International Journal of Advanced Science and Technology
Vol.118 (2018), pp.81-94
http://dx.doi.org/10.14257/ijast.2018.118.08

An Empirical Study on Technology Development of EDR-based Multi-Layer Ransomware Defense Platform

Hyung-Taek Lee[1], Soo-Sang Kim[2], Seok-Hee Lee[3], Hoo-Ki Lee[4] and Gwang-Yong Gim[5*]

[1,2,3,4]06978 Dept. IT Policy Management, Graduate School Soongsil Univ., 369 Sangdo-ro, Dongjak-gu, Seoul, Republic of Korea
[5]06978 Dept. Business Administration, Soongsil Univ., 369 Sangdo-ro, Dongjak-gu, Seoul, Republic of Korea
[1]htlee@innotium.com, [2]sskim@comtec.co.kr, [3]chris@lghitach.co.kr, [4]hk0038@korea.kr, [5]gygim@ssu.ac.kr

Abstract

Ransomware, unlike the existing malicious code, encrypts or blocks the data or DB and causes the business interruption. Therefore, the strategic goal of this defense technology is to ensure the continuity of the organization.

This study aims to protect our information assets from Ransomware by developing an economical and effective defense model by combining action-based prior blocking technology, data backup technology, and non-encrypted Ransomware and information leakage malignant code.

And this study examined EDR based multi-layered defense platform (EMRDP) which composed a software authentication algorithm (SAA), behavior based detection, analysis and blocking algorithm (BDA), real - time encrypted security backup algorithm (SBA) as one platform in order to respond to intelligently evolving ransomware attack and overcome limitation of existing ransomware defense system.

As a result of applying a prototype for the proposed model, when the three algorithms (SAA, BDA, SBA) proposed in this model was applied in stages, this study confirmed validated performance verification which detected and blocked 100% of all the 11 kinds of new and variant ransomware.

Keywords: *Ransomware, EDR, Multi-layer Ransomware Defense Platform, SAA, BDA, SBA, EMRDP*

1. Introduction

1.1. Purpose of the Study

The ransomware attack, which is aimed at monetary profit, is strong. According to the Korea Internet & Security Agency (KISA) data, among 1,095 malignant codes that attacked Korea in the second half of 2017, ransomware accounted for 74% of the total, 810, and as the ransomware attacks, evolving into intelligence, diversification, and targeting type, are expected to increase even more, the cyber world can never be safer without solving this ransomware problem [1].

Global security companies and domestic security officials all point ransomware as the biggest security threat also this year. Domestic ransomware damage amounted to 700 billion won in 2017, and it is anticipated that the damage will increase to 1.5 trillion won by 2018, requiring advance prevention [2][3].

Received (January 3, 2018), Review Result (March 20, 2018), Accepted (March 26, 2018)
* Corresponding Author

ISSN: 2005-4238 IJAST

Table 1. Korea Malignant Code Infringement Status in the 3rd~4th quarter of 2017

No.	Malignant code type	Q3 2017		Q4 2017		Total of Q3~Q4	
		Cases	Ratio	Cases	Ratio	Cases	Ratio
1	Ransomware	347	77.0%	463	72.0%	810	74.0%
2	Information capture	44	10.0%	82	13.0%	126	11.5%
3	Remote control	8	1.5%	25	4.0%	33	3.0%
4	Adware	0	-	0	-	0	-
5	Pharming	31	7.0%	21	3.0%	52	4.7%
6	DDoS	0	-	0	-	0	-
7	Downloader	14	3.0%	2	0.4%	16	1.5%
8	Injector	8	1.5%	4	0.6%	12	1.1%
9	Others	0	-	46	7.0%	46	4.2%
Total		452	100%	643	100%	1,095	100%

1.2. Research Objects and Methods

Behavior-based detection and blocking technology that detects and blocks the abnormal behavior process of encrypting data is vulnerable to the new and variant ransomware that is evolving intelligently, which means that new security technology development is urgently needed [3][4]. In addition, ransomware, which is a non-cryptographic method that does not encrypt files, is increasing, but behavior-based technology is vulnerable to this defense, so technological evolution is necessary [4][5].

Ransomware, unlike the existing malicious code, encrypts or blocks the data or DB and causes business interruption. Therefore, the strategic goal of this defense technology is to ensure the continuity of the organization.

This study, based on the analysis of 10,408 ransomware attack types reported by the Korea Ransomware Infringement Response Center (RanCERT) over the past 2 years and 10 months, is going to analyze the weaknesses of existing security technologies to defend ransomware and verify the excellence of the newly designed and developed EDR-based multi-layer defense platform through laboratory experiments and actual user environment experiments [5][6].

2. Related Researches

2.1. Ransomware Classification

Ransomware is divided into indiscriminate attacks distributed indiscriminately via Internet and e-mail based on attack target and targeted attack that attacks specific site.

Indiscriminate attacks are categorized into four types according to data attack types: encrypting ransomware, non-encrypting ransomware, information leakage ransomware (Leakware), and mobile ransomware [6][7].

Encrypting Ransomware means demanding money on the condition for decipherment after encrypting user files without consent. Non-encrypting ransomware is a malignant code that infects computer systems, restricts access, and demands ransom money [3][8]. Information leakage ransomware (Leakware) is a malicious code that leaks user data and threatens to publicly publish user data if the user does not pay ransom money and mobile ransomware is a malignant code which

blocks access instead of encrypting data as it can easily restore data through online synchronization [7][11].

Targeted attack is a malignant code that has data worth paying for money, but they search for companies with vulnerable security in advance and hack into the administrator PC for a long time after illegal infiltration and obtain access authority, encrypts the DB data of the server and demand money[3][12]. Representing targeted attack is Erebus ransomware, which attacked a web-hosting company in Korea in June 2017. With this attack, the Erebus hacker collected KRW $ 1.3 million (USD 1,200,000) in bitcoins, and with the success of this attack, this type of attack is spreading among hackers [20].

2.2. Ransomware Attack Status

Thus, this study analyzed 10,408 cases of ransomware infringement damages reported to the Korean ransomware Infringement Response Center (RanCERT) between 2 years and 10 months (2015. 3 ~ 2017.12) as in [Table 2] by type and victim group.

The ransomwares that attacked Korea in 2015 are 8 different types, which are Teslacrypt2.2 (43%), Crypt0-Locker (38%), Cryptowall3.0 (12%) accounted for 93%, 13 types like Cerber (68%) and Locky (12%) in 2016, 11 types of Cerber6 (73%) and Sage2.2 (15%) in 1~3 quarters in 2017, and 10 types like the variant Magniber (60%) caused serious damage in the 4th quarter of 2017 [3][20].

Table 2. Domestic Ransomware Victim Status [2]

Division	2015				2016				2017			
	1Q	2Q	3Q	4Q	1Q	2Q	2Q	4Q	1Q	2Q	2Q	4Q
Damage Cases	7	378	212	2,081	629	1,390	408	828	992	1,747	981	775
Yearly total	2,678				3,255				4,475			
Total	Ransomware Damage Report from 2015 to 2017 (Unit: case): Total 10,408 cases											

As for the ransomware that caused damages, encryption ransomware by the indiscriminate attack occupies 99%, and as for the damages by device, PC is 99% and the servers and mobile devices is 1% level. The attack scope of this encryption ransomware was not only the data in the user's PC Hard Disk Drive but also the external storage device connected to it, the shared file between the employee PCs, the file shared by the file server, and the database of the server accessible by the user [8][13].

The various types of ransomwares that have indiscriminately attacked PC users have evolved one-step further and is now called WannaCry. This is a hacking tool from the US National Security Agency (NSA) that was hijacked by hackers in May 2017, which infected more than 100 million computers in more than 100 countries around the world one day after its release, putting the entire world into fear of cyber terrorism [6][14].

The attack was a "network worm" that exploited a vulnerability in the Windows operating system's SMB (Server Message Block) remote code, which could spread quickly because the PC or server were infected just by connecting to the Internet.

Also, in June of 2017, 'Internet Nayana', a domestic web hosting company, was attacked by a targeted site 'Erebus' ransomware, and 3,400 websites that entrusted web hosting were shut down as the data saved in 153 servers among 300 servers, and after negotiating with ransomware hacker and paying KRW 1.3 billion, DB was decrypted and normalized [9][20].

2.3. Ransomware Attack Feature Analysis

Ransomware-encoded files are almost impossible to decrypt without the decryption key provided by the hacker, and the penetration technology has evolved further, neutralizing the behavior-based security technology by using the zero-day method without attacking with the same signature pattern and the decoy type is also bypassing. In other words, if defense technology improves, hackers are getting faster in patches and more advanced [10].

Analysis of 10,408 damage records reported to the Korea Ransomware Infringement Response Center for 2 years and 10 months from February 2015 to December 2017 reveals two characteristics. The first is that the work has been stopped because the existing security technologies such as a signature-based vaccine, firewall, and email filter products cannot defend ransomware completely. The second is that only the users who normally backed up could continue their works right away after recovering again. This is that ransomware made a turning point for innovation in traditional security technologies [3][14].

The ransomware attack path has three forms: attack via web browser, attack via spam, attack through TORONTO and P2P [5]. As shown in Table 3 below, the three-year average from 2015 to 2017 shows that 70% of users are infected by Drive-By-Download (DBD) method through a website infected with ransomware while internet surfing, 25% were infected through spam attachment viewing, and 5% were infected by Toronto and P2P (Peer to Peer) methods [2].

Table 3. Analysis of Korean Ransomware Infection Path (2015 ~ 17)

Infection path	Web browser	E-mail Attachments	P2P
Percentage	70%	25%	5%

Ransomware attack targets are analyzed as 11% for home PCs, 25% for small businesses, 42% for small and medium-sized businesses, 4% for middle standing enterprise PCs and servers and 18% for large enterprises and government PCs and servers. This analysis shows that 78% of households, small business owners, and SMEs lacked of budget and manpower, and 11% of middle standing companies, large corporations, and government agencies that can invest in information security, meaning they have very inequitable security [3][20].

Table 4. Analysis of Korean Ransomware Infection Path (2015 ~ 17)

Attack target	Home	Small business	Small and medium companies	Middle standing companies	Large companies/government
Percentage	11%	25%	42%	4%	18%

2.4. Ransomware Encryption Technology Analysis

The encryption technology of ransomware has evolved into three stages as shown in [Table 5]. In the first stage, the decryption key of the encrypted file is embedded in ransomware, so it can be easily decrypted by the cryptographic expert, making it evolved into the 2nd stage, but the vulnerability is also exposed in the second stage, and ransomware hackers developed it to the 3rd stage encryption technology and now the majority of ransomwares distributed now use this technique [6][15].

Table 5. Ransomware Encryption Evolution Phase

Encryption technology evolution phase	[Phase 1] Encryption technology	[Phase 2] Encryption technology	[Phase 3] Encryption technology
Applied technology	• Self-generated encryption algorithm • Save ransomware's own key • Symmetric encryption Decryptability	• Random key generation algorithm • Using RSA • Asymmetric encryption • Encryption of file unit	• Random key generation algorithm • Asymmetric encryption • Receiving C & C Server RSA Key • Decryption difficulty is high

In the analysis of this ransomware encryption method, as shown in [Table 6], it is classified into 5 kinds, such as the original file deleted after encryption file creation, the encryption target file is directly encrypted, the memory variation after mapped in the memory to the encryption target file, and encryption after changing encryption target file name and extension, and a new file change after hard-link creation for encryption [8][16].

Table 6. Diversification of Ransomware Encryption Techniques

Diversification of ransomware Encryption Types	1. Delete the original file after creating the encryption file 2. Direct Encryption of Encrypted Files 3. After mapping to memory for the file to be encrypted, memory modulation 4. Encrypting after changing file name and extension 5. Change the new file after hard-link creation for encryption

2.5. R&D of Various Ransomware Defense System

Traditionally, we have been using signature-based vaccines, firewalls, and email filter products to protect against malignant code, but we have not been able to defend the evolving ransomware based on zero-day attacks. To solve this problem, various types of ransomware correspondence technologies have been developed as shown in [Table 7] below [10].

Representative defense technologies include anti-virus, behavior-based, data backup, APT defense, document centralization based (ECM), and network separation.

Table 7. Domestic Ransomware Defense Technology Status

No.	Defense types	Applied technology	Limitations
1	Anti-Virus	▪ Signature-based blocking ▪ Decoy-based types blocking ▪ Block folder protection encryption ▪ Low cost of introduction ▪ Suitable for SMEs/individuals	▪ Unable to defend against server attack via PC ▪ First Victim on Zero-Day Attack ▪ Unable to defend during ransomware upgrade
2	Behavior-Based	▪ Behavior based zero-day attack blocking ▪ Abnormal process blocking ▪ Low cost of introduction ▪ Suitable for SMEs/individuals	▪ vulnerable in defenses against new/variant ransomware ▪ Vulnerable for normal process injection

3	Data Backup	▪ Backup technology (encryption/incremental backup) ▪ Backup storage protection technology ▪ Blocking/recovering when ransomware accesses ▪ Ensuring uninterrupted business continuity ▪ Suitable for SMEs/individuals	▪ Unable to defend against server attack via PC ▪ Impossible to advance block ransomware attack ▪ Cost of storage introduction
4	APT Defense	▪ Detecting/blocking abnormal behavior ▪ Block parent ransomware ▪ Scan email attachments ▪ Suitable for large companies/institutions	▪ Encryption during normal process injection ▪ Degradation of new/variant blocking rate ▪ High introduction cost
5	ECM	▪ Document centralization / local control ▪ White list-based blocking ▪ Apply diffusion prevention technology	▪ Unable to defend against server attack via PC ▪ PC user data sector infection ▪ Encryption during normal process injection ▪ High introduction cost
6	Network Separation	▪ Physical/logical network separation ▪ Separation of internet and business networks ▪ 10 types related like network-link Including product	▪ ransomware defense vulnerability when using mixed network ▪ High adoption cost (about 1.5 billion won for 500 persons) ▪ Long time to build

Analysis of the defense effectiveness against the introduction cost of the six ransomware defense methods described in [Table 7] shows that the anti-virus and ECM methods have low defense rates and the network separation and APT defense methods have high introduction costs. Behavior-based method and data backup method are relatively high in defense rate and low in introduction cost than other defense method [11][16].

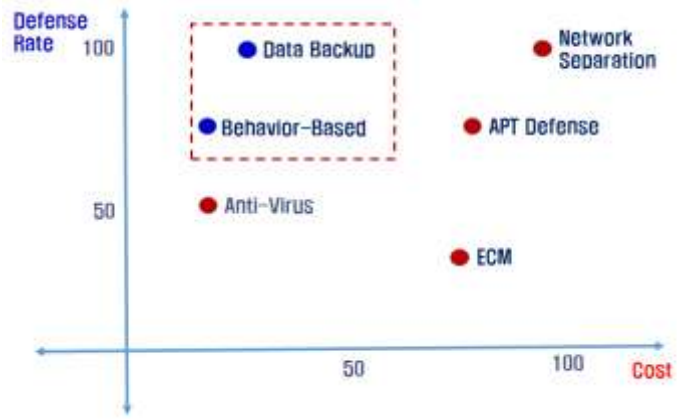

Figure 1. Defense Cost Against Introduction Cost

Each method has merits and limitations, so two or three methods must be introduced at the same time to protect the transcription data from ransomware. In this case, not only the high introduction cost but also the post-construction management cost are increased, and the problem of the organic cooperation among the products cannot be obtained when the problem occurs [12].

As shown in [Figure 1], the majority of domestic victims are SMEs and small business owners lacking budget and manpower, and large corporations and public institutions are relatively better than SMEs, but they are also faced with budget shortages. In order to solve these problems, it is necessary that the multi-layered defense function designed by considering two aspects of the economic efficiency of the introduction of the defense solution and satisfaction of the technical performance is constituted as one defense platform [13][17].

3. Research Model: EDR-based Multi-Layer Defense System against Ransomware Attack

3.1. Highly Available Ransomware Defense System Analysis

Malignant code is a signature-based vaccine that is inexpensive and effective at endpoints, but it is vulnerable to zero-day attacks and cannot effectively defend ransomware, so behavior-based ransomware defense technology that detects and blocks anomalous behavior has been developed.

As shown in Table 8, when signature-based technology is compared with behavior-based dictionary blocking technology, ransomware attacks are characterized as zero-day attacks, while signature-based techniques cannot detect signature, and it can also block the bypass attack. However, the behavior-based technology is not able to treat automatically due to the characteristics of ransomware, and manager intervention is essential [14][18].

Table 8. Signature-Based Technology vs. Behavior-based Proactive Blocking Techniques

Item	Signature-based technology	Behavior-based advance blocking technology
Main product line	Anti-Virus, Firewall, IPS	Behavior Based Products
Detection method	Malignant code signature comparison	Malicious abnormal behavior
New malignant code Detection (Zero-day attack)	Undetectable	Detectable
Malicious behavior detection	Some detection	Detectable
Bypass Attack	Possible	Impossible
Automatic treatment	Possible	Impossible
Administrator responsiveness	None	Administrator judgment is essential

However, this behavior-based technology also has limitations in stopping ransomware, which produces new variants. Based on the latest ransomware testing of products that are considered to be the best defending ransomware, it shows 81% defense success rate [15][19]. This means that behavior-based technologies are also incomplete to defend the evolving ransomware. The conditions and method of testing will be described in detail in Chapter 3 of this study.

Table 9. Ransomware Defense Test of Behavior-Based Dictionary Blocking Technology

Item	Win7	Win8.1	Win10
Magniber(.kgpvwnrj)	○	○	○
Magniber(.vbdrj)	○	○	○
Locky(.asasin)	○	○	○
Locky(.lukitus)	○	○	○
CRBR	○	○	○
Matrix	○	○	○
Sage 2.2	X	X	X
Spora	○	○	○
xzzx	○	○	○
GlobeImposter	○	○	○
xzzx	X	X	X

Behavioral-based technology has a higher defense success rate than signature-based technology, but there is still a 10% vulnerability, so additional defensive technologies need to be fused to compensate this. That is data backup technology. Data backup technology is a prerequisite for resuming business operations in case of emergency against a disaster. Unlike other malware, ransomware encrypts business files and stops work, so business continuity is the most important factor.

Table 10 shows the behavior based proactive blocking technology and data backup technology based on the five categories of business continuity guarantee, stability, convenience, availability and security from the viewpoint of ransomware defense [19].

Table 10. Behavior-based Dictionary Blocking Technology vs Data Backup Technology

Item	Advance detection & blocking	Data Backup
Ransomware response method	Behavior-based advance detection and blocking	Pre-backup and post-recovery
Ensure business continuity	Usual	High
Technical stability	Usual	High
Technical convenience	High	Usual
Technical Availability	High	Usual
Technical Security	Low	Low

Data backup technology has high reliability and stability of work, while convenience and availability are low, security is low, and behavior based technology has high convenience and high availability and low security [20]. Both technologies are evaluated as not being able to defend unencrypted ransomware and prevent information leakage, resulting in poor security.

Therefore, this study aims to protect our information assets from Ransomware by developing an economical and effective defense model with organically combining action-based prior blocking technology and data backup technology, and addition of the technology to defend non-encrypted Ransomware and information leakage malignant code in advance [20].

3.2. Components of the Model

In order to solve the limitations of the existing ransomware defense system, this study suggests models of a software authentication algorithm (SAA), behavior-based detection, analysis and blocking algorithm, BDA), real-time Secure Data Backup Algorithm (SBA), and real-time Central Management System (CMS) to detect and respond to Endpoint Detection & Response (EDR) Based Multi-layer Ransomware Defense Platform (EMRDP) as shown in [Figure 2] below. The functions of each algorithm are as follows:

First, the Software Authentication Algorithm (SAA) is a technology that identifies the threat software in real time when the software is executed, detects the modified type, verifies its reliability, and allows access to important data. It verifies and blocks ransomware or new malignant code aiming information capture through real-time verification of digital signatures and white-list and black-list-based software authentication registered in database (DB) of defense platform.

Second, Behavior-based Detection, Analysis and Blocking Algorithm (BDA) prevents detection, analysis, blocking and spreading of processes that malicious software bypassing SAA level defense accesses and encrypts files.

Third, the Secure Backup Algorithm (SBA) performs backup by encrypting the files and databases newly created and changed events in the system simultaneously to the local and remote repositories in real time. The stored data is safely protected from ransomware.

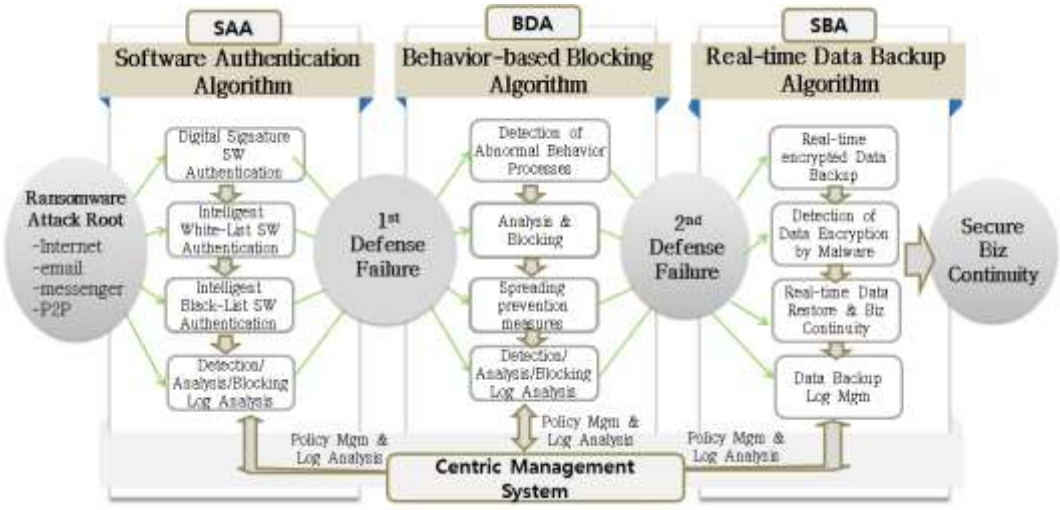

Figure 2. EDR-Based Multi-Layer Ransomware Defense Platform

4. Empirical Analysis

4.1. Experimental Goals

This study developed EMRDP model which is a multi-layer defense platform to overcome the limitation of existing security system which is vulnerable to ransomware defense.

The first goal of the experiment through prototype is to validate SAA by detecting, analyzing and blocking unauthorized malicious software. In cooperation with the Korea ransomware Infringement Response Center, this study adopted and verified 11 types of ransomware such as 10 types of ransomware that caused actual damages for the last 6 months and 1 self-produced ransomware.

The second goal of the experiment is to validate the BDA phase of detecting, analyzing and blocking the anomalous process of accessing and encrypting files and databases in an unusual way bypassing the SAA phase.

The third goal of the experiment is to verify the SBA phase of whether the data in the backup repository is safe from ransomware when the ransomware defense fails in the SAA and BDA phases.

4.2. Configuration of Experiment Environment

The experimental environment consists of three components as shown in [Figure 3]: Centric Server, Backup Storage, and Endpoint Agent.

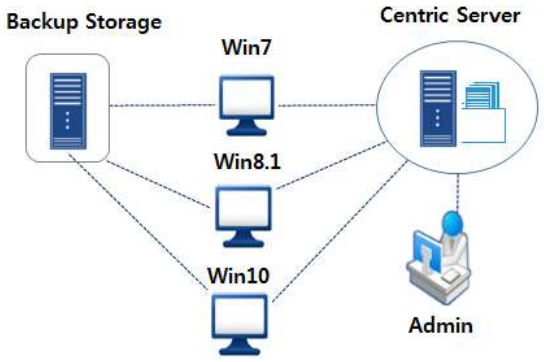

Figure 3. Configuration of Experiment Environment

The three major elements of the experiment were classified into network, hardware, and software as shown in [Table 11], and experimental data included 65 folders, 1,500 files, 10GB capacity, and 12 major extensions. As for an experiment ransomware this study selected eleven types, including 10 types that can operate and 1 type of self-produced ransomware, except for the same hash value among 95 ransomware types collected from October to November 2017.

Table 11. Details of Experiment Environment

Environment configuration	Endpoint Agent	Centrix Server	Backup Storage
Network	External: Dedicate-10M	External: Dedicate-10M	External: Dedicate-10M
	Internal: 100M	Internal: 100M	Internal: 100M
Hardware	CPU : Xeon 2.4GHz	CPU : Xeon 2.4GHz	CPU : Xeon 2.4GHz
	Memory : 64Gb	Memory : 64Gb	Memory : 64Gb
Software	HDD : 1TB SATA	HDD: 1TB SATA	HDD : 1TB * 5EA
	OS: Win 7/8/10	OS ： CentOS 7.2	RAID： 5
Experimental data	65 folders, 1,500 files, 10GB capacity, 12 types of extensions		
Experimental ransomware	Total 11 types 1. Actual attack ransomware: 10 types (Magniber(.kgpvwnr/.vbdrj), Locky(.asasin / .lukitus), CRBR, Matrix, Sage 2.2, Spora, xzzx, GlobeImposter) 2. Self-produced ransomware: 1 type		
Experimental period	2017.11.01. - 2017.11.30. (Weekly experiment)		

4.3. Experiment Result

4.3.1. BDA Performance Verification

In order to compare the performance of the SAA phase with the BDA phase, the BDA phase was first tested. First, Win7, Win8.1, and Win10 OS were installed on the three PCs, and the prototype agent was installed, and then the experiment ransomware was run in order as shown in [Table 12]. The experiment was performed 132 times over 4 times in a week. As a result, it succeeded in detection and interception of 108 times, but with 24 failures, the average was 81%. Ransomware, which failed to defend, was Sage2.2 and self-produced ransomware, but it was found to be vulnerable to the type of encrypting files by direct attack.

Table 12. BDA Performance Verification Result

Item	Win7	Win8.1	Win10
Magniber(.kgpvwnrj)	○	○	○
Magniber(.vbdrj)	○	○	○
Locky(.asasin)	○	○	○
Locky(.lukitus)	○	○	○
CRBR	○	○	○
Matrix	○	○	○
Sage 2.2	X	X	X
Spora	○	○	○
xzzx	○	○	○
GlobeImposter	○	○	○
xzzx	X	X	X

4.3.2. SAA Performance Verification

The performance test of the SAA phase is the same as the BDA phase, and as shown in [Table 13], the experiment was performed 132 times over 4 times in total, and recorded 100% defense rate with success in both detection and blocking. The BDA phase is vulnerable to the type of directly attacking and encryption of files, but it is 100% blocked in the SAA phase, proving the stability of this algorithm.

Table 13. SAA Performance Verification Result

Item	Win7	Win8.1	Win10
Magniber(.kgpvwnrj)	○	○	○
Magniber(.vbdrj)	○	○	○
Locky(.asasin)	○	○	○
Locky(.lukitus)	○	○	○
CRBR	○	○	○
Matrix	○	○	○
Sage 2.2	○	○	○
Spora	○	○	○
xzzx	○	○	○
GlobeImposter	○	○	○
xzzx	○	○	○

4.3.3. SBA Performance Verification

The SBA phase performance test, which verifies the data of the backup repository from 11 ransomware attacks, is performed in the same environment and condition as the BDA phase, and it succeeded in blocking and recorded a 100% defense rate. Both the local HDD repository and the data in the remote repository using VPN were safely protected from ransomware.

Table 14. SBA Performance Verification Result

Item	Win7	Win8.1	Win10
Magniber(.kgpvwnrj)	○	○	○
Magniber(.vbdrj)	○	○	○
Locky(.asasin)	○	○	○
Locky(.lukitus)	○	○	○
CRBR	○	○	○
Matrix	○	○	○
Sage 2.2	○	○	○
Spora	○	○	○
xzzx	○	○	○
GlobeImposter	○	○	○
xzzx	○	○	○

5. Conclusion

5.1 Summary of Research Results

This study examined EDR based multi-layered defense platform (EMRDP) which composed a software authentication algorithm (SAA), behavior based detection, analysis and blocking algorithm (BDA), real - time encrypted security backup algorithm (SBA) as one platform in order to respond to intelligently evolving ransomware attack and overcome limitation of existing ransomware defense system.

As a result of applying a prototype for the proposed model, when the three algorithms (SAA, BDA, SBA) proposed in this model was applied in stages, this study confirmed validated performance verification which detected and blocked 100% of all the 11 kinds of new and variant ransomware.

In addition, ransomware has the characteristic of encrypting data backed up by the network, so protecting the backup storage is very important in terms of ensuring business continuity. In this experiment, it is also confirmed that it protects backed up data by blocking 100% ransomware attack.

Although the defense rate of existing ransomware defense system responded with fragmentary function with low defense rate, it would be meaningful in that this study is suggesting a new direction of research so that users under threats of ransomware can use informationized system safely by composing and developing 4-phase defense platform based on EDR.

5.2 Limitations of Research and Future Research Tasks

Thes empirical results of the EMRDP model proposed in this study were carried out in a laboratory, so there is a limitation to apply the result in actual operational environment for a long time and proving. Also, considering the ransomware characteristic that does not attack with the same pattern, the experiment ransomware is also limited as a sample. Additional empirical researches on the development of technology to defend ransomware attacking DB server is needed in the future

References

[1] Korea Ransomware Infringement Response Center (RanCERT), Ransomware Infringement Analysis Report 2017, **(2017)** January.
[2] H.-T. Lee, "Ransomware Defense Strategic Goals Are Guaranteed for Business Continuity", Newspaper, **(2017)** December 5.
[3] https://en.wikipedia.org/wiki/Ransomware, **(2017)** January 17.
[4] H.-T. Lee, Security Column, "Hospital medical data is dangerous", Hospital Newspaper, **(2017)** June 19.
[5] Korea Ransomware Infringement Response (RanCERT) Center lecture materials, **(2016)** January.
[6] Ransomware Infringement Analysis and Response Strategy, **(2016)** October.
[7] S. Mook Choi, "An Empirical Study on Crawler-based Security Control Model", Doctoral Thesis, Soongsil University Graduate School, **(2017)**.
[8] Korea Internet & Security Agency, Cyber Threat Trend Report for Q4 2017, **(2018)**, pp. 15-16.
[9] H. G. Kim, D. H. Jung, P. G. Jin, C. M. Han and G. B. Kim, "Typification of Ransomware Encryption Pattern and Detection model based on $UsnJnr l", Journal of Digital Forensics, **(2018)** February.
[10] Ransomware Infringement Analysis and Response Strategy, **(2016)** January, pp. 3-8.
[11] G. Won Seo and H. Won Kim, "Types and trends of the ransomware", Journal of Korea Information Science Society, **(2016)** June, pp. 1116-1117.
[12] H.-T. Lee, Security Column, "The strategic goal of Ransomware defense is to ensure business continuity", Korea Electronic News Paper, **(2017)** December 5.
[13] S.-M. Ha, T.-H. Kim and S. Jung, "Design and Implementation of a Cloud-Based Recovery System against Ransomware Attacks", Journal of the Korea Institute of Information Security & Cryptology, vol. 27, no. 3, **(2017)** June, pp. 521-530.
[14] J. Hyun Kim, K. Sung Park and Y. Ho Park, "A study of vulnerability analysis of ransomware detection techniques", Proceedings of Symposium of the Korean Institute of communications and Information Sciences, **(2017)** June, pp. 590-591.
[15] J.-m. Youn, J.-g. Jo and J.-c. Ryu, "Methodology for Intercepting the Ransomware Attacks Using File I/O Intervals", Journal of the Korea Institute of Information Security & Cryptology, vol. 26, no. 3, **(2016)** June, pp. 645-653.
[16] H.-s. Yoon, K.-h. Song and K.-H. Lee, "FAIR-Based BIA for Ransomware Attacks in Financial Industry", Journal of the Korea Institute of Information Security & Cryptology, vol. 27, no. 4, **(2017)** August, pp. 873-883.
[17] J.-W. Kim, S.-H. Ji and S.-R. Kim, "A Machine Learning based Ransomware Detection Model using a Hybrid Analysis", Journal of Security Engineering, vol. 14, no. 4, pp. 263-280.
[18] http://www.earticle.net/article.aspx?sn=315242, **(2017)** December 1.
[19] https://thehackernews.com/search/label/zero%20day, **(2017)** December 1.
[20] Innotium, Multi-Layer Defense Solution for Ransomware Attack, 2018 Ransomware Defender Conference, **(2018)** February.

Authors

Hyung-Taek Lee, (htlee@innotium.com)

He works as a CEO at Innotium Inc, Development Company for Ransomawre Defense and Data Security and he works for Ransomeware Infringement Response Center (RanCERT), and he is studying in Soongsil University Graduate School of IT Policy Management. His research areas are Cyber Security, Data Security, Cloud Plaform, Big Data, Artifical Inteligence, and Software Engineering.

Soo-Sang KIM, (sskim@comtec.co.kr)

He works as a managing Director at Comtec Information Co., Ltd, System Integration Service company. And he is studying in Soongsil University Graduate School of IT Policy Management. His interests are Network Security, Blockcahin, SDN, SDDC, Cloud Plaform, Big Data and Artifical Inteligence,.

Seok-Hee Lee, (chris@lghitachi.co.kr)

He works as a Managing Director at the Department of Solution & Service Business Division at LG Hitachi Ltd. and he is studying in Soongsil University Graduate School of IT Policy Management. His research areas are IoT, Big Data, Fintech, and Payment Solution with Biometrics, etc.

Hoo-Ki Lee, **(**hk0038@korea.kr)

He works as a cyber security expert at the Ministry of Culture, Sports and Tourism. Dr. Lee has been interested in research on Cyber Security, Information Security, Information system disaster recovery, and Malicious code analysis. He published various papers on cyber security in the journal.

Gwang-Yong Gim, (gygim@ssu.ac.kr)

He works as a professor at the Department of Business Administration of Soongsil University. Dr. Gim has been interested in research such as 4th Industry Revolution, ICT ODA, intellectual property rights, service science, big data analysis, S/W industrial policy, and open innovation. He published a number papers on journals such as Information Science, Fuzzy sets and System, journals of society of management information systems, and journals of management science.