Transactions of the Korean Nuclear Society Spring Meeting
Gwangju, Korea, May 30-31, 2013

Major Cyber threat on Nuclear Facility and Key Entry Points of Malicious Codes

Ickhyun Shin, Kookheui Kwon
[a]*Korea Institute of Nuclear Nonproliferation and Control, Expo-ro 573, Yusung-gu, Daejeon, Korea 305-348*

1. Introduction

In 2010, Iranian uranium enrichment facility was sabotaged by the malicious code named "Stuxnet". This cyber security incident explicitly shows that the domestic intranet system which is not connected to the Internet can be compromised by the USB based malware which was developed by the state-sponsored group. It also tells that the actor for cyber-attack has been changed from script kiddies to state's governments and the target has been changed to nation's main infrastructures such as electricity, transportation and etc. Since the cyber sabotage on nuclear facility has been proven to be possible and can be replicated again with same method, the cyber security on nuclear facility must be strengthened.

In this paper, it is explained why the malicious code is the one of the biggest cyber threat in nuclear facility's digital I&C(Instrumentation and Controls) system by analyzing recent cyber attacks and well-known malicious codes. And a feasible cyber attack scenario on nuclear facility's digital I&C system is suggested along with some security measures for prevention of malicious code.

2. Cyber Threats on Nuclear Facility

In this section, cyber attack trends extracted from recent cyber incidents and well-known malicious codes are described to show that the cyber threat on nuclear facility is the real that we are facing now and one of the major cyber threats is malicious code. And it is also introduced how easy the malicious code can be infected.

2.1 Cyber Attack Trends

There have been growing cyber threats using malicious code by state-sponsored group or team in recent years. The ROK especially have been cyber-attacked several times in recent 4 years. In 2009 and 2011, major websites were unavailable by the DDoS, Distributed Denial of Service, attack which creates a lot of traffic to targeted websites from Zombie PCs which are infected of malicious code. And in 2011 one of the ROK's major bank was cyber attacked. Bank's main server was compromised through the supplier's laptop which was infected of malicious code downloaded from P2P website.

The attackers of these cyber incidents are believed to be a state-sponsored group and they carried out APT(Advanced Persistent Threat) cyber attacks on specific targets. And the nation's main infrastructures such as government organization, financial company and broadcaster were the main target of cyber attack. And most of the attackers created malicious code and infected PCs to gather information for further attack on main server system.

These characteristics of cyber attack can also be found in global cyber attack trends which can be captured from well-known malicious codes such as Stuxnet, Duqu, Flame and etc. The Stuxnet, as mentioned earlier, was created by the state sponsored group for targeting the Iranian nuclear facility. [1] And the Flame and Duqu codes are also believed to be created by the state-sponsored group and are being used for targeted cyber espionage in Middle Eastern states. [2][3]

2.2 Method of Malicious Code Infection

The attackers have stronger preference for the development of malicious code than directly attacking the company's computer network. This is because that infecting PCs with malicious code is much easier than directly penetrating the computer network installed with several security systems such as firewall, intrusion detection system. And there are a lot of vulnerable web-sites such as gambling, porn, game, P2P on which the attackers can easily implant their viruses. And those are the web-sites that general PC users usually visit and download illegal software which may be included with malicious code.

Once the PC is infected with malicious code, it can be used for DDoS attack or transferring the information within the PC to attacker without the PC user's knowledge. Therefore it is very feasible that the nuclear facility's important information can be sent to an attacker if the administrator's PC is compromised. And the information can be used for making another malicious code for further cyber attack by the attackers.

Therefore it can be easily concluded from the cyber incidents and infection methods that the malicious code is one of the biggest cyber threat on nuclear facility

3. Cyber Attack Scenario and its Prevention

In this section, one of the feasible cyber attack scenarios for digital I&C system of nuclear facility are suggested along with some security measures for

prevention of cyber attack. The scenario is developed based on the previous incidents and current cyber attack trends.

3.1 Cyber Attack Scenario

A very first step for cyber attack on digital I&C system of nuclear facility is to gather information. The attackers need to know how the system protected and designed and composition so that they can later develop facility-specific malicious code. To gather information, they will develop malicious code such as Duqu and Flame which are used as cyber espionage tool and then distribute the code through the vulnerable websites such as illegal gambling, game, porn or P2P and etc. Once the malicious code substitute or attached to the normal file of the website, then the code will be quickly and easily distributed.

And when the code reached to the user of the targeted nuclear facility, the attacker will be able to gather information. Then the attacker can develop the code specially fit to the facility digital I&C system. This code can also be distributed through the same method used when gathering information. But since the Digital I&C computer network is not connected to the outer internet, some media such as USB, laptop is needed to connect to the computer network. When the code is hided into USB in the type of patch file, it will be automatically carry out what the code is supposed to do. And the code will finally fulfill its mission such as sabotage and etc.

3.2 Three Entry Points and Some Security Measures

There is no other proven or known way to cyber-attack the digital I&C system except physically infecting the digital I&C computer network with malicious code. Therefore it is most important that malicious code is not introduced to the computer network of digital I&C.

It is easily seen from the above scenario that there are three entry points which the malicious code can be entered into the computer network. The first entry point is when the general PC connects to the vulnerable websites. And the second point is when the compromised media storage such as USB connects to the PC which is in the corporate intranet. And the last point is when the compromised media storage connects to the PC or Server which is in the digital I&C computer network.

Cyber security measures on the first and second entry point should be to prevent the malicious code so that important data cannot be leaked to the attacker for further attack and malicious code for destructive purpose cannot be delivered to the digital I&C computer network. Some of the security measures are as follows; establishment of media protection policy and procedures, the use of real-time virus checking software, prohibition of access to the illegal websites, provision of malicious code awareness training and etc. And one of the most effective measures could be the separation of intranet and internet.

And Security measures on third entry point should ensure that there are no uncontrolled or unauthorized activities including the use of USB or laptop for maintenance or other purpose. Some of the security measures are as follows; establishment of personnel security policy and procedures, control of use of portable media and storage devices such as USB, laptop, smart-phone and etc, authorization process for access to the server or pc and etc.

Suggested security measures are just small portion of the whole measures. Therefore the important thing is that a lot of security activities should be carried out in this 3 entry points

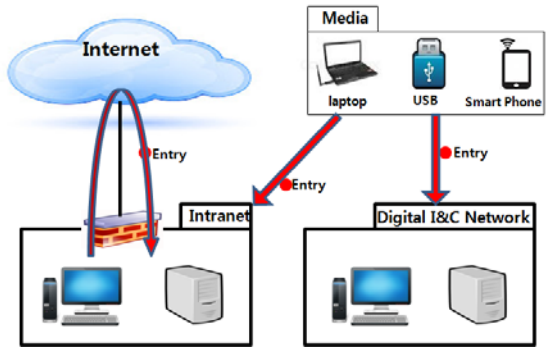

Fig. Entry points of malicious codes in nuclear facility computer networks

4. Conclusions

As experienced from the cyber sabotage on Iranian nuclear facility in 2010, cyber attack on nuclear facility can be replicated by infecting the computer network with malicious codes. One of the cyber attack scenario on nuclear digital I&C computer network with using malicious code was suggested to help security manager establishing cyber security plan for prevention of malicious code. And some security measures on prevention of malicious code are also provided for reference

REFERENCES

[1] Chen, Thomas M., and Saeed Abu-Nimeh. "Lessons from stuxnet." Computer44.4 (2011): 91-93.
[2] Naughton, John. "How the Flame virus has changed everything for online security firms." The Guardian (2012).
[3] Bencsáth, Boldizsár, et al. "Duqu: Analysis, detection, and lessons learned."ACM European Workshop on System Security (EuroSec). Vol. 2012. 2012.