KARA
Korea Anti Ransomware Alliance

2024.1Q

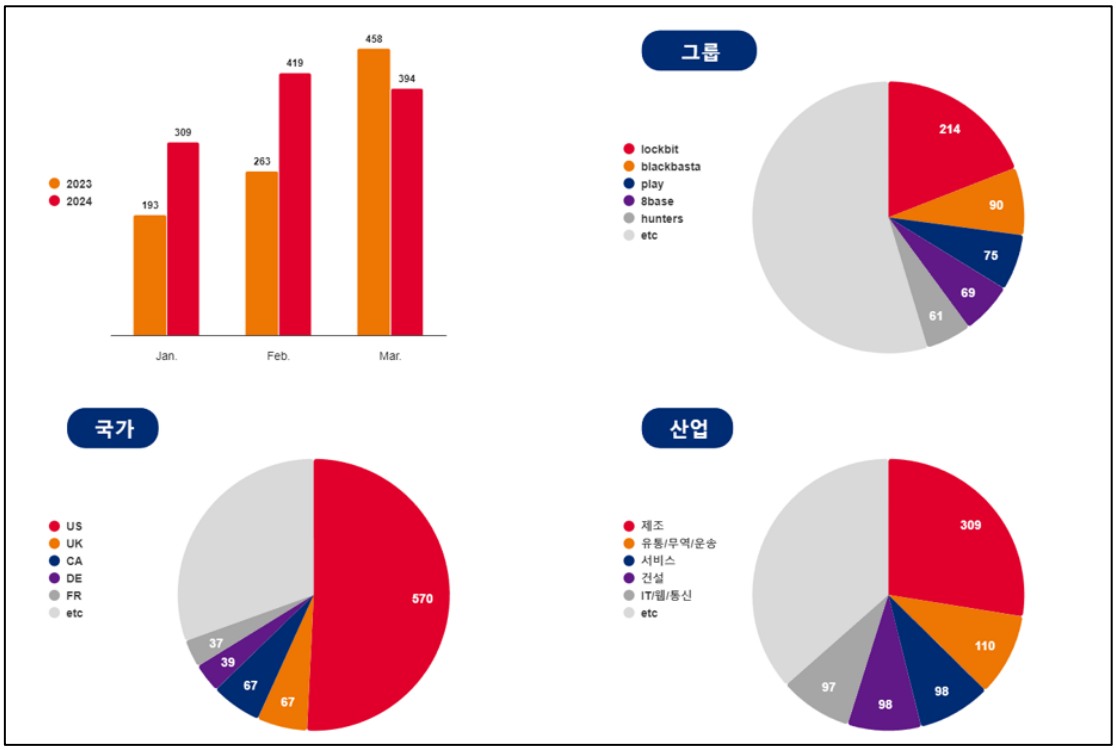
KARA 랜섬웨어 동향 보고서

KARA 랜섬웨어 동향 보고서

EQST Lab팀 이호석, 정민수, 이현아

랜섬웨어 트렌드

1. 1분기 랜섬웨어 활동 통계



[랜섬웨어 그룹 활동]

2024년 1분기의 랜섬웨어 피해 사례 수는 지난 분기 914건에 비해 약 23%가 증가한 1,122건으로 나타났다. BlackCat(Alphv)의 활동 중단과 LockBit의 인프라 압수, Rhysida 랜섬웨어 복호화 도구 출시 등의 소식이 연달아 전해지고 있음에도 불구하고 랜섬웨어로 인한 피해는 지속되고 있다.

LockBit은 인프라 압수와 연이은 조직원들의 체포에도 굴하지 않고 가장 많은 피해 조직을 만들어 내고 있다. LockBit 그룹은 국제 공조를 통한 Cronos 작전[1]으로 인해 주요 인프라가 압수되었지만, 새로운 인프라를 통해 활동을 재개하며 이전처럼 활동을 이어나가고 있다.

BlackBasta는 2023년 4월경에 발견된 샘플에 한해 암호화 로직의 결함이 확인되어 복호화 도구인 Black Basta Buster가 개발되었는데, 이후 버전부터는 해당 결함을 패치하여 복호화 도구 사용이 불가능해졌다. 최근엔 ConnectWise의 ScreenConnect[2] 취약점 CVE-2024-1709[3]를 악용하여 취약한 서버를 공격한 정황이 확인되어 한차례 이슈가 되기도 했다. ScreenConnect 취약점은 BlackBasta뿐만 아니라 LockBit, Bloody 그룹도 악용한 정황이 포착되었는데, Play 랜섬웨어 그룹도 이 대열에 합류한 것으로 확인되었다.

---

[1] Cronos 작전 : LockBit의 범죄 생태계를 파괴하기 위한 사이버 교란 작전

[2] ScreenConnect : 인터넷이나 다른 네트워크를 통해 컴퓨터를 원격으로 제어할 수 있는 원격 테스크톱 소프트웨어

[3] CVE-2024-1709 : ScreenConnect 23.9.7 버전 이하에서 발생하는 인증 우회 취약점

Play 그룹은 특히 작년에 스위스 정부 및 군대를 대상으로 소프트웨어 솔루션을 제공하는 업체인 Xplain을 타깃으로 공격해서 정부 문서 65,000건을 유출시켰던 사실이 최근 공식적으로 확인되어 이슈가 되었다. 다크웹 유출 사이트에는 지난해 5월에 게시했지만, 스위스 정부는 3월에 들어서야 공식 성명을 통해 정부 문서가 유출되었음을 밝혔고 해당 문서 내에는 기밀 정보를 비롯한 민감한 정보가 포함되어 있어 2차 피해가 발생할 가능성이 다분해 대책 마련이 촉구될 것으로 보인다.

BlackCat(Alphv) 그룹은 3월 초, UnitedHealth의 Change Healthcare로부터 약 350BTC(한화 약 310억 원)를 갈취한 뒤 계열사에게 수익 배분을 하지 않아 해당 계열사로 추정되는 "notchy"라는 사용자가 다크웹 포럼에 불만을 표출하는 사건이 발생했다. notchy는 BlackCat(Alphv)의 사기 행각을 증명하기 위해 비트코인 주소를 게시했으며 3월 1일 자로 350BTC를 받은 거래 내역을 증빙했다. 결국 며칠 뒤 BlackCat(Alphv)은 다크웹 유출 사이트를 법 집행 기관에 의해 압수당한 것으로 가장한 뒤 활동을 중단한 채로 잠적했다.

이처럼 다양한 랜섬웨어 사건 사고들이 발생하여 피해 사례가 꾸준히 발견되고 있는 모습을 보이고 있으며, 대규모 공격이나 공급망 공격[4] 등을 노리고 취약점을 악용하는 사례 역시 지속적으로 발견되고 있는 추세이다. 또한 랜섬웨어 그룹들은 합법적인 도구나 드라이버[5]를 공격에 악용하여 탐지를 우회하거나 실적이 저조한 부분을 상쇄시키기 위해 공격 타깃을 넓히는 등 다양한 전략을 사용하기 때문에 조직에서는 올바른 보안 정책을 준수하고 시스템을 최신 상태로 유지하는 것을 권장한다.

2. 랜섬웨어 트렌드

✓ 합법적인 도구를 악용하는 공격자들

기존에는 랜섬웨어 그룹들이 공격에 맞춤형 도구를 제작해서 사용하는 경향이 있었다. 대표적으로 Ryuk 그룹의 맞춤형 정보 탈취 도구 Ryuk Stealer와 LockBit 그룹의 StealBit가 이에 해당된다. 그러나 최근에는 탐지 우회를 위해 피해자의 시스템 내에 있는 합법적인 도구나 상용 RMM(Remote Monitoring and Management) 도구[6]를 공격에 악용하는 LotL(Living off the Land) 공격[7]으로 노선을 변경했다.

최근 Cactus 랜섬웨어 그룹이 글로벌 에너지 기업인 슈나이더 일렉트릭에 대한 공격 수행 시 AnyDesk, Splashtop, SuperOps[8] 등의 도구를 피해자의 시스템에 배포하여 초기 침투 및 내부 전파에 악용한 정황이 발견되기도 하였으며, LockBit 랜섬웨어 그룹 또한 Citrix Bleed 취약점인 CVE-2023-4966[9] 을 악용하여 초기 침투를 수행한 후 원격 접속 솔루션(ScreenConnect, TeamViewer 등)을 설치하고 기존 피해자의 시스템에 존재하는 합법적인 도구를 악용하여 공격을 수행했다.

랜섬웨어 그룹들은 RMM 및 시스템에 설치되어 있는 도구를 활용하여 초기 침투, 정보 유출, 내부 전파 등 탐지를 우회하기 위해 다양한 공격에 전략적으로 사용하고 있다.

---

[4] 공급망 공격 : 공격자가 제품이나 서비스의 공급 과정에 침투하여 전체 사용자에게 영향을 주는 공격 기법

[5] 드라이버 : 운영 체제와 하드웨어 장치 간의 통신을 가능하게 하는 소프트웨어

[6] RMM 도구 : 원격 위치에서 컴퓨터 및 네트워크 장비를 모니터링하고 관리할 수 있는 소프트웨어

[7] LotL 공격 : 공격자가 이미 시스템에 설치된 소프트웨어나 도구들을 사용하여 탐지를 회피하며 악성 행위를 수행하는 공격 기법

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

[9] CVE-2023-4966 : NetScaler ADC 및 Citrix NetScaler Gateway의 특정 버전 이하에서 발생하는 민감 정보 노출 취약점

✓ 랜섬웨어 공격에 사용되는 취약한 드라이버

합법적인 서명이 되어 있어 시스템은 정상 드라이버로 인식하지만 실제로는 취약한 드라이버를 악용하는 것을 BYOVD(Bring-Your-Own-Vulnerable-Driver) 기법이라고 한다. 작년부터 BYOVD 기법이 랜섬웨어 공격 사례에서도 확인되면서 주목받기 시작했는데, 올해 들어서도 Kasseika 랜섬웨어 그룹이 공격에 BYOVD 기법을 사용해서 보안 솔루션을 우회한 정황이 확인되었다.

BYOVD 기법은 서명된 드라이버를 사용하여 커널 레벨에서 실행되기 때문에 관리자 권한 보다 높은 시스템 권한을 통해 보안 솔루션을 손쉽게 우회할 수 있다는 특징을 악용한 공격 기법이다. BYOVD 공격의 대표적인 케이스로 Lazarus 그룹[10]이 국내 보안 솔루션을 악용하여 초기 침투한 뒤 취약한 드라이버 모듈을 사용하여 Anti-Virus를 무력화 한 사례가 있다. Lazarus와 같이 주로 APT 그룹[11]들이 사용하던 BYOVD가 랜섬웨어 공격으로 옮겨와서 BlackByte, Cuba, Akira, AvosLocker 등의 랜섬웨어 그룹들이 악용하게 되었는데, 1분기에 Kasseika 그룹도 이 대열에 합류한 것이다. Kasseika는 시스템 내의 보안 솔루션을 비활성화할 수 있는 권한을 가진 취약한 드라이버를 피해자의 시스템에 다운로드한 뒤 실행시켜 보안 솔루션을 무력화했으며, 이후 랜섬웨어를 유포해 시스템을 암호화 시켰다.

✓ 공격 타깃의 다변화

많은 수의 RaaS(Ransomware-as-a-Service)[12] 그룹들은 운영 측에서 자체 규정을 수립하여 이를 준수하지 않는 계열사에 대해 페널티를 부과하는 방식으로 그룹을 운영해 나가고 있다. 물론 규정은 그룹별로 상이하나, 한 가지 공통된 규칙을 꼽자면 의료, 교육, 비영리 단체를 포함한 주요 기반 시설에 대한 공격을 금지하는 조항이다. 이러한 조직에 대해 공격을 수행하게 되면 상당이 큰 사회적 혼란을 야기하게 되며, 타 랜섬웨어 그룹보다 수사 기관의 표적이 될 확률이 높기 때문에 대다수의 랜섬웨어 그룹들은 해당 기관에 대한 공격에 있어서 조심스러운 태도를 보일수 밖에 없다.

하지만 랜섬웨어로 인한 피해자들의 몸값 지불 비율이 줄어들면서 랜섬웨어 그룹들은 수익 감소의 국면을 맞이하게 되었다. 공교롭게도 주요 기반 시설 특성상 랜섬웨어 공격으로 인해 시스템이 마비가 되었을 경우 대중의 불편함과 막심한 손해가 수반될 수밖에 없다는 점을 노린 공격자들은 점차 주요 기반 시설 쪽으로 눈을 돌리고 있는 모습을 보이고 있다.

Cactus 랜섬웨어 그룹은 미국에 한 재정적 어려움을 겪던 헬스케어 조직인 Petersen Health Care를 공격하여 파산에 이르게 하기도 하였다. BlackCat(Alphv) 역시 UnitedHealth의 Change Healthcare로부터 약 350BTC(한화 약 310억 원)를 갈취하였고, 한 공격자는 Phobos 랜섬웨어 변종인 BackMyData 랜섬웨어 공격을 통해 루마니아 전역의 병원 100여 곳에 대해 운영을 중단시켰다. 이러한 주요 기반 시설에 대한 공격을 통해 운영에 차질을 빚게 하거나 이를 빌미로 거액을 갈취하는 행위를 통해 타 업계에 비해 큰 피해를 안길 수 있다는 점을 노린 공격자들이 더욱 늘어난다면 사회적 혼란이 야기될 수 있어 이러한 움직임을 면밀히 살피고 대비할 필요가 있다.

[10] Lazarus 그룹 : 북한의 정찰총국 소속 해킹 그룹

[11] APT 그룹 : 정교하고 장기적인 사이버 공격 활동을 목적으로 한 국가 지원 해킹 조직

[12] RaaS : 서비스형 랜섬웨어의 약어로, 랜섬웨어 그룹들이 계열사나 공격자에게 대가를 받고 랜섬웨어를 제공해주는 형태

✓ 랜섬웨어 그룹의 폐쇄와 복호화 도구의 등장

2024년 1분기에는 대형 랜섬웨어 그룹들이 잇따라 법 집행 기관에 의해 인프라를 압수 당하고, 다양한 랜섬웨어의 복호화 도구가 출시되는 등 랜섬웨어 공격자들에게는 악재가 연달아 이어지고 있다.

RaaS 그룹의 대표격이라고 할 수 있는 LockBit은 2024년 2월 국제 법 집행 기관들에 의해 인프라를 압수당하고 LockBit 4.0으로 추측되고 있는 LockBit-NG-Dev(LockBit-NextGeneration-Development) 및 맞춤형 정보 탈취 도구인 StealBit, 복호화 키 등이 공개되어 결국 폐쇄될 것이라 예상했으나, 새로운 다크웹 유출 사이트를 통해 활동을 재개하였다.

또 다른 대형 RaaS 그룹인 BlackCat(Alphv)에 대한 Exit Scam[13] 정황이 발견되었다. 러시아 해킹 포럼 RAMP[14]에 "notchy"로 불리는 계열사가 Change Healthcare 공격으로 인해 얻은 수익 350BTC(한화 약 310억 원)을 배분 받지 못하여 불만을 표시하며 증거로 비트코인 지갑 주소 거래 내역을 첨부한 글을 게시하여 논란이 시작되었다. 이후 BlackCat(Alphv)은 다크웹 유출 사이트를 법 집행 기관에 의해 폐쇄된 것으로 가장하였으나 NCA, FBI는 이와 관련이 없다고 주장하여 Exit Scam 의혹이 불거져 만 갔다. 결국 Tox 메신저[15] 상태 메시지마저 "Selling source code 5kk"로 변경하여 500만 달러(한화 약 67억 원)에 랜섬웨어 소스코드를 판매하겠다는 의사를 내비쳐 Exit Scam 정황이 기정사실화가 되었다.

랜섬웨어 복호화 도구 역시 꾸준히 출시되고 있는 상태이다. 대표적으로 Rhysida 랜섬웨어에 대한 복호화 도구가 국민대학교와 KISA에 의해 개발되었으며, Babuk 랜섬웨어의 변종인 Tortilla 랜섬웨어와, BlackBasta 4월에 유포한 샘플과, Mallox 랜섬웨어의 2022년 10월부터 2024년 2월까지 유포된 Mallox 랜섬웨어의 일부 변종에 대한 복호화 도구가 개발되었다.

이러한 사건들의 발생으로 보아서는 랜섬웨어 위협이 감소되었다고 판단할 수 있는데, 오히려 다크웹 포럼에서는 계열사 모집에 대한 광고가 급증하고 있다. 즉, 이 빈자리는 소규모 RaaS 그룹들이 채우고 있다는 것이다. 특히 Medusa 그룹의 경우는 계열사 모집 공고에서 계열사에게 지불하는 대금을 70~90% 상당으로 상향할 것이며 프리미엄 멤버십 제도를 운영하는 등 기존 RaaS 그룹들과 협력하는 것 이상으로 매력적인 선택지를 제공해 주고 있다.

RansomHub 그룹은 BlackCat(Alphv)으로 인해 깨진 RaaS 생태계의 신뢰를 회복하기 위해 계열사가 몸값을 직접 갈취한 뒤 일부 대금만 운영 측에 전달하는 방식으로 운영하고 동시에 여러 RaaS 그룹의 계열사로 활동할 수 있도록 룰을 수립하여 계열사들의 불안감을 잠재우겠다고 선언했다. Cloak 랜섬웨어 그룹 역시 85%의 대금을 계열사에게 제공하고, 계열사로 활동하기 위한 계약금을 지불하지 않고 인터뷰 과정만 거쳐서 계열사를 모집하고 있다.

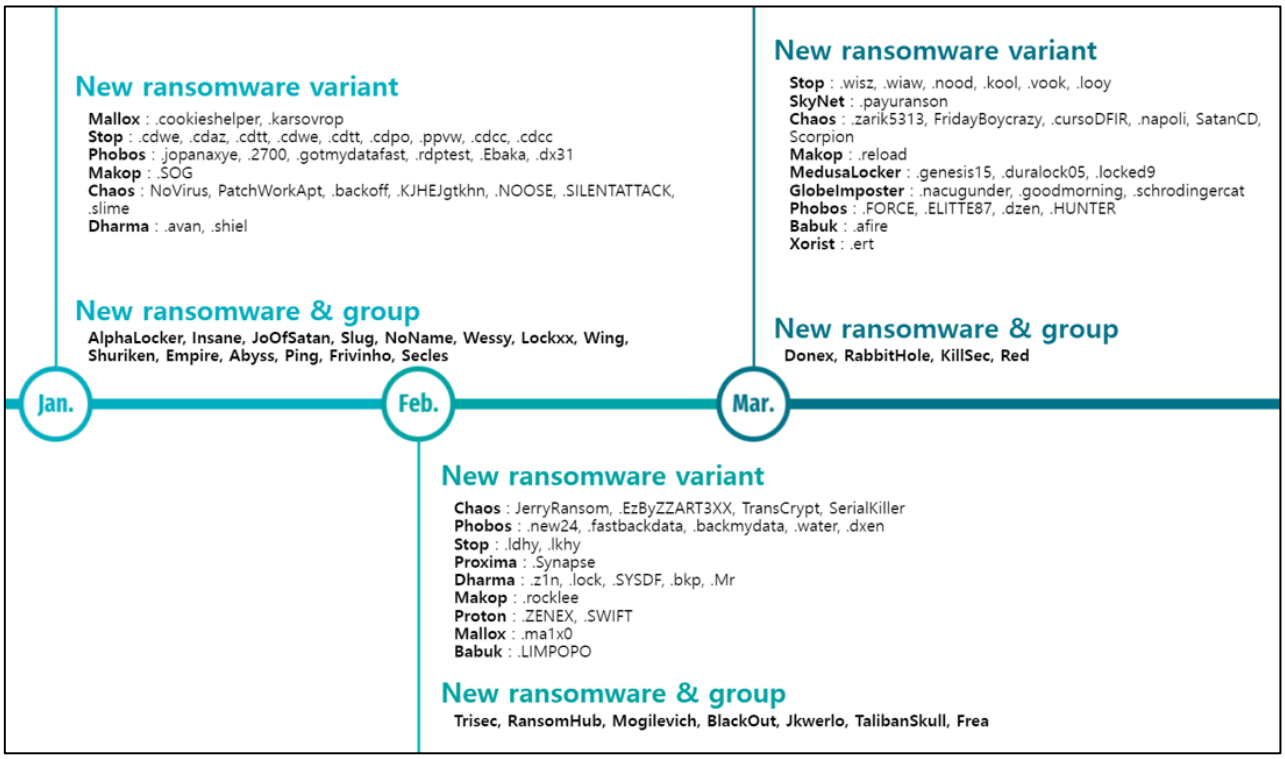
이렇게 대형 랜섬웨어 그룹이 위기를 겪는 사이 이탈되는 인력들을 자신들의 조직으로 끌어들이기 위한 소규모 RaaS 그룹들의 움직임은 한동안 지속될 것으로 보인다. 즉, 기존에 활동하던 랜섬웨어 공격자들이 다른 그룹으로 이동한다는 뜻이므로 랜섬웨어로 인한 실질적 위협이 감소되었다고 보기보다는 RaaS 생태계에 변화가 이루어지고 있다고 볼 수 있다.

[13] Exit Scam : 대금을 지불하지 않고 사업을 중단한 뒤 잠적하는 사기 행위

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

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

3. 신규 랜섬웨어 및 그룹 활동



[신규/변종 랜섬웨어]

1분기에는 11개의 신규 랜섬웨어 그룹이 발견되었다. AlphaLocker 그룹은 현재까지 9개의 조직에 대한 공격 사실을 주장했으며, 이미 8개의 조직에 대한 데이터를 유출시킨 상태이다. Insane과 JoOfSatan, Slug 그룹은 다크웹 유출 사이트를 개설한지 얼마 되지 않았으나 현재는 사이트에 접속이 되지 않는 상태이다. Donex 그룹은 DarkRace 계열의 랜섬웨어를 사용하고 있으며, 현재까지 5개의 조직에 대한 데이터를 유출시킨 상황이다. RabbitHole 그룹은 다크웹 유출 사이트를 개설만 해 놓은 상태이며, BlackOut 그룹의 경우에는 캐나다의 제조업체와 프랑스의 한 종합병원에 대해 탈취한 데이터를 자신들이 운영하는 다크웹 유출 사이트에 게시해 놓았다. 아래는 주요 신규 랜섬웨어 그룹에 대한 설명이다.

- **NoName**

  NoName 그룹의 다크웹 유출 사이트가 LockBit의 유출 사이트와 유사한 포맷을 사용하고 있어 두 그룹 간 연관성이 의심되고 있다. 특히, NoName 그룹에 의해 유출된 회사들이 2023년 LockBit의 피해 조직과 일치하며, 랜섬노트의 형식까지 매우 비슷한 것으로 밝혀져, 이는 NoName 그룹이 LockBit을 모방하여 유명세를 얻으려는 움직임으로 보인다. 최근 들어 NoName의 DDoS 공격 수행으로 인해 법 집행 기관이 PowerOFF 작전[16]을 펼쳐 클리어 웹[17] 사이트가 압수된 것으로 확인되었다.

- **Trisec**

  Trisec 그룹은 피해자에게 몸값을 직접 제시하던 여타 랜섬웨어 그룹들과 다르게 피해자가 최초 몸값을 제안하도록 하는 방식을 사용하고 있다. 또한 이들은 러시아나 중국이 아닌 튀니지 기반의 그룹으로 추정되는데, Trisec이 운영 중인 텔레그램

[16] PowerOFF 작전 : DDoS 공격 서비스 인프라를 폐쇄하기 위해 국제 수사 기관 연합이 펼치는 작전

[17] 클리어 웹 : 일반적인 검색 엔진을 통해 접근이 가능한 웹 사이트

채널과 다크웹 유출 사이트에서는 튀니지 국기와 찬양하는 문구가 기재되어 있으며 포럼에서 튀니지 출신의 공격자를 모집한다는 글을 게시하는 등의 행보를 보이고 있기 때문이다. 현재는 다크웹 유출 사이트가 폐쇄된 상태이다.

- **RansomHub**

RansomHub 그룹이 사용하는 랜섬웨어는 Go언어[18] 기반의 랜섬웨어로, 쿠바, 북한, 중국, 루마니아, CIS 국가[19]를 제외한 대상에 대해 공격을 수행한다고 주장하며, 한번 몸값을 지불했던 조직에 대해서는 추가 공격을 진행하지 않을 것이며 이러한 규칙을 어긴 계열사에 대해서는 조치를 취할 것이라는 입장을 밝혔다. BlackCat(Alphv) 계열사 'notchy'는 공격 당시 사용했던 회사 데이터를 가지고 있어, 이를 통해 RansomHub와 협력하여 다시 한번 Change Healthcare를 공격했다고 주장하기도 했다.

- **Mogilevich**

Mogilevich는 미국의 비디오 게임 유통사이자 소프트웨어 개발사인 Epic Games에 대한 데이터와 아일랜드 외무부의 문서를 탈취했다고 주장했으나, 이에 대한 증거가 확인되지 않아 허위 주장이라는 의견이 분분했으며, 결국 공격 그룹이 아닌 사기 조직임을 시인하며 한화 약 1억 6천만 원에 달하는 수익을 공개한 후 잠적했다.

- **KillSec**

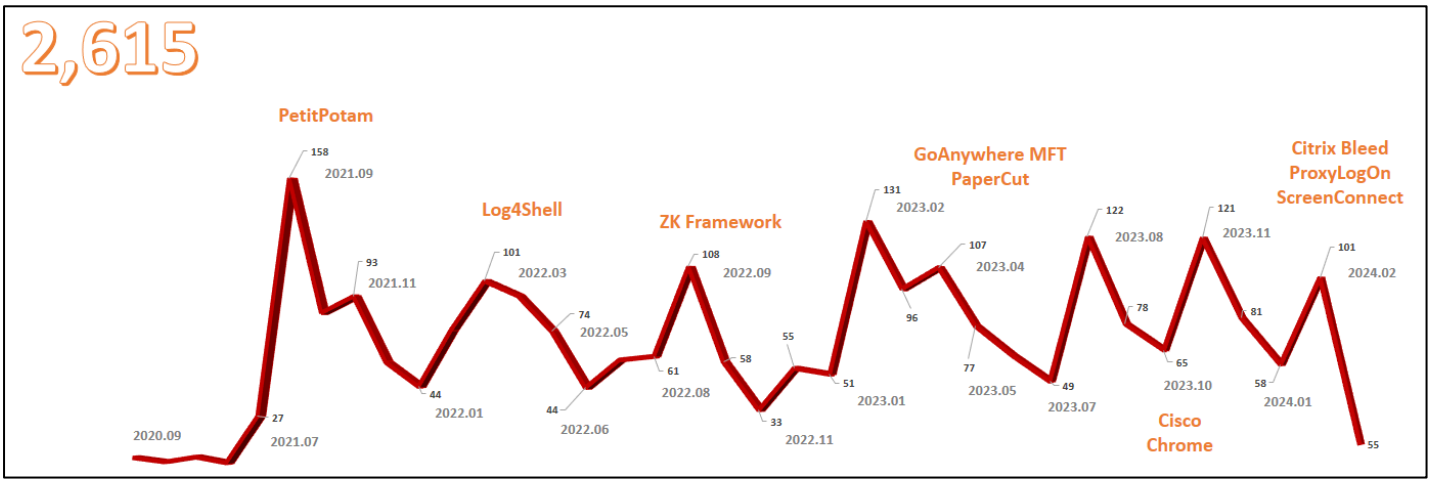
2023년부터 활동을 개시한 그룹으로, 같은 해 10월 24일 텔레그램 채널을 개설하여 활동을 이어 나가던 중 11월 13일 텔레그램에 게시한 루마니아 경찰 조직의 200,000건의 데이터를 게시 후 협박하여 1,500유로(한화 약 221만 원)를 갈취한 것으로 주장했지만, 진위 여부는 확인되지 않았다. 이후 3월 22일 다크웹 유출 사이트가 확인되면서 윤곽이 드러났으며, 4개 조직에 대한 유출 데이터와 함께 과거 텔레그램에서 공개한 데이터를 같이 게시하였다.

[18] Go 언어 : Google에서 생산성을 높이기 위해 개발한 오픈소스 프로그래밍 언어

[19] CIS 국가 : 소련의 해체로 독립한 국가들의 국제기구. 러시아, 몰도바, 벨라루스, 우즈베키스탄, 카자흐스탄 등이 포함됨

LockBit 그룹 상세 분석

1. LockBit 개요



[LockBit 그룹의 공격 사례]

LockBit 은 2019 년도 9 월에 ABCD 라는 이름의 랜섬웨어로 활동을 시작한 그룹이다. 이후 2020 년 1 월에 LockBit 이라는 이름을 달고 러시아어 기반 포럼에 등장하여 본격적인 랜섬웨어 활동을 개시했다. 이후 LockBit 2.0(Red), LockBit 3.0(Black), LockBit Green 을 출시하고 RaaS 활동을 점차 넓혀가며 명실상부 대형 랜섬웨어 그룹으로 자리매김했다. 또한, LockBit 은 이력서를 위장한 피싱 공격, 1-day 취약점을 악용한 공격을 과거부터 꾸준히 사용하며 대규모 공격을 수행해왔다.

2022 년 6 월에는 LockBit 3.0 에 대한 빌더[20]가 유출되어 Bloody 그룹이나 Synapse, Buhti, Darkrace 등의 다양한 랜섬웨어 그룹들이 유출된 빌더를 차용하여 다양한 변종을 만들어내 현재까지도 꾸준히 악용되고 있는 실정이다.

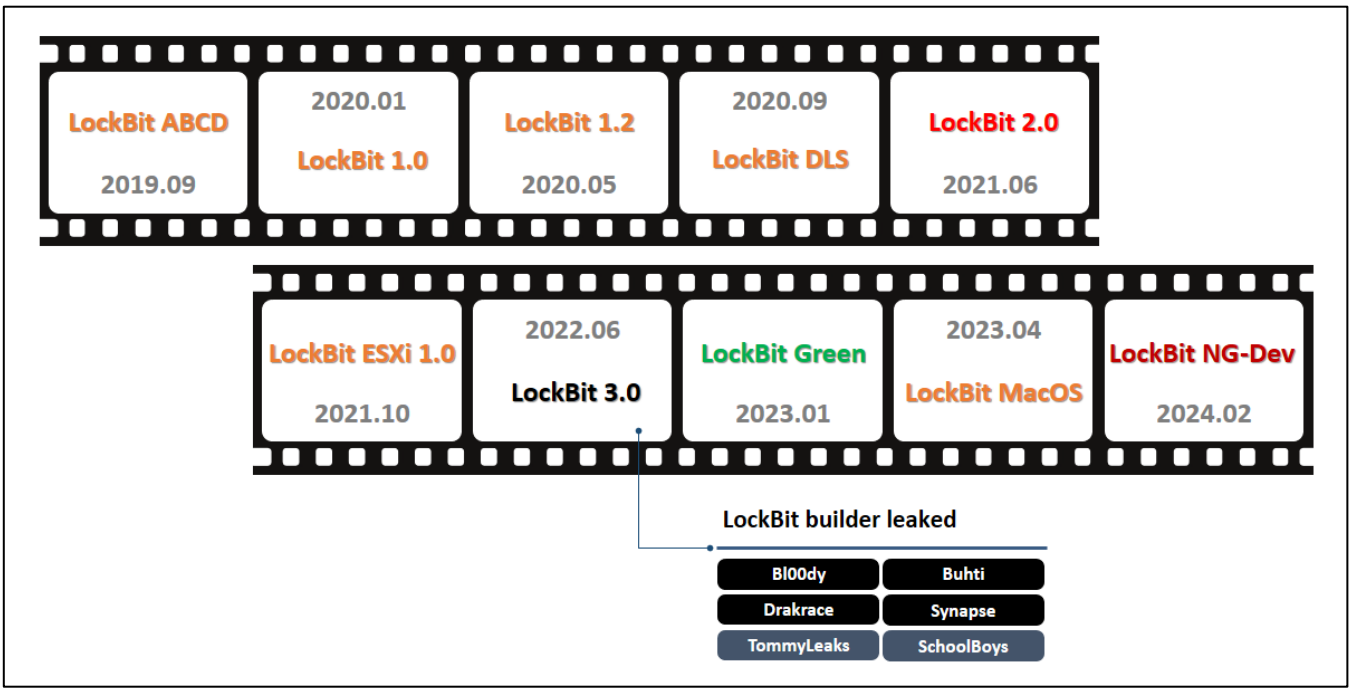
LockBit 의 멤버는 운영자로 추정되는 3 명 이상의 인물이 사용하는 "LockBit"과 "LockBitSupp" 계정 외에 알려진 바가 없었는데 얼마 전 Cronos 작전을 통해 큰 타격을 입었을 때, 활동 중인 계열사 목록이 법 집행 기관에 의해 유출되었다. 해당 목록에 따르면 약 200 개의 계열사가 존재하며, 이는 2 년간 모집한 계열사라고 밝혔지만, LockBit 의 운영자에 따르면 확보한 200 여 개의 계열사는 실제 신원과 연관이 없음을 밝히며 완전히 인프라를 파괴시키지 못했다고 전했다. 그럼에도 불구하고 과거 LockBit 계열사로 활동한 러시아계 캐나다인이 4 년형의 징역형을 선고받았고, 한화 약 11 억 4 천만 원에 상당하는 벌금을 지불하라는 판결이 내려져 LockBit 그룹과의 공방은 계속되고 있다.

LockBit 은 그간 세계적으로 약 2,610 여 상당의 조직에 대해 공격을 수행했으며 범죄 수익으로 한화 약 2,000 억 원 상당을 갈취해 상당한 영향력을 행사하고 있는 그룹인 만큼 국내에서도 LockBit 랜섬웨어가 지속적으로 유포되고 있다. 특히나 이력서, 입사지원서 등을 위장하여 피싱 메일로 유포되므로 수상한 메일의 첨부파일을 다운로드하는 행위는 삼가야 한다는 보안 인식 제고가 필요하다.

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

2. LockBit 타임라인

✓ 버전 히스토리



[LockBit 랜섬웨어 버전 히스토리]

- **LockBit ABCD**

  LockBit ABCD 버전은 2019년 9월에 발견되었으며, 생성되는 랜섬노트에 따라 3가지 버전이 존재한다. 랜섬노트에 공격자 메일 주소 기재, 다크웹 협상 사이트 주소 기재 그리고 Base64[21]로 인코딩된 Personal ID만 기재되어 있는 불안정한 버전이 발견되었다. 초기 버전인 만큼 전략적 선택을 위한 여러 버전이 존재하는 것으로 보인다.

- **LockBit 1.0**

  LockBit 1.0 버전은 기존 ABCD 랜섬웨어와 코드 유사도가 74% 이상이며, 2020년 1월에 발견되었다. 같은 달 17일, LockBit은 XSS 러시아 해킹 포럼에 RaaS인 LockBit 랜섬웨어는 여러 가지 기능을 제공하고 글을 쓴 시점까지 한 번도 복호화 되지 않았다고 주장했다. 또한 CIS 국가에 대한 공격을 금하며, 랜섬웨어 대여 조건을 개별적으로 협상하고, 공격 경험자를 우대한다는 사항을 제시했다. RaaS란 Ransomware-as-a-Serivce의 약자로, 랜섬웨어 운영자가 금전을 대가로 계열사가 공격에 사용할 수 있도록 랜섬웨어를 대여해 주는 사이버 범죄 비즈니스 모델을 지칭한다.

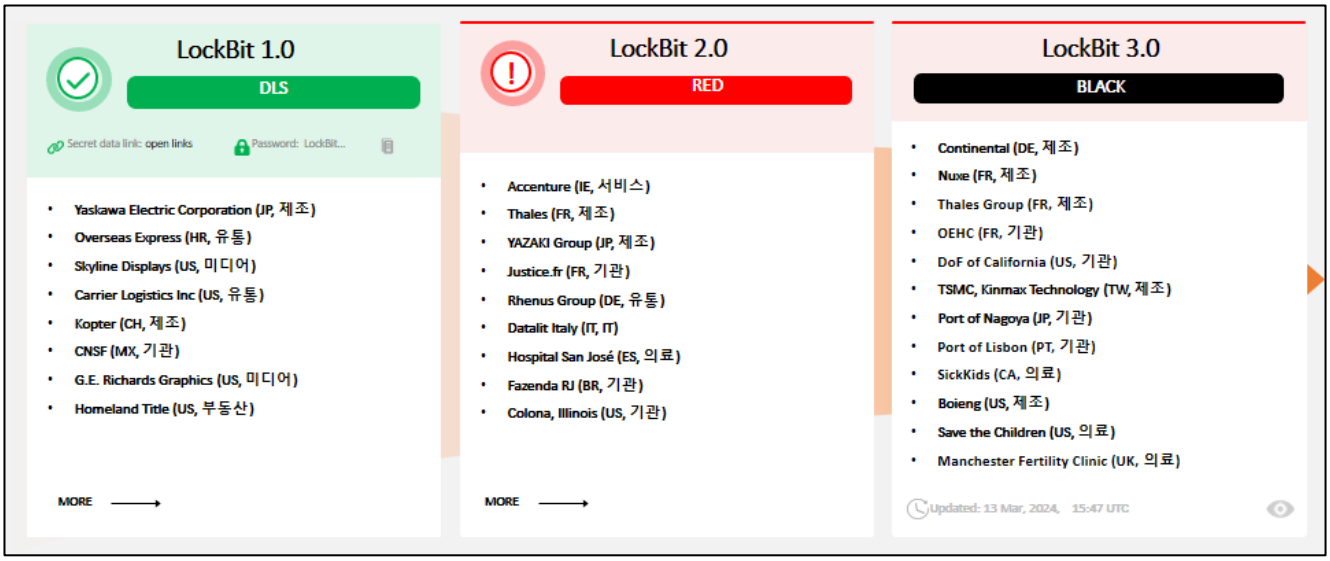
- **LockBit 1.2**

  LockBit 1.2 버전은 2020년 5월에 발견되었으며, 이전 버전과 크게 다른 부분은 랜섬노트의 내용이 변경된 것과 hta 랜섬노트 생성 및 출력 기능을 추가하였다는 것이다. 또한 해당 시기부터 다크웹 유출 사이트를 운영하기 시작했다.

[21] Base64 : 바이너리 데이터를 ASCII 문자열로 변환하는 인코딩 방식

- **LockBit DLS(Dedicated/Data Leak Site)**

LockBit은 샘플의 버전이 갱신됨에 따라 다크웹 유출 사이트 또한 리뉴얼 해왔는데, LockBit 버전 1.0의 다크웹 유출 사이트는 2020년 9월 16일에 발견되었다. 이들은 이중 협박 방식을 적용하기 위해 피해자들의 데이터를 게시할 유출 사이트를 다크웹에 개설하였으나, 초반에는 몇 달간 자체 유출 사이트를 잘 사용하지 않고 Maze 랜섬웨어 그룹의 유출 사이트에 함께 게시하며 협력하는 모습을 보여줬다. 이후, 버전 2.0의 리뉴얼된 유출 사이트는 2021년 7월 초에 발견되었고, 현재까지 사용되고 있는 버전 3.0의 유출 사이트는 2022년 6월 17일에 발견되었다.



[데이터 유출 사이트 변화와 피해 사례]

- **LockBit 2.0(Red)**

LockBit 2.0은 1.0 버전과의 코드가 유사하지 않으며 2021년 6월에 발견되었다. 여러 시행착오를 거친 끝에 어느 정도 모양새를 갖춰 현재의 LockBit과 흡사한 완성도를 보이는 버전이라고 할 수 있다. 또한 맞춤형 정보 탈취 도구 StealBit 사용과 더불어 내부 전파를 위한 PsExec[22] 사용을 통해 더욱 치밀한 공격 수법을 수립했다. LockBit은 2.0 버전에서 본격적으로 빠르고 효과적인 암호화를 수행하기 위해 멀티 스레드[23] 방식, I/O Completion Port,[24] 부분 암호화 방식을 적용하였고,

[22] PsExec : 네트워크 상의 다른 컴퓨터에서 프로그램을 원격으로 실행할 수 있게 하는 유틸리티

[23] 멀티 스레드 : 여러 작업을 동시에 처리하기 위해 하나의 프로그램 내에서 여러 스레드를 생성하여 실행하는 기술

[24] I/O Completion Port : 효율적인 비동기 입출력 처리를 위한 시스템 API

암호화 알고리즘도 기존의 AES[25]+RSA[26] 조합에서 AES + Curve-25519[27]/Xsalsa20-Poly1305[28] 조합으로 변경하였다. 즉, 암호화 키를 알아내지 못하게 하면서도 큰 크기의 파일에 대해서도 빠르게 암호화를 할 수 있게 되었다는 것이다.

랜섬웨어	암호화 속도	100GB 파일을 암호화 하는데 걸리는 시간
LockBit 2.0	373 MB/s	4분 28초
LockBit 1.0	266 MB/s	6분 16초
Cuba	185 MB/s	9분
BlackMatter	185 MB/s	9분
Babuk	166 MB/s	10분
Sodinokibi	151 MB/s	11분
RagnarLocker	151 MB/s	11분

[LockBit 랜섬웨어 암호화 속도 비교, 출처 : GRIDINSOFT]

- **LockBit ESXi 1.0**

LockBit은 다양한 플랫폼을 타깃 하는 것을 목표로 Linux 및 ESXi[29] 환경을 감염 시킬 수 있는 버전의 랜섬웨어를 제작했다. 기본적인 사항은 LockBit 2.0과 동일하지만, 이때부터 실행 인자에 따라 전체 암호화와 부분 암호화를 결정하는 방식을 채택했다. 이러한 실행 인자 기반 암호화 방식의 채택은 기업 서버의 상당수가 Linux와 ESXi 기반이라는 점을 통해 각 조직의 상황에 맞게 암호화를 수행하기 위함으로 보인다. ESXi 기능을 통해 관리하는 VM(Vritual Machine)[30]도 모두 암호화가 가능하여 감염되었을 경우 큰 피해가 야기되므로 주의가 필요하다.

- **LockBit 3.0(Black)**

LockBit 3.0은 2022년 6월에 공개된 버전으로, LockBit Black 버전으로 식별되기도 하는데, 이는 BlackMatter 랜섬웨어의 코드와 약 60% 유사하며 그룹 간에도 연관성이 의심되기 때문이다. BlackMatter의 경우 소스 코드를 판매한 흔적은 찾아볼 수 없는데, LockBit 3.0은 이와 상당히 높은 코드 유사도 및 흐름을 보여준 것이다. 더불어 BlackMatter 개발자가 LockBit 3.0 개발에 참여한 점이 밝혀지고, BlackMatter의 활동 중단 이후 피해자들을 LockBit의 협상 사이트로 안내하여

---

[25] AES : 대칭 키 암호화 방식의 일종으로 고정된 크기의 데이터 블록을 암호화, 랜섬웨어에서는 주로 파일을 암호화 시킬 때 사용하는 알고리즘

[26] RSA : 공개 키 암호화 방식 중 하나로, 랜섬웨어에서는 주로 파일을 암호화 시킨 키를 보호할 때 사용하는 알고리즘

[27] Curve-25519 : 공개 키 암호화 알고리즘 중 하나로, 빠르고 안전하며 쉽게 구현할 수 있는 타원 곡선을 사용하여 키 교환 수행. 랜섬웨어에서는 주로 파일을 암호화 시킨 키를 보호할 때 사용하는 알고리즘

[28] Xsalsa20-Poly1305 : 고성능 스트림 암호화(Xsalsa20)와 무결성 보장을 위한 메시지 인증 코드 생성(Poly1305)을 결합한 암호화 기법. 랜섬웨어에서는 주로 파일을 암호화 시킬 때 사용하는 알고리즘

[29] ESXi : 물리적 하드웨어 위에서 여러 가상 머신을 구동할 수 있게 해주는 하이퍼바이저

[30] VM : 실제 물리적 하드웨어를 사용하지 않고 소프트웨어로 구현된 가상 머신

LockBit Black이라는 이름이 붙여졌다.

LockBit 3.0이 발견되고 3개월이 지난 2022년 9월, LockBit 3.0 빌더가 유출되었다. "LockBitSupp"는 내부 개발자가 LockBit 운영 측의 태도에 불만을 품고 보복 차원에서 LockBit 3.0의 빌더를 유출했다고 밝혔다. 과거 Conti, Babuk 소스 코드가 유출되어 수많은 변종이 생성된 것과 같이 유출된 LockBit 3.0 빌더를 이용해 Bloody, Buhti, Darkrace 등의 그룹이 파생되었다. Bloody 그룹은 PaperCut, PrintNightmare, ScreenConnect 취약점을 악용하여 현재까지도 활동하고 있는 그룹이다.

- **LockBit Green**

2023년 1월, LockBit은 유출된 Conti 랜섬웨어의 소스 코드를 차용하여 LockBit Green을 출시했다. LockBit Green과 Conti v3 사이의 소스 코드 유사도는 약 89%로, Conti 랜섬웨어 코드를 그대로 사용하되 설정과 디자인만 일부 개량한 버전이다. 실제 공격에 사용되는 사례가 일부 확인되었지만 주요 서비스로 활용하기보단 과거 Conti 계열사들이 선호하여 출시된 것으로 확인되었다.

- **LockBit MacOS**

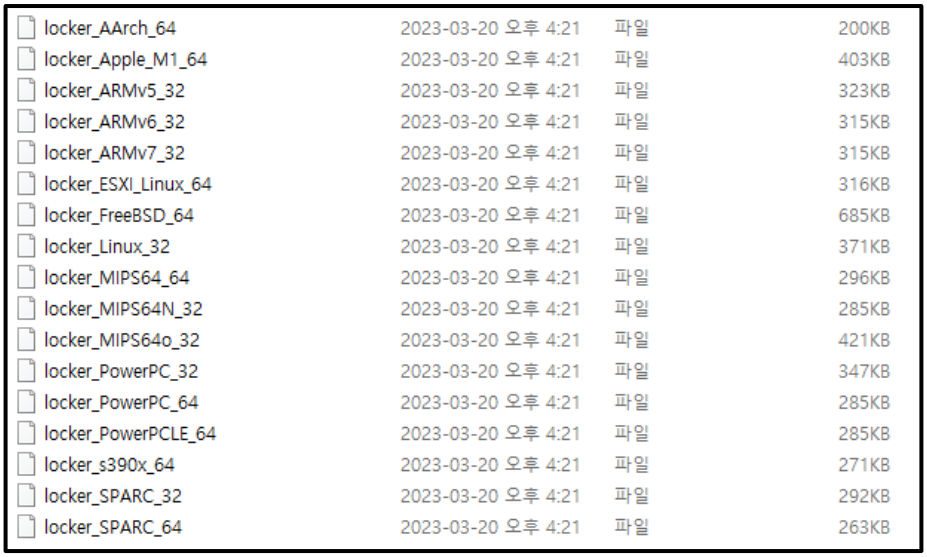
LockBit 3.0과 Green을 통한 활발한 활동을 보이던 LockBit은 MacOS에도 손을 뻗으려 했던 모습이 포착되었다. 2022년 11월에 제작되었던 것으로 보이는 LockBit MacOS 변종은 ESXi 버전의 변종과 상당히 코드가 유사한데, 내부적으로 Windows OS에 관련된 문자열이 나열되어 있고, 서명이 유효하지 않아 실행이 되지 않고, 만약 실행된다 하더라도 BOF(Buffer Over Flow)[31]로 인해 충돌이 발생하기 때문에 테스트 버전으로 추정된다. ARM[32], FreeBSD[33], MIPS[34] 등 다양한 플랫폼을 타깃으로 한 변종도 함께 발견되어 랜섬웨어 생태계에서 LockBit의 입지를 더욱 공고히 하려는 의도가 엿보인다.

[31] BOF : 프로그램이 데이터를 버퍼에 저장할 때 할당된 메모리를 초과하여 데이터를 쓰는 오류로 이로 인해 보안 취약점이 발생할 수 있음

[32] ARM : 저전력 소비에 최적화된 프로세서 아키텍처로 주로 모바일 장치와 임베디드 시스템에서 사용

[33] FreeBSD : 유닉스 계열의 오픈소스 운영 체제 중 하나

[34] MIPS : RISC(Reduced Instruction Set Computing) 기반의 프로세서 아키텍처



locker_AArch_64	2023-03-20 오후 4:21	파일	200KB
locker_Apple_M1_64	2023-03-20 오후 4:21	파일	403KB
locker_ARMv5_32	2023-03-20 오후 4:21	파일	323KB
locker_ARMv6_32	2023-03-20 오후 4:21	파일	315KB
locker_ARMv7_32	2023-03-20 오후 4:21	파일	315KB
locker_ESXI_Linux_64	2023-03-20 오후 4:21	파일	316KB
locker_FreeBSD_64	2023-03-20 오후 4:21	파일	685KB
locker_Linux_32	2023-03-20 오후 4:21	파일	371KB
locker_MIPS64_64	2023-03-20 오후 4:21	파일	296KB
locker_MIPS64N_32	2023-03-20 오후 4:21	파일	285KB
locker_MIPS64o_32	2023-03-20 오후 4:21	파일	421KB
locker_PowerPC_32	2023-03-20 오후 4:21	파일	347KB
locker_PowerPC_64	2023-03-20 오후 4:21	파일	285KB
locker_PowerPCLE_64	2023-03-20 오후 4:21	파일	285KB
locker_s390x_64	2023-03-20 오후 4:21	파일	271KB
locker_SPARC_32	2023-03-20 오후 4:21	파일	292KB
locker_SPARC_64	2023-03-20 오후 4:21	파일	263KB

[다양한 플랫폼을 타깃한 LockBit 랜섬웨어]

- **LockBit NG-Dev(Next Generation-Development)**

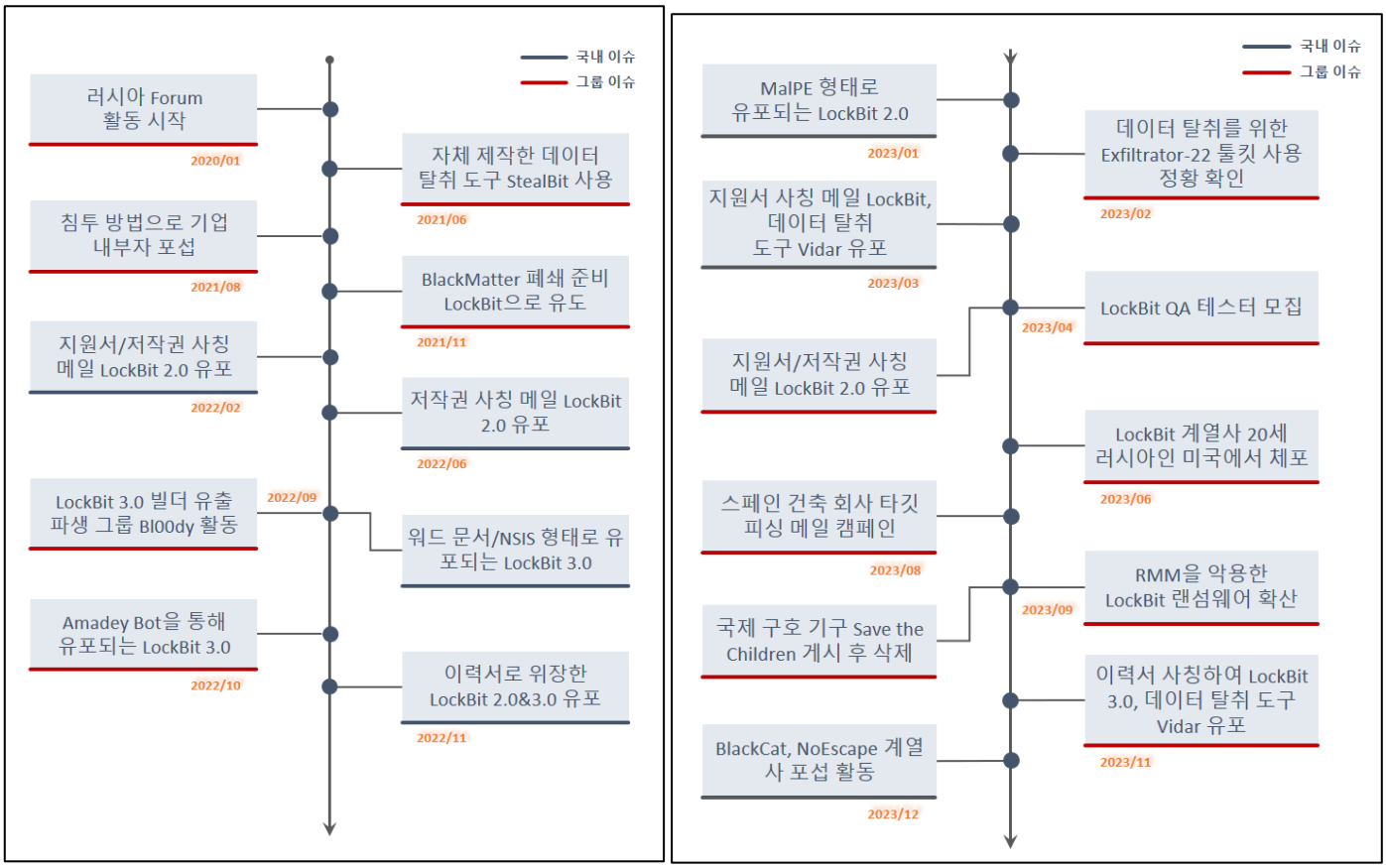
  2024년 2월 19일, FBI를 비롯한 국제 수사가 이루어진 끝에 LockBit은 결국 무력화된 듯했다. 피해 조직의 목록이 즐비하던 다크웹 유출 사이트의 모습이 수사 기관에 의해 압수되었다는 내용의 페이지로 변경된 것이다. CVE-2023-3824[35] 취약점으로 인해 내부 시스템이 압수되었으며 이를 통해 알려진 것이 NG-Dev 버전이다. 이전 버전의 LockBit과는 사뭇 다른 점들을 찾을 수 있었는데, 닷넷(.NET)[36]으로 개발되었고, Configuration[37]에 기존에는 없었던 기능과 제외된 기능이 존재했다. 물론 LockBit 측에서 정식으로 배포하지 않았기에 제외된 기능들이 추가될 가능성이 존재하지만 3.0 버전과 비교했을 때 기능이 줄어든 것을 확인할 수 있었다. 2월 24일, LockBit이 다시 제자리를 찾아 활동을 개시해 앞으로 NG-Dev를 보완하여 공격에 사용한다면 LockBit 3.0 이후 랜섬웨어 시장에 새로운 전환점이 될 것으로 보인다.

[35] CVE-2023-3824 : PHP의 확장 기능에서 특정 함수의 부적절한 버퍼 처리로 버퍼 오버플로가 발생하여 원격 코드 실행이 가능한 취약점

[36] 닷넷(.NET) : MS에서 개발한 Windows 프로그램 개발 및 실행 환경

[37] Configuration : 랜섬웨어 실행 시 설정 값을 담고 있는 파일 혹은 데이터

✓ 주요 사건



[LockBit 그룹의 주요 사건 1]

LockBit의 RaaS로써의 본격적인 활동 시작은 2020년 1월 러시아 포럼에서 포착되었다. 이듬해 6월에는 맞춤형 정보 탈취 도구인 StealBit을 출시해 공격에 사용하기 시작했는데, StealBit은 Ryuk 그룹[38]의 Ryuk Stealer, BlackMatter의 ExMatter와 같이 LockBit 그룹에서 자체 제작한 맞춤형 정보 탈취 도구이다. 마찬가지로 LockBit은 2년 뒤인 2023년 2월에도 이전 계열사였던 공격자가 개발한 데이터 탈취 도구인 Exfiltrator-22를 공격에 사용한 정황이 포착되어 자체적인 인프라 구축에 꽤나 힘썼던 것으로 보인다.

비슷한 맥락에서 LockBit은 기업의 내부자를 모집하여 수수료 절감과 자체 전략 수립을 도모하기도 하였다. 랜섬웨어 공격을 위해서는 탈취한 자격 증명이 담긴 Infostealer[39] 로그를 구매하는 등의 방식을 통해 초기 침투를 수행하지만, 이 과정에서 들어가는 비용과 인적 자원을 줄이기 위해 LockBit은 초기 침투 과정부터 자체적으로 수행하기로 한 것이다. 또한 랜섬웨어 그룹 최초로 자체 QA 테스트 및 버그 바운티[40]를 진행하며 자체 기술력을 보강하는 데 심혈을 기울였다.

그러나 2023년 9월 무렵부터는 합법적인 RMM 도구를 공격에 사용하기 시작하며 이전과는 다른 움직임을 보였다. 기존의 자체 맞춤형 도구 사용이 보안 솔루션에 탐지되어 무력화되기 때문에 이를 방해하기 위해 LockBit은 LotL 공격을 수행하거나 합법적인 RMM 도구들을 피해자의 시스템에 설치하여 정보 유출, 네트워크 확산 등에 악용하기 시작한 것이다.

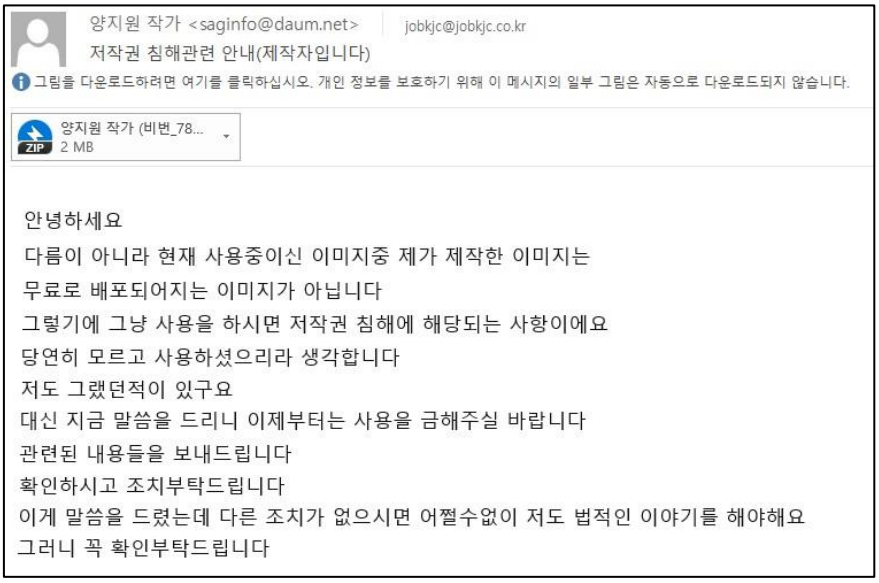
[38] Ryuk 그룹 : 서비스형 랜섬웨어를 제공하는 그룹으로 주로 피싱 메일이나 뱅킹 악성코드를 통해 유포됨(현재는 활동 종료)

[39] InfoStealer : 자격증명 혹은 가상화폐 지갑 주소 등을 탈취하는 정보 탈취형 악성코드

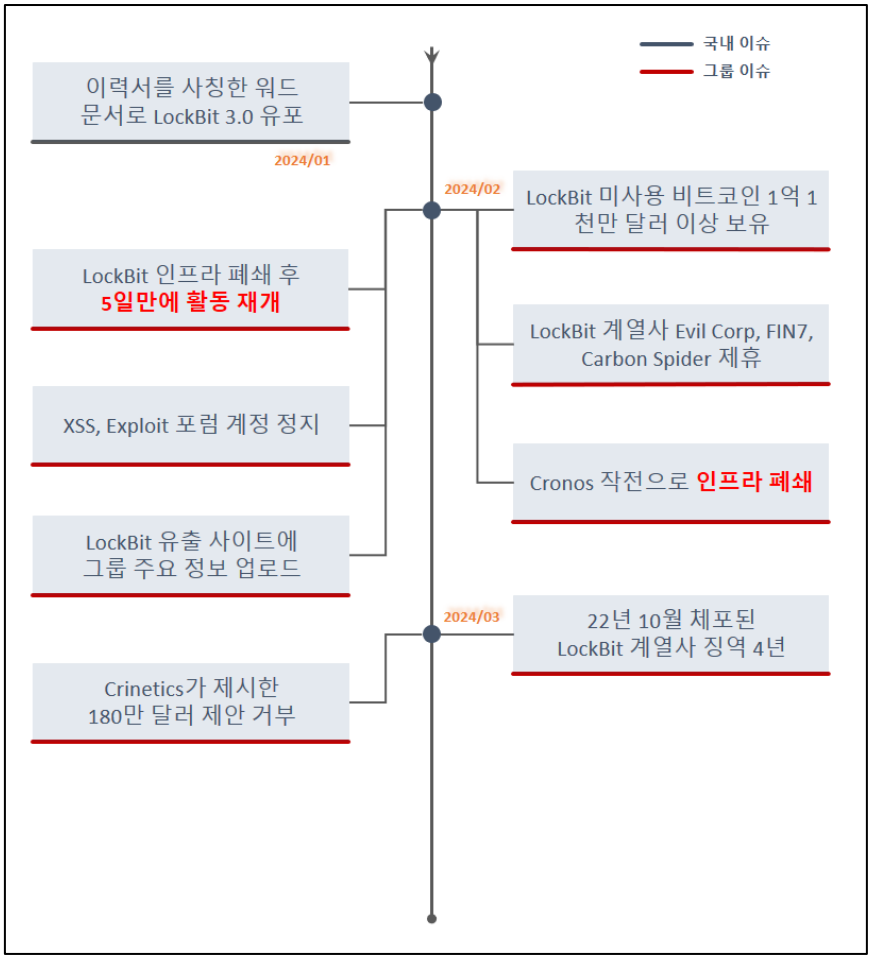
[40] 버그 바운티 : 기업의 소프트웨어나 시스템의 보안 취약점을 찾는 것에 대해 보상을 지급하는 제도

이처럼 다양한 전략을 수립하여 활동해온 LockBit도 몸값 지불 비율 감소를 피해 갈 수 없었다. 이를 극복하기 위해 LockBit은 비영리 단체나 병원 같은 민감 조직에 대한 공격을 금한다는 규칙에서 벗어나 공격 대상을 넓힌 것이다. 일례로 LockBit의 특정 계열사가 소아과 병원인 "SickKids Children"을 공격한 사건으로 논란이 일자, 이들을 제명하겠다고 밝혔으나 몇 개월 지나지 않아 어린이 보호 단체인 "Save the Children"을 공격한 것이다. 소아과 병원 공격 건으로 사회적 비난을 받고 다크웹에서 게시글을 삭제했음에도 불구하고 "Save the Children"에 이어 "Capital Health"라는 의료기관을 공격하여 7TB의 데이터를 빌미로 금전을 요구한 것으로 보아 이러한 일련의 행보가 우연이 아닌 계획된 전략임을 시사한다.

한편, LockBit 랜섬웨어는 국내에서도 꾸준히 유포되고 있다. 주로 저작권 침해, 입사 지원서 등 문서 파일로 가장한 첨부파일이 담긴 악성 메일로 유포되고 있다. 스팸 메일로 분류되거나 보안 솔루션에 탐지되는 것을 회피하기 위해 비밀번호가 설정된 압축파일을 첨부하는 치밀함을 보이기도 했다.


양지원 작가 <saginfo@daum.net> jobkjc@jobkjc.co.kr
저작권 침해관련 안내(제작자입니다)
그림을 다운로드하려면 여기를 클릭하십시오. 개인 정보를 보호하기 위해 이 메시지의 일부 그림은 자동으로 다운로드되지 않습니다.
양지원 작가 (비번_78...
2 MB
ZIP
안녕하세요
다름이 아니라 현재 사용중이신 이미지중 제가 제작한 이미지는
무료로 배포되어지는 이미지가 아닙니다
그렇기에 그냥 사용을 하시면 저작권 침해에 해당되는 사항이에요
당연히 모르고 사용하셨으리라 생각합니다
저도 그랬던적이 있구요
대신 지금 말씀을 드리니 이제부터는 사용을 금해주실 바랍니다
관련된 내용들을 보내드립니다
확인하시고 조치부탁드립니다
이게 말씀을 드렸는데 다른 조치가 없으시면 어쩔수없이 저도 법적인 이야기를 해야해요
그러니 꼭 확인부탁드립니다

[LockBit 랜섬웨어가 첨부된 악성 이메일]

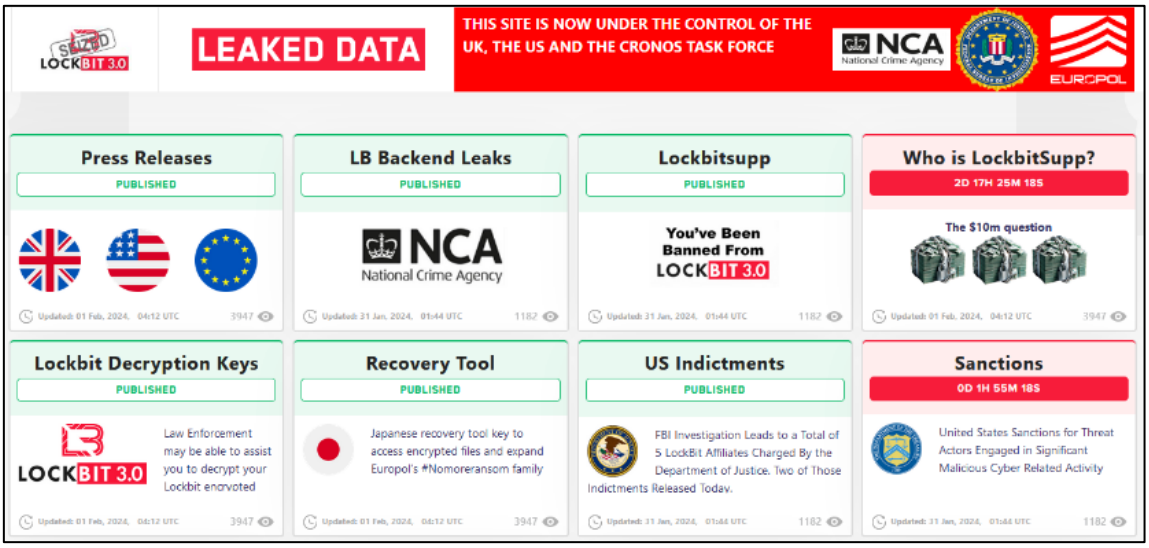


[LockBit 그룹의 주요 사건 2]

현재는 운영 측의 Exit Scam으로 활동이 중단된 BlackCat(Alphv)은 2023년 12월, 오류로 인해 잠시 인프라가 중단된 적이 있는데 운영상의 문제가 발생하여 운영이 중단되는 듯한 모습을 보이기도 했다. 또한 비슷한 시기에 NoEscape 랜섬웨어 그룹은 운영 측의 Exit Scam으로 인해 계열사들이 대금을 정산 받지 못한 채로 갈 곳을 잃기도 했는데, LockBit은 이틈에 계열사를 확보하기 위해 BlackCat(Alphv)과 NoEscape의 랜섬웨어 개발자를 회유하는 글을 다크웹 포럼에 게시하여 포섭 활동을 펼쳤다.

[LockBitSupp가 게시한 다크웹 포럼 게시글]

수년간 파죽지세를 보이던 LockBit의 활동은 이처럼 영원할 것으로 보였으나 이들 역시 좁혀진 수사망을 피해 갈 수는 없었다. 2024년 2월 20일, 결국 LockBit의 인프라가 수사 기관에 의해 폐쇄된 사태가 발생한 것이다. 공격에 가담한 계열사도 연달아 체포가 되었고 LockBit의 대표에게 1,500만 달러(한화 약 200억 원)의 현상금이 붙었다. 수사 기관은 인프라 폐쇄뿐만 아니라 StealBit의 경유지 서버와 복호화 키, 새로운 버전의 랜섬웨어인 LockBit NG-Dev의 샘플 등 내부 자원을 압수 후 관련 데이터를 공개했다.



[압수된 LockBit 유출 사이트]

LockBit의 기세를 꺾은 해당 사태의 시발점은 생각보다 허무했다. LockBit 측이 내부 인프라에 패치가 되지 않은 버전의 PHP[41]를 사용하고 있어 수사 기관이 CVE-2023-3824[42]를 통해 LockBit의 시스템에 침투한 것이다. 해당 작전은 Cronos 작전으로 세간에 알려졌으며 거대 랜섬웨어 그룹인 LockBit은 결국 종말을 맞이한 듯했다. 그러나 인프라가 압수된 지 5일 만에 LockBit은 새로운 인프라를 통해 복귀했으며 한 외신과의 인터뷰에서 단지 게을러서 PHP 패치를 하지 않아 발생한 문제이며, 비즈니스

[41] PHP : 서버 측에서 실행되는 스크립트 언어

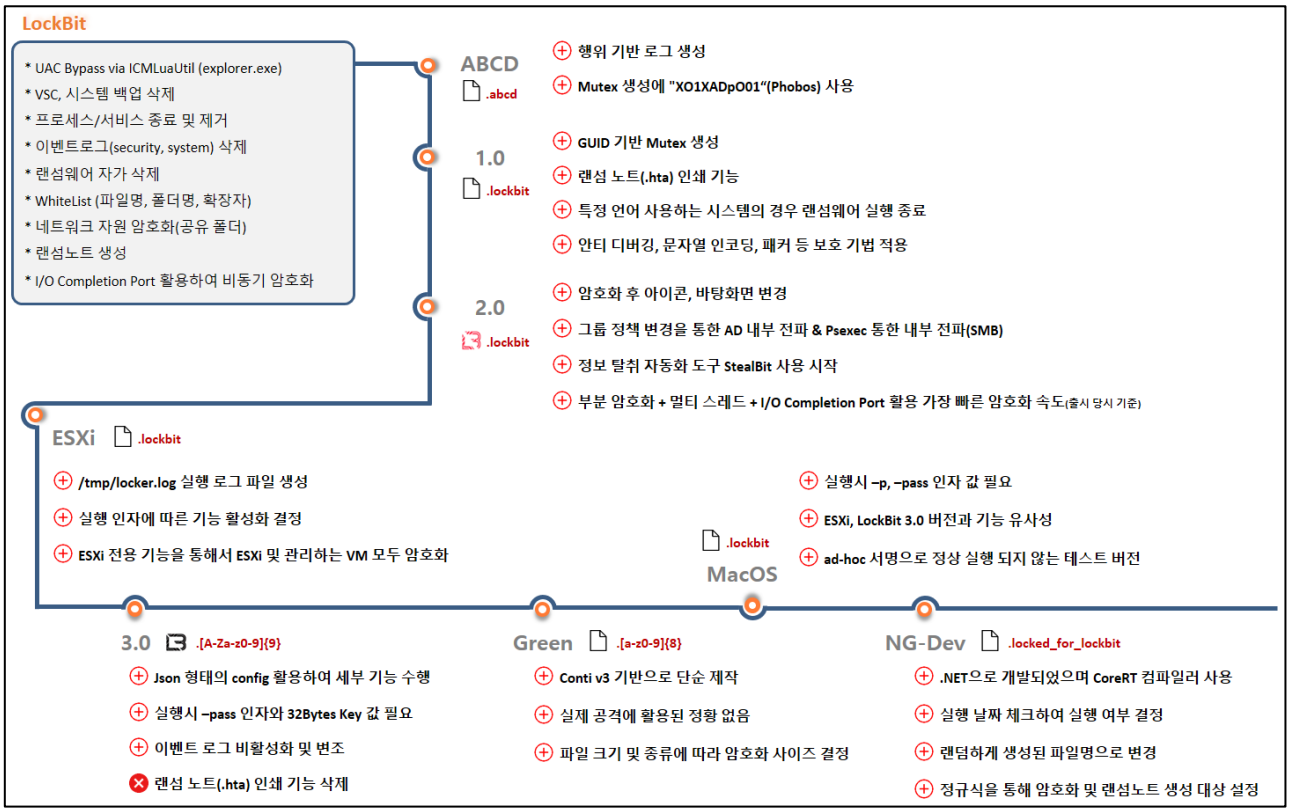
[42] CVE-2023-3824 : PHP의 Phar 아카이브 내의 파일 이름에 대한 길이 검사가 충분하지 않아 발생하는 취약점

엔 아무런 이상이 없기 때문에 앞으로도 수사 기관은 자신을 막을 수 없을 것이라는 자신감을 보이기까지 했다.

LockBit의 복귀 이후, 2022년 10월에 체포되었던 계열사 Mikhail Vasiliev(미하일 바실리예프)에게 징역 4년형과 86만 달러(한화 약 11억 6천만 원)의 배상 명령이 떨어졌지만, 70개 이상의 조직을 공격하고 다크웹 유출 사이트에 탈취한 데이터를 빌미로 협박을 지속하는 모습을 보이고 있다. 그중 제약 회사인 Crinetics는 LockBit으로부터 비밀 유지를 위반하여 400만 달러(한화 약 53억)를 지불하라고 협박당했지만 재정상의 이유로 제시한 180만 달러를 단호하게 거절하며 협상을 종료하는 등 강경한 모습을 보이기도 했다.

3. LockBit 랜섬웨어 심층 분석

✓ 버전별 특징



[LockBit 랜섬웨어 버전별 특징]

LockBit 랜섬웨어는 다양한 플랫폼을 대상으로 여러 버전이 존재하는데, 플랫폼별로 유사한 기능을 지원하거나 버전별로 공통점과 상이한 점이 존재한다. 공통적으로 UAC(User Access Control)[43] 우회와 VSC(Volume Shadow Copy)[44] 삭제, 프로세스 및 서비스 종료 등의 기능을 수행한다. LockBit 랜섬웨어의 버전 별 세부 정보는 아래와 같다.

[43] UAC : 시스템에 영향을 줄 수 있는 작업에 대한 허용 여부를 확인하는 보안 메커니즘

[44] VSC : Windows 시스템에서 파일이나 볼륨의 특정 시점의 백업 복사본을 생성하는 기능

- **ABCD**

ABCD 는 LockBit 의 전신으로, 수행하는 행위에 대한 기록을 "resultlog.reg", "resultlog.dll" 파일 생성을 통해 기록한다. 중복 실행 방지를 위해 Mutex[45] 를 생성하는데, 이때 사용하는 문자열이 "XO1XADpO01"로 Phobos 랜섬웨어에서 사용하는 Mutex 와 동일하다. 또한, "Restore-My-Files.txt" 라는 이름의 랜섬노트도 Phobos 의 것과 같은 이름을 사용하는 것으로 보아, 활동 개시 초반의 두 그룹 사이에 연관성이 있음을 시사한다.

```
strcpy(mutex_name, "XO1XADpO01");
if ( OpenMutexA(0x1F0001u, 0, mutex_name)
  || (CreateMutexA(0, 0, mutex_name),
      SetUnhandledExceptionFilter(TopLevelExceptionFilter),
      SetErrorMode(2u),
      SetPriorityClass((HANDLE)0xFFFFFFFF, 0x100u),
      !EncryptFunction()) )
{
  ExitProcess(0xFFFFFFFF);
}
```

[ABCD Mutex 생성 과정]

- **LockBit 1.0~1.3**

LockBit 1.0 대 버전부터는 Mutex 생성에 GUID 를 사용하였고, hta 형태의 랜섬노트를 생성 및 출력하는 기능이 추가되었다. 피해자의 시스템 언어를 확인하는 기능을 통해, CIS 국가에 대해서는 공격을 수행하지 않으려는 듯한 의도를 내비치기 시작했다. 이는 LockBit 의 기반이 러시아계 포럼에서 비롯된 것이라는 사실을 통해 납득 가능한 부분이라고 할 수 있다. 추가적으로 패커 및 프로텍터(UPX, ASPack, zprotect)[46] 사용을 통해 분석 방해와 탐지 우회 등의 효과를 노렸으나 그리 효과적인 선택이 아니라고 느꼈던 LockBit 은 이후부터 코드를 보호하려는 데 별다른 노력을 기울이지 않는 모습을 보이고 있다.

- **LockBit 2.0(Red)**

LockBit 2.0 에선 이전 버전과 큰 차이점이 몇 가지 존재한다. 암호화 작업에 있어서 멀티 스레드 방식을 통해 병렬로 처리해 속도 향상을 도모했다. 더불어 이전에 사용하던 AES+RSA 암호화 알고리즘 조합을 선택하지 않고, AES+Curve-25519/XSalsa20-Poly1305 조합으로 변경하여 용량이 큰 파일에 대해서도 빠른 암호화를 할 수 있게 되었다. 추가적으로 파일 크기에 따라 전체 암호화와 부분 암호화를 결정하는 기능을 추가하여 1MB 이상 크기의 파일에 대해서는 부분 암호화를 수행하게 구성해 놓은 것으로 보아 암호화 작업에 심혈을 기울인 것으로 보인다.

```
if ( _RegCreateKeyExW(0x80000001, v45, 0, 0, 0, 0xF003F, 0, &hKey, &v48) )
{
  libsodium_init(user_public_key, &user_private_key);
  curve25519_xsalsa20poly1305(user_public_key, aes_key, 0x40ui64, &lockbit_public_key);
  cleare_user_private_key(&user_private_key, 255, 32);
  goto LABEL_67;
}
```

[LockBit 2.0 암호화 알고리즘]

[45] Mutex : 여러 스레드를 실행하는 환경에서 같은 자원에 여러 스레드가 동시에 접근하지 못하도록 막아주는 기술

[46] 패커 및 프로텍터 : 랜섬웨어 소스 코드를 압축, 암호화 및 난독화하여 분석을 방해하는 소프트웨어

- **LockBit ESXi**

  ESXi 버전의 LockBit 은 2.0 버전과 기술적으로 크게 상이하지 않다. 한 가지 추가된 기능은 실행 인자에 따라 전체 암호화와 부분 암호화를 결정짓게 하는 기능이 추가된 것이다. 또한 ESXi 의 파일뿐만 아니라 관리하는 모든 VM 을 암호화 시키며 이러한 모든 행위의 과정은 /tmp/locker.log 에 기록된다.

```
randombytes_buf(v59, 32LL);
if ( curve25519_xsalsa20poly1305(v39, v59, 32LL, publickey, v20) )
  goto LABEL_19;
all_bytes_readed += a4;
if ( iMinfilesize > a4 )
  goto LABEL_19;
v23 = v49;
if ( v49 > a4 )
{
  N_bytes = encrypt_small_file(a1, a3, a4, a5);
  goto LABEL_33;
}
if ( !wholefile_flag )
{
  if ( beginfile_flag )
  {
    N_bytes = encrypt_file_first_N_bytes(a1, a3, a4);
  }
  else
  {
    spots = create_spots(a4, v53, v49);
    N_bytes = encrypt_file_by_spots(a1, a3, a4, spots, v53[0], a5, v23, v9, a8);
  }
```

[LockBit ESXi 암호화 방식]

- **LockBit 3.0(Black)**

  LockBit 3.0 은 Salsa20+RSA 조합의 암호화 알고리즘을 사용하고, 역시 파일 크기에 따라 전체 암호화와 부분 암호화 방식으로 나뉜다. 그동안 쌓인 노하우를 통해 개발한 버전으로 한동안은 세상에서 가장 빠른 암호화 속도를 가진 랜섬웨어로 알려졌다. json[47] 형태로 구성된 Configuration 을 활용하여 세부 기능을 조절할 수 있고, 일부 샘플은 –pass 인자와 함께 32Bytes 의 Key 를 입력해야 실행이 가능하다는 특징이 있다. 사후 사고 분석을 방해하기 위해 이벤트 로그를 비활성화하고 변조하는 기능이 존재하며, 유출된 3.0 버전의 빌더를 확인한 결과 30 개의 기능 정책이 존재하여 LockBit 그룹이 상당히 공을 들여 제작한 랜섬웨어라는 것을 알 수 있다.

[47] json : 데이터를 저장하거나 전송할 때 사용되는 경량의 데이터 교환 형식, 읽거나 파싱 하기 쉬운 텍스트 기반 구조

```
commandline = get_commandline();
key_flag = get_key(commandline, key);          // get -p <key> / --pass <key>
if ( key_flag )
{
  decode_1(v11, key);
  v10 = decode_2(v11, v12, v9);
  ImageBaseAddress = NtCurrentPEB()->ImageBaseAddress;
  v4 = ImageBaseAddress + ImageBaseAddress[15];
  v5 = *(v4 + 3);
  text_section = v4 + 0xF8;
```

[LockBit 3.0 –pass 인자 전달 과정]

- **LockBit Green**

LockBit Green 은 유출된 Conti 의 소스코드를 차용한 만큼 ChaCha20[48]+RSA 조합의 암호화 알고리즘에 따라 동작하며, 파일 크기에 따른 부분 암호화를 수행한다는 사실은 같지만, 가상머신 파일에 대해서는 20%만 암호화하고, 특히나 내용이 중요한 DB 파일은 전체를 암호화하는 치밀함을 보였다.

- **LockBit MacOS**

MacOS 버전의 LockBit 은 LockBit 2.0 과 LockBit ESXi 버전을 섞어놓은 듯한 모습을 보인다. 암호화 방식은 2.0 버전과 같으며 이외 인자 전달과 정책적인 부분은 ESXi 버전과 동일하고, 암호화 예외 확장자에 ".exe", ".dll"과 같이 MacOS 와는 전혀 관계없는 확장자가 포함되어 있다. 실행된다고 하더라도 BOF(Buffer Over Flow)가 발생하여 충돌이 발생한다는 점은 미완성된 테스트 코드로 분석된다.

```
fprintf(
  stderr,
  "%s\n",
  "Usage: %s [OPTION]... -i '/path/to/crypt'\n"
  "Recursively crypts files in a path or by extention.\n"
  "\n"
  "Mandatory arguments to long options are mandatory for short options too.\n"
  "  -i, --indir        path to crypt\n"
  "  -m, --minfile      minimal size of a crypted file, no less than 4096\n"
  "  -r, --remove       self remove this file after work\n"
  "  -l, --log          prints the log to the console\n"
  "  -n, --nolog        do not print the log to the file /tmp/locker.log\n"
  "  -d, --daemonize    runs a program as Unix daemon\n"
  "  -w, --wholefile    encrypts whole file\n"
  "  -b, --beginfile    encrypts first N bytes\n"
  "  -e, --extentions   encrypts files by extentions\n"
  "  -o, --nostop       prevent to stop working VM\n"
  "  -p, --wipe         wipe free space\n"
  "  -s, --spot         upper bound limitation value of spot in Mb\n"
  "\n");
```

```
Usage: %s [OPTION]... -i '/path/to/crypt'
Recursively crypts files in a path or by extention.
Mandatory arguments to long options are mandatory for short options too.
  -i, --indir        path to crypt
  -m, --minfile      minimal size of a crypted file, no less than 4096
  -r, --remove       self remove this file after work
  -l, --log          prints the log to the console
  -n, --nolog        do not print the log to the file /tmp/locker.log
  -d, --daemonize    runs a program as Unix daemon
  -w, --wholefile    encrypts whole file
  -b, --beginfile    encrypts first N bytes
  -e, --extentions   encrypts files by extentions
  -o, --nostop       prevent to stop working VM
  -t, --wipe         wipe free space
  -s, --spot         upper bound limitation value of spot in Mb
  -p, --pass         password
  -f, --full         full log
  -a, --delay        start delay in minutes
  -y, --noexts       do not search for extentions
  -v, --vmdk         search for extentions inside VMDK files
```

[인자별 수행 기능(좌: LockBit ESXi, 우: LockBit MacOS)]

- **LockBit NG-Dev(Next Generation-Development)**

NG-Dev 에서는 2.0 버전 이전처럼 암호화에 AES+RSA 조합을 사용하고 패커를 사용하는 것으로 회귀했다. 한 가지 독특한 점은 기존 랜섬웨어 사이에서는 파일 크기에 따라 부분 암호화를 수행하는 것이 정론처럼 사용되어 왔으나, NG-Dev 에서는 파일 확장자에 따라 3 가지 암호화 모드를 제공한다는 것이다. 이 방식은 Configuration 에 기입이 가능하며,

[48] ChaCha20 : 고성능 스트림 암호화 알고리즘으로 비교적 간단한 구조를 가지며 높은 보안성과 빠른 처리 속도를 가짐. 랜섬웨어에서는 주로 파일을 암호화 시키는 데 사용

실행 날짜 체크를 통한 실행 여부 결정과 자가 삭제, 파일 이름 변경 등 다양한 기능에 대해 Custom 이 가능하다. 맞춤형 랜섬웨어 느낌으로 제작된 NG-Dev 는 3.0 버전에 비해 기능은 줄었지만 추후 기능이 추가될 가능성을 배제할 수 없다.

✓ 랜섬노트 변화

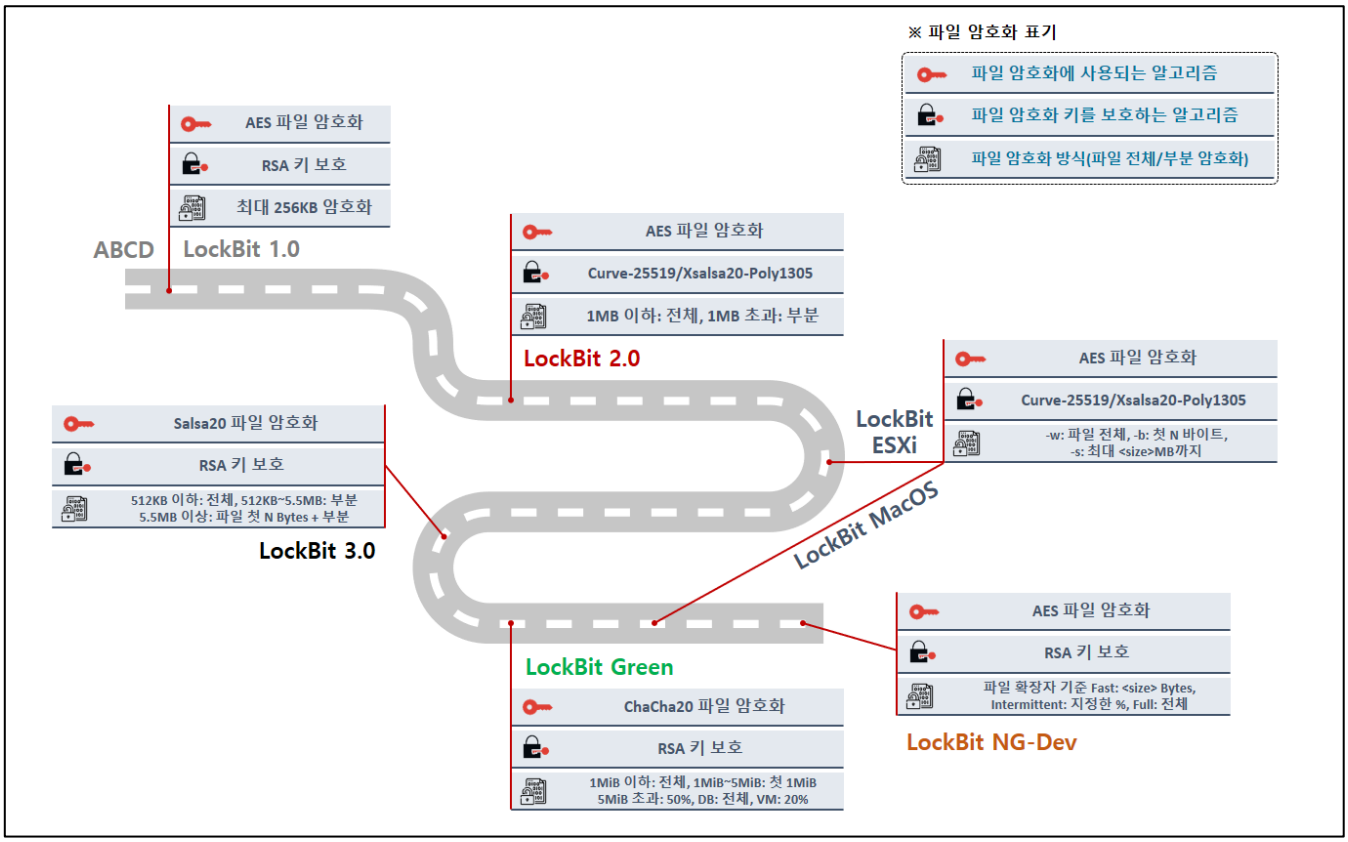
LockBit ABCD 버전과 1.0 버전의 랜섬노트는 거의 유사하나 ABCD 버전에서는 다크웹 협상 사이트로 안내하고 있고 1.0 버전은 다크웹 뿐 아니라 클리어 웹 협상 사이트도 제공하고 있어 접근성을 높이는 방식으로 더 많은 피해자가 몸값을 지불할 수 있도록 랜섬노트를 구성했다는 특징이 있다.

LockBit 2.0 버전은 다크웹 유출 사이트와 협상 사이트의 주소를 모두 기재하여 피해자에게 데이터 유출의 부담을 주고 있으며, 랜섬노트에 피해자 고유의 Decryption ID를 기재하여 협상 시 피해자를 구분하는 수단으로 사용하고 있다.

3.0과 Green 버전은 사용하는 랜섬노트가 동일하며 DDoS 공격으로 인해 특정 도메인이 사용 불가 상태가 되었을 때를 대비하여 여러 개의 도메인을 기재해 놓았고, 마찬가지로 접근성을 높이기 위해 클리어 웹 사이트 도메인도 여러 개를 기재해 놓았다.

[LockBit 랜섬노트 변화]

✓ 파일 암호화



[LockBit 버전별 파일 암호화 방식]

LockBit 랜섬웨어는 2.0 버전부터 사용하는 암호화 방식의 판도가 크게 뒤바뀌었다. LockBit은 속도 향상을 위해 2.0버전에서는 RSA를 선택한 대신, Curve-25519 알고리즘으로 키 교환을 수행한 뒤 대량의 데이터를 빠르게 암호화 시킬 수 있는 Xsalsa20, 암호화의 무결성을 보장하는 Poly1305를 통해 복호화가 어려우면서도 속도가 빠른 암호화 과정을 구현했다. 이후 LockBit ESXi, MacOS 버전에서 같은 암호화 알고리즘을 재사용했다. LockBit 3.0, NG-Dev 버전에서는 Salsa20/AES + RSA 암호화 알고리즘을 다시 사용하였지만 파일을 암호화하는 로직을 조금 더 세분화하여 속도를 향상시켰다.

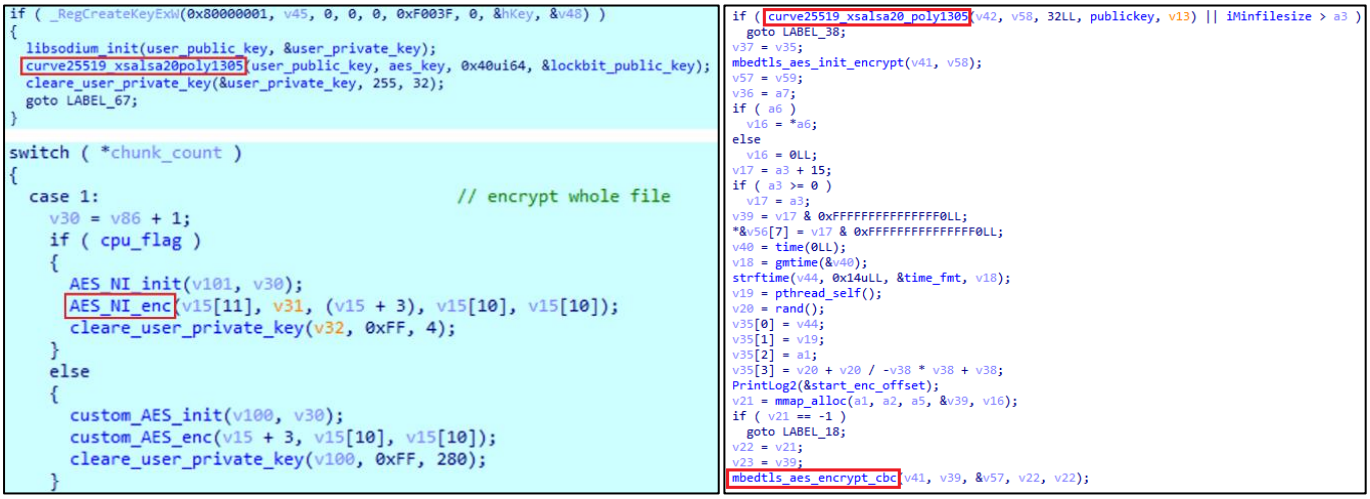
```
if ( aes_complete_flag
  || (block_size = Size,
      chunk_size_1[0] = *&chunk2[13136].InternalHigh,
      chunk_size_1[1] = *&chunk2[13137].Internal,
      memcpy(&v66, &unk_4169C8, Size),
      Offset = chunk2 + v79,
      RSA_Encyption(&RSA_PublicKey, aes_key, aes_block, 0, block_size + 32, chunk_size_1, &chunk2[29] + v79)) )
```

```
if ( _RegCreateKeyExW(0x80000001, v45, 0, 0, 0, 0xF003F, 0, &hKey, &v48) )
{
  libsodium_init(user_public_key, &user_private_key);
  curve25519_xsalsa20poly1305(user_public_key, aes_key, 0x40ui64, &lockbit_public_key);
  cleare_user_private_key(&user_private_key, 255, 32);
  goto LABEL_67;
}
```

[키 보호 알고리즘의 변화(상: LockBit ABCD~1.3, 하: LockBit 2.0)]

LockBit 2.0과 MacOS 버전은 파일 암호화에 AES 알고리즘을 사용하고, 해당 키를 보호하는 데는 Curve-25519와 Xsalsa20-Poly1305 알고리즘을 사용한다. 이처럼 암호화에 사용하는 알고리즘이 같은데, 한 가지 차이는 MacOS는 전달되는 인자에 따라 암호화 방식이 분기된다는 것이고, 2.0은 파일의 크기에 따라 분기된다.

또한 ESXi 버전과 동일하게 MacOS 버전에서는 실행 인자에 따라 전체 암호화와 부분 암호화를 결정하는데, "-w" 인자는 파일 전체를 암호화 시키고, "-b" 인자는 앞부분 N 바이트만 암호화 시키며, "-s" 인자는 함께 전달하는 사이즈만 암호화 시키는 방식으로 동작한다.

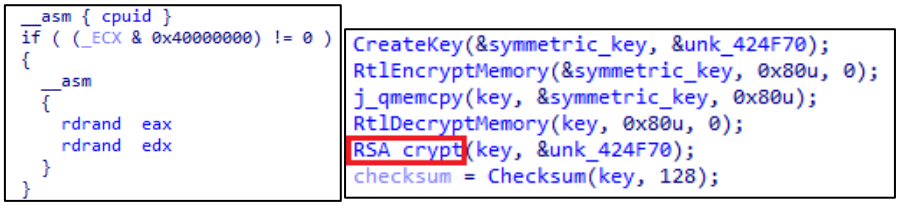


```
if ( _RegCreateKeyExW(0x80000001, v45, 0, 0, 0, 0xF003F, 0, &hKey, &v48) )
{
  libsodium_init(user_public_key, &user_private_key);
  curve25519_xsalsa20poly1305(user_public_key, aes_key, 0x40ui64, &lockbit_public_key);
  cleare_user_private_key(&user_private_key, 255, 32);
  goto LABEL_67;
}
switch ( *chunk_count )
{
  case 1:                                   // encrypt whole file
    v30 = v86 + 1;
    if ( cpu_flag )
    {
      AES_NI_init(v101, v30);
      AES_NI_enc(v15[11], v31, (v15 + 3), v15[10], v15[10]);
      cleare_user_private_key(v32, 0xFF, 4);
    }
    else
    {
      custom_AES_init(v100, v30);
      custom_AES_enc(v15 + 3, v15[10], v15[10]);
      cleare_user_private_key(v100, 0xFF, 280);
    }
```

```
if ( curve25519_xsalsa20_poly1305(v42, v58, 32LL, publickey, v13) || iMinfilesize > a3 )
  goto LABEL_38;
v37 = v35;
mbedtls_aes_init_encrypt(v41, v58);
v57 = v59;
v36 = a7;
if ( a6 )
  v16 = *a6;
else
  v16 = 0LL;
v17 = a3 + 15;
if ( a3 >= 0 )
  v17 = a3;
v39 = v17 & 0xFFFFFFFFFFFFFFF0LL;
*&v56[7] = v17 & 0xFFFFFFFFFFFFFFF0LL;
v40 = time(0LL);
v18 = gmtime(&v40);
strftime(v44, 0x14uLL, &time_fmt, v18);
v19 = pthread_self();
v20 = rand();
v35[0] = v44;
v35[1] = v19;
v35[2] = a1;
v35[3] = v20 + v20 / -v38 * v38 + v38;
PrintLog2(&start_enc_offset);
v21 = mmap_alloc(a1, a2, a5, &v39, v16);
if ( v21 == -1 )
  goto LABEL_18;
v22 = v21;
v23 = v39;
mbedtls_aes_encrypt_cbc(v41, v39, &v57, v22, v22);
```

[암호화 키 보호 및 파일 암호화 과정(좌: LockBit 2.0, 우: LockBit MacOS]

LockBit 3.0 의 경우는 현재 피해자의 CPU 가 지원하는 난수 생성 명령어를 통해 대칭 키를 생성하고, RSA 알고리즘으로 암호화를 통해 보호한 다음 체크섬[49]으로 유효성을 검증한다.



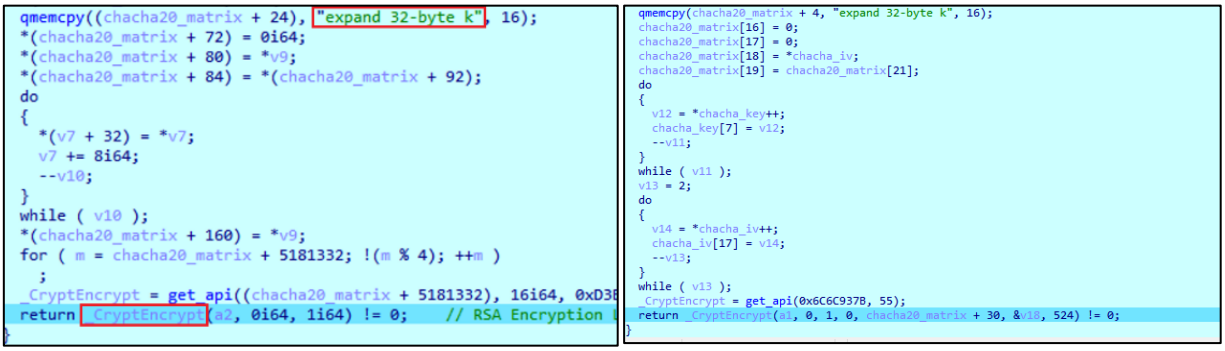
```
__asm { cpuid }
if ( (_ECX & 0x40000000) != 0 )
{
  __asm
  {
    rdrand  eax
    rdrand  edx
  }
}
```

```
CreateKey(&symmetric_key, &unk_424F70);
RtlEncryptMemory(&symmetric_key, 0x80u, 0);
j_qmemcpy(key, &symmetric_key, 0x80u);
RtlDecryptMemory(key, 0x80u, 0);
RSA_crypt(key, &unk_424F70);
checksum = Checksum(key, 128);
```

[LockBit 3.0 키 생성 및 보호 과정(좌: 대칭 키 생성, 우: 대칭 키 보호)]

[49] 체크섬 : 암호화 키가 오류 없이 생성되었는지 검증하는데 사용하는 값

LockBit Green 은 ChaCha20 과 RSA 암호화 알고리즘을 사용하여 제작되었다. 이는 Conti 소스코드를 그대로 사용하고 일부 설정값만 변경하였기 때문에 상당 부분 동일한 코드를 확인할 수 있다.



```
qmemcpy((chacha20_matrix + 24), "expand 32-byte k", 16);
*(chacha20_matrix + 72) = 0i64;
*(chacha20_matrix + 80) = *v9;
*(chacha20_matrix + 84) = *(chacha20_matrix + 92);
do
{
  *(v7 + 32) = *v7;
  v7 += 8i64;
  --v10;
}
while ( v10 );
*(chacha20_matrix + 160) = *v9;
for ( m = chacha20_matrix + 5181332; !(m % 4); ++m )
  ;
_CryptEncrypt = get_api((chacha20_matrix + 5181332), 16i64, 0xD3
return _CryptEncrypt(a2, 0i64, 1i64) != 0;    // RSA Encryption
}
```

```
qmemcpy(chacha20_matrix + 4, "expand 32-byte k", 16);
chacha20_matrix[16] = 0;
chacha20_matrix[17] = 0;
chacha20_matrix[18] = *chacha_iv;
chacha20_matrix[19] = chacha20_matrix[21];
do
{
  v12 = *chacha_key++;
  chacha_key[7] = v12;
  --v11;
}
while ( v11 );
v13 = 2;
do
{
  v14 = *chacha_iv++;
  chacha_iv[17] = v14;
  --v13;
}
while ( v13 );
_CryptEncrypt = get_api(0x6C6C937B, 55);
return _CryptEncrypt(a1, 0, 1, 0, chacha20_matrix + 30, &v18, 524) != 0;
}
```

[LockBit Green 암호화 과정(좌: LockBit Green, 우: Conti)]

LockBit 의 주요 버전에서는 공통적으로 파일 속도 향상을 위해 I/O Completion port 를 활용하여 비동기 암호화 방식[50]을 사용한다. 윈도우에서 제공하는 비동기 I/O 처리 방법 중 가장 뛰어난 성능을 보장하며, 기존의 스레드와 같은 비동기 처리 방식보다 Context Switching[51] 비용이 줄어들며 효율적인 스레드 사용으로 CPU 점유율[52]을 낮출 수 있다. 이러한 방식을 통해 LockBit 은 상대적으로 빠른 암호화를 제공하고 있다.

```
NumberOfConcurrentThreads = 2 * SystemInfo.dwNumberOfProcessors;
ExistingCompletionPort = CreateIoCompletionPort(0xFFFFFFFF, 0, 0, 2 * SystemInfo.dwNumberOfProcessors);
v35 = 0;
if ( SystemInfo.dwNumberOfProcessors )
{
  CreateThread = ::CreateThread;
  do
  {
    t_handle1 = CreateThread(0, 0, Encryption_Func, 0, 0, &ThreadId);
    t_handle2 = CreateThread(0, 0, Encryption_Func, 0, 0, &ThreadId);
    v29 = 1 << v35;
    v30 = t_handle2;
    SetThreadAffinityMask(t_handle1, 1 << v35);
    SetThreadAffinityMask(v30, v29);
    CreateThread = ::CreateThread;
    ++v35;
  }
  while ( v35 < SystemInfo.dwNumberOfProcessors );
}
```

```
::NumberOfProcessors = NumberOfProcessors;
_NtCreateIoCompletion = resolve_NtCreateIoCompletion();
if ( _NtCreateIoCompletion(&dword_4E2520, 0x1F0003, 0, v41) >= 0 )
{
  ExistingCompletionPort = sub_4BABA0((4 * ::NumberOfProcessors));
  if ( ExistingCompletionPort )
  {
    v37 = 0;
    if ( !::NumberOfProcessors )
      return 1;
    while ( 1 )
    {
      *(ExistingCompletionPort + 4 * v37) = create_thread(Encryption_Function, 0);
      v38 = *(ExistingCompletionPort + 4 * v37);
      if ( v38 == -1 )
        break;
      v47 = 1 << v37;
      _NtSetInformationThread = resolve_NtSetInformationThread(v38, 4, &v47, 4);
      _NtSetInformationThread();
      if ( ++v37 >= ::NumberOfProcessors )
        return 1;
    }
  }
  NtClose_0(j);
```

```
CpuNum = check_cpunum();
if ( (CpuNum & 0x20) != 0 )
  CpuNum = 32;
v1 = 2 * CpuNum + 1;
v5 = 0;
ExistingCompletionPort = CreateIoCompletionPort(-1, 0, 0, v1);
if ( ExistingCompletionPort )
{
  do
  {
    Thread = CreateThread(0, 0, EncryptFunction, 0, 0, 0);
    v3 = Thread;
    if ( Thread )
    {
      HideThreadFromDebugger(Thread);
      NtClose(v3);
      ++v5;
    }
    --v1;
  }
  while ( v1 );
}
RtlInitializeCriticalSection(&unk_D15888);
```

[I/O Completion port 사용(상: LockBit 1.0, 좌측 하단: LockBit 2.0, 우측 하단: LockBit 3.0)]

[50] 비동기 암호화 방식 : 암호화 방식을 멀티 스레드로 병렬 처리하여 빠른 작업이 가능

[51] Context Switching : 현재 실행 중인 스레드 상태를 저장하고 다른 스레드를 로드하여 CPU 제어권을 전환하는 과정

[52] CPU 점유율 : CPU가 특정 작업을 수행하는 데 소비하는 시간의 비율. 시스템의 성능 효율을 평가하는 지표 중 하나

✓ 취약점 악용 침해 위협

[LockBit이 악용한 취약점]

LockiBit 은 공격 시 주로 취약점을 악용한 초기 침투를 선호한다. 국내에서는 피싱 메일을 통해 전파되는 케이스가 대부분이지만, 기업과 같은 조직에서 주로 사용하는 솔루션에 대한 취약점을 악용해 대규모 공격을 노리는 것이 LockBit 의 전략이라고 할 수 있다.

LockBit 은 초기 버전부터 다양한 취약점을 통해 랜섬웨어 공격을 수행해왔다. 다수의 윈도우 관련 취약점, Log4Shell, PaperCut, GoAnywhere MFT, Cisco ASA/FTD, Citrix Bleed 등 전 세계적으로 파급력이 큰 다수의 취약점을 공격에 사용했으며, 최근 LockBit 은 ScreenConnect 취약점인 CVE-2024-1709 를 악용하여 다수의 피해 사례가 확인되고 있다.

작년까지 많이 확인되었던 초기 침투 방식은 주로 오래된 취약점을 사용하여 패치되지 않은 서버를 대상으로 대규모 공격을 수행하는 특징이 있었다. 오래된 취약점은 PoC(Proof of Concept)[53]등 다양한 사례가 공개되어 있어 0-day 취약점[54]이나 1-day 취약점[55]을 사용하는 것보다 리소스 소모가 적지만 패치 적용 여부 및 환경에 따라 제한적일 수 있다. 이러한 제한 사항을 반영하듯 최근 들어서는 1-day 취약점을 사용하여 공격을 수행하는 모습이 다수 확인되었으며, LockBit 랜섬웨어뿐만 아니라 BlackBasta, Bloody, Play 랜섬웨어 그룹 등 다양한 그룹에서 1-day 취약점을 악용하여 공격을 수행하는 모습이 확인되고 있다.

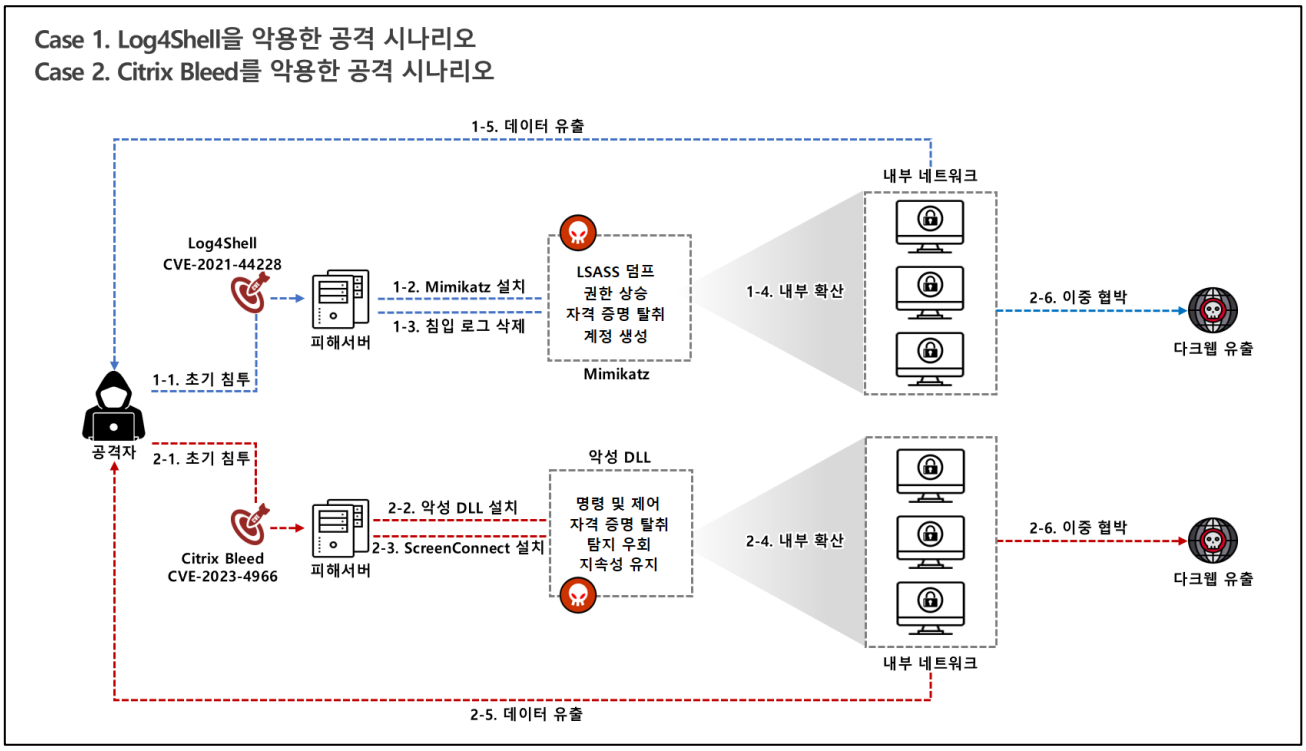
[53] PoC : 취약점을 실제로 악용할 수 있음을 보여주는 코드

[54] 0-day 취약점 : 공개적으로 알려지지 않아 패치가 존재하지 않는 보안 취약점으로, 발견 즉시 악용될 소지가 있어 위험성이 높은 취약점

[55] 1-day 취약점 : 이미 공개되어 패치가 제공된 취약점을 의미하나, 아직 많은 시스템에서 패치가 적용되지 않았을 수 있으므로 공격자가 악용할 여지가 있는 취약점

0-day, 1-day 취약점을 악용하는 이유로는 패치가 불가하거나 패치가 적용되지 않았을 확률이 높아 더 많은 이들을 대상으로 공격을 수행하고자 하는 전략 중 하나로 보인다.

✓ LockBit 공격 시나리오



[취약점을 악용한 LockBit 공격 시나리오]

Case 1 은 전 세계적으로 큰 혼란을 불러온 Log4Shell 을 악용한 랜섬웨어 공격 사례이다. Log4Shell 은 널리 사용되는 자바 기반의 로깅 유틸리티인 Log4j를 대상으로 원격 코드 실행을 할 수 있는 취약점이다. LockBit은 Log4Shell을 통해 피해 서버에 침투한 뒤, 자격 증명 탈취를 통한 권한 상승을 위해 Mimikatz[56]를 시스템 내에 설치한다. 이후 침투한 흔적이 담긴 로그를 삭제하고 PsExec 와 RDP(Remote Desktop Protocol)[57]를 통해 내부 네트워크로 이동하여 FileZilla[58]를 사용해 시스템 내에 존재하는 파일들을 유출시킨다. 모든 과정이 끝나면 랜섬웨어를 시스템에 유포시켜 시스템을 암호화 시키고 탈취한 데이터와 암호화된 파일을 인질 삼아 이중 협박을 수행한다.

Case 2 는 Citrix Bleed 를 악용한 공격 사례이다. Citrix Bleed 는 NetScaler ADC 및 NetScaler Gateway [59] 환경에서 악용이 가능하며, 의도하지 않은 민감 정보가 공개되는 정보 노출 취약점이다. 해당 취약점을 통해 피해 서버에 침투를 성공한 LockBit 은 이후 C2 통신[60]을 수행하는 악성 DLL 을 시스템에 설치하여 지속적으로 피해 시스템에 자격 증명 탈취와 같은 명령을 수행시킨다. 또한 탐지 우회 기능도 포함되어 있어 보안 솔루션에 탐지되지 않은 채로 악성 DLL 과 함께 설치한 ScreenConnect 를 통해 내부 네트워크로 이동하여 중요한 파일을 외부로 유출시키고, 시스템을 암호화 시켜 이중 협박을 수행한다.

---

[56] Mimikatz : Windows 시스템에서 자격증명과 같은 민감 정보를 수집하는 도구

[57] RDP : 다른 컴퓨터를 원격으로 제어할 수 있도록 해주는 프로토콜

[58] FileZilla : 파일 전송 소프트웨어

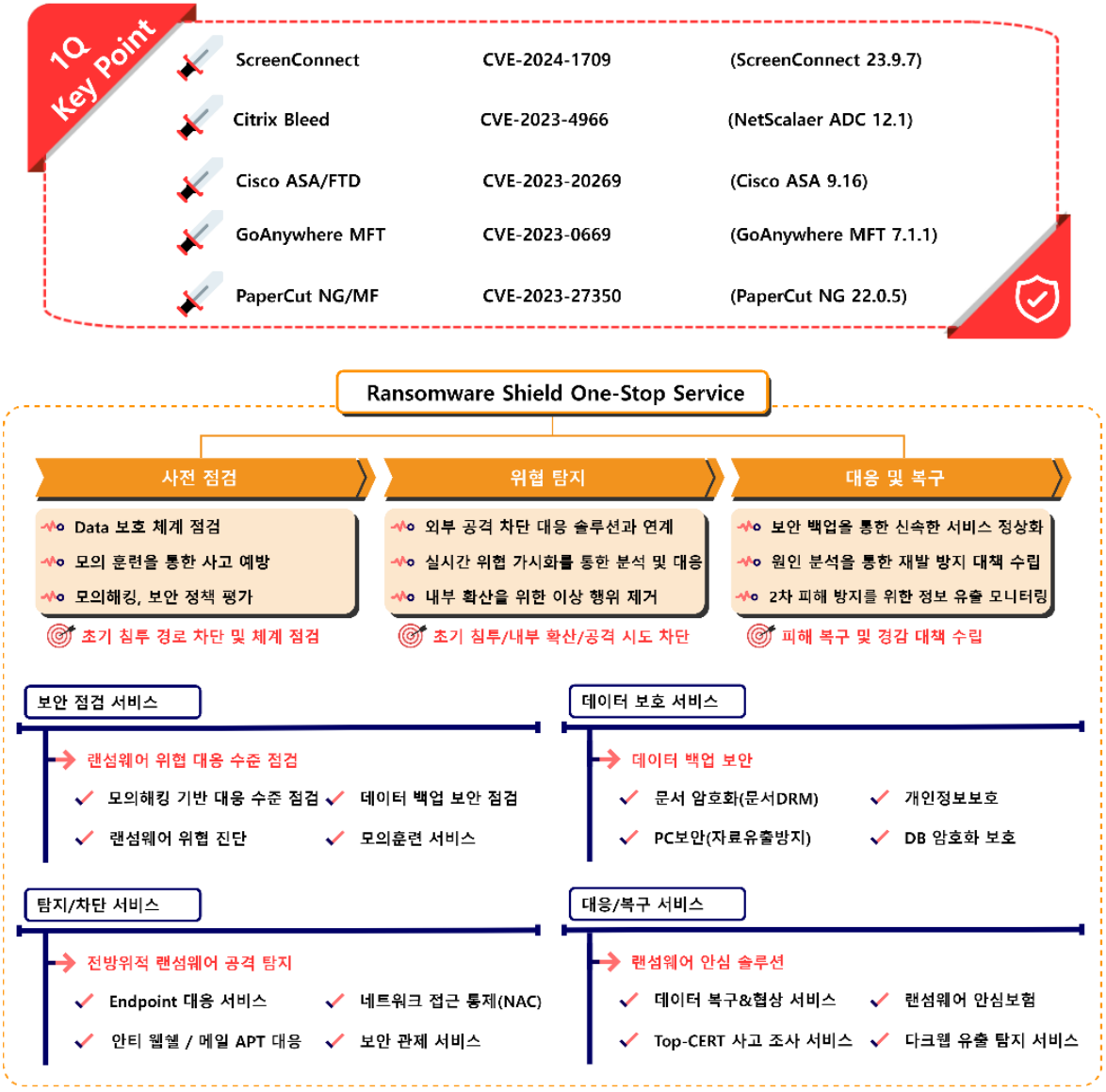
[59] NetScaler ADC 및 NetScaler Gateway : Citrix Systems에서 제공하는 네트워크 장비 및 소프트웨어 솔루션

[60] C2 통신 : 악성코드가 감염된 호스트와 공격자 서버 간에 명령을 전송하고 데이터를 수집하는 통신 방식

랜섬웨어 Mitigations

1. LockBit 랜섬웨어 대응방안 안내

LockBit 랜섬웨어는 주로 피싱 메일이나 취약점을 악용한 초기 침투를 통해 감염된다. 특히 기업을 비롯한 조직에서 사용하는 소프트웨어 솔루션에 대한 취약점을 주로 악용하여 대규모 공격을 도모하기도 하며, 최근에는 공급망 공격을 수행하려는 움직임을 보이고 있다. 이러한 피해를 예방하기 위해서는 취약점이 패치된 최신 버전의 소프트웨어를 적용하는 것과 더불어 악성 메일 훈련, 모의 해킹, 보안 체계 점검 등의 사전 점검이 가장 중요하며, 위협 탐지를 통해 실시간으로 위협에 대응하는 것이 필요하다. 추후 발생할 수 있는 피해를 경감시킬 수 있는 랜섬웨어 안심보험 서비스와 다크웹에 유출된 데이터 모니터링 등의 서비스를 고려하는 것을 추천한다.



[LockBit 랜섬웨어 Mitigations]

부록

1. LockBit이 악용한 소프트웨어 취약점

CVE	설명	영향 버전	패치 버전
CVE-2018-13379	Fortinet의 보안 OS FortiOS에서 SSL VPN[61]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	Windows에서 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 Log4j에서 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	F5의 어플리케이션 배포 네트워크 장비인 BIG-IP, BIG-IQ에서 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	MS의 전자 메일 서버인 Exchange Server에서 발생하는 원격 코드 실행 취약점	Exchange Server 2013, 2016, 2019	KB5000871 업데이트
CVE-2021-36942	Windows Server에서 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 Framwork에서 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	Forta의 보안 관리 파일 전송 소프트웨어 GoAnywhere MFT에서 원격 코드 실행이 가능한 취약점	7.1.1 이하	7.1.2 이상
CVE-2023-20269	통합 보안 플랫폼 Cisco ASA와 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 PaperCut에서 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 Gateway에서 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

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

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

[LockBit이 악용한 소프트웨어 취약점]

안녕을 지키는 기술 | SK 쉴더스

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 EQST/SI솔루션사업그룹 & KARA(Korea Anti Ransomware Alliance)
제　작 : SK쉴더스 마케팅그룹