



Spacenet 0.0.1 User's Guide

December 21 , 2017

© Spaceb4r - © SPB Spaceb4r Production for Cyber Weapons Development



Table of Contents

1 Overview.....	5
2 Pre-Deployment.....	8
2.1 Python.....	9
2.2 Server Configuration.....	9
2.3 Database Initialization.....	9
3 Deployment.....	10
3.1 Starting The C&C.....	10
3.2 C&C Execution.....	10
4 Web Interface.....	10
4.1 Password Creation.....	10
4.2 Overview.....	11
4.3 Zombie List.....	11
4.3.1 Multiple Command Execution.....	12
4.3.2 Remove Bots.....	12
4.4 Database.....	12
4.5 Bot Page.....	13
4.5.1 Remote Shell Commands.....	13
4.5.2 Zombie Resources.....	14
4.5.2.1 Grabbed Forms.....	14
4.5.2.2 Chrome Data.....	14
4.5.2.3 Keylogger Results.....	14
5 The Agent.....	15
5.1 Pre-Build Settings.....	15
6 Spacenet Agent Builder V0.0.1.....	16
7 Troubleshooting.....	18
8 For Further Assistance.....	18

Table Of Changes

Date	Change Description	Authority
21/12/2017	Created Project	SPB
29/12/2017	Modified Doc	SPB



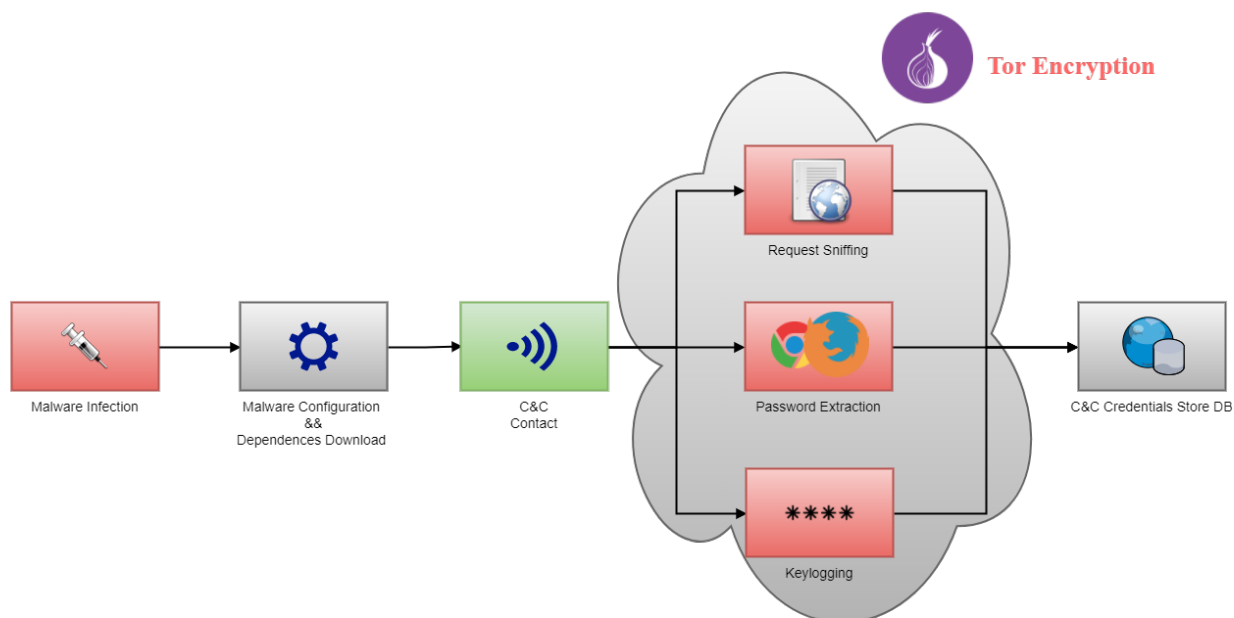
Spaceb4r Production
for Cyber Weapons Development

1 Overview

Spacenet is a multi-client Command & Control (C&C) server , meant for remote credential stealing . It has different functions but the primaries are : interactive shell and password extraction. By design , the extraction includes different tools that make easier catch all the browser password that the victim types.

The server is meant to be completely untrackable, it has been built to work next to Tor software to guarantee a hidden connection. The main workflow about the networking is represented by the image below:

SPACENET FLOW CHART



The web interface allows to administrate every side of the botnet , including an internal database to consult all the password received by the C&C server.

Spacenet guarantees a clear running under the following operating systems and processor architecture . The tables below reference to the use of both parts of the the project : C&C , Agent.

Agent		
Currently Supported Platforms	Lastest Available Version	
	Tested	Untested
Windows10 x64	Beta	
Windows10 x64	0.0.1	
Windows7 x64	0.0.1	
Windows(*) x64		0.0.1




C&C Server		
Currently Supported Platforms	Lastest Available Version	
	Tested	Untested
Kali Linux x64	0.0.1	
Ubuntu 14.04 x64	0.0.1	
(*) Linux x64		0.0.1




(*) : All Linux distro.

NOTE : Spacenet has been created to run under Linux x64 and under Windows environment all the server properties could not work correctly . It's highly recommended to start the C&C under Linux x64 environment and in case accessing to the web interface from Windows browser .

The Spacenet release consists of the following files .

Python Scripts (.py)	
Filename	Function
chart.py	Generates 2 temporary files for the world image generator.
db_init.py	Creates the database to handle bots data : main.db .
log.py	Module containing routine to write logs to file and printing them out.
makedir.py	Simple addictional module to create a new directory.
runner.py	Generates world map by country bot density.
server.py	Main script to start the C&C and all relative functions.
sort.py	Finds and delete the oldest screenshot received for bot

	in case of maximum store screens reached.
Resources and Folders	
html <DIR>	This folder contains all the html files used by Spacenet for the Web Gui.
	
Account.html	On this page user can view all the access data of the admin and can modify the password for the Web Gui.
AdminPasswordSet.html	Notifies the new password has been set successfully.
Bot.html	To work on a single bot and consulting all the single payload results.
Cache.html	To view all the grabbed HTTP forms.
Chrome.html	From here user can access to : Keywords searched, History, Autofill fields.
CreatePassword.html	Landing page for the first web interface use, here the final user has to set the admin password.
DbPass.html	Database of stored passwords, provided with filters and research bars.
Disconnect.html	After the logout the final user will be redirected to this page .
error.html	In case of 'error 500 : Internal Server Error' will be generated this temporary page to redirect the user.
Info.html	In this page will be reported all the bot machine info.
Keylog.html	To view all the keystrokes stored.
List.html	Here there's the complete list of the bots stored.
Login.html	Landing page to access to the web interface.
LoginEr.html	Redirecting from Login.html in case of wrong password.
Overview.html	This is the heart of the C&C server , here's the world map with the density of the bots for country and from here user can access to all Spacenet main functions.
OsSummary.html	All infected operative systems will be reported on this page.
Timeout.html	After the idle timeout by the final user, the session will be closed and the user needs to login again.
conf <DIR>	Here are defined the static dirs and sockets settings for the C&C server and the web interface, there's also the requirements.txt file necessary for the dependeces installation.
 server.conf requirements.txt	
DumpDir <DIR>	Here is stored all the data taken from the bots : Passwords , etc. All sorted by folder and IPs.
 ...	

logs <DIR>	Write to Logs/SpacenetLog-[time].txt at every action performed.
 Log.py ...	All logs files are stored in this folder.
Static <DIR>	flags <DIR> images <DIR> Inside these two subfolders there are all the images used for the web interface.
 ...	
TempDir <DIR>	This is the temporary directory , here Spacenet stores some tmp files necessary for some internal functions.
 ...	

NOTE: It's recommended to not remove any of these files , because Spacenet is optimized to automatically delete unnecessary resources.

2 Pre-Deployment

Before the initial deployment , Tor software must be downloaded and installed on the operative system. To install Tor on the Linux machine, the user can follow the instructions below:

```
sudo apt-get install Tor
```

Modify the `torrc` file inside the folder `Browser/TorBrowser/Data/Tor/` or if Tor has been used without TorBrowser the file will be located inside `/usr/local/etc/tor/torrc` or `/etc/tor/torrc` or `/etc/torrc`; in the middle section of the file there's a line including the following text :

```
##### This section is just for location-hidden services ###
```

This section consists of groups of lines, each representing one onion service. By default all the lines are commented out (the line starts with '#') , so onion services are disabled. Each group of lines consists of one *HiddenServiceDir* line, and one more *HiddenServicePort* lines .

Add the following lines to the `torrc` , modifying the ip below with the LAN ip of the user machine (eg. 192.168.1.254) :

```
HiddenServiceDir /Library/Tor/var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:8080
```

Save this file to perform the changes , now Tor is ready to start the onion service . Once Tor starts it will automatically create the *HiddenServiceDir* specified and it will create two files there : `private_key` , `hostname` . Inside the *hostname* file Spacenet

will read the onion hostname and that will become the address to connect to access to the web interface .

NOTE : *It's recommended downlading the Tor Browser to test immediatly the correct server working. For more informations about Tor configuration there's the doc on the official website project (<https://www.torproject.org/docs/tor-onion-service.html.en>)*

2.1 Python

Spacenet is a software Python based, on the most of Linux x64 distro Python is pre-installed on the system , if it's not is necessary to download it from the official website : <https://www.python.org/downloads/> and get the version 2.7 .

Once Python has been set successfully on the server must be installed the requirements via `pip`; inside the main folder in `conf` subfolder there's the file `requirements.txt` , running it via console with the following command will install all dependences :

```
pip install -r requirements.txt
```

NOTE : *If some libraries missing there are the official python dependeces and they need to be installed manually .*

2.2 Server Configuration

Once Tor is successfully set, it must be necessary edited the configuration file of Spacenet . This is located inside the main folder of the software with the path `conf/server.conf` . The only lines in the file that have to be modified are the following:

```
server.socket_host: '127.0.0.1'  
server.socket_port: 8080
```

The user needs to edit these lines with the relative Ip address and the listener port and save it.

NOTE : *The best solution is to set a lan Ip address of the machine and proceed with the port forwarding on the main gateway of the implant server .*

2.3 Database Initialization

Spacenet needs to store all bot informations inside the `main.db` file database and it must be generated running the Python script `db_init.py` inside the main folder of the application.

3 Deployment

3.1 Starting The C&C

To access to the C&C administration the main script needs to be started. The main workflow is easy , the console will be used as Log live handler and everything happens on the C&C will be printed out and saved under the `Log` file folder .

3.2 C&C Execution

Once Spacenet has been launched will be printed , the local address and the port where the C&C server is currently listening and the .onion hostname . The address that the software print on the console when it starts are the URL links where the web interface resides so to administration and to access the C&C must open those URLs from a web browser.

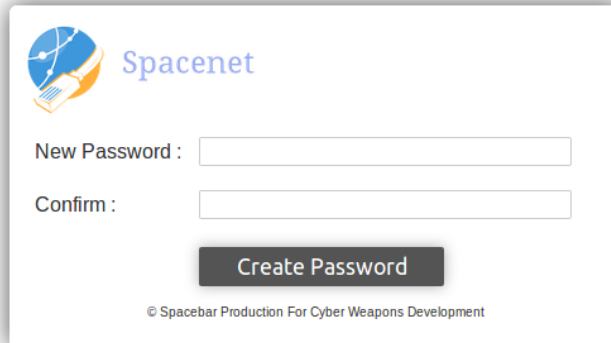
The example below is what Spacenet will print on startup :

```
[ INFO ] [ 17:31:41 ] Starting onion server on : http://example.onion:8080  
[ INFO ] [ 17:31:41 ] Starting clearnet server on : http://192.168.1.254:8080
```

4 Web Interface

4.1 Password Creation

The landing page of the web interface is the new password creation . The access to the C&C server is protected with a login form. When the new password is created it gets encrypted with `SHA256`. From inside the server it's possible changing the password . The image below shows the current style of the admin password creation page.



The image shows a web form for creating a new password. It features the Spacenet logo at the top left, which consists of a blue circle with a white network-like pattern and the word 'Spacenet' in blue. Below the logo, there are two input fields: 'New Password :' and 'Confirm :'. A dark grey button with the text 'Create Password' is positioned below the input fields. At the bottom of the form, there is a small copyright notice: '© Spacebar Production For Cyber Weapons Development'.

Once the new password has been created the user will be redirected to the login page .

NOTE: *Once the password is created it can't be recovered in anyway .*

4.2 Overview

This is the heart of the server, here the user has a complete view of all its bots divided for each country on the curtain on the right and a world map colored for density in each country.



The scale is really simple , more blue is the country more , major will be the zombie density . This page shows also all the bots stored inside the `beta_db` and all the online machines in that moment.

From here there are two ways that the user can take , the first is `viewing all zombies` and the second one is accessing to one of the pages of the `C&C` curtain on the top.

4.3 Zombie List

By clicking on "View All Zombies", Spacenet will print up all the stored bots , the main table will show each bot with the following format :

Name	Last Connection	Ip	Os	Sel.	Country
Desktop-test	Sun Dec 3 19:25:49 2017	192.168.0.1	Windows 10	<input type="checkbox"/>	[FLAG]
...	<input type="checkbox"/>	...

The `Name` for the bot will be represented by the computer hostname (*this option can be customized into the settings file*) and from here it's possible to access to a remote shell and operating in detail with the bot selected.

`Last Connection` show , if the bot is offline , the last time online or it will print out `Online` .

The `Ip` shows the Ip source of the bot connection .

The `Os` prints the Operative System that the bot is running .

The `Sel.` Is just a checkbox that will be used for the `Run On Selection` command.

Under `Country` will be displayed a little flag of the country where the bot is located.

4.3.1 Multiple Command Execution

In the main window of the List page, there's one of the most useful features of the botnet, the chance to forward a command to multiple bots; this can be done by typing the choosen command inside the textbox after the `Run Command On Selection` : and clicking `Send` .The command will be forwarded to all the bot with the checkbox under the table voice `Sel.` Checked . At least must be selected one bot to forward correctly the command.

4.3.2 Remove Bots

One of the most useful feature in a botnet is the multiple agent remove, with this function the user can select the bots from the *bot list page* and click on `Remove Selected Bots` to uninstall the Agent from the relative infected machine. To re-integrate the removed bots the server must be restarted.

4.4 Database

All the credentials and password stolen from all the bots are saved automatically under the main folder `DumpDir/` , the passwords are classified by IP while the other data such as : sniffed authentications , Chrome Data , etc.. are sorted by folder renamed with the `bot Name` . Using this page is easier to consult all the stored password , furthermore is possible filtering them by more options : `Keyword` , `Ip` , `Chrome Passwords` , `Firefox Passwords` , `PayPal` , and `Facebook` . These are the pre-made filters and selecting one of them and by clicking `Go` , Spacenet will search in all password files stored, the word to filter. The same mechanism can be applied by

sorting the passwords by `Keyword` or `Ip`, the only change is that the user needs to click on the relative `Send` button.

Under the window `Matches` , Spacenet will print out the result of the query, otherwise if there are not passwords stored or the filter doesn't return any result , it will be displayed `No Results` .

4.5 Bot Page

The main function of the single bot page is the reverse shell on that specific machine. Typing the command and clicking `Send`, the command will be executed on the remote zombie. In the bigger textbox will be showed the result of each command executed . The syntax of the command that's being executed is the following :

```
> command [PENDING...]
```

The `[PENDING...]` syntax means that the command has been sent to the client and it's going to be executed as soon possible. The commands can be forwarded to the bot even if the remote machine is currently offline , the execution will be performed on the bot start up, until that moment the `[PENDING...]` status will persist.

4.5.1 Remote Shell Commands

The reverse shell offers a multipart solution for the best remote command forwarding and the control of the botnet features. All the commands are shown in the following table :

Command Name	Arguments	Description
persistence	install	Install a Key inside the registry of the machine to start the agent on every reboot .
	remove	Remove the Key from the registry to avoid the start of the Agent on every reboot.
	status	Check the Persistence status inside the remote machine, the results are the following : Persistence is ON Persistence is OFF
chrome		Extract all Chrome password stored and send them to the C&C.
firefox		Extract all Firefox password stored and send them to the C&C.
keylogger	start	Starts a daemon hidden keylogger to capture every key pressed.
	update	Send all the stored keys to the C&C.
(*) By default the		

keylogger sends randomly all the stored keys to the C&C.		
--	--	--

4.5.2 Zombie Resources

Inside this window there are more action pages for the complete monitoring of the single bot .

4.5.2.1 Grabbed Forms

The Spacenet Agent is provided with an integrated HTTP sniffer, this routine intercepts all the Authentication Requests and sends them to the C&C everytime a new authentication is grabbed.

Every captured request will be displayed in this window following the table below :

Request Type:	POST
Host Website:	Www.example.com
User Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) ...
Language:	en-EN
Hour:	11/11/17 20:34:22
Cookie:	__utmt=1; ipb-session_id=7dcbda ...
Payload-Credentials:	auth_key=...%username=test... %password=tst

4.5.2.2 Chrome Data

The agent is programmed to extract all the : History, Searched Words, Autocomplete Fields, from Chrome browser of the victim . If the cache of the target browser is not cleaned often recovering this data may take some minutes moreover if Spacenet is working on onion extension. After recovering, all data will be displayed in this window splitted up in 3 sub windows.

NOTE: Spacenet to avoid user browser crash will print all the data for a maxium lenght of 1k lines. The complete file will be saved under `DumpDir/<botid>/AFC.txt, .../HIC.txt, .../KRC.txt` .

4.5.2.3 Keylogger Results

If Spacenet has received from the bot Agent the keystrokes they will be displayed in this window, otherwise it will print out No Keystrokes Found. All the keystrokes are saved under `DumpDir/<botid>/Keystrokes.txt` .

5 The Agent

Spacenet is released with the integrated Agent that in this case represent the main malware . The best definition of the Agent is Trojan Horse Botnet Agent; this software has been created to gain the complete access to a remote machine .

This section of the project includes a collection of source codes necessary to build the .exe final virus; the collection of the agent codes is various and contains every file to guarantee the correct working of the software.

5.1 Pre-Build Settings

Inside the main folder of the Agent there's a file named as `settings.py`, this file contains all the agent network and routines settings :

Setting Name	Function
SERVER_URL	Defines the URL the Agent needs to connect to.In a common case it's the C&C server URL. Is necessary to specify the port into the url string, using the following format "http://server-url:port"
PROXY_TOR_IP	By default the Agent connects to the local proxy Tor proxy if installed . In this setting must be declared the IP of the proxy.
PROXY_TOR_PORT	Following the IP configuration here must be reported the port of the Tor proxy.
BOT_ID	On the first connection to the C&C, the Agent will set this argument with the target machine hostname but it can be customized for a specific target.
AUTO_PASSWORD_SENDER	On the startup, the Agent will check this function and if it's set on <code>True</code> , then automatically will extract and send all password stored from <i>Google Chrome</i> and <i>Mozilla Firefox</i> to the C&C.
AUTO_GET_SNIFFER	On the startup, the Agent will check this function and if it's set on <code>True</code> , then automatically the sniffer authentication will launched.
AUTO_KEYLOGGER	On the startup, the Agent will check this function and if it's set on <code>True</code> , then automatically will start the daemon hidden keylogger.
DEBUG	This function has been meant for the development of the Agent, if it's set on

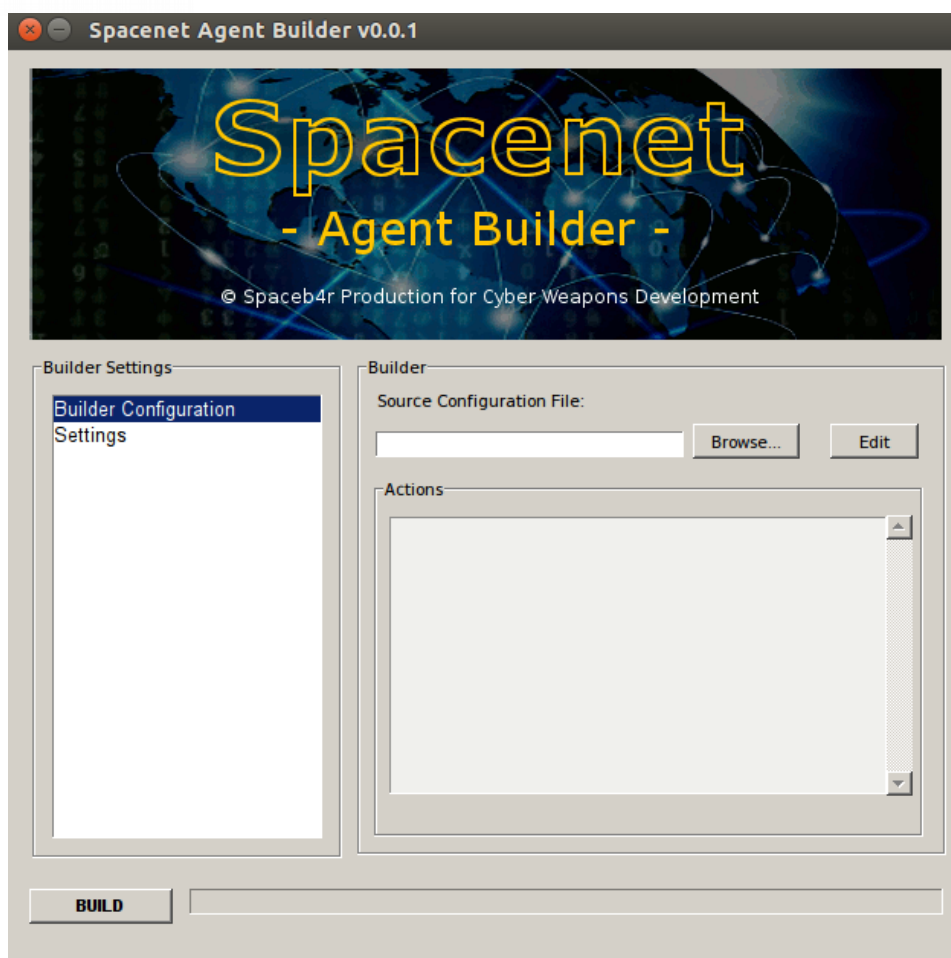
	<code>True</code> then all the debug print functions will be showed in a console.
IDLE_TIME	This is a timer kind setting, if the victim keeps in idle for more than the time set then the connection will automatically drop.
REQUEST_INTERVAL	Between each command executed from the C&C there's a delay time that can be changed. It's recommended leave this parameter as default.
PAUSE_AT_START	On the Agent startup there's a little delay of time specified in this settings. It's recommended leave this parameter as default.
AUTO_PERSIST	On the startup, the Agent will check this function and if it's set on <code>True</code> , then it will automatically add a rkey into the Windows registry of the victim machine to launch the Agent on every reboot.

Once all the settings are been confirmed and saved, now the Agent is ready to be compiled into .exe file.

6 Spacenet Agent Builder V0.0.1

For this step is necessary to have installed on a Windows or Linux machine the python library `pyinstaller`.

Spacenet is provided with an Agent Builder Program that can be used to generate a .exe file ready to be distributed.



The workflow of the builder is not hard, the first thing to do is to load the `settings.py` file of the agent, better is if already configured or when loaded the user can edit it by clicking on `Edit` . If the settings file is successfully loaded the server will return an OK message in the Action Logs listbox; now it's possible to change the settings of the malware under the Tab Settings :

In the following table it's explained the complete function of the Builder Settings Tab.

Setting Name	Function
CONVERT TO ONE FILE	By checking this option, the Agent will be compressed in one single file.
WINDOWED MODE	By checking this option, the Agent will be provided with a console starting windowed.
HIDE CONSOLE	By checking this option, the Agent console provided will be hidden.

DEBUG EXE	By checking this option, the console will be visible and all error messages will be printed.
ICO FILE	By clicking on the "Browse" button the user can choose a custom icon for the malware.
OUTPUT FOLDER	By clicking on the "Browse" button the user can choose a custom path to get the agent.exe file.
EXE FILE NAME	Here is possible to change the output agent.exe filename.
Build Dropper	By checking this option, the Builder will generate the dropper file too.
Build Agent	By clicking on this button the agent will be created .

NOTE: *Spacenet agent needs Tor to connect to the C&C , so before starting the main workflow, the agent will try to launch tor browser from the folder location created by the dropper. Anyway the user can create its own dropper but a tor thread has to be run. One technique to launch Tor in hidden mode is reported below :*

- *Copy the file "torrc.default" from "\Tor Browser\Browser\TorBrowser\Data\Tor" to "\Tor Browser\Browser\TorBrowser\Tor".*
- *From the last folder launch the command 'tor.exe --defaults-torrc \torrc.default'*

So a Tor proxy will be started on localhost : 9050 . The best to do is to compress a copy of Tor bundle and use a dropper to decompress it on the victim machine. For more info the user can take a look to the dropper.py file .

7 Troubleshooting

The agent is programmed to try the connection to the C&C server until it gets connected, if for some reason the agent is closed or whatever, the connection will be reset on the next machine reboot. It's possible to reinitialize the main, be careful that this will bring to the lost of all stored bots, but Spacenet can be reused more times.

8 For Further Assistance

For any additional assistance , please consult one of the Spacenet developers. For bug or errors please report them one of Spacenet developers, as soon possible the new version of the software will be released free for who bought it.