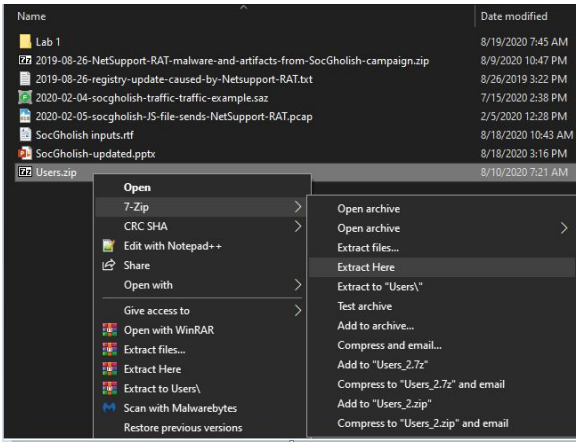
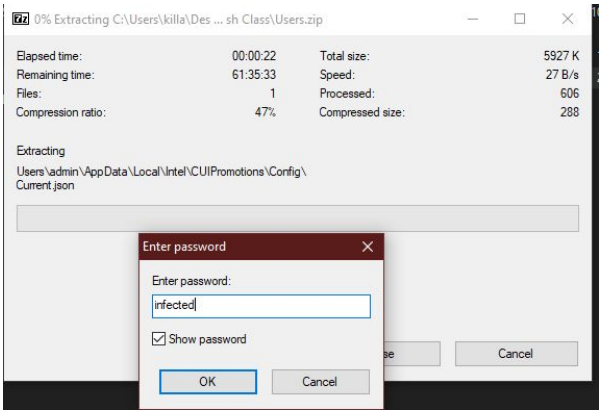
This document provides the answers/walk throughs to Lab #2 questions on slide 16 for this lesson.

Disclaimer: In this lab we will be dealing with files pulled from a computer infected with a RAT. This sample had been chosen since I was able to alter the settings of the files to render it inert. There is no risk of “infecting” yourself in this lab, but one or two of the files may be flagged by an antivirus.

Open the “Users” zip file and unzip the contents with the password “infected”



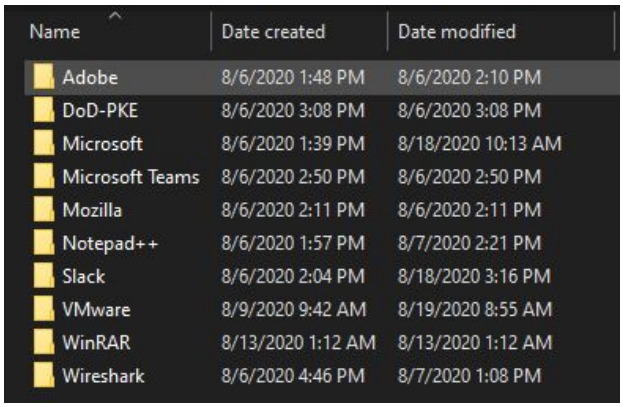


Note: The password “infected” is sort of the infosec community standard for encrypting malware samples such as this.

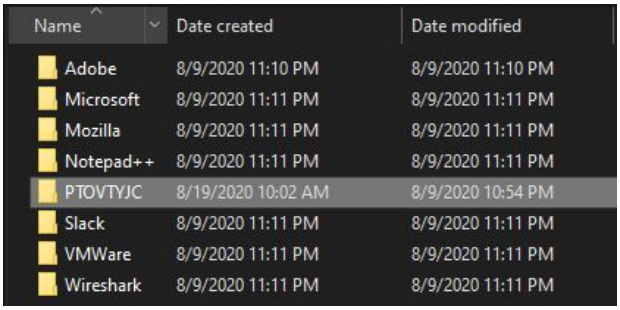
This zip file has had it's user AppData populated with some legit data, what folder stands out as suspicious?

An easy way to tell what's legitimate is to compare your system or a known good image to the host you're investigating.

A. By comparing the two roaming folders side-by-side (left non suspect, right suspect). We can see the folder "PTOVTYJC" seems suspect for a few reasons.
   a. All capital letters seems out of place from other normal folders
   b. The folder name appears to be randomly named
   c. The creation date appears to be more recent than the other folders



Name	Date created	Date modified
Adobe	8/6/2020 1:48 PM	8/6/2020 2:10 PM
DoD-PKE	8/6/2020 3:08 PM	8/6/2020 3:08 PM
Microsoft	8/6/2020 1:39 PM	8/18/2020 10:13 AM
Microsoft Teams	8/6/2020 2:50 PM	8/6/2020 2:50 PM
Mozilla	8/6/2020 2:11 PM	8/6/2020 2:11 PM
Notepad++	8/6/2020 1:57 PM	8/7/2020 2:21 PM
Slack	8/6/2020 2:04 PM	8/18/2020 3:16 PM
VMware	8/9/2020 9:42 AM	8/19/2020 8:55 AM
WinRAR	8/13/2020 1:12 AM	8/13/2020 1:12 AM
Wireshark	8/6/2020 4:46 PM	8/7/2020 1:08 PM



Name	Date created	Date modified
Adobe	8/9/2020 11:10 PM	8/9/2020 11:10 PM
Microsoft	8/9/2020 11:11 PM	8/9/2020 11:11 PM
Mozilla	8/9/2020 11:11 PM	8/9/2020 11:11 PM
Notepad++	8/9/2020 11:11 PM	8/9/2020 11:11 PM
PTOVTYJC	8/19/2020 10:02 AM	8/9/2020 10:54 PM
Slack	8/9/2020 11:11 PM	8/9/2020 11:11 PM
VMWare	8/9/2020 11:11 PM	8/9/2020 11:11 PM
Wireshark	8/9/2020 11:11 PM	8/9/2020 11:11 PM

Open the text file, "2019-08-26-registry-update-caused-by-Netsupport-RAT"

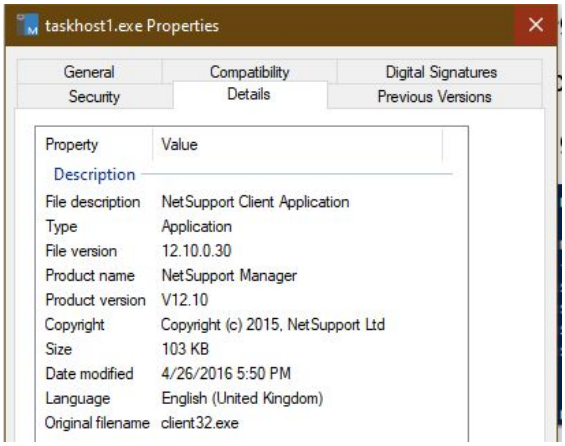
What would be the result of the malware setting this registry key?

```
Key Name:          HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Class Name:        <NO CLASS>
Last Write Time:   8/26/2019 - 7:05 PM
Value 0
  Name:            jscheck
  Type:            REG_SZ
  Data:            C:\Users\[username]\AppData\Roaming\PTOVTYJC\taskhost1.exe
```

A. The binary named "taskhost1" in the roaming folder will be run when the user logs in next.

In regards to this executable does there appear to be any deception going on?

Right click on the “taskhost1.exe” binary and open the properties section.



A. The executable from the Run key set by the malware, “taskhost1.exe” appears to not match up with it’s internal name “client32.exe” so it would appear that the malware is attempting to masquerade as a legitimate windows binary.

If we were looking at a process list on a host without considering the path, what would this process look like?

A. For the purposes of this lab, the current executable will not run but would look like the below process output.

```
PS C:\Users\IEUser\Downloads> Get-NetTCPConnection -State Established | Select-Object LocalAddress,RemoteAddress,RemotePort,State,OwningProcess


LocalAddress  : 192.168.152.128
RemoteAddress : 62.172.138.35
RemotePort    : 80
State         : Established
OwningProcess : 4284

LocalAddress  : 192.168.152.128
RemoteAddress : 52.242.211.89
RemotePort    : 443
State         : Established
OwningProcess : 2668



PS C:\Users\IEUser\Downloads> get-process -id 4284

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    379      27     5256      17640       0.16   4284   1 taskhost1


PS C:\Users\IEUser\Downloads> get-process -id 4284 | Select-Object Name,Path,Company

Name      Path                                                Company
----      ----                                                -------
taskhost1 C:\Users\IEUser\AppData\Roaming\PTOVTYJC\taskhost1.exe NetSupport Ltd


PS C:\Users\IEUser\Downloads>
```

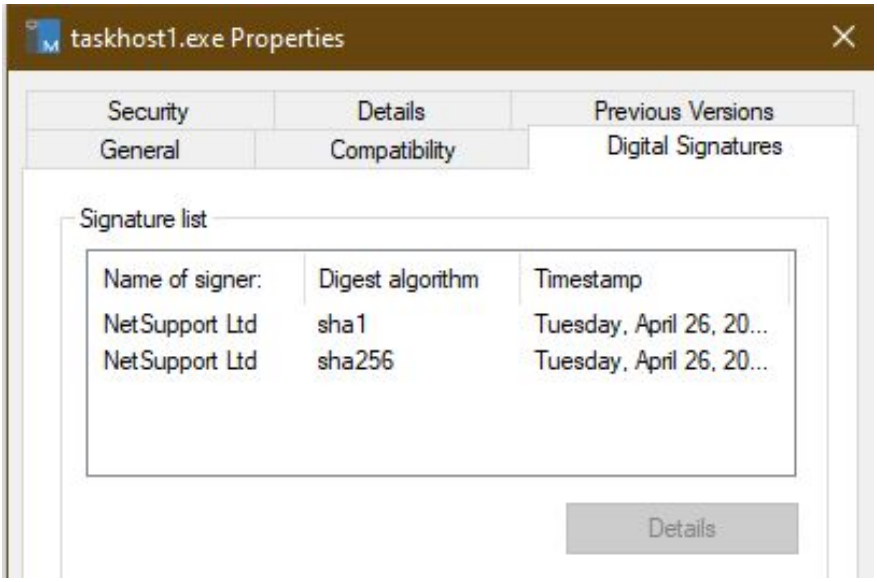
Looking at a list of executables normally on a windows host, nothing is usually named “taskhost1” but there appears to normally be a process named “taskhostw”, the RAT appears to be trying to look like this process on windows host.

```
PS C:\Users\IEUser\Downloads> Get-Process task* | select-object Name,Path,Company,StartTime

Name      Path                                                Company              StartTime
----      ----                                                -------              ---------
taskhost1 C:\Users\IEUser\AppData\Roaming\PTOVTYJC\taskhost1.exe NetSupport Ltd       8/19/2020 6:55:55 AM
taskhostw C:\Windows\system32\taskhostw.exe                   Microsoft Corporation 8/13/2020 2:41:03 PM


PS C:\Users\IEUser\Downloads>
```

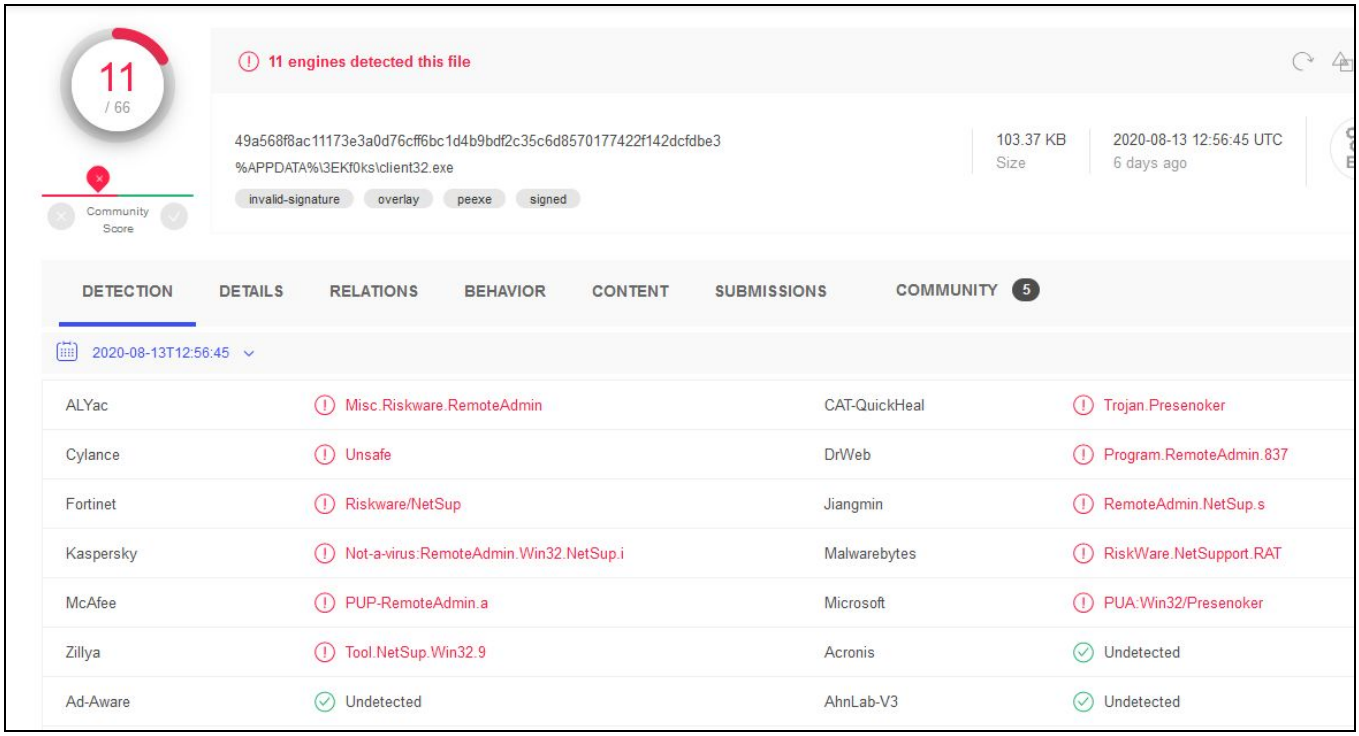
```
PS C:\windows> Get-ChildItem task*.exe -Recurse -ErrorAction SilentlyContinue | select-object Name | Group-Object Name

Count Name                      Group
----- ----                      -----
    8 taskmgr.exe               {@{Name=taskmgr.exe}, @{Name=taskmgr.exe}, @{Name=Taskmgr.exe}, @{Name=Taskmgr.exe}...}
    2 taskhostw.exe             {@{Name=taskhostw.exe}, @{Name=taskhostw.exe}}
    4 taskkill.exe              {@{Name=taskkill.exe}, @{Name=taskkill.exe}, @{Name=taskkill.exe}, @{Name=taskkill.e...
    4 tasklist.exe              {@{Name=tasklist.exe}, @{Name=tasklist.exe}, @{Name=tasklist.exe}, @{Name=tasklist.e...


PS C:\windows>
```

What about this executable would make it difficult to be detected by an Antivirus?

A. The executable is signed by a legitimate company, “Net Support Ltd”.



B. Most of the signatures that come up the binary show things such as “RiskWare” or remote admin, which for a sysadmin might be the kind of thing that gets ignored if they are using this or similar tool for remote administration.



C. In fact if we google this tool we can actually see the site to purchase a legitimate copy from.

If this executable is “legitimate” what makes this of use to an attacker?

A. The “client32.ini” file contains the configuration for the RAT, in it we can see the network address it is configured to communicate with.
B. In the provided example, we can see it was configured to communicate with an IP address.

```
[HTTP]
GatewayAddress=72.52.96.203:443
GSK=FK;N@BDL9C=MBGGA:F=H@JDM:G>JBM
```

The below example is from another sample found online, we can see this was configured to communicate with two different domains.

```
[HTTP]
GatewayAddress=networko.org:443

SecondaryGateway=fourseasondiscountslist.xyz:443
GSK=FL;O@OFC:M@KDAGC:I
```