Inside the SharpPanda's Malware Targeting Malaysia

By Anonymous

Published: 2024-05-24 · Archived: 2026-04-05 20:17:28 UTC

This post was authored by NetbyteSEC Detecx team.

In April 2024, the NetbyteSEC (NBS) team discovered a tweet from Group IB Threat Intelligence indicating the detection of several malware instances associated with SharpPanda uploaded to VirusTotal. This piqued the NBS team's interest to dig more, particularly focusing on the samples that are linked to Malaysia as the uploader of the sample on the VirusTotal platform was identified from Malaysia.

Figure 1: Tweet from Group IB Threat Intelligence

Based on the IOCs (Indicators of Compromise), it appears that the SharpPanda team targeted another Southeast Asian country besides Malaysia.

NBS team collected all the IOCs from Twitter's thread of the tweet and retrieved the samples from VirusTotal for further analysis. In this case, the NBS team solely focuses on the samples that are linked to Malaysia.

Way before the tweet, another independent security researcher (@4rchib4ld) reported the same context of threat information regarding SharpPanda sample that was uploaded from Malaysia.

Figure 2: Tweet from independent security researcher associated with SharpPanda

Thank you to Group IB and (@4rchib4ld) for the malware hunting findings.

1.0 Executive Summary

The NBS team recently conducted an analysis on a malware sample that belongs to SharpPanda's APT group that is targeting Malaysia around March to April 2024. Based on the intelligence, the sample leverages a malicious executable that perform the backdoor connection giving access to the attacker once the malware infects the victims. NBS team is unable to identify how the threat actor distributed the malware. Nevertheless, typically, this kind of malware campaign might involve sending the malicious document and executable file as an attachment in the email. Based on our analysis of one of the samples executable, the final objective of the malware is to provide the backdoor connection towards the C2 server.

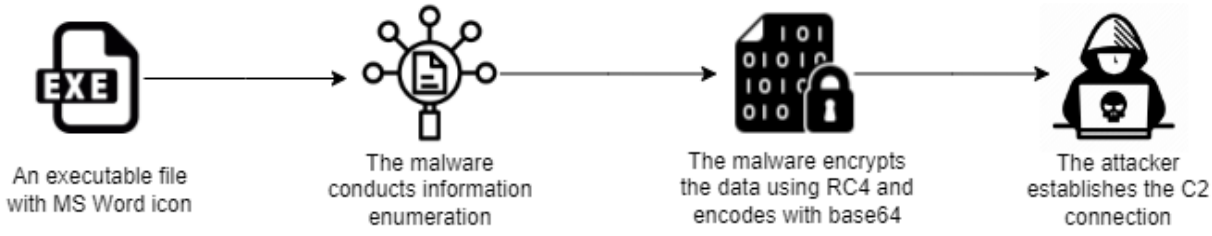

Figure 3: Graph flow of the malware

2.0 Technical Analysis

In this technical analysis, the NBS team was able to retrieve those samples that were uploaded to VirusTotal and conduct malware analysis and reverse engineering on the sample. The name of the sample executable is "REKOD MINIT KSN KEPADA YAB PM 2023 - 15.exe" (SHA1: ba12750f122462d16b4847adcb927b86af60b5d6)

Initial Analysis

Upon initial analysis, it is apparent that the attacker is leveraging the Microsoft Word icon for the executable file to deceive users, making the malicious file appear harmless and increasing the likelihood of it being clicked.

Figure 4: The executable file with Microsoft Word icon

The initial assessment of the executable on VirusTotal, as of the time of this writing, shows that the malware executable has a high detection of Antivirus with a current detection score 46/72 as shown in the figure below. This high detection suggests that the malware has a significant ability to infect.

Figure 5: VirusTotal result

Pivoting our analysis of the network connection results in the VirusTotal sandbox reveals that the malware makes few connections to an endpoint, 185.239.226.91, located in Hong Kong.

Figure 6: Network connection results in the VirusTotal

Based on the figure above, the malware communicates with the C2 server by sending encoded and encrypted strings append in the full URL parameter.

String Decryption

Upon reverse engineering the malware sample, it was found that the malware employs a significant amount of simple XOR decryption on encrypted strings which will be used for the rest of the malware's functionality. This is observed that numerous functions within the malware perform decryption of the strings before proceeding to the actual functionality.

Figure 7: XOR decryption on encrypted strings

After finishing the decryption process for the encrypted values, the strings will be utilized in several functionalities, such as constructing URL paths, employing Windows APIs, defining mutex names, and various others.

Mutex Creation

Upon decrypting the encrypted strings, the malware proceeds to create a mutex with the name "*mt_app_http_get_zed2vsp*" typically to avoid multiple infections in the same machine.

Figure 8: Mutex creation

We can double-confirm the mutex creation by reviewing the Handles object of the executable's process.

Figure 9: Review Handles object to validate the mutex creation

OS Information Enumeration

Furthermore, the malware proceeds to another crucial function which is collecting all the operating system information and compiling the results into a single log string. In the following figure, the code performs all the information enumeration and appends it to an acronym accordingly.

Figure 10: Information enumeration

The attribution of the acronym is as follows:

1. HTN = Hostname
2. OSN = OS Name
3. OSV = OS Version
4. URN = Username
5. ITF = Network Interface
6. PGF = Program Files (Installed)
7. PSL = Running Processes

Below is the sample of collected data from NBS's lab host:

```
HTN:DESKTOP-XXXX; OSN:Windows 10 Enterprise; OSV:10.0.19046; URN:mare; ITF:N:1 {4380E106-0381-4C7A-8D3F-928628(
```

Data Encryption and Encoding

After collecting all the necessary data, the malware begins encrypting the long string using RC4 and encodes it with base64 for the ease of appending it to the URL path parameter.

The function in the figure below demonstrates the RC4 encryption process applied to the data.

Figure 11: RC4 encryption process

The function below demonstrates the process of base64 encoding applied to the RC4 encrypted data.

Figure 12: Base64 encoding process

After completing the encoding and encryption processes, the malware constructs a string builder for the URL path and appends the base64 encoded data into the URL path parameter, which will be used for the C2 communication.

Figure 13: The process of constructing string builder and appending base64 encoded data into URL path

C2 Communication

Utilizing the previously mentioned URL decoding and string constructor, the malware employs the Windows Socket Windows API to establish the communication to the threat actor server.

Figure 14: Establish C2 connection using Windows Socket Windows API

This communication can be seen by sniffing the network communication as shown in figure below:

Figure 15: Malware communication after the host has been infected

3.0 Summary

The malware initially performs extensive string decryption to prepare for the sequential function. Utilizing the decrypted strings, it creates a mutex in the infected host to prevent multiple infections. Subsequently, the malware gathers various information about the infected host and encrypts it using the RC4 algorithm. The resulting data is then encoded with base64 and appended to the URL path. In the final stage of functionality, it initiates C2 communication using the previously mentioned URL path and the encrypted data.

4.0 IOCs

Network:

- 185.239.226.91

Hash:

- SHA256: 20a4256443957fbae69c7c666ae025522533b849e01680287177110603a83a41

Source: https://notes.netbytesec.com/2024/05/inside-sharppandas-malware-targeting.html