Keep up with Ransomware

ESXi 서버 타깃 랜섬웨어 위협

최근 국내 랜섬웨어 피해 신고가 2018 년 22 건에서 2022 년 325 건으로 14 배 급증하며 수많은 기업들이 사이버 보안 위협에 직면하고 있다. 특히 랜섬웨어 공격 그룹끼리 서로 확인된 취약점을 공유하고, 다양한 전략과 탐지 회피 기법을 적용하는 등 더욱 치밀하고 고도화되는 양상이다. 이에 국내 최대 규모 화이트 해커 그룹이자 보안 기술 연구 전문가 집단인 EQST 는 매달 랜섬웨어 위협 동향을 분석하여 대응에 필요한 정보를 공유하고자 한다.

■ 개요

랜섬웨어 위협의 진원지가 서비스형 랜섬웨어(RaaS)로 이동하고 있다. 2023 년 2 월, 전월 대비 확인된 랜섬웨어의 피해 건수가 증가한 가운데, 상위 5 개 그룹 및 다양한 그룹에 의해 피해가 발생했던 전월과는 달리 2 월에는 서비스형 랜섬웨어인 LockBit 그룹에 의한 피해 건수가 압도적으로 많이 발생했다.

이는 Hive 랜섬웨어 그룹의 몰락과 다른 소규모 그룹의 활동이 주춤한데 비해, LockBit 그룹은 다른 그룹으로부터 흡수한 수많은 파트너 그룹을 통해 몸집을 키우고 있기 때문으로 분석된다.

2021 년 6 월 활동을 시작한 Hive 랜섬웨어 그룹은 서비스형 모델을 통해 전 세계 1,500 개 이상의 기업에 피해를 입혔고, 피해 기업으로부터 약 1 억 달러 이상의 수익을 벌어들인 대형 해킹 조직이다. 하지만 Hive 랜섬웨어 그룹은 2022 년 7 월부터 FBI 가 은밀히 수행한 네트워크 침투로 인해 몰락했다. FBI 가 네트워크를 침투해 1,300 개 이상의 암호 해독키를 획득 후 배포했기 때문이다. 해당 공격으로 Hive 그룹은 수익 모델을 잃어 활동의 막을 내리게 됐다.

하지만 안타깝게도 지난달 대규모 랜섬웨어 공격 사례가 또다시 발생했다. 취약한 ESXi[1] 서버를 대상으로 공격이 이뤄졌으며, 이미 2 년전 발견된 CVE-2021-21974[2] 취약점을 사용한 것으로 분석됐다. 해당 취약점은 이미 패치가 완료되었으나 패치 되지 않은 취약한 서버를 검색해 엑시악스(ESXiArgs)[3]로 불리는 랜섬웨어(쉘 스크립트와 ELF 파일)를 통해 암호화를 시도했다.

CISA[4]는 대규모 랜섬웨어 공격이 발생함에 따라 피해를 경감시키기 위해 암호화 방식의 허점을 통해 감염된 ESXi 가상 머신 환경을 복구할 수 있는 툴을 배포했다. 하지만 공격자가 이를 인지하고 암호화 방식을 바꿔 다시 공격을 시도하고 있으며, 지금까지도 취약한 서버를 대상으로 랜섬웨어 공격을 이어가고 있다.

또한 리눅스 및 ESXi 서버를 대상으로 공격을 시도하는 또 다른 네바다(Nevada) 랜섬웨어가 발견되기도 했다. 해당 랜섬웨어 역시 CVE-2021-21974 취약점을 사용하고 있으며, ESXiArgs 랜섬웨어와 마찬가지로 대규모 공격을 시도하고 있는 것으로 확인됐다. 이처럼 취약한 ESXi 서버의 대규모 감염 사례가 지속적으로 확인되고 있어 주의가 필요하다.

이러한 대규모 랜섬웨어 공격과 더불어 다크웹을 통한 이중 협박 전략을 사용하는 신규 랜섬웨어 그룹인 DarkBit, Medusa 가 발견되고 있다. 또한 V IS VENDETTA 그룹의 활동 정황도 다크웹에서 발견되고 있다. 기존 Cuba 랜섬웨어 그룹의 유출 사이트 URL 과 동일한 URL 을 포함하고 있으며, 'test.'가 추가된 URL 을 사용하여 Cuba 랜섬웨어 그룹의 서브 도메인으로 확인된다.

마지막으로 국내 제조 관련 중소기업 중 한 곳이 Mallox 랜섬웨어에 감염되어 유출된 데이터가 다크웹에 게시된 사실이 확인됐다. Mallox 랜섬웨어는 취약한 MS-SQL 을 대상으로 공격을 시도하는 랜섬웨어로, 파일 암호화 및 데이터 유출을 통해 이중 협박 전략을 구사한다. MS-SQL 계정 관련 공격을 통해 서버에 접속 후 추가로 설치한 원격 프로그램으로 랜섬웨어 공격을 시도하거나, SQL 을 이용하여 스크립트 혹은 파워쉘 명령어를 통해 랜섬웨어 공격을 수행한다. 데이터베이스 서버는 감염될 경우 기업에서 제공하는 대부분의 서비스를 정상적으로 운용할 수 없어 암호화된 파일을 최우선으로 복호화를 해야 하는 중요한 시스템이다. 취약한 데이터베이스는 공격자 입장에서 손쉽게 침투할 수 있는 경로 중 하나로 MS-SQL 을 사용하는 국내 기업의 적절한 보안 조치가 필요하다.

---

1 VMware 에서 개발한 가상화 OS

2 VMware ESXi OpenSLP 에서 힙 오버플로우(heap overflow)로 인해 발생하는 원격코드실행 취약점

3 일종의 랜섬웨어로, 프랑스의 국가 침해 대응 센터(CERT)가 2 월 3 일 먼저 발견해 경고. VMWare 의 ESXi 라는 하이퍼바이저들을 노리는 랜섬웨어임을 프랑스에서 발표.

4 CISA(Cybersecurity and Infrastructure Security Agency, 미국 사이버 보안 전담 기관)

■ 랜섬웨어 뉴스

ESXiArgs 랜섬웨어, 전세계의 ESXi 서버를 대상으로 공격

- 공격자들은 Shodan, Censys 와 같은 공개출처정보를 통해 ESXi 서버를 탐색
- OpenSLP[5] 원격 코드 실행 취약점(CVE-2021-21974)을 이용해 초기 침투
- 전 세계적으로 3,000 개 이상, 국내에서는 최소 20 개 이상의 서버가 감염된 것으로 추정
- 미국 CISA 에서 감염 환경 복구 툴을 공개했으나, 업데이트를 통해 복구 불가하도록 수정

VMware ESXi 서버를 노리는 Royal 랜섬웨어 리눅스 변종

- 리눅스를 지원하는 기능을 추가하였으며 VMware ESXi 서버를 타깃으로 공격
- 실행 옵션을 제공하며 옵션에 따라 암호화 프로세스 기능 수행

윈도우와 VMware ESXi 서버를 노리는 Nevada 랜섬웨어

- 2022 년 12 월 RAMP 포럼을 통해 러시아, 중국 해커 및 계열사를 모집
- 윈도우와 리눅스를 대상으로 Salsa20 알고리즘을 통해 파일 암호화
- 실행 옵션을 제공하며 옵션에 따라 악성 기능 수행

SentinelLabs, Clop 변종 랜섬웨어 복호화 툴 배포

- 2022 년 12 월 26 일 Linux 운영체제를 대상으로 하는 Clop 랜섬웨어 발견
- 파일 암호화에 사용되는 키를 보호하는 과정에서 결함 발견
- SentinelLabs 에서 복호화 툴을 무료로 배포

Clop 랜섬웨어는 GoAnywhere 취약점을 이용하여 130개의 조직을 침해했다고 주장

- Clop 랜섬웨어 공격자는 GoAnywhere MFT 보안 파일 전송 도구의 RCE 취약점(CVE-2023-0669)으로 130 개 이상의 조직에서 데이터를 탈취했다고 주장
- 2020 년 12 월 Accellion FTA 제로데이 취약점(CVE-2021-27101~27104)을 통해 100 여개 회사의 데이터를 탈취했을 때와 유사한 상황

미국의 시스템을 겨냥한 새로운 MortalKombat 랜섬웨어

[5] 근거리 통신망에서 서비스를 찾을 수 있도록 하는 서비스 검색 프로토콜(Open-source Service Location Protocol)

- Xorist 랜섬웨어의 변종인 MortalKombat 랜섬웨어와 정보 유출형 악성코드 Laplas Clipper 를 통해 금전적 이득을 취함
- 미국에 집중적인 피해를 일으켰으며 피싱 메일을 통해 유포
- 시스템의 주요 파일들을 암호화 대상에 포함시켜 시스템이 정상 구동하지 않을 수 있음

랜섬웨어로 피해를 입은 태평양 섬 국가 중 하나인 통가

- 통가의 국영 통신사인 TCC 가 Medusa 랜섬웨어 그룹에게 공격당해 업무 프로세스 지연
- Medusa 그룹은 주로 RDP 취약점을 통해 침투

의료 및 기타 주요 인프라 분야에 대한 북한의 랜섬웨어 공격

- 미국 정부기관 및 국가정보원은 북한의 랜섬웨어 공격에 대한 합동 보고서 발간
- CVE-2021-44228, CVE-2021-20038, CVE-2022-24990 취약점을 이용하여 공격
- Maui, H0lyGh0st 랜섬웨어를 사용

미국과 영국의 TrickBot, Conti 랜섬웨어 조직원에 대한 제재

- 미국과 영국의 보건 서비스, 병원 등에 대해 광범위한 공격을 했으며 영국은 이들 그룹이 2,700 만 파운드의 수익과 149 건 이상의 공격을 수행한 것으로 확인
- 러시아 조직원 7 명에 대해 미국과 영국의 모든 재산 및 자금을 차단

러시아인 Dubnikov는 Ryuk 랜섬웨어 그룹의 자금 세탁 혐의에 대해 인정

- Denis Mihaqlovic Dubnikov 및 공범 13 명은 Ryuk 랜섬웨어 자금 세탁 활동에 참여
- 2023 년 4 월 11 일 최종 판결이 이루어지며 유죄가 인정되면 최고 징역 20 년, 감독 조건부 석방 3 년, 최대 50 만 달러의 벌금을 선고받을 수 있음

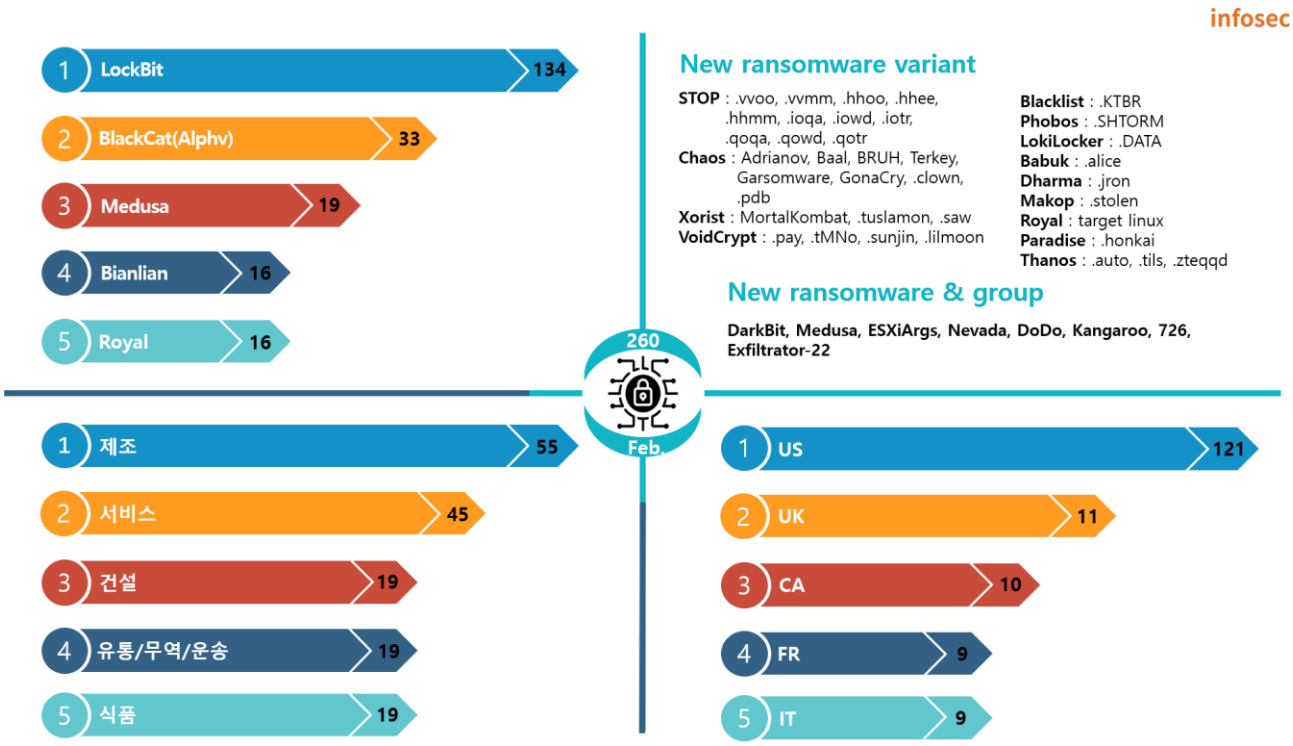
Lockbit 랜섬웨어와 연관된 공격 프레임워크 Exfiltrator-22

- 랜섬웨어, 데이터 유출 등의 다양한 기능을 포함하는 공격 프레임워크 데모 비디오 공개
- Lockbit 3.0 에서 사용한 도메인 프론팅 기술과 동일한 C2 인프라 사용으로 Lockbit 3.0 의 계열사 혹은 멤버에 의해 개발된 도구로 추정

MortalKombat 랜섬웨어 무료 복호화 툴 공개

- 비트디펜더 社는 MortalKombat 랜섬웨어에 대한 무료 복호화 툴을 공개
- Laplas 클립보드 하이재커는 수동으로 제거 필요

■ 랜섬웨어 뉴스



새로운 위협

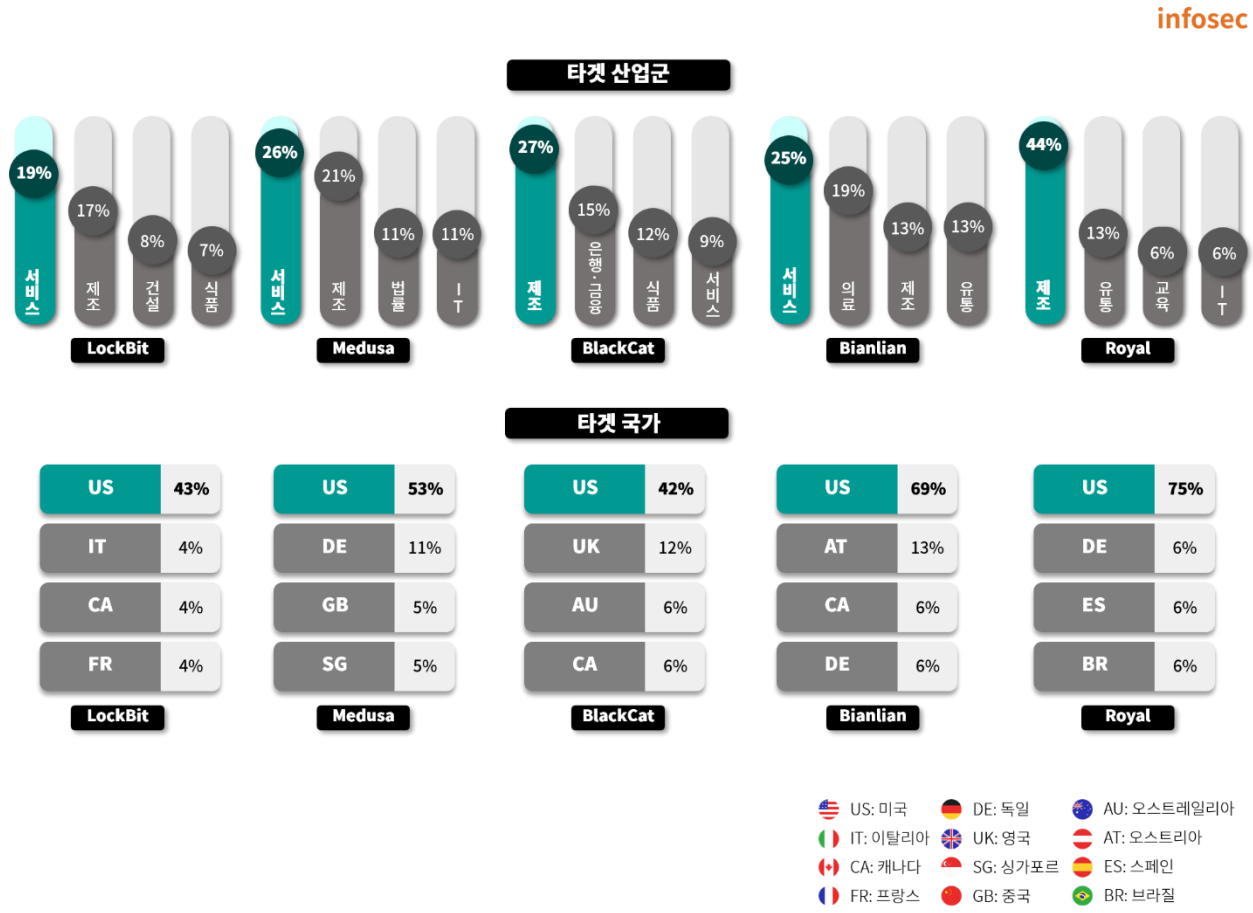
Stop, Chaos 랜섬웨어의 변종이 다수 출현하고 있으며 DarkBit, Medusa, ESXiArgs, Nevada, DoDo, Kangaroo, 726, Exfiltrator-22 랜섬웨어가 새로 발견되고 있다. DarkBit, Medusa 랜섬웨어는 다크웹을 통해 데이터를 유출하여 이중 협박 전략을 사용하는 그룹으로 확인된다. 특히 Medusa 랜섬웨어는 신규 그룹임에도 불구하고 다크웹을 통해 총 19 건의 희생자를 게시하는 등 다수의 피해를 입히고 있다. 또한 리눅스와 ESXi 서버를 대상으로 ESXiArgs, Nevada 랜섬웨어의 대규모 공격 사례 및 Royal 랜섬웨어의 리눅스 변종이 발견되는 등 전 세계적으로 대규모 피해 사례가 지속적으로 발생하고 있어 새로운 위협에 대한 특별한 주의가 필요하다.

Top5 랜섬웨어

지난 2 월 랜섬웨어 피해 건수를 확인해보면, 기존 랜섬웨어 그룹 중 LockBit 랜섬웨어 그룹의 공격은 한달 간 총 134 건으로 확인된다. 이는 전월 대비 큰 폭으로 증가한 수치로 타 랜섬웨어 그룹과 비교해도 월등히 높다. 또한 전월 대비 가장 큰 폭으로 희생자를 증가시켜 서비스형 랜섬웨어 중 가장 큰 위협이 되고 있다.

Top5 랜섬웨어를 분석해보면 대부분의 랜섬웨어 공격은 여전히 제조, 서비스 산업에 집중되고 있다. 특히 BlackCat(Alphv), Bianlian 랜섬웨어 그룹은 제조, 서비스와 더불어 은행/금융과 의료/제약/복지 산업을 대상으로 높은 공격 횟수를 보였다.

Top5 를 비롯해 2 월 한달 간 활동한 랜섬웨어의 희생자가 속한 국가를 살펴보면 주로 미국을 타깃으로 한 공격 사례가 가장 많은 것으로 확인되고 있으며, 이외에는 불특정 국가를 대상으로 공격이 분포되어 있다.



■ 랜섬웨어 집중 포커스

ESXiArgs 랜섬웨어

2 월 초 CERT-FR(French Computer Emergency Response Team)에 의해 ESXi 서버를 대상으로 한 랜섬웨어 공격이 발견되었다. 해당 공격은 ESXi 의 CVE-2021-21974 취약점을 이용하여 이루어졌으며 2021 년 2 월 VMVMware 는 해당 취약점을 수정한 패치를 배포하였다. 하지만 여전히 패치를 적용하지 않은 취약한 ESXi 서버가 다수 존재하여 대규모 감염 사례가 발생하고 있으며, Shodan, Censys 와 같은 오픈 검색 서비스를 이용하여 손쉽게 검색이 가능해 공격자들은 이러한 정보를 수집해 공격에 활용하였다. 현재까지 밝혀진 사항을 살펴보면 CVE-2021-21974 취약점 외에도 CVE-2022-31699[6], CVE-2020-3992[7] 등 다양한 취약점을 사용했을 가능성을 배제할 수는 없다.

ESXiArgs 랜섬웨어는 Sosemanuk 암호화 알고리즘을 사용해 파일을 암호화하는데 해당 알고리즘은 리눅스를 대상으로 제작된 CheersCrypt, PrideLocker, Yanluowang 랜섬웨어에서 발견된 이력이 있으며, Babuk 랜섬웨어 코드 유출 이후 파생된 일부 랜섬웨어에서 사용하고 있어 Babuk 랜섬웨어를 기반으로 작성한 것으로 추정된다.

[6] VMware ESXi OpenSLP 에서 발생하는 힙 오버플로우 취약점

[7] VMware ESXi OpenSLP 에서 Use-after-free 로 인해 발생하는 원격코드 실행 취약점

ESXiArgs

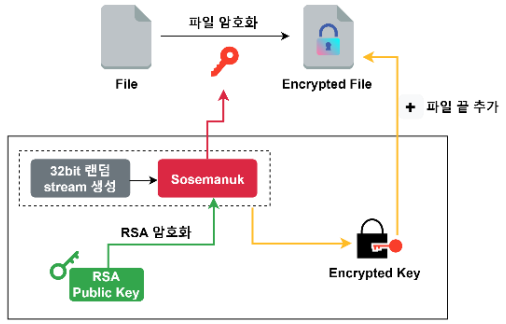
암호화

encrypt.sh (ELF encryrptor loader) -----call-----> encrypt (ELF encryptor)

```
"usage: encrypt <public_key> <file_to_encrypt> [<enc_step>] [<enc_size>] [<file_size>]");
"       enc_step    -   number of MB to skip while encryption");
"       enc_size    -   number of MB in encryption block");
"       file_size   -   file size in bytes (for sparse files)\n");
```

암호화 키

Sosemanuk 스트림 암호화를 사용하여 파일 암호화 후 RSA 공용키로 보호하여 파일 끝에 추가



암호화 대상

.vmdk .vmx .vmxf .vmsd .vmsn .vswp .vmss .vmem .nvram

업데이트

파일 크기에 따라 암호화를 제외하는 부분이 증가하여 CISA에서 이를 이용한 설정 파일 복구 방안 제시
공격자는 이를 확인 후 1MB만 Skip 하도록 업데이트

```
size_kb=$(du -k $file_e | awk '{print $1}')
if [[ $size_kb -eq 0 ]]; then
  size_kb=1
fi
size_step=0
if [[ $(($size_kb/1024)) -gt 128 ]]; then
  size_step=$((($size_kb/1024/100)-1))
fi
```

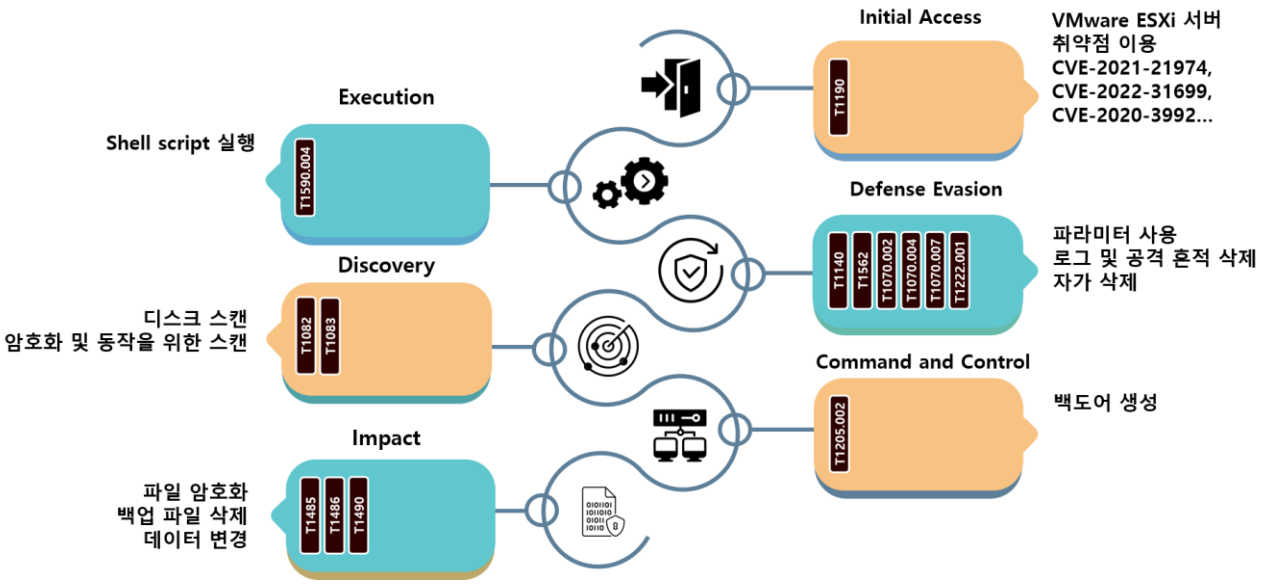
```
size_kb=$(du -k $file_e | awk '{print $1}')
if [[ $size_kb -eq 0 ]]; then
  size_kb=1
fi
size_step=1
```

특징

- Sosemanuk 알고리즘
- 암호화 키 보호 (RSA)
- 부분 암호화
- 로그, 공격에 사용된 파일, 백업, 스케줄러, 네트워크 흔적 삭제
- vmtools.py 파이썬 스크립트 백도어
- ESXi 취약점

ESXiArgs 랜섬웨어 전략

infosec



ESXiArgs 랜섬웨어는 공개된 정보를 통해 ESXi 서버 중 취약한 서버를 대상으로 공격을 시도한다. 오픈 검색 서비스를 통해 ESXi 서버를 검색 후 패치 되지 않은 서버에 대해 원격 코드 실행 혹은 인증 우회 취약점 등을 이용하여 최초 침투를 시도한다. Shell script 와 ELF 파일을 통해 암호화 대상을 선정 후 Sosemanuk 알고리즘을 이용해 암호화하고 사용된 암호화 키는 RSA 공개키로 암호화하여 보호하는 전략을 사용하였다.

해당 랜섬웨어는 빠르게 암호화를 수행하기 위해 파일의 일부분만 암호화하는 부분 암호화 전략을 사용하는데 파일의 크기가 크면 클수록 암호화하지 않는 부분이 증가한다. 특히 가상 환경 특성상 큰 파일이 다수 존재하기 때문에 CISA 에서는 환경 설정 복구를 통해 정상 구동 시킬 수 있는 스크립트를 공개했다. 이러한 부분 암호화에 대한 이슈가 발생하자 공격자는 즉시 대응하여 Shell script 를 수정 후 공격에 사용하였다. ESXiArgs 랜섬웨어의 배후 공격자는 모니터링을 통해 빠르게 대응하고 있음을 알 수 있으며, 즉각 대응이 어려운 늦은 밤 시간을 노려 취약한 서버를 대상으로 대규모 공격을 주기적으로 수행하고 있다.

ESXiArgs 랜섬웨어가 발견된 서버에서 Python 으로 작성된 백도어 또한 발견되었다. 해당 백도어는 전송된 명령어를 수행하거나 Reverse shell[8]을 실행하여 지정한 호스트와 포트로 연결한다. 즉, 지속 실행되는 것이 아니라 모든 암호화 작업이 끝나면 로그 파일, 백업 파일, 공격에 사용한 흔적 등과 함께 삭제하여 탐지를 회피하기 위한 전략을 사용한다.

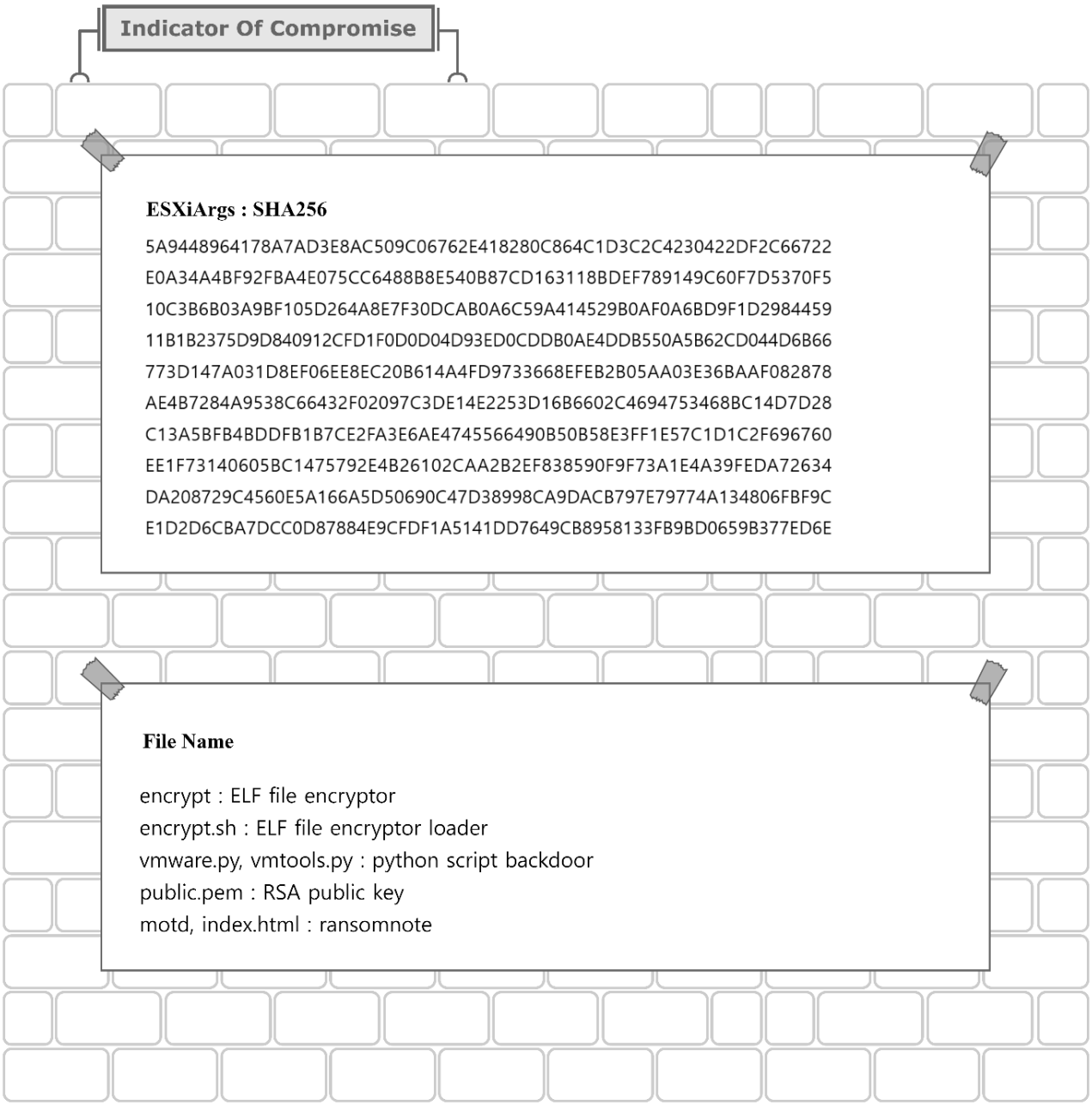
마지막으로 ESXiArgs 랜섬웨어는 다크웹 사이트를 운영하지 않으며 비트코인 주소와 Tox Chat[9] ID 를 제공하여 연락하도록 안내하고 있다. 정교한 공격을 수행하는 전략보다 알려진 취약점을 이용해 패치 되지 않은 서버를 공략하는 쉬운 접근 방법을 사용하고 있다. 또한 유출된 Babuk 랜섬웨어를 기반으로 작성한 랜섬웨어로 추정되는 점과 이중 협박 전략을 사용하지 않는 점 등을 고려해 봤을 때, 불특정 다수를 노려 많은 감염 서버를 확보 후 금전적 이익을 취하는 전략을 선택한 것으로 보인다.

알려진 취약점을 이용하여 공격을 시도하는 만큼 VMware ESXi 서버를 사용하고 있다면 최신 버전의 패치를 적용하고, SLP 서비스를 사용하지 않도록 적용해야 한다. 아울러 외부에 노출되지 않도록 ESXi 서버에 대한 조치가 필요하다.

[8] 타깃이 수신 상태를 유지하고 공격자가 타깃으로 접속하는 형태

[9] 단대단 암호화를 지원하는 메신저

■ IoC


Indicator Of Compromise
ESXiArgs : SHA256
5A9448964178A7AD3E8AC509C06762E418280C864C1D3C2C4230422DF2C66722
E0A34A4BF92FBA4E075CC6488B8E540B87CD163118BDEF789149C60F7D5370F5
10C3B6B03A9BF105D264A8E7F30DCAB0A6C59A414529B0AF0A6BD9F1D2984459
11B1B2375D9D840912CFD1F0D0D04D93ED0CDDB0AE4DDB550A5B62CD044D6B66
773D147A031D8EF06EE8EC20B614A4FD9733668EFEB2B05AA03E36BAAF082878
AE4B7284A9538C66432F02097C3DE14E2253D16B6602C4694753468BC14D7D28
C13A5BFB4BDDFB1B7CE2FA3E6AE4745566490B50B58E3FF1E57C1D1C2F696760
EE1F73140605BC1475792E4B26102CAA2B2EF838590F9F73A1E4A39FEDA72634
DA208729C4560E5A166A5D50690C47D38998CA9DACB797E79774A134806FBF9C
E1D2D6CBA7DCC0D87884E9CFDF1A5141DD7649CB8958133FB9BD0659B377ED6E
File Name
encrypt : ELF file encryptor
encrypt.sh : ELF file encryptor loader
vmware.py, vmtools.py : python script backdoor
public.pem : RSA public key
motd, index.html : ransomnote

■ 참고 사이트

URL: https://www.cisa.gov/uscert/ncas/alerts/aa23-039a

URL: https://www.vmware.com/security/advisories/VMSA-2021-0002.html

URL: https://www.vmware.com/security/advisories/VMSA-2022-0030.html

URL: https://www.vmware.com/security/advisories/VMSA-2020-0023.html

URL: https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/

URL: https://www.bleepingcomputer.com/news/security/new-esxiargs-ransomware-version-prevents-vmware-esxi-recovery/

URL: https://www.sentinelone.com/labs/cl0p-ransomware-targets-linux-systems-with-flawed-encryption-decryptor-available/

URL: https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/

URL: https://www.bleepingcomputer.com/news/security/new-mortalkombat-ransomware-targets-systems-in-the-us/

URL: https://therecord.media/tonga-is-the-latest-pacific-island-nation-hit-with-ransomware/

URL: https://www.bleepingcomputer.com/news/security/north-korean-ransomware-attacks-on-healthcare-fund-govt-operations/

URL: https://www.bleepingcomputer.com/news/security/us-and-uk-sanction-trickbot-and-conti-ransomware-operation-members/

URL: https://www.bleepingcomputer.com/news/security/linux-version-of-royal-ransomware-targets-vmware-esxi-servers/

URL: https://www.bleepingcomputer.com/news/security/new-nevada-ransomware-targets-windows-and-vmware-esxi-systems/

URL: https://www.bleepingcomputer.com/news/security/new-exfiltrator-22-post-exploitation-kit-linked-to-lockbit-ransomware/

URL: https://www.bleepingcomputer.com/news/security/new-mortalkombat-ransomware-decryptor-recovers-your-files-for-free/