

GENI Short Lab: Ransomware

By Marco Lin

2019/11/20

1. Log into the machine

```
marco — m_lin23@client: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 26210 — 80x24
[Enter passphrase for key '/Users/marco/.ssh/id_geni_ssh_rsa':
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * MicroK8s 1.15 is out! Thanks to all 40 contributors, you get the latest
   greatest upstream Kubernetes in a single package.

   https://github.com/ubuntu/microk8s

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

m_lin23@client:~$
```

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

```
m_lin23@client:~/workingSpace$ ls
A_Classified_View_on_North_Korea_Nuclear_Power.txt  Survey_of_Nuclear_Energy.txt  scan_directories.py
A_Second_View_on_North_Korea.txt                    Understanding_Nuclear_Power.txt
m_lin23@client:~/workingSpace$ cat A_Classified_View_on_North_Korea_Nuclear_Power.txt
North Korea's nuclear weapons program has moved back to the front pages with the unprecedented acknowledgement by North Korea during talks this week in Beijing that the North has developed nuclear weapons. News of this revelation came as Assistant Secretary of State for East Asian Affairs James A. Kelly was preparing to leave Beijing for consultations in Seoul, and leaves the future of the talks uncertain and the threat of a potential escalation in tensions on the peninsula high. This is but the latest step in a simmering crisis that began with the admission by North Korea, after being confronted with hard evidence by Assistant Secretary Kelly in October 2002, that it has been pursuing in secret a nuclear weapons program in violation of the Agreed Framework of 1994 and its adherence to the Nonproliferation Treaty (NPT). Pyongyang's subsequent actions in asserting the right to possess nuclear weapons, breaking the seals on its nuclear reactor put there by the International Atomic Energy Agency, withdrawing from the NPT and the expulsion of IAEA inspectors
```

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

```
m_lin23@client:~/workingSpace$ python scan_directories.py
```

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

[illegible]

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 to 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.

