# KrakenKeylogger Challenge

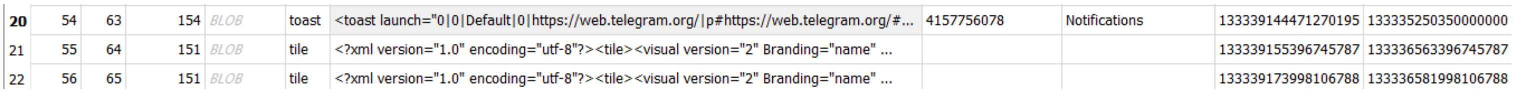
Scenario:

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.

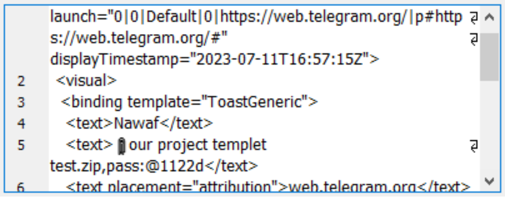
The helper's demand for payment revealed that he was actually a threat actor. The company's digital forensics team was called in to investigate and identify the attacker, determine the extent of the attack, and assess potential data breaches. The team must analyze the employee's computer and communication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

Task 1:
What is the the web messaging app the employee used to talk to the attacker?

I checked the Notifications artifact inside the "C:\Users\Bubble\Desktop\challenge\Users\OMEN \AppData\Local\Microsoft\Windows\Notifications" and opened the file wpndatabase.db with DB Browser.
Then I checked the Notification table and noticed the Telegram application at the bottom.



| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **20** | 54 | 63 | 154 | *BLOB* | toast | <toast launch="0\|0\|Default\|0\|https://web.telegram.org/\|p#https://web.telegram.org/#... | 4157756078 | Notifications | 133339144471270195 | 133335250350000000 |
| 21 | 55 | 64 | 151 | *BLOB* | tile | <?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" ... | | | 133339155396745787 | 133336563396745787 |
| 22 | 56 | 65 | 151 | *BLOB* | tile | <?xml version="1.0" encoding="utf-8"?><tile><visual version="2" Branding="name" ... | | | 133339173998106788 | 133336581998106788 |

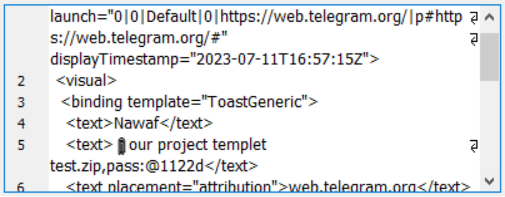


```
launch="0|0|Default|0|https://web.telegram.org/|p#http
s://web.telegram.org/#"
displayTimestamp="2023-07-11T16:57:15Z">
 <visual>
  <binding template="ToastGeneric">
   <text>Nawaf</text>
   <text> 📎our project templet
test.zip,pass:@1122d</text>
   <text placement="attribution">web.telegram.org</text>
```

Answer: telegram

Task 2:
What is the password for the protected ZIP file sent by the attacker to the employee?

Same like task 1

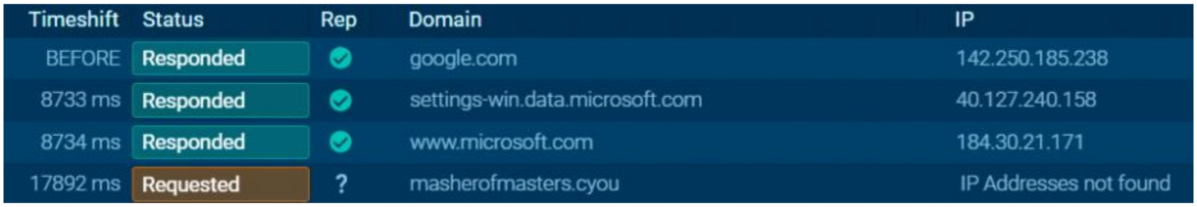


```
launch="0|0|Default|0|https://web.telegram.org/|p#http
s://web.telegram.org/#"
displayTimestamp="2023-07-11T16:57:15Z">
 <visual>
  <binding template="ToastGeneric">
   <text>Nawaf</text>
   <text> 📎our project templet
test.zip,pass:@1122d</text>
   <text placement="attribution">web.telegram.org</text>
```

Answer: @1122d

Task 3:
What domain did the attacker use to download the second stage of the malware?

I checked the Downloads folder of the user and noticed the project files.
I executed the templet file inside AnyRun and checked the domain.

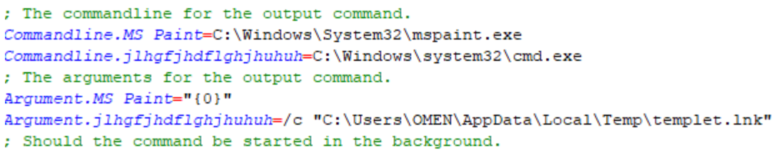


| Timeshift | Status | Rep | Domain | IP |
|---|---|---|---|---|
| BEFORE | Responded | ✓ | google.com | 142.250.185.238 |
| 8733 ms | Responded | ✓ | settings-win.data.microsoft.com | 40.127.240.158 |
| 8734 ms | Responded | ✓ | www.microsoft.com | 184.30.21.171 |
| 17892 ms | Requested | ? | masherofmasters.cyou | IP Addresses not found |

Answer: masherofmasters.cyou

Task 4:
What is the name of the command that the attacker injected using one of the installed LOLAPPS on the machine to achieve persistence?

I noticed the folder Greenshot inside the AppData\Roaming and the folder contains only one file Greenshot.ini
I opened it with Notepad++ and analyzed it until I saw a command with the path of the malicious file templet

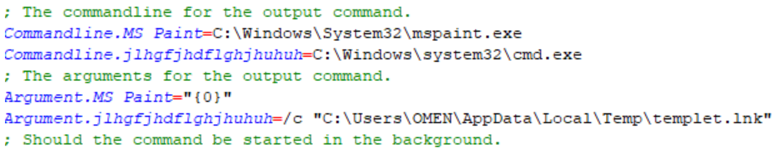


```
; The commandline for the output command.
Commandline.MS Paint=C:\Windows\System32\mspaint.exe
Commandline.jlhgfjhdflghjhuhuh=C:\Windows\system32\cmd.exe
; The arguments for the output command.
Argument.MS Paint="{0}"
Argument.jlhgfjhdflghjhuhuh=/c "C:\Users\OMEN\AppData\Local\Temp\templet.lnk"
;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

Answer: jlhgfjhdflghjhuhuh

Task 5:
What is the complete path of the malicious file that the attacker used to achieve persistence?

Same as previous task

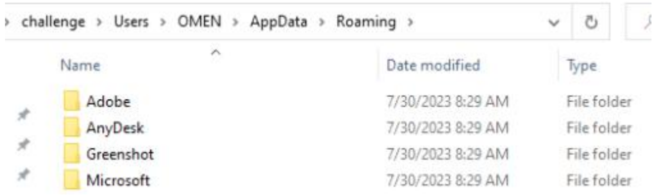


```
; The commandline for the output command.
Commandline.MS Paint=C:\Windows\System32\mspaint.exe
Commandline.jlhgfjhdflghjhuhuh=C:\Windows\system32\cmd.exe
; The arguments for the output command.
Argument.MS Paint="{0}"
Argument.jlhgfjhdflghjhuhuh=/c "C:\Users\OMEN\AppData\Local\Temp\templet.lnk"
;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

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

Task 6:
What is the name of the application the attacker utilized for data exfiltration?

In the same path like task 4, there is remote access tool AnyDesk inside the AppData\Roaming



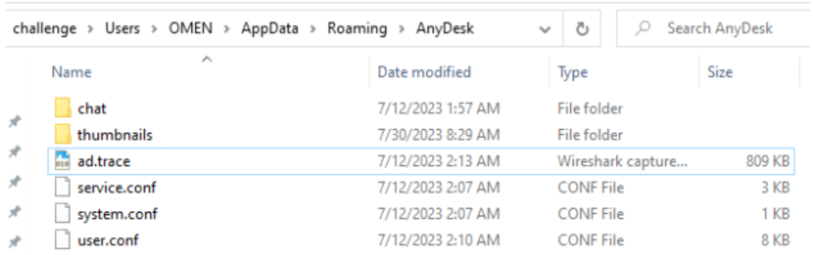
› challenge › Users › OMEN › AppData › Roaming ›

| Name | Date modified | Type |
|---|---|---|
| Adobe | 7/30/2023 8:29 AM | File folder |
| AnyDesk | 7/30/2023 8:29 AM | File folder |
| Greenshot | 7/30/2023 8:29 AM | File folder |
| Microsoft | 7/30/2023 8:29 AM | File folder |

Answer: AnyDesk

Task 7:
What is the IP address of the attacker?

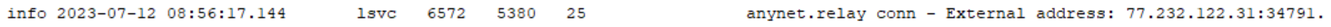
Inside the AnyDesk folder I saw several files and one file look like a Wireshark file but when I tried to open it its didn’t worked so I open it with Notepad++ and searched for "address"



challenge › Users › OMEN › AppData › Roaming › AnyDesk

Search AnyDesk

| Name | Date modified | Type | Size |
|---|---|---|---|
| chat | 7/12/2023 1:57 AM | File folder | |
| thumbnails | 7/30/2023 8:29 AM | File folder | |
| ad.trace | 7/12/2023 2:13 AM | Wireshark capture... | 809 KB |
| service.conf | 7/12/2023 2:07 AM | CONF File | 3 KB |
| system.conf | 7/12/2023 2:07 AM | CONF File | 1 KB |
| user.conf | 7/12/2023 2:10 AM | CONF File | 8 KB |



```
info 2023-07-12 08:56:17.144       lsvc    6572    5380    25              anynet.relay conn - External address: 77.232.122.31:34791.
```

Answer: 77.232.122.31