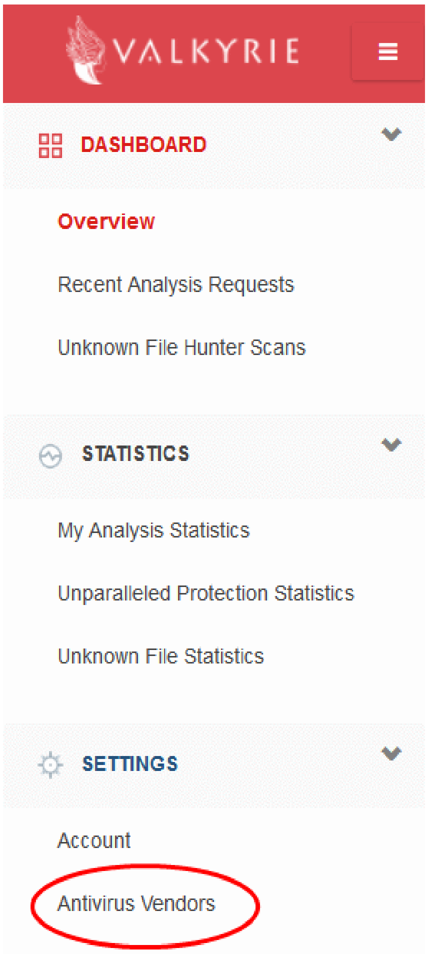
Api Key	Creation Date	Source	License ID	License Type	License Start Date	License End Date	License Status
b13e33ed-8937-4c22-ba46-ad3b275efbdb	2015-09-08 14:55:59	-	-	-			-
44199f5b-b117-43b0-9685-1aae7f6797e7	2017-09-16 16:30:48	CDM	0d8780f2-1d91-4040-87d3-338e2f8ff4a6	FREE-LICENSE	2017-05-05 17:51:08	2018-05-05 17:51:08	Expired
46e4fce5-26bd-4328-b556-700b9c1863d9	2015-09-04 16:12:39	korumail	VALKYRIE-PREMIUM-62dbf852-60a3-4e73-b76a-cac3ecac7327	PREMIUM-LICENSE	2016-02-01 00:00:00	2028-01-01 00:00:00	Valid

User Information

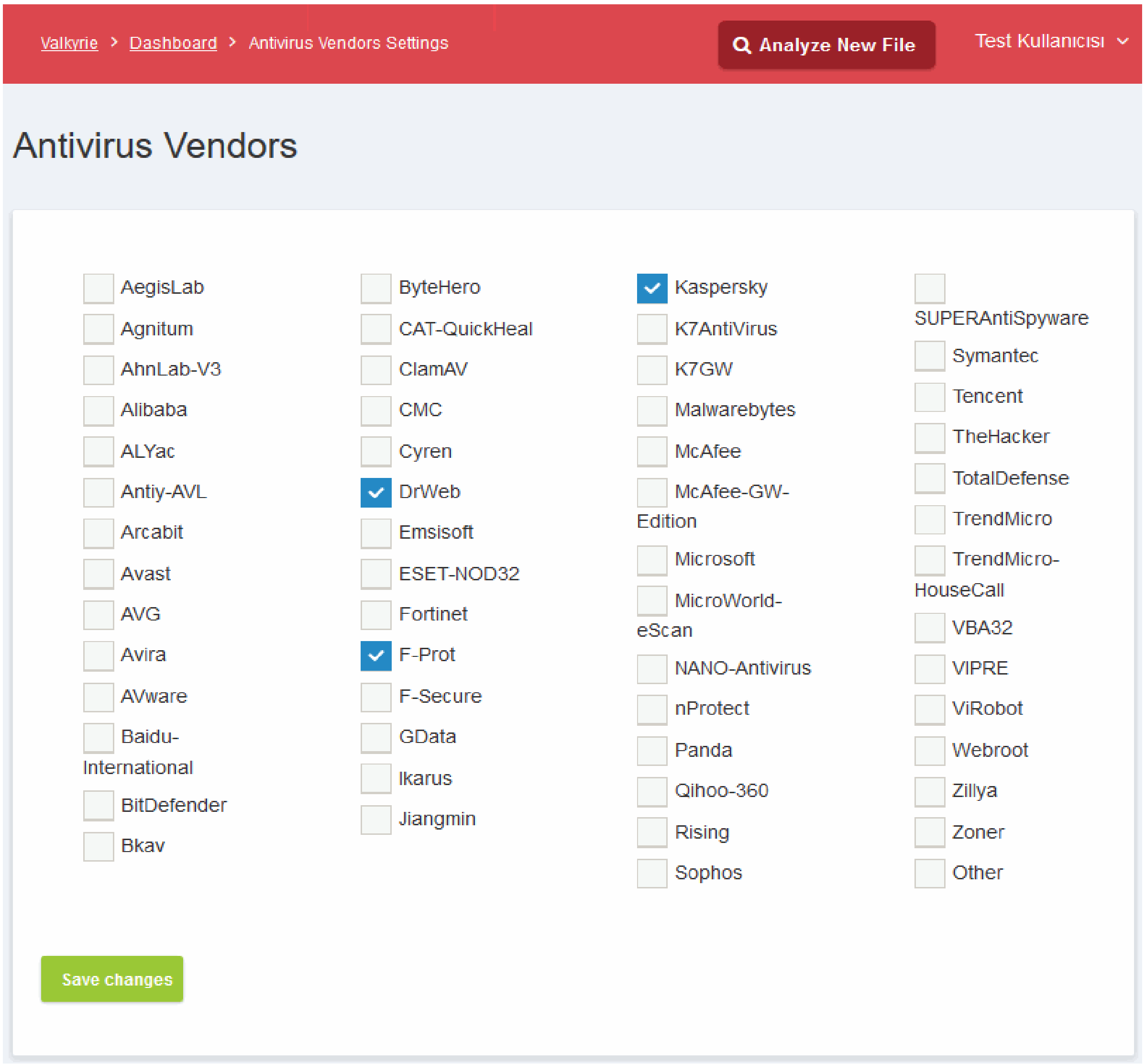
- First Name/ Last Name - The names that you provided during account creation. You can update these if required. Your name is shown at the top-right corner after signing into your account.
- Email - The email address that was provided during account creation. This field cannot be edited.
- Send Forensic Analysis Notifier E-mail - Send an email alert each time an unknown and potentially malicious file is identified
- Send Kill Chain Notifier E-mail – Send an email alert each time a piece of malware is discovered.
- Current Password - You need to enter your existing password if you wish to reset it
- Click 'Clear form' to reset data
- License Information – Subscription details for the current account
- Click 'Save changes' to apply your new settings.

4.8.2 Antivirus Vendors

- Choose all antivirus software vendors that you use or have used in the past.
- Valkyrie uses this data to measure it's performance against leading antivirus products.
- For example, if Valkyrie finds a zero-day threat, it will check whether the threat was also found by your selected vendors. You can view this information in the 'Unparalleled Protection Statistics' section.
- Click the hamburger menu button top-left
- Click 'Settings' > 'Antivirus Vendors' in the left-hand menu



The 'Antivirus Vendors' screen will open:



Antivirus Vendors

□ AegisLab
□ Agnitum
□ AhnLab-V3
□ Alibaba
□ ALYac
□ Antiy-AVL
□ Arcabit
□ Avast
□ AVG
□ Avira
□ AVware
□ Baidu-International
□ BitDefender
□ Bkav
□ ByteHero
□ CAT-QuickHeal
□ ClamAV
□ CMC
□ Cyren
☑ DrWeb
□ Emsisoft
□ ESET-NOD32
□ Fortinet
☑ F-Prot
□ F-Secure
□ GData
□ Ikarus
□ Jiangmin
☑ Kaspersky
□ K7AntiVirus
□ K7GW
□ Malwarebytes
□ McAfee
□ McAfee-GW-Edition
□ Microsoft
□ MicroWorld-eScan
□ NANO-Antivirus
□ nProtect
□ Panda
□ Qihoo-360
□ Rising
□ Sophos
□ SUPERAntiSpyware
□ Symantec
□ Tencent
□ TheHacker
□ TotalDefense
□ TrendMicro
□ TrendMicro-HouseCall
□ VBA32
□ VIPRE
□ ViRobot
□ Webroot
□ Zillya
□ Zoner
□ Other

Save changes

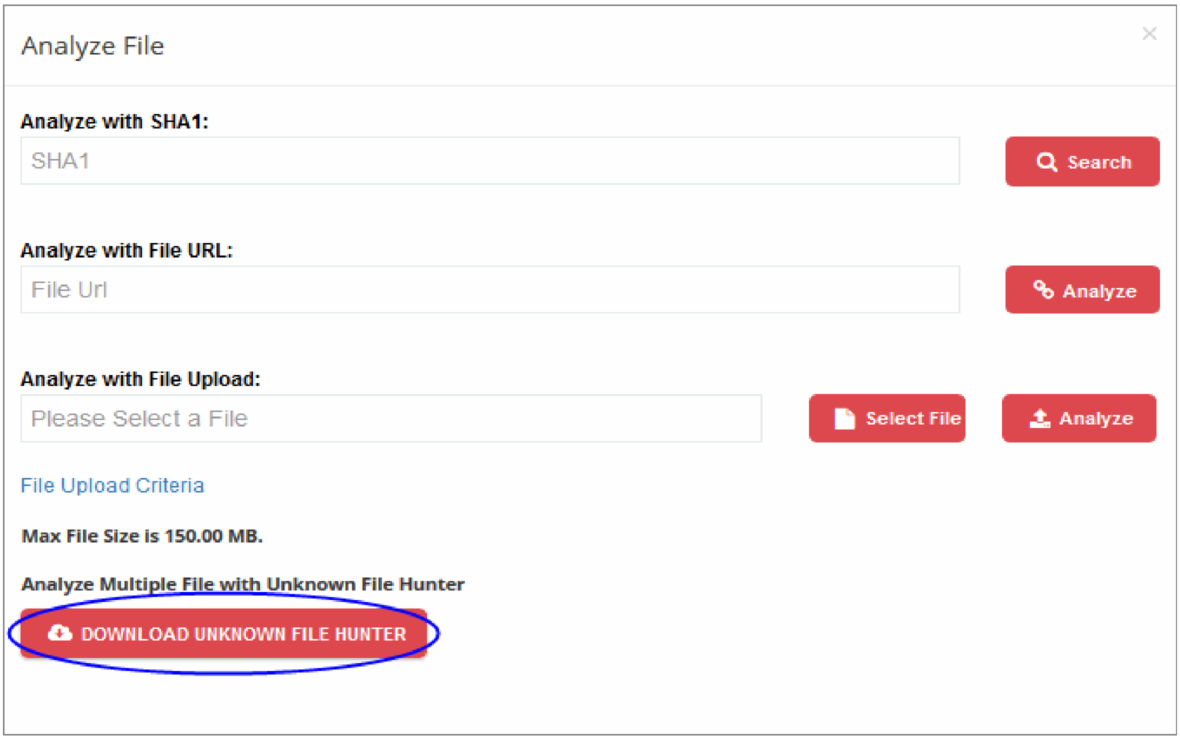
- Select the vendor(s) that you are currently using or deselect a vendor.
- Click the 'Save Changes' button to update the vendor.

5 Unknown File Hunter Tool

- Comodo Unknown File Hunter (UFH) is a lightweight scanner capable of identifying previously undetected threats on a network.
- After a scan, it classifies all audited files as 'Trusted / Clean', 'Malicious', 'Unknown', 'Not Analyzed' or 'In Analysis'.
- While 'Trusted' files are OK and 'Malicious' files should be deleted immediately, it is the 'Unknown' category which houses most zero-day threats.
- The scanner lets you upload unknown files to Valkyrie to establish whether or not they are malicious. You can view the results of these tests in the Valkyrie interface.
- There are two ways to download the tool:
- From the main Valkyrie interface

OR

- Click the 'Analyze New File' button
- Then click the 'Download Unknown File Hunter' button



Analyze File

Analyze with SHA1: SHA1

Analyze with File URL: File Url

Analyze with File Upload: Please Select a File

File Upload Criteria

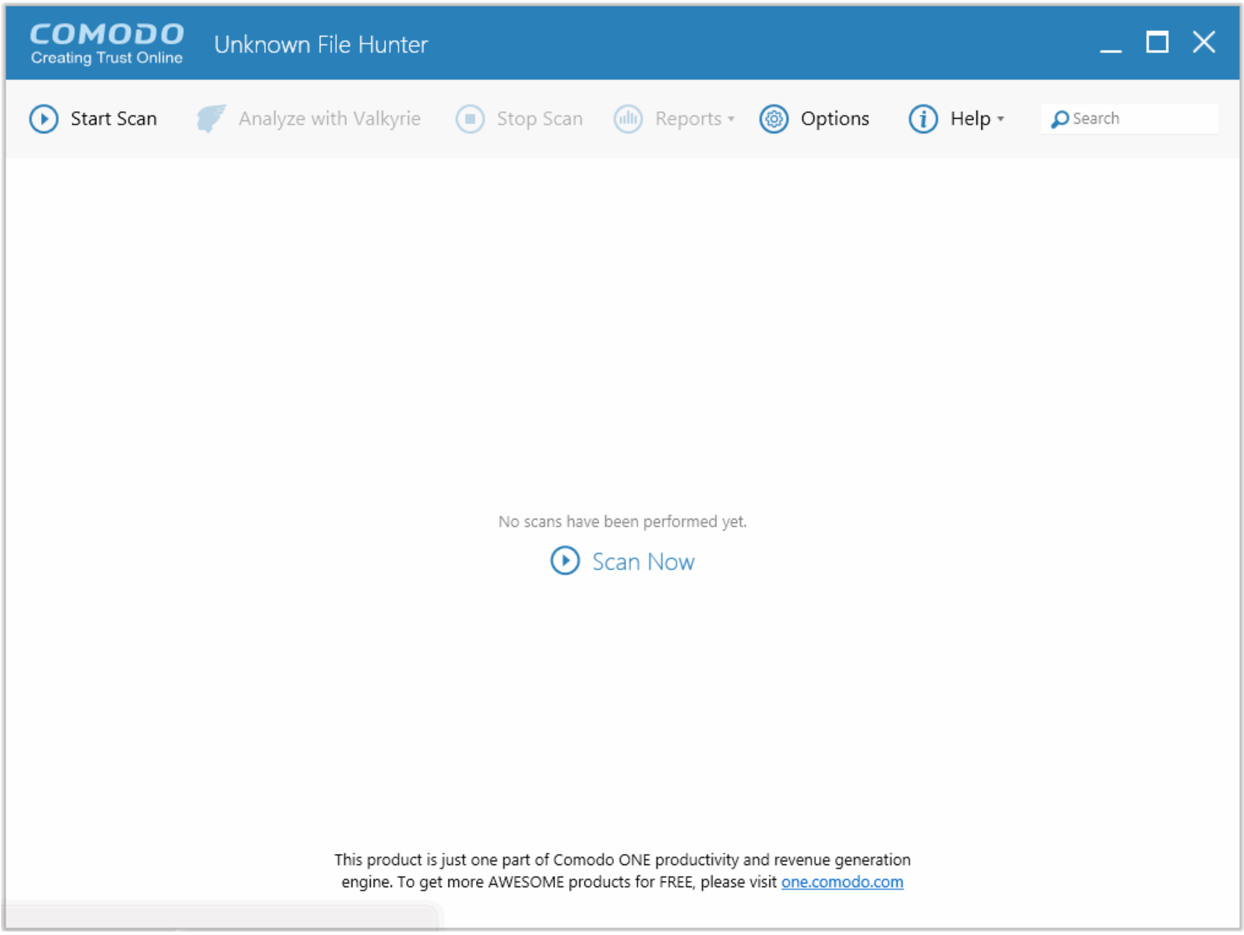
Max File Size is 150.00 MB.

Analyze Multiple File with Unknown File Hunter

- Save the setup file to your local device.

Scan your network

- Run the UFH executable to start the utility
- Click 'Scan Now' to select the endpoints you wish to scan:



No scans have been performed yet.

This product is just one part of Comodo ONE productivity and revenue generation engine. To get more AWESOME products for FREE, please visit one.comodo.com

How to use the Comodo UFH tool

Step 1 - Getting started

- Login to your Valkyrie account at **https://valkyrie.comodo.com/login**
- Download, install and run 'Unknown File Hunter'
- Click 'Scan Now'

Step 2 - Specify targets and run a scan

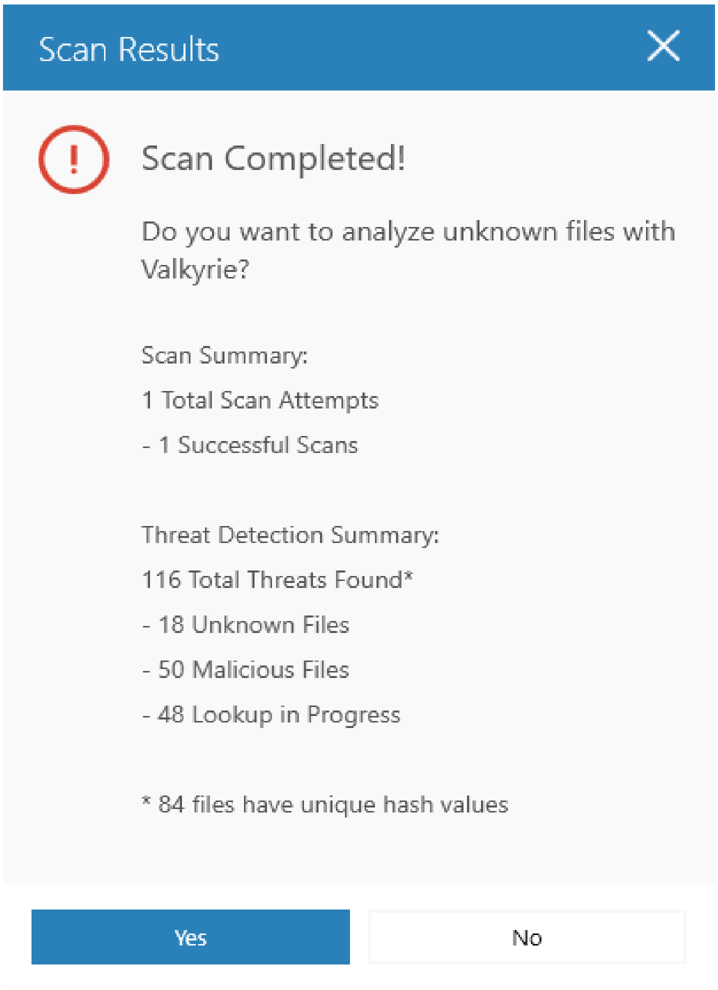
The utility provides four methods of specifying target endpoints:

- **Active Directory -** Import target computers via active directory.
- **Workgroup -** Add computers that belong to a particular work group.
- **Network Address -** Specify individual host names, IP addresses or IP ranges for scanning.
- **This Computer -** Scan your local device for unknown files. You can run quick, full or custom scans.

If you need more help to specify targets, refer to our online guide at **https://help.comodo.com/topic-400-1-794-10428-Scanning-Computers.html**. Click 'Start Scan' to begin the scan.

Step 3 - Submit unknown files to Valkyrie (optional) and view results

Upon scan completion, you will see a results summary as follows:



Scan Results

Scan Completed!

Do you want to analyze unknown files with Valkyrie?

Scan Summary:

1 Total Scan Attempts

- 1 Successful Scans

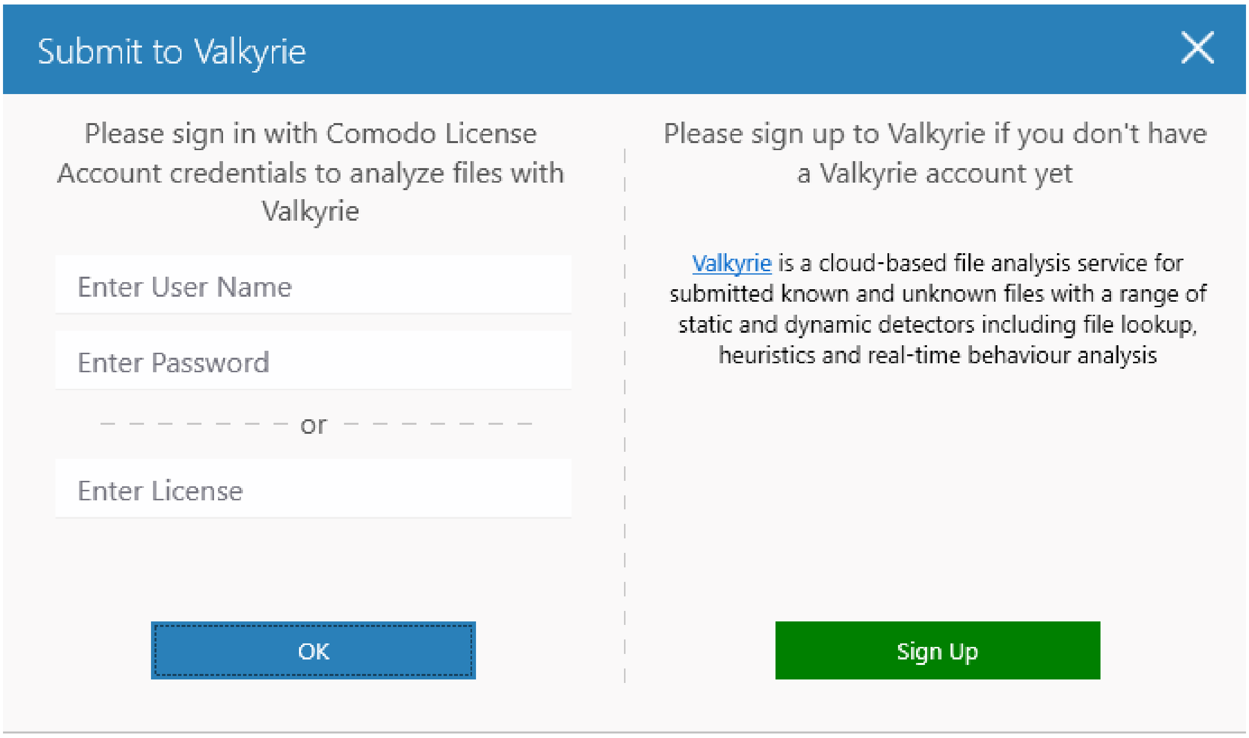
Threat Detection Summary:

116 Total Threats Found*

- 18 Unknown Files
- 50 Malicious Files
- 48 Lookup in Progress

* 84 files have unique hash values

- You have the option to upload unknown files (aka 'unique hash values') to Valkyrie for analysis.
- Click 'Yes'. The 'Submit to Valkyrie' dialog will be displayed.



Submit to Valkyrie

Please sign in with Comodo License Account credentials to analyze files with Valkyrie

Enter User Name

Enter Password

or

Enter License

Please sign up to Valkyrie if you don't have a Valkyrie account yet

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, heuristics and real-time behaviour analysis

- Enter your username / password or license to login to Valkyrie and upload your files

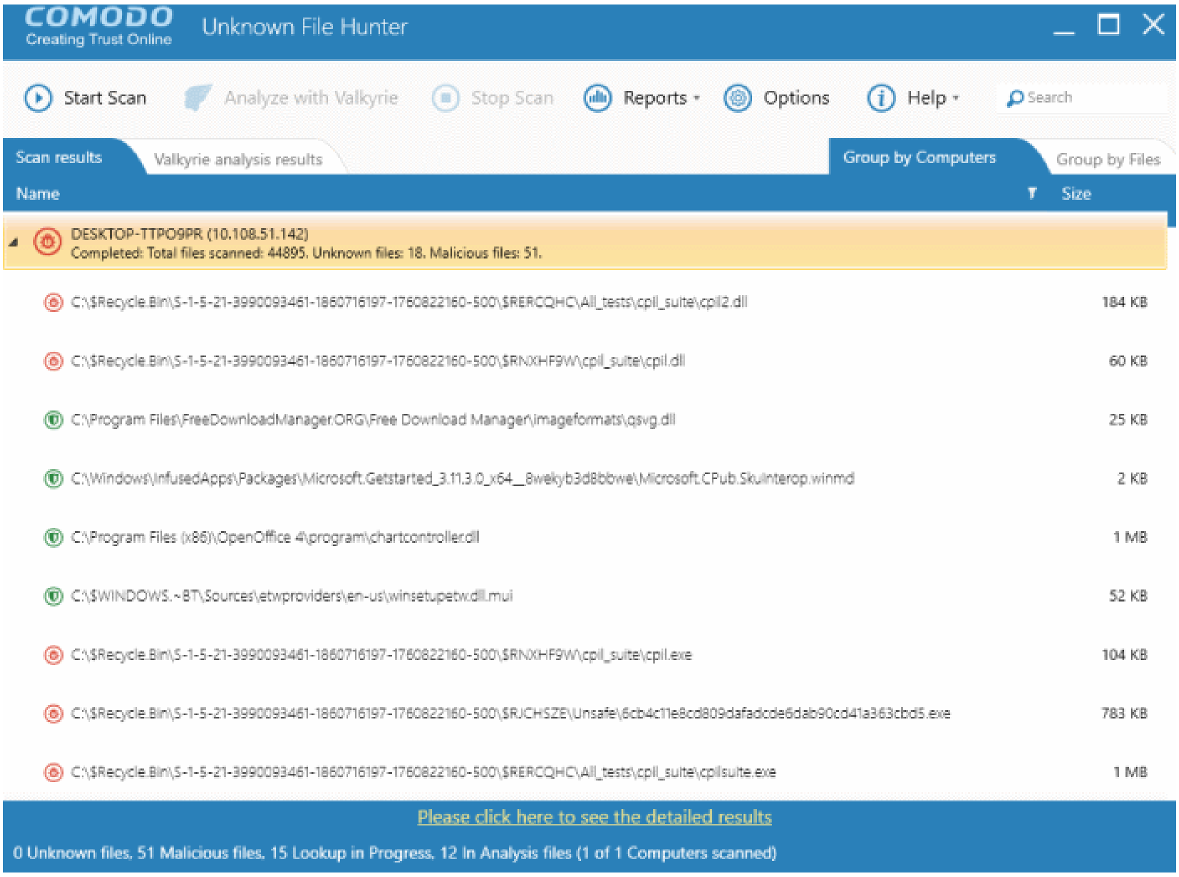
OR

- Click 'Sign Up'. If you do not have an account. You will be taken to Comodo Valkyrie subscription page.

Valkyrie is an automated, cloud-based behavior analysis system which subjects unknown files to a battery of static and dynamic tests to try and discover malicious or anomalous behavior.

After the analysis is complete, you can generate the 'Unknown File Hunter Scans' report. See **Unknown File Hunter Scans** for more help with this.

- Next, go back to the Unknown File Hunter interface. All 'Unknown' files from the local scan will be shown in the 'Scan results' tab. Valkyrie detection will be displayed in the 'Valkyrie analysis results' tab:

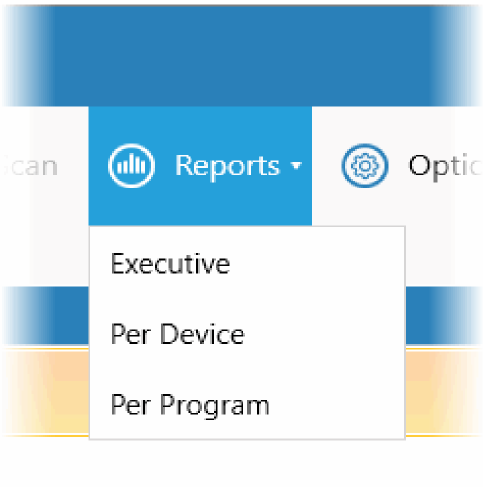


Name	Size
DESKTOP-TTPO9PR (10.108.51.142) Completed: Total files scanned: 44895. Unknown files: 18. Malicious files: 51.	
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-1760822160-500\$RERCQHC\All_tests\cpil_suite\cpil2.dll	184 KB
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-1760822160-500\$RNXHF9W\cpil_suite\cpil.dll	60 KB
C:\Program Files\FreeDownloadManager.ORG\Free Download Manager\imageformats\qsvg.dll	25 KB
C:\Windows\InfusedApps\Packages\Microsoft.Getstarted_3.11.3.0_x64__8wekyb3d8bbwe\Microsoft.CPub.SkuInterop.winmd	2 KB
C:\Program Files (x86)\OpenOffice 4\program\chartcontroller.dll	1 MB
C:\$WINDOWS.~BT\Sources\etwproviders\en-us\winsetupetw.dll.mui	52 KB
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-1760822160-500\$RNXHF9W\cpil_suite\cpil.exe	104 KB
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-1760822160-500\$RJCHSZE\Unsafe\6cb4c11e8cd809dafadcde6dab90cd41a363cbd5.exe	783 KB
C:\$Recycle.Bin\S-1-5-21-3990093461-1860716197-1760822160-500\$RERCQHC\All_tests\cpil_suite\cpilsuite.exe	1 MB

Please click here to see the detailed results

0 Unknown files. 51 Malicious files. 15 Lookup in Progress. 12 In Analysis files (1 of 1 Computers scanned)

- The bottom of the Unknown file hunter analysis results page displays a summary of files that are (still) unknown and those that CUFH found to be malicious. You can view a more detailed version of these results in the Valkyrie interface. To do so, click 'Please click here to see the detailed results'. For more details on these results, see **Valkyrie Analysis Results.**
- You also can view detailed reports by clicking the 'Reports' tab at the top of the UFH interface:



- Executive - Top level summary of scan results.
- Per Device - Scan results per device scanned.
- Per Program - Scan results which provide details of each unknown / malicious program, and the devices upon which it was found.

For more details about reports, see **Reports**.

For more help with Unknown File Hunter, please see our online guide at **https://help.comodo.com/topic-400-1-794-10426-Introduction-to-Comodo-Unknown-File-Hunter.html**

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 : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**