**Task 1. Basic Static Analysis**

* The Malware Analysis Cloud Machine you prepared in a previous project, running Windows Server 2016

**Downloading and Extracting the Sample**

Using Firefox, download this file:

**key.7z**

You need 7-zip to extract the file. If you don't have it installed, download and install the 64-bit version from:

[**https://www.7-zip.org/**](https://www.7-zip.org/)

Right-click the **key.7z** file and click **7-Zip**, "**Extract Here**". Enter a password of **malware**

The sample appears, named **key.exe**.

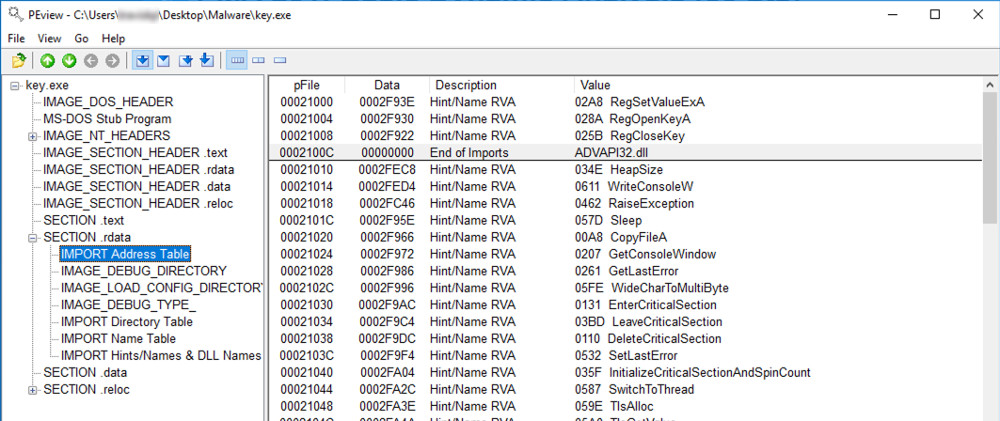
**Using PEview**

Open **key.exe** in PEview.

As shown below, if you expand "**SECTION .rdata**" and click "**IMPORT Address Table**", one of the three DLL's imported is [advapi32.dll](https://www.file.net/process/advapi32.dll.html).

As you scroll you will see functions such as [WriteConsoleW](https://docs.microsoft.com/en-us/windows/console/writeconsole), [GetConsoleWindow](https://docs.microsoft.com/en-us/windows/console/getconsolewindow), [WideCharToMultiByte](https://docs.microsoft.com/en-us/windows/win32/api/stringapiset/nf-stringapiset-widechartomultibyte), and [GetStringType](https://docs.microsoft.com/en-us/windows/win32/api/stringapiset/nf-stringapiset-getstringtypew) which assist us in identifying what the exe is doing.

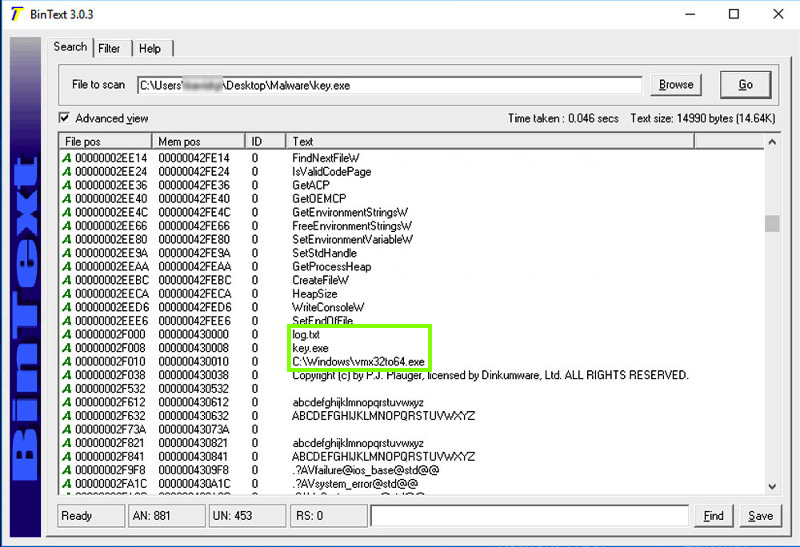
The other two DLLs are [kernel32.dll](https://www.file.net/process/kernel32.dll.html), and [user32.dll](https://www.processlibrary.com/en/directory/files/user32/19597/).



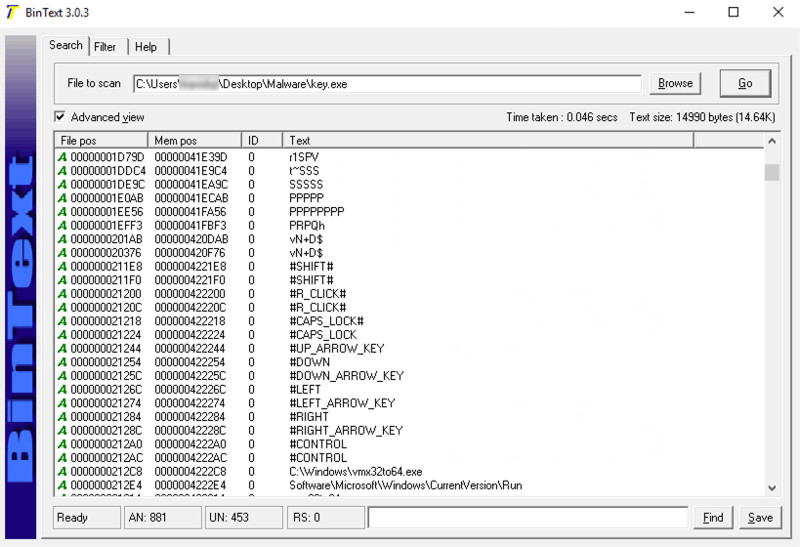
**Using BinText**

Examine the strings in **key.exe** and find these items, as shown below.

* **log.txt** -- A txt file
* **key.exe** -- The program name
* **C:\windows\vmx32to64.exe** -- An interesting file



Scroll up and find the key definitions, including **#SHIFT#** and **#CAPS\_LOCK#**, as shown below. These look like strings used by a keylogger.



**Task 2. Preparing for Dynamic Analysis**

Dynamic analysis is simple: run monitoring tools, then run the malware, and let it have its way with our virtual machine. This is a sloppy technique, trusting a system that is being infected, but it usually works.

We will use these three programs to see what the malware does:

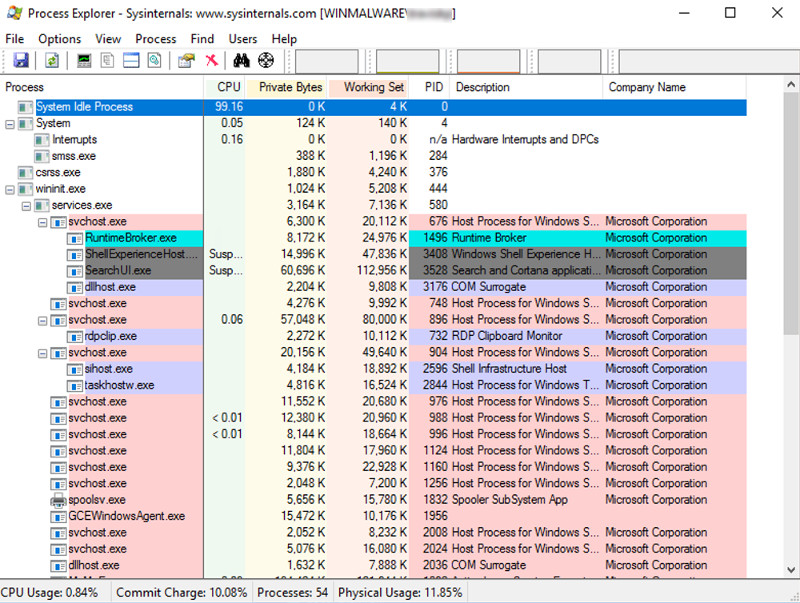
1. Process Explorer
2. Wireshark
3. Process Monitor

**Install and Run Process Explorer**

Download Process Explorer from <https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer>

Extract the zip file and open **procexp64**

Process Explorer shows currently running processes, with far more detail than Task Manager. It doesn't keep a log of them, so it's harmless to leave running.



**Install and Run Wireshark**

Go to <https://www.wireshark.org/index.html#download> and save/run the **Windows Installer (64-bit)** file.

Install Wireshark with the default options

Start Wireshark and begin capturing packets from the interface that goes to the Internet, it should be "Ethernet".

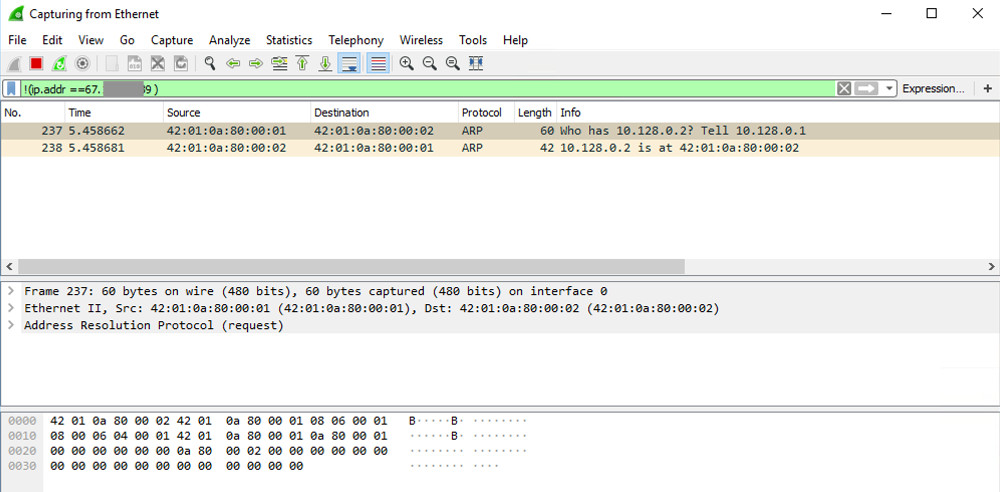
There will be a lot of traffic at the start because you are running RDP from your host machine to the Windows cloud machine.

To filter out the RDP traffic, enter this into the Wireshark command line, replacing 192.168.10.10 with your host machine IP address:

**!(ip.addr == 192.168.10.10)**

Note: To get the ip of your host machine, Google search "[What's My IP?](https://www.google.com/search?q=what%27s%20my%20ip)

Once that command is entered, you can stop and start the capture again by clicking the red box and the blue fin above the command line. Close any open web browsers to limit the traffic.



Note: For this project, no web requests will be made by the malware, but it's a good idea to monitor network traffic when running malware.

**Install and Start Process Monitor**

Process Monitor logs all the events in Windows Event Viewer, which will typically be hundreds of thousands of events. Don't leave it running for too long or it will use up all the RAM and crash.

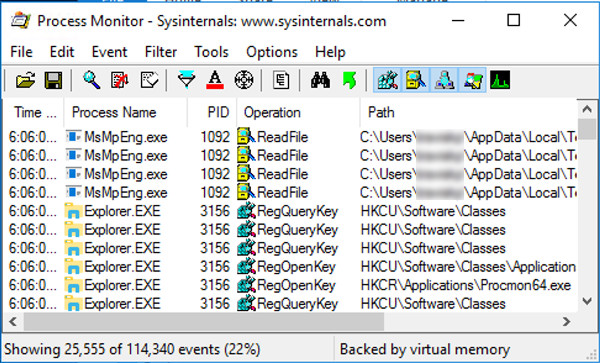
It's best to start Process Monitor last, so you can exclude all the harmless processes the other tools are using.

Go to <https://docs.microsoft.com/en-us/sysinternals/downloads/procmon> and download / extract Process Monitor.

Launch Process Monitor. If a Security Warning box pops up, allow the software to run.

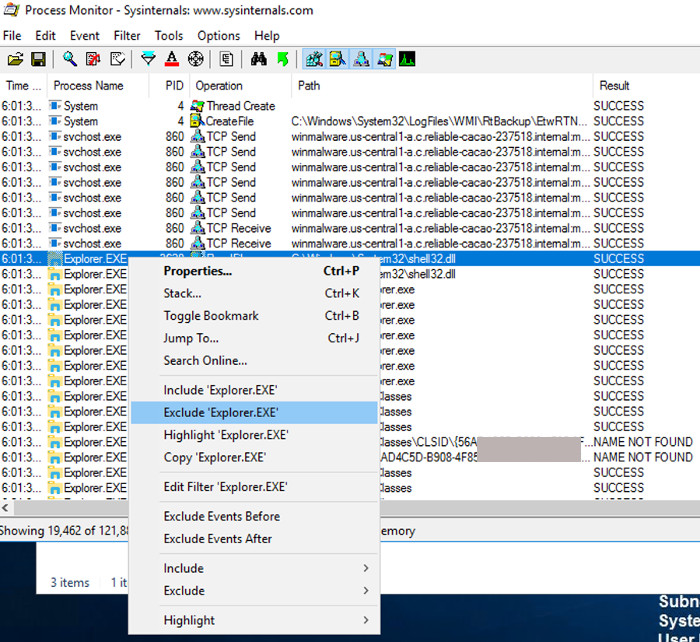
Agree to the license.

You see Process Monitor, with a lot of visible events, as shown below.

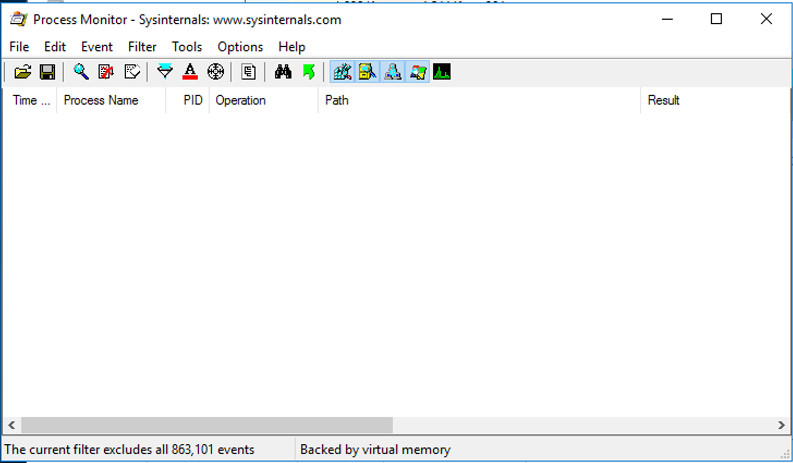


**Excluding Harmless Processes**

In Process Monitor, right-click the name of one of the visible processes, such as **explorer.exe**, and click "**exclude 'lsass.exe'**", as shown below:



Repeat the process until all current processes are hidden, as shown below. There were a lot of processes to ignore, around 15 to 20.



**Running the Malware**

In File Explorer, right-click **key.exe** and choose **Run as Administrator**.

***RUN THE MALWARE AS ADMINISTRATOR!***

If you run it without Administrator privileges, the persistence mechanism will fail and you won't be able to find flag 221.3 below.

**Wireshark**

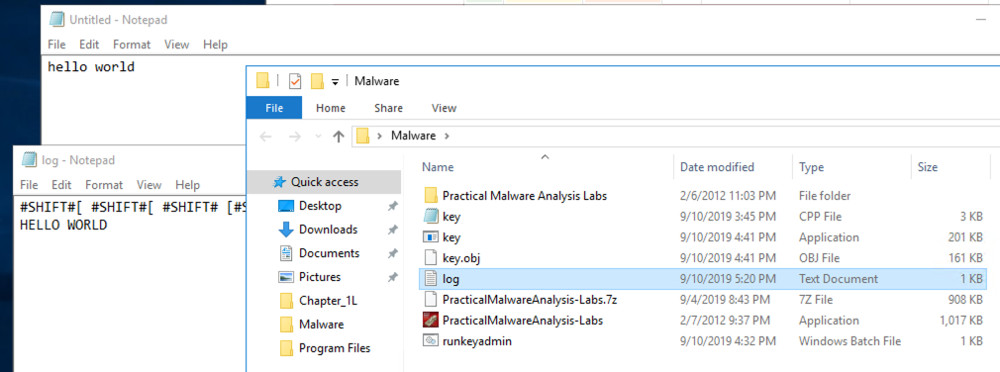
No unusual traffic appears in Wireshark, because this sample doesn't use the Internet. Close Wireshark.

|  |
| --- |
| **Flag 221.1: Viewing the Running Malware in Process Explorer (10 pts)**  In Process Explorer, in the top pane, find **key.exe** and click it.  Find the name of the exe covered in green in the image below. That is the flag.  https://bowneconsultingcontent.com/pub/PMA/pma221/pma201_peflag.jpg |
| **Flag 221.2: Viewing the Running Malware in Process Monitor (5 pts)**  Go to ProcMon and scroll until you get to key.exe. You can view the steps the malware is taking.  https://bowneconsultingcontent.com/pub/PMA/pma221/pma201_procmon1.jpg  This malware creates an executable file in the Windows directory.  https://bowneconsultingcontent.com/pub/PMA/pma221/pma201_procmon2.jpg  The malware also creates persistence by modifying the run registry key for the current user (HKCU = HKEY\_CURRENT\_USER). The programs referenced in this key will be executed when the user logs in.  Find the path of that key and take note of it.  https://bowneconsultingcontent.com/pub/PMA/pma221/pma201_procmonflag.jpg  The flag is the text covered in green. | |

**Test out the keylogger**

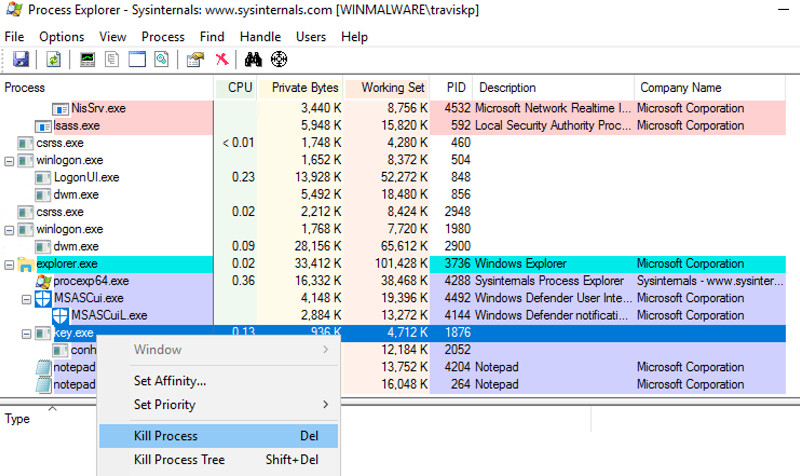
Open notepad and type some text.

In File Explorer, go to the folder where key.exe is, find **log.txt** and open it. You see the captured keystrokes, as shown below.



**Persistence Mechanism**

In Process Explorer, right click **key.exe** and choose **Kill Process**.



This stops the keylogger for the current sesssion. However, the malware has written itself into the registry, so it will start back up at the next reboot.

**Restart the machine** and reconnect through RDP.

|  |
| --- |
| **Flag 221.3: Persistence (10 pts)**  Open **Process Explorer**, find and click the new keylogger file, **vmx32to64.exe**.  From the Process Explorer menu bar, click **View**, "**Show Lower Pane**" **View**, "**Lower Pane View**", **Handles**.  The flag is covered by a green rectangle in the image below.  https://bowneconsultingcontent.com/pub/PMA/pma221/pma201_procexflag2.jpg |
| **Flag 221.4: Removing persistence (5 pts)**  Open **command prompt** and type in **regedit**  Navigate to the path we saw in 2.2: **HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**  https://bowneconsultingcontent.com/pub/PMA/pma221/pma201_persistflag.jpg  The flag is the text covered in green. | |

Right click **vmx32to64** and **delete** the registry key.

|  |
| --- |
| **Flag 221.5: Run Key (10 pts extra)**  Download this sample and unzip it with the password **malware**  **key12.7z**  Use the same dynamic anaysis tools to monitor the behavior of this sample. Find the Registry action shown below. The flag is covered by a green rectangle.  https://bowneconsultingcontent.com/pub/PMA/pma221/PMA221-1.png |
| **Flag 221.6: DNS Traffic (10 pts extra)**  Examine the network traffic generated by the key12.exe sample.  Find the key in the DNS traffic, as shown below.  https://bowneconsultingcontent.com/pub/PMA/pma221/PMA221-2.png | |

|  |
| --- |
| **Flag 221.7: HTTP Traffic (10 pts extra)**  Download this sample and unzip it with the password **malware**  **key13.7z**  Examine the network traffic generated by the key13.exe sample.  Find the key in the HTTP traffic, as shown below.  https://bowneconsultingcontent.com/pub/PMA/pma221/PMA221-3.png |