Analysis of Cyber Attacks and Security Intelligence*

Youngsoo Kim[1], Ikkyun Kim[1], and Namje Park[2,**]

[1] Cyber Security Research Laboratory,
Electronics and Telecommunications Research Institute (ETRI),
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
{yskim,ikkim}@etri.re.kr
[2] Department of Computer Education, Teachers College,
Jeju National University, Jeju, Korea
namjepark@jejunu.ac.kr

Abstract. A cyber attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft. Cyber attack is also known as a computer network attack (CNA). Cyber attacks occurred targeting banks and broadcasting companies in South Korea on March 20. The malware involved in these attacks brought down multiple websites and interrupted bank transactions by overwriting the Master Boot Record (MBR) and all the logical drives on the infected servers rendering them unusable. It was reported that 32,000 computers had been damaged and the exact amount of the financial damage has not yet been calculated. More serious is that we are likely to have greater damages in case of occurring additional attacks, since exact analysis of cause is not done yet. APT(Advanced Persistent Threat), which is becoming a big issue due to this attack, is not a brand new way of attacking, but a kind of keyword standing for a trend of recent cyber attacks. In this paper, we show some examples and features of recent cyber attacks and describe phases of them. Finally, we conclude that only the concept of security intelligence can defend these cyber threats.

Keywords: Cyber Attacks, Security Intelligence, MBR, APT, Threat.

1 Introduction

Advanced persistent threat (APT) usually refers to a group, such as a foreign government, with both the capability and the intent to persistently and effectively target a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information, [1] but applies equally to other threats

* This research was funded by the MSIP(Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2013.
** Corresponding author.

James J. (Jong Hyuk) Park et al. (eds.), *Mobile, Ubiquitous, and Intelligent Computing*,
Lecture Notes in Electrical Engineering 274,
DOI: 10.1007/978-3-642-40675-1_73,

such as that of traditional espionage or attack[2]. Other recognized attack vectors include infected media, supply chain compromise, and social engineering. Individuals, such as an individual hacker, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target[3].

APT(Advanced Persistent Threat), which is becoming a big issue due to this attack, is not a brand new way of attacking, but a kind of keyword standing for a trend of recent cyber attacks[1]. Originally, this word was used as a type of specific security threats in US Air Force, but it has been recognized as a new paragon of cyber attacks since stuxnet, which is a malware being used to hack Iran's nuclear power facilities, was found. Stuxnet greatly impacted the society to show the possibility that cyber threats, regarded as one of the group activities for political end before, can paralyze industry control system and cause a large-scale of financial damages.

After stuxnet, similar cyber attacks have occurred all over the world. In 2009, Operation Aurora being used to leak secrets and falsify source codes from more than 30 huge firms such as Google, Adobe, and Juniper, became a diplomatic issue between US and China, since, US claimed that Chinese hackers took lead attacks using this malware, Operation Aurora, but China denied and criticized US. Hacking groups such as Anonymous or LulzSec claiming to stand for Hacktivism have attacked HBGary, a security company, US agencies of FBI and CIA, and subsidiaries of SONY. In 2011, The Night Dragon hacking attacks were targeted at some of the world's largest petrochemical companies, including Shell, Exxon Mobile, BP, Marathon Oil, ConocoPhillips, and Baker Hughes. Numerous critical data in gas and oil area were leaked by this attack. Additionally, EMC/RSA, a security company, was attacked by cyber terror using social engineering methods and classified data of SecureID, OTP(One-Time Password) solution, was stolen. In March of the same year, more than 150 French diplomats' computers were attacked and Paris G20 files were stolen in cyber attack. Furthermore, around 760 firms, including almost 20 percent of the top Fortune 100 companies in the US, turned out to have suffered similar cyber attack, under investigation of hacking case which Lockheed Martin, America's largest defense contractor, was attacked by massive cyber attack.

We can find some domestic examples of cyber attack at ease. 7.7 DDoS attack and 3.4 DDoS attack occurred at July of 2009 and March of 2011 targeting popular web pages and portals, and caused economic losses of 0.4 million dollars. NH's online network paralysis with long-term penetration had become a big issue, because NH's banking services delayed for a few days, and had given rise to need of forensic readiness[2]. Additionally, in 2011, a cyber terror thought to be jamming of North Korea had caused paralysis of wireless networks in northern part of Seoul for a while, and we had become to know that North Korea's cyber offensive skills are as good as or better than their counterparts. Actually, a reporter of Fox news said that North Korean military has around 30,000 electronic warfare specialists and they have become the elite core of the military. He also said that the regime now culls the brightest students from the nation's universities and funnels them into special secret schools that concentrate on hacking and developing cyber warfare programs, and North Korea has the capability to paralyze the US Pacific Command and cause extensive damage to defense networks inside the US.