Spillover Effect of Ransomware: Economic Analysis of Web Vulnerability Market

Jaehee Lee, and Kyungho Lee*
CIST, Korea University, Seoul, Korea
{foodlook, kevinlee}@korea.ac.kr

Abstract

The number of ransomwares reported having increased rapidly since 2013, the range of ransomware victims is expanding beyond its traditional domain of PC users to include firms, hospitals and government organizations; and the technologies used to create ransomware are becoming increasingly sophisticated. This paper conducts time series analysis on software vulnerability price data from SCIP's database vulDB and CVE data from NIST database NVD to find out if the spread of ransomwares around 2013 triggered price changes in software vulnerabilities used to create them. The time frame for our analysis is from 2011 to 2016, and we pay special attention to the time periods before and after 2013, the point of ransomware surges. Our analysis reveals that the number of software vulnerabilities related to ransomware spiked, and that the average price of these vulnerabilities fell during the period between 2013 to early 2014. At the time, there were several events that took place in the security industry that may have triggered these changes. First, there was entry of gray market brokers such as Zerodium and ransomware developers that started to buy up vulnerabilities as selling ransomware on the black market was becoming part of the business portfolio of cyber-criminal organizations. This could have contributed to the increase in vulnerabilities reported, which could also be considered as representative of the number of vulnerabilities traded. Such suspected shift in demand for vulnerabilities, as well as the spread of ransomware around 2013, could have encouraged hackers and security researchers to engage in searching for vulnerabilities and developing their exploits for sale. This would have raised the supply of vulnerability exploits, particularly those relevant to ransomware and imposed a downward pressure on their prices. Overall, our paper offers empirical evidence demonstrating that the market participants affecting software vulnerability market is not limited to software vendors and hackers but extends to cybercrime groups and researchers serving their crimeware demands.

Keywords: Economics of Information Security, Vulnerability market, Ransomware as a service, Empirical analysis of vulnerability market

1 Introduction

In March 2016, an e-mail attaching a Word file was sent to a director in a Korean advertising agency. This director, having overseen a department that frequently exchanged emails with external companies, opened the attached Word file without any doubt. Opening the email, the director encounters an error window. Thinking that the transferred file is broken, the director closes windows of the files he was working on and goes for lunch. Meanwhile, Microsoft Office files (pptx, word, xlsx, etc.) on his computer are encrypted, with their extension changed to locky. The director, now back from lunch, tries to open a 300-page PowerPoint file that he had put together for a meeting scheduled for tomorrow, but finds himself unable to do so. On his desktop is a window suggesting that the data on his computer will be lost unless the director paid bitcoins, and some explanation on how hard it is to decrypt AES-128

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 3, Article No. 20 (November 15, 2017)
*Corresponding author: Center for Information Security Technologies, Korea University, 145, Anam-ro, Seongbuk-gu, Seoul, Korea, Tel: +81-2180-3937

and RSA-2048 encoded data. This happened in a Korean advertising company last March. In recent years, Ransomware has become rampant. While there is a clearly effective way to prevent falling prey to ransomware, not opening emails from unknown email addresses, circumventing ransomware victims has been difficult in practice because operations of most firms, such as the ad company involve frequent email contacts with people from external organizations. Ransomware is a new type of cybercrime that seeks to extort ransom in the currency of bitcoins in exchange for the key to decrypt the encrypted files on the infected computer. Since 2013, the number and types of Ransomware have increased, and there are now many cyber-criminal organizations engaging in its production and distribution. Ransomware makes use of technologies to infect the victim's PC with its malware. The software used here is an exploit kit. A typical example is the ANGLER Exploit Kit of the wildly viral Crytowall ransomwares. In this study, we attempt to find out if the surge of ransomwares since 2013 have had an influence on the price of vulnerabilities whose exploits comprise ransomware exploit kits. We compare the prices of vulnerability exploits consisting of ransomware exploit kits. By doing so, we identify a spillover effect of a security trend over the trade of a group of vulnerabilities, most of which incidentally are of software with large user base. Note that while many security companies and researchers have studied ransomware encryption technologies, the types of ransomware exploit kits, and the status of crime organizations, no research has addressed the implications of the ransomware fad upon the economic dimension of software vulnerability trade.

2 Related Work

2.1 History of Ransomware

The first malware in the form of ransomware was discovered in 1989. The first malware, AIDS Trojan, was distributed by PC Cyborg via floppy disk [2]. In 1996, a document on malicious encryption called "Cryptovirology" was released[13]. In 2005, several ransomwares arose, including Kotten and GPCoder. Among them, GPCoder was the most threatening because it used 1024bit RSA algorithm to encrypt files, rendering data recovery very difficult[12]. In 2012, a large number of ransomware called Reveton was distributed as Fig1[8]. PC users that were victims of Reveton were convinced, as informed by Reveton malware, that the FBI had encrypted their files for legitimate reasons, and made payments to recover their files, only to discover later that Reveton had never actually encrypted their files[8]. According to Brian Krabs, Reveton collected about $1.3 million per a month through such scheme[3]. In 2016, Shadow Brokers who hacked NSA and leaked several kinds of zero-day exploit sold their plunders[9]. Those exploits are developed by NSA researchers, but they didn't report those vulnerabilities. That bring calamity upon oneself. On Friday, May 12, 2017 a large cyberattack was launched using WannaCrypt ransomware. This ransomware targeting Microsoft Windows systems especially using the exploits which were leaked by Shadow Brokers locked over 230,000 computers in 150 countries[6]. Shadow Brokers promised from June to release tools every month to anyone willing to pay for access to some of the tech world's biggest commercial secrets.

2.2 Technical Analysis of Ransomware

Technical analysis of ransomware has been conducted by many security researchers as well as security companies. The Cisco Talos Blog lists the history of ransomwares and details the exploit kit used in creating them[7]. It is important to note that the target of ransomware attack has shifted from PC users to specific target firms; since 2016, there have been numerous ransomwares created to attack specific target firms. For instance, SAMSAM targets the jboss application platform used in US hospital PCs as Fig2. SAMSAM attacks unpatched vulnerabilities, uploading the JSP web shell on the target server

Figure 1: Reveton Warning

and propagating ransomware [4]. Ransomware-as-a-service has thus become part of e-Crime in that ransomware has performed a cost-effective attack aimed at specific companies.

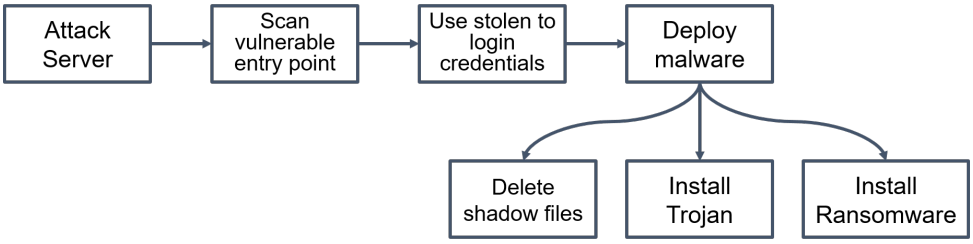

Figure 2: Spread Process of SamSam

2.3 Change of Target

In the past, ransomware targeted random computer users or general corporate employees. But ransomwares since beginning of 2016 appear to have been produced to attack a specific company or industry. The aforementioned SAMSAM was a ransomware attack against hospitals [4]. In recent years, hackers have begun to distribute ransomware to educational institutions as well as hospitaAls. According to Bitsight's recent report, which analyzes ransomware attacks on over 20,000 organizations, about 10% of all education institutions were found to have been under ransomware attack [1]. There have even been ransomware attacks on the police. The files in the system of the Van Stable Police Department were encrypted and the police dispatching software and record management system were paralyzed. As such, the range of targets of ransomware attacks is expanding.

2.4 Ransomware as a service

With the success of ransomware, hackers are reported to have begun selling ransomwares on darknet, no longer limiting their activities to ransomware distribution. According to reports from HEIMDAL Security, ransomwares are nowadays sold for around 39 dollars on darknet[11]. The ransomware called Stampado employs social engineering techniques to infect victims' PCs and requests money, threatening to delete the user's files every six hours if the given ransom is not paid. Locky is a recently released ransomware, and it is reported that the producer or seller of Locky hands it over to those intending to distribute it for a portion of the amount paid by the victim. According to Cisco Talos Research, Locky

attacks 90,000 victims each day, and about 2.9% of victims pay the ransom[7]. If the payment amount is between 0.5 and 1.0 BTC (Bitcoin), the net profit per day is at least 0.5 BTC x 90,000 x 731.51 ($/ BTC) x 2.9% = $954,620 and as high as $1,909,241. Locky distributes ransomware using the Angler Exploit Kit (Angler EK). The amount of ransomware financial extortion enabled by Angler EK is then $60,000,000 per a year[7]. It is worth noting that we are seeing an increase in the value of the Exploit Kit. According to reports from HEIMDAL Security, the Angler Exploit Kit is based on exploits primarily targeting vulnerabilities in Adobe Flash Player. The profit distribution structure of CRYPTOWALL is expressed as the following diagram as Fig3[10].

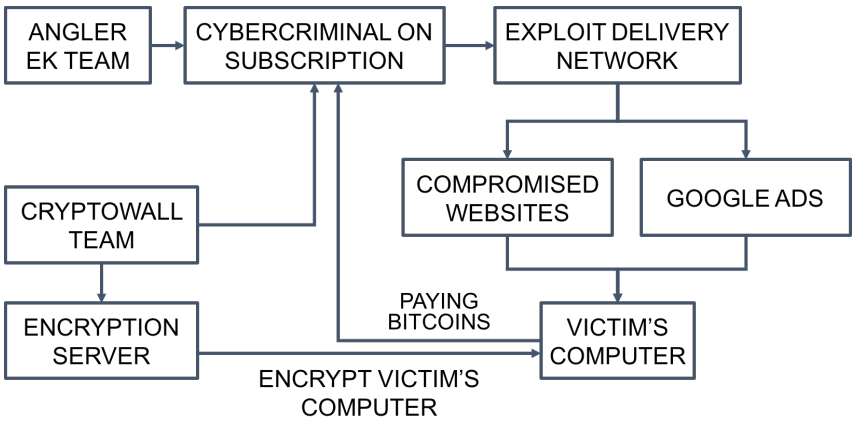

Figure 3: CRYPTOWALL and ANGLER EK Profit Share Framework

This profit distribution structure has raised the value of vulnerabilities involved in ANGLER EK. In this paper, we conduct a study to identify a correspondence between the time of ransomware surges and changes in vulnerability price. We hypothesize that the surge in ransomware attacks affected the vulnerability market, causing changes in price of vulnerabilities used to produce ransomware.

3 Methodology

3.1 Study Goal

The key idea of this paper is to compare the price of vulnerabilities (Adobe Flash, Internet Explorer, MS Word, etc.) frequently used in making ransomware before and after ransomwares started to become popular. In 2013. The purpose of this study is to demonstrate that the fad of ransomware attacks coincided with price changes in vulnerabilities traded in the vulnerability market. Our hypothesis is therefore as follows.

Hypothesis: The price of vulnerabilities will rise around 2013, when there was a notable spread of ransomwares.

3.2 Dataset

Our analysis on the price of vulnerabilities traded in the black market for software vulnerabilities was based on vulDB, database on vulnerability price provided by SCIP. VulDB contains data on prices of vulnerabilities traded from 2011 to November 2016, encompassing information on a total of 42,895 vulnerabilities. We also use data on attack vectors of each vulnerability, and our source of data for this information is NIST's vulnerability database that contains information on the CVSS score of all reported

vulnerabilities. For ease of statistical analysis, we assigned the following values to each measure of the attack vector.

3.2.1 How to collect a vulnerability price

Security consulting group 'SCIP' have been observing the exploit market for more than a decade which allows them to develop a model to predict exploit prices. They call the basic price the "0-day price" which does not consider time-based factors (e.g. disclosure, IDS signatures, patches, etc.) This base price consists of approx. 30 elements. The most important are:

* Vulnerability class
* Network or local attack
* Prerequisites
* Authentication required
* Impact of confidentiality, integrity, availability
* Amount of expected/available exploits
* Popularity of vendor, product and/or vulnerability
* Criticality of the affected product in common environments

It depends how the vulnerability is structured which will define the price level. They have got a team which is monitoring different hacking platforms and the Darknet on a daily basis [more details]. We have quantified the data provided by SCIP. First, the severity of the vulnerability was replaced by numbers from 1 to 3 for each stage as Table1. And we devided the range of vulnerability price and assigned a value per each range as Table2

Table 1: CVSS Score Value

Attack Vector	Attack Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Value
Local	High	Multiple	None	None	None	1
Adjacent	Medium	Single	Partial	Partial	Partial	2
Network	Low	None	Complete	Complete	Complete	3

Table 2: 0-day Price Value

0-day Price	Value
$0 - $1,000	1
$1,000 - $2,000	2
$2,000 - $5,000	3
$5,000 - $10,000	4
$10,000 - $25,000	5
$25,000 - $50,000	6
$50,000 - $100,000	7
$100,000 - $500,000	8

3.3 Research Method

In order to compare the price of Web vulnerabilities traded in the dark market, we collected the price information registered in the vulDB provided by SCIP from January 2011 to April 2016. Based on this information, we conducted time series analysis to observe fluctuations in price of the vulnerabilities used to create ransomware. The independent variable is time, unit being year from 2011 to 2016. This timeframe includes three years before and after 2013, when ransomwares became very popular. The dependent variable is 0-day exploit price. We have calculated the average price using data from vulDB. The control variable was software type.

4 Result

This section presents the results of our research. First, we analyzed the overall fluctuation of price the vulnerability market. Second, we analyzed the price fluctuation of vulnerabilities associated with ransomwares.

4.1 Overall Analysis

We analyzed the vulnerability price changes through the SCIP data since the first report of the vulnerability for the first time. As a result, the following results were obtained as Fig4.

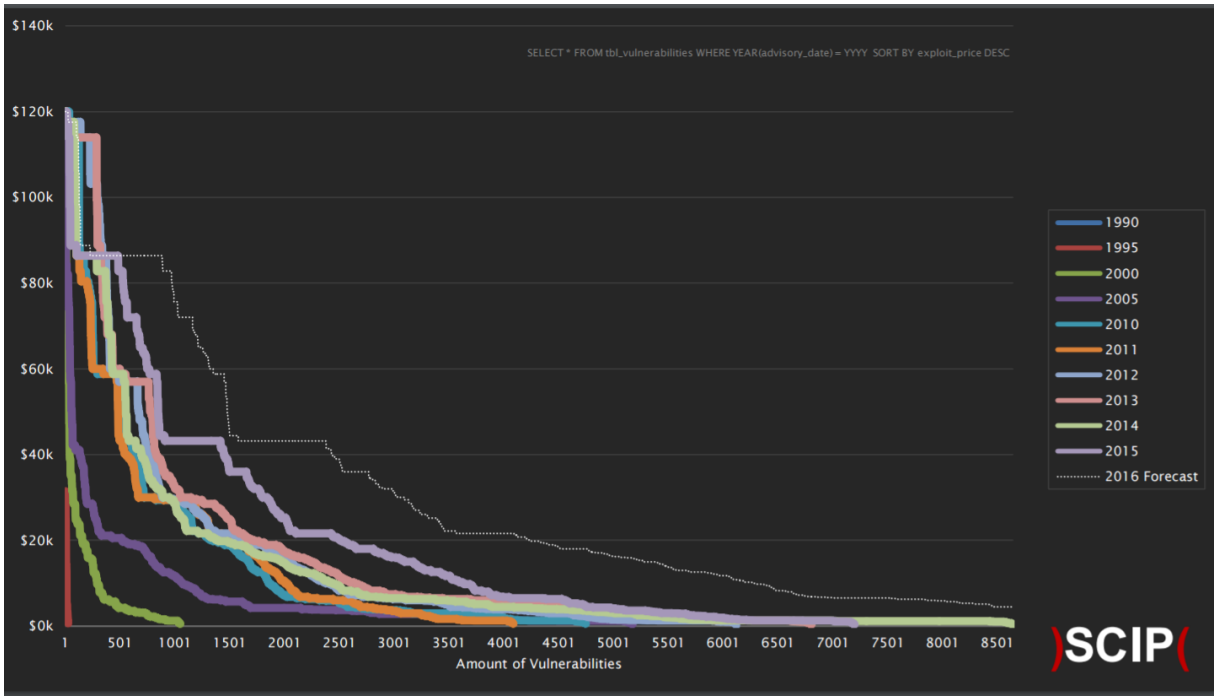

Figure 4: Overall Analysis of Vulnerability Price

The results above show that the price of the vulnerability has been continuing to shift since 1990. SCIP predicted that the price of vulnerabilities would rise significantly in 2016 due to the execution of various bug bounty programs.

Analyzing the average price fluctuation of the vulnerability shows the following results as Table3.

Table 3: Average Vulnerability Price

Year	Attack Vector	Attack Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Price
2011	2.779	2.452	2.850	1.914	1.973	1.973	4.121
2012	2.765	2.283	2.815	1.932	2.010	1.972	3.901
2013	2.698	2.196	2.807	1.930	1.929	1.983	4.115
2014	2.971	2.370	2.682	2.146	2.167	2.093	3.413
2015	2.952	2.684	2.974	2.341	2.176	2.075	4.381
2016	2.595	2.372	2.596	1.870	1.825	1.859	4.415
Average	2.816	2.400	2.780	2.052	2.035	2.006	4.009

The price of the vulnerabilities appears to be determined by their respective CVSS score. Despite that the average value of each CVSS score component element fell in 2016, the average 0-day vulnerability price was the highest in the last six years. In addition, we can confirm that the average price of 0-day had dropped significantly in 2014.

4.2 Vulnerability Related with Ransomware

The purpose of this study is to analyze how the prices of vulnerabilities that are confirmed to have been or likely to be used in ransomware exploit kits have changed. Before analyzing, we investigated to identify the kinds of vulnerabilities used in such exploit kits. Trend Micro's report 'EVOLUTION OF EXPLOIT KITS' was a source of this investigation [5]. This report shows the vulnerabilities used in exploit kits. According to the results show that software whose vulnerabilities were targeted by these exploit kits were Microsoft's Silverlight, Internet Explorer vulnerability, Adobe's Flash Player, Acrobat vulnerability, and Oracle's Java. Based on the results, we identified vulnerabilities among the vulnerabilities listed in our datasets that were or could have been part of the exploit kit. These vulnerabilities amounted to a total of 3922. As we did when analyzing the entire data set, we conducted time series analysis to analyze the trade price of the vulnerability by year. As a result, the results were obtained as Table4.

Table 4: Average Vulnerability Price related with Ransomware

Year	Attack Vector	Attack Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Price
2011	2.572	2.204	2.981	2.336	2.308	2.387	6.451
2012	2.642	1.850	2.829	2.379	2.346	2.383	6.369
2013	2.639	2.023	2.955	2.309	2.282	2.207	6.350
2014	2.984	2.126	2.883	2.194	2.197	2.199	6.604
2015	2.877	2.623	2.988	2.278	2.306	2.184	6.339
2016	2.832	2.093	2.904	2.061	1.988	2.999	6.300
Average	2.812	2.246	2.935	2.232	2.218	2.180	6.390

In the results above, the average price of all vulnerabilities was 4.009, while the average price of vulnerabilities used in Ransomware was 6.390. These indices translate to the following prices: $5,000 to $10,000 for 4.009 of average price of all vulnerabilities, and $25,000 to $50,000 for 6.390 for prices of vulnerabilities associated with creating ransomware. The latter is 5 times as high as the former. This can partly be attributed to the fact that ransomwares tend to employ vulnerabilities in software with large

user base, which enable a greater number of targets to be exploited and hence are usually more expensive that vulnerabilities of software with small user base. The comparison is as Fig5.

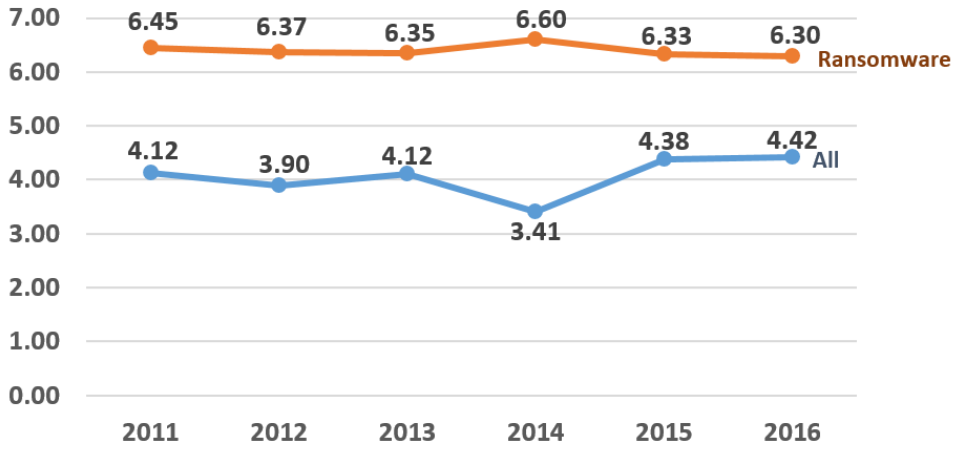

Figure 5: Price Differentials Between Whole Vulnerability and Vulnerability related with Ransomware

Our analysis reveals some interesting points. First, the average price of vulnerabilities increased by 0.254 from 2013 to 2014. However, from 2015, the average price of vulnerabilities in 2015 was below the average of those over the period from 2011 to 2016. Second, it can be seen the average score of Attack Vector increased greatly from 2013 to 2014. The results above suggest that the Spillover Effect of Ransomware is only ending in 2014. However, there are two things that are common in the vulnerabilities used in ransomware: the attack vector of their CVSS scores are mostly network, authentication none, and confidentiality impact partial. Thus, we searched for vulnerabilities that share these characteristics and analyzed their price over the subject years.

Table 5: Average Vulnerability Price of Each Software

Software	2011	2012	2013	2014	2015	2016
Internet Explorer	6.66	6.91	7.15	6.97	6.95	6.70
Microsoft Silverlight	-	-	5.33	-	4.50	5.00
Adobe Flash Player	6.59	6.58	6.82	6.32	6.07	6.09
Adobe Acrobat/Reader	6.39	6.29	5.99	5.87	5.91	6.14
Oracle Java	-	5.91	6.04	6.15	7.21	7.13
Average	6.60	6.71	6.49	6.63	6.37	6.33

Table 6: The Number of Vulnerability of Each Software

Software	2011	2012	2013	2014	2015	2016
Internet Explorer	46	27	118	374	294	105
Microsoft Silverlight	-	-	3	-	4	2
Adobe Flash Player	61	66	58	106	395	253
Adobe Acrobat/Reader	52	7	67	78	66	225
Oracle Java	-	95	949	246	101	171
Average	212	145	423	640	990	706

Unlike our hypothesis, the price of most vulnerabilities declined from 2013, as did their average price. However, the number of reported vulnerabilities and the total number of vulnerabilities increased each year significantly.

- *In case of vulnerabilities of the Internet Explorer, the number of reports also increased by 3.17 times from 118 in 2013 to 374 in 2014. Meanwhile, the average price of vulnerabilities declined from 7.15 to 6.97.*
- *For Adobe Flash Player vulnerabilities, the number of reports also increased by 1.83 times from 58 in 2013 to 106 in 2014. Meanwhile, the average price of vulnerabilities has decreased from 6.82 to 6.32.*
- *For Adobe Acrobat vulnerabilities, the number of reports also increased 1.67 times from 67 in 2013 to 78 in 2014. Meanwhile, the average price of vulnerabilities declined from 5.99 in 2013 to 5.87 in 2014.*
- *For Oracle Java vulnerabilities, the number of reports also decreased from 949 in 2013 to 246 in 2014. However, the average price of vulnerabilities increased by 1.02 times from 6.04 to 6.15.*

Key Findings: With vulnerabilities of the Internet Explorer, Adobe Flash Player and Adobe Acrobat, the average price decreased while their supply increased. With vulnerabilities of Oracle Java, on the other hand, the average price, as did its supply, fell.

4.3 Discussion

The objective of this paper is to compare the price of vulnerabilities (Adobe Flash, Internet Explorer, Oracle Java, etc.) frequently used in ransomware to the that of the average price in software vulnerability market over the time period from 2011 to 2016, thereby identifying a significant price change that coincides with surges in ransomware. A notably significant coincidence of the two could be suggestive of that the rise of ransomware affected the vulnerability market, affecting its price level. Our original hypothesis predicted that the prices of vulnerabilities would soar from 2013, when ransomwares surged. However, unlike our hypothesis, the price appears to have decreased while the supply of the vulnerability increased, possibly due to limited demand. It should also be noted that the number of vulnerabilities that are associated with the exploit kit used in ransomware is increasing rapidly each year. Although this study targets vulnerabilities registered in NVD, it is likely that some of the vulnerabilities traded in the black market through the platform of darknet are not part of our data. Once these vulnerabilities are considered, the number of vulnerabilities traded is expected to be larger than that considered in this paper.

5 Conclusion

This study is important because it shows that the amount of trade of vulnerabilities related to ransomware is increasing. It is possible that cyber-criminal organizations' making of ransomware as part of their profit-making ventures has triggered this increase. The results of this study could be used to design additional research that analyze financial motivations of vulnerability trade in the gray and black market. Such research would be useful for making of policy on expanding the bug bounty programs, run by individual software vendors as well as trade platforms such as Zeroday Initiative and Hackerone. Note that the white market has become increasingly less competitive, with its meager monetary rewards, compared

to the gray and black markets where brokers such as Zerodium pay hefty sums for vulnerabilities. Naturally, hackers are more likely to be attracted to trade vulnerabilities they find in gray or black markets. Especially, in case of software with many users such as Internet Explorer and Adobe Flash, the price they can claim is very high due to the network effect that accompany such software. If it is difficult to secure price competitiveness, it is necessary to restrain the vulnerability of black market through other policy measures. In this study, we did not present a concrete solution, so future research will analyze the intrinsic and extrinsic motivation of hackers and suggest a solution to induce more hackers into the white market.

Acknowledgments

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2017-2015-0-00403) supervised by the IITP(Institute for Information and communications Technology Promotion)

References

[1] A. I. Anton, T. Levin, M. Scholl, N. A. Sokol, N. DFO, et al. Information security and privacy advisory board (ispab), June 2009. `https://www.nist.gov/programs-projects/information-security-and-privacy-advisory-board-ispab` [Online; Accessed on October 3, 2017].

[2] J. Bates. Trojan horse: Aids information introductory diskette version 2.0. *Virus Bulletin*, pages 3–6, 1990.

[3] A. Bhardwaj, V. Avasthi, H. Sastry, and G. Subrahmanyam. Ransomware digital extortion: a rising new age threat. *Indian Journal of Science and Technology*, 9:14, 2016.

[4] R. Brewer. Ransomware attacks: detection, prevention and cure. *Network Security*, 2016(9):5–9, September 2016.

[5] J. C. Chen and B. Li. Evolution of exploit kits. Trend Micro, 2015. `https://www.slideshare.net/ArpITSharma110/evolution-ofexploitkits` [Online; Accessed on October 3, 2017].

[6] J. M. Ehrenfeld. Wannacry, cybersecurity and health information technology: A time to act. *Journal of Medical Systems*, 41(7):104, 2017.

[7] T. Group. Threat spotlight: Cisco talos access to massive international exploit kit generating 60m annually from ransomware alone. Technical report, Cisco Talos, 2015.

[8] M. McCarthy. *Cybercrime and the Law in Ireland: How present is the danger of becoming a victim of cybercrime and how does the law in Ireland act as a protector and a deterrent?* PhD thesis, Dublin, National College of Ireland, 2010.

[9] D. Sanger. Shadow brokers leak raises alarming question: Was the nsa hacked. *New York Times. Retrieved August*, 27:2016, 2016.

[10] H. Security. Angler exploit kit infrastructure analysis - the rundown you need to read. Technical report, HEIMDAL Security, 2016.

[11] H. Security. Security alert: New and cheap stampado ransomware for sale on the dark web. Technical report, HEIMDAL Security, 2016.

[12] S. A. Shivale. Cryptovirology: Virus approach. *International Journal of Network Security & Its Applications (IJNSA)*, 3(4):33–46, July 2011.

[13] A. Young and M. Yung. Cryptovirology: Extortion-based security threats and countermeasures. In *Proc. of the 1996 IEEE Symposium on Security and Privacy (SP'96), Oakland, California, USA*, pages 129–140. IEEE, May 1996.

Author Biography

Jaehee Lee received the B.S. in Physics from Korea University in 2015. Currently he is in master degrees in Korea University. Also he is a senior researcher of Stealien Inc. Recently, he is conducting research on cyber defense area. He is also conducting research on automobile security threats as well as cyber defense.

Kyungho Lee received his Ph.D degree from Korea University. He is now a professor in the Graduate School of Information Security, Korea University, and has been leading the Risk Management Laboratory in Korea University since 2012. He was a former CISO at NHN Corporation, and CEO of SecuBase Corporation.