Keep up with Ransomware

다시 돌아온 LockBit, 끝나지 않은 랜섬웨어 공격

■ 개요

2024 년 2 월 랜섬웨어 공격에 따른 피해 사례는 전월(299 건) 대비 약 40% 증가한 418 건으로 나타났다. 공격자들이 연이어 체포되고 있음에도 불구하고 랜섬웨어 피해 사례는 꾸준히 증가하는 추세다. 이러한 상황 속에서 가장 주목할 이슈는 서비스형 랜섬웨어(RaaS[1])그룹 LockBit 의 인프라가 FBI[2], NCA[3], Europol[4] 을 비롯한 11 개국 기관들에 의해 무력화됐다고 알려졌으나, LockBit 은 5 일 만에 새로운 다크웹 유출 사이트를 공개하며 활동을 재개한 것이다.

2019 년 처음 등장한 LockBit 은 지속적인 업데이트를 통해 영향력을 확대하고 있으며 2022 년부터 가장 많은 피해를 끼친 랜섬웨어 그룹으로 성장했다. LockBit 은 오랜 활동 기간과 영향력에 비해 핵심 개발자의 부재, 비정상적인 데이터 유출, 계열사 간 정산 오류 등으로 안정적으로 운영되지 못했음에도 글로벌 영향력을 행사하는 랜섬웨어 그룹으로 평가받고 있으며, 여러 국가 기관의 주목을 받고 있는 상황이다. 그러나, 2024 년 2 월 20 일, 국제 수사기관들이 공조한 Cronos 작전[5]을 통해 LockBit 인프라 일부를 압수했고, LockBit 의 다크웹 유출 사이트는 폐쇄 전까지 법 집행 기관의 통제를 받았다.

[1] RaaS (Ransomware-as-a-Service) : 랜섬웨어 그룹들이 계열사나 공격자에게 대가를 받고 랜섬웨어를 제공해주는 형태

[2] FBI (Federal Bureau of Investigation) : 미국 법무부 산하의 법 집행 기관

[3] NCA (National Crime Agency) : 영국 내무부 산하의 법 집행 기관인 국립범죄청

[4] Europol : 유럽 연합(EU)의 법 집행 기관

[5] Cronos 작전 : LockBit 의 범죄 생태계를 파괴하기 위한 사이버 교란 작전

출처: 압수된 LockBit 3.0 랜섬웨어 그룹 데이터 유출 사이트

수사기관에 의해 LockBit 관계자들은 폴란드와 우크라이나에서 체포되었고, 공격에 사용되었던 각종 계정도 정지됐다. 해당 과정에서 LockBit 인프라의 소스 코드와 계열사의 정보, LockBit 4.0 으로 추정되는 LockBit-NG-Dev(LockBit-NextGeneration-Development) 랜섬웨어, 기존 LockBit 3.0 과의 유사성 및 특징 등 정보가 공개됐다.

또한, 수사기관들은 LockBit 의 복호화 키를 활용해 복호화 도구를 만들어 배포했다. 이외에도 LockBit 이 자체적으로 개발한 정보 탈취 자동화 도구 StealBit 의 인프라 분석 등 공격에 관련된 여러 분석 자료를 세상에 공개했다. 해당 정보들은 다크웹 유출 사이트를 통해 약 4 일간 게시됐다. 이후 다크웹 유출 사이트를 폐쇄하며 LockBit 의 활동도 마무리되는 듯했지만, 이들은 새로운 다크웹 유출 사이트를 통해 활동 재개 소식 및 그룹 활동이 지속될 것임을 알렸다.

Cyclops 리브랜딩 그룹 Knight 의 행보가 눈에 띄고 있다. Knight 는 2023 년 6 월에 발견된 이들은 당시 Windows, Linux, macOS, ESXi[6], Android 플랫폼을 감염시킬 수 있는 빌더 [7] 를 제공했다. 이들은 파일 암호화만 진행하는 경량 버전의 랜섬웨어를 배포하는 등 꾸준한 활동을 이어오다가, 같은 해 12 월부터는 급격히 모습을 감췄다. 운영해오던 데이터 유출 사이트는 2024 년 2 월 14 일 오프라인 상태로 변경됐다.

[6] ESXi : VM 웨어에서 개발한 호스트 컴퓨터에서 다수의 운영체제를 동시에 실행시킬 수 있는 UNIX 기반 논리적 플랫폼

[7] 빌더 : 환경 설정을 통해 원하는 기능으로 이루어진 랜섬웨어를 만들 수 있는 랜섬웨어 제작 툴

2024 년 2 월 18 일 RAMP 포럼[8]을 통해 깜짝 모습을 드러낸 Knight 관계자는 자신들의 랜섬웨어 소스 코드를 판매한다는 소식을 전했다. 판매하는 코드는 2023 년 11 월에 출시된 Knight 3.0 버전으로, 코드 내에 관리자 패널과 암호화 도구를 포함하고 있다. 해당 코드를 신뢰할 수 있는 개인에게만 판매한다고 밝힌 것으로 보았을 때, 활동을 잠정 중단하는 것으로 보인다.

한편, 최근에 원격 데스크톱 솔루션의 신규 취약점이 랜섬웨어 공격에 활용된 정황이 확인됐다. 해당 취약점은 ConnectWise 의 ScreenConnect[9] 취약점으로, CVE-2024-1708[10], CVE-2024-1709[11] 에 해당한다. 공격자는 해당 취약점을 통해 원격 데스크톱에 임의의 코드를 실행하거나 관리자 권한을 가진 계정을 생성하고 활용할 수 있다. 실제로 LockBit 은 CVE-2024-1709 취약점을 통해 911 시스템에 연결된 원격지에 랜섬웨어를 배포했으며, BlackCat(Alphv)은 의료기관을 공격하기 위해 취약점을 활용한 것으로 추정된다. BlackBasta 와 Bloody 그룹도 초기 침투로 ScreenConnect 취약점을 악용한 것으로 보인다. 해당 취약점이 패치되지 않은 서버가 많아 각별한 주의가 필요하다.

[8] RAMP 포럼 : 딥웹 및 다크웹에서 해킹 도구를 팔거나 관련 정보를 주고 받는 러시아 해킹 포럼

[9] ScreenConnect : 인터넷이나 다른 네트워크를 통해 컴퓨터를 원격으로 제어할 수 있는 원격 데스크톱 소프트웨어

[10] CVE-2024-1078 : 공격자가 취약한 인스턴스에서 원격으로 코드를 실행할 수 있는 경로 탐색 취약점

[11] CVE-2024-1079 : 공격자가 취약한 인스턴스에 시스템 관리자 계정을 생성할 수 있는 인증 우회 취약점

■ 랜섬웨어 뉴스

infosec

LockBit Cronos 작전으로 인한 일시적 폐쇄

- FBI, 유로폴, NCA 등 11개국 기관 협조
- PHP 취약점 (CVE-2023-3824*)을 통해 인프라 침투 및 무력화
- 4일간 LockBit 블로그에 복호화 도구나 관계자 체포와 같은 주요 정보 공유
- LockBit, PHP가 설치되지 않은 백업 서버를 통해 약 5일만에 복구 완료
- 탈취된 암호화키는 전체 키의 2.5%이며, 유출된 계열사 정보 또한 실제 신원은 포함되지 않았다 주장

* CVE-2023-3824: PHP archive 파일 로드 시 발생하는 스택 버퍼 오버플로우를 통해 원격 코드 실행이 가능한 취약점

법 집행 기관, 압수한 LockBit 블로그 통해 Cronos 작전 관련 주요 정보 공개

- LockBit의 인프라를 압수했으며, 소스 코드와 계열사 정보와 같은 인프라 정보 일부 공개
- LockBit 4.0 으로 추정되는 .NET 기반 랜섬웨어 LockBit-NG-Dev 버전 발견
- 자체 제작한 정보 탈취 자동화 도구 StealBit 인프라 분석
- 폴란드와 우크라이나에서 LockBit 관계자 4명 체포 소식 전달

Knight 랜섬웨어, RAMP 포럼에서 개인 사용자에게 판매

- Cyclops 라는 유저가 RAMP 포럼에 Knight 3.0 버전의 소스코드를 판매하는 글을 게시
- 관리 패널, 암호화기가 포함되어 있으며, 신뢰된 개인 사용자에게만 판매

원격 데스크톱 솔루션 ScreenConnect 취약점을 악용한 랜섬웨어

- CVE-2024-1708, CVE-2024-1709로, 경로 탐색과 인증 우회 가능
- 2024년 2월 13일 취약점이 공개되었으며, 2월 19일 패치 공개
- LockBit, BlackCat(Alphv), BlackBasta, Bloody 등 다수 그룹, 실제 공격에 사용한 정황 포착

미 국무부, BlackCat(Alphv) 최대 1,500만 달러 현상금 부과

- 주요 관계자의 신원이나 위치를 식별하면 최대 1,000만 달러 제공
- 체포 또는 유죄 판결로 이어지는 정보에는 최대 500만 달러 제공

GO 언어* 기반 신규 랜섬웨어 그룹 Ransomhub, JKwerlo 등장

- Ransomhub 그룹, CIS, 쿠바, 북한, 중국, 루마니아와 비영리단체 공격 대상 제외
- JKwerlo, 프랑스어와 스페인어를 사용하는 사용자를 타깃으로 공격 수행

* Go 언어 : Google에서 생산성을 높이기 위해 개발한 오픈소스 프로그래밍 언어


Rhysida, 미국의 소아 치료 기관 Luire Children's Hospital 공격
Luire Children's Hospital 측, 지난달 31일 랜섬웨어 피해 사실 인지 후 내부 시스템 오프라인으로 전환
2월 27일, Rhysida 랜섬웨어 그룹 다크웹 유출 블로그에 피해 사실 게시
Mogilevich, 미국의 비디오 게임 배급사 Epic Games와 아일랜드 외무부 공격 주장
계정 정보, 소스코드를 포함한 Epic Games 데이터와 아일랜드 외무부 문서를 탈취했다고 블로그에 게시
Epic Games는 피해 사실을 확인할 수 없다 주장
아일랜드 외무부 또한 공격 증거가 존재하지 않으며, Mogilevich 그룹이 허위로 게시 중이라 주장

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

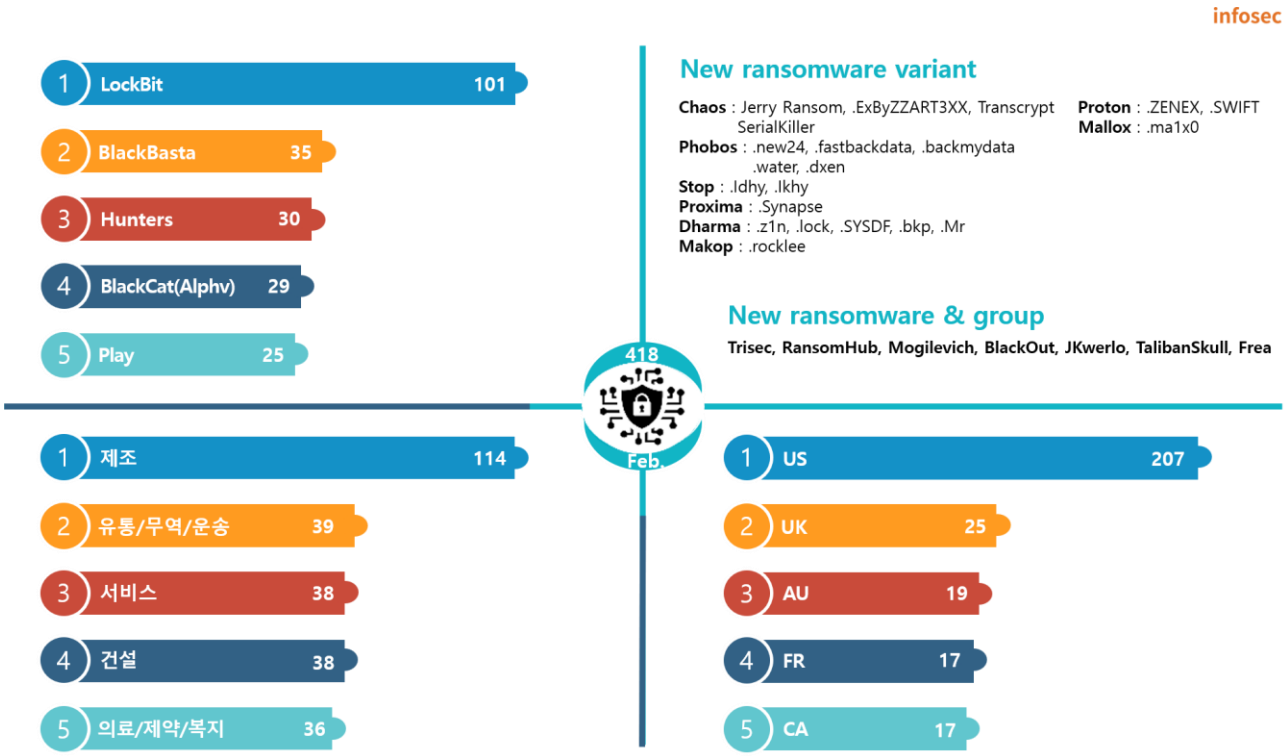


그림 2. 2024 년 2 월 랜섬웨어 위협 현황

새로운 위협

LockBit 그룹이 국제 기관에 의해 인프라를 압수당하고, BlackCat(Alphv) 그룹에 현상금이 부과되는 등 랜섬웨어 그룹들이 견제를 받고 있는 상황임에도 불구하고, 신규 랜섬웨어 그룹이 꾸준히 등장하며 랜섬웨어 위협이 지속되고 있다.

Trisec 그룹은 피해자가 직접 최초 몸값을 제안하도록 하는 독특한 방식을 사용한다. 피해자에게 몸값을 제시하는 일반적인 방식과는 다소 다른 모습이다. 이들의 텔레그램 채널에서는 튀니지 국기를 사용하고 있으며, 다크웹 유출 사이트에는 '튀니지에 영광을 바친다'는 문구를 기재하고 있다. 또한 포럼을 통해서 튀니지 출신의 인재를 모집한다는 글을 게시하는 등 튀니지 국가 기반의 그룹임을 나타내는 정황들이 확인되고 있다.

Ransomhub 는 Go 언어[12]를 기반으로 여러 플랫폼을 감염시킬 수 있는 랜섬웨어다. 이들의 다크웹 유출 사이트에 공지한 자신들의 규칙에 따라 CIS[13], 쿠바, 북한, 중국, 루마니아는 공격하지 않으며, 이미 공격당한 대상을 재 공격하지 않는다. 보통 CIS 국가만 공격하지 않는 것과 달리, 공격 대상 제외 국가에 쿠바, 북한, 중국, 루마니아가 포함되어 있다는 사실은 해당 국가 출신의 해커가 포함되어 있을 가능성으로 볼 수 있다. 한편 이들은 보통 포럼을 통해서 계열사를 모집한다.

2 월 21 일에 랜섬웨어 그룹 Mogilevich 가 새롭게 등장했다. 이들은 미국 비디오 게임 유통사이자 소프트웨어 개발사인 Epic Games 의 계정 정보 및 소스코드를 포함한 데이터와 아일랜드 외무부의 문서 데이터를 탈취했다고 주장했다. 그러나 Epic Games 와 아일랜드 외무부에서 탈취한 데이터 샘플이나 직접적인 피해 증거가 확인되지 않았다. 이후 3 월 3 일 탈취 수법과 약 1 억 6 천만 원(원화)의 수익을 직접 공개하며, 스스로가 사기꾼임을 입증하고 종적을 감췄다.

[12] Go 언어 : Google 에서 생산성을 높이기 위해 개발한 오픈소스 프로그래밍 언어

[13] CIS (Commonwealth of Independent States) : 소련의 해체로 독립한 국가들의 국제기구. 러시아, 몰도바, 벨라루스, 우즈베키스탄, 카자흐스탄 등이 포함됨

Top5 랜섬웨어

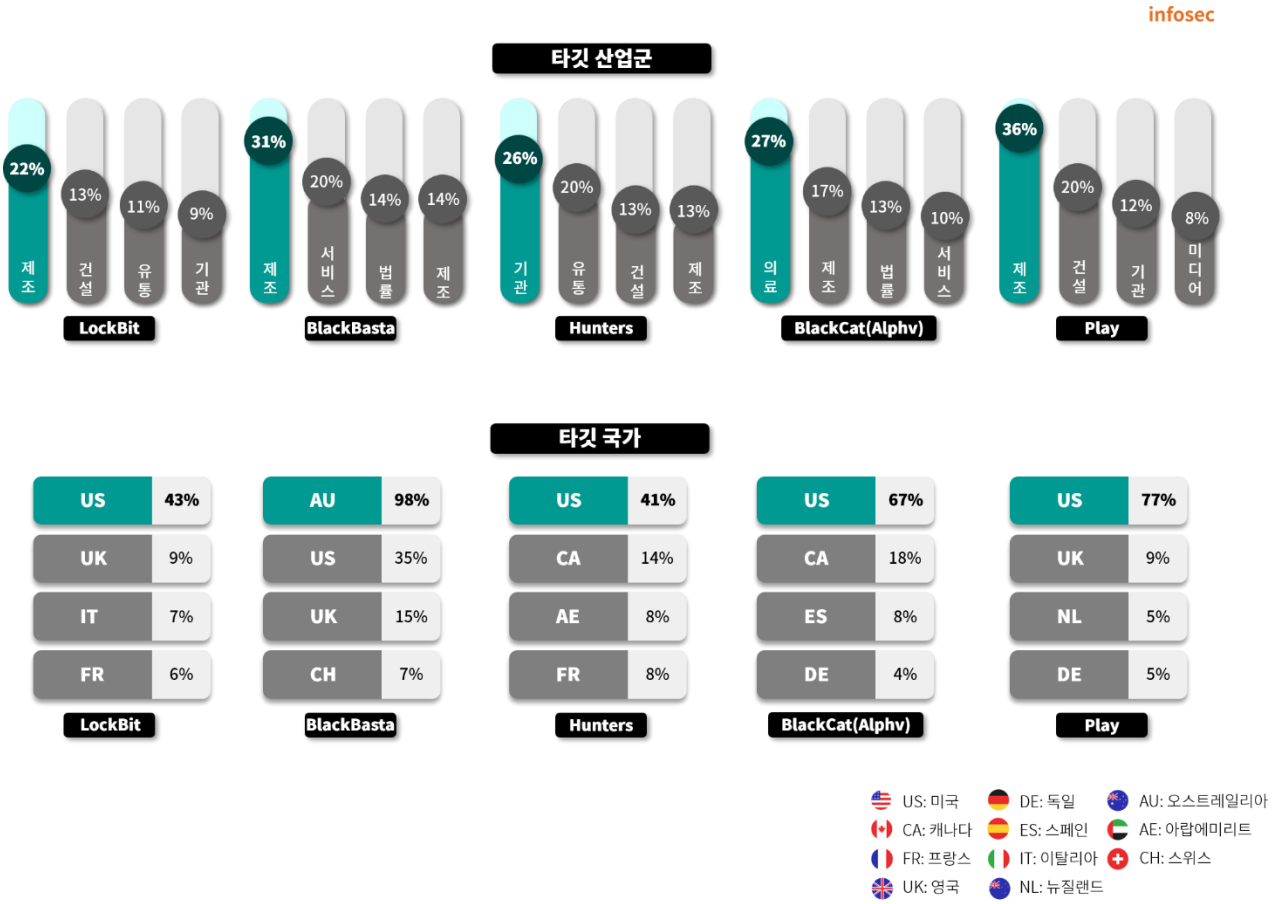


그림 3. 산업/국가별 주요 랜섬웨어 공격 현황

LockBit 은 국제 공조로 인프라가 압수된 상황에서도 백업 서버를 통해서 5 일 만에 복귀해 시선을 모았다. LockBit 은 인프라를 압수당해도 문제를 최소화할 수 있도록 인프라를 분산시킬 예정이라고 발표했다. 또한 새로운 다크웹 유출 사이트의 첫 게시글로 FBI 를 등록했으며, 텍스트 파일을 통해 Cronos 작전이 실질적으로 큰 피해를 주지 않았음을 전달했다. 이외에도 LockBit 이 원격 데스크톱 솔루션인 ScreenConnect 의 최신 취약점을 이용하여 미국의 911 시스템을 사용하는 원격지에 랜섬웨어를 배포한 정황도 포착됐다.

BlackCat(Alphv)은 지난해 12 월 이후부터 미국 의료 시설에 대한 공격을 이어가고 있다. 2 월부턴 ScreenConnect 신규 취약점을 활용해 미국의 의료 시설을 공격하고 있는 것이 확인됐다. FBI 는 BlackCat(Alphv)에 관련된 정보를 제공할 경우 최대 1,500 만 달러의 현상금을 지급할 것을 발표했다. 또한 FBI, CISA[14], HHS[15] 는 미국 병원을 표적으로 한 BlackCat(Alphv) 랜섬웨어 공격에 대해 추가적으로 경고했다.

Play 랜섬웨어 그룹은 2022년 6월 등장해 현재까지 약 360개의 조직(국가 주요 기반 시설 포함)을 공격했다. 이로 인해 지난해 12 월 CISA 및 ACSC[16] 는 Play 에 대해 경고하는 합동 사이버 보안 권고문을 발표하기도 했다. 최근에는 미국 식음료 기업인 Welch's 를 공격하여 시스템 운영을 중단시켰으며, 해당 기업의 기밀 데이터와 고객 문서, 금융 정보들을 탈취했다고 밝혔다.

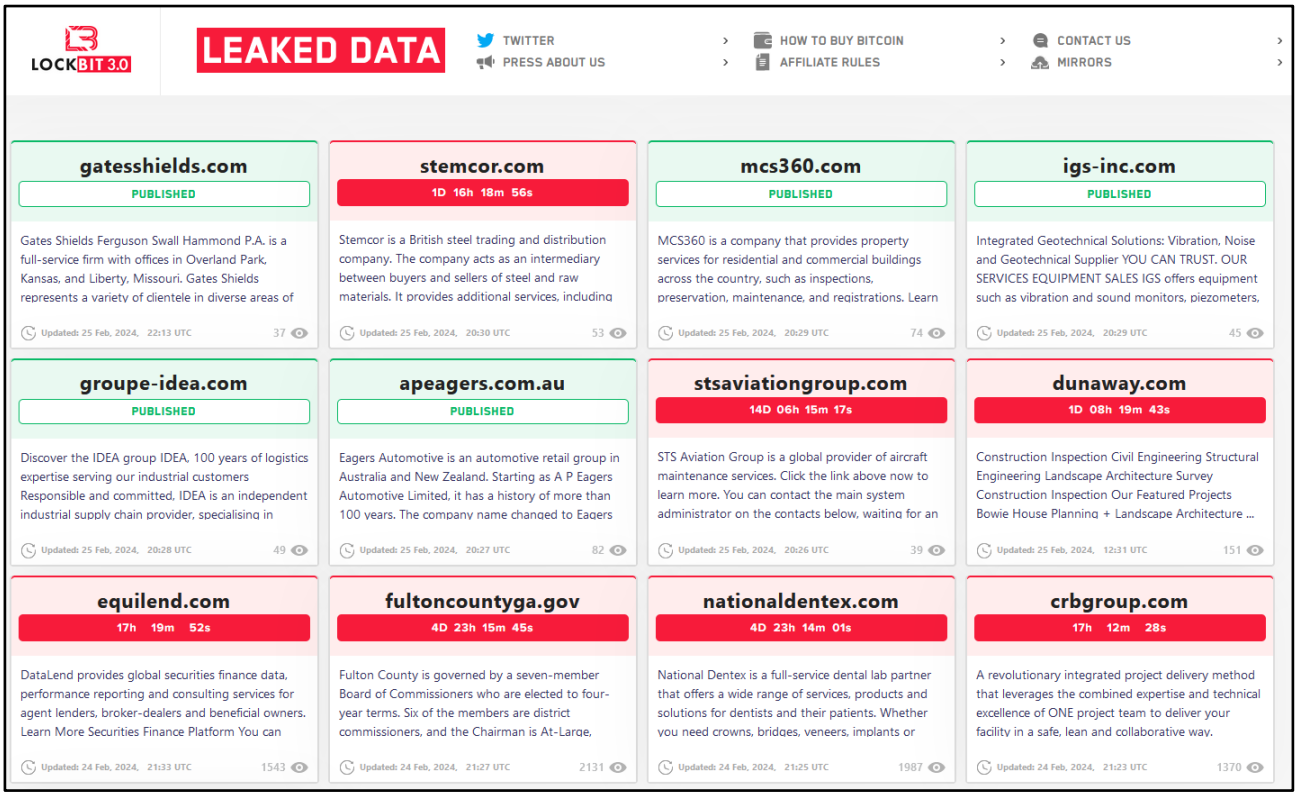
대부분의 랜섬웨어는 상대적으로 보안이 취약한 제조업을 대상으로 랜섬웨어 공격을 수행하는 반면, Hunters 랜섬웨어는 제조업 공격 비율이 13%로 상대적으로 낮고 주요 기관과 유통업을 주 타깃으로 공격을 수행했다. 또한 BlackBasta 랜섬웨어는 다수의 호주 업체가 사용중인 호스팅 서비스를 공격하여 공격 대상 국가에서 호주가 가장 높은 수치를 기록하는 등 다른 공격 양상을 보였다.

[14] CISA (Cybersecurity & Infrastructure Security Agency) : 미국 국토안보부 산하의 사이버보안 및 인프라 보안국

[15] HHS (United States Department of Health and Human Services) : 미국 보건복지부

[16] ACSC (Australian Cyber Security Centre) : 호주 정부의 사이버 보안 주도 기관인 호주 사이버 보안 센터

■ 랜섬웨어 집중 포커스

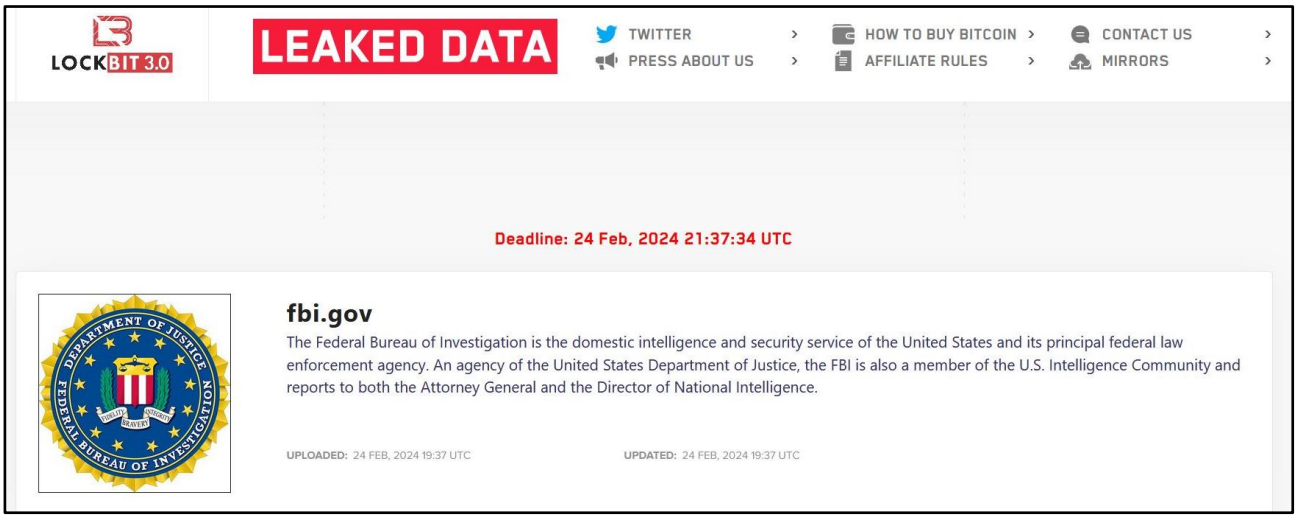


출처: LockBit 3.0 랜섬웨어 그룹 데이터 유출 사이트

LockBit 는 2019 년 9 월부터 4 년간 활동 중이며, 여러 계열사를 대상으로 랜섬웨어를 제공하고, 탈취한 몸값의 일부를 수수료로 받는 RaaS 형태의 랜섬웨어 조직이다. LockBit 은 체계적이고 효과적인 공격을 위해서 지속적으로 자체 시스템을 업데이트해 왔다. 일례로 이들의 정보 탈취 도구인 StealBit 과 그룹 정책을 통한 내부 전파 기능이 추가된 LockBit 2.0(Red) 버전을 2021 년 6 월 업데이트했으며, 2022 년 6 월에는 BlackMatter 랜섬웨어와 유사한 탐지 회피 기법이 적용된 LockBit 3.0(Black) 버전을 공개했다. 2023 년 1 월에는 Conti 랜섬웨어를 재사용한 LockBit Green 버전도 등장했다.

LockBit 은 일반적인 랜섬웨어 그룹의 운영과는 다른 치밀한 모습을 보인다. 랜섬웨어를 3.0 버전으로 업데이트한 후, 랜섬웨어의 취약점으로 인해 복호화 도구가 출시되는 것을 예방하기 위한 버그 바운티 [17] 를 개최했다. 이를 통해 비즈니스 아이디어를 제안받고 다크웹 유출 사이트, Tox 메신저 [18], Tor 네트워크 [19]를 통해서 자신들의 IP 나 위치 정보와 같은 신원 정보가 노출되지 않는지 등을 점검한다.

2024 년 2 월 20 일 영국, FBI, Europol 등 11 개국 기관들은 Cronos 작전을 통해 LockBit 의 다크웹 유출 사이트와 일부 데이터들을 압수했다. 공격에 사용되는 서버 34 개와 계정 14,000 개를 포함한 범죄 인프라를 무력화했다고 발표했다. 이 과정에서 LockBit 4.0 버전 혹은 새로운 버전으로 사용될 수 있는 .NET[20] 으로 개발된 LockBit-NG-Dev 랜섬웨어가 발견됐다. 이 밖에도 이들은 압수한 유출 사이트를 통해서 2 월 25 일까지 LockBit 의 활동과 관련한 여러 정보들을 게시했다. 게시된 정보에는 StealBit 인프라, 계열사 명단, 관계자 체포 소식, 복호화 키 및 도구 배포, LockBit 계정 폐쇄 소식 등 다수의 내용이 포함됐다.



출처: LockBit 3.0 랜섬웨어 그룹 데이터 유출 사이트

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

[18] Tox 메신저: 메시지와 사용자의 개인 정보 보호 기능을 제공하는 메신저

[19] Tor 네트워크: 사용자의 온라인 활동을 숨기는 익명성 보호 네트워크

[20] .NET : MS 에서 개발한 Windows 프로그램 개발 및 실행 환경

LockBit 은 인프라를 압수 당한지 5 일 만에 새로운 다크웹 유출 사이트를 통해 활동을 재개했다. 이들은 백업된 서버 데이터를 통해 다크웹 유출 사이트를 복구했으며, PHP 취약점(CVE-2023-3824[21])이 패치된 버전으로 수정했다.

새로운 유출 사이트에는 가장 첫 번째로 FBI 를 게시하고 Cronos 작전과 관련된 이야기를 전했다. 탈취당한 복호화 키는 전체 키의 2.5%뿐이며, 발표한 계열사 정보도 실제 신원 정보를 포함하고 있지 않다고 말했다. 이들은 “압수당한 데이터들이 아주 일부에 불과해 LockBit 의 활동에 전혀 문제없다”고 덧붙였다. LockBit 은 이번 사건을 계기로 인프라와 운영적 측면을 더 강화할 것이라고 발표했다. 이와 함께 다른 랜섬웨어 그룹에게 PHP 취약점(CVE-2023-3824)을 통해서 공격당할 수 있다고 경고하는 메시지도 전달했다.

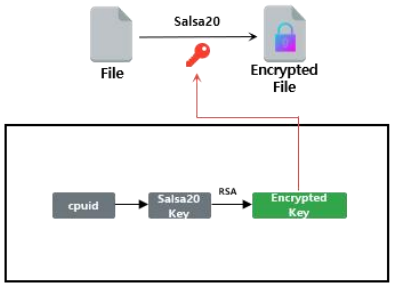
여러 국가 기관이 수개월 동안 국제 공조를 진행했음에도 불구하고 LockBit 은 빠르게 복귀 후 새로운 유출 데이터를 업로드 중이다. 이번 사건을 계기로 LockBit 랜섬웨어 그룹의 행보가 주목되는 가운데, LockBit 3.0 의 랜섬웨어를 자세히 살펴보고자 한다. 더불어 LockBit 그룹의 전략에 대비한 대응 방안을 제시한다.

[21] CVE-2023-3824 : PHP 애플리케이션 배포 및 설치에 사용되는 PHP Archive 파일을 읽어 올 때 발생하는 원격 코드 실행 취약점. PHP 8.0.30 이전의 8.0.* 버전, 8.1.22 이전의 8.1.* 버전, 8.2.8 이전 버전의 8.2.* 버전이 해당된다.

LockBit 3.0 Ransomeware

암호화 키

Salsa20 알고리즘으로 파일 암호화를 하고, 해당 키를 RSA로 보호



암호화 방식

512KB 이하: 파일 전체 암호화
512KB 초과 5.5 MB 이하: 최초 512KB 암호화
5.5 MB 초과 60.5MB 이하: 5.5MB 마다 512KB 암호화
60.5MB 초과 253MB 이하: 최초 5MB 암호화 후 15.5MB 마다 512KB 암호화
253MB 초과 1GB 이하: 최초 5MB 암호화 후 31MB 마다 1MB 암호화
1GB 초과: 최초 15MB 암호화 후 102.5MB 마다 2.5MB 암호화

특징

랜섬노트

[A-Za-z0-9]{9}_README.txt

변경 확장자

.[A-Za-z0-9]{9}

RSA 공개키로 생성한 해시값의 앞 9글자

제작 언어

C/C++

그림 4. LockBit 3.0 랜섬웨어 개요

LockBit 3.0 랜섬웨어 전략

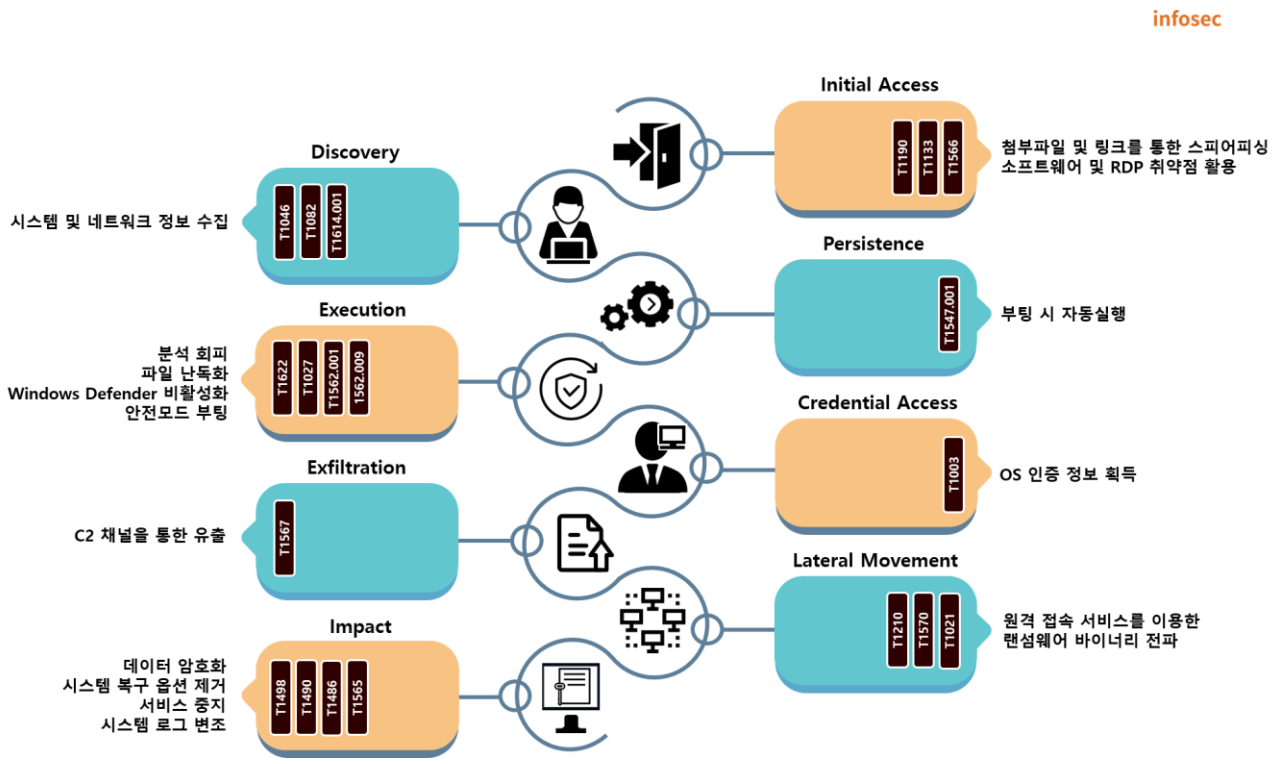


그림 5. LockBit 3.0 랜섬웨어 공격 전략

LockBit 3.0 랜섬웨어는 계열사별로 다양한 초기 침투 방식을 사용한다. 취약한 소프트웨어나 RDP[22] 취약점을 통해서 초기 침투를 시도하거나, 윈도우 설치 파일로 위장한 NSIS[23] 실행파일 형태로 배포해 침투하는 경우도 있다. 국내에서는 파일 아이콘 변경을 통해 이력서로 위장한 실행파일이나, 문서에 포함된 스크립트를 통해서 감염시키는 버전도 발견됐다. 필요에 따라서 C2 서버[24]로부터 랜섬웨어를 다운로드 받거나, 압축된 랜섬웨어를 이용하는 경우도 존재한다.

추가적으로 자격 증명 탈취, 시스템 데이터 수집, 내부 전파, 원격 접속, 데이터 유출을 위한 도구들을 다운로드 받아 사용한다. 악성 도구와 자체 제작한 정보 탈취 도구뿐만 아니라, 공격을 목적으로 제작되지 않은 정상 도구를 공격에 활용하기도 한다.

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

[23] NSIS (Nullsoft Scriptable Install System) : 스크립트 기반으로 동작하는 Windows용 설치 시스템

[24] C2 서버 (Command & Control 서버) : 공격자가 초기 침투에 성공한 장치와 통신을 유지하고 명령 및 제어 전달이 가능한 도구 및 기술 집합

파일명	설명
Chocolatey	Windows 소프트웨어를 위한 명령줄 기반 패키지 관리자
Rclone	외부 스토리지 관리 및 업로드/다운로드 프로그램
WinSCP	컴퓨터와 서버 간 파일을 전송하거나 관리할 수 있는 Windows 프로그램
PsExec	로컬/원격 시스템에 임의의 프로세스를 실행할 수 있는 도구
StealBit	자체 개발한 정보 탈취 자동화 도구
Mimikatz	Windows 시스템의 메모리에서 비밀번호나 자격 증명과 같은 민감 정보를 추출하는 도구

표 1. LockBit 3.0 이 사용한 도구

LockBit 랜섬웨어는 명령어 실행 인자를 확인하여 여러 가지 기능을 수행할 수 있으며 공격의 편의성 및 효율성을 위한 기능으로 제공한다. 특히, 랜섬웨어 실행에 필요한 키를 입력해야 파일 암호화가 진행된다.

유출된 LockBit 3.0 빌더에 따르면, 분석가가 쉽게 랜섬웨어를 분석하지 못하도록 랜섬웨어 일부를 인코딩하여 보호하는 기능이 존재한다. 보호된 파일의 경우, -pass 인자와 함께 32Bytes 길이의 키를 입력하지 않으면, 파일이 디코딩되지 않아 파일 암호화와 내부 전파와 같은 기능이 실행되지 않고 종료된다.

인자	설명
-path {path}	지정한 경로만 암호화
-pass {32Bytes key}	랜섬웨어 실행에 필요한 키 입력
-safe	안전모드로 부팅 후 파일 암호화
-wall	바탕화면 변경 및 랜섬노트 출력
-gspd	그룹 정책 수정 및 내부 전파
-psex	관리 공유를 이용한 내부 전파
-gdel	그룹 정책 변경 사항 삭제
-del	실행 후 자가 삭제

표 2. LockBit 3.0 랜섬웨어 인자

파일 암호화나 레지스트리 조작 등 시스템 구성요소 접근에는 관리자 권한이 필요한데 UAC[25] 우회를 통해 강제적으로 시스템 구성요소에 접근 후, 관리자 권한을 가진 프로세스의 권한을 복제하여 사용한다. 권한 상승 이후에는 실행중인 프로세스와 보안과 백업에 관련된 서비스를 종료한 뒤, 피해자가 임의로 복구하는 것을 방지하기 위해 VSC[26] 를 삭제한다. 이후 드라이브와 네트워크 리소스에 접근하여 대상을 수집하고 파일 암호화를 진행한다.

랜섬웨어 전파를 위해서 PsExec 도구를 사용해 원격으로 명령을 실행시키거나, 그룹 정책을 수정하여 AD[27] 의 도메인 서버를 감염시키는 방식을 사용한다. LockBit 3.0 실행 시 -psex 인자나 -gspd 인자와 함께 실행해야 내부 전파가 이루어진다.

LockBit 은 위와 같이 파일 암호화와 내부 전파를 위한 시스템 구성요소 관리 외에도, 다양한 요소를 변경해 침투한다. 바탕화면과 암호화된 파일의 아이콘을 자체 생성한 이미지 파일로 바꾸며, 랜섬웨어를 시작 프로그램으로 등록한다. 사용자가 해당 시스템을 부팅하면 자동으로 랜섬웨어가 실행되는 구조다. 뿐만 아니라 랜섬웨어에 하드코딩된 문자열을 통해서 이벤트 로그 [28] 데이터를 덮어 씌우고, 이벤트 로그를 비활성화 해 LockBit 랜섬웨어의 공격 흔적을 삭제해 추적을 회피하고 공격 벡터를 확인하기 어렵도록 탐지 및 분석을 방해한다.

[25] UAC (User Account Control) : 시스템에 영향을 줄 수 있는 작업을 허용 여부를 확인하는 보안 매커니즘

[26] VSC (Volume Shadow Copy) : Windows 시스템에서 파일이나 볼륨의 특정 시점의 백업 복사본을 생성하는 기능

[27] AD (Active Directory) : 조직 내의 자원 및 권한 등을 관리할 수 있는 Windows 기반 중앙집중관리 서비스

[28] 이벤트 로그 : 시스템의 성능, 오류, 경고, 운영 정보 등 중요 정보가 기록된 데이터

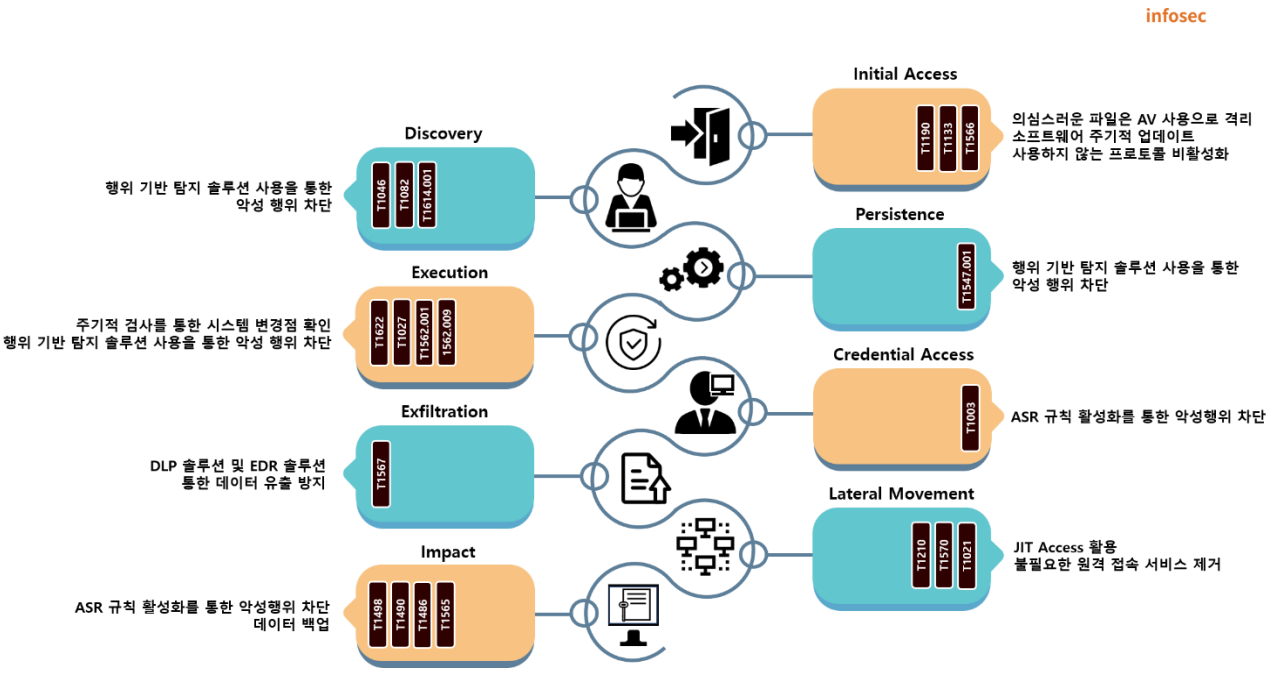


그림 6. LockBit 3.0 랜섬웨어 대응방안

LockBit 은 메일의 첨부파일을 통해서 랜섬웨어 실행을 유도한다. 첨부된 파일은 악성 스크립트가 포함된 파일이거나 문서 아이콘으로 위장한 실행 파일이다. 국내에서는 이력서나 저작권 위반 사칭 메일로 위장하여 유포된 바 있다. 따라서 출처가 불분명한 이메일의 첨부파일이나 링크를 실행하지 않도록 주의하고, Anti-Virus 를 사용하여 프로그램이나 스크립트가 실행되지 못하도록 관리해야 한다. 또한, 소프트웨어의 취약점이나 프로토콜 취약점을 이용해 직접 배포하기도 한다. 따라서 소프트웨어나 운영체제를 취약하지 않은 버전으로 주기적으로 업데이트하고, 사용하지 않는 프로토콜은 비활성화해 감염을 예방해야 한다.

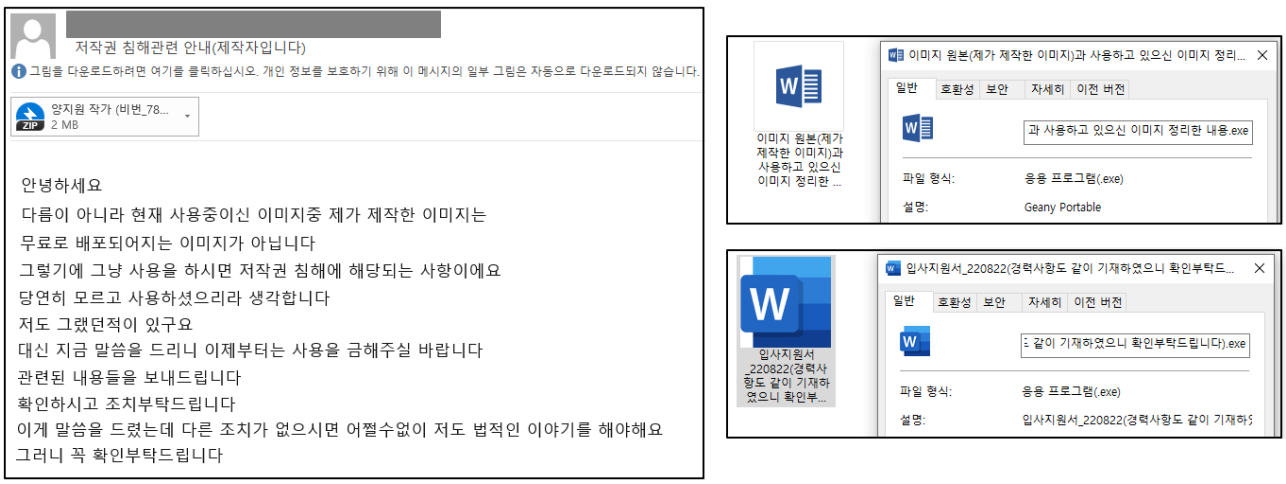


그림 7. LockBit 3.0 이 국내에 유포한 메일과 악성 파일

CVE	설명	영향 버전	패치 버전
CVE-2018-13379	Fortinet 의 보안 OS FortiOS 에서 SSL VPN[29]을 사용하는 경우, 시스템 파일을 다운로드 받을 수 있는 파일 경로 탐색 취약점	5.4.6 ~ 5.4.12 5.6.3 ~ 5.6.7 6.0.0 ~ 6.0.4	5.6.8 이상 6.0.5 이상
CVE-2020-0796	Windows 에서 사용하는 자원 공유 프로토콜인 SMB 3.1.1 에서 발생하는 원격 코드 실행 취약점	Windows 10 & Server 2016 (build 1903, 1909)	KB4551762 업데이트
CVE-2021-44228	JAVA 기반의 오픈소스 로깅 라이브러리 Log4j 에서 발견된 원격 코드 실행 취약점	2.0-beta9 ~ 2.15.0 (2.12.2, 2.12.3, 2.3.1 제외)	2.12.2, 2.12.3, 2.3.1, 2.16.0 이상
CVE-2021-22986	F5 의 애플리케이션 배포 네트워크 장비인 BIG-IP, BIG-IQ 에서 발생하는 원격 코드 실행 취약점	패치 버전 이전의 16.0.*, 15.1.*, 14.1.*, 13.1.*, 12.1.*	16.0.1.1 이상 15.1.2.1 이상 14.1.4 이상 13.1.3.6 이상 12.1.5.3 이상
CVE-2021-26855 **CVE-2021-26857** **CVE-2021-26858** **CVE-2021-27065**	MS 의 전자 메일 서버인 Exchange Server 에서 발생하는 원격 코드 실행 취약점	Exchange Server 2013, 2016, 2019	KB5000871 업데이트
CVE-2021-36942	Windows Server 에서 인증되지 않은 공격자가 도메인 컨트롤러를 통해 다른 서버에 인증하도록 허용 가능한 취약점	2008 r2 sp1, 2016, 2008 sp2, 2012, 2012 r2, 2020 h2, 2004, 2019	KB5005076 혹은 KB5005106 업데이트
CVE-2022-3653	크롬 브라우저의 Vulkan 그래픽 엔진에서 발생하는 힙 버퍼 오버플로우 취약점	107.0.5304.62 미만	107.0.5304.62 이상
CVE-2022-36537	오픈 소스 JAVA 프레임워크 Zk Framework 에서 발생하는 취약점으로, POST 요청을 조작하여 중요한 정보에 접근할 수 있는 취약점	9.6.1, 9.6.0.1, 9.0.1.2, 8.6.4.1	9.6.2 이상
CVE-2023-0669	Forta 의 보안 관리 파일 전송 소프트웨어 GoAnywhere MFT 에서 원격 코드 실행이 가능한 취약점	7.1.1 이하	7.1.2 이상
CVE-2023-20269	통합 보안 플랫폼 Cisco ASA 와 차세대 위협 방어 플랫폼 Cisco FTD 소프트웨어의 원격 액세스 VPN 취약점으로 인해 자격 증명을 획득할 수 있는 취약점	9.19.1.18 이하	9.20 이상
CVE-2023-27350 **CVE-2023-27351**	인쇄 관리 소프트웨어 PaperCut 에서 사용자 증명을 우회하여 관리자로 서버에 접근 후 원격 코드 실행이 가능한 취약점	15.0.0 ~ 20.1.7, 21.0.0 ~ 21.2.11, 22.0.0 ~ 22.0.9	20.1.7 이상 21.2.11 이상 22.0.9 이상
CVE-2023-4966	네트워킹 제품인 NetScaler ADC 및 NetScaler Gateway 에서 발생하는 정보유출 취약점	패치 버전 이전의 14.1*, 13.1*, 13.0*	14.1-8.50 이상 13.1-49.15 이상 13.0-92.19 이상
CVE-2024-1709	원격 데스크톱 솔루션 ScreenConnect 취약점으로, 원격 데스크톱에 시스템 관리자 계정을 생성할 수 있는 인증 우회 취약점	23.9.7 이하	23.9.8 이상

표 3. LockBit 3.0 이 악용한 소프트웨어 취약점

[29] VPN (Virtual Private Network) : 개인 정보를 보호하고 지역 제한을 우회하기 위해 사용하는 가상 네트워크

초기 침투 이후에는 탐지 회피와 지속성 확보를 위해서 레지스트리를 조작하거나 Anti-Virus 서비스를 종료시키고 안전 모드로 부팅하는 방식을 사용한다. 이러한 시스템 기능 악용을 예방하기 위해 행위 기반 탐지 솔루션을 사용할 것을 권장한다.

랜섬웨어 전파를 위해서 그룹 정책을 수정하거나, 원격으로 명령어를 실행한다. 이를 방지하기 위해서 JIT Access[30] 방법을 사용해 정해진 시간에 최소 권한의 원칙으로 이용 권한을 부여하도록 한다. 이와 함께 지속적인 모니터링을 통해 AD 에 등록된 서비스와 그룹 정책 목록을 확인하는 등 의심스러운 사항이 없는지 살펴봐야 한다.

데이터 탈취, 백업 데이터 삭제 및 파일 암호화에 대해서도 대비가 필요하다. DLP[31] 솔루션이나 EDR[32] 솔루션을 활용하여 데이터 유출을 방지할 수 있다. 또한, 파일 복구를 위하여 정기적으로 백업을 생성하여 관리해야 하며, NAS[33] 와 백업 저장소의 데이터를 삭제하는 경우도 존재하므로, 별도의 네트워크나 저장소에 데이터를 소산 백업[34] 하여 관리하는 것을 권장한다.

[30] JIT Access (Just-in-Time Access) : 애플리케이션이나 시스템에 접근하기 위해 부여된 권한이 사전에 결정된 기간에만 제공되는 접근 방식

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

[32] EDR (Endpoint Detection and Response) : 컴퓨터와 모바일, 서버 등 단말기에서 발생하는 악성 행위를 실시간으로 감지하고 분석 및 대응하여 피해 확산을 막는 솔루션

[33] NAS (Network Attached Storage) : 네트워크에 연결되어 여러 사용자가 데이터를 공유하고 접근할 수 있는 저장 장치

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

Indicator Of Compromise

Lockbit 3.0 : SHA256

5c9b94f7aed569bb91c77cb0bf8a4f0c13145f8ac35bccc961c973720e46cc62
a4219b77de0ee4c2e17011b95acc69432bcb1a8dc4eb761027b9c997144a76dd
cafaaadd3747dfec3df88a34fea56695a0b5b03b27091b770075a72b03d2d105
917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2
535e0dbd97cb9ea66f375400b550dd3bcad0788a89fb46996a651053a2df07c3

임서은.docx (Dropper) : SHA256

1f0617725b2a0b0c3bb1067f0b77da049da0545710d9743813969b3bbcc563f4

저작권 침해관련 안내(제작자입니다).eml : SHA256

4ade4f6ed21b33f627fcc704db4cbfb3dd807516c1e6fc52ae6edb8a66bc80a5

File Name

임서은.docx
sed.exe
저작권 침해관련 안내(제작자입니다).eml
입사지원서_220822(경력사항도 같이 기재하였으니 확인부탁드립니다).exe
이미지 원본(제가 제작한 이미지)과 사용하고 있으신 이미지 정리한 내용.exe

■ 참고 사이트

URL : https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

URL : https://www.boannews.com/media/view.asp?idx=126668&page=1&kind=1

URL : https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/b/LockBit-attempts-to-stay-afloat-with-a-new-version/technical-appendix-LockBit-ng-dev-analysis.pdf

URL : https://www.state.gov/reward-offers-for-information-on-LockBit-leaders-and-designating-affiliates/

URL : https://www.nomoreransom.org/en/decryption-tools.html

URL : https://home.treasury.gov/news/press-releases/jy2114

URL : https://www.secureworks.com/blog/LockBit-in-action

URL : https://seed.kisa.or.kr/kisa/Board/167/detailView.do

URL : https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

URL : https://asec.ahnlab.com/ko/31620/

URL : https://nvd.nist.gov/vuln/detail/CVE-2022-36537

URL : https://nvd.nist.gov/vuln/detail/CVE-2023-20269

URL : https://nvd.nist.gov/vuln/detail/CVE-2023-27350

URL : https://nvd.nist.gov/vuln/detail/CVE-2023-27351

URL : https://nvd.nist.gov/vuln/detail/CVE-2023-4966

URL : https://nvd.nist.gov/vuln/detail/CVE-2024-1709

URL : https://nvd.nist.gov/vuln/detail/CVE-2021-26855

URL : https://nvd.nist.gov/vuln/detail/CVE-2023-0669

URL : https://nvd.nist.gov/vuln/detail/CVE-2018-13379

URL : https://nvd.nist.gov/vuln/detail/CVE-2020-0796

URL : https://nvd.nist.gov/vuln/detail/CVE-2021-22986

URL : https://nvd.nist.gov/vuln/detail/CVE-2021-36942

URL : https://nvd.nist.gov/vuln/detail/CVE-2022-3653