Keep up with Ransomware

BlackBasta 의 허점을 공략한 복호화 도구의 등장

■ 개요

2024 년 1 월 랜섬웨어 공격으로 인한 피해 사례 발생 건수는 전월(420 건) 대비 약 30% 감소한 299 건으로 나타났다. 국제 수사기관의 공조로 랜섬웨어 공격자들이 연이어 체포됐으며, 이 소식이 빠르게 전해지면서 랜섬웨어 그룹들의 활동이 위축되었다. 이와 함께 지난 12 월 발견된 신규 랜섬웨어 그룹들의 추가적인 공격 활동이 없었기 때문으로 분석된다.

하지만 다양한 수단과 방법을 사용한 랜섬웨어 공격이 발생했다. 특히, 상용 RMM(Remote Monitoring and Management)[1] 도구를 랜섬웨어 공격에 악용한 사례가 이목을 끌었다. Cactus 랜섬웨어 그룹은 AnyDesk, Splashtop, SuperOps[2] 등의 RMM 솔루션을 사용해 글로벌 에너지 기업 슈나이더 일렉트릭 기업 네트워크를 공격했다.

또한, 원격 제어 소프트웨어 TeamViewer[3]를 통해 전파되고 있는 LockBit 랜섬웨어의 변종도 발견됐다. 유출된 계정을 이용해 TeamViewer 에 로그인한 후, 네트워크 내 PC 에 접근해 랜섬웨어를 전파하는 방식으로 공격이 이뤄졌다. 공격에 사용된 랜섬웨어는 기존 LockBit 랜섬웨어와 소스코드는 동일하지만 랜섬노트에는 차이를 보여, 유출된 LockBit 의 빌더로 제작된 랜섬웨어로 추정되고 있다.

[1] RMM : 원격 모니터링 및 관리 도구

[2] AnyDesk, Splashtop, SuperOps : 원격 데스크톱 및 IT 관리를 위한 클라우드 기반 솔루션

[3] TeamViewer : 사용자가 인터넷을 통해 원격으로 다른 컴퓨터에 접속하고 제어할 수 있는 소프트웨어

Akira, BlackByte, AvosLocker, RobbinHood, Kasseika 등의 랜섬웨어 그룹들은 BYOVD(Bring-Your-Own-Vulnerable-Driver)[4]를 이용한 공격을 하고 있다. 특히, Kasseika 랜섬웨어 그룹은 랜섬웨어가 보안 솔루션에 감지되지 않도록 하기위해 BYOVD 를 사용한 것으로 확인됐다.

2022 년부터 국내에서는 이력서, 저작권 침해를 가장한 피싱 메일을 통해 LockBit 랜섬웨어가 유포되고 있다. 피싱 메일에는 문서 파일을 가장한 NSIS(Nullsoft Scriptable Install System)[5] 실행파일이 첨부되어 있어, 파일이 실행되면 암호화 및 데이터 유출 공격에 노출된다. 과거 피싱 메일은 어색한 한국어를 사용해 의심할 여지가 있었으나, 최근에는 생성형 AI 의 발달로 더욱 자연스럽고 속기 쉬운 형태로 진화하고 있다. 따라서 출처가 불분명한 이메일은 열람하지 않아야 하며, 매크로를 포함한 MS Office 문서 파일(.XLSM, .DOCM), 실행 가능한 파일(.EXE, .SCR, .BAT)의 첨부파일은 실행하지 않도록 주의를 기울여야 한다.

한편, 신규 랜섬웨어 그룹 NoName 은 LockBit 과의 연관성이 의심되고 있다. NoName 랜섬웨어 그룹의 다크웹 유출 사이트의 포맷은 LockBit 의 유출 사이트와 유사하며, 피해자로 게시된 사례가 동일하게 게재되어 있다. 또, 랜섬노트 내용도 상당히 유사해 NoName 그룹이 LockBit 과 연관된 조직일 가능성이 제기되고 있다. 다만, LockBit 의 유명세를 이용해 NoName 그룹의 영향력을 높이려는 의도일 수 있어 아직 지켜볼 필요가 있다.

이처럼 다양한 형태의 랜섬웨어 위협이 지속되고 있는 가운데, BlackBasta 변종 랜섬웨어와 Babuk 계열인 Tortilla 랜섬웨어에 대한 복호화 도구가 공개됐다. 23 년 4 월 BlackBasta 변종 랜섬웨어에 의해 감염 당한 경우, 파일크기가 5KB~1GB 사이즈인 경우 복구가 가능하다. Tortilla 랜섬웨어는 모든 피해자에게 똑같은 개인 키를 사용하여 암호화하기 때문에 Tortilla 에 의해 피해를 입은 사람이라면 누구나 복호화 도구를 사용하여 복구할 수 있다.

[4] BYOVD : 공격자가 이미 존재하는 취약한 드라이버를 사용하여 시스템 보안을 우회하는 공격 기법

[5] NSIS : 스크립트 기반으로 동작하는 Windows 용 설치 시스템

■ 랜섬웨어 뉴스

infosec

SRLabs, BlackBasta 랜섬웨어 일부 복호화 도구 공개

- 23년 4월경 사용한 변종 랜섬웨어를 대상으로 복호화 도구 공개
- 5KB~1GB 파일 대상으로 복구 가능, 1GB 이상 파일은 첫 5KB 제외한 파일 복구 가능, 그 이하는 불가
- 64Bytes의 암호화 바이트의 평문을 알고 있을 경우에만 가능

Babuk 변종 Tortilla 랜섬웨어 복호화 도구 공개

- Cisco Talos는 Babuk 랜섬웨어의 변종인 Tortilla 랜섬웨어에 대한 복호화 도구를 출시
- 네덜란드 법 집행 기관과의 위협 인텔리전스 공유로 공격자 체포
- Tortilla 캠페인은 Microsoft Exchange 서버의 ProxyShell 취약점을 악용하여 공격

LockBit, 세계적인 샌드위치 체인 Subway 공격 주장

- LockBit은 Subway의 데이터를 탈취했다고 주장하며 협상에 응하지 않을 시 경쟁 업체에 데이터를 팔겠다고 협박
- Subway는 이에 대해 조사 중임을 밝힘

Medusa 랜섬웨어 그룹, Water for People 비영리기관 공격

- Medusa 랜섬웨어 그룹이 다크웹 유출 사이트에 Water for People을 공격했다는 게시글 작성
- 현재는 협상이 결렬되어 유출 데이터를 게시한 상태

3AM 랜섬웨어, BlackSuit 랜섬웨어 그룹과의 연관성 제기

- 이전 Conti 그룹의 멤버로 구성된 Royal(現 BlackSuit) 그룹과 전술, 인프라 등 상당 부분이 유사
- 동일한 IP, 프록시, 포트 등의 인프라를 활용하여 공격
- 이외에도 공격을 위해 IcedID를 사용한 흔적 발견

* IcedID : 다른 악성코드를 전달하는데 사용되는 악성코드

BlackCat(Alphv) 소스코드 XSS 포럼에서 4,000만원 수준으로 판매

- 한 유저가 XSS 포럼에 BlackCat(Alphv) 랜섬웨어의 소스코드를 판매하는 글을 게시
- 해당 글을 올린 계정이 밴 처리되어 스캠으로 추정

* XSS 포럼 : 해킹을 통해 탈취한 데이터 및 랜섬웨어 등을 판매하는 다크웹 포럼

러시아의 TrickBot 개발 및 운영자 5년 징역형 선고

- 미 법무부는 러시아 국적의 40세 남성에 대해 TricKBot 생성 및 운영 혐의로 징역형 선고
- TrickBot은 랜섬웨어를 전달하는데 사용

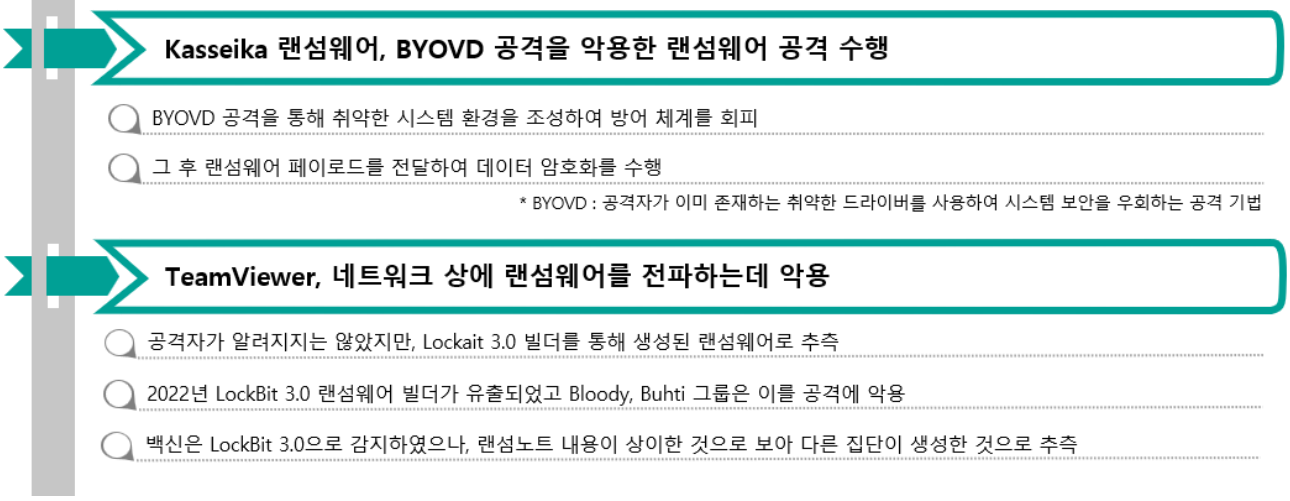

Kasseika 랜섬웨어, BYOVD 공격을 악용한 랜섬웨어 공격 수행
BYOVD 공격을 통해 취약한 시스템 환경을 조성하여 방어 체계를 회피
그 후 랜섬웨어 페이로드를 전달하여 데이터 암호화를 수행
* BYOVD : 공격자가 이미 존재하는 취약한 드라이버를 사용하여 시스템 보안을 우회하는 공격 기법
TeamViewer, 네트워크 상에 랜섬웨어를 전파하는데 악용
공격자가 알려지지는 않았지만, Lockait 3.0 빌더를 통해 생성된 랜섬웨어로 추측
2022년 LockBit 3.0 랜섬웨어 빌더가 유출되었고 Bloody, Buhti 그룹은 이를 공격에 악용
백신은 LockBit 3.0으로 감지하였으나, 랜섬노트 내용이 상이한 것으로 보아 다른 집단이 생성한 것으로 추측

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

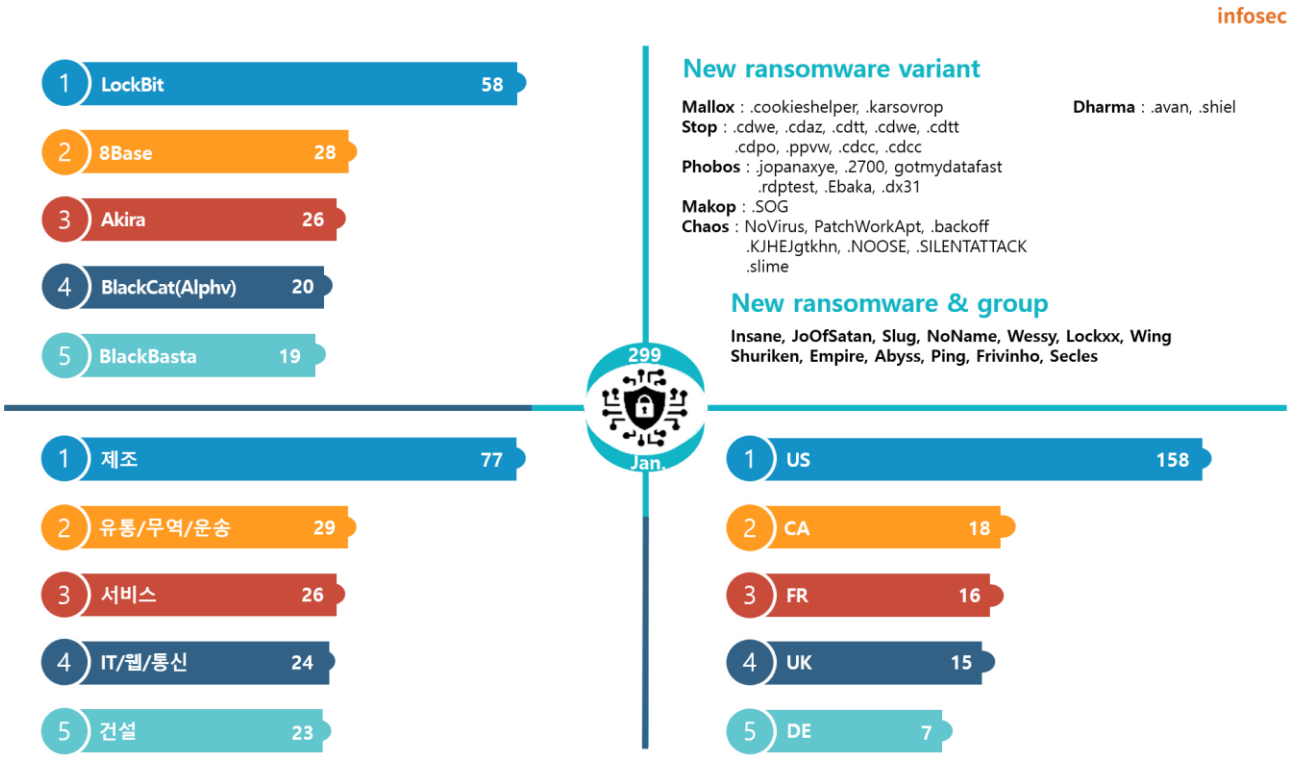


그림 2. 2024 년 1 월 랜섬웨어 위협 현황

새로운 위협

2024 년 1 월, 랜섬웨어로 인한 피해 사례는 지난해 12 월 대비 약 30% 감소했으나, 신규 랜섬웨어 그룹이 꾸준히 발견되는 등 변종 랜섬웨어의 위협이 지속되고 있다.

Insane 랜섬웨어 그룹은 다크웹 유출 사이트 메인에 자신들의 랜섬웨어 특징을 공개했다. 이들은 AES 암호화를 통해 네트워크 내의 모든 파일을 감염시키고 시스템의 정보를 탈취한다고 주장했으며, 덧붙여 Anti-Virus 에 절대 탐지되지 않는다고 밝혔다. 그러나 이러한 주장은 신규 랜섬웨어의 특성상 탐지된 기록이 없기 때문에, 시그니처 기반으로 탐지하는 보안 솔루션에 한해서 탐지 회피가 가능할 것으로 보인다.

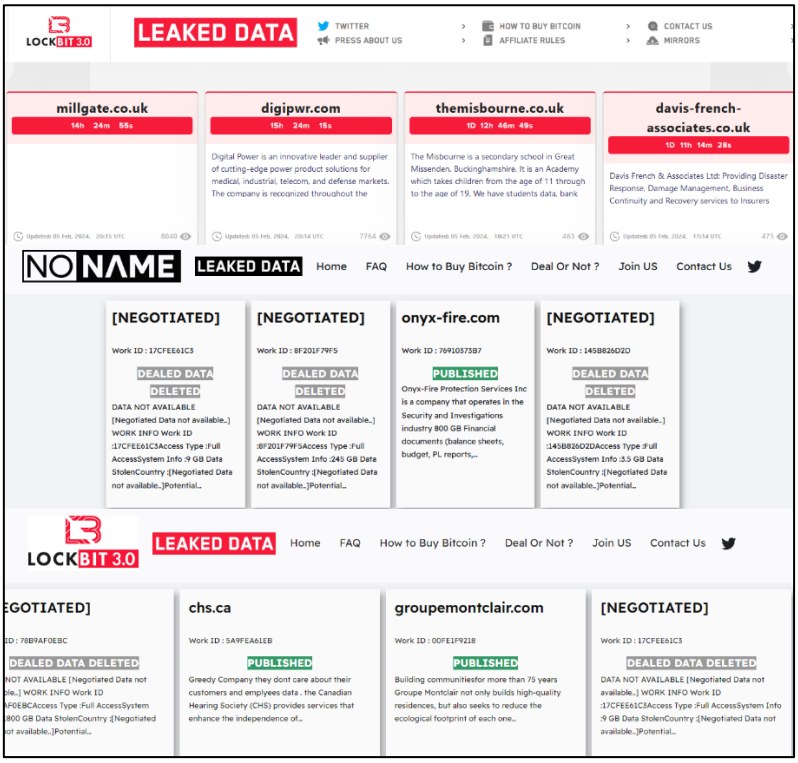


그림 3. LockBit, NoName, Fake LockBit 유출 사이트 비교

NoName 그룹은 LockBit 랜섬웨어 그룹과 연관성이 제기되고 있는 그룹이다. NoName 그룹의 다크웹 유출 사이트에 게재된 공격 사례가 2023 년 LockBit 에서 게시했던 공격 사례와 일치하고 있으며, 다크웹 유출 사이트의 형식 또한 LockBit 과 유사한 모습을 보이고 있다. 또 다른 LockBit 모방 그룹인 Fake LockBit 도 발견됐다. 이들은 보편적인 랜섬웨어 그룹들이 활동하는 다크웹이 아닌 대부분의 사람이 일반적으로 사용하는 서피스 웹에서 LockBit 의 이름을 사칭하여 활동하고 있는 가짜 LockBit 그룹이다.

NoName 랜섬웨어 그룹과 Fake LockBit 그룹 간의 연관성도 발견됐다. 두 랜섬웨어 그룹의 유출 사이트는 같은 도메인 등록 기관(NameCheap)을 이용하고 있으며, 같은 날짜(2023 년 11 월 4 일)에 등록되었다. 이를 통해 NoName과 가짜 LockBit의 배후는 LockBit의 계열사라는 가능성보다 단지 유출된 빌더를 이용한 모방 그룹. 즉, LockBit 의 유명세를 이용하려는 전략의 일환이라는 가능성에 무게가 실리고 있다. 추후 이들의 행보를 더 지켜봐야 결론을 내릴 수 있을 것으로 보인다.

이번 달 새롭게 발견된 랜섬웨어의 대다수는 과거 랜섬웨어 빌더 혹은 코드가 유출된 랜섬웨어의 변종으로 확인된다. Chaos 랜섬웨어의 변종인 Wessy 랜섬웨어는 .NET 으로 작성되었으며, .NET Reactor 난독화가 적용되어 있다. LokiLocker 랜섬웨어의 변종인 Shuriken 은 시작 프로그램, 작업 스케줄러에 등록되어 사용자 로그온 시 winlogon.exe 를 위장하여 실행되고 작업관리자를 실행하지 못하도록 비활성화 한다. 이 랜섬웨어는 별도의 텔레그램 메신저 계정을 통해 연락을 취하도록 설정되어 있다. Babuk 랜섬웨어의 변종 Abyss 랜섬웨어는 암호화 후 바탕화면과 랜섬노트를 통해 연락 방법을 안내하는데, 현재 안내하고 있는 다크웹 주소에는 접근할 수 없는 상태다.

Top5 랜섬웨어

그림 4. 산업/국가별 주요 랜섬웨어 공격 현황

LockBit 은 몇 달 전 발생한 계열사 이탈 등의 운영 이슈를 극복하고 다시 활발하게 활동하고 있다. 최근에는 세계적인 샌드위치 프랜차이즈 기업 써브웨이(Subway)를 공격했다고 밝혔다. 여전히 악성 매크로가 담겨있는 MS Office 문서 파일 형태의 랜섬웨어를 이력서, 입사지원서 등으로 위장해 유포하고 있다.

최근 LockBit 그룹은 의료 기관을 타깃으로 한 공격도 주저하지 않는 등 과감한 행보를 보이고 있다. 불과 1 년 전, 어린이 병원을 공격한 후 사과문을 게시하고 무료로 복호화 도구를 제공한 전력과 상반된 행보다.

랜섬웨어 그룹들이 의료 기관을 공격하기 꺼려하는 이유는 수사 기관의 타깃이 될 가능성이 높기 때문이다. 그럼에도 불구하고 LockBit 은 랜섬웨어 몸값 지불 확률을 높이고자 전략을 변경하고 의료기관 공격을 시도하고 있다. 물론 환자 생명에 지장이 생기는 의료 시스템에 대한 공격을 수행하는 것은 아니다. 환자들의 민감 데이터들을 탈취해 의료 기관으로 하여금 몸값을 지불할 수밖에 없게 만드는 치밀한 방식으로 공격을 전개하고 있다.

Akira 랜섬웨어는 최근 핀란드를 대상으로 다수의 공격을 진행하고 있다. 이들은 Cisco VPN[6] 취약점(CVE-2023-20269[7])를 악용하여 네트워크에 침투하고 NAS(Network-Attached Storage)[8] 및 백업 장치를 타깃으로 삼아 백업 데이터를 삭제하고 파괴하는 전략을 사용한다. 이로 인해 핀란드의 국가사이버안보센터(NCSC-FI)는 Akira 랜섬웨어 공격에 대해 경고하며 "3-2-1 백업 규칙"을 따라 피해를 최소화할 것을 강조했다. "3-2-1 백업 규칙"은 서로 다른 **두 위치**에 최소 **3 개**의 사본을 만들고 그 사본 중 **하나**는 네트워크에서 완전히 분리된 상태로 유지하는 규칙이다.

BlackBasta 랜섬웨어에 대한 복호화 도구가 공개됐다. 이는 2023 년 4 월 공격에 사용된 변종 랜섬웨어에 대한 복호화 도구 'Black Basta Buster'로 BlackBasta 의 암호화 결함을 통해 제작됐다. 5KB 미만의 파일은 복구가 불가능하나, 5,000Btyes~1GB 사이의 파일은 전체 복호화가 가능하다. 만약 파일 크기가 1GB 를 초과할 경우, 처음 5KB 는 손실되고 나머지 부분은 복구가 가능하다.

BlackCat(Alphv) 그룹은 지난해 12 월 FBI 와의 대립 이후 압수된 사이트들 외 다른 인프라를 이용해 활동을 이어가고 있다. 최근에는 다크웹 유출 사이트에서 기존 데이터의 흔적을 삭제하고 새로운 피해 조직들만 게시하고 있다. 1 월에는 의료/복지 업계의 의료 간병 서비스 기업을 공격해 한때 해당 기업의 사이트를 마비시키기도 했다. 기존의 BlackCat(Alphv) 은 CIS 국가, 원자력 발전소 및 병원을 포함한 주요 기반 시설 등에 대한 공격을 수행하지 않는다는 규칙이 있었으나, FBI 에 의해 인프라가 압수된 이후에는 이러한 규칙을 철회하며 의료 업계에 대한 공격을 계속하고 있다.

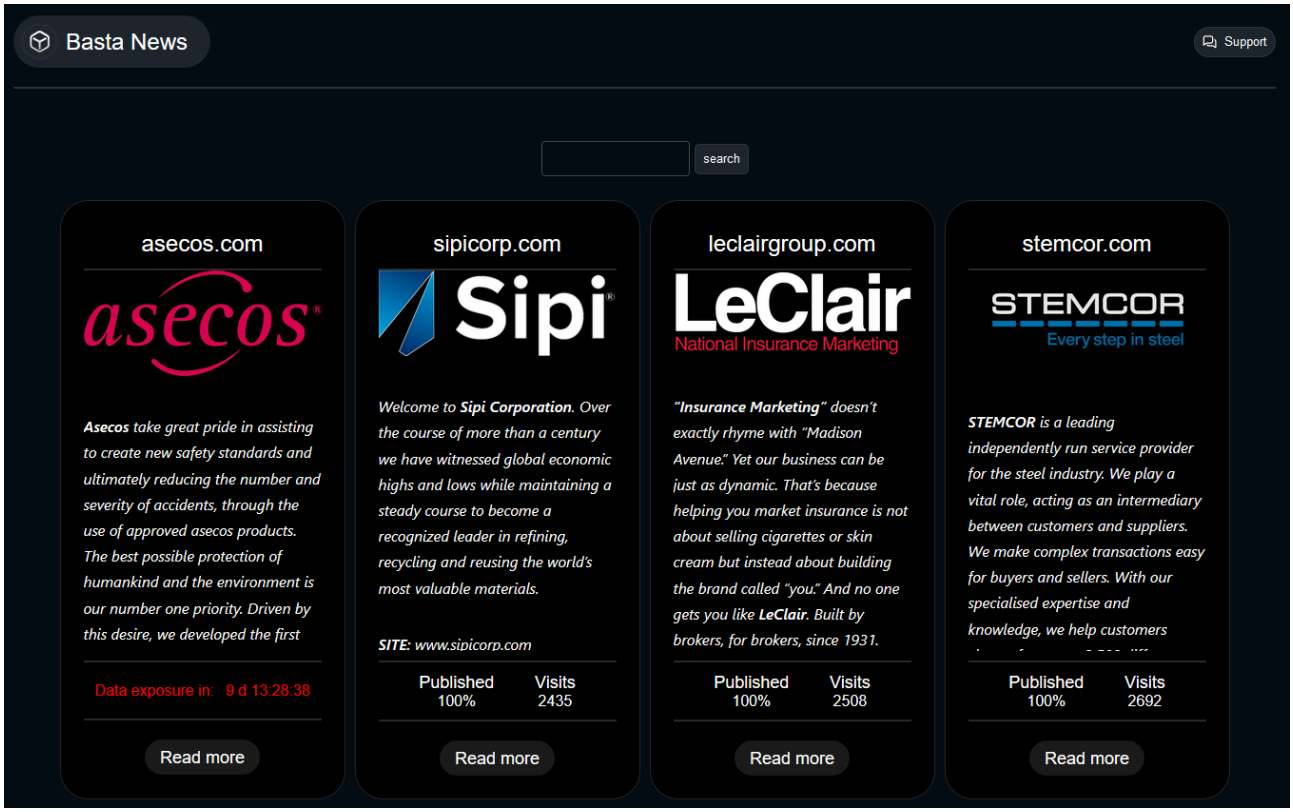
[6] VPN : 인터넷 상에서 개인 정보를 보호하고 지역 제한을 우회하기 위해 사용하는 가상의 보안 네트워크

[7] CVE-2023-20269 : 부적절한 인증, 권한 부여, 계정 관리 등으로 인해 공격자가 VPN 접근 권한을 획득할 수 있는 취약점

[8] NAS : 네트워크에 연결되어 여러 사용자가 데이터를 공유하고 접근할 수 있는 저장 장치

■ 랜섬웨어 집중 포커스

BlackBasta 랜섬웨어 개요



출처: BlackBasta 랜섬웨어 그룹 데이터 유출 사이트

BlackBasta 랜섬웨어는 2022 년 4 월 등장해 2 주 동안 스무 곳 이상을 공격해 유출 데이터를 다크웹 블로그에 게시하며 파급력을 과시한 랜섬웨어 그룹이다. 현재까지 이들은 340 개가 넘는 조직에게 몸값을 요구했으며, 협상을 통해서 총 1 억 700 만 달러(한화 약 1,430 억)에 달하는 암호화폐를 확보한 것으로 알려졌다(2023 년 11 월 기준). 이들은 미국과 유럽 국가들의 조직을 주요 타깃으로 하며, Windows 버전 뿐 아니라 VMware ESXi[9]를 감염시키는 Linux 버전의 랜섬웨어도 배포하고 있다.

[9] VMware ESXi: 호스트 컴퓨터에서 다수의 운영체제를 동시에 실행시킬 수 있는 Unix 기반 논리적 플랫폼

이들은 시스템에 최초 침투를 하기 위해 메일의 첨부파일이나 링크를 이용하고 있다. 악성 메일에 첨부된 압축 파일이나 문서 파일 실행을 조장해 QakBot[10] 설치를 유도한다. 이후, 설치된 QakBot 을 이용해 내부 데이터를 수집하고 BlackBasta 랜섬웨어 공격을 진행한다. BlackBasta 는 감염된 타깃에게 몸값 요구하고, 데이터 유출을 빌미로 추가 협상을 진행하는 이중 협박 방식을 취하고 있다.

BlackBasta 가 최초 침투를 위해 사용한 QakBot 은 Lockbit, Knight, REvil 과 같은 여러 랜섬웨어 그룹들이 최초 침투 및 랜섬웨어 배포를 위해서 사용하는 악성코드다. 2008 년에 등장한 QakBot 은 금융 사기에 주로 활용되었으며, 2019 년부터 랜섬웨어 배포에도 활용되기 시작했다. 2023 년 8 월 FBI 의 대규모 작전에 의해 QakBot 의 악성코드 인프라가 무력화됐지만, 같은 해 12 월에 새로운 버전의 QakBot 이 등장하며 여전히 최초 침투에 사용되고 있다. BlackBasta 는 QakBot 과 유사한 Pikabot[11]도 공격에 사용하고 있다.

독일의 보안 연구소인 SRLabs 는 2023 년 12 월 27 일 그들의 GitHub[12]에 BlackBasta 복호화 도구인 Black Basta Buster 를 공개했다. SRLabs 는 2022 년 11 월부터 2023 년 12 월 초에 이르는 버전의 BlackBasta 랜섬웨어에서 암호화 키가 재사용되는 취약점을 발견하였고, 이를 이용하여 파일 전체 혹은 일부를 복구할 수 있는 도구를 개발했다. 하지만, BlackBasta 랜섬웨어는 Black Basta Buster 를 이용해도 암호화된 파일을 복구할 수 없도록 복호화 도구 공개보다 앞서 키 재사용 취약점을 재빠르게 수정했다.

[10] QakBot (Qbot) : 백도어, 데이터 탈취, 내부 전파, 원격 코드 실행, 파일 다운로드와 같은 기능을 제공하는 악성코드의 한 종류

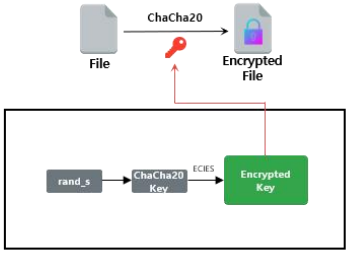
[11] Pikabot : 백도어, 데이터 탈취, 내부 전파, 원격 코드 실행, 파일 다운로드와 같은 기능을 제공하는 악성코드의 한 종류

[12] Github : 웹 기반 소스코드 버전 관리 및 협업 플랫폼

BlackBasta Ransomeware

암호화 키

ChaCha20알고리즘으로 파일 암호화를 하고, 해당 키를 ECIES*로 보호



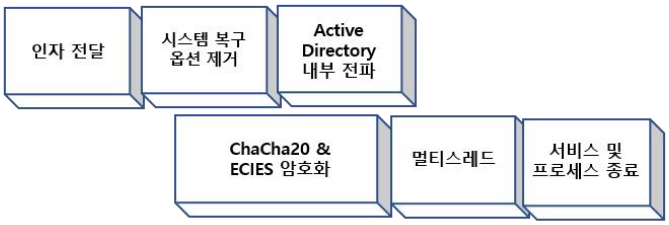
암호화 방식

5KB 미만: 파일 전체 암호화

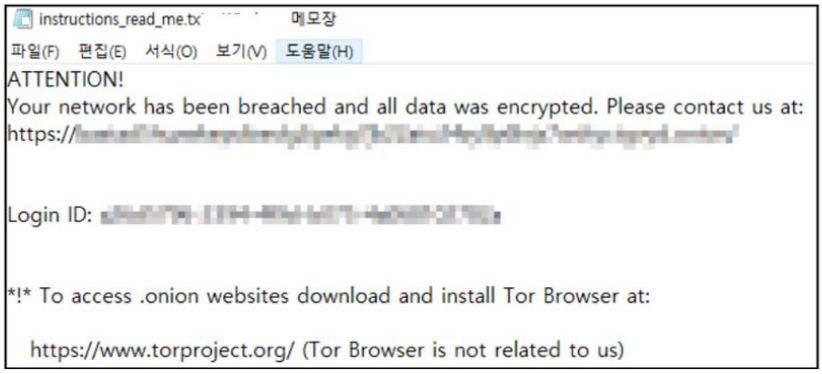
5KB 이상: 앞부분 전체 암호화 후 잔여 영역 부분 암호화

파일의 크기	전체 암호화 크기	부분 암호화 간격
0 - 5KB	모든 데이터	0B
5KB - 5MB	5KB	640B
5MB - 50MB	5KB	1.28KB
50MB - 1GB	5KB	6.4KB
1GB - 10GB	15KB	12.8KB
10GB 이상	50KB	64KB

특징



랜섬노트



instructions_read_me.txt

변경 확장자

.7wdojib58

제작 언어

C/C++

** Elliptic Curve Integrated Encryption Scheme (ECIES): 비대칭키를 이용해서 대칭키를 생성하며, 생성된 대칭키로 데이터를 암호화 한 후, 메시지 인증 코드(MAC)를 추가하는 방식의 암호화 프레임워크*

그림 5. BlackBasta 랜섬웨어 개요

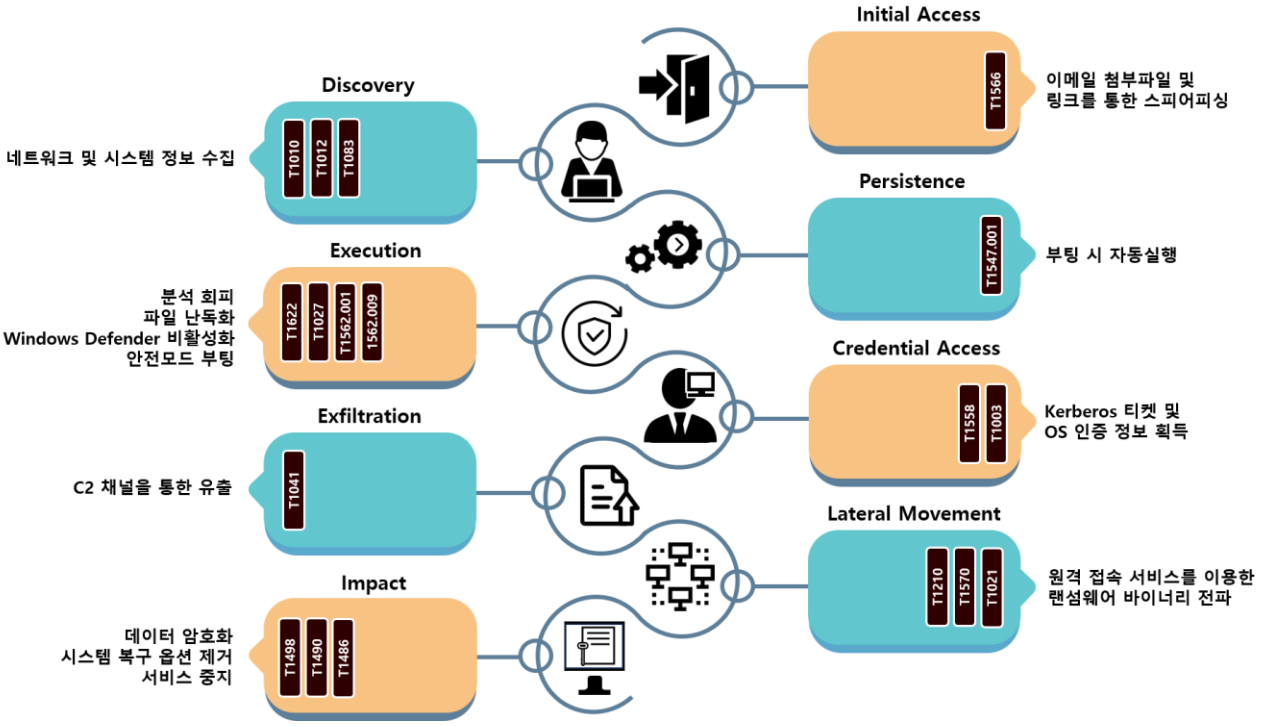


그림 6. BlackBasta 랜섬웨어 공격 전략

BlackBasta 는 주로 스피어피싱[13]을 통해서 최초 침투를 수행한다. 메일에 압축파일이나 매크로가 삽입된 문서 파일을 첨부한 후, 사용자가 첨부파일을 실행하면 감염되는 방식이다. 첨부파일을 열어보거나 링크를 클릭하면 함께 첨부되어 있는 스크립트를 통해서 QakBot 이 설치되며, Qakbot 은 탐지 우회, 자격 증명 탈취, 랜섬웨어 배포 및 내부 전파를 위해 Mimikatz[14], Cobalt Strike[15], PsExec[16]와 같은 여러 도구를 추가적으로 설치한다.

[13] 스피어피싱 : 특정인을 대상으로 하는 공격으로, 대상을 속여 개인정보 유출이나 악성코드 다운로드를 유도하는 공격 기법

[14] Mimikatz : Windows 시스템의 메모리에서 비밀번호나 자격증명과 같은 민감 정보를 추출하는 도구

[15] Cobalt Strike : 시스템 권한 확보 및 계정 정보 탈취, 측면 이동, C2 통신과 같은 기능을 가진 침투 테스팅 도구

[16] Psexec : 로컬/원격 시스템에 임의의 프로세스를 실행할 수 있는 도구

추가적으로 설치된 도구들을 이용해 Anti-Virus 서비스를 종료하거나 안전모드로 부팅하는 등 탐지 우회를 위한 작업을 우선 수행한다. 이후, 사용자 폴더나 기업의 기술 문서와 같이 협박에 사용할 민감 데이터를 확보하며, 랜섬웨어 파일을 배포하고 실행시킨다. 이렇게 수집한 데이터와 암호화된 파일을 활용해 이중 협박을 시도한다.

BlackBasta 랜섬웨어는 명령어 실행 인자를 우선적으로 확인한다. 해당 인자를 통해서 여러 가지 기능을 수행할 수 있다. 또한, 별도의 인자 전달 없이도 정상적으로 실행되는 것으로 보았을 때 공격의 편의성 및 효율성을 위해 추가한 기능으로 보인다.

인자	설명
-thread {int}	암호화 수행 시 생성되는 스레드 개수 설정 (기본 4 개)
-nomutex	뮤텍스[17] 생성 비활성화
-file {file_name}	지정한 파일만 암호화
-bomb	AD[18]를 통한 BlackBasta 내부 전파
-disablewhitelist	암호화 예외 항목 비활성화
-forcepath {path}	지정한 경로만 암호화
-nordp	RDP[19] 레지스트리 설정 기능 비활성화

표 1. BlackBasta 랜섬웨어 인자

실행 인자 중 -bomb 인자의 경우, LDAP 쿼리[20]를 활용해 같은 AD 서버에 존재하는 모든 PC 에 랜섬웨어 파일을 전파 및 실행시키는 기능을 수행한다. AD 서버에서 관리하는 모든 사용자 단말기 내 C:₩Windows₩bb.exe 경로에 랜섬웨어 파일을 복제해 실행한다.

[17] 뮤텍스 (Mutex) : 여러 스레드를 실행하는 환경에서 같은 자원에 여러 스레드가 동시에 접근하지 못하도록 막아주는 기술

[18] Active Directory(AD): MS 에서 제공하는 디렉토리 서비스 기능으로, 조직 내의 자원 및 권한 등을 관리할 수 있는 Windows 기반 중앙집중관리 서비스

[19] Remote Desktop Protocol (RDP) : 다른 컴퓨터를 원격으로 제어할 수 있도록 해주는 프로토콜

[20] LDAP 쿼리 : 네트워크상에서 조직이나 개인, 파일, 디바이스 등을 찾아볼 수 있게 해주는 소프트웨어 프로토콜 (LDAP)에서 사용하는 명령어

BlackBasta 랜섬웨어는 64B 단위로 암호화를 진행하며, 빠른 암호화를 위해 멀티스레드를 활용하고 파일 크기에 따라 암호화 방식을 다르게 적용하고 있다. 2022 년 11 월부터 2023 년 12 월 초 사이에 만들어진 구 버전의 BlackBasta 는 파일 크기에 따라 총 3 가지 방식으로 파일을 암호화한다. 5KB 미만의 파일은 모든 데이터를 암호화하며, 5KB 이상에서 1GB 미만의 파일은 192B 마다 64B 만 암호화를 수행한다. 1GB 이상의 파일은 최초 5KB 를 모두 암호화하며, 나머지 영역은 6.4KB 마다 최초 64B 만 암호화를 수행한다.

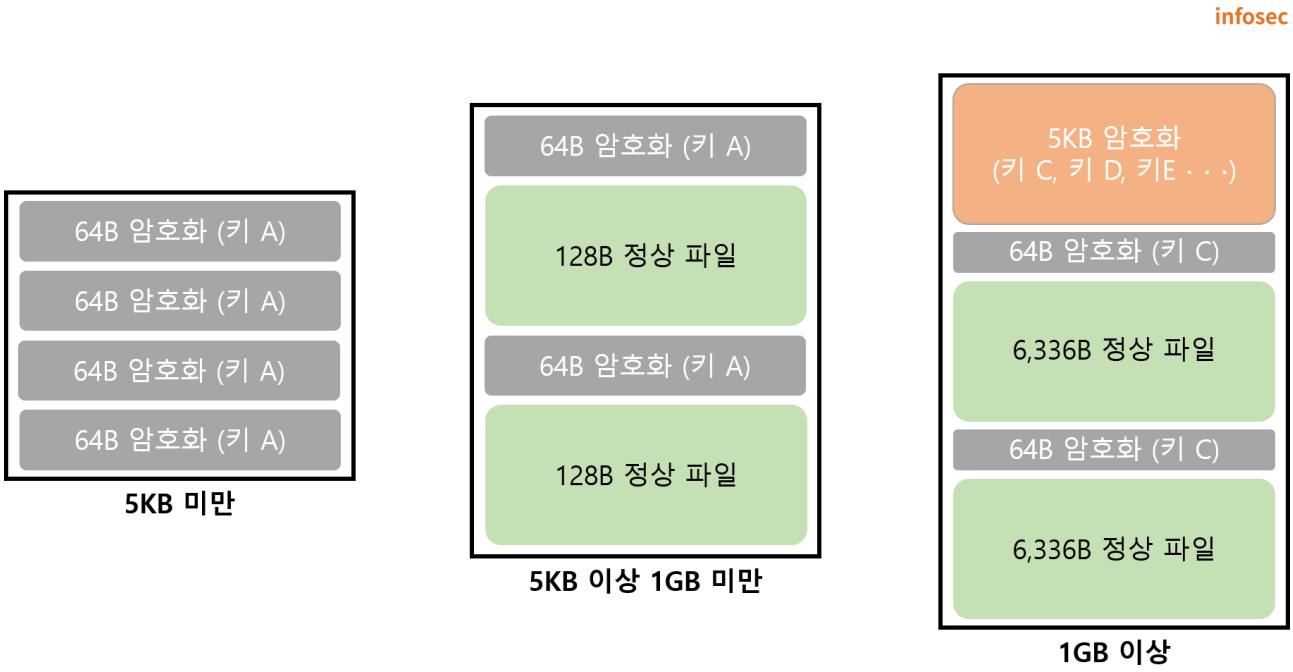


그림 7. 구 버전 BlackBasta 의 키 중복 사용

구 버전의 BlackBasta 랜섬웨어는 크기가 1GB 이상인 파일을 암호화할 때, 파일의 최초 5KB 는 매번 키를 갱신하여 암호화하며, 나머지 과정에서는 키를 갱신하지 않고 동일한 키를 사용한다. 해당 암호화 방식은 파일이 0x00 값으로 이루어진 영역에서 암호화 키가 그대로 노출되는 문제가 발생한다. 노출된 암호화 키를 이용하면 파일 전체 혹은 일부를 복구할 수 있다. SRLabs 에서 배포한 복호화 도구 역시 이 점을 이용했다. 다만, 키가 중복 사용된 부분만 복구 가능하기 때문에 1GB 이상의 파일은 처음 5KB 를 복구할 수 없다.

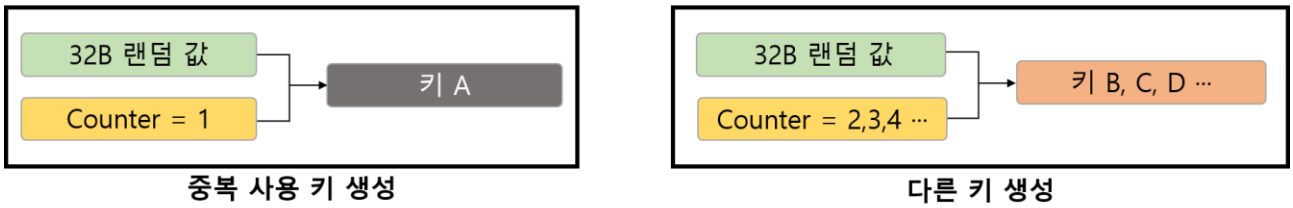


그림 8. 키 생성 방식

암호화 키는 파일마다 32B 의 랜덤한 값과 1 로 설정된 Counter 값을 이용해서 생성되며, Counter 값을 1 씩 증가시켜 다른 키를 생성할 수 있다. 구 버전에서 1GB 미만의 파일은 Counter 값이 1 로 설정된 키를 중복해 사용하며, 1GB 이상인 파일의 처음 5KB 를 암호화할 때만 다른 키를 생성해 사용한다.

2023 년 12 월 중순부터 만들어진 최신 버전의 BlackBasta 랜섬웨어에서는 일부 개선작업이 이뤄졌다. 5KB 미만의 파일은 모든 데이터를 암호화하며, 5KB 이상의 파일은 앞부분만 전체 암호화하고 나머지 영역은 부분 암호화한다. 5KB 이상의 파일은 파일 크기에 따라 전체 암호화 크기와 부분 암호화 간격을 다르게 진행한다. 요약하자면, 기존에 비해 데이터 크기 기준을 좀 더 세분화하여 총 6 가지의 파일 암호화 방식을 사용한다.

파일 크기	전체 암호화 크기	부분 암호화 간격
0 – 5KB	모든 데이터	0B
5KB – 5MB	5KB	640B
5MB – 50MB	5KB	1.28KB
50MB – 1GB	5KB	6.4KB
1GB – 10GB	15KB	12.8KB
10GB 이상	50KB	64KB

표 2. 파일 크기에 따른 암호화 방식

또한, 동일한 키를 사용하는 구 버전의 문제점도 보완됐다. 이제는 파일 내에서 키가 중복되어 사용되지 않도록 사용된 키는 반드시 초기화를 진행한다. 따라서, 키가 노출되더라도 해당 키를 사용한 부분만 복구가 가능하며, 전체는 복구가 어렵다.

infosec

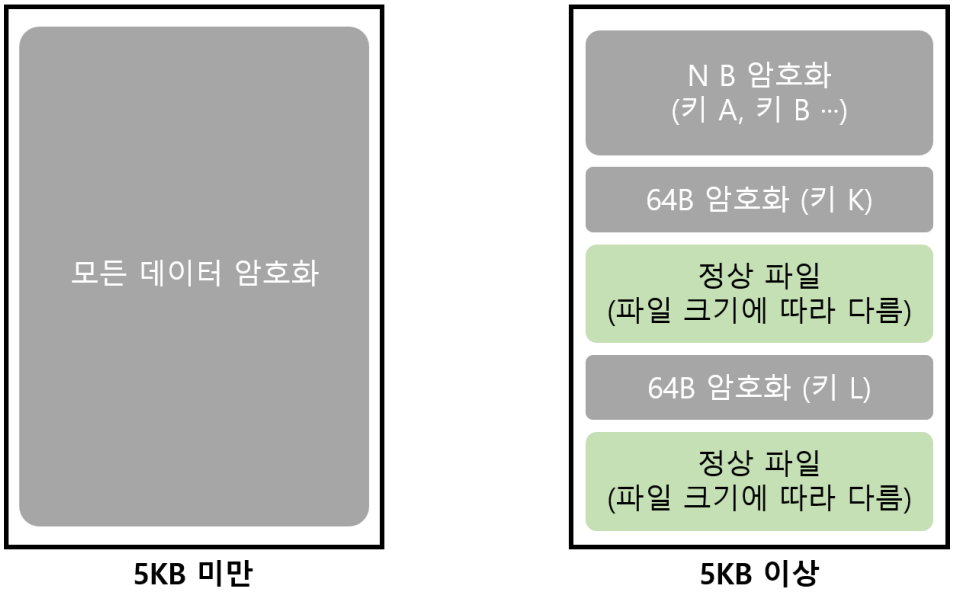


그림 9. 최신 버전 암호화 방식

BlackBasta 랜섬웨어 대응방안

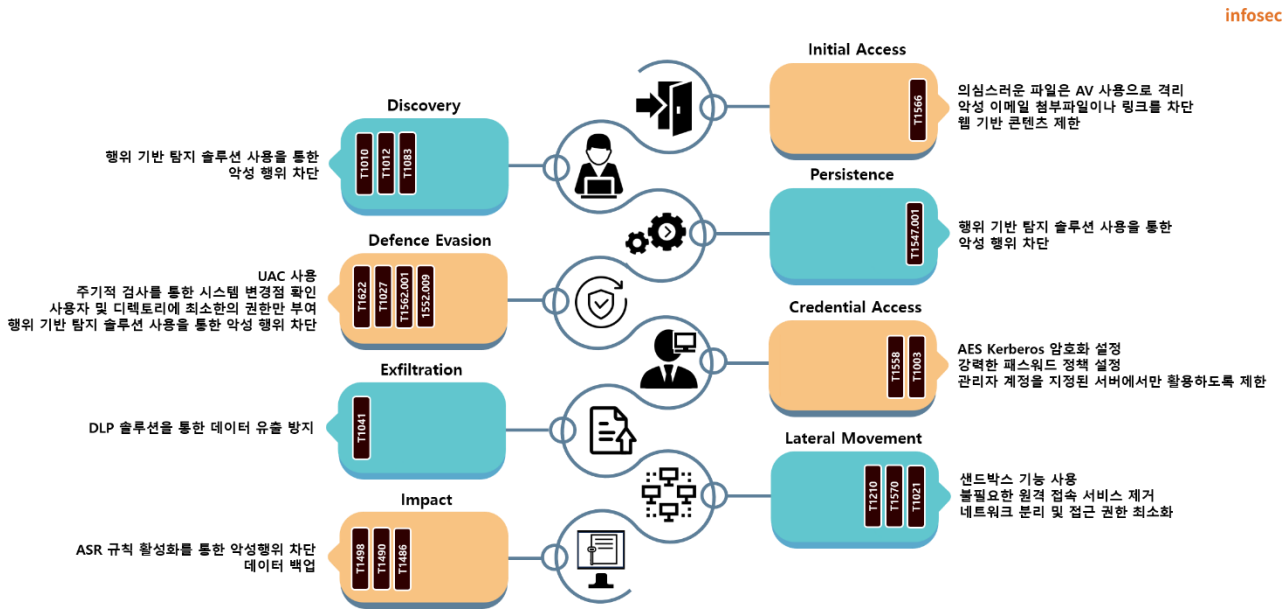


그림 10. BlackBasta 랜섬웨어 대응방안

BlackBasta 는 스피어피싱을 통해서 최초 침투를 시도한다. 따라서, 웹에서 다운로드 받은 컨텐츠를 차단하거나 별도의 Anti-Virus 를 사용해 다운로드 받은 악성 파일이 실행되지 않도록 대비할 수 있다. 특히, 출처를 알 수 없는 메일의 링크나 파일을 열람하지 않도록 경각심을 가져야 하며, 보안 인식 제고를 위해 악성 메일 모의 훈련을 통해 감염을 예방해야 한다.

최초 침투 이후에는 탐지를 회피하고 지속적으로 실행하기 위해서 레지스트리를 조작하거나 Anti-Virus 서비스를 종료시키고 안전모드로 부팅하는 방식을 사용한다. 이는, 행위 기반 탐지 솔루션 사용을 통해 차단할 수 있다.

또한, AD 계정 탈취를 시도하고 탈취한 계정을 이용해 AD 서버 내의 모든 사용자에게 랜섬웨어를 전파한다. 따라서 AD 서버 관리자 계정이 쉽게 탈취되지 않도록 강력한 암호화 방식을 사용해야 한다. 또한, 계정이 탈취되더라도 서버를 장악할 수 없도록 사용자 및 서비스 계정의 권한을 최소한으로 부여하고 분리해 관리하는 등의 방법을 통해 예방해야 한다. 이와 함께 지속적인 모니터링을 통해 AD 에 등록된 서비스와 그룹 정책 목록에 의심스러운 사항이 없는지 확인해야 한다.

데이터 탈취, 백업 데이터 삭제 및 파일 암호화에 대한 대비도 필요하다. DLP[21] 솔루션을 활용해 데이터가 유출되어 악용하는 것을 방지해야 한다. 또한, 정기적인 백업을 통해 파일을 관리해야 한다. 한편, Akira 랜섬웨어와 같이 NAS 와 백업 저장소의 데이터를 삭제하는 경우도 존재하므로 별도의 네트워크나 저장소에 데이터를 소산 백업[22]해 관리하는 것을 권장한다.

[21] Data Loss Prevention (DLP) : 데이터의 흐름을 감시하여 중요 정보 유출을 감시/차단하는 데이터 유출 방지 솔루션

[22] 소산 백업 : 백업된 데이터를 일정거리 떨어진 장소에 분리 보관하는 방식

Indicator Of Compromise

BlackBasta(April. 2023) : SHA256

fe87fa7714266548fa5da52455f1788f588417ee800c86768d163abd279d0279
ef2a754a8e713fd6deaa642e2220af372fd310a755a02126938ff233b16a4a83

BlackBasta(December. 2023) : SHA256

f971a05b8540fa6af8cb6c54d2c2de00c54fa99a4e86615daca03a6d7c0e4e6f
b32daf27aa392d26bdf5faafbaae6b21cd6c918d461ff59f548a73d447a96dd9

File Name

4WCB3ACCQFJBTGE966849RFVY6.bdq.00000000_BITDEFENDER.out
STUDIO_BBG.dll
RibbonGadgets.EXE

■ 참고 사이트

URL : https://www.bleepingcomputer.com/news/security/new-black-basta-decryptor-exploits-ransomware-flaw-to-recover-files/

URL : https://directoryadmin.blogspot.com/2014/12/ldap-queries-for-users-computers-groups.html

URL : https://securityscorecard.com/research/a-deep-dive-into-black-basta-ransomware/

URL : https://www.zscaler.com/blogs/security-research/back-black-basta

URL : https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta

URL : https://www.sentinelone.com/labs/black-basta-ransomware-attacks-deploy-custom-edr-evasion-tools-tied-to-fin7-threat-actor/

URL : https://www.zscaler.com/blogs/security-research/tracking-15-years-qakbot-development