A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. How the initial infection happened?  
   The initial infection happened when user ran an executable from OCT 12.zip folder. There are multiple executables available in that folder out of which 4.exe was run by the user. After this, it started executing multiple other executables and eventually files started getting encrypted, indicating an ransomware attack. I can see ransomnote on startup as well.

A screenshot of a computer

Description automatically generated

1. Where did it come from?  
   The virus was downloaded from appbox, highlighted URL in the screenshot above. The timestamp for this download is 06/18/2022 at 10:02:57AM. The malicious executable was ran at 10:03:38 AM from OCT 12 folder.

A screenshot of a computer

Description automatically generated

1. How did it spread?  
   Initially 4.exe was ran by an user then it further began executing multiple other executables as shown in the screenshot. Initial execution started on 06/18/2022 10:03:38AM followed by process with Record ID 10 that was executed on 10:03:41AM and so on.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. What are the IOCs present, their correlations and name of malware  
   I can see all files are encrypted with RYK extension. It is an indication that the name of malware is Ryuk. I can also see that under startup items there is RyukReadMe.html which can be the ransom note.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. How many times was the UAC program invoked and what dates/times?  
   The Following two Event ID’s are related to UAC: 4648, 4688.  
   There is no log for 4688 but I can see logs for 4648 with the event description summary as “A logon was attempted using explicit credentials”   
   Total 4 times UAC was invoked and following are date and time for the same:  
   6/18/2022 9:57:43 AM  
   6/18/2022 9:57:43 AM

6/18/2022 9:57:45 AM  
6/18/2022 9:58:08 AM

A screenshot of a computer

Description automatically generated

1. What is the hostname and vendor of the machine?  
   Hostname is T433-MILIND-COM  
   If there was MAC address present, I can search for that MAC Address on OUI lookup to get vendor name. I cannot see vendor name present here.

A screenshot of a computer

Description automatically generated

1. What can you infer from Google searches?  
   From the Google searches I can infer that the person is interested in researching about two different topics (Wireshark and Toronto star).

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Based on the Google search results, what can you learn?    
   Based on recent google search results, I can learn that the user is interested in learning about analyzing network traffic (Wireshark) and the user is also interested in local news or current events in Toronto (Toronto star)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. How many times did different users' login to the machine? What were the date and times?   
   There are multiple users but I could find only one user with a valid name (T433-COMP4071) who logged in on 06/18/2022 09:58:08 AM

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. When, how many and what kind of USB devices are connected to the computer?  
   Six USB devices connected to the computer. Following are the names:  
   ROOT\_HUB , ROOT\_HUB20, ROOT\_HUB30, VID\_0E0F&PID\_0003 (USB composite device), VID\_0E0F&PID\_0003&MI\_01, VID\_0E0F&PID\_0003&MI\_00  
     
   Kind of USB devices: USB Composite Device, USB2.0, USB3.0

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. What user accounts were saved for website and what were the websites? Explain what the user was doing there.  
   I found password token for T433-COMP4071 user. I can also check that under potential browser activity there is “request\_token” mentioned in the URL. User is browsing twitter and it is likely that the user has twitter credentials saved in the browser.

A screenshot of a computer

Description automatically generated

1. What files were downloaded using Google Chrome? What URLs did they come from?  
   Volatility, Wireshark, An APK file and multiple files from app box are downloaded using google chrome. URL for the source from where multiple files were downloaded is - <https://app.box.com/s/2g2gj39kdl9wwam7ybkallfukdedntdx/folder/89904775115>  
     
   Volatility- <http://downloads.volatilityfoundation.org/releases/2.6/volatility_2.6_win64_standalone.zip>  
     
   Wireshark- <https://1.na.dl.wireshark.org/win64/Wireshark-win64-3.6.1.exe>  
     
   APK file- <https://app.dn1102.online/Polkadot.apk>

A screenshot of a computer

Description automatically generated

1. What URLs did the malware come from?  
   Malware came from following URL- <https://app.box.com/s/2g2gj39kdl9wwam7ybkallfukdedntdx/folder/89904775115>

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. What auto suggest keyword searches do you see? What do you infer from them?

URL1)[https://www.google.com/search?**q**=torontostar&rlz=1C1CHBF\_enCA989CA989&**oq**=torontostar&aqs=chrome..69i57j0i10i512l9.3504j0j7&sourceid=chrome&ie=UTF-8](https://www.google.com/search?q=torontostar&rlz=1C1CHBF_enCA989CA989&oq=torontostar&aqs=chrome..69i57j0i10i512l9.3504j0j7&sourceid=chrome&ie=UTF-8)

URL2)[https://www.google.com/search?**q**=wireshark&rlz=1C1CHBF\_enCA989CA989&**oq**=wireshark&aqs=chrome..69i57j0i433i512j0i512l8.1801j0j7&sourceid=chrome&ie=UTF-8](https://www.google.com/search?q=wireshark&rlz=1C1CHBF_enCA989CA989&oq=wireshark&aqs=chrome..69i57j0i433i512j0i512l8.1801j0j7&sourceid=chrome&ie=UTF-8)

I see that both oq and q are same for all URL’s present in search history, hence there are no auto suggest keyword searches present here.