TECHNICAL SESSION 3 (14:30~15:45)

• Usability of Software Weakness Discovery based on the Binary File Visualization
/ Keon-Ho Park, Sang-Hoon Choi, Chul-Woo Kim, Ki-Woong Park
/ Sejong University, Pace University / Korea

• Education Measurement and Academic Planning Case Study of Information and Production Technology Management Department
/ Hathairat Ketmaneechairat, Rathartip Jaijing, Anusorn Kalapakdee, Kannika Kaewthong
/ King Mongkut's University of Technology North Bangkok / Thailand

• Detecting Ransomware with File System-Awareness Scheme in Cloud Computing Environment
/ Woo-Jin Jeon, Sang-Hoon Choi, Ki-Woong Park
/ Sejong University / Korea

• Integration of Curvelet transform and Probabilistic principal component analysis for detection of Alzheimer's disease and pathological brain image
/ Debesh Jha, Goo-Rak kwon
/ Chosun University / Korea

• Interactive Dance Performance System Based on Wireless Wearable Gesture Sensing Device
/ Guan-I Lin, Chien-Wen Cheng
/ National Taipei University of Technology / Taiwan

Detecting Ransomware with File System-Awareness Scheme in Cloud Computing Environment

Woo-Jin Jeon, Sang-Hoon Choi, Ki-Woong Park*
SysCore Lab., *Dept. of Computer and
Information Security
Sejong University
Seoul, Korea
woojinjeon929@gmail.com, csh0052@gmail.com, woongbak@sejong.ac.kr*

***Abstract*— Ransomware is an attack that infects computer systems and encrypts files or devices to restrict user access. Because these attacks can also be applied to cloud computing environments, we thoroughly analyzed previous Ransomware detection works to find suitable Ransomware attack detection methods for cloud computing environments. As a result, we found two major problems. The first problem is high system overhead when detecting Ransomware attacks. The second problem is that new or variant Ransomware can attack by bypassing commonly used signature or behavior-based detection solutions. In this paper, we propose a method called FACE that can detect Ransomware attack in a more efficient manner through the file system-awareness scheme in a cloud computing environment. FACE aims to minimize the overhead of monitoring and analysis and to block detection bypass. The experimental results of our scheme show that disk performance has a penalty of 0.3% less than when do not monitored.**

Keywords—Cloud Computing, Disk Monitoring, File System, Ransomware

I. Introduction

Ransomware has widespread since the advent of CryptoLocker in 2013 [1, 2]. As Ransomware attacks increase, many works have been conducted to defend them. In these works, methods such as signature-based detection [3, 4, 5] and entropy detection [6] have been proposed. However signature-based detection methods are difficult to detect new or modified Ransomware that bypasses detection. In addition, entropy measurement whenever disk reads and writes occur can result in significant system overhead. As a remedy to these problems, we have profiled various tasks that Ransomware performs. As a result, we verified that the file system metafile changed when Ransomware was running. With this feature, Ransomware can be detected efficiently.

In this paper, we present a Ransomware detection method, FACE, based on file system-awareness scheme in a cloud computing environment [7]. The proposed method extracts and detects the feature that the file system metadata is changed when Ransomware encrypts the file. With this approach, which can avoid drawbacks of previous detection methods.

*: Corresponding Author (Ki-Woong Park, woongbak@sejong.ac.kr)
This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (NRF-2017R1C1B2003957)

The composition of the paper is organized as follows: In Section 2, we discuss relevant works. In Section 3, we present the framework for detecting a Ransomware in a cloud computing environment using file system metadata that changes according to file events. In Section 4, we evaluate the performance of our implemented Ransomware detection system. Finally, we present the conclusions in Section 5.

II. Related Work

In this section, we analyze and classify the previous works related to Ransomware detection and draw out the limitations.

A. Behavior-based Ransomware Detection

CryptoDrop, proposed by Scaife, Nolen, et al. in 2016, is an early-warning detection system that alerts users during suspicious file activity by analyzing a series of actions that must be performed in order for Ransomware to work [8]. The system provides a metric to detect and calculate these entropy measures by capturing the entropy of the read / write operation. This detection system can detect variant Ransomware that may not be detected in signature scanning. However, a significant amount of overhead required for performing monitoring to measure entropy.

B. Ransomware Detection over the Entropy Measurement

In 2016, Kharraz, Amin et al. proposed UNVEIL, a novel dynamic analysis system that detects the operation of the Ransomware by automatically generating an artificial user environment [9]. This method can specifically identify the behavior of Ransomware. However, a large amount of system resources are consumed in the process of generating an artificial user environment and performing dynamic analysis. Therefore, the detection performance is degraded.

III. Design of the FACE

In this section, we present the overall architecture and detecting mechanisms of FACE. FACE works in the cloud computing environment on the host system and can detect Ransomware attacks on user instances. It is also designed to minimize the overhead of detection.

In this work, NTFS (New Technology File System) was selected as a case among various file systems. However, this work can be extended to various file systems that provide journaling metadata [10] values.

A. *Monitor the Metadata of File System*

The meta regions of the file system is generally structured to store and manage all information related to file events. Therefore, information such as file rename, modification, deletion, and encryption can be obtained through metadata, and such data is classified into each meta property.

Ransomware executes a malicious script and finds the file on the user PC and encrypts it. When encryption is performed, the metadata of the file system changes. Therefore, by monitoring only the metadata regions in which the encryption log is recorded, it can be detected more efficiently than previous detection methods.

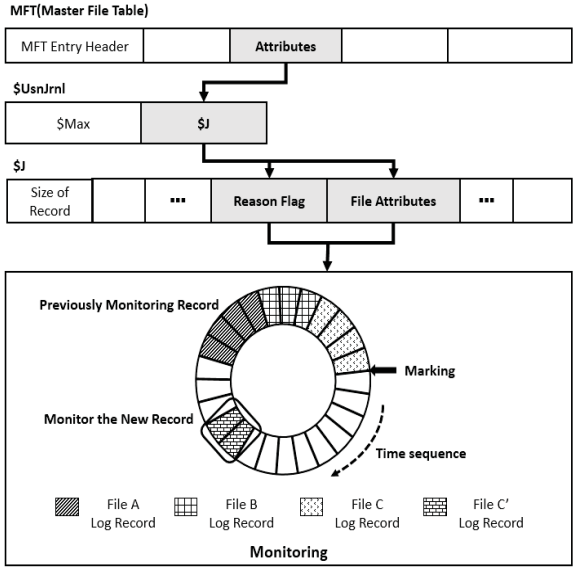

Fig. 1. Procedure of FACE to Monitor Metadata

Fig. 1 shows the procedure for monitoring specific metadata being changed. In order to monitor the change of system metadata information, we designed as follows. Navigate the location of the MFT (Master File Table) regions where the metadata is stored and find out the *$J* attribute of the *$UsnJrnl* entry. When value of disk volume is changed, the *$J* attribute stores the corresponding log record as the *$DATA* attribute. Therefore, we monitored the Reason Flag (`0x28`) and File Attributes (`0x34`) Journal Entry values of the *$J* attribute. Monitoring the Flag can get detailed information about the object where the event occurred. To monitor, check the location of the cluster where the first entry of the MFT starts and check the *$J* attribute flag of *$UsnJrnl*. The entry being monitored is recorded on the metadata in time-ordered sequence. The frequency at which records are added can be specified using FSUTIL [11] (1 to 4,294,967,295 seconds). In order to efficiently monitor the metadata, we apply the marking method that monitor the novel record after the previously monitored point.

B. *Ransomware Detection Framework with File System-Awareness scheme*

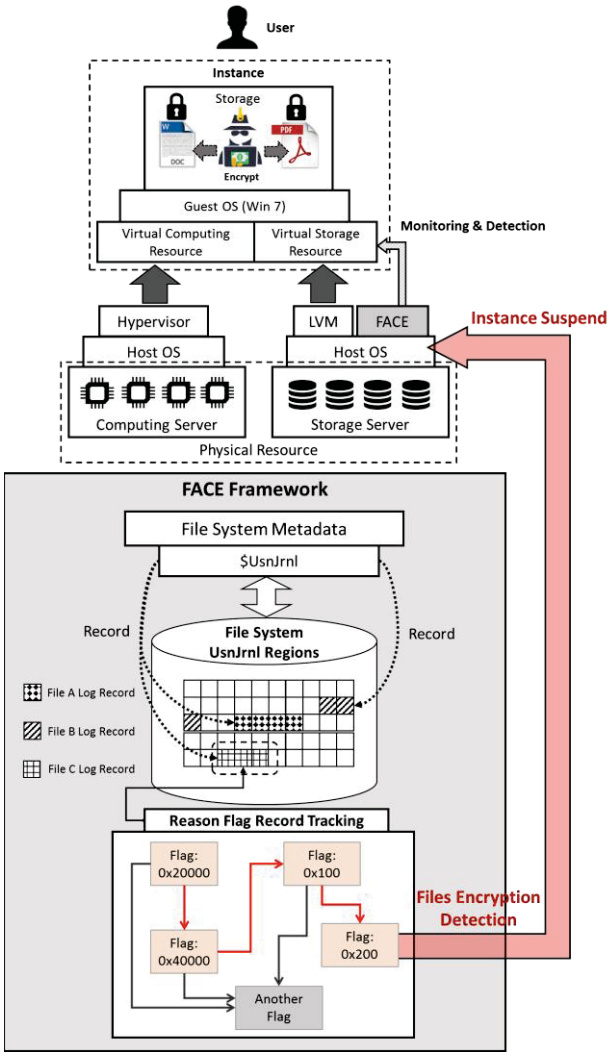

Fig. 2. Ransomware Detection Framework in Cloud Computing Environment

Fig. 2 shows the overall framework of our FACE to detect Ransomware in a cloud computing environment. The cloud platform consists of compute node where the instance is installed and storage node that provides the volume to the instance by setting the physical disk as LVM (Logical Volume Manager) [12]. The FACE framework detects Ransomware by monitoring the Flag of the *$J* attribute in the *$UsnJrnl* entry. The Ransomware detection mechanism classifies the flag changes when the files are encrypted and it is also implemented to detect flag change flow when an event occurs. Since FACE operates on the storage node, it does not use the internal resources of the user instance during monitoring and does not affect the user's virtualized computing resources. Therefore, it can be seen that there is little overhead penalty when compared with the behavior-based detection method, and the FACE proposed in this paper can be operated efficiently in cloud server running multiple instances.

IV. Experiment

In this section, we present the performance results obtained with our prototype version of FACE implemented in cloud computing environment. Performance results are compared to five of the best anti-virus software selected by AV-TEST [13], a reputable international organization.

A. Experiment Environment

To evaluate the performance of FACE, we constructed Openstack newton environment. The operating system of the host machine running the cloud platform used Ubuntu 16.04-64 bit, and the hypervisor installed KVM (QEMU). The virtual machine allocates a block disk (HDD) of 100GB and the operating system uses Windows7 64bit.

B. System Overhead Evaluation of FACE

In this experiment, we measured the CPU usage and read performance of the disk by installing HD Tune [14] inside the virtual machine to evaluate the system overhead caused by monitoring for the detection of Ransomware in the cloud computing environment. HD Tune is a disk performance benchmarking program.

TABLE Ⅰ. Overhead Performance Evaluation by Monitoring

Anti-Virus Software	**Performance Evaluation Items**	
	CPU Usage (%)	***Read Performance (MB/s)***
None	1.0	30.4
FACE	1.1	30.3
V3 Lite	25.5	27.4
Avast Antivirus	26.2	28.1
AVG Antivirus	26.9	27.9
Avira Security Suite	47.2	17.3
Kaspersky Free	26.2	25.4

The performance evaluation results are shown in TABLE I. We compared CPU utilization and disk read performance for three cases. The first is when no monitoring is performed, the second is when monitoring with antivirus software, and the last is when monitoring with our FACE. If monitoring is not performed, the CPU usage of the virtual machine is 1% and the disk read performance is 30.0MB/s. Based on this, FACE present 0.1% CPU overhead and 0.3% read performance overhead. On average, 29.34% of CPU overhead occurred and 17.04% of read performance overhead occurred when monitoring with anti-virus software. As a result, FACE has up to 25 times less CPU overhead than V3, the highest performance antivirus engine.

V. Conclusion

Our aim in this study was to provide Ransomware detection scheme tailored for a cloud computing environment. To accomplish this task, we thoroughly reviewed the previously Ransomware detection method. As a result, we have minimized overhead and have derived computationally efficient Ransomware detection with file system-awareness scheme. In addition, Monitoring is performed on the host machine, not the virtual machine in the cloud computing environment. So, it is designed not to affect the computing resources of virtual machine. This has been proven by experiments in the performance evaluation section. In our future work, we intend to devise a file recovery scheme using journaling metadata.

References

[1] Kelion, L. "Cryptolocker ransomware has infected about 250000 pcs." BBC, 12/2013 (2013).

[2] Hampton, Nikolai, and Zubair A. Baig. "Ransomware: Emergence of the cyber-extortion menace." (2015).

[3] Nieuwenhuizen, Daniel. "A behavioural-based approach to ransomware detection." Whitepaper. MWR Labs Whitepaper (2017).

[4] Ahmadian, Mohammad Mehdi, Hamid Reza Shahriari, and Seyed Mohammad Ghaffarian. "Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomwares." Information Security and Cryptology (ISCISC), 2015 12th International Iranian Society of Cryptology Conference on. IEEE, 2015.

[5] Bhardwaj, Akashdeep, et al. "Ransomware digital extortion: a rising new age threat." Indian Journal of Science and Technology 9 (2016): 14.

[6] Shukla, Manish, Sutapa Mondal, and Sachin Lodha. "POSTER: Locally Virtualized Environment for Mitigating Ransomware Threat." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016.

[7] Armbrust, Michael, et al. "A view of cloud computing." Communications of the ACM 53.4 (2010): 50-58.

[8] Scaife, Nolen, et al. "Cryptolock (and drop it): stopping ransomware attacks on user data." Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on. IEEE, 2016.

[9] Kharraz, Amin, et al. "UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware." USENIX Security Symposium. 2016.

[10] Fuller, Billy J. "Single transaction technique for a journaling file system of a computer operating system." U.S. Patent No. 6,021,414. 1 Feb. 2000.

[11] Fellows, Geoff. "NTFS volume mounts, directory junctions and $ Reparse." Digital Investigation 4.3 (2007): 116-118.

[12] Teigland, David, and Heinz Mauelshagen. "Volume Managers in Linux." USENIX Annual Technical Conference, FREENIX Track. 2001.

[13] AV-TEST: www.av-test.org.

[14] HD Tune: www.hdtune.com.