리눅스 및 ESXi 클라우드 호스트 환경에서의 랜섬웨어 행위 분석

최진우[1], 김진우[2]

[12]광운대학교(학부생, 교수)

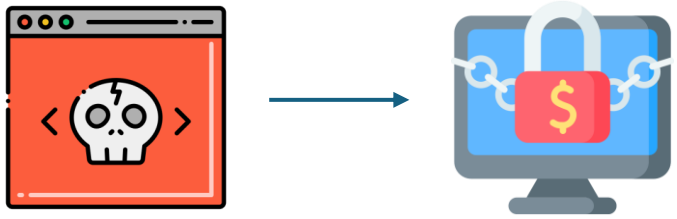
CNS Lab Cognitive & Network Security Lab

광운대학교 KwangWoon University

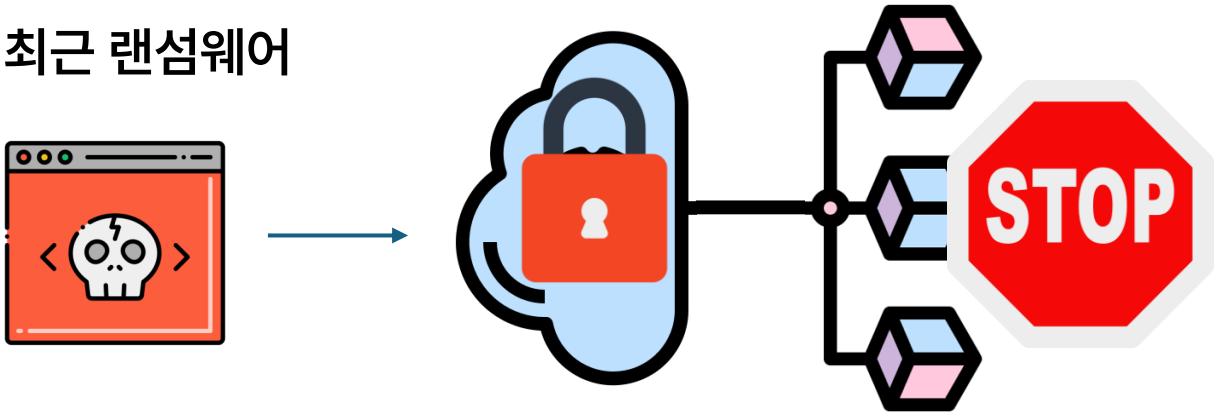
연구 배경

- 최근 랜섬웨어 공격 양상[1]
  - 가상화 인프라 표적
  - 단일 호스트 감염이 다수 가상머신의 동시 마비로 이어져 더 큰 피해를 초래

기존 랜섬웨어



최근 랜섬웨어

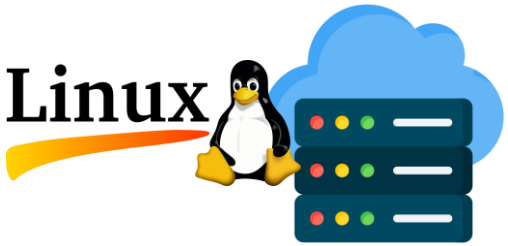


[1] VMware TAU. “VMware Threat Report –Exposing Malware in Linux-Based Multi-Cloud Environments” VMware Security Blog. 2022

논문 Overview

① 

Cloud Ransomware



Linux Cloud Host

Behavioral analysis

② 

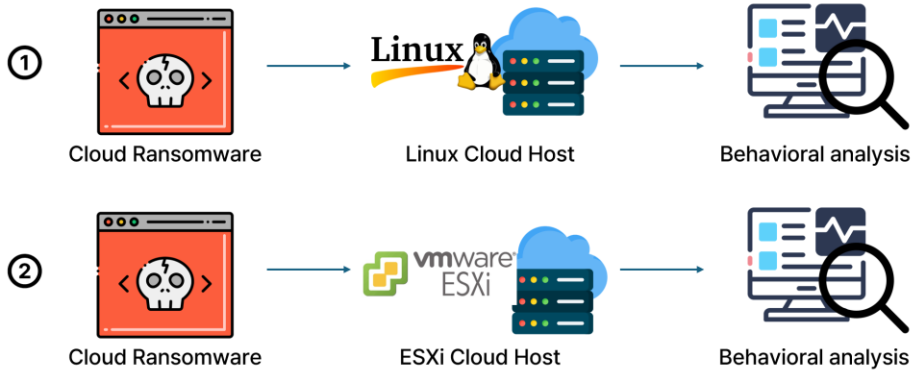
Cloud Ransomware

ESXi Cloud Host

Behavioral analysis

논문 Overview

- 클라우드 랜섬웨어 샘플 배포 및 분석[1]
  - 리눅스 호스트 환경, ESXi 호스트 환경

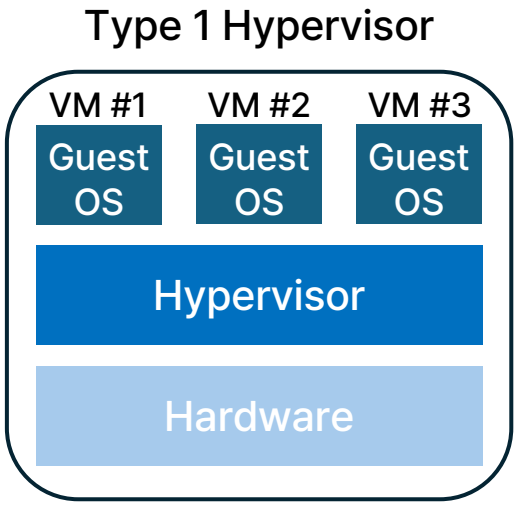


- ESXi 환경을 타깃하고 있는 것을 확인
  - 리눅스 기반 샘플이지만, ESXi에서 VM 데이터를 저장하는 위치인 /vmfs/volumes 경로 안의 파일들을 암호화

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

배경지식

- ESXi 하이퍼바이저
  - VMware vSphere의 Type-1(베어메탈) 하이퍼바이저
  - 범용 OS 없이 하드웨어 위에서 가상머신 실행



- 랜섬웨어
  - 피해자의 데이터나 시스템 접근을 제한한 뒤 금전을 요구하는 악성 소프트웨어

- 클라우드 랜섬웨어
  - ESXi와 같은 하이퍼바이저에서 구동되는 VM들을 암호화하는 악성 코드

배경지식

- 클라우드 랜섬웨어 공격과정 (5단계)

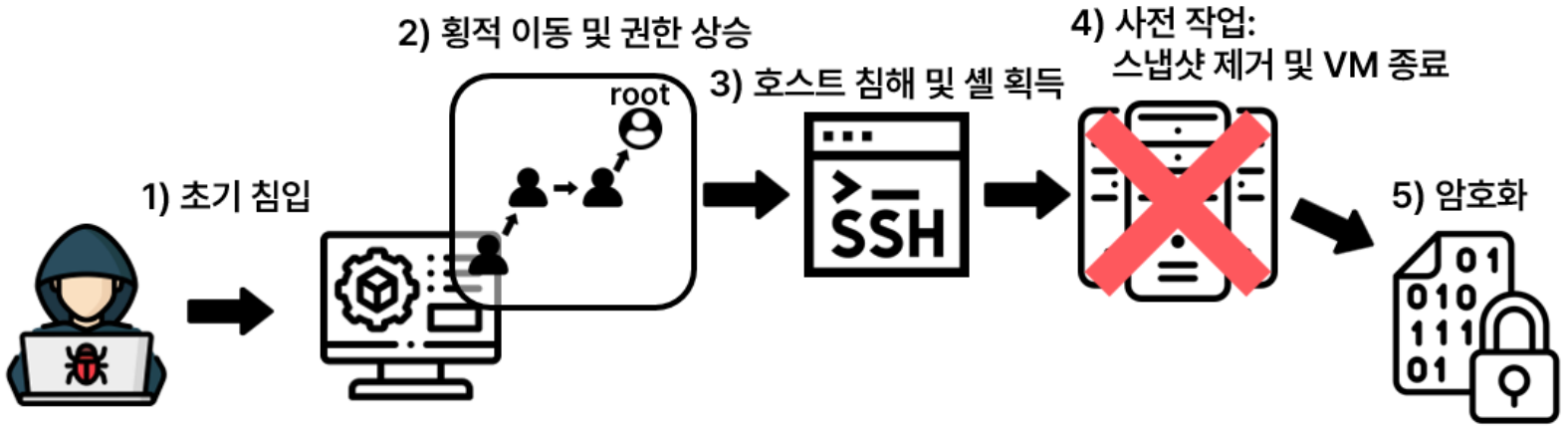
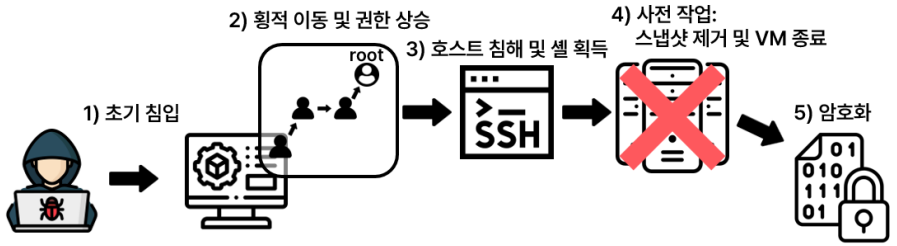


Fig 1. Cloud Ransomware Overview

클라우드 랜섬웨어 공격 과정 (1 ~ 3)

1) 초기 침입 :

피싱, 취약점 악용 등으로 최초 접근권 확보



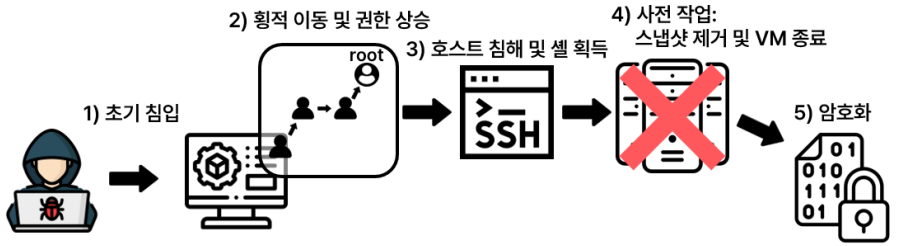
2) 횡적 이동 및 권한 상승 :

초기 침입 이후, 다른 관리 시스템으로 이동하며 중앙 관리자 권한 확보

3) 호스트 침해 및 셸 획득 :

SSH 원격 세션 등을 통해 ESXi 호스트에서 셸 환경 확보

클라우드 랜섬웨어 공격 과정 (4 ~ 5)



4) 사전작업 :

복구 가능성을 낮추기 위한 스냅샷 삭제, VM 종료 등의 활동

5) 암호화 :

가상 디스크 파일(*.vmdk), VM 메모리 백업 파일(*.vmem) 등 암호화

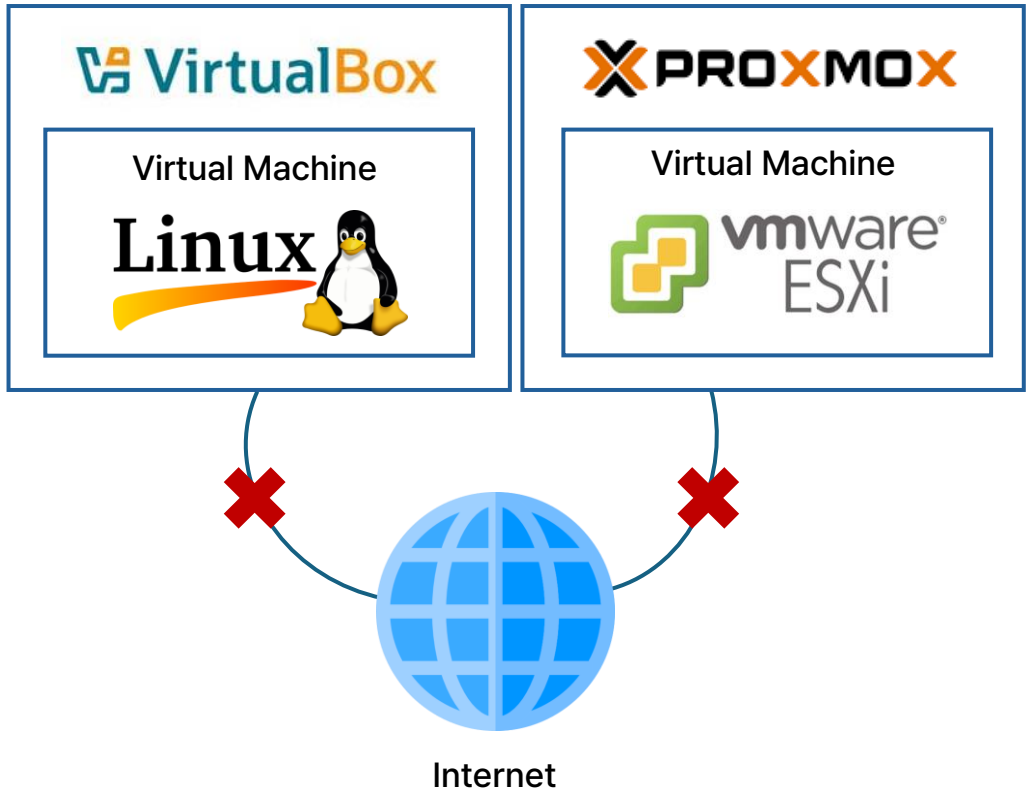
*랜섬노트(Ransom note) 생성

*랜섬노트 : 암호화되었음을 알리며, 금전을 요구하는 내용이 담긴 문서

분석 환경 구성

1) 리눅스 환경 :
   - Oracle Virtualbox
   - Ubuntu 24.04 LTS (64-bit)
   - 내부 네트워크 모드

2) ESXi 환경 :
   - Proxmox
   - ESXi 7.0U3 / ESXi 8.0U3
   - 네트워크 디바이스 제거



리눅스 환경에서의 분석

- /vmfs/volumes/ 경로에 미끼 파일 생성
- 해당 파일들을 리눅스 기반 랜섬웨어 샘플들이 암호화 하는지 확인

➔ 리눅스 환경임에도, 대부분(약 70%)의 샘플들이 암호화 및 랜섬노트 생성

랜섬웨어 샘플 정리

패밀리	샘플 개수	리눅스 환경에서 실행	/vmfs/volumes 암호화
Blackmatter	3	O	X
Darkside	5	△ (4/5)	△ (4/5)
Defray	32	O (경로 필요)	O (경로에 따라 다름)
Ech0raix	8	△ (6/8)	X
Erebus	3	O	X
Gonnacry-c	4	△ (1/4)	X
Hellokitty	5	O (경로 필요)	O (경로에 따라 다름)
REvil	5	O (경로 필요)	O (경로에 따라 다름)
Vicesociety	1	O (경로 필요)	O (경로에 따라 다름)
Total	**66**	**60**	**47**

- **가장 많은 비율을 차지하는 패밀리 :**
  Defray : 32개
- **인자로 경로를 입력 받아야 하는 패밀리 :**
  Defray, Hellokitty, REvil, Vicesociety
- **네트워크 연결 문제로 실행이 안 되는 경우 존재**

랜섬웨어 샘플 패밀리 별 특징

- Darkside :

  암호화하는 확장자 및 경로가 하드코딩 됨, 특정 크기 이상의 파일 전부 암호화

- Hellokitty :

  인자로 받은 경로에 대해 암호화 진행, 추가 인자들을 통해 랜섬웨어 행동 조절 가능

- REvil :

  ESXi에서 관리 도구로 사용되는 esxcli 명령 호출, -s 옵션을 통해 모든 VM 중지

ESXi 환경에서의 분석

- 리눅스 환경에서 /vmfs/volumes 경로 암호화 확인

➔ ESXi 환경에서도 실행 확인 필요 (ESXi 7.0U3)

➔ Darkside 샘플을 우선적으로 실행

```
[root@localhost:/vmfs/volumes/68c25a0d-ee3f6f36-39ec-bc24116d493a/Ubuntu-VM] ls
Ubuntu-VM-flat.vmdk.darkside  Ubuntu-VM.vmsd              Ubuntu-VM.vmx~
Ubuntu-VM.nvram               Ubuntu-VM.vmx               darkside_readme.txt
Ubuntu-VM.vmdk                Ubuntu-VM.vmx.lck           vmware.log
```

Darkside 샘플 실행 결과

```
[CFG] Root Path......................./vmfs/volumes/
[CFG] Key Size.....................548 Bytes
[CFG] Public Key.....................VALID
[CFG] Part Size.....................500mb
[CFG] Space Size.....................0mb
[CFG] Min Size.....................1mb
[CFG] Search Extension.....vmdk,vmem,vswp,log,vmsn
[CFG] New Extension.....................darkside
[CFG] Thread Count.....................4
[CFG] ReadMe File.....................darkside_readme.txt
[CFG] ReadMe Size.....................1969 Bytes
[CFG] Landing URL#[01].....http://catsdegree.com/cebcbedcdede
[CFG] Landing URL#[02].....http://temisleyes.com/dcdeacadedac
[CFG] User ID.....................8601c7eb0c6a974
[CFG] RC2 Key.....................OK
```

Darkside 샘플 출력

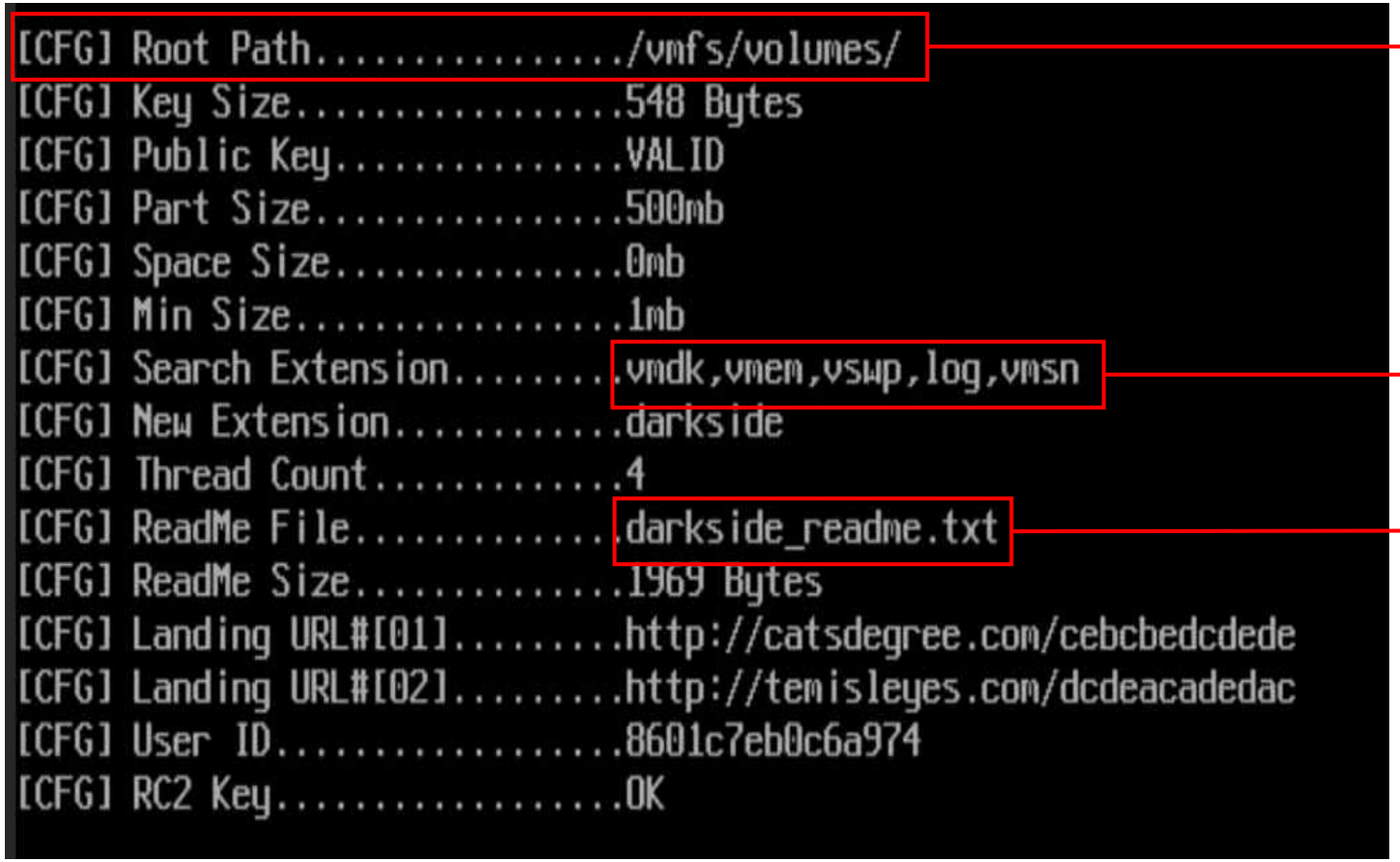
Darkside 샘플 실행 결과

- 타깃 디렉토리(/vmfs/volumes/...) 파일 암호화 확인

- .darkside 확장자로 바뀜 (암호화)
  .vmdk -> .vmdk.darkside

- 랜섬노트 생성
  darkside_readme.txt

Darkside 샘플 출력



암호화 대상 경로

암호화 대상

랜섬노트 이름

결론

- 결론
  - 리눅스 기반 클라우드 랜섬웨어 샘플을 두 가지 환경에서 실행 및 분석
  - 그 결과, ESXi 호스트 가상머신 또한 타깃하고 있고 실행도 가능함을 확인

- 향후 연구 목표
  - 클라우드 호스트 환경의 암호화는 가동중인 VM들의 중단으로 이어짐
  - ESXi 환경 전용 랜섬웨어 탐지 및 대응 시스템 개발
  - ESXi에서 얻을 수 있는 로그 및 데이터 활용 예정

랜섬웨어 탐지 시스템


log, API 데이터 등
LOG
vmware ESXi
랜섬웨어
탐지 모델
(transformer)
1. True/False
2. Family

감사합니다