

# APT attack response system through AM-HIDS

Seoung-Pyo Hong\*, Chae-Ho Lim\*\*, Hoon Jae Lee\*\*\*

\*Department of Ubiquitous IT, Dongseo University, Busan 47011 Republic of Korea

\*\*Bitscan INC, Seoul 04789 Republic of Korea

\*\*\*Division of computer engineering, Dongseo University, Busan 47011 Republic of Korea

debiii@naver.com, skscogh@naver.com, hjlee@dongseo.ac.kr

**Abstract**— In this paper, an effective Advanced Persistent Threat (APT) attack response system was proposed. Reference to the NIST Cyber Security Framework (CRF) was made to present the most cost-effective measures. It has developed a system that detects and responds to real-time AM-HIDS (Anti Malware Host Intrusion Detection System) that monitors abnormal change SW of PCs as a prevention of APT. It has proved that the best government-run security measures are possible to provide an excellent cost-effectiveness environment to prevent APT attacks.

**Keywords**— APT, AM-HIDS, Malicious, Anti, White List

## I. INTRODUCTION

The non-face-to-face telecommuting system is being activated due to the COVID-19 epidemic virus. Remote access is a RAT(Remote Access Terminal) function, and the US-CERT of the US DHS has also issued a warning that it is being exploited by malicious cyber actors of COVID-19[1].

The content of COVID-19 is used as a bait to distribute malicious code using phishing, and domain registration including corona-related phrases, and remote working infrastructure are the main targets of attack. Google has been announced as “more than 200 million corona-related cyber attack attempts every day”[2]. APT attack is a social engineering technique that induces user clicks and executes remote access. “It is not an exaggeration to say that North Korean hackers are always with Koreans.” [3] In the report, “there are the KHNP hacking, the 3-20 computer turmoil, and the Nonghyup computer network paralysis. There are also reports such as the Aegis ship-submarine blueprint and the North Korean hacker.”[4] Military hacking attempts are also very serious, with 95,000 cases a day [5].

In the simulated hacking of organizations A and B, they experienced 1) RAT code production, 2) social engineering penetration, and 3) internal network transmission. Institution C blocks e-mails at the source, discovers and invades web application vulnerabilities, and sees more infected PCs in the internal network. The vaccine cannot detect the new APT. It is based on the known MD5 (Message Digest), and the attack bypasses the vaccine. As shown in Table 1, the target code is classified into the White List, Black List, and Gray List, and reverse engineering is analyzed in the gray list classified as abnormal.

TABLE 1. WHITE LIST RULE DATABASE

| List       | Description                                                                                                                   |
|------------|-------------------------------------------------------------------------------------------------------------------------------|
| White List | Host, Port Number, List of application that exist in the system based on the execution time process and well-defined criteria |
| Black List | List already determined to be associated with malicious activity                                                              |
| Grey List  | Individual lists that have not yet been set to malware                                                                        |

An internal PC is exposed to an unauthorized URL (URI) on the external Internet. A user clicks from the external Internet to infect. Recently, there is a lot of pornography. Inside your organization, you have to find a way to detect external malicious URLs (URIs) and provide a real-time Black List. In order to respond to these attacks, it is a matter of operating and providing the Black List for Web servers, and how often should it be detected? Is the problem. Table 2 summarizes cyber threats for the time being and shows the direction of APT countermeasures for each threat.

TABLE 2. CYBER MALWARE BEHAVIOR CLASSIFICATION IN KOREA

| Cyber threat                 | Description                      | Remark                   |
|------------------------------|----------------------------------|--------------------------|
| APT (PC HD)                  | Send E-mail (phishing)           | SW Access Control        |
| APT Malicious Web (URL)      | Malicious URL Use (3-20 terror)  | Black-List               |
| APT (Mobile)                 | Malicious URL use                | Further study            |
| SW Code vulnerability attack | Scan and then attack immediately | Safety code verification |

## II. RELATED RESEARCH

APT[6] refers to a country or group that has long-term undiscovered unauthorized access to the targeted system. have a security threat of C.I.A. (Confidentiality, Integrity, Assurance) of malicious code that is for political and

economic reasons and that steals, intercepts, or interferes with economic foundations. The targets include government, defense, finance, industry and telecommunications, and are not detected using intelligent attack vectors such as social engineering. The average stay time of APT is reported as 71 days, 177 days and 204 days.

In particular, APT 38 and APT 37 were reported as North Korea's APT activities [7]. APT is divided into 1) Reconnaissance, 2) Preparation, 3) Targeting, 4) Other Access, 5) Data Gathering, 6 and Maintenance procedures [8]. Figure 1 shows a model for preventing and detecting APT. Since it is usually run on a PC, von Neumann presents a defensive model according to the computer structure.

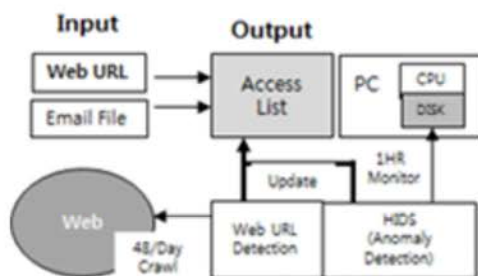


Figure 1. System model

The Cybersecurity framework is applied to this paper as a U.S standard. Table 3 presents a cross-cyber security framework.

TABLE 3. NIST CYBER SECURITY FRAMEWORK

|                      | Description         | Paper Apply              |
|----------------------|---------------------|--------------------------|
| Asset Identification | Goal Identification | Web URL<br>Hard Disk     |
| Protect              | Access Control      | Black List               |
| Detection Analysis   | Detection Technique | Regex.<br>Anomaly Detect |
| Response             | Accident Response   | Attacker Response        |
| Repair               | Accident Handling   | Asset Repair             |

### III. APT MEASURE

While the organization is using vaccine AVS, attackers mostly bypass Anti-Virus System (AVS). In Virus Total, which incorporates AVS technology around the world, an attacker validates AVS technology and modifies RAT (Remote Access Terminal) tools, etc. to make a variant virus without having to make a separate code to prevent them from being detected by AVS. AVS assumes only known detections and assumes real-time presence in the Black List. The White List assumes the existence of a unique White List for each individual organization, since the verified SW in the organization is different from each other.

Malicious code analysis can be classified into four categories: static analysis, dynamic analysis, automation analysis, and detailed analysis. In this paper, the technical system using static analysis is described as the same as the existing vaccine. Every file has its own hash value or has its own API and string. For hash values, the results can be obtained by comparing them with engines of many vaccines, such as Virus Total. This analysis is a normal behavior detection technique.

Vaccines in Korea include V3 Lite, pills, and virus chasers, while foreign vaccines typically include Avast and Microsoft Defender, which are built into Windows 10. The content described in this paper has the same method of detecting with existing vaccines, but only modified programs are examined, except those previously examined during the second examination after the first examination, as shown in Figure 2. In this area, the inspection time can be greatly reduced, and the detection rate can be further increased by conducting the inspection at intervals of one hour from the beginning of the initial inspection. membership of any professional organization (e.g. Senior Member IEEE).

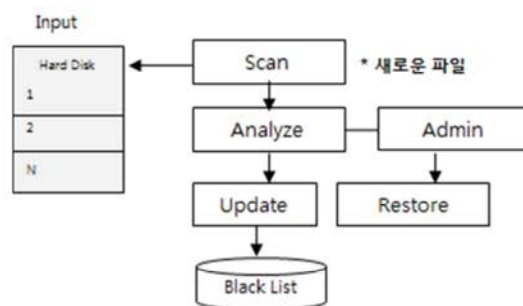


Figure 2. HIDS Model

The methods presented in this paper show the same or similar strings in the case of malicious codes. First, define the string as White List in the normal program, and define the string extracted from the malicious code as Black List. The way the entire file was scanned was by subdirectory search using Java recursive. After changing the retrieved file to binary string among Java libraries, normal/unusual classification was done through a comparison process with the normal program strings. During the first and second inspection of the program, only the modified program was classified as normal and abnormal, eliminating unnecessary time to process files without content changes. Adds a newly discovered malicious string to the Black List. Table 4 shows the White List, which uses the 'Bintext' program to extract program strings to extract normal program strings.

TABLE 4. STRINGS EXTRACTED FROM NORMAL PROGRAMS

| White List                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------|
| @shell32.dll, NOTEPA~1.EXE, !This program cannot, be run in DOS mode, .text, RegCloseKey, .rsrc, @.reloc, VS_VERSION_INFO, [apturer, mscorlib |

The process of comparing normal program strings with malicious code strings is the most basic method in static analysis. But it is also the fastest way to check. The inspection time can be greatly reduced by examining only the modified data except the previously inspected test data. The method presented in this paper is the same as the first test, but only the modified data is examined as seen earlier from the second test. Figure 3 illustrates the data capacity that Windows Defender and the method proposed in this paper are used to check the entire file on the same hard disk. The first starting point starts at the same point at 100% pre-capacity, since both methods require the entire file to be scanned. Subsequently, the proposed method would only perform a check on the modified files, which would result in a sharp drop in processing capacity.

Table 5 above shows Window Defender for 456.19GB of files and the processing speed of malware detection in the method proposed in this paper. Reduce time by about 6.5 times.

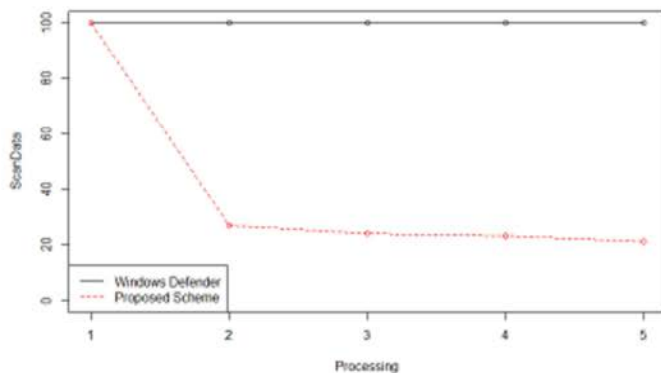


Figure 3. Processing Data Volume Comparison

TABLE 5. COMPARISON OF PROCESSING TIME

|                  | Capacitive | Processing Speed |
|------------------|------------|------------------|
| Windows Defender | 456.19 GB  | 39sec ~ 42sec    |
| Proposed Scheme  |            | 6sec ~ 9sec      |

Figure 4 shows the processing speed of the two methods compared. The proposed method of method did not make any technical changes. It can be seen as excellent in terms of speed to re-examine only changed files, such as changes in files from the criteria for scanning the entire file and modified dates. Windows Defender performs well when scanning entire files. However, as mentioned earlier, the string comparison analysis is performed with only the changed contents. Future tasks are expected to increase the detection rate by upgrading more detailed analysis, hash value comparison, and analysis algorithms.

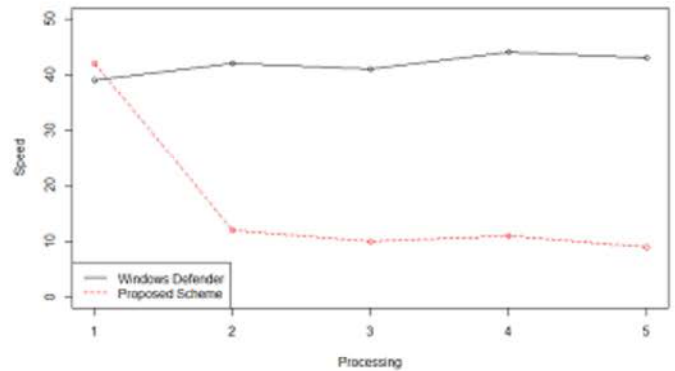


Figure 4. Processing Speed Comparison

As we saw earlier, the inspection process will be carried out every hour, enabling rapid response even if the internal PC is infected. Most importantly, identifying unknown abnormalities through normal behavior profiling measures the victory or failure of national cybersecurity and is an issue that requires a lot of research across all industrial sectors.

#### IV. CONCLUSIONS

In this paper, As malicious codes become more advanced, hackers use e-mail the most as a major means of infiltrating into the government, businesses, and organizations. There are many e-mail infections, but infection through Web malicious URLs is more important. As the threat of attacks on e-mail and Web malicious URLs increases, companies are raising the system security level, but companies are rarely able to recover. The deadliest threat to companies is social engineering hacking techniques. Social engineering techniques should be recognized and prepared by all employees, including security personnel, to prevent and minimize damage. The AM-HIDS-based APT measurements presented in this paper are expected to be the most cost-effective.

#### ACKNOWLEDGMENT

This is research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology grant number:NRF-2016R1D1A1B01011908

#### REFERENCES

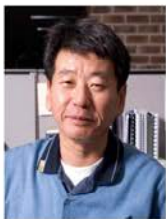
- [1] "The Cybersecurity Skills Crisis in Numbers.",Trustwave, accessed Feb 16, 2016, <https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/the-cybersecurity-skills-crisis-in-numbers/>
- [2] "The U.S.Hits the 9-Million Mark as Infections Keep Surging",The New York Times, accessed Oct 30, 2020, <https://www.nytimes.com/live/2020/10/29/world/covid-19-coronavirus-updates>
- [3] "Five Hacks Showing North Korea's Cyber Warfare Capabilities",BBC News, accessed Oct 12, 2017, <https://www.bbc.com/korean/news-41584327>

- [4] "Aegis-Submarine Design Diagram, Stolen by China Hacker", dongA, accessed Oct 31, 2017, <http://www.donga.com/news/article/all/20171031/87033410/1>
- [5] "95,000 military hacking attempts a day", Hani, accessed June 16, 2009, <http://www.hani.co.kr/arti/PRINT/360750.html>
- [6] "M-Trends 2019: Celebrating 10 Years of Incident Response Reporting", FIREEYE, accessed Mar 04, 2019, <https://www.fireeye.com/blog/executive-perspective/2019/03/mtrends-2019-celebrating-ten-years-of-incident-response-reporting.html>
- [7] Sulwha Lim, Jongsoo Kim, Junkeun Yang, Chacho Lim. (2014). APT status and new malicious code countermeasure. Journal of Information Security Society, 24(2), 63-72
- [8] "Advanced Persistent Threats: A Decade in Review", Command Five, accessed, June 2011, <http://cml1989.tistory.com/attachment/cfile28.uf@256A373A54334BB406ACCD.pdf>



**Seoung-Pyo Hong**

He received the B.S., degrees from Dept. of Computer Engineering, Dongseo University, South Korea, in 2020. Since 2020, he is currently a Master course in the Dep. of Computer Engineering, Dongseo University, South Korea. His research interests include Digital Forensic, Malicious Analysis, Computer Security



**Chae-Ho Lim**

He received the B.S degree in Computer Science and Engineering(CSE) from Hongik University in Korea 1996 and his received the M.S degree in CSE from Konkuk University in 1999 and his received the Ph.D degree in CSE from Hongik University in 2000, His resarch interests are in the security topic of Internet Security and Software Security and Risk Management



**HoonJae Lee**

He received the B.S., M.S. and Ph.D. degree in Electrical Engineering from Kyungpook national university in 1985, 1987 and 1998, respectively. He had been engaged in the research on cryptography and network security at Agency for Defense Development from 1987 to 1998. Since 2002 he has been working for Department of Computer Engineering of Dongseo University as an associate professor, and now he is a full professor. His current research interests are in security communication system, side-channel attack, USN & RFID security. He is a member of the Korea institute of Information security and cryptology, IEEE Computer Society, IEEE Information Theory Society and etc.