Keep up with Ransomware

다양한 플랫폼 타깃한 Knight 랜섬웨어 위협

■ 개요

2023 년 9 월 랜섬웨어 공격으로 인한 피해 사례 발생 건수는 전월(401 건) 대비 23.7% 증가한 496 건으로 나타났다. 이는 LockBit 랜섬웨어 그룹에 의한 피해 사례가 늘어난 것과 함께, 최근에 발견된 랜섬웨어 그룹인 Cactus, Ransomed, LostTrust 의 활발한 활동과 관련이 있다. 이러한 랜섬웨어 이슈들이 연이어 발생하며 위협이 지속되고 있다.

최근 LockBit 계열사의 공격 캠페인에서 LockBit 랜섬웨어가 차단되자, Rust [1] 계열의 신규 랜섬웨어인 3AM 을 사용하여 시스템을 감염시키는 사례가 발견됐다. 3AM 은 아직 다른 랜섬웨어 그룹과의 연관성이 밝혀지지 않았으나, LockBit 계열사에서 사용되면서 화제가 된 랜섬웨어다. 이번 공격은 LockBit, 3AM 랜섬웨어를 선택적으로 사용하여 랜섬웨어 감염 성공률을 높이기 위한 전략으로 보인다.

또한 LockBit, Akira 랜섬웨어 그룹이 Cisco 의 네트워크 보안 솔루션인 ASA(Adaptive Security Appliance) 및 FTD(Firepower Threat Defense)의 취약점 CVE-2023-20269[2]를 악용한 공격 사례도 확인됐다. 최근 공격자들은 하나의 취약점을 악용하여 다수의 기업을 대상으로 공격하는 전략을 많이 사용하는 추세를 보이고 있다.

[1] Rust : 프로그래밍 언어의 일종으로, 악성코드 제작자들은 빠른 암호화 속도, 분석 및 탐지 우회 등의 이점이 있어 사용

[2] CVE-2023-20269 : ASA 및 FTD 소프트웨어 무단 접근 취약점

뿐만 아니라, LockBit 랜섬웨어 그룹은 국내 대기업 기업의 데이터 800GB 를 확보하고 협약서, 탈취한 데이터 리스트와 용량 등 샘플 데이터를 게시하며 7 일 후 모든 데이터를 공개하겠다는 협박 게시물을 올렸다. 해당 데이터는 태양광 사업을 담당하는 중국의 한 공장에서 유출된 것으로 파악되었으며, 피해 기업은 LockBit 랜섬웨어 그룹과의 협상을 거부했다. 이에 LockBit 랜섬웨어 그룹은 업무 관련 문서, 그림 파일, 데이터베이스 관련 파일 등을 포함한 약 100GB 의 압축 파일과 데이터 리스트를 게시했다. 최근 국내 기업들 사이에서 랜섬웨어 감염과 이중 협박 사례가 잇따라 발생하고 있으므로 주의가 필요하다.

BianLian 은 꾸준한 활동을 이어오고 있는 랜섬웨어 그룹으로, 최근 탈취한 데이터를 익명으로 게시한 후 이를 조용히 삭제한 사건으로 인해 세간의 분노를 샀다. 게시물은 '**** **e ******e* ***e*********'와 같이 익명으로 게시되었지만, 약 25,000 명의 직원을 고용하고 116 개국에서 활동하는 세계 최고의 비영리 기관이라는 설명과 마스킹 된 문자를 통해 비영리 자선단체인 'Save The Children International'임이 드러났다. 이 사실이 알려지자 우려 섞인 반응으로 각종 커뮤니티에서 비판의 여론이 발생했다. 이에 BianLian 랜섬웨어 그룹은 이튿날 게시물을 조용히 삭제하면서 사태를 진정시키려는 모습을 보였다.

LostTrust 로 불리는 신규 랜섬웨어 그룹의 동향도 심상치 않다. LostTrust 랜섬웨어 그룹은 총 53 건의 피해 사례를 다크웹 유출 사이트에 게시하며 새롭게 등장했다. 이들이 사용하고 있는 랜섬웨어는 SFile 랜섬웨어와 코드 유사성이 확인되고 있어 소스 코드를 차용했거나 리브랜딩의 의혹이 제기되고 있다. 한편, 이들의 유출 사이트 디자인 및 그룹 소개 문구는 MetaEncryptor 랜섬웨어 그룹과 유사한 모습을 보이고 있다. 이는 모방을 통해 홍보하기 위한 전략 중 하나로, 이번에 새로 발견된 CryptBB 랜섬웨어 그룹 역시 8base 랜섬웨어 그룹을 단순 모방하여 활동을 시작하고 있다.

Knight 랜섬웨어 그룹은 Cyclops 랜섬웨어 그룹이 리브랜딩 된 그룹으로, Windows, Linux, macOS, ESXi[3], Android 플랫폼을 모두 감염시킬 수 있는 빌더를 제공하고 있으며, 이를 위해 약 3 년 동안 개발해온 것으로 알려졌다. Knight 랜섬웨어 그룹은 계열사의 원활한 공격을 지원하기 위해 암호화 및 정보 탈취형 악성코드를 포함한 풀 버전과 파일 암호화만 진행하는 경량 버전의 랜섬웨어를 제공하고 있다. 또한 이들은 많은 계열사를 확보하기 위해 피싱, 스팸 메일과 사회공학기법을 통한 접근을 적극적으로 시도하고 있다. Knight 랜섬웨어 그룹은 최근 이탈리아에서 스팸 메일 캠페인을 진행하고 있는 것이 확인되었으며 문서 파일로 위장한 실행 파일을 실행하도록 유도하는 전략을 사용하고 있다.

[3] ESXi : VMware 에서 개발한 가상화 OS

한편, Knight 랜섬웨어는 LockBit 과 Babuk 랜섬웨어와 연관성이 있다는 주장이 제기됐으며, 실제 분석 결과 암호화 로직의 코드 유사성이 확인됐다. 이처럼 랜섬웨어 그룹 간에 코드나 TTP(Tactics Techniques and Procedures)[4] 의 유사성이 종종 발견되는데, 이는 랜섬웨어를 제작할 때 유출된 코드를 참고하여 제작하거나, 랜섬웨어 그룹 간에 정보 교류 및 협업이 진행되고 있음을 나타내는 증거다.

영향력 있는 정보 탈취형 악성코드인 Vidar 와 RedLine 의 공격자들은 정보 탈취형 악성코드를 유포했던 방식 그대로 랜섬웨어를 유포하기 시작했다. 이는 동일한 유포 경로를 사용하여 새로운 전략이나 기술을 처음부터 개발하거나 적용할 필요 없이 기존의 자원을 활용하여 공격의 범위를 확장하는 전략을 사용한 것으로 보인다. 이때 사용한 랜섬웨어는 Knight 랜섬웨어를 배포한 것으로 확인됐다. 이처럼 많은 공격자 그룹은 TTP 를 재사용하고 일부만 수정하여 사용하고 있어 효과적인 대응을 위해 공격자 관점의 분석이 더욱 중요해지고 있다.

최근 랜섬웨어 그룹들은 초기 침투 방법으로 취약점을 악용한 공격과 피싱, 스팸 메일, 사회공학기법 등 다양한 방법으로 공격을 수행하고 있다. 전문적인 지식을 통해 발견하는 취약점을 악용한 침투와 비교적 손쉬운 기술인 사회공학기법을 이용한 상반된 전략이 모두 발견되고 있다. 이러한 전략은 LockBit, BlackCat 과 같은 대형 공격 그룹과 신규/소규모 랜섬웨어 계열사간의 기술력 차이로 볼 수도 있지만, 랜섬웨어 그룹이 최초 설계한 전략을 쉽게 바꾸지 않는다는 점에 주목할 필요가 있다. 따라서, 랜섬웨어를 효과적으로 차단하기 위해서는 기업 환경에 맞는 적절한 대응 단계를 수립하고 랜섬웨어 그룹의 전략과 전술을 사전에 파악하여 능동적이고 선제적인 조치가 필요하다.

[4] TTP : 공격자의 전략과 전술, 절차를 표현하는 방법

■ 랜섬웨어 뉴스

infosec

LockBit, 제조업체 공격을 통한 영국 국방부 데이터 탈취

- LockBit, 영국 국방부 데이터 유출
- 유출 데이터에는 여러 중요 국방 시설의 정보 포함
- 제조사 Zaun이 피해를 입었으나, 주요 데이터는 손상되지 않았다고 주장
- 공급망 공격에 대한 우려가 커지고 있으며, 영국 국방부는 해당 사건 언급에 대해 거부

Ransomed, 세계 최대 항공기 제조사 Airbus 공격

- Airbus의 공급 업체 정보가 다크웹에 유출되어 조사 중
- 해커는 터키 항공사 직원 계정을 해킹하여 네트워크에 접근
- Airbus는 이전에도 중국 해커에 위해 공격 당함

BianLian, Save the Children 공격을 통해 7TB 데이터 탈취

- BianLian, Save the Children 공격을 통해 약 7TB의 데이터를 탈취
- 수 많은 어린이들에게 영향을 미칠 수 있어 비판의 목소리가 이어짐

TrickBot 및 Conti 조직원 11명 제재

- TrickBot 및 Conti 조직은 세계적으로 1억 8천만 달러(한화 약 2,413억 원)를 탈취, Conti 조직은 와해됨
- 제재로 인해 조직원의 모든 금융 거래가 금지되었으며 조직에 영향을 미침

LockBit 및 Akira, Cisco VPN 취약점 악용 공격

- Cisco 社, VPN 서비스 취약점이 LockBit과 Akira에 의해 악용되고 있음을 경고
- 해당 취약점은 공격자가 초기 침투를 위해 Brute Force Attack을 수행할 수 있게 함
- 피해를 예방하기 위해 MFA(Multi Factor Authentication) 조치가 필요

* MFA : 사용자에게 암호 이외의 추가 정보 입력을 요구하여 계정 인증을 하는 과정

Cuba, 탐지 어려운 신규 악성코드 유포

- Cuba, 신규 악성코드에 암호화된 데이터 사용을 통해 백신 탐지 회피 기능 탑재
- 해당 그룹은 공격에 자체 제작 도구를 사용하며 지속적으로 개선해 나가고 있음

3AM, LockBit의 대안으로 부상

- 3AM, Rust로 작성되었으며 LockBit을 통한 공격이 실패하자 이를 유포
- LockBit의 계열사에 의해 사용된 만큼, 타 공격자들에게 신뢰성을 확보할 가능성 있음

BlackCat(Alphv), Sphynx 변종으로 Azure Storage 공격

- Sphynx 변종을 통한 Azure Cloud Storage 암호화 과정에서 탈취한 Microsoft 계정 악용
- 보안 정책을 수정하여 약 40개의 Azure Storage 계정 암호화
- BlackCat(Alphv)은 지속적으로 전략을 개선해 나가며 전 세계 기업을 대상으로 공격 수행

* Azure Storage : 클라우드 기반의 데이터 저장 및 관리 서비스

IAB, Microsoft Teams 피싱을 통해 계정 탈취

- 초기 침투 경로를 제공하는 IAB 그룹 중 하나가 Microsoft Teams를 통한 피싱 공격을 수행 중
- Microsoft는 해당 공격 방어를 위해 Teams에서 외부 사용자를 더 잘 식별하고 경고하는 업데이트 수행

Vidar 및 RedLine, 랜섬웨어로 전향

- Vidar 및 RedLine 그룹이 랜섬웨어를 유포하는 것으로 전환
- 사용자는 파일 다운로드 시 검증되지 않은 출처를 피하고 시스템 보안을 강화해야 함

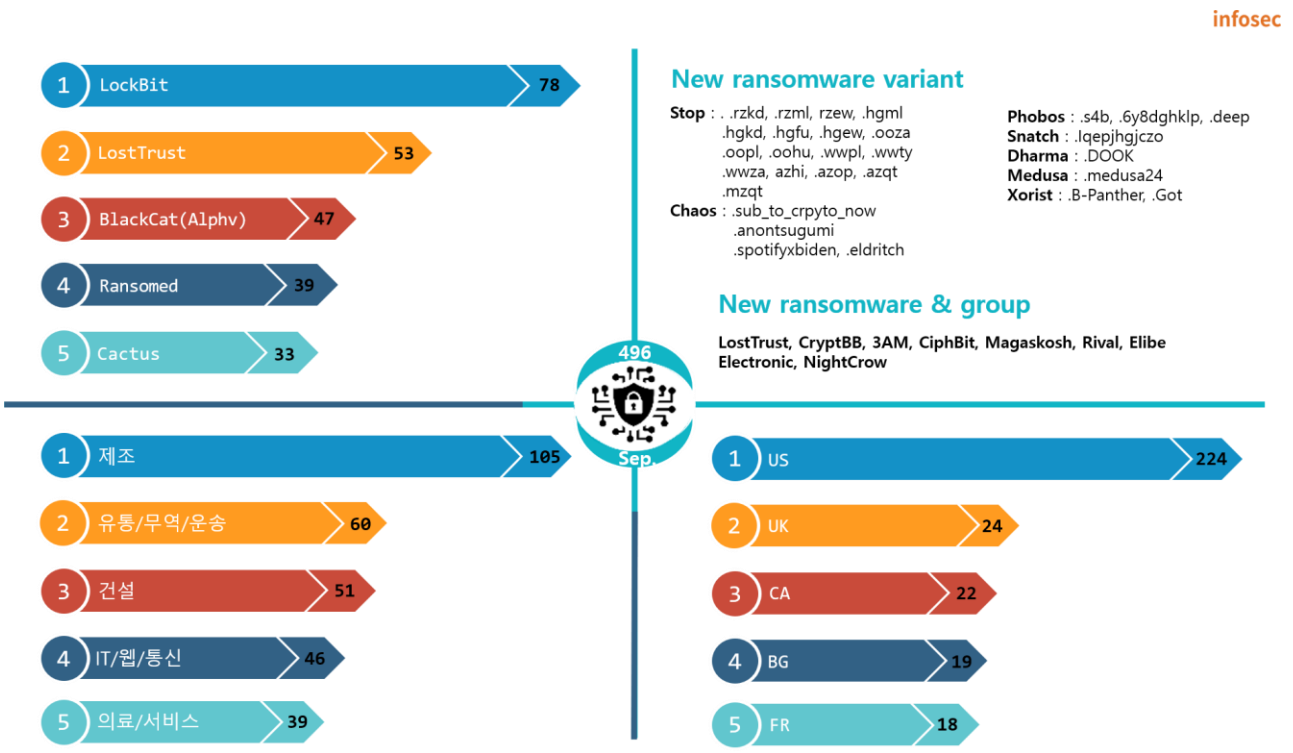
Ransomed, 일본 대형 제조, 통신 기업 공격

- 일본 제조 업체인 Sony 기업 공격 후 금전 협박을 시도했으나 협상이 되지 않아 유출 데이터 게시
- 일본 대형 기업인 NTT 도코모를 공격 후에 복호화 금액으로 101만 5000달러(한화 약 13억 6070만원) 요구

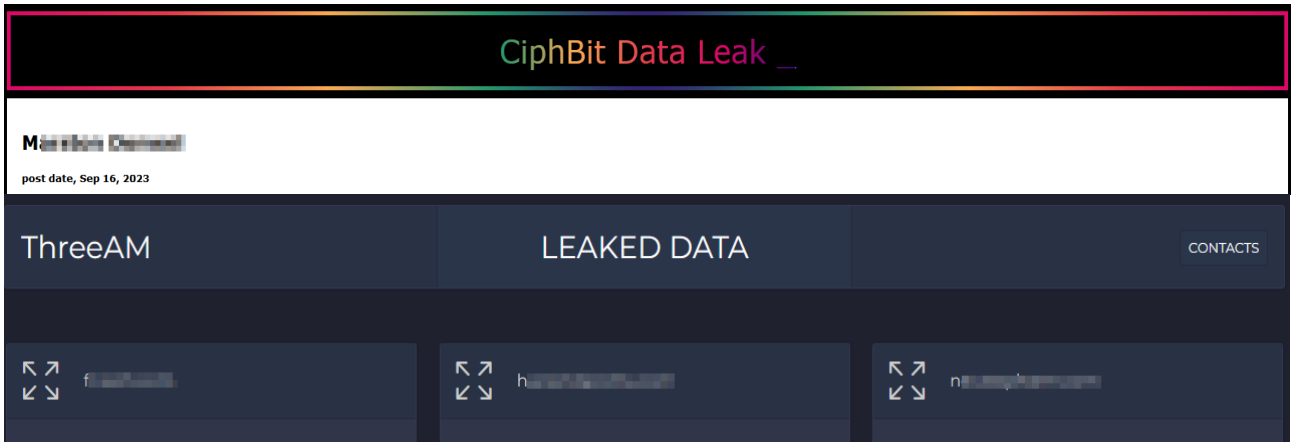
Rhysida, 쿠웨이트의 재무부 공격

- 재무부의 일부 시스템이 랜섬웨어에 영향을 받아 차단 조치
- 정부의 금융 시스템은 분리되어 있어 급여 이체 절차는 영향이 없다고 밝힘

■ 랜섬웨어 위협



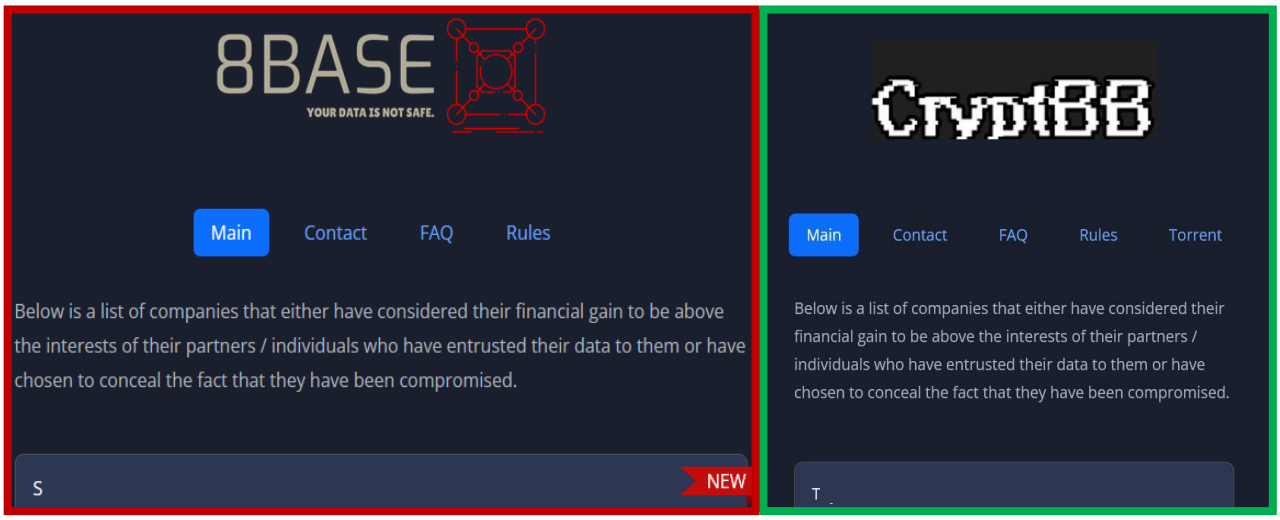
새로운 위협



*출처: CiphBit, 3AM 랜섬웨어 그룹 사이트 이미지

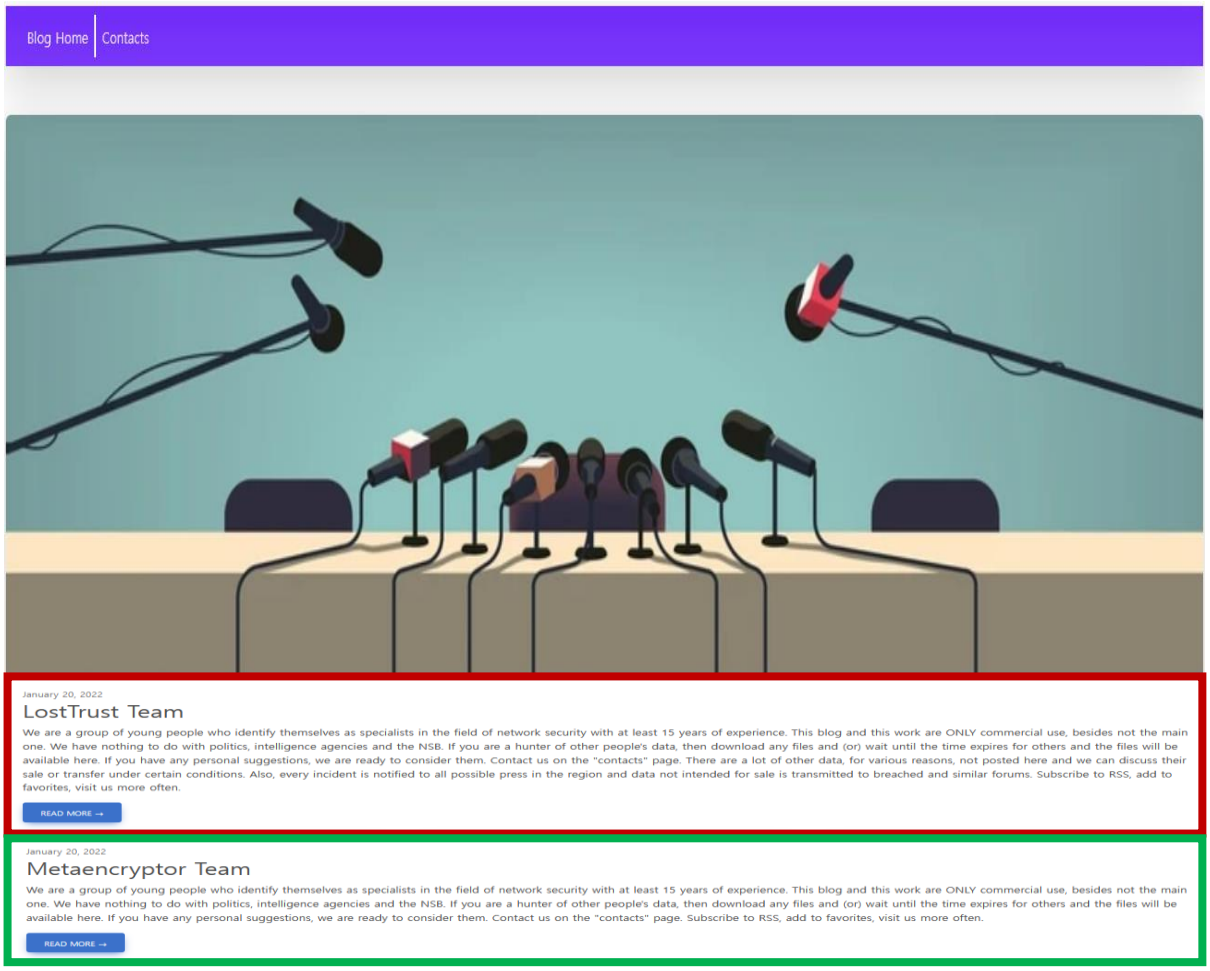
최근 신·변종 랜섬웨어와 관련 그룹들의 활동이 심상치 않은 모습을 보이고 있다. 새롭게 발견된 3AM 랜섬웨어는 LockBit 계열사가 공격 수행 중 보안 시스템에 의해 차단되자 대안으로 사용된 것으로 확인됐다. 3AM 은 기존 랜섬웨어 샘플 군과의 연관성은 확인되지 않고 있다. 3AM 랜섬웨어는 Rust 언어로 작성됐으며, 부분 암호화, 로컬/네트워크 드라이브 암호화, 랜섬노트에 기재되는 Access key 등의 옵션을 제공하고 있다.

CiphBit 그룹은 등장과 동시에 8 개의 피해 기업 데이터를 공개했다. 이들은 랜섬웨어를 유포하는 전략으로 불가리아 경찰을 가장하는 방식을 사용했다. 유포된 모든 경로가 확인되지 않았지만, 대부분은 피싱 메일을 통해 유포되기 때문에 출처가 의심되는 이메일의 첨부파일이나 링크는 클릭하지 않는 것이 중요하다. 수사기관의 경우에는 개인에게 메일을 통해 출석을 요구하지 않는다는 사실을 인지하고 있어야 피해를 예방할 수 있다.



*출처: 8base, CryptBB 랜섬웨어 그룹 사이트 이미지

9 월 새롭게 발견된 CryptBB 랜섬웨어 그룹은 8base 랜섬웨어 그룹과 상당히 유사한 모습을 보이고 있다. CryptBB 그룹은 8base 그룹과 동일한 다크웹 유출 사이트 디자인 및 피해 대상을 일부 게시했다. 하지만, 이들의 그룹 사이트에는 8base 그룹에서 이미 게시한 일부 데이터만 존재하고 지속적으로 업데이트가 되지 않고 있어 8base 그룹을 모방한 것처럼 보인다. 이를 뒷받침하듯 8Base 측은 CryptBB 그룹과의 연관성은 없으며 단지 자신들을 모방하고 있다고 주장했다.



*출처: LostTrust, MetaEncryptor 랜섬웨어 그룹 사이트 이미지

이와 비슷하게 지난 8 월 발견된 MetaEncryptor 그룹과 9 월에 발견된 LostTrust 랜섬웨어 그룹의 사례도 있다. 두 랜섬웨어 그룹은 동일한 다크웹 유출 사이트 디자인과 비슷한 소개 문구를 사용하고 있다. 하지만 앞서 설명한 CryptBB, 8base 그룹 사례와는 달리 게시한 피해 대상이 모두 다른 특징을 보이고 있다(MetaEncryptor 그룹 12 건, LostTrust 그룹 53 건). 이처럼 랜섬웨어 그룹 간의 모방이 빈번해지고 있다. 이는 홍보 효과를 얻거나 자신들의 위협을 과시하기위한 전략 중 하나로 볼 수 있다.

Top5 랜섬웨어

LockBit 랜섬웨어 그룹은 지난달에 이어 이번달에도 활발한 활동을 보이며 많은 피해 사례를 발생시켰다. 최근 LockBit 랜섬웨어 그룹은 운영 이슈로 인해 많은 계열사가 이탈하거나 불만을 표출하는 등 한차례 해프닝이 있었다. 이를 극복하고 이전과 같은 영향력을 과시하기라도 하듯 지난달 122 건에 이어 이번 달에는 78 건의 피해 사례를 기록했다.

최근 LockBit 랜섬웨어 그룹은 대규모 공격의 일환으로 상용 원격 모니터링 및 관리 도구인 RMM(Remote Monitoring and Management)을 악용하여 타깃 네트워크에 침투하고 전파하는 랜섬웨어 공격을 지속적으로 수행하고 있다. 특히, 이들은 합법적인 소프트웨어를 사용하여 탐지를 회피하는 전략을 사용하고 있어 주의가 필요하다. 또한, RMM 도구를 악용하는 방식의 공격이 수행되고 있는 만큼 다중 인증을 설정하고 피싱에 주의하는 등 개인 및 조직의 보안에 힘써야 한다.

새롭게 발견된 LostTrust 랜섬웨어 그룹은 앞서 언급한 바와 같이 MetaEncryptor 그룹과 다크웹 유출사이트의 동일한 디자인과 비슷한 문구 사용으로 연관성 혹은 모방의 가능성이 있다. 그러나, 아직 이들과 다른 그룹 간의 모방 및 연관성이 있는지 대해서 직접적으로 밝혀진 내용은 없다. 다만 LostTrust 랜섬웨어를 분석한 결과, 2020 년에 발견된 SFile 랜섬웨어와 코드 유사성이 확인되고 있어 해당 소스 코드를 차용했거나 리브랜딩 했을 가능성이 있다. LostTrust 랜섬웨어 그룹은 9월 총 53건의 피해 기업을 게시했으며, LockBit 랜섬웨어와 비교될 만큼 상당히 많은 수의 피해를 발생시킨 것으로 확인된다.

BlackCat(Alphv) 그룹은 미디어, 리조트, Azure Storage 등 다양한 대상을 타깃으로 삼아 꾸준히 공격을 수행하고 있다. 이들은 Windows를 비롯해 Linux, ESXi 등 다양한 환경을 대상으로 공격을 수행할 수 있는 랜섬웨어 변종을 보유하고 있다. 또한, RMM, 취약점 등을 악용한 공격도 지속하고 있어 상당히 위협적인 그룹이라고 할 수 있다.

지난 8 월에 발견된 Ransomed 그룹도 다양한 분야의 기업들을 대상으로 공격을 시도하고 있다. 8 월에 발견되었음에도 불구하고 77 개의 많은 계열사를 보유하고 있는 것으로 확인됐다. 특히, 이들은 사이버 범죄 활동 외에도 여러 합법적 사업체를 보유하고 있으며, 사업체에 자금을 조달하기 위해 사이버 범죄로 갈취한 금전을 세탁하는 방식으로 운영하고 있다고 주장하고 있다.

Cactus 랜섬웨어 그룹은 지난 3 월 처음 발견됐으나, 7 월부터 다크웹 유출 사이트를 개설하며 다양한 활동을 펼치고 있다. 이들은 탐지를 회피하기 위해 바이너리를 자체 암호화하는 방식을 사용하는데 주로 VPN 취약점을 악용한 초기 침투 방법을 사용하는 것으로 확인된다. 주로 미국, 영국 등 영어권 국가를 대상으로 제조, 유통, 건설 등 산업 전반에서 랜섬웨어 공격을 수행하고 있으며, 파일 암호화 전 탈취한 데이터를 유출 사이트에 게시하여 협박하는 전략을 사용하고 있다.

■ 랜섬웨어 집중 포커스

Knight 랜섬웨어 개요

*출처: Knight 랜섬웨어 그룹 사이트 이미지

Knight 는 2023 년 6 월경에 발견된 Cyclops 가 리브랜딩 한 랜섬웨어 그룹이다. 이전에 발견된 Cyclops 랜섬웨어는 비주류 언어인 Go 언어로 개발되었으나 Knight 랜섬웨어는 플랫폼 별로 다양한 빌더를 제공해 Windows, Linux, macOS, ESXi, Android 플랫폼을 모두 감염시킬 수 있도록 설계됐다. 랜섬웨어 공격도 다양한 방식으로 전개 중이다. 암호화 또는 정보 탈취형 악성코드를 포함한 풀 버전 랜섬웨어와 파일 암호화만 진행하는 경량 버전을 혼용해 배포하고 있다. 최근에는 Tripadvisor 컴플레인을 가장한 스팸 캠페인 공격도 확인됐는데, 해당 캠페인에서는 Microsoft Excel 의 추가 기능 파일인 .xll[5] 형태로 공격을 시도했다.

Knight 랜섬웨어 그룹은 러시아와 유럽 출신 해커 4 명으로 구성되어 있다. RaaS(Ransomware-as-a-Service)로 제공되는 Knight 랜섬웨어는 오랜 기간 준비된 것으로 확인된다. 이들은 서비스를 제공받는 계열사를 위해 사용하기 편리한 인터페이스를 구축하고 경량 버전, 풀 버전 등 여러 공격 방법 및 다양한 플랫폼을 공격할 수 있도록 서비스를 제공하고 있다. 특히 풀 버전에서 제공하는 정보 탈취형 악성코드에 감염될 경우, 탈취된 데이터와 개인 정보가 2 차 공격에도 사용할 수 있으며, 유출된 정보를 이용해 이중 협박도 받을 수 있어 주의가 필요하다.

[5] xll : C 언어 계열로 작성된 DLL 파일로 Microsoft Excel 에서 사용자 지정 함수 또는 기타 기능을 개발하여 Excel 에서 사용할 수 있도록 하는 추가 기능 파일

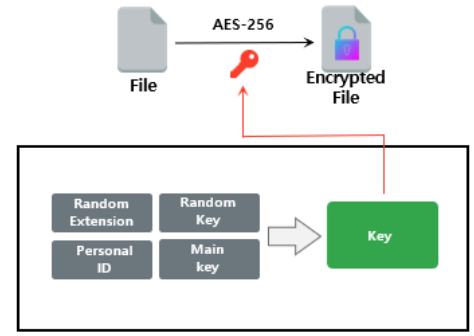
Knight 랜섬웨어 그룹은 일반적인 서비스형 랜섬웨어에서 제공하는 기능뿐만 아니라 차별화되고 고도화된 기능을 제공하고 있다. 이들은 복호화 비용 지불을 위한 간소하고 자동화된 결제 시스템, 계열사별 독립적인 다크웹 채팅 및 피해자별 개별 지갑 주소 제공, 그리고 맞춤형 지원을 통해 계열사가 요구하는 사항을 적극적으로 반영하여 지원하고 있다. 이러한 모습은 상당한 기술력을 보유하고 있음을 시사하며, 다른 서비스형 랜섬웨어들과는 차별화된 기능이다. 이러한 차별성을 강조하며 Knight 랜섬웨어 그룹은 계열사를 늘리기 위해 적극적인 홍보와 활동을 이어가고 있다.

Knight 랜섬웨어는 버전에 따라 랜덤한 확장자 또는 'knight_l'를 사용하며, 파일 용량이 클 경우 간헐적으로 암호화를 수행하고 각 파일마다 다른 키를 사용하여 복호화를 어렵게 한다는 특징이 있다. 또한, 실행을 위해서는 Access-Key 또는 서버에서 제공하는 바이너리를 통해 쉘코드를 생성 후 실행이 필요하여 임의로 분석하기 어려운 구조를 가지고 있다. 암호화 키 생성 과정에는 랜덤 확장자 + 피해자 고유 ID + 주요 키 + 랜덤 키의 조합이 필요하며 랜덤하게 형성되는 요소들에 대해서 파악하고 복호화 한다는 것은 매우 어려운 일이므로 임의로 랜섬웨어를 복호화 하지 못하도록 여러 방어 기제를 조합한 것으로 보인다. 한편, ChaCha20 + AES256 을 사용하는 암호화 로직은 LockBit 과 Babuk 의 로직과 유사하여 연관성이 의심되기도 한다.

Knight Ransomware

암호화 키

AES-256으로 파일 암호화를 수행하고 해당 키를 ChaCha20으로 암호화



특징

RaaS

DLL Side-Loading

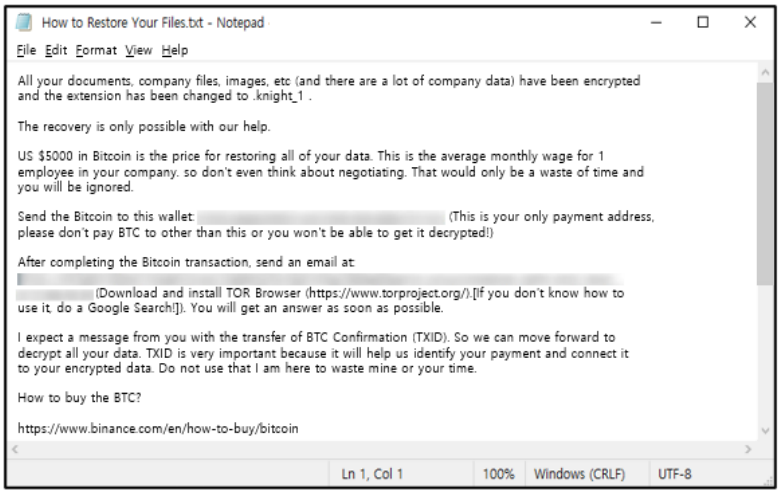
부분 암호화

AES-256 & ChaCha20 암호화

Anti-VM & Anti-Sandbox

서비스 프로세스 종료

랜섬노트



How To Restore Your Files.txt

변경 확장자

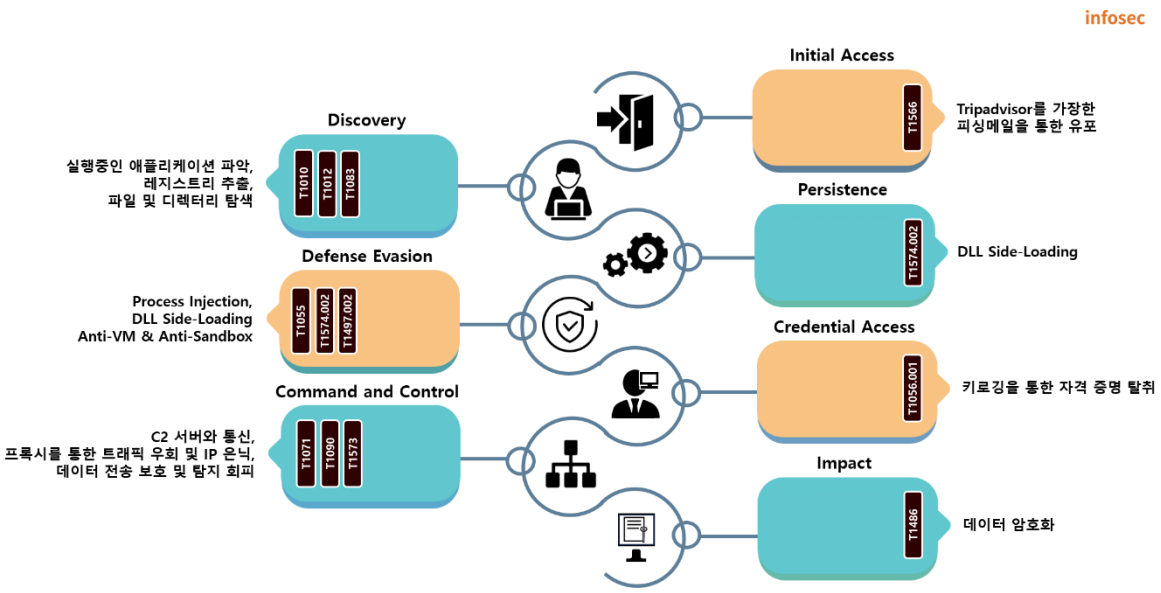
무작위 생성

Knight_I

제작 언어

C++

Knight 랜섬웨어 전략



Knight 랜섬웨어는 Windows, Linux, macOS, ESXi, Android 와 같이 다양한 플랫폼을 타깃으로 한다. 이 랜섬웨어는 최근 Tripadvisor 의 컴플레인 페이지를 가장하여 피싱 메일을 통해 유포되고 있다. 피싱 메일에 연결된 페이지를 통해 최초 실행되는 Shellcode 가 다운로드 되며 두번의 복호화 이후 정상 프로세스에 Injection[6] 후 실행된다. 탐지 회피 기술로는 DLL Side-Loading[7], Anti-VM[8] 및 Anti-Sandbox[9] 기법과 파일 및 실행에 필요한 정보를 난독화 하는 특징을 가지고 있다.

Knight 랜섬웨어는 개인 정보 탈취를 위해 키로깅[10]을 사용하여 사용자의 입력을 가로채기도 한다. 이 밖에도 추가적인 행위를 위해 시스템, 네트워크, 소프트웨어, 파일 및 디렉토리에 대한 검색을 수행하여 다양한 정보를 수집하고, 중요 데이터 수집을 위해 스크린 샷을 찍는 기능과 클립보드 데이터를 수집하는 기능도 탑재되어 있다.

---

[6] Injection : 악의적인 DLL 을 정상 프로그램에 삽입하여 실행하는 기법

[7] DLL Side-Loading : 프로그램에서 사용하는 정상 DLL 대신 악의적인 DLL 을 로드하여 실행하는 공격 기법

[8] Anti-VM : 가상머신에서 실행 중인지 검증하여 분석을 우회하는 기법

[9] Anti-Sandbox : 샌드박스에서 실행 중인지 검증하여 분석을 우회하는 기법

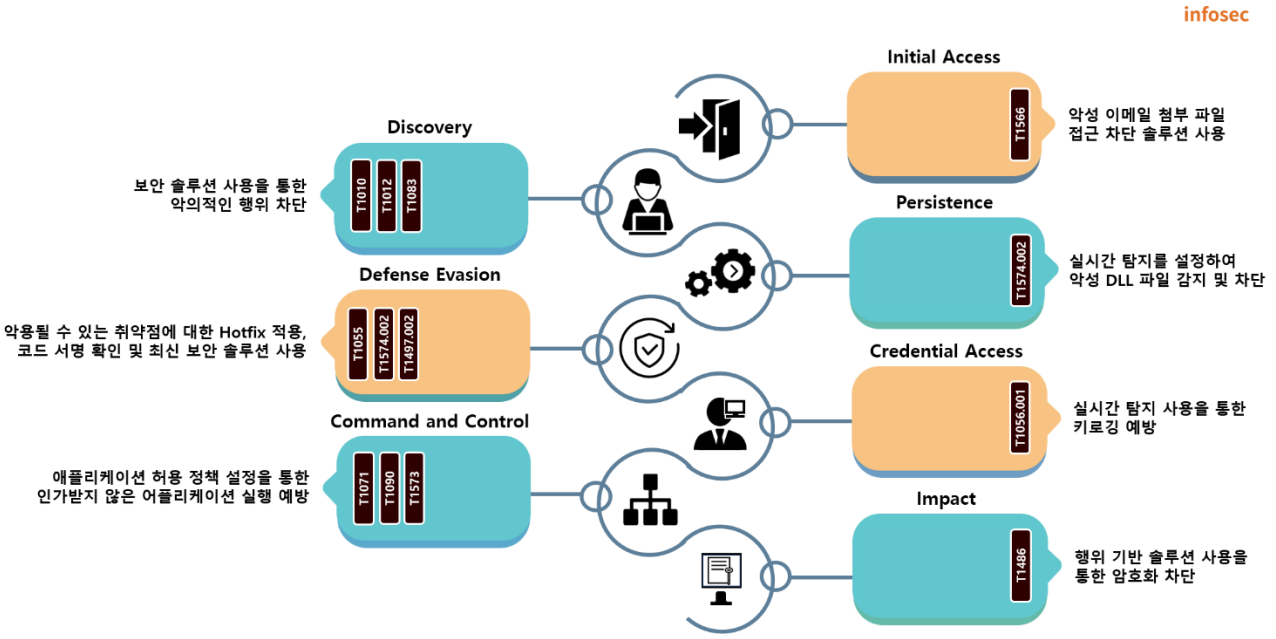
[10] 키로깅 : 사용자가 키보드로 입력하는 키를 기록하는 기법

특히, Knight 랜섬웨어는 로컬 드라이브와 SMB(Server Message Block)[11]를 통한 네트워크 파일 암호화까지 가능하다. 주목할 점은 보통의 랜섬웨어는 복구를 방해하기위해 데이터 백업 무력화 기능을 수행하는데, 특이하게도 Knight 랜섬웨어에서는 해당 기능이 확인되지 않아 경우에 따라서 일부 복구가 가능할 수도 있다.

Knight 랜섬웨어는 파일 암호화뿐만 아니라 풀 버전에서 제공하는 정보 탈취형 악성코드를 통해 파일 암호화 전 데이터를 유출하는 이중 협박 전략을 사용하고 있다. 정보 탈취형 악성코드는 탈취 대상 파일의 최대 크기, 데이터를 분할하여 전송할 수 있는 옵션, 탈취 대상 경로, 확장자 등 다양한 옵션을 제공하고 있다.

[11] SMB : 네트워크에 존재하는 자원을 공유할 수 있도록 설계된 윈도우 운영체제의 프로토콜

Knight 랜섬웨어 대응방안



Knight 랜섬웨어는 기본적인 시스템의 기능을 악용하여 악성 행위를 수행하기 때문에 대응 방안이 제한적이다. 먼저, Knight 랜섬웨어는 피싱 메일 캠페인으로 유포되고 있어 출처가 불분명한 이메일의 첨부파일이나 링크 등을 실행하지 않도록 주의해야 한다. 보다 적극적인 대응을 위해서는 악성 메일을 차단하는 시스템, 콘텐츠 무해화 솔루션(CDR) 등을 적용할 필요가 있다.

두번째로는 Knight 랜섬웨어는 시스템 내에서 은밀히 동작하고 탐지를 피하기 위해 레지스트리 조작 및 각종 시스템 요소들에 대해 검색을 수행한다. DLL Side-Loading 과 Process Injection 을 통해 권한 상승 및 파일 암호화를 수행하는 것이 이들의 대표적인 방법이다. 이러한 합법적인 시스템 기능을 악용하는 것을 예방하기 위해서는 악의적인 행위를 탐지하는 실시간 보안 솔루션 사용을 통해 랜섬웨어를 차단해야 한다. 또한, 내부 확산 과정에서 SMB 를 통한 네트워크 암호화를 진행하기 때문에 SMB 포트 차단을 통한 선제적 예방 조치가 필요하다.

마지막으로, 시스템 최신화 및 보안 패치를 적용할 수 있도록 정기적인 업데이트가 필요하며 로그 이벤트, 이상 징후를 탐지할 수 있는 모니터링을 통해 위협을 탐지할 수 있어야 한다. 환경에 따라 모든 방어적 조치를 적용하기 어려울 수 있지만 기업 환경에 맞는 프로세스를 수립하여 단계별로 랜섬웨어를 차단 및 경감시킬 수 있는 방안을 수립해야 한다.

Indicator Of Compromise

Knight : SHA256

5ACE35ADEB360B9E165E7C55065D12F192A3EC0CA601DD73B332BD8CD68D51FE

75E227A3A41DC1C2D4384E877D88F9A06437A49F2C71F8EFA7E2CC60BAB6CC4A

4F1E46AC9E46F019D3BE3173F0541F5ED07BDE6389180CD7E8255D35B49F812E

DCD45491DD78122EFEDE7AE460A4D3E0B20AEB13965A8EB14EEF862FBCE66366

262618E0D48DB5B244759E07787DDE11736555AC0BD3C64FEE2556DA50DEA02

9123E42CDD3421E8F276AC711988FB8A8929172FA76674EC4DE230E6D528D09A

File Name

TripAdvisor Complaint - Possible Suspension.exe
TC4ShellHost.64.exe
TripAdvisor_Complaint-Possible-Suspension.xll
TripAdvisor-Complaint-Avywfp.PDF.htm

■ 참고 사이트

URL : https://cert-agid.gov.it/news/il-ransomware-knight-distribuito-in-italia-tramite-falsa-fattura/

URL : https://gridinsoft.com/blogs/qakbot-hacked-removed-from-700k-machines/

URL : https://www.mirror.co.uk/news/uk-news/russia-linked-hackers-hit-uk-30850139

URL : https://thecyberexpress.com/cactus-ransomware-group-major-corporations/

URL : https://www.bleepingcomputer.com/news/security/cisco-warns-of-vpn-zero-day-exploited-by-ransomware-gangs/

URL : https://www.bleepingcomputer.com/news/security/us-and-uk-sanction-11-trickbot-and-conti-cybercrime-gang-members/

URL : https://www.scmagazine.com/brief/save-the-children-suspected-to-be-compromised-by-bianlian-ransomware

URL : https://www.bleepingcomputer.com/news/security/hackers-use-new-3am-ransomware-to-save-failed-lockbit-attack/

URL : https://www.infosecurity-magazine.com/news/cuba-ransomware-undetectable/

URL : https://www.bleepingcomputer.com/news/security/ransomware-access-broker-steals-accounts-via-microsoft-teams-phishing/

URL : https://www.trendmicro.com/en_us/research/23/i/redline-vidar-first-abuses-ev-certificates.html?&web_view=true

URL : https://www.teiss.co.uk/news/news-scroller/airbus-investigating-major-cyber-attack-claimed-by-the-ransomed-hacker-group-12856

URL : https://cybersecuritynews.com/ransomed-vc-japanese-giants/

URL : https://securityaffairs.com/151501/cyber-crime/rhysida-ransomware-kuwait-ministry-of-finance.html