KrakenKeylogger (Cyber Defenders) - Walkthrough

Wednesday, September 11, 2024 6:27 PM

Story:
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.

Q1: What is the the web messaging app the employee used to talk to the attacker?

- To answer this question, I used 'SQLiteDB' to parse Windows Notifications artifacts.

  This feature captures real-time notifications for various events like email alerts, application updates, security alerts, reminders, and other app-specific notifications. Investigators can extract valuable details, such as the content or text of the notification displayed to the user.

  Path: C:\Users\%USER%\AppData\Local\Microsoft\Windows\Notifications\wpndatabase.db

  By analyzing the "Notification" tab, I found that the user had been using '**Telegram**'.

```
" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockD
```

```
" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockD
|Default|0|https://web.telegram.org/|p#https://web.telegram.org/#" displayTimestamp="2023-07-11T16:57:15Z">...
" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockD
" encoding="utf-8"?><tile><visual version="2" Branding="name" baseUri="http://blob.weather.microsoft.com/static/mws-new/" hint-lockD
```

Q2: What is the password for the protected ZIP file sent by the attacker to the employee?

- In the Telegram notification itself, we are able to see the password to the zip file (@1122d)

```
2  <visual>
3   <binding template="ToastGeneric">
4    <text>Nawaf</text>
5    <text> our project templet test.zip,pass:@1122d</text>
6    <text placement="attribution">web.telegram.org</text>
7    <image placement="appLogoOverride"
src="C:\Users\OMEN\AppData\Local\Google\Chrome\User
Data\Notification
```

Q3: What domain did the attacker use to download the second stage of the malware?

I checked the 'Downloads' folder and found the extracted ZIP containing two files: the project itself and a 'template' shortcut file.
After extracting the hashes from both files, I discovered that the 'template' file is flagged as highly malicious.
A search of the hash on VirusTotal revealed that the first HTTP request was made to **'hxxps://masherofmasters.cyou/chin/se1.hta'.**

HTTP Requests

CONNECT https://masherofmasters.cyou/chin/se1.hta

GET http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt 200

GET http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c 200

GET http://www.microsoft.com/pki/certs/MicCodSigPCA_08-31-2010.crt 200

GET http://www.microsoft.com/pki/certs/MicrosoftTimeStampPCA.crt 200

Q4: What is the name of the command that the attacker injected using one of the installed LOLAPPS on the machine to achieve persistence?

- That was a great question! First of all, I accessed the LOLAPPS project (https://lolapps-project.github.io/).
  The first application used for persistence was 'GreenShot.'
  When I navigated the compromised user's AppData folder, I identified the use of this program.

  For LOLAPPS:
  Any Greenshot plugin can be used for persistence, the simplest being the "External command plugin," which runs a command line. To modify the "Greenshot.ini" file in "%AppData% \Greenshot", you can add an "[ExternalCommand]" configuration. Add a new name to the "Commands" parameter, insert the payload into the "Commandline.<name>" and "Argument.<name>," and then add the name to the "Destinations" parameter. parameters, and finally, open "Preferences -> Destination" and enable the new external command.

  I navigated to the "Greenshot.ini" file located at 'challenge\Users\OMEN\AppData\Roaming \Greenshot,' searched for 'Command' in the INI file, and found the suspicious argument.

```
; Greenshot ExternalCommand Plugin configuration
[ExternalCommand]
; The commands that are available.
Commands=MS Paint,jlhgfjhdflghjhuhuh
; Redirect the standard error of all external commands, used to output as warning to the greenshot.log.
RedirectStandardError=True
; Redirect the standard output of all external commands, used for different other functions (more below).
RedirectStandardOutput=True
; Depends on 'RedirectStandardOutput': Show standard output of all external commands to the Greenshot log, this can be usefull for debugging.
ShowStandardOutputInLog=False
; Depends on 'RedirectStandardOutput': Parse the output and take the first found URI, if a URI is found than clicking on the notify bubble goes there.
ParseForUri=True
; Depends on 'RedirectStandardOutput': Place the standard output on the clipboard.
OutputToClipboard=False
; Depends on 'RedirectStandardOutput' & 'ParseForUri': If an URI is found in the standard input, place it on the clipboard. (This overwrites the output from
OutputToClipboard setting.)
UriToClipboard=True
; 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
```

Q5: What is the complete path of the malicious file that the attacker used to achieve persistence?

- We already found it in the question above **(C:\Users\OMEN\AppData\Local\Temp\templet.lnk**)

Q6: What is the name of the application the attacker utilized for data exfiltration?

- As before, when I navigated in the 'Appdata' I found that was a usage of 'Anydesk'

Q7:What is the IP address of the attacker?

- To address this question, I accessed to the AnyDesk folder and found the file 'ad.trace' which contains trace logs of the remote connections.

  I filtered 'Logged In' and found the answer which is **77.232.122.31**