

Forum:[Hack Forums](#)

Thread: [Assistance removal of RAT/Trojan](#)

Pestik - April 3, 2024, 9:07 am

Just need guidance on full removal of RAT

Context: Partner's mum downloaded a zip file from adobe cloud with a .pdf with extension of vbs. (opening properties from the user's computer) off the top of my head and tried opening it

In addition, sent via spoof email + (hidden Microsoft word) > proof of zipped file
<https://imgur.com/a/VqKD6jF> - opened .pdf.lnk

Ran the pdf.lnk on sandbox - <https://tria.ge/240403-pw444sdf49/behavioral2> and it blue screened after 2-3mins

Results from virustotal:

<https://www.virustotal.com/gui/file/cc45b6994df0b4c0ea68f6b98548e3dbce7019e43df43790200bef925697abda/community>

User is window 11 operated.

Have/currently ran:

- Bitdefender (full system scanning atm) - <https://imgur.com/IXYRsyP>
- malware bytes (done scan + rootkit scan) - nil detected
- rkiller

Anything else that I may have missed or need to do to cleanse it completely?

Fludems - April 3, 2024, 1:12 pm

MSConfig / Task Manager - Start up processes

Registry for Start up processes

But then it could also bind to typical applications like CMD / Notepad / Chrome

I would highly recommend just reformatting and re-installing windows from fresh.

You can get persistence techniques that will make it still present past a re-installation of windows and format but the likelihood it's in use here is close to nill unless the victim is in some level of power where it's warranted.

It also might just ransomware the whole PC within a certain time frame and you might miss something and bam.

If you for some reason can't reformat and you have to manually remove, use tools like netstat to see what processes are talking to external endpoints. I'd also try and do all this offline so the 'control centre' isnt sending any commands to the device.

Py_Dev - April 3, 2024, 4:03 pm

I would use ESET nod 32 if I were you. Deep system scan.

Hello,

Thanks for all the details provided, in addition to Bitdefender I would recommend you to run the following :

- Malwarebytes : <https://www.malwarebytes.com/mwb-download/thankyou>
- Hitman Pro : <https://www.hitmanpro.com/en-us/downloads>

This is what I've found with the tria.ge report, however be aware that making a fresh install is always better :

The Bitdefender scan didn't see the following registry key entry :

Code

```
\REGISTRY\USER\S-1-5-21-566096764-1992588923-1249862864-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Hopbine204 = "%Corequisite205% -w 1  
$Brnebilletternes=(Get-ItemProperty -Path 'HKCU:\monti\').Retfrdiggres;%Corequisite205%  
($Brnebilletternes)"
```

Could you please check if the registry key is still in the registry ?

The Bitdefender scan didn't see the following files :

2 files have been downloaded by the initial "Eric Ferber.pdf.lnk" executable, the files are :
cvc1.png > renamed as and saved here : \Users\Public\Tas2s3Dsarat.pdf > which seems to be the PDF file opened in the Monitor of tria.ge
cvc2.png > renamed as and saved here : \Users\Public\Tkaour.vbs > which as been executed

Could you please check if the files are still on the computer ?

These file have been downloaded from the following domain :

Registered on Cloudflare

Spoiler ([Click to View](#))

Registrant Contact Information:

Name : N/A N/A

Organization : unknown

Address : 65 yetersr

City : atlanta

State / Province : AK

Postal Code : 45433

Country : US

Phone : +1.434444444

Fax : +0.0

Email : ritual4cash@proton.me

I'll report this domain

The Tkaour.vbs script has been obfuscated and I wasn't able to deobfuscate it, however the tria.ge report shows what actions were made by it, most of them were reading files and registry keys, but 3 were creating / editing :

Spoiler ([Click to View](#))

File Create

proc 108

path : \Device\ConDrv\\Connect

op : CreateModify

status : 0x00000000

File Create

proc : 108

path : \Device\ConDrv\\Input

op : CreateModify

status : 0x00000000

File Create

proc : 108

path : \Device\ConDrv\\Output

op : CreateModify

status : 0x00000000

These actions could be associated to establishing a remote access.

With the hash of Tkaour.vbs retrieved from tria.ge :

0183c2db2157c8b9797996d34238ca9412e781b2118205715d594b684d1aa956 :

I was able to find the following VT report :

<https://www.virustotal.com/gui/file/0183c2db2157c8b9797996d34238ca9412e781b2118205715d594b684d1aa956>

Tkaour.vbs downloaded 6 files, 5 of them seem harmless, but the .CAB file is interesting because it could be related to the \Device\ConDrv modifications.

This file given (authrootstl.cab), we can retrieve the hash :

1ed81fa8dfb6999a9fedc6e779138ffd99568992e22d300acd181a6d2c8de184 :

Taking a quick look on the web gives us a any.run report :

<https://any.run/report/1ed81fa8dfb6999a9fedc6e779138ffd99568992e22d300acd181a6d2c8de184/22db8a23-ea4a-4393-89ca-c1c52681bc4d>

Seems that this file is not a driver file, but a certificate. Could you check in the certmgr.msc if there is something named :

- authrootstl

The malware changed many settings in MSEDGE.EXE, especially related to security, I would recommend you to reset your web browser to a default state.

Binance - April 18, 2024, 6:44 pm

Bippity boppity. It's mining cryptocurrency on her property.

Burger - April 19, 2024, 8:10 am

(Apr 18, 2024 06:44 PM)Kalidrex Wrote: [\[CITE\]](#) Bippity boppity. It's mining cryptocurrency on her property.

You got me hollerin, good one pal.

Bastille - May 10, 2024, 2:14 am

(Apr 18, 2024 06:44 PM)Kalidrex Wrote: [\[CITE\]](#) Bippity boppity. It's mining cryptocurrency on her property.

Hey, curious to know what makes you think it's a miner, did you see something in the reports ?