Keep up with Ransomware

지속되는 BlackSuit 랜섬웨어 위협

■ 개요

2023 년 12 월 랜섬웨어 공격으로 인한 피해 사례 발생 건수는 전월(497 건) 대비 약 15% 감소한 420 건으로 나타났다. 이번 달에도 많은 랜섬웨어 이슈들이 발생했는데, 그중에서도 주목할 이슈는 대표적인 RaaS(Ransomware-as-a-Service) 그룹인 BlackCat(Alphv)의 랜섬웨어 인프라가 FBI 국제 공조에 의해 상당 부분 무력화된 것이다. BlackCat(Alphv)은 전 세계적인 악명을 떨치고 있는 랜섬웨어 그룹으로 과거 Colonial Pipeline 을 공격했던 Darkside 가 전신이다. 이들은 1,000 개가 넘는 기업과 기관을 대상으로 데이터를 탈취해왔으며, 피해자들로부터 갈취한 범죄 수익은 3 억 달러(한화 약 3950 억 원)에 이른다.

FBI 는 이번 국제 공조를 통해 BlackCat(Alphv)의 네트워크 및 다크웹 사이트 일부를 폐쇄시키고 이들이 주로 사용하는 **랜섬웨어 복호화 키**를 확보했다. 이로써 BlackCat(Alphv)의 공격으로 피해를 입었던 400 여 개의 학교 와 병원 등의 주요 기반 시설에서 복구 금액인 약 6,800 만 달러(한화 약 886 억 원)를 지불하지 않고도 랜섬웨어에 의해 피해를 입었던 인프라를 복구할 수 있게 됐다. 그러나 BlackCat(Alphv)은 이를 단순 호스팅 문제라고 주장하며 다크웹 유출 사이트를 다시 오픈했으며, 계열사들에게 병원 및 원자력 발전소와 같은 민감한 인프라를 대상으로도 공격 수행을 허가하는 취지의 공지사항을 게시했다. 이후 또다시 FBI 가 유출 사이트를 압수했지만, 이들은 계속해서 다른 도메인을 통해 유출 사이트를 오픈하고 여러 대상을 타깃으로 공격을 수행하고 있다는 글을 게시하고 있다.

한편, BlackCat(Alphv)이 어려움을 겪는 동안 또 다른 주요 랜섬웨어 그룹 LockBit 이 BlackCat(Alphv)의 계열사에 LockBit 으로 합류할 것을 제안한 정황이 확인됐다. 실제로 BlackCat(Alphv)의 공격 사례로 게시됐던 독일 에너지청 관련 자료가 LockBit 의 다크웹 사이트에 등록되기도 했다. BlackCat(Alphv) 그룹은 최근 사건을 언급하며 LockBit 에 대한 감사를 표현하는 게시글을 XSS(Cross-Site Scripting) 포럼[1]에 작성했다. LockBit 또한 카르텔 형성의 필요성을 언급하며 응원의 메시지와 협력이 필요하다고 전했다.

[1] XSS 포럼 : 해킹 도구를 팔거나 관련 정보를 주고받는 다크웹 포럼

최근 글로벌 법 집행기관들의 협력으로 인해 많은 랜섬웨어 그룹들이 압박 받아 사라지고 있다. 이러한 상황은 주요 랜섬웨어 그룹들의 경각심을 불러일으키고 있다. 이번 계기로 랜섬웨어 카르텔이 형성된다면 전술, 전략적 변화가 발생할 수 있으며, 이로 인한 위협이 급증할 수 있다. 이를 미리 예방하고 대응하기 위해서는 선제적이고 통합적인 대응이 필요하다.

협력 관계를 조성하기 위한 움직임은 다른 랜섬웨어 그룹들에서도 확인되고 있다. 최근 BianLian 과 White Rabbit, Mario 랜섬웨어 그룹이 공동으로 APAC(Asia-Pacific) 지역의 금융 기관을 목표로 특정 해상 물류 회사의 비즈니스 계정을 해킹하여 악성 이메일을 배포하는 BEC(Business Email Compromise)[2] 공격을 수행한 것이 확인됐다. 동시에 이들은 중국, 대만, 태국, 한국, 인도 등의 IP 를 악용하여 비밀번호 Brute Force Attack[3]을 통한 Microsoft Exchange 서버 해킹을 시도하기도 했다. 이로 인해 랜섬웨어 감염과 데이터 탈취 등의 피해가 발생했으며, 피해 기업들은 금전을 요구하는 협박성 이메일과 전화에 시달렸다.

앞으로 랜섬웨어 그룹 간의 협력은 더욱 늘어날 것으로 예상된다. FBI 를 비롯한 국제 수사 기관이 기존의 IP 차단과 같은 완화적인 대응을 넘어 공격자들의 근거지를 직접 타격하는 방식의 움직임을 보이고 있기 때문이다. 또한, IAB(Initial Access Broker)[4]의 중요성이 강조됨에 따라 이들과 협력하는 랜섬웨어 그룹들이 늘어나고 있으며, 서로의 공격 전략과 인프라가 겹쳐 협력하는 상황이 발생할 것으로 보인다.

이 밖에도 Royal 에서 BlackSuit 로 리브랜딩 한 랜섬웨어 그룹이 국내 A 기업을 공격한 것으로 확인됐다. BlackSuit 가 다크웹 유출 사이트에 게시한 데이터에는 고객의 개인 정보도 포함되어 있어 해당 서비스 이용자들은 피싱이나 스미싱과 같은 추가적인 범죄에 노출될 수 있어 주의가 필요하다. 실제로 개인 정보가 노출된 일부 피해자들이 유출 사건을 언급하며 사과의 뜻으로 주식을 선물하겠다는 취지의 피싱 문자를 수신한 것으로 확인됐다. 이러한 피싱 문자를 수신했을 경우, 수사 기관에 신고 혹은 삭제하여 2 차 피해를 예방하고, 확인이 어려운 상황일 경우 관련 기관에 문의하는 등 주의해야 한다. BlackSuit 는 해당 기업을 포함해 12 월에만 건설, 교육, 유통 등 국내외 5 개 기업의 유출 데이터를 게시했다.

[2] BEC : 공격자가 신뢰할 수 있는 인물로 가장하여 이메일을 통해 돈이나 기밀 정보를 요구하는 행위

[3] Brute Force Attack : 가능한 모든 조합을 시도하여 비밀번호를 해독하는 무차별 대입 공격 기법

[4] IAB : 초기 침투 경로를 판매하는 개인 혹은 집단

■ 랜섬웨어 뉴스

infosec

중국, ChatGPT를 악용해 랜섬웨어 공격에 사용한 공격자 4명 체포

- ChatGPT를 통해 랜섬웨어를 개발한 혐의로 4명을 체포
- 중국 A회사 시스템에 랜섬웨어 공격 후, 몸값으로 20,000 Tether(한화 약 2,640만 원) 요구
- 체포된 공격자들은 랜섬웨어 개발, 최적화 과정에서 ChatGPT 사용

BlackCat(Alphv) 다크웹 유출 사이트, FBI에 의해 폐쇄

- BlackCat(Alphv)은 그간 1,000여개의 조직으로부터 3억 달러(한화 약 3,950억 원)의 몸값을 갈취
- FBI는 복호화 도구를 손에 넣어 400여개의 조직에 대해 무료로 복호화 서비스 제공
- BlackCat(Alphv)과 수사기관이 실랑이를 벌이며 유출 사이트 폐쇄와 복구를 반복

BlackBasta 랜섬웨어의 결함을 통해 복호화 도구 개발

- BlackBasta 랜섬웨어 피해 복구를 돕는 복호화 도구, 독일 SRLabs에서 출시
- BlackBasta 측은 결함을 인지하고 새롭게 수정된 랜섬웨어를 배포

핵티비즘 그룹 SiegedSec, 다크웹 유출 사이트 폐쇄

- 2022년 2월부터 활동을 개시한 친 러시아 성향의 핵티비즘 그룹 SiegedSec의 다크웹 유출 사이트 폐쇄
- SiegedSec은 GhostSec과 같이 다른 핵티비즘 그룹과도 제휴를 맺는 등 활발한 활동을 지속해 옴

DragonForce, 야쿠르트 호주 지사를 비롯한 21개 조직 공격

- DragonForce는 12월 20일 유출 사이트에 야쿠르트 호주 지사에 대한 공격을 주장 후 95GB 상당의 데이터 유출
- 12월에 처음 발견된 그룹으로, 핵티비스트 그룹인 DragonForce Malaysia와는 연관성이 밝혀지지 않음
- 이외에도 제조, 건설, 유통 등의 다양한 산업군에 대한 공격을 수행

Werewolves, 다양한 산업군에 걸친 공격 수행하여 23개 조직 침해 주장

- 12월에 처음 발견된 Werewolves는 러시아어로 작성된 서피스 웹 사이트를 운영
- 자체 버그바운티를 운영하며, 전 세계 기업의 사이버 보안을 강화하는 것을 사명이라고 주장

* 서피스 웹 : 검색엔진으로 찾을 수 있는 일반적인 웹 사이트

RansomedVC의 계보를 잇는 신규 랜섬웨어 그룹 Raznatovic 등장

- 12월에 처음 발견된 Raznatovic는 RansomedVC의 인프라를 구매한 것으로 추정
- 다크웹 유출 사이트에 5개의 조직에 대한 게시글을 업로드하였으나 현재는 접속 불가

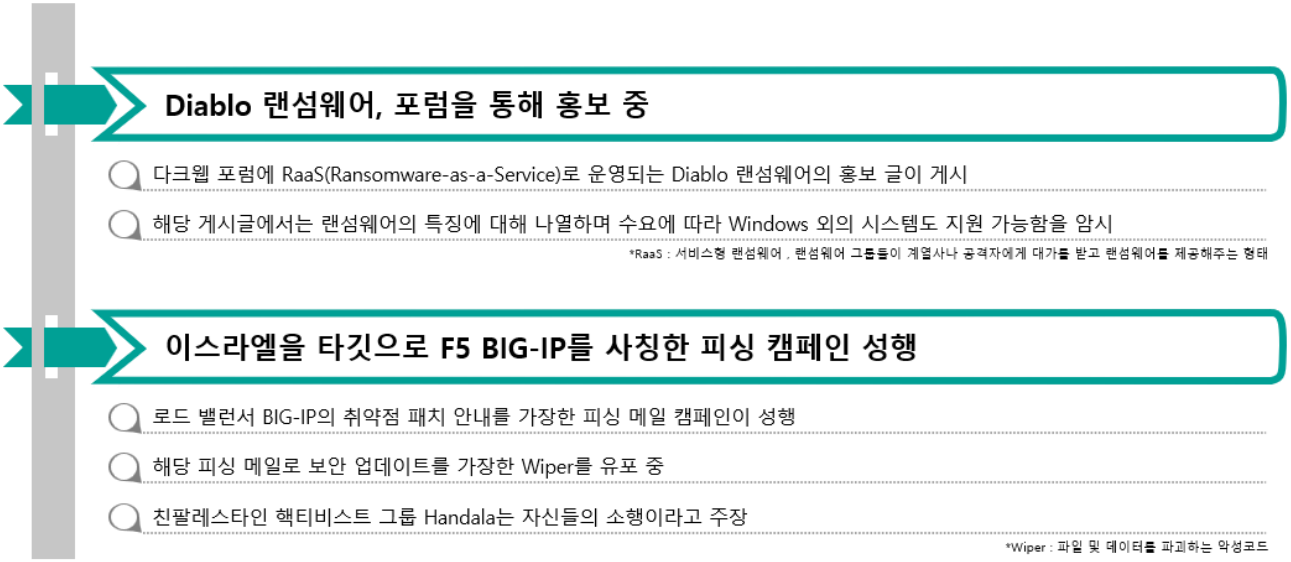

Diablo 랜섬웨어, 포럼을 통해 홍보 중
다크웹 포럼에 RaaS(Ransomware-as-a-Service)로 운영되는 Diablo 랜섬웨어의 홍보 글이 게시
해당 게시글에서는 랜섬웨어의 특징에 대해 나열하며 수요에 따라 Windows 외의 시스템도 지원 가능함을 암시
*RaaS : 서비스형 랜섬웨어 , 랜섬웨어 그룹들이 계열사나 공격자에게 대가를 받고 랜섬웨어를 제공해주는 형태
이스라엘을 타깃으로 F5 BIG-IP를 사칭한 피싱 캠페인 성행
로드 밸런서 BIG-IP의 취약점 패치 안내를 가장한 피싱 메일 캠페인이 성행
해당 피싱 메일로 보안 업데이트를 가장한 Wiper를 유포 중
친팔레스타인 핵티비스트 그룹 Handala는 자신들의 소행이라고 주장
*Wiper : 파일 및 데이터를 파괴하는 악성코드

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

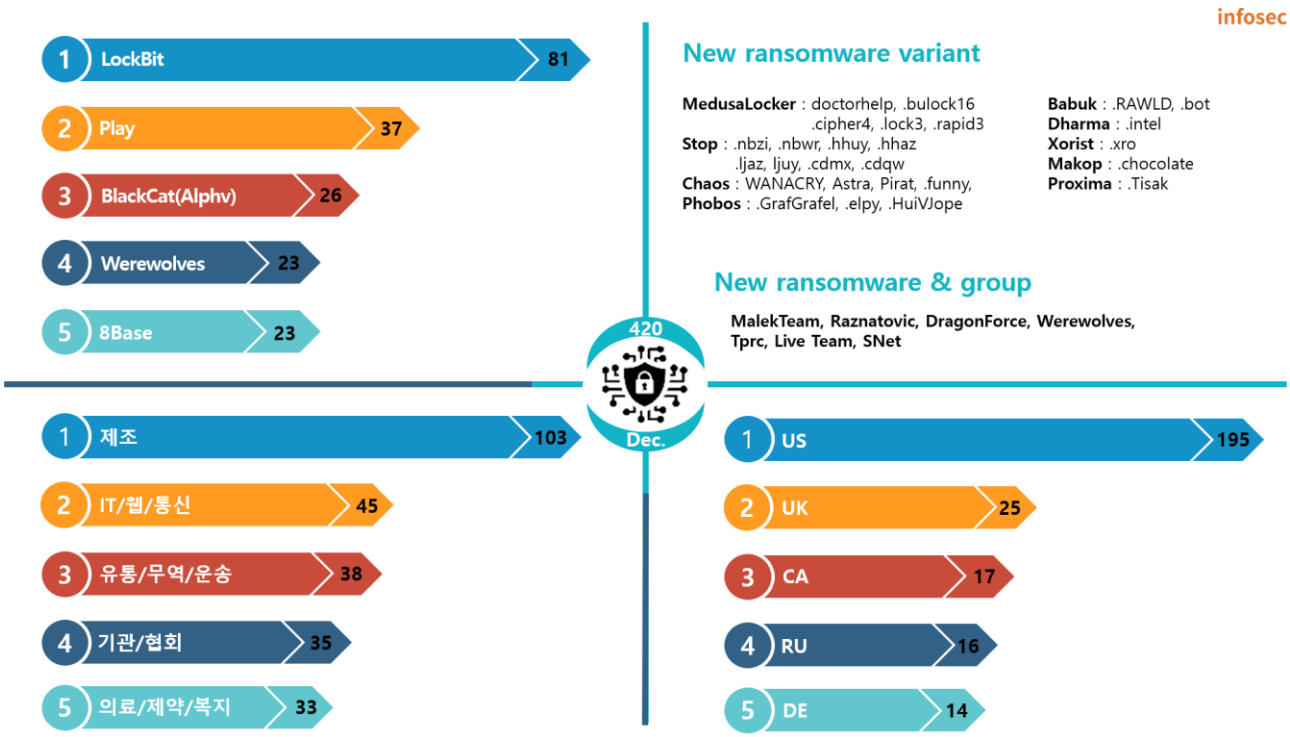


그림 2. 2023 년 12 월 랜섬웨어 위협 현황

새로운 위협

12 월 새롭게 발견된 신규 랜섬웨어 그룹으로는 Malek Team, Raznatovic, DragonForce, Werewolves 가 있다. Malek Team 은 서피스 웹 사이트와 텔레그램 채널을 운영하고 있으며 자신들을 사이버 해킹 분야의 다국적 팀으로 소개하고 있다. 이들은 이스라엘의 병원과 제조업체를 포함한 5 개 조직에 대해 공격을 수행했다는 글을 게시했으며, 이 중 일부는 유출 데이터도 포함된 것으로 확인됐다.

Raznatovic의 경우는 RansomedVC의 계보를 잇는 그룹이다. RansomedVC는 지난 10월에 활동을 개시해 소니(Sony)를 해킹했다고 주장하며 주목받은 랜섬웨어 그룹이다. 이들은 활동 개시 첫 주에만 200 명 이상의 회원을 확보한 이력을 보유하고 있다. 그러나 수사기관의 압박이 시작되자 돌연 랜섬웨어 빌더를 포함한 각종 인프라를 판매한다는 글을 포럼에 게시한 후 6 명이 체포됐으며, 어리고 미숙한 계열사 고용 등의 이유로 사라졌다. 이후, 자신들을 'Ransomed.VC aka Raznatovic'라고 소개하는 그룹이 활동을 개시한 것으로 보아 Raznatovic 가 인프라를 구매한 것으로 추정된다.

Werewolves 그룹은 등장 이후 심상치 않은 움직임을 보이고 있다. 이 그룹이 운영하는 서피스 웹 사이트에는 23 개나 되는 조직의 데이터를 탈취했다고 주장하는 글과 일부 유출 데이터가 게시되었다. 또한 사이트에서는 버그 바운티[5]를 자체적으로 개최하고 있으며 웹 사이트 취약점, 소프트웨어 취약점, Tor 브라우저 취약점 등을 제보하는 자에게 최대 100 만 달러(한화 약 13 억 2000 만원)의 현상금을 지불한다고 명시하고 있다.

Chaos 랜섬웨어의 변종인 Astra 랜섬웨어도 발견됐다. Chaos는 2021년 6월에 처음 발견되어 여러 버전이 출시됐으며, 다크웹 해킹 포럼에 빌더가 공개되어 불특정 다수가 이를 악용한 변종을 대량 생산하기도 했다. 이후 Yashma, Onyx 등 다양한 이름의 랜섬웨어들이 Chaos를 기반으로 등장하여 많은 피해를 발생시키기도 했다. 이번에 발견된 Astra 랜섬웨어도 Chaos 를 기반으로 하고 있다. AES 로 파일을 암호화하고 해당 키를 RSA 로 보호한다는 특징으로 인해 복호화가 어려워 감염 예방에 힘써야 한다.

[5] 버그 바운티 : 기업의 소프트웨어나 시스템의 보안 취약점을 찾는 것에 대해 보상을 지급하는 제도

Top5 랜섬웨어

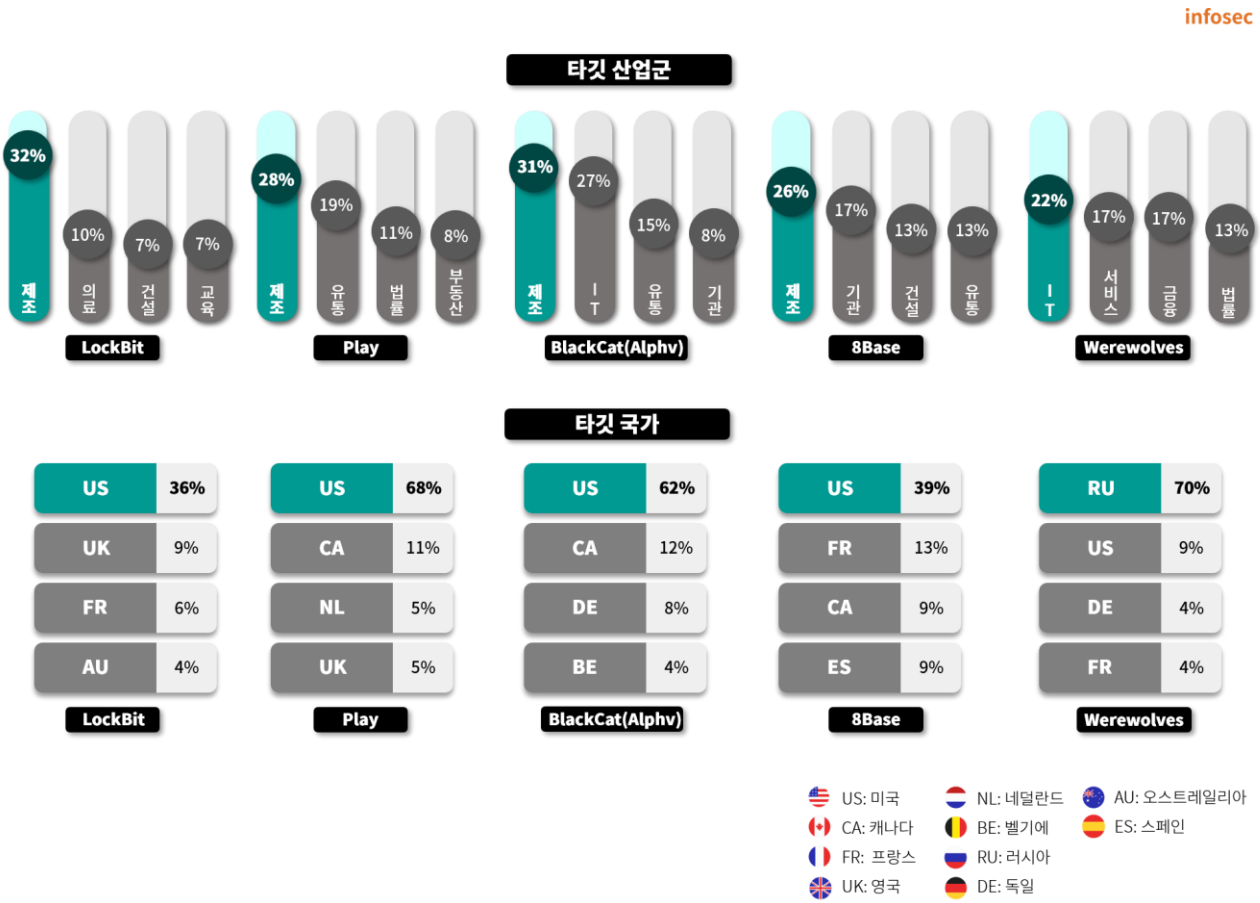


그림 3. 산업/국가별 주요 랜섬웨어 공격 현황

12 월 가장 많은 피해를 발생시킨 랜섬웨어 그룹은 LockBit 이다. LockBit 은 독일 에너지청인 Dena 에 대해 공격을 수행했다고 주장하며, 12 월 26 일까지 협상에 응하지 않을 시 데이터를 유출시키겠다는 협박성 글을 게시하기도 했다. Dena 는 사이버 공격이 있었다는 사실은 인정했지만 랜섬웨어로 인한 공격인지에 대해서는 밝히지 않았다. 또한, LockBit 은 BlackCat(Alphv)이 폐쇄된 것을 기회로 삼아 BlackCat(Alphv)의 개발자 및 계열사에 대해 협업을 제안하기도 했다. 실제로 기존 BlackCat(Alphv) 사이트에 있던 Dena 자료가 LockBit 유출 사이트에도 게시됨에 따라 이적한 계열사가 존재하는 것으로 보인다.

Play 랜섬웨어 그룹은 2022 년 6 월부터 10 월 사이에 전 세계 약 300 개 조직을 공격했으며, 그중 일부는 국가 주요 기반 시설도 포함되어 있어 상당히 큰 영향력을 행사하는 그룹으로 알려져 있다. 이로 인해 최근 FBI 는 미국의 사이버 보안 및 인프라 보안국(CISA) 및 호주 사이버 보안 센터(ACSC)와 함께 Play 에 대해 경고하는 합동 사이버 보안 권고문을 발표하기도 했다.

BlackCat(Alphv)은 국제 수사 기관의 공조로 인해 인프라 폐쇄와 복구를 반복하고 있다. 이들은 FBI 가 인프라를 폐쇄시켰음에도 다시금 인프라를 복구하고 FBI 에 보복하겠다는 선언을 했다. 또한 XSS 포럼에서 BlackCat(Alphv)과 LockBit 은 랜섬웨어 카르텔을 형성해야 한다는 대화를 주고받기도 해 추후 협력 관계가 형성될 수도 있고, 수사 기관의 관심을 돌리기 위해 이전과 같이 리브랜딩 수순을 거칠 가능성도 있다.

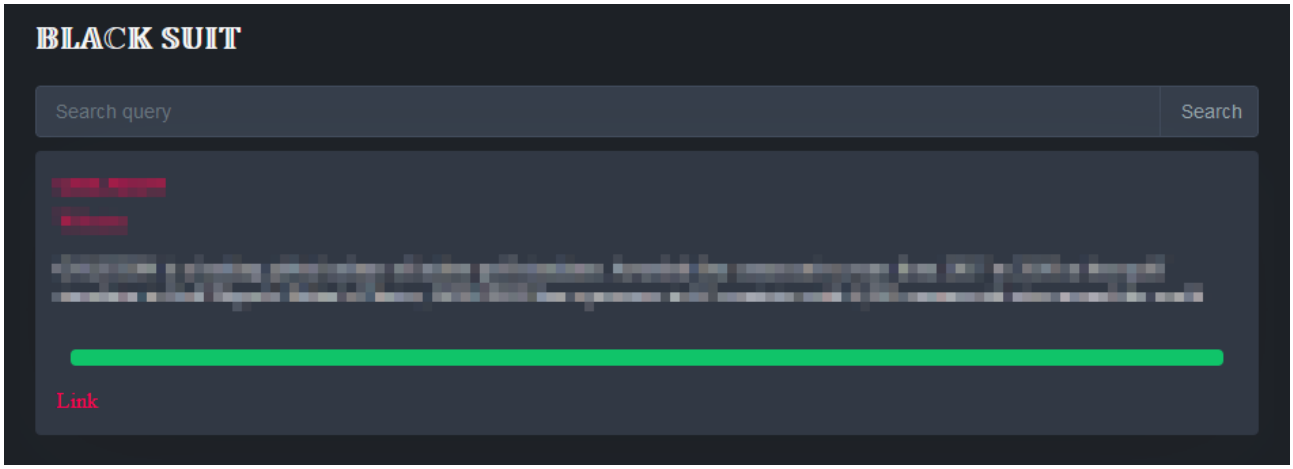
8base 랜섬웨어 그룹은 2023 년 5 월 다크웹 유출 사이트를 개설한 이후 꾸준히 활동을 이어가고 있다. 이들은 Phobos 랜섬웨어의 변종을 활용해 공격을 수행하고 있다. 특히, SmokeLoader[6]를 통해 랜섬웨어를 유포하거나 난독화된 랜섬웨어를 로더 자체에 포함하여 시스템을 감염시킨다. 이처럼 SmokeLoader 는 주로 피싱 메일을 통해 배포되므로 출처가 불분명한 이메일의 첨부파일은 가급적 다운로드를 지양하여 감염을 예방할 것을 권장한다.

Werewolves 는 12 월에 새롭게 발견된 랜섬웨어 그룹이다. 이들은 LockBit 3.0 랜섬웨어와 유출된 Conti 의 해킹 도구들을 사용해 취약한 공공 서비스를 대상으로 공격을 수행하고 있다. 이들로 인해 23 개의 조직이 수백 테라바이트의 데이터를 탈취당하는 피해를 입었다. 그중 16 개 기업은 러시아를 대상으로 수행된 공격이다. 또한 LockBit 3.0 을 사용하는 점과 LockBit 에서 게시한 피해 조직과 6 건이 겹치는 등 LockBit 과의 연관성이 제기되고 있다.

[6] SmokeLoader : 감염된 시스템에 다른 악성코드를 다운로드하는 데 사용되는 악성코드

■ 랜섬웨어 집중 포커스

BlackSuit 랜섬웨어 개요



출처: BlackSuit 랜섬웨어 그룹 다크웹 유출 사이트

BlackSuit는 2023년 5월 등장했으며, Royal 이 리브랜딩한 랜섬웨어 그룹이다. 이들은 Windows와 Linux 를 모두 타깃으로 공격해 몸값을 요구하는 동시에 데이터를 유출하겠다고 협박하는 이중 협박 방식을 취하고 있다.

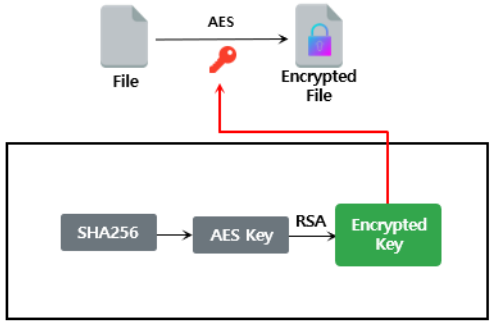
BlackSuit 의 전신인 Royal 은 2022 년 6 월에 활동을 종료한 Conti 랜섬웨어가 해체되고 난 뒤에 파생된 랜섬웨어 그룹이다. 등장 이래로 350 개가 넘는 조직에 대해 협박을 통해 2 억 7,500 만 달러(한화 약 3,627 억 원) 상당의 금액을 요구한 것으로 밝혀졌으며, 다크웹 유출 사이트에 데이터가 게시된 조직만 해도 200 개의 업체를 상회한다. 이렇듯 상당한 영향력을 보여주던 Royal 은 2023 년 5 월 미국 댈러스 시를 공격한 뒤로 수사기관의 압박이 거세지자 7 월경부터 잠잠한 모습을 보이더니 결국 10 월에 자취를 감춘 채 BlackSuit로 완전히 리브랜딩을 완료했다.

BlackSuit 는 피싱 메일의 첨부파일, 토렌트 웹 사이트, 악성 광고 등을 통해 전파되고 있으며, 최근 국내 A기업의 유출 데이터를 공개하는 사건이 발생했다. A기업은 랜섬웨어 공격이 발생한지 3주가 지나서야 고객에게 피해 사실을 고지하고 일부 고객의 개인정보가 유출된 사실을 밝혔다. 또한, 랜섬웨어 공격 이후 일부 사용자는 A 기업을 사칭한 피싱 문자를 받는 등의 피해를 입기도 했다. 이처럼 유출된 개인정보를 통해 피싱이나 스미싱 등의 2 차 피해가 발생할 수 있어 각별히 주의가 필요하다.

BlackSuit Ransomware

암호화 키

AES-256-CBC 알고리즘으로 파일 암호화를 하고, 해당 키를 RSA로 보호



암호화 방식

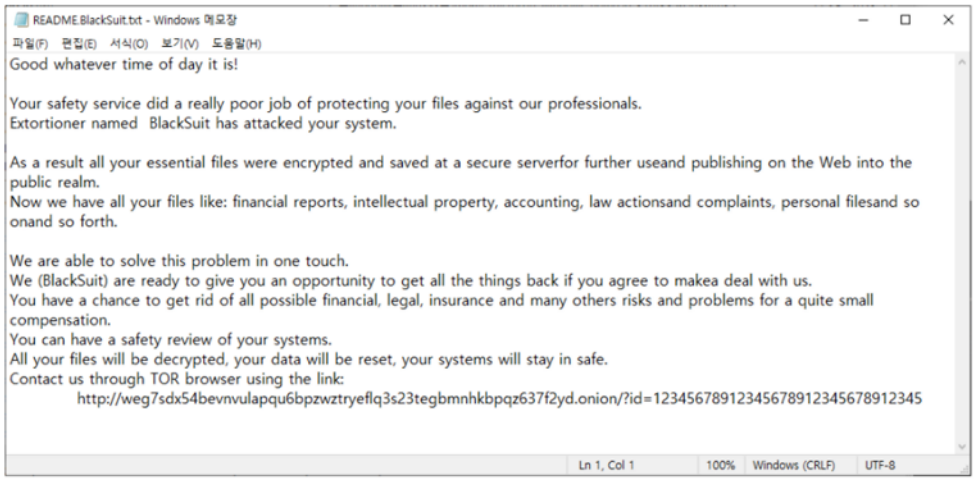
파일 크기 256KB 이상 : 파일 크기의 약 10% 간격으로 간헐적 암호화

파일 크기 256KB 미만 : 파일 전체 암호화

특징

- 인자전달
- 시스템 복구 옵션 제거
- 부분 암호화
- AES & RSA 암호화
- Royal 리브랜딩
- 멀티쓰레드

랜섬노트



README.BlackSuit.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

Good whatever time of day it is!

Your safety service did a really poor job of protecting your files against our professionals.
Extortioner named BlackSuit has attacked your system.

As a result all your essential files were encrypted and saved at a secure serverfor further useand publishing on the Web into the public realm.
Now we have all your files like: financial reports, intellectual property, accounting, law actionsand complaints, personal filesand so onand so forth.

We are able to solve this problem in one touch.
We (BlackSuit) are ready to give you an opportunity to get all the things back if you agree to makea deal with us.
You have a chance to get rid of all possible financial, legal, insurance and many others risks and problems for a quite small compensation.
You can have a safety review of your systems.
All your files will be decrypted, your data will be reset, your systems will stay in safe.
Contact us through TOR browser using the link:
http://weg7sdx54bevnvulapqu6bpzwztryeflq3s23tegbmnhkbpqz637f2yd.onion/?id=12345678912345678912345678912345

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

README.BlackSuit.txt

변경 확장자

.BlackSuit

제작 언어

C/C++

그림 4. BlackSuit 랜섬웨어 개요

BlackSuit 랜섬웨어 전략

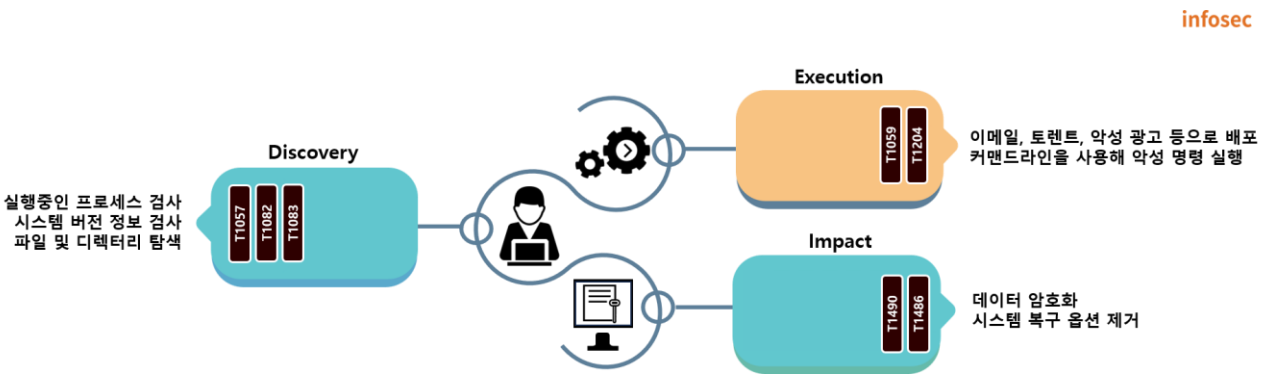


그림 5. BlackSuit 랜섬웨어 공격 전략

BlackSuit 랜섬웨어는 첨부파일에 랜섬웨어를 첨부하거나 랜섬웨어가 실행되게 하는 매크로를 포함한 문서 파일을 첨부해 파일 실행 시 사용자도 모르게 감염되게 하는 공격을 진행한다. 또한, 악성 광고 등 클릭과 동시에 자동으로 랜섬웨어가 설치되는 사이트로 리다이렉트 되거나 다운로더 형태의 악성코드를 통해 설치되기도 해 주의가 필요하다.

해당 랜섬웨어는 다양한 인자 전달을 통해 공격자가 편의를 도모한 것으로 보이며, 특정 인자가 전달되지 않으면 암호화가 진행되지 않고 즉시 프로세스가 종료되도록 설계돼 있다. 이는 탐지 우회 및 분석 방해의 효과를 노린 것으로 분석된다.

인자	설명
-p {target path}	지정된 경로의 내용만 암호화
-name {32byte string}	고유 ID, 전달되지 않을 경우 프로세스 종료
-percent {0~100}	암호화 강도 지정
-list {text files}	암호화 할 대상이 작성된 텍스트 파일
-delete	자가 삭제
-network	네트워크 공유 자원 암호화
-local	로컬 시스템 암호화
-disablesafeboot	안전 모드 부팅 비활성화
-noprotect	뮤텍스 생성 비활성화

표 1. BlackSuit 랜섬웨어 인자

BlackSuit 의 인자 중, 특히 주목해야 할 인자는 -name 과 -percent 다. 매크로나 스크립트를 통해 랜섬웨어가 실행될 때 -name 인자와 함께 전달되는 32byte 의 문자열은 피해자의 고유 ID 로 사용되며 랜섬노트에도 기재된다. 만약 해당 인자가 전달되지 않을 경우 프로세스가 종료되며, 해당 인자 값은 단순히 피해자를 식별하기 위한 값으로 사용되어 32byte 문자열 형태만 전달되면 랜섬웨어 실행이 가능하다.

-percent 인자와 함께 전달되는 인수를 통해서 암호화 강도를 지정할 수 있는데, 256KB 이상의 파일에 대해서 간헐적인 암호화 방식을 채택한 BlackSuit 는 -percent 인자가 전달되지 않을 경우에는 기본적으로 100 이 전달된 것으로 간주하여 파일 크기의 약 10% 단위로 간헐적 암호화를 진행한다.

$$N = \left(\frac{X}{10}\right) \times \left(\frac{\text{Original File Size}}{100}\right)$$

[BlackSuit 암호화 강도 계산식]

- N : 간헐적 암호화에 사용될 바이트 수
- X : -percent 인자와 함께 전달되는 인수의 값
- 계산된 N 은 최종적으로 16 의 배수로 값을 내림

BlackSuit 는 커맨드 라인 명령 실행을 통해 VSC(Volume Shadow Copy)[7]를 Quiet 옵션으로 피해자 모르게 삭제해 사용자가 임의로 복구할 수 없도록 막는다. 이를 통해 안전 모드로 부팅해 피해자가 복구 옵션을 사용하는 것을 막기 위해 safeboot 옵션을 제거한다. 이 랜섬웨어는 32Bit 프로그램이지만, 64Bit 의 경우에도 VSC 를 통한 복구를 막기 위해 64Bit 에 해당하는 명령어도 함께 실행시키는 용의주도함을 보이고 있다. 이러한 명령들이 실행되고 나면 그 즉시 컴퓨터가 재부팅 되어 사용자가 어떠한 조치도 취할 수 없이 랜섬웨어에 속수무책으로 당하게 된다.

[7] VSC : Windows 시스템에서 파일이나 폴더의 백업 사본을 생성하고 유지하는 기능

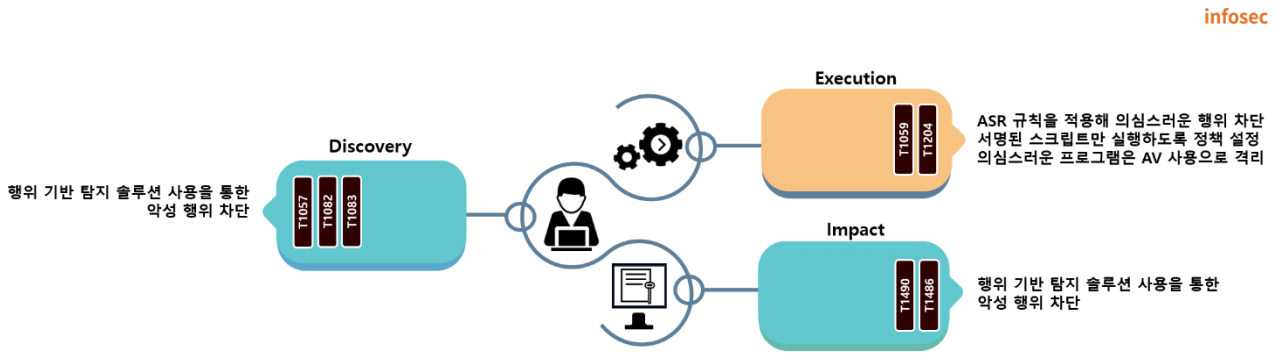


그림 6. BlackSuit 랜섬웨어 대응방안

BlackSuit 랜섬웨어의 행위들은 대부분 시스템의 기본 기능을 악용하므로 시그니처 기반의 보안 솔루션에서는 정확한 구분이 어려울 수 있다. 이러한 문제를 해결하기 위해 행위 기반으로 탐지하는 보안 솔루션을 사용하거나 ASR(Attack Surface Reduction)[8] 규칙을 활성화시킨다면 시스템 기본 기능이지만 비정상적으로 발생한 부분에 대해서 차단할 수 있다.

이러한 케이스의 랜섬웨어는 무엇보다 사전에 감염을 방지하기 위해 힘써야 한다. 다양한 경로로 감염될 수 있는 만큼 조직에서는 구성원들의 보안 인식 제고를 위한 교육을 진행하는 등의 방법이 필요하다.

특히, 출처를 알 수 없는 이메일의 첨부파일을 다운로드하거나 열어보는 행위, 애플리케이션의 공식 홈페이지가 아닌 곳에서 다운로드하거나 업데이트를 수행하는 행위, 취약한 웹 사이트의 광고 배너를 클릭하는 등의 행위 등은 조심해야 한다. 개인 혹은 조직에서 보안 인식 제고를 위해 구성원들에게 이러한 행동을 자제할 것을 권고한다면 랜섬웨어의 감염 가능성을 최소화할 수 있을 것이다.

[8] ASR : 악성코드의 공격 경로를 차단하는 기법

Indicator Of Compromise

BlackSuit : SHA256

90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c

1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e

449df90b819d01d290d218929bd33ee24941b3e6c00cdedc0e6f2714aea8460b

feced22ef920c40e032e12b9eb315591a7b6adcd371453c7d2fa08e2c8972aac

File Name

sys32.exe

■ 참고 사이트

URL : https://www.bleepingcomputer.com/news/security/fbi-alphv-ransomware-raked-in-300-million-from-over-1-000-victims/

URL : https://www.bleepingcomputer.com/news/security/how-the-fbi-seized-blackcat-alphv-ransomwares-servers/

URL : https://techcrunch.com/2023/11/15/cisa-fbi-royal-ransomware-blacksuit-sanctions/

URL : https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupts-emergency-care-at-german-hospitals/

URL : https://www.resecurity.com/blog/article/Exposing-Cyber-Extortion-Trinity-BianLian-White-Rabbit-Mario-Ransomware-Gangs-Spotted-Joint-Campaign

URL : https://thecyberexpress.com/werewolves-ransomware-group/

URL : https://www.scmp.com/tech/tech-trends/article/3246612/chatgpt-aided-ransomware-china-results-four-arrests-ai-raises-cybersecurity-concerns

URL : https://www.bleepingcomputer.com/news/security/fake-f5-big-ip-zero-day-warning-emails-push-data-wipers/