리눅스 및 ESXi 클라우드 호스트 환경에서의 랜섬웨어 행위 분석*

최진우[1†], 김진우[2‡]

[12]광운대학교 (학부생, 교수)

An Empirical Analysis of Ransomware Behavior on Linux and ESXi Cloud Hosts

Jin-u Choi[1], Jin-woo Kim[2]

[12]Kwangwoon University(Undergraduate student, Professor)

요 약

본 논문에서는 최근 클라우드에서 가상머신(VM)을 표적으로 공격하는 랜섬웨어 샘플들을 리눅스 호스트 및 ESXi 호스트 환경에 배포하여 분석하였다. 분석 결과, 대부분의 랜섬웨어 샘플들이 ESXi 호스트 디스크 저장소 경로인 /vmfs/volumes/를 암호화하는 동작을 관찰하였다. 가상 머신 디스크 파일(VMDK) 및 스냅샷 등 VM 관련 파일들이 해당 경로에 저장된다는 점을 고려할 때, 이러한 클라우드 랜섬웨어들은 단일 물리 호스트에서 다수의 VM을 동시에 손상시킬 수 있어 매우 치명적이다. 본문에서는 리눅스 환경과 ESXi 호스트 환경에서의 행위 분석 실험 결과를 요약 정리하여 향후 실용적인 대응책을 도출하는데 기여하도록 한다.

I. 서론

최근 클라우드에서의 랜섬웨어 공격은 가상화 인프라를 직접 표적으로 삼는 양상으로 확산되고 있다. 워크로드가 소수의 하이퍼바이저에 집중되는 클라우드 환경의 특성상, 단일 호스트 감염이 다수 가상머신(VM)의 동시 마비로 이어질 수 있다는 점에서 매우 높은 피해 위험을 가진다[1].

본 연구는 이러한 위험성을 확인하기 위하여 리눅스 기반 랜섬웨어 샘플 중 ESXi 호스트의 가상머신 디스크 저장 경로인 /vmfs/volumes/를 암호화하는 바이너리 샘플을 실험 환경에 배포하여 분석하고, 해당 샘플들이 ESXi 호스트 내에서도 실제로 동작할 수 있음을 실험적으로 확인하였다. 이를 통해 향후 클라우드 랜섬웨어 대응책 마련에 기여하고자 한다.

* 이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2024-00457937)

† 주저자, wlsgudy3@kw.ac.kr

‡ 교신저자, jinwookim@kw.ac.kr

II. 배경지식

2.1 ESXi 하이퍼바이저

ESXi는 VMware vSphere의 타입-1(베어메탈) 하이퍼바이저로, 범용 OS 없이 하드웨어 위에서 직접 동작하여 가상머신을 실행한다. VMkernel이 CPU·메모리·네트워크·디스크를 관리하며, vCenter Server가 다수 ESXi 호스트를 중앙 관리하는 구조를 가지고 있다.

ESXi 하이퍼바이저의 정확한 시장 점유율은 공개된 학술 통계로 명확히 확인하기 어렵지만, 산업 조사 보고서와 시장 분석에서 VMware 솔루션이 여전히 가상화 시장에서 높은 점유율을 차지하고 있음을 알 수 있다. 예를 들어, MaximizeMarketResearch[2]는 VMware가 하이퍼바이저 시장 데이터셋의 약 84%를 점유하는 것으로 보고하고 있다. 이를 통해 ESXi가 여전히 널리 채택되고 있음을 유추할 수 있다.

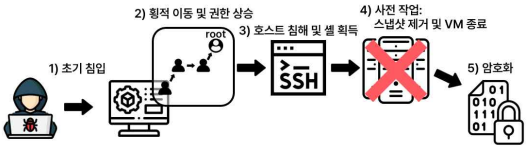

Fig. 1. Cloud ransomware overview

2.2 클라우드 랜섬웨어

클라우드 랜섬웨어는 ESXi와 같은 하이퍼바이저에서 구동하는 VM들을 특정하여 암호화하는 악성 코드를 지칭한다. Fig. 1은 ESXi 환경에 랜섬웨어가 배포되고 암호화를 진행하는 과정에 대한 개요이며 일반적으로 5가지 단계로 공격을 수행한다.

1) 초기 침입: 공격자는 피싱을 통한 사용자 계정 탈취, 공개된 관리 포트의 취약점 악용 등 내부 네트워크나 ESXi 관리 인터페이스에 최초 접근권을 확보한다.

2) 횡적 이동 및 권한 상승: 초기 침입 후, 공격자는 내부에서 추가 자격 증명을 획득하거나 이미 확보한 계정을 통해 다른 관리 시스템으로 이동하며 중앙 관리자 권한을 확보한다.

3) 호스트 침해 및 셸 획득: 공격자는 SSH 원격 세션, 업로드된 실행 파일 등을 통해 ESXi 호스트에서 셸 환경을 확보한다.

4) 사전작업: 공격자는 복구 가능성을 낮추기 위해 스냅샷을 삭제하거나 백업 프로세스를 종료시킨다. 또한 정상적인 암호화를 위해 VM을 종료시킨다.

5) 암호화: 랜섬웨어는 /vmfs/volumes/ 아래의 가상 디스크 파일(*.vmdk), 스냅샷 메모리 상태 파일(*vmsn), VM 메모리 백업 파일(*.vmem) 등을 암호화하고 파일명을 변경한다. 또한 README_TO_RESTORE 등의 이름을 가진 랜섬노트도 함께 생성한다.

최종적으로 해당 호스트에서 실행 중이던 다수의 VM이 동시에 가용성을 상실하며 데이터 복구가 어려워진다.

III. 클라우드 랜섬웨어 분석

3.1 분석 환경 구성

본 연구에서는 분석을 위해 1) 리눅스 기반, 2) ESXi 기반의 총 2가지 환경을 구성하였다. 리눅스 환경의 실험은 Oracle Virtualbox를 사용하여 Ubuntu 24.04 LTS (64-bit) VM을 구성하여 진행되었다. 모든 실험은 내부 네트워크 모드로 진행하여, 호스트 및 외부 네트워크와 차단된 상태에서 진행되었다. ESXi 환경의 실험은 Proxmox를 사용하여 ESXi 7.0U3과 ESXi 8.0U3 VM을 구성하여 진행되었다. 랜섬웨어를 실행시킬 때는 네트워크 디바이스를 제거하여, Proxmox 호스트 및 외부 네트워크와 차단된 상태에서 진행되었다. 동적 분석에는 VMware Threat Report 2022에서 제공한 malware dataset[3]중 랜섬웨어 샘플 66개가 사용되었으며 Table 1은 이를 요약한 것이다.

Table 1. Ransomware samples analyzed

Family	Count	Execution in Linux Environment	Encryption of /vmfs/volumes/
Blackmatter	3	O	X
Darkside	5	△ (4/5)	△ (4/5)
Defray	32	O (path required)	O (varies by path)
Ech0raix	8	△ (6/8)	X
Erebus	3	O	X
Gonnacry-c	4	△ (1/4)	X
Hellokitty	5	O (path required)	O (varies by path)
REvil	5	O	O (varies by path)
Vicesociety	1	O	O (varies by path)
Total	**66**	**60**	**47**

3.2 리눅스 환경에서의 동적 분석

샘플들이 리눅스 환경에서 /vmfs/volumes/ 경로를 암호화하는지 실험을 수행하였다. 네트워크 연결 등의 문제로 실행이 되지 않은 일부 샘플을 제외하면 대부분의 샘플들이 암호화를 진행하고 랜섬 노트를 생성하였다.

이 샘플들을 크게 2가지로 나눠볼 수 있다. 먼저 /vmfs/volumes/ 경로가 하드코딩 되어있는 샘플로, Darkside 패밀리가 이에 속한다. 다음으로는 Defray 패밀리처럼 실행할 때 인자로 경로를 넣어주는 샘플들이다. 이러한 샘플들은 인자로 넣어준 경로에 따라 /vmfs/volumes/ 경

로를 암호화하기도 하고, 하지 않기도 한다.

랜섬웨어 패밀리 별로 행동의 차이도 존재했다. Darkside 패밀리는 암호화하는 확장자나 경로 등이 하드코딩 되어있고, 파일 크기가 특정 크기 이상일 경우엔 전부 암호화하였다. Hellokitty 패밀리는 암호화 경로 외의 인자들을 통해 랜섬웨어 프로그램의 행동을 조절할 수 있었다. REvil 패밀리는 ESXi에서 관리 도구로 사용되는 esxcli 명령을 호출하는 것을 확인할 수 있었고, --silent 또는 -s 옵션을 통해 실행 중인 모든 VM들을 중지시키고 암호화를 진행할 수 있었다.

정리하면, 리눅스 환경을 타겟하는 샘플들 중의 일부가 ESXi의 가상머신 디스크 파일의 경로를 암호화할 수 있음을 확인하였다. 또한 Darkside, REvil 패밀리처럼 /vmfs/volumes/ 경로를 명시적으로 하드코딩하거나 -s 옵션 등으로 VM을 종료시키는 등의 ESXi 환경도 함께 목표로 하는 샘플들도 확인할 수 있었다. 따라서 ESXi 환경에서 정상적인 실행이 가능한지 확인할 필요가 있다.

3.3 ESXi 환경에서의 동적 분석

리눅스 환경에서 /vmfs/volumes/ 경로를 암호화한다는 것을 확인했으므로, 동일한 샘플들이 ESXi 환경에서도 가상머신 디스크 파일을 암호화할 수 있는지를 검증하기 위한 실험을 수행하였다. 그 중 우선적으로 Darkside 패밀리에 속하는 샘플들로 실험을 수행하였다. 공격자가 루트 권한을 가지며, 바이너리가 /bin/ 디렉터리에서 실행되는 것으로 가정하였다. Fig. 2를 보면 ESXi 환경에서 /vmfs/volumes 경로 내의 .vmdk 파일이 .darkside 확장자로 암호화되었고, darkside_readme.txt라는 랜섬노트가 생성된 것을 확인할 수 있다. Fig. 3은 샘플의 출력 중 일부로, Root Path로 /vmfs/volumes/ 경로가 명시적으로 지정되어 있는 것을 확인할 수 있다.

Fig. 2. Execution result of the Darkside sample

Fig. 3. Output of the Darkside sample

IV. 결론 및 향후 연구

본 연구에서는 클라우드 랜섬웨어 샘플이 ESXi 호스트 가상머신 디스크 파일이 저장되는 /vmfs/volumes 경로를 명시적으로 타깃으로 삼고 있음을 동적 분석을 통해 확인하였다. 또한 그 중 일부는 ESXi 환경에서 정상적으로 동작하며 .vmdk 파일 등을 암호화하여 가상머신의 가용성을 손상시킴을 확인하였다.

향후 연구에서는 이러한 실험 결과를 바탕으로, ESXi 전용 랜섬웨어 탐지 및 대응 시스템의 개발을 목표로 한다. ESXi에서 제공하는 호스트 로그 및 API 데이터를 학습 데이터로 활용하여 랜섬웨어 행위를 자동으로 분류/탐지할 수 있는 Transformer 기반 모델을 설계 및 구현할 예정이다. 이를 통해 클라우드 환경에서 치명적으로 작용할 수 있는 랜섬웨어의 탐지 효율을 높이고, ESXi 호스트의 보안 강화에 기여하고자 한다.

[참고문헌]

[1] VMware TAU. “VMware Threat Report - Exposing Malware in Linux-Based Multi-Cloud Environments” VMware Security Blog. 2022

[2] Maximize Market Research. “Hypervisor Market: Global Industry Analysis and Forecast (2024-2030).” Industry Report. 2024.

[3] VMware Threat Report 2022: Dataset Metadata. https://github.com/vmware-samples/tau-research/tree/main/2022-H1-Exposing-Malware-in-Linux-based-Multi-Cloud-Environments. 2022.