GENI Short Lab: Ransomware

By Marco Lin

2019/11/20

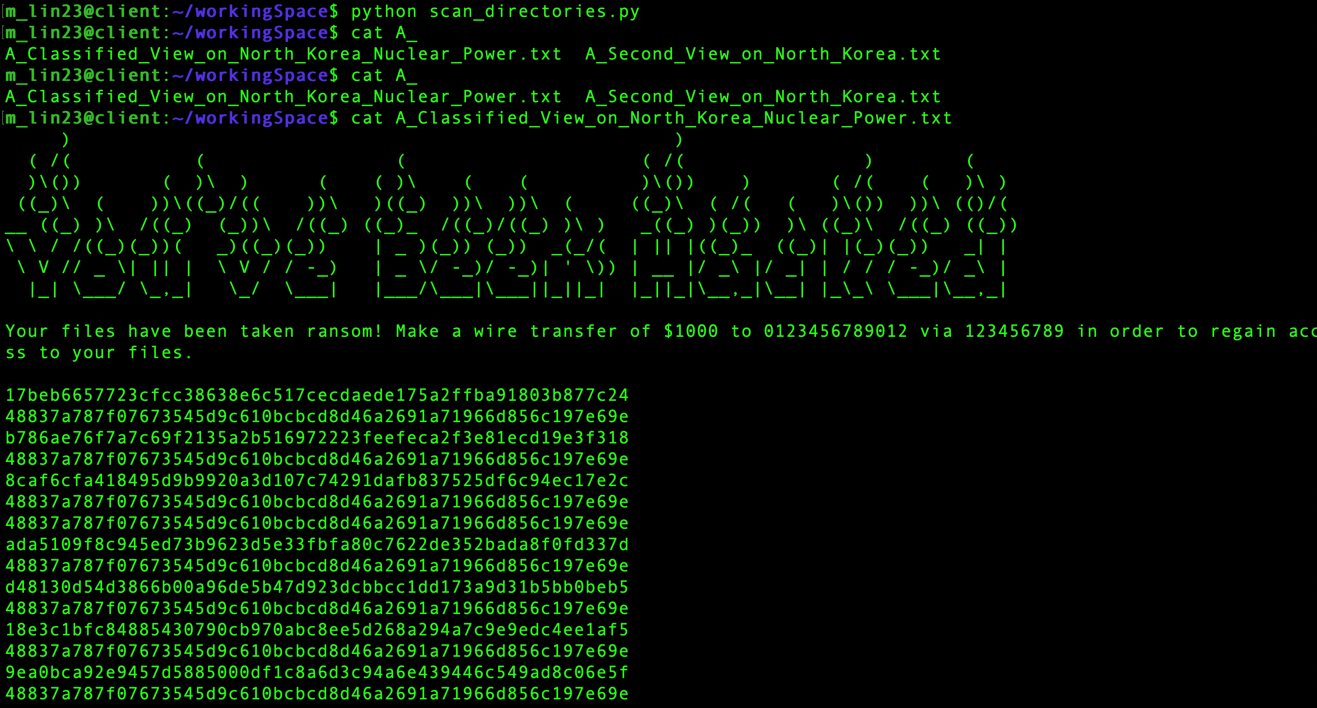
1. **Log into the machine 一張含有 螢幕擷取畫面, 監視器 的圖片

   自動產生的描述**
2. **Find all the files by using the proper directory listing commands and view those files.**

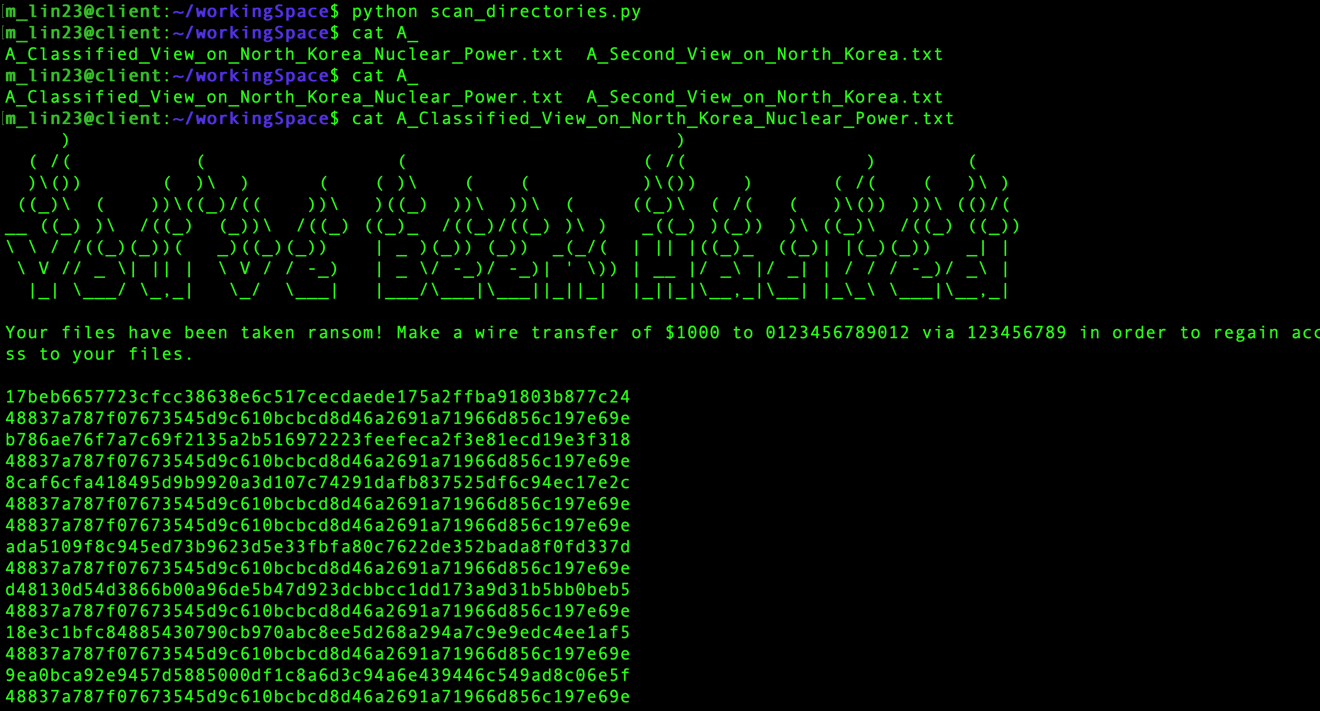
**一張含有 綠色, 室外 的圖片

自動產生的描述**

1. **Run the file scan\_directories.py to scan your machine for viruses by using the following command:**

****

1. **Open the text files again, after the scan\_directories.py has been executed.**

****

1. **What do you think happened? Can you convert the files back to their original form?**

After we run the scan\_directories.py, the program encrypts the text files on my terminal. It depends on situation. If we know the way of encryption, that maybe have chance to covert the files back to their original form. In this case, we know the program uses sha224, we can reverse the process top recovery it.

1. **Open the file scan\_directories.py with your favorite text editor. What do you think this code is doing?**

The code is reading each line in each file and encrypting the files.

**一張含有 螢幕擷取畫面 的圖片

自動產生的描述**

1. **Should you run a file that someone sent you on an email, even if this looks like a file sent by your manager/instructor/ someone you know? Why?**

No, this is because the email may contain this malicious code, and after I run the file, my device may get attack.