**Delivery of new Pika Bot malware using the .jar file**

It has been quite some time since I have delved into the deep execution of malware and found the recent sample of Pika Bot quite interesting to execute, especially in the behavioral analysis.

So, the malware spreading email body says, “Have you checked the invoice which I shared with you yesterday” and the password for unzipping the file is also mentioned in the body. And please be aware that if you get an email which has the above wordings restrict yourself from downloading the attachment.

A red and black logo

Description automatically generated

**fig.1** this is how the file is sent as an attachment.

Now let us proceed with the static analysis of the sample by using the common threat intelligence source Virus Total to check the malicious score of the sample. When we unzip the above file, we get a .jar file which is the abbreviation for a “**Java Archive**” file.

A logo of a jar

Description automatically generated

**fig.2** this the actual payload which when exec will contact CNCs.

The static analysis of the .jar file is as follows.

A screenshot of a computer

Description automatically generated**fig.3** static analysis using VT.

***DYNAMIC ANALYSIS***

Now for dynamic analysis rename the .jar file to .zip to know the contents of the file.

A screen shot of a computer

Description automatically generated

**fig.4** contents of the jar file.

As we see one of the contents is .class file is a compiled java file by the java compiler and can be executed by JVM and JRE. We can execute how a normal class is executed.

We can use the following command in command prompt “**java filename**”.

Now open the command prompt in the extracted file in order to be hassle free from navigating through paths. And open the process hacker to have a look on the processes getting spawned when this main payload is executed.

A black background with white text

Description automatically generated

**F ig.5** command to execute the .class file.

When the above command is given in the command prompt a process injection will be done through ctfmon.exe which is a legit process from Microsoft which controls various inputs from the user such as KB stokes, Mouse clicks.

A blue and yellow number

Description automatically generated with medium confidence

**fig.6** ctfmon.exe the injected process.

When we navigate to the network tab of the process hacker, we can get the various CNCs which the malicious ctfmon.exe is communicating with.

A screenshot of a computer

Description automatically generated

**fig 7**. process injection through legit process.

As we can see the IP addresses in the above screenshot when we search these addresses in the one of the open-source intelligence tools called **Virus Total** and navigate to community tab we can see that it is a new type of Pika Bot

Another Way of finding out CNC is as follows.

A screen shot of a computer

Description automatically generated

**fig.8** folder contents.

As we know the above files are the contents of the folder. All other files have their extensions except the file with the name “**723079**”.

First let us check what is the exact extension of the file.

A screenshot of a computer

Description automatically generated

**fig.9** magic number of the file with no extension.

As we know that “4D 5A” is the exact magic number of the “**.dll**” (dynamic link library) file. After renaming the file with its corresponding extension and we also know that the dll files should be registered first in order to make the same executable. Now enter the below command to register the same and the communication with the malicious CNCs will get spawned.

“**rundll32.exe (file name with ext) DllRegisterServer**”

A screen shot of a computer

Description automatically generated

**fig.10** dll register.

As soon as we run the statement as seen [fig.7](https://cdn-images-1.medium.com/max/800/1*aie2U5-mMVUMum6enDW4xg.png) the CNCs will start getting spawned.

A screenshot of a computer screen

Description automatically generated

**fig.11** CNCs using dll.

This is another way of getting the malicious IPs or CNCs