Experience on Investigating Cyber Incident and Enhancing Cyber Security at KINAC

Jeong-ho Lee
KINAC, 1418, Yuseong-daero, Daejeon, Republic of Korea 34101
**Corresponding author: friend25kr@kinac.re.kr*

1. Introduction

Early this year, KINAC experienced a cyber incident. A network management system at KINAC was infected by a malicious software. The malicious software tried to connect a remote host in Bulgaria and to download subsequent files.

This activity draw attention of the cyber security center of the internet service provider. It was an unusual activity to connect and download files from a Bulgarian host at night after all employees left the office. The cyber security center[1] informed the unusual activity to KINAC.

With the notification, KINAC started to look into the suspicious activity and figured out main causes. As we looked into the incident, we figured out points of improvement. In this paper, we would like to share our experience and lessons learned.

2. Notification of Cyber Incident

In the morning of January 6 in 2021, the cyber security division at KINAC got the email from the cyber security center at KISTI. The email contained detailed information on a suspicious activity happened the last night. The suspicious activity was that one system at KINAC tried to connect a remote host in Bulgaria. As well, the cyber security center informed that the suspicious activity was done by a worm virus.

The system, carried out the suspicious activity, was the client of the network management system (NMS) at KINAC. The NMS plays role to monitor servers and network elements at the intranet. KINAC has two NMS in its intranets. One is for the outer intranet, which connects to KREONet [1], the other is for the inner intranet. The system was the client of the NMS for the outer intranet.

3. Investigation of the Incident

As notified the incident, the first measure we took was to isolate the suspicious system from the network and to look into the firewall log to figure out its pivoting activities. We analyzed communication log to find systems which the suspicious system tried to connect. Unfortunately, there was another system that the suspicious system was tried to connect in the outer intranet. We suspected that system was compromised and also isolated it.

Also, we looked into the firewall log to figure out other attempts to connect remote hosts from the infected system. Unfortunately, there was another attempt to connect the Bulgarian host from the same system six months ago. This told us that the system was infected at least six months ago. As well, the system tried to reach hosts in U.S., France, and China from time to time.

The following investigation was on the remote host in Bulgaria. The IP address that the infected system tried to connect belongs to the company called Zetta Hosting Solution [2] in Bulgaria. Several incidents [3] were reported to make use of IP addresses belonging to the company. Especially, one of the IP addresses was used by the hacker called W0rm_M1st [4] in Namibia. We black-listed all IP addresses in the firewall.

Finally, we took a close look into the infected system. The first approach we took was to compare software and files between two NMS clients. As mentioned earlier, there were two NMS, one for outer intranet and the other for inner intranet at KINAC. We assumed the client for the inner intranet NMS was intact. We expected comparing software and files between the infected client and the intact client would provide clues to find the worm virus. Comparing all software and files in two systems was not easy work without automated tool. Fortunately, the compared systems were based on Windows 7, and we could use Windows Sysinternals [5].

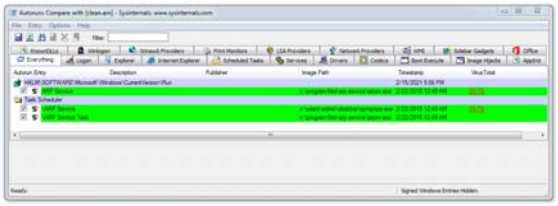

Figure 1. Example of Windows Sysinternals.

Comparing two systems greatly helped us to narrow down suspicious executable files. However, seeking solid evidence was a difficult and consuming job. We connected the infected system to internet monitoring network activities of those suspicious executable files. It was a time-consuming job since malwares were not activated all the time. We monitored those executable files for several weeks and found three malwares.

During the investigation process, we realized several facts. The vaccine software could not help to find any malicious software we found. Thus, we notified the

1 The cyber security center monitors network traffic of Korea Research Environment Open Network (KREONet) at Korea Institute of Science and Technology Information (KISTI). KISTI is the internet service provider of KINAC.

malwares to the vaccine software manufacturer. Also, we found out there were several employees' personal computers to tried to connect the rogue IP addresses. We notified to all those employees to format and reinstall their personal computers.

4. Lessons Learned from the Incident

We learned several lessons from the incident. First of all, we haven't pay attention to security logs from network security devices. The worm virus we found was tried to connect at least twice to the Bulgarian host for six months. We could have detected that activities if we had closely looked at security logs.

Another lesson we learned was that there was a blind spot for security management. The infected NMS client was using Windows 7, which was obsoleted. As Microsoft stopped technical supports on Windows 7, employees' personal computers were upgraded to the up-to-date operating system. However, we found out there were several devices including the NMS clients. As well, as we investigated every device on KINAC intranets, we found out that there were several systems that did not have necessary security software installed and was not applied security policies on.

At last, the painful lesson we learned was that we did not have enough resources to investigate cyber incidents. Even though, we experienced similar incidents couple of time for years, we did not have necessary infrastructure or software tools for conducting cyber forensics. During the investigation, we struggled to set up internet connection isolated from intranets in order to monitor network behaviors of the identified suspicious executable files. Also, we started to collect freeware or open-source software tools for investigation.

5. Conclusion

From the beginning of 2021, KINAC experienced painful cyber incidents. However, from the incident, KINAC learned valuable lessons. For the post incident measures, KINAC re-structured its intranets applying defensive computer security architecture. KINAC divided subnets based on its functions and had been applying security policies. Moreover, KINAC have been improving its own security management.

REFERENCES

[1] https://www.kreonet.net/
[2] https://www.zettahost.com/
[3] https://app.any.run/tasks/5bf0bdfb-423b-4587-8a6b-13b03ce5bafe/
[4] https://mirror-h.org/zone/2043320/
[5] https://docs.microsoft.com/en-us/sysinternals/downloads/file-and-disk-utilities