

ZLAB

Malware Analysis Report: Wonder Botnet



Cyber Security Strategists

Malware Analysts:

Antonio Pirozzi
Antonio Farina
Luigi Martire



CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

14/09/17

Table of Contents

Introduction	3
Basic static Analysis	4
Downloader	4
Payload/Bot.....	4
Behavioural Analysis.....	5
Advanced analysis	7
Evasion Techniques	7
Malware's control flow	8
Bot ID creation	10
Commands List.....	11
Kill Switch	12
Yara Rules.....	12



CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Introduction

Surfing the darknet, we found a forum in which some users shares many cracked software each other. One of these software promises to generate Premium Account for Netflix services for free. So we decided to analyze it. With our surprise, we discovered that it is a malware (without generating any Netflix account, unfortunately).

This malware is not indexed yet: only one site on the Clearnet takes track of it and it was uploaded for the first time around September 20th, probably by the author in order to test its stealthy. Studying the malware, we realized that it is a bot that belongs to an alive botnet. We were able to estimate the size of the botnet analyzing the number of visits to the Pastebin page that contains the payload. In fact, the malware is composed by a first part, which is a downloader for a second part, which is a real bot, just uploaded on Pastebin.

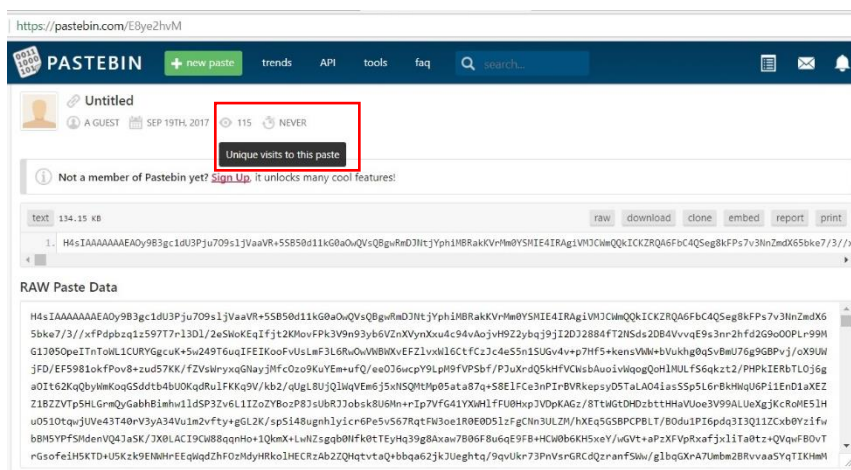


Figure 1 - Number of visits on Pastebin page

There is no existing report, obviously, about this sample. So, we need to analyze in deep the malware to understand its complete behavior.



CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Basic static Analysis

Downloader

Filename: wonder.exe

MD5	486954967e02a2e1577bd7dd91026102
SHA-1	27b2fc98c91dddf002cda77da3f44cf9a05d7fba
SHA-256	c3f5f5bfe39b55ffe0343950e0a4bf0433c35679a01daf07ce6c0ccc7d4da9b7
File size	365 KB

Table 1 - Generic Info about Wonder Downloader

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	8192	356430	356864	6.36	333d1fa80982740c38c328758a25a0fc
.sdata	368640	744	1024	0	0f343b0931126a20f133d67c2b018a3b
.rsrc	376832	14836	14848	3.54	7efbba2830bd6c256834d59b603c3827
.reloc	393216	12	512	0.1	3ab6459b0ec4dbdfcacb9dcb539ef38d

Table 2 - Info about Wonder Downloader's Sections

Payload/Bot

Filename: payload.exe

MD5	84fdbcb1f23f592543381c85527c19aaa
SHA-1	cc2f96a2f4dbc4b0176bab37c22a48ebfe1bac06
SHA-256	15d390626fea8d06adc261e0588ec40d17b6a62a2320313073ba94809c5e0f4d
File size	205 KB

Table 3 - Generic Info about Wonder Bot



CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	8192	206549	206848	6.24	2d1cfb1bcee6b60316b0c9fc2bee80bd
.rsrc	221184	1566	2048	3.45	74f34801399fa96d53ef643d453214bb
.reloc	229376	12	512	0.1	4cbddac565068df73961e06ff96179f5

Table 4 - Info about Wonder Bot's Sections

Using some static analysis tools, such as PEiD, we discovered that the malware is based on .NET Framework and it is written in C#.

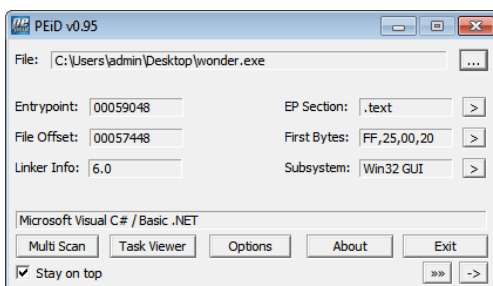


Figure 2 - PEiD view

Behavioral Analysis

The infection starts with the execution of the “wonder.exe” file, which is the downloader of the effective payload. The downloader tries to connect to “pastebin.com” in order to retrieve the encoded payload. Otherwise, if there isn’t internet connection, the file “wonder.exe” crashes with the following screen.

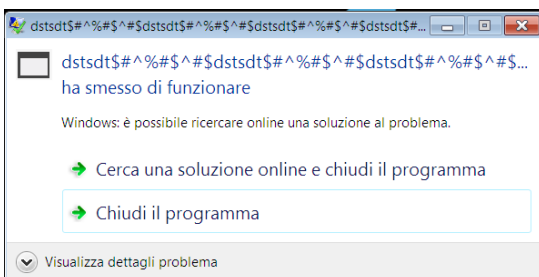


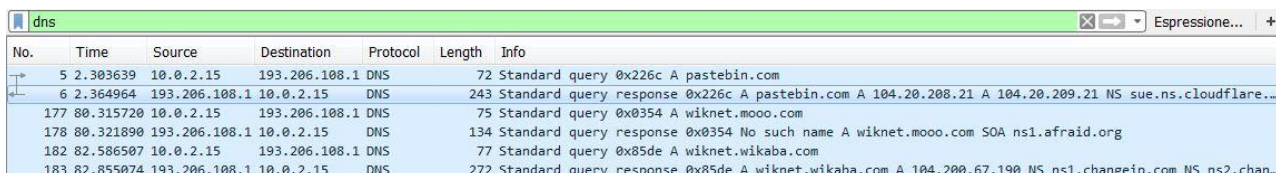
Figure 3 - Wonder crash screen



CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

In a standard condition, in which the internet connection is up, the downloader retrieves from “https://pastebin.com/raw/E8ye2hvM” the bot payload to execute.

When the payload starts, in the first time it tries in vain to resolve the domain “**wiknet.mooco.com**” because it’s not registered. Successively, it resolves “**wiknet.wikaba.com**” to the IP “**104.200.67.190**”.



No.	Time	Source	Destination	Protocol	Length	Info
5	2.303639	10.0.2.15	193.206.108.1	DNS	72	Standard query 0x226c A pastebin.com
6	2.364964	193.206.108.1	10.0.2.15	DNS	243	Standard query response 0x226c A pastebin.com A 104.20.208.21 A 104.20.209.21 NS sue.ns.cloudflare.com
177	80.315720	10.0.2.15	193.206.108.1	DNS	75	Standard query 0x0354 A wiknet.mooco.com
178	80.321890	193.206.108.1	10.0.2.15	DNS	134	Standard query response 0x0354 No such name A wiknet.mooco.com SOA ns1.afraid.org
182	82.586507	10.0.2.15	193.206.108.1	DNS	77	Standard query 0x85de A wiknet.wikaba.com
183	82.855074	193.206.108.1	10.0.2.15	DNS	272	Standard query response 0x85de A wiknet.wikaba.com A 104.200.67.190 NS ns1.changeip.com NS ns2.chan...

Figure 4 - DNS traffic of the malware

Accessing to this site using a browser, we have the following screen:

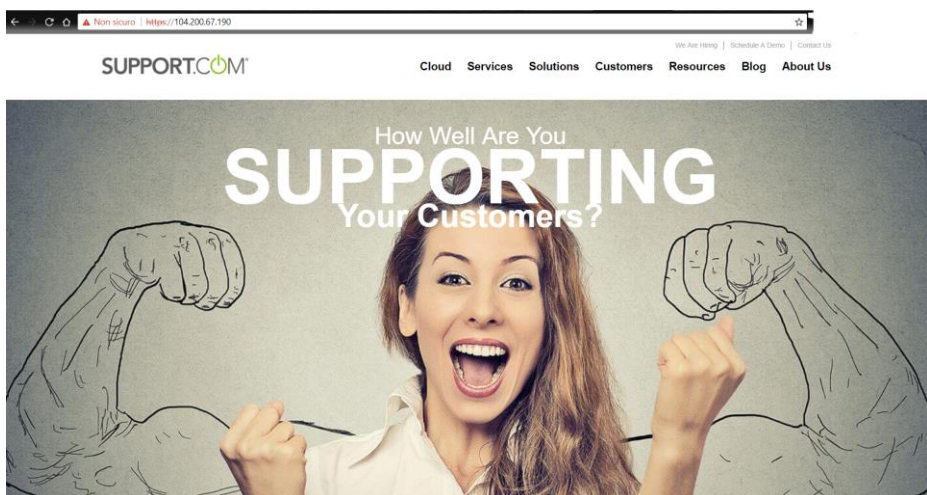


Figure 5 - Fake site screen

This is a fake page of another existing site, “www.support.com”, which has the same front-end page. The interesting thing about the fake page is that every link on it refers to the original page: so, if we click on one link of them, we are redirected on the corresponding page on “support.com”.

At this point, the only reasonable hypothesis is that this IP refers to a Command and Control.

From the point of view of the behavioral analysis, the only suspicious activities found are:

- The DNS requests showed in Figure 3.
- The creation of a file in “AppData/Local/Temp” path, probably used as support for the bot actions.
- The persistence mechanism, adding to “C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup” a link to itself.

All the traffic between the bot and the C2C is on TLSv1 layer, so we can’t see.



CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Advanced analysis

Using specific tools to analyse .NET applications, we deobfuscated and decompiled the bot and we found much more information about it.

Evasion Techniques

As all the sophisticated malwares, it applies some evasion techniques in order to avoid the detection and the analysis:

```
if (File.Exists(Environment.GetFolderPath(Environment.SpecialFolder.System) + "\\vmGuestLib.dll"))
{
    Application.Run(new Form0());
    Environment.Exit(1);
}
else if (File.Exists(Environment.GetEnvironmentVariable("windir") + "\\vmbusres.dll"))
{
    Application.Run(new Form0());
    Environment.Exit(1);
}
```

Figure 6 - Searching of VBox libraries

In the Figure 5 we can see that the malware searches for some specific **virtualization software** libraries, such as “vmGuestLib.dll” and “vmbusres.dll”, in order to realize that it is in a virtual environment and do not show its malicious behavior. In fact, if its conditions are verified, it can kill itself or show the following windows:



CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

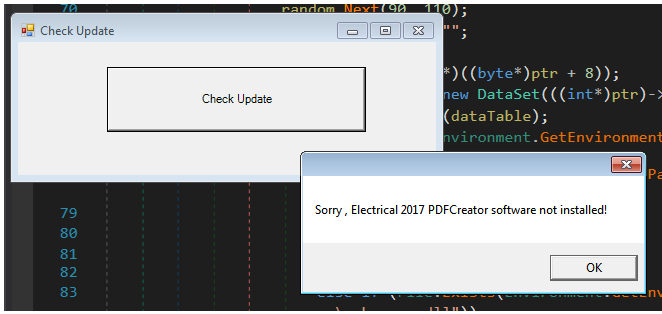


Figure 7 - Evasion technique

Malware's control flow

With our advanced techniques, we extracted the complete working scheme of the malware.



CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

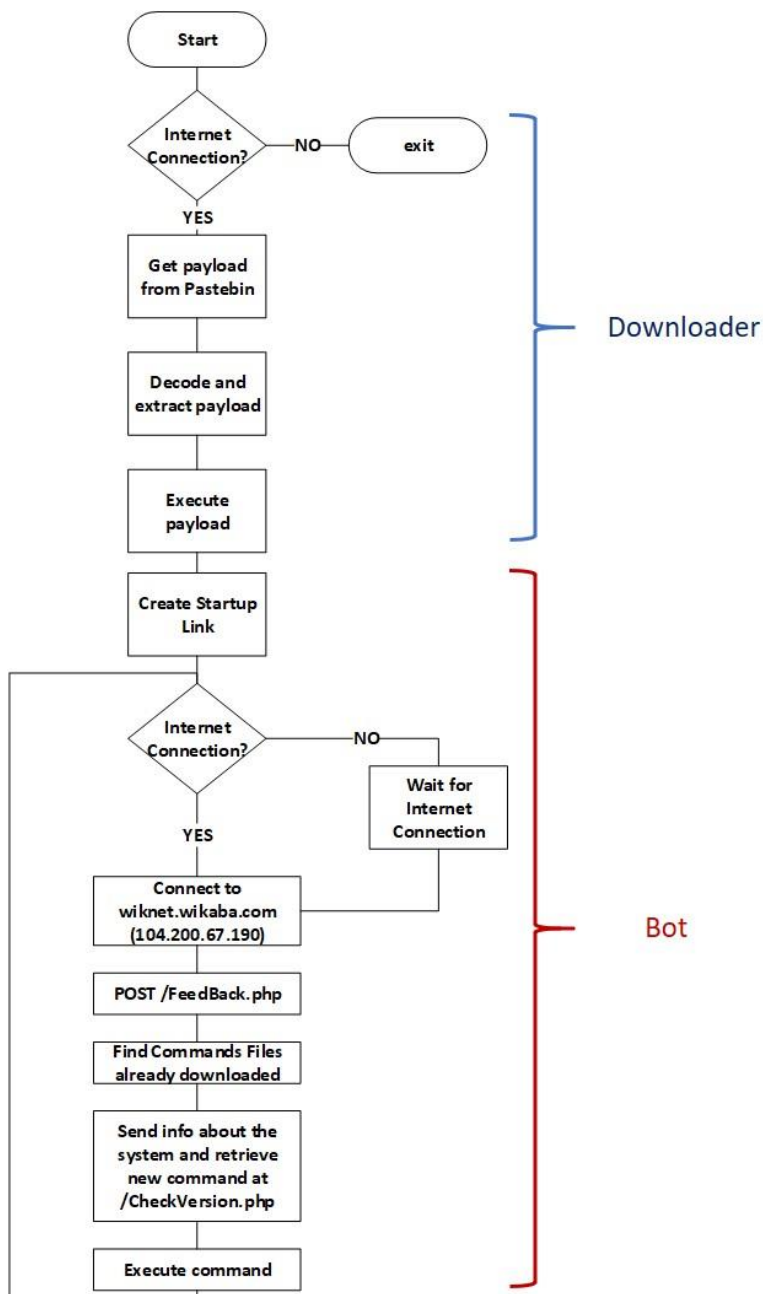


Figure 8 - Complete scheme of the malware's behavior

As above mentioned, the malware's logic can be divided in two parts: downloader logic and bot logic.

Downloader Logic:

- *Check Internet connection:* the first stage is control whether the connection is present. If it isn't the malware kill itself.
- *Download the payload from "pastebin.com/raw/E8ye2hvM":* the payload is codified in Base64 and it is encapsulated into a GZ archive.



CSE CyberSec Enterprise SPA
 Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
 Email: info@csecybsec.com
 Website: www.csecybsec.com

```
pastebin.com/raw/E8ye2hvM
H4sIAAAAAAAEAOy9B3gc1du3Pju709s1jVaaVr+5S5B0d11kG0a0wQVs0BgwrM0JNtjYphiMBRakKvRmM0YSMIE4IRAgIvHJ3CwmQkICZKZRA6FbC4Q5eg8kFPs7v3NnZmdX65bke7/3//xFPdpbzq1z597T7r13D1/2e5WoKEqI fjt2KMo
vH9Z2ybgj9jI2Dj2884fT2N5ds2DB4VvVqE9s3nr2Hfd269o00PLr99M61J050pe1TnTowl1CURYGcuk+5w249T6uqIFE1KooFvUsLmf3L6Rw0wVNBWvEFZ1vxw16CtfczJc4e55n1SUGv4v+p7Hf5+kensVWw+bVukhg0q5vBmU76g9G
57KK/FZVsWryxqGlayjHfC0zo9kuYEm+uTq/ee0JwcpY9LpM9Fp58f/PJuxrd05KHfVcwsbAu0iVWgog0e1JULF56qkzt2/PHPKERbLLOJ6ga0Ie62KqQbyWmKog5ddt4BUOKqRulFKKq9V/kbZ/qUGL8UjQ1hqvEm6j5xh5QhtH
5TALAO4ias5Sp5LeRbKHmqu6P11End1AXEZZ1BZZ1Tp5HLGrm0yGabh8imhw11d5P3Zv611IZoZVBozP83UbrJJobsk8U6In+Tp7VfG41YXmH1FFU0hxpJDPpKAGz/8TtwkGDHdztHHaUoe3v99ALUeXgJKcRoHE51Hu0510tqwJUV
Si48ugnhyicr6P5v567RqtFh3oe1R0E051zFgCln3UL2M/hXEq5G58BPCLT/B0du1PI6pdq3I3Q11ZCxb0YziFwbM5YF5MdenVQ4JaSk/JX0LAC19Cw88qanHo+1QkmX+LwNzsgb0Mfk0tTEyHq3988Aaw7866F8u6E9FB+HCW
a0tz+QqwFB0vTr6sofeih5KTD+u5Kzk9ENHrEEqWqdzHFOzMDyHRko1HECRzAb2ZQhvtQ+bbqa62jkJueghtq/9qvUkr+73PnVsrGRcdQzranf5hw/g1bqGx-A7Umb2BRvvaSYqTIKHmMMDx1E7P+117i00TMRglcLSWv5MGj2qt
50VnAs5ve4nqVv1Dt8pRGIw7BcebDrBrOPImXU2rTpFBDRoyDyVn117xvJmvmZ1G2IRXQnchZnDR2R219u+7QX/ey81tnU0YGemorObtt4KhH#Mayx+A9mZjjGLW5ahzHabQinJ2fi6AJ1+rKX7NH2gbcZ6o+fmAx2V1UwNuFzR1qdi
v5W0zkt6MS1tkon5QTPCnz788Y08TxfHS1vzzEskQLY5jbnx+akC59JDIYQzTh5HjHTz8R9H2sP5ast359p1CdbzBEXzIzspYZ2LXqXy56hec27313vVfILyTAz9BKNe1T8X0av01KGNq+PzPkJNEH73BVyUfyqkPXDzVQB8cRYVPTN
cht62vd1gnUqC7bSrrFoga3cL5/0Kv11qfpcYhu713s5ahBZ1ne5tP8nRt/hPIpudfRvdr5Rg777suUD294RjWBavcZv29NY785/CWP6URkOW301nzFifryvp/H1oJa0mns/pRwbPCo/V+PY52qq9FzWf0p7U1B8kfxUdGq90xN53axI
```

Figure 9 - Raw data of the payload

- Decode and extract the retrieved payload.
- Execute the payload: the bot is executed in the same address space of the downloader.

Bot Logic:

- Create Startup link: the persistence mechanism is implemented adding to "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup" a link to the file that contains the downloader, for two reasons:
 - The payload will be downloaded on every reboot of the machine, so the bot code could be modified by the author, who could implement new features.
 - The bot code is loaded in the downloader's memory space so it is never written on the disk of victim's machine.
- Check Internet connection: if it isn't present the bot waits for it.
- Connect first to "wiknet.mooc.com" without response. After it resolves "wiknet.wikaba.com" to the IP address "104.200.67.190".
- Send POST request to the "/FeedBack.php" path: the bot reveals its existence to the C2C sending a request with the "User-Agent" header with its own Bot_ID (which we successively deepen).
- Find commands files already downloaded: the bot searches the commands downloaded in the previous contact with C2C, which are stored in some files in the "AppData/Local/Temp" path.
- Send info about the system and retrieve new commands at "/CheckVersion.php" path: the bot sends all the info gathered about the victim machine to the C2C through a POST request at the specified path. The response contains the new command that will be execute by the bot.
- Execute the command just received.

Bot ID creation

Because of its "bot nature", once installed on the victim machine, the bot has to create an ID for identify itself into the botnet. This ID is forged encrypting some host information using MD5 algorithm and adding a static string to it.



CSE CyberSec Enterprise SPA
 Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
 Email: info@csecybsec.com
 Website: www.csecybsec.com

```

1 string ID = MD5(string.Concat(
2     Environment.MachineName,
3     Environment.UserName,
4     Environment.Version,
5     Environment.OSVersion)
6 ) + "Random";

```

Figure 10 - Bot ID creation

Commands List

The bot receives some commands from C2C. Through the advanced analysis we have reported a list of all available commands. Some commands, at this time, are not implemented yet. The list of commands is:

KEYWORD	Add all files contained in a specific folder into a rar archive
KEY	Create a file "ky" in the path. This file is a trigger to upload all info gathered to the C2C at the path "/log.php"
KEYS	Delete the "ky" file
REUPLOAD	Contact the C2C at the path "/FeedBack.php"
RESTARTME	Restart the bot
BLOCK	Create the kill switch and stop the bot
SCREEN	Take a screenshot
LAN	Create a file "LA" in the path. This file is a trigger to a feature not implemented yet.
LANS	Delete the "LA" file
USB	Create a file "us"+BOT_ID in the path. This file is a trigger to infect Removable Devices.
USBS	Delete the "us"+BOT_ID file
HD	Create a file "hd"+BOT_ID in the path. This file is a trigger to infect Hard Drives.
HDS	Delete the "hd"+BOT_ID file
SHUTDOWN	Shutdown the system
RESTART	Reboot the system
PROCANDSOFT	List all active processes and all installed softwares
DEL - TEMP	Delete all files in "AppData/Local/Temp" path
RAR	Create a RAR archive adding to it all the information gathered. The archive is sent to the C2C.
RARM	Create a RAR archive adding to it all the information gathered in that month. The archive is sent to the C2C.
RARW	Create a RAR archive adding to it all the information gathered in that week. The archive is sent to the C2C.
KILL	Kill a specific process

Table 3 - Commands List



CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

Kill Switch

The malware can be stopped by the C2C using the command "BLOCK". This command creates a new file in the "AppData/Local/Temp" path called:

"Block~" + BOT_ID

Where BOT_ID is the same string showed in Figure 9.

The file can be used also as a vaccine by the user to avoid the infection.

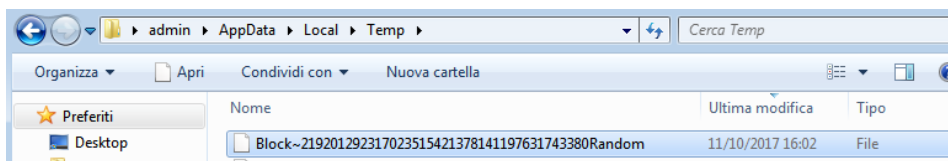


Figure 11 - Kill Switch

Yara Rules

```
import "pe"

rule Wonder_Botnet_Downloader {

    meta:
        description = "Yara Rule for Wonder Botnet Downloader identification"
        author = "CSE CybSec Enterprise - Z-Lab"
        last_updated = "2017-10-19"
        tlp = "white"
        category = "informational"

    condition:
        (
            pe.version_info["CompanyName"] contains
            "stsdt$#^%#$^#$dstsdtd$#^%#$^#$dstsdtd$#^%#$^#$dstsdtd$#^%#$^#$"
            or
            pe.version_info["Comments"] contains
            "stsdt$#^%#$^#$dstsdtd$#^%#$^#$dstsdtd$#^%#$^#$dstsdtd$#^%#$^#$"
            or
            pe.version_info["FileDescription"] contains
            "stsdt$#^%#$^#$dstsdtd$#^%#$^#$dstsdtd$#^%#$^#$dstsdtd$#^%#$^#$"
            or
            pe.version_info["LegalCopyright"] contains
            "stsdt$#^%#$^#$dstsdtd$#^%#$^#$dstsdtd$#^%#$^#$dstsdtd$#^%#$^#$"
            or
            pe.version_info["LegalTrademarks"] contains
            "stsdt$#^%#$^#$dstsdtd$#^%#$^#$dstsdtd$#^%#$^#$dstsdtd$#^%#$^#$"
            or
        )
}
```



CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com

```

        pe.version_info["ProductName"] contains
        "stsdtd$#^%#$^#dstdtd$#^%#$^#dstdtd$#^%#$^#dstdtd$#^%#$^#"
        )
    and pe.number_of_imports == 1 and pe.imports("mscoree.dll")
}

rule Wonder_Botnet_Bot {
    meta:
        description = "Yara Rule for Wonder Botnet Payload identification"
        author = "CSE CybSec Enterprise - Z-Lab"
        last_updated = "2017-10-19"
        tlp = "white"
        category = "informational"

    strings:

        // SmartAssembly Obfuscator
        $a = "SmartAssembly"

        // MD5 encryption
        $b = "MD5CryptoServiceProvider"

    condition:
        $a and $b and
        (
            pe.version_info["Comments"] contains "Folder Details"
            or
            pe.version_info["LegalCopyright"] contains "Copyright Folder"
            or
            pe.version_info["LegalTradeMarks"] contains "Folder Details"
        )
        and pe.number_of_imports == 1 and pe.imports("mscoree.dll")
}

```



CSE CyberSec Enterprise SPA
Via Giovanni Paisiello 416, Rome, Italy 00198, Italia
Email: info@csecybsec.com
Website: www.csecybsec.com