

A2019 - Check URLs Threats from VirusTotal Portal

[Readme](#)

Table of Contents

1. Introduction	3
1.1 Overview	3
1.2 Use Cases	3
2. Requirements & Prerequisites	4
2.1 System Requirements	4
2.2 Prerequisites	4
3. Getting Started	5
3.1 Quick Start	5
3.1.1 Setup	5
3.1.2 Configuration	10
4. Support & FAQs	22
4.1 Support	22
4.2 FAQs	22
Appendix A: Record of Changes	23
Appendix B: References	24

1. Introduction

This document contains all essential information for the user to make full use of this A2019 *(Bot/Command Package)*. It includes a description of the functions and capabilities and step-by-step procedures for setup & configuration of the *(Bot/Command Package)*.

1.1 Overview

The Bot extracts information from the web portal [virustotal.com](https://www.virustotal.com) based on a suspicious URL. At the entrance waits for a CSV file of the URLs to be queried and generates to the output an excel file with the relevant quantification of your cyber threats.

1.2 Use cases

The key use cases include:

- *Check for a URL the number of malicious threats*
- *Check for a URL the number of malware threats*
- *Check for a URL the number of Phishing threats*
- *Check for a URL the number of Suspicious threats*
- *Get the domain owner email from abuse domain*
- *Get the Abuse domain Contact Phone*
- *Get the Domain Creation Date.*

2. Requirements & Prerequisites

2.1 System Requirements

[Enterprise A2019 \(Cloud deployed\) and Community Edition device requirements.](#)

Machine hardware specifications: 8 GB RAM

Operating system versions: MS Windows 10

Browser types supported: MS Internet Explorer

Command packages: Analyze, Application, Boolean, Browser, Comment, CSV/TXT, Datetime, Delay, Error Handler, Excel Advanced, File, Folder, IF, List, Logtofile, Loop, Message Box, Number, Python Script, Recorder, Screen, Simulate Keystroke, Step, String, System, Taskbot, Windows.

2.2 Prerequisites

[*Python.exe*](#)

[*Whois64.exe*](#)

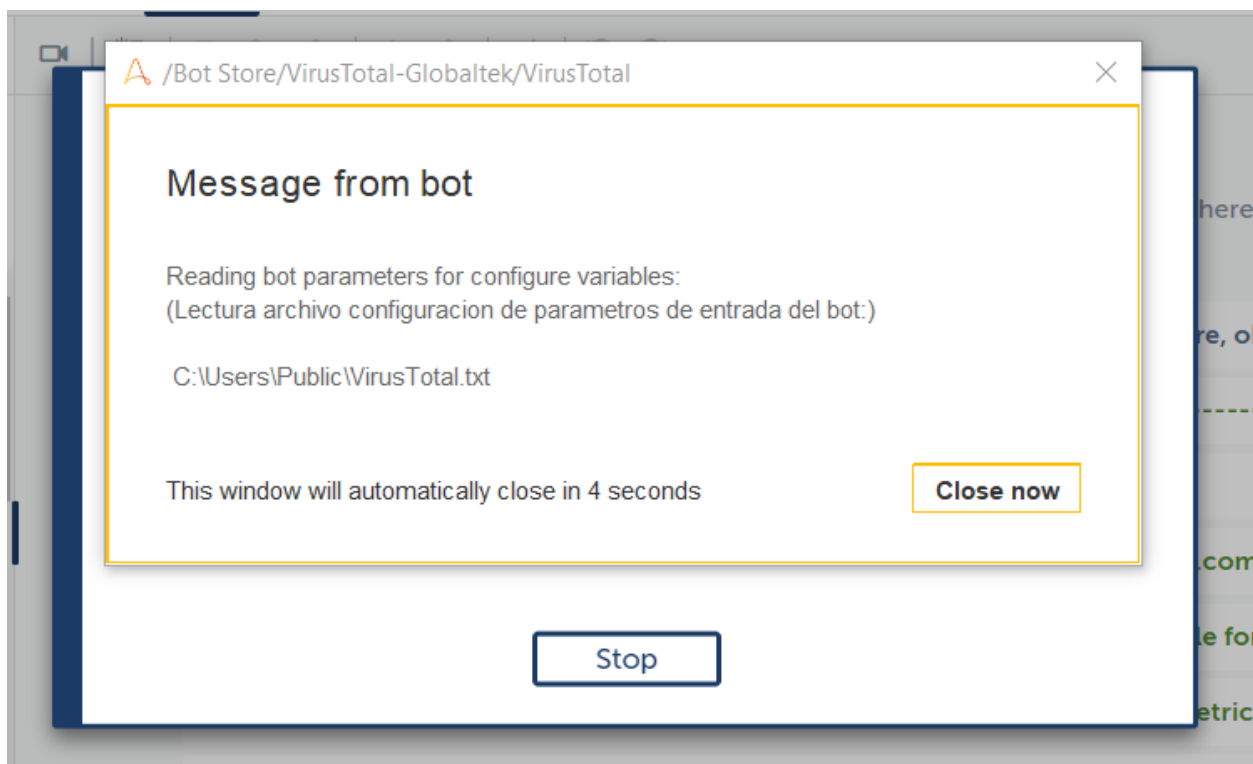
[*Whois64.bat Wrapper \(Included into the A2019 Control Room\)*](#)

3. Getting Started

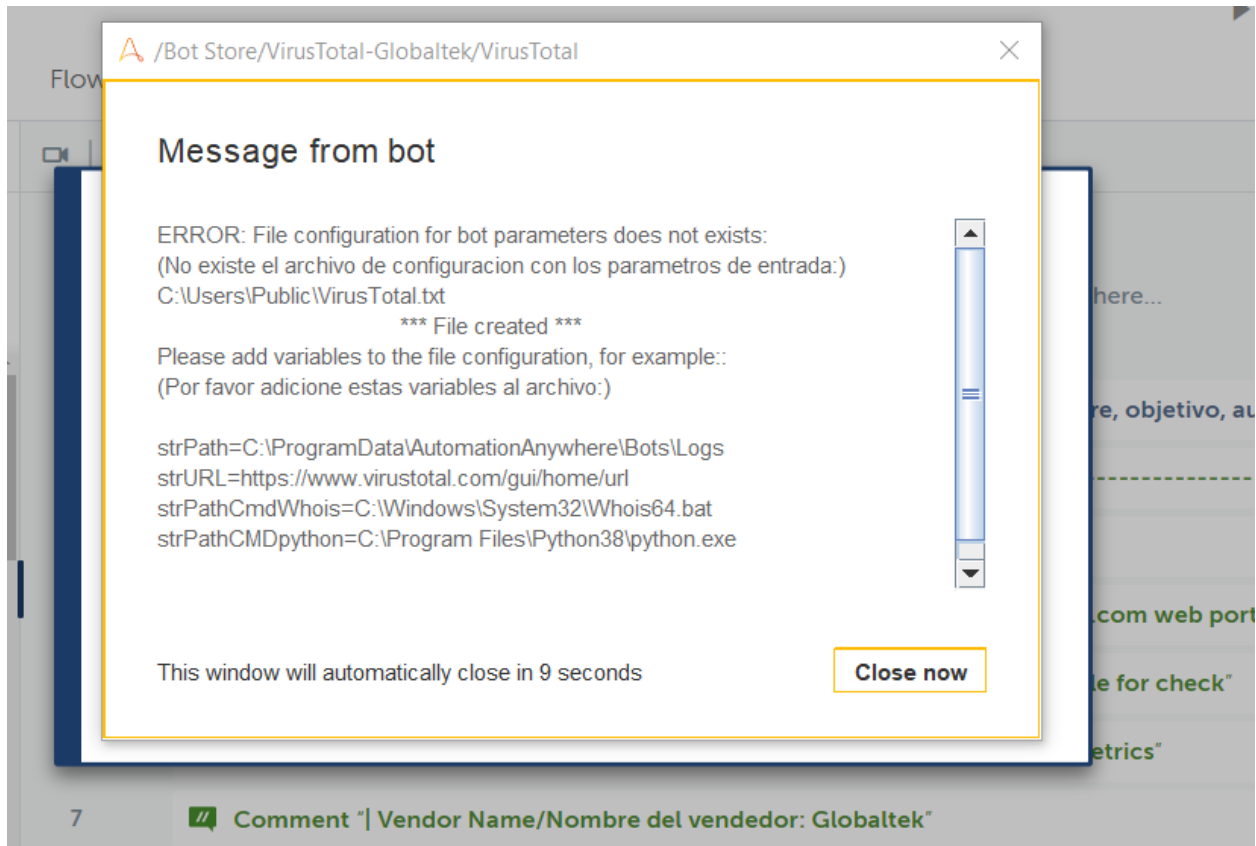
3.1 Quick Start

3.1.1 Setup

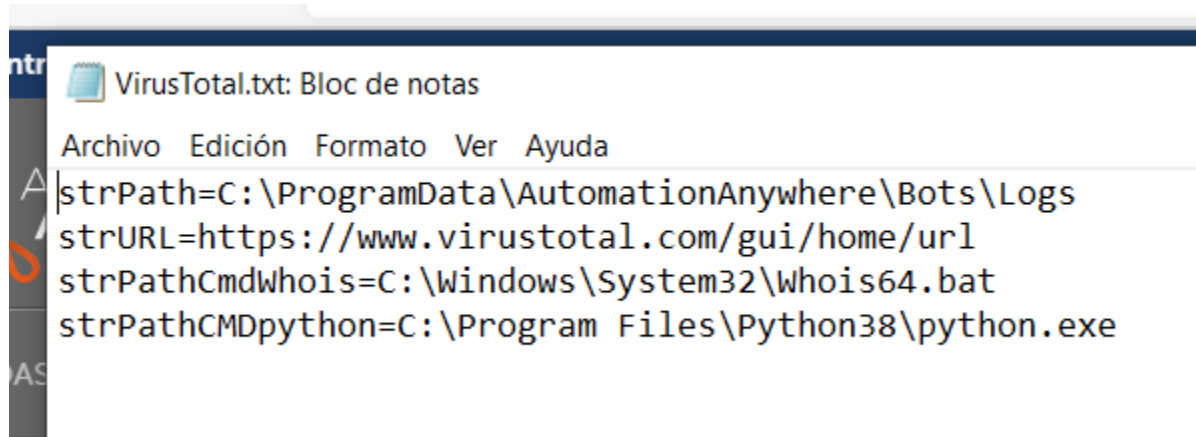
Step 1. First time run the virustotal bot, it looks the file parameters configuration into C:\Users\Public\VirusTotal.txt directory



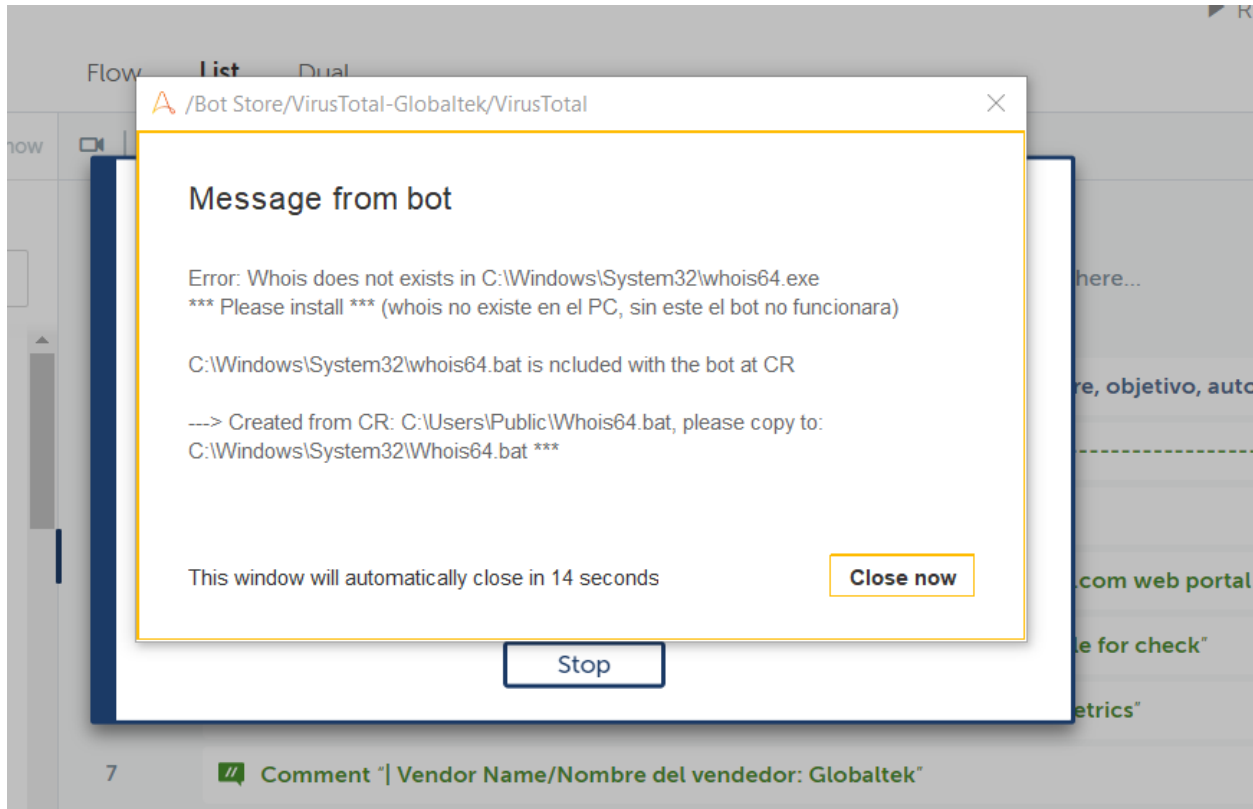
Step 2. If the file configuration does not exist, then it will create a file parameters configuration into C:\Users\Public\VirusTotal.txt directory



Step 3. The bot will automatically open the notepad, please edit and modify the parameters to indicate the preferred working directory



Step 4. Install whois64.exe as an external windows program in the strPathCmdWhois route

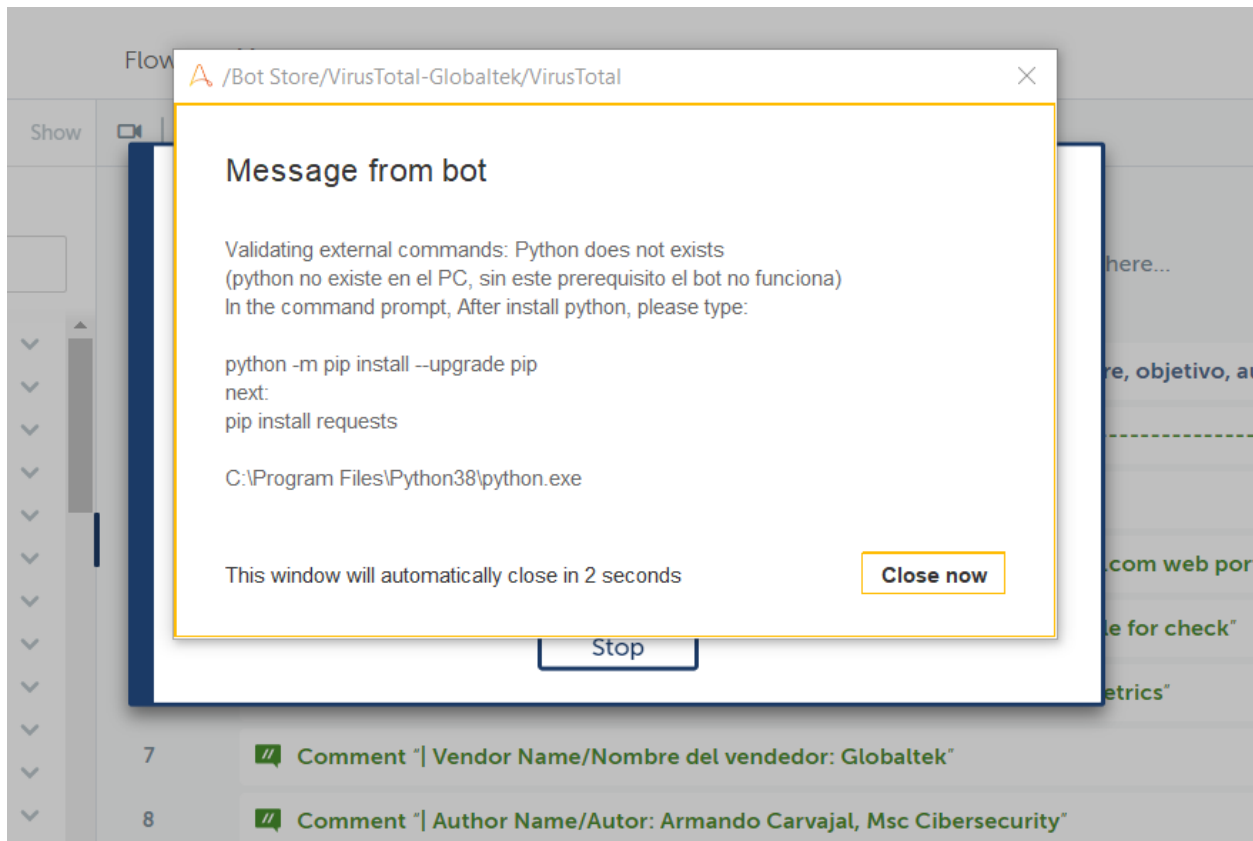


Step 5. Edit if necessary C:\Users\Public\Whois64.bat

Copy C:\Users\Public\Whois64.bat to C:\Windows\System32\Whois64.bat

> Windows-SSD (C:) > Windows > System32				
Nombre	Fecha de modificación	Tipo	Tamaño	
whoami.exe	7/12/2019 4:09 a. m.	Aplicación	72 KB	
Whois64.bat	30/04/2020 6:34 p. m.	Archivo por lotes ...	1 KB	
whois64.exe	11/12/2019 8:39 a. m.	Aplicación	511 KB	
wiaacmgr.exe	7/12/2019 4:09 a. m.	Aplicación	97 KB	

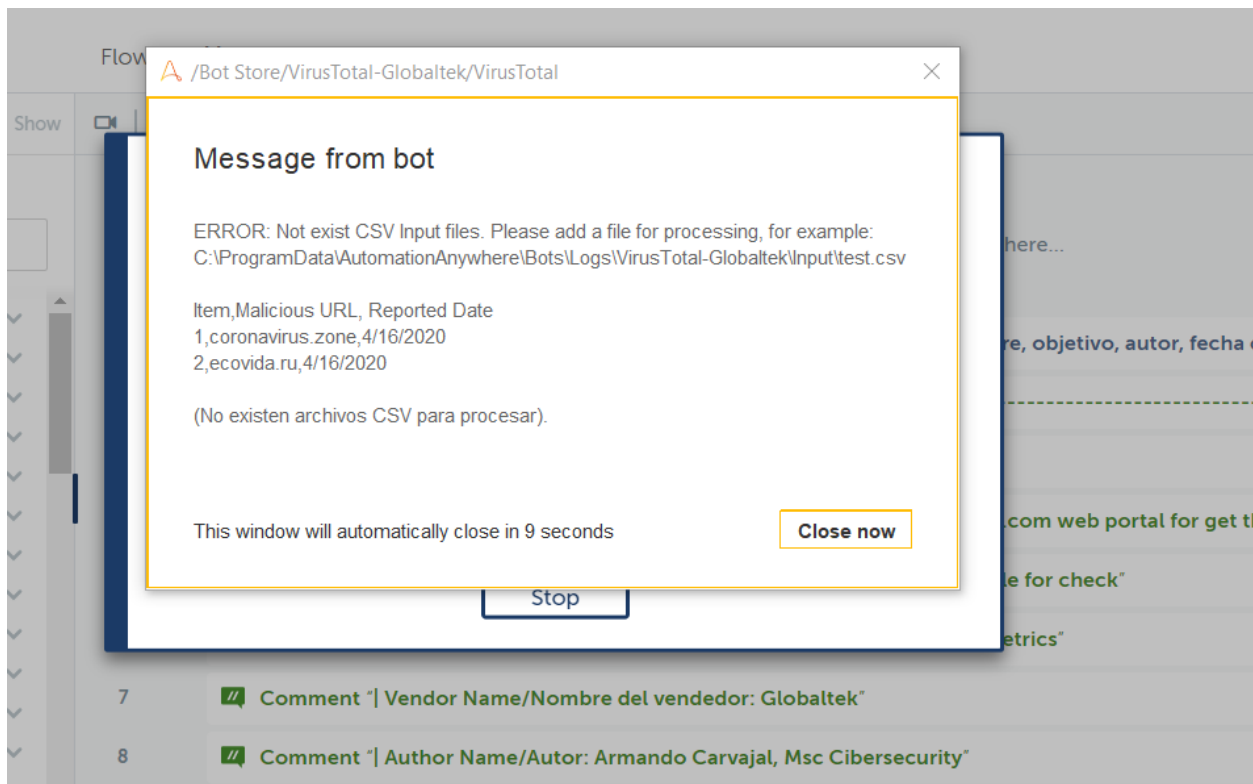
Step 6. Install python as an external windows program in the strPathCMDpython route



End of setup.

3.1.2 Configuration and Use

Step 1. After configured the bot, the first time run the bot, the bot automatically looks the CSV file inputs malicious URLs. If the input file does not exist, you will see the next error



Step 2. Prepare a CSV file with malicious URLs, for example the "test.csv" file:

	A	B	C
1	Item	Malicious URL	Reported date
2	1	coronavirus.zone	4/16/2020
3	2	ecovida.ru	4/16/2020
4	3	feenixlanguage.com	4/16/2020
5	4	impots-covid19.com	4/16/2020
6	5	kbfvzoboss.bid	4/16/2020
7	6	pescaturismocorona.it	4/16/2020
8	7	treatmentcovid2019.com	4/16/2020
9	8	update-apk.net	4/16/2020
10	9	www.coronavirus.app	4/16/2020
11	10	https://coronavirus.app/map?selected=zC03Urt1iJb2Tf6p0jd	4/16/2020
12	11	https://netflix-usa.net/?periodo-de-aislamiento-libre	4/16/2020
13			

Step 3. Please add a file within to the input directory with malicious URLs

Windows-SSD (C:) > ProgramData > AutomationAnywhere > Bots > Logs > VirusTotal-Globaltek

Nombre	Fecha de modificación	Tipo	Tamaño
Config	4/08/2020 7:35 p. m.	Carpeta de archivos	
Errors	4/08/2020 7:35 p. m.	Carpeta de archivos	
Input	7/08/2020 12:37 p. m.	Carpeta de archivos	
Output	7/08/2020 1:13 p. m.	Carpeta de archivos	
TMP	7/08/2020 11:32 a. m.	Carpeta de archivos	

SSD (C:) > ProgramData > AutomationAnywhere > Bots > Logs > VirusTotal-Globaltek > Input

Nombre	Fecha de modificación	Tipo	Tamaño
test.csv	7/08/2020 12:36 p. m.	Archivo de valores...	1 KB

End of setup

- For Configuring the Bot – Configurable variable list:

INPUT VARIABLES				
Variable Name	Type	Mandatory	Purpose	Example Input
strPath	String	Yes	Path for the configure template from which the Bot reads the value from path	strPath = C: \ ProgramData \ AutomationAnywhere \ Bots \ Logs
strURL	String	Yes	URL for the configure template from which the Bot reads the value from VirusTotal URL portal	strURL = https://www.virustotal.com/gui/home/url
strPathCmdWhois	String	Yes	Path and Executable File Name for the configure template from which the Bot reads the value from. Format – Path\Filename. Extension This wrapper read the executable from whois64.exe	strPathCmdWhois = C:\Windows\System32\Whois64.bat
strPathCMDpython	String	Yes	Path and Executable File Name for the configure template from which the Bot	strPathCMDpython = C:\Program Files\Python38\python.exe

			<i>reads the value from.</i> <i>Format – Path\Filename. Extension</i> <i>This is the executable from python.exe</i>	
--	--	--	--	--

End of configurable variable list.

. Explain how a customer can use the bot once it's configured – walk through examples.

Step 1. Open the virustotal bot at the private bot store (Control Room A2019)

Bots > My bots > Private

My bots

+ Create new ▾ ⬇ Import bots...

PUBLIC PRIVATE

Private bots and files cannot be viewed by other people. If a bot or file has been checked out from the Public tab, it can be viewed and run by other people, but cannot be edited.

Folders

- Bots
- Bot Store
- Botname-VendorName
- VirusTotal-Glob...

Name ▾ Search

Files and folders (2)

	T. 41	NAME 12	STATUS	SIZE	LAST MODI...	MODIFIED BY
☐		Configuration	N/A	N/A	22:28:11 -05 2020-08-02	dev_00
☐		VirusTotal	Checked out	172.97 KB	23:39:52 -05 2020-08-04	dev_00

100 ▾ per page

Step 2. Edit the VirusTotal bot

Triggers

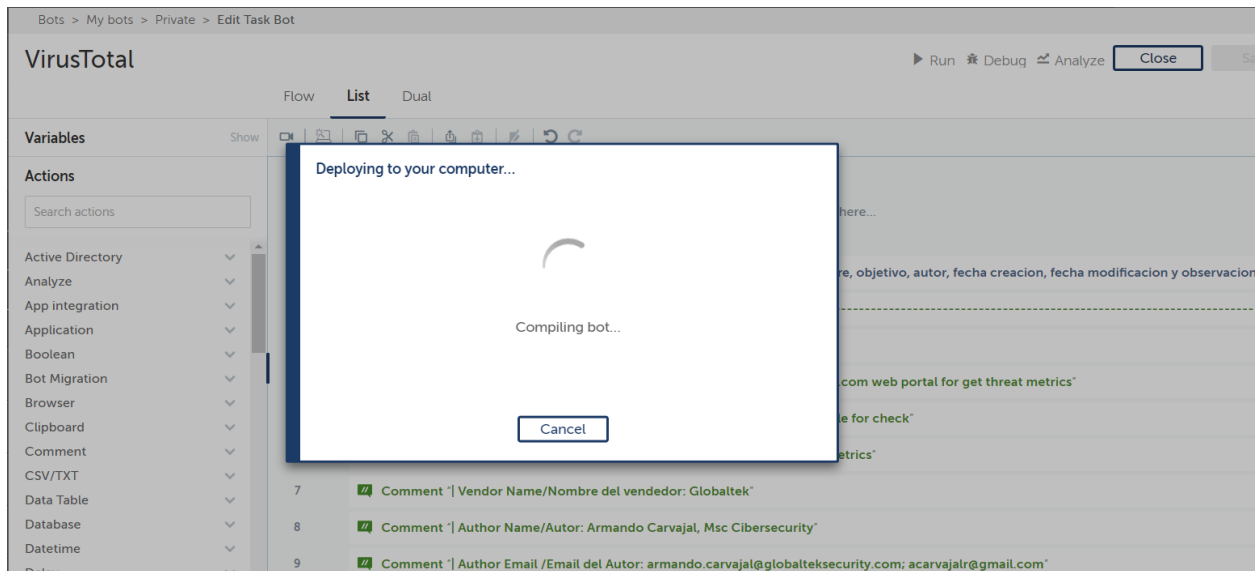
Drag a trigger here...

Start

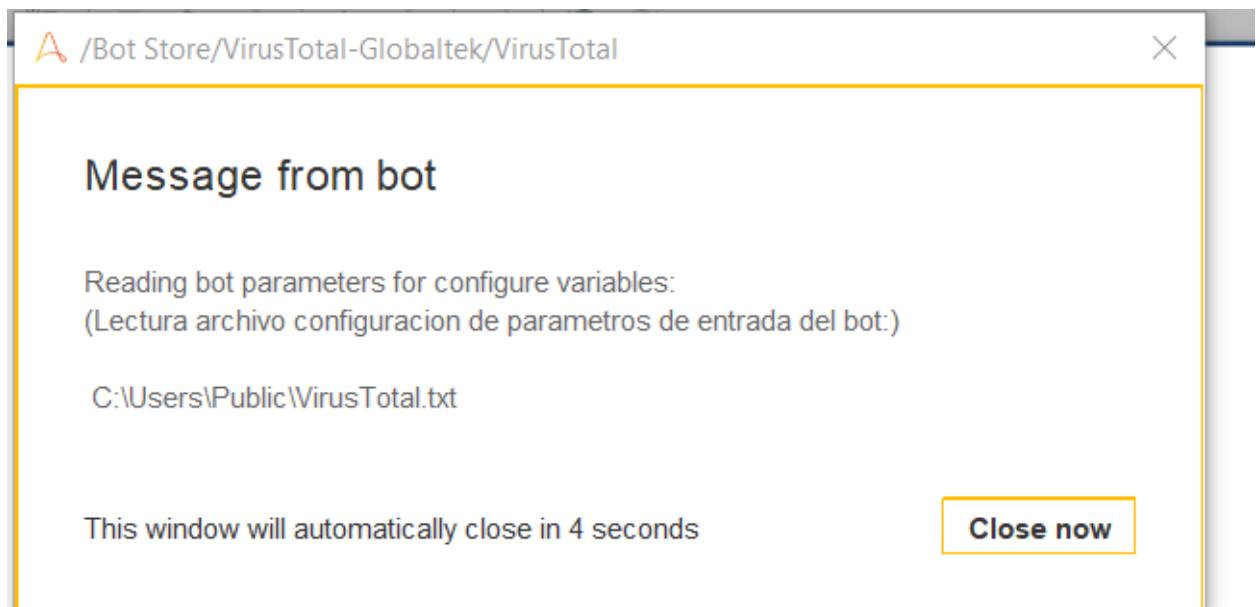
- Step "REQUIRED: Bot identification information/Identificacion del BOT (Nombre, objetivo, autor, fecha creacion, fecha modificacion y observaciones)"
- Step "1. Get automatically the bot name - Obtiene el nombre del bot"
- Step "2. REQUIRED: Verify Bot Name and Vendor Name"
- Step "3. Read Bot parameters - Lectura del archivo de configuracion parametros entrada del bot"
- Step "4. Set directories from configuration file - Configura Rutas o carpetas del proyecto para portabilidad"
- Step "5. Make directories for the bot - Crear carpetas para el bot"
- Step "6. Validating external commands - Valida la existencia de los comandos externos y sus carpetas"
- Step "7. Delete temp files - Borrar archivos temporales"
- Error handler: Try

End

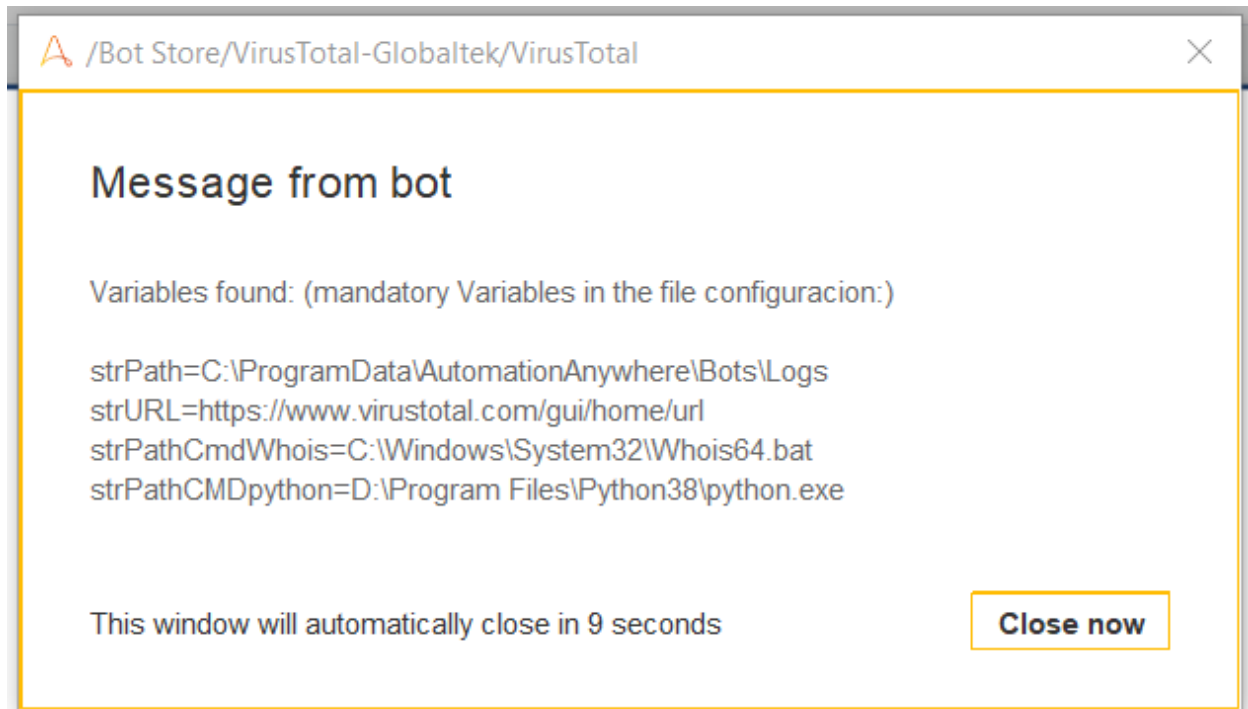
Step 3. Run the VirusTotal bot



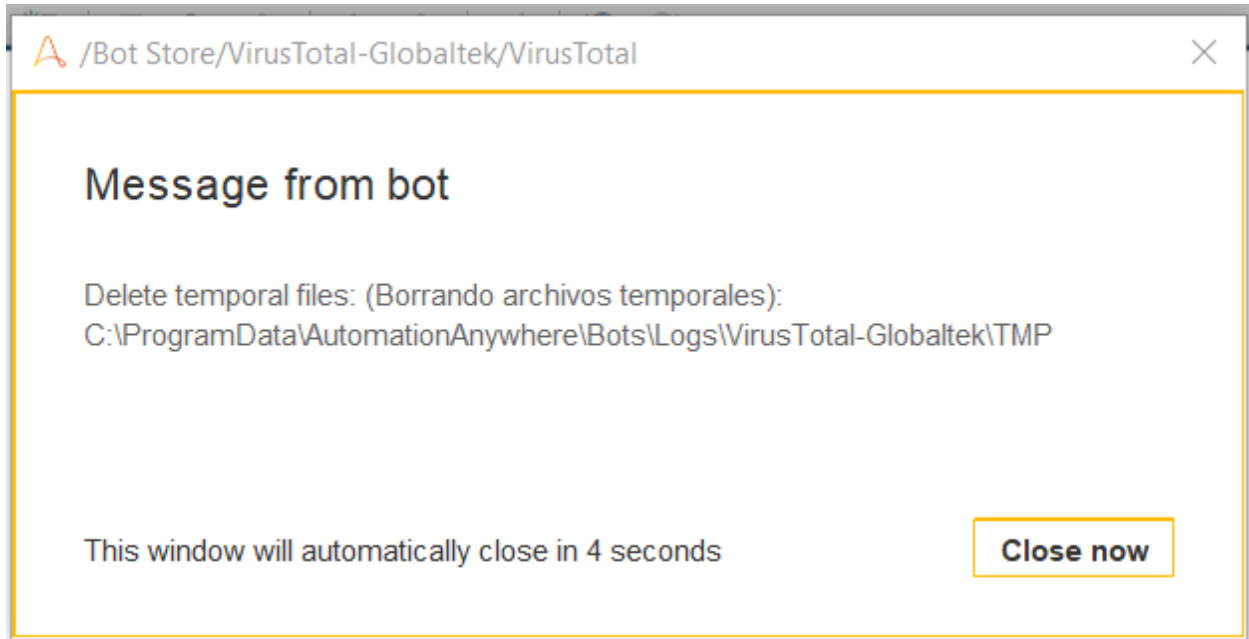
Step 4. Reading bot parameters



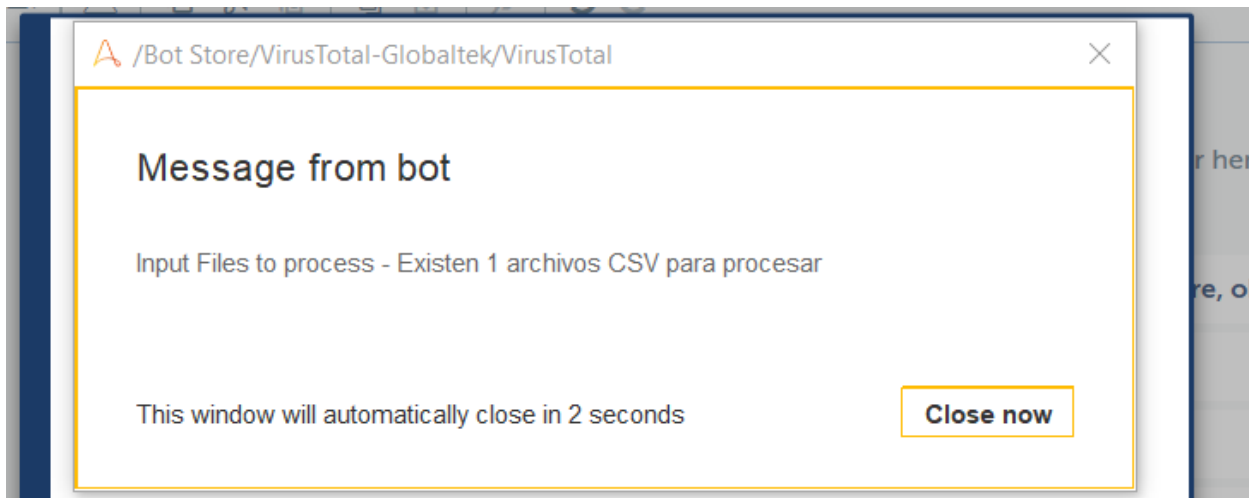
Step 5. Load parameters configuration



Step 6. Delete temporal files



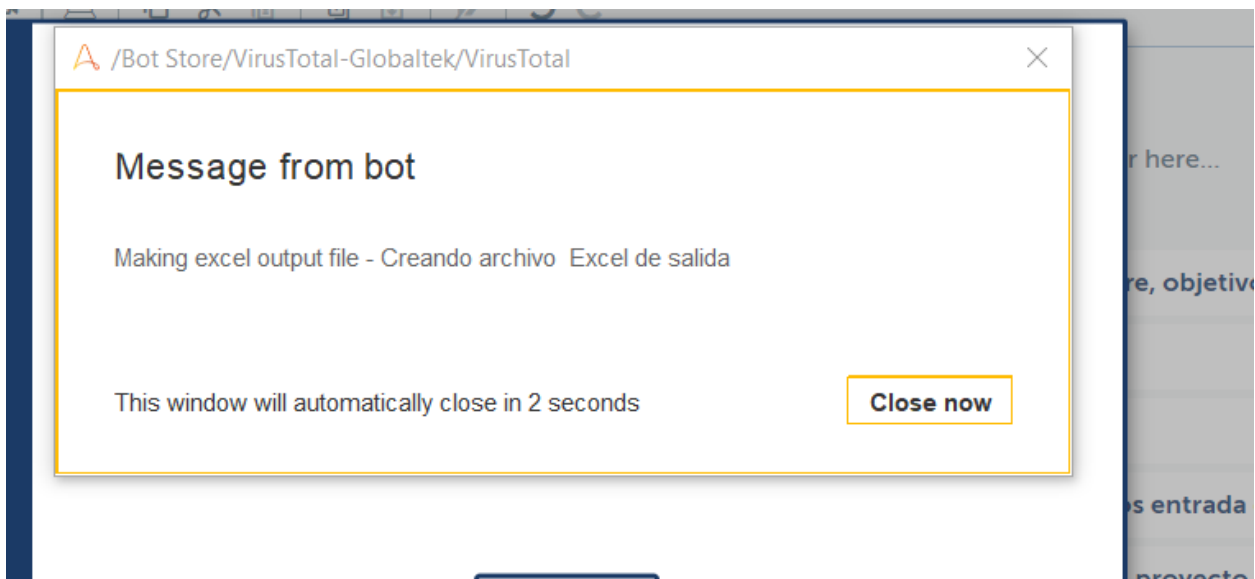
Step 7. Input files to process



Step 8. Create CSV disaster Recover file



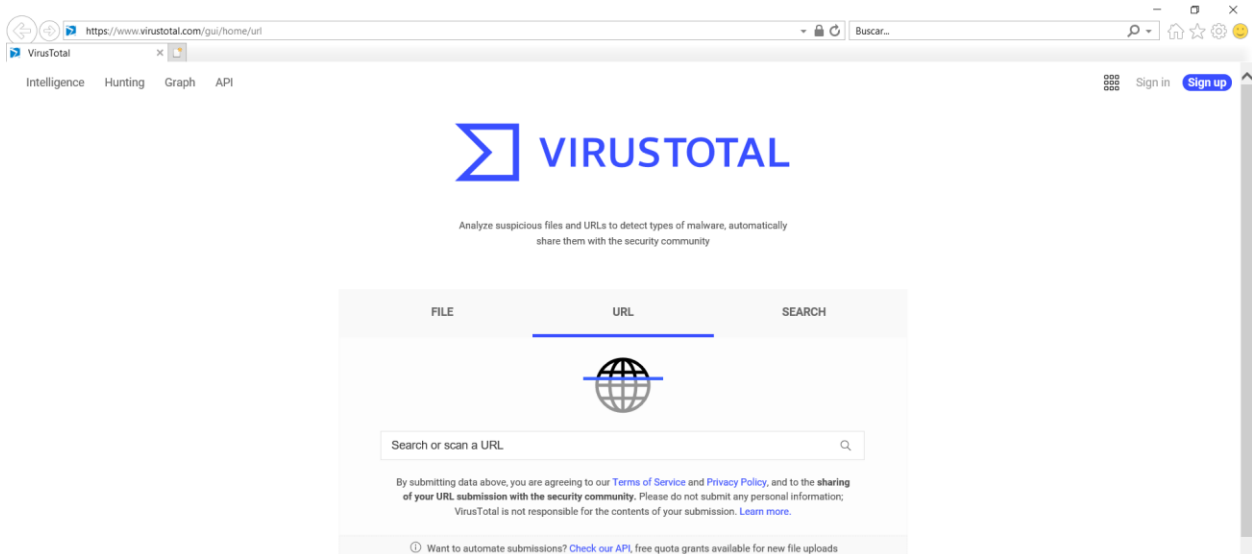
Step 9. Make excel output file



Step 10. Excel headers for the output

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Item	Verified URL	Reported date	Total Score	Malicious	Malware	Phishing	Suspicious	Abuse Contac	Abuse Contac	Domain Creation Date		
2													
3													
4													

Step 11. Open the virustotal portal and put the malicious URL



The screenshot shows the VirusTotal website interface. At the top, there's a navigation bar with links for Intelligence, Hunting, Graph, and API. The main heading is "VIRUSTOTAL" with a tagline: "Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community". Below this, there are three tabs: FILE, URL (which is selected), and SEARCH. Under the URL tab, there's a search bar with the placeholder text "Search or scan a URL". Below the search bar, there's a disclaimer: "By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your URL submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#)." At the bottom, there's a link: "Want to automate submissions? Check our API, free quota grants available for new file uploads".

Step 12. Gets information about malicious URL threats

https://www.virustotal.com/gui/url/11708c5ce8451c2b5c605984c0997b9827aa53caeb72ff3b19ab684a260ec7e5/detection

VirusTotal

http://coronavirus.zone/

5 / 79

Community Score

5 engines detected this URL

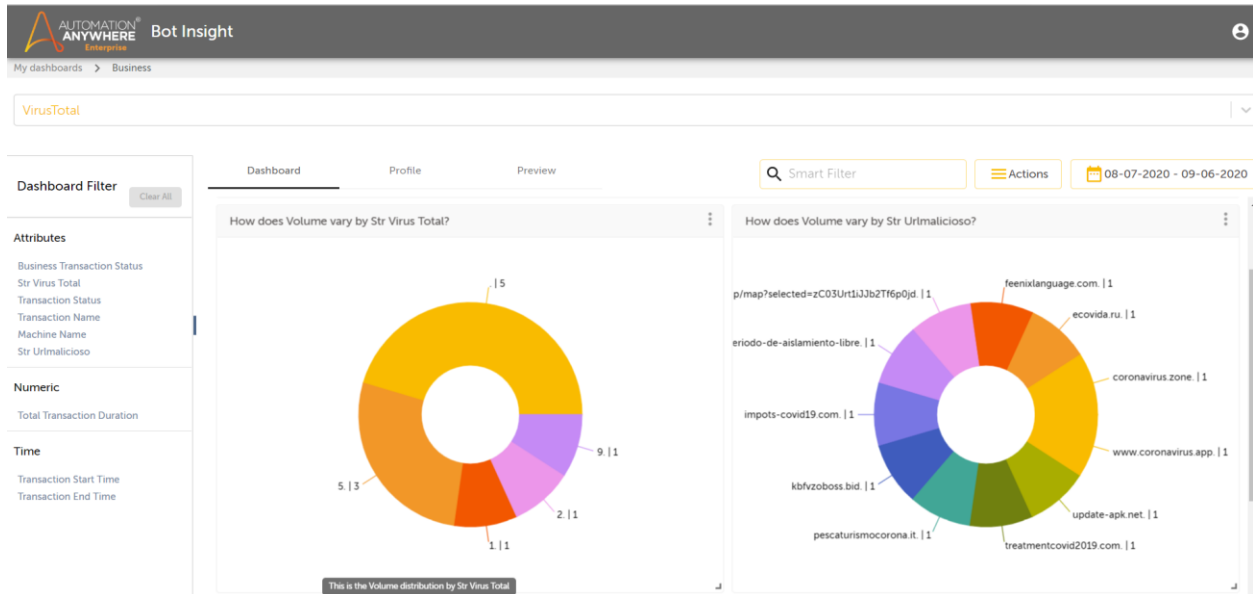
http://coronavirus.zone/ coronavirus.zone 200 Status text/html;... Content Type

DETECTION	DETAILS	LINKS	COMMUNITY
Antiy-AVL	Malicious	ESET	Malware
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
Sangfor Engine Zero	Malware	DNS8	Suspicious
Sophos AV	Suspicious	ADMINUSLabs	Clean
AegisLab WebGuard	Clean	AlienVault	Clean

Step 13. The excel output file when finish the process

A	B	C	D	E	F	G	H	I	J	K
Item	Verified URL	Reported date	Total Score	Malicious	Malware	Phishing	Suspicious	Abuse Contact Email	Abuse Contact Phone	Domain Creation Date
1	coronavirus.zone	4/16/2020	5	2	3		2	abuse@porkbun.com	1.503850835	2020-01-24T16:12:33Z
2	ecovida.ru	4/16/2020	5	1		4				
3	feenixlanguage.com	4/16/2020	9	6		3	1		91.1204989	2009-09-14T10:58:08Z
4										
5										

Step 14. The Insight output



End of user guide

4. Support & FAQs

4.1 Support

Free bots are not officially supported. You can get access to Community Support through the following channels:

- You can get access to Community Support, connecting with other Automation Anywhere customers and developers on [APeople](#) – the [Bot Building Forum](#), the [Bot Store Support Forum](#), or the [Developers Everywhere Group](#).
- Automation Anywhere also provides a [Product Documentation portal](#) which can be accessed for more information about our products and guidance on [Enterprise A2019](#).

4.2 FAQs

Instructions: Add any Frequently Asked Questions related to Bot that you think would be helpful to the customer

For questions relating to Enterprise A2019: See the [Enterprise A2019 FAQs](#).

Appendix A: Record of Changes

Instructions: Provide information on the version number, the date of the version, the author/owner of the version, and a brief description of the reason for creating the revised version.

No.	Version Number	Date of Change	Author	Notes
1	1.0	August 7, 2020	Armando Carvajal	Public in Bot store Whois wrapper support

Appendix B: References

No.	Topic	Reference Link
1	Overview of Enterprise A2019	Click here
2	Guidance: Building basic A2019 bots	Click here
3	Guidance: Building A2019 action packages	Click here
4	APeople Community Forum	Click here
5	Automation Anywhere University	Click here