Keep up with Ransomware

LockBit 의 새로운 움직임

■ 개요

2025 년 2 월 랜섬웨어 피해 사례 수는 지난 1 월(722 건) 대비 약 48% 증가한 1067 건을 기록했다. 2 월에 피해 사례가 급증한 이유는 Clop 그룹이 Cleo 의 파일 전송 솔루션 취약점을 악용해 피해자를 연달아 공개했기 때문이다. 이들은 2 월에만 전체 피해 사례의 27%에 해당하는 287 건을 공개했으며, 기업명이나 피해 기업의 웹페이지 주소를 알파벳 순으로 공개하고 있기 때문에 앞으로 더 많은 피해자가 나올 것으로 보인다.

유로폴, NCA 등 범죄 수사 기관들의 글로벌 공조 수사를 통해 Phobos 랜섬웨어와 연관이 있는 8Base 그룹의 관계자들이 체포됐다. 이들은 2019 년부터 조사를 시작해 2024 년 한국에서 Phobos 랜섬웨어의 관계자를 체포했으며, 25 년 2 월에는 Phobos Aetor 작전의 일환으로 태국에서 8Base 그룹 관계자 4 명을 체포하고 컴퓨터 사기·손상·강탈 등 11 가지 혐의로 기소했다.

BlackBasta 의 내부 구성원으로 추정되는 ExploitWhispers 가 텔레그램을 통해 BlackBasta 의 채팅 내역을 공개했다. 공개된 채팅은 23 년 9 월부터 약 1 년간 주고받은 Matrix[1] 채팅 내역으로, 50 명의 사용자가 주고받은 20 만개의 메시지다. ExploitWhispers 는 BlackBasta 그룹이 러시아의 은행을 공격한 것에 대한 보복으로 채팅 내역을 공개한 것이라고 밝혔다. 공개된 채팅 내역에 따르면 이들은 정보 탈취형 악성코드를 통해 인증 토큰이나 저장된 브라우저 비밀번호 등을 탈취하며, 탈취한 계정 정보로 침투 테스트를 진행하고 있다. 또한 금융, 제조업을 우선적으로 공격 대상으로 지정했다. 이들은 총 62 개의 CVE[2] 를 언급했으며, Paloalto 의 보안 장비 OS 에서 발생한 원격 코드 실행 취약점 CVE-2024-3400 을 가장 많이 언급했다. 이외에도 이들은 잘 알려진 취약점의 개념 증명 코드를 주로 활용하려는 모습이 확인됐다. 때문에 공격을 방지하기 위해서는 정기적으로 소프트웨어나 버전 업데이트를 통해 취약점을 빠르게 보호하는 것이 필요하다.

[1] Matrix: 오픈소스 기반의 탈중앙화된 실시간 커뮤니케이션 프로토콜로, 메시징, 음성 및 영상 통화, 파일 공유 등이 가능

[2] CVE: 소프트웨어 및 하드웨어의 보안 취약점을 식별하기 위한 식별 번호 체계

2022 년부터 RTM Locker 로 활동하던 그룹이 신규 RaaS[3] 파트너를 모집하기 시작했다. RTM Team 은 다크웹 자체 포럼을 보유하고 있는 그룹으로, RTM Locker 로서 계열사를 모집한 이력이 존재하고 버전도 3.0 까지 업데이트하며 활동을 이어왔다. 24 년 9 월부터는 자체 포럼에 더 이상 글이 게시되지 않는 상태였으나, 25 년 2 월에 자신들의 포럼이 아닌 러시아 해킹 포럼에 RTM Team RaaS 파트너 모집 글을 게시해 다시 활동을 시작하려는 조짐을 보이고 있다. 이들의 홍보 글에 따르면 RaaS 에서 사용하는 랜섬웨어는 기존의 RTM Locker 3.0 과는 다르게 기능을 상세히 설명하고 있으며 NixOS[4], BSD[5] 공격 대상 플랫폼이 추가됐다. 현재 파트너는 러시아어 사용자만 모집하고 있고, 파트너 수수료는 30%로 시작해서 세부 조건을 추후에 조정하는 방식이다.

지난달에 이어 2 월에도 국내 침해 사례가 발견됐다. Lynx 그룹이 국내 자동차 부품 제조업체를 공격해 내부 데이터를 공개했다. 이들은 2 월 5 일 데이터 공개 예고 글을 업로드했으며, 그로부터 일주일 뒤에 약 12GB 크기의 전체 데이터를 공개했다. 유출된 자료에는 견적서·비밀유지계약서·감사자료·견적서·청구서 등의 업무 관련 문서로 확인됐다.

[3] RaaS (Ransomware-as-a-Service): 랜섬웨어를 서비스 형태로 제공해서 누구나 쉽게 랜섬웨어를 만들고 공격할 수 있도록 하는 비즈니스 모델

[4] NixOS: 높은 재현성과 신뢰성을 가진 패키지 매니저 Nix 를 사용하는 Linux 기반의 운영체제

[5] BSD: 미국 캘리포니아 대학 버클리에서 개발한 유닉스 계열의 운영체제

■ 랜섬웨어 뉴스

Clop 그룹, Cleo 취약점 악용한 대규모 공격 피해자 명단 및 데이터 공개

- Cleo의 파일 전송 솔루션 Cleo Harmony, VLTrader, LexiCom의 취약점(CVE-2024-50623, CVE-2024-55956) 악용
- 알파벳 순으로 추가 피해 기업 공개 중
- 2월에는 총 287건의 추가 피해자 공개

신규 Linkc, RunSomeWares 그룹 등장

- Linkc 그룹은 2월 19일에 피해자 1건 게시
- RunSomeWares 그룹은 2월 27일에 피해자 4건 일괄 게시

신규 Anubis 그룹, 피해자 4건 게시

- 러시아 해킹 포럼 Ramp 포럼에서 RaaS 파트너를 모집하는 글 게시
- 랜섬웨어 서비스 외에도 데이터 협박, 접근 권한 판매 등 다양한 서비스도 함께 제공
- 23일 파트너 모집글 게시 이후 다크웹 유출 사이트에 25일부터 피해자 게시 시작

BlackBasta 내부 채팅 내역 일부 공개

- 내부 구성원으로 추정되는 ExploitWhispers 유저가 보복성으로 1년치 채팅 내역을 공개
- 50명의 사용자가 주고 받은 20만개의 메시지 데이터
- 채팅 내역에 따르면 정보 탈취 도구를 악용해 계정 정보를 탈취하며, 해당 정보로 침투 시도를 테스트
- 그 외에 알려진 취약점에 대한 개념 증명 코드가 공개되면 활용하려고 시도


RTM Team, 신규 RaaS 파트너 모집
기존에 사용하던 RTM Locker 3.0 에서 업데이트 진행 후 서비스 제공
파트너는 러시아어 사용자만 모집하고 있으며, 초기 수수료 30%로 시작해 추후 조정하는 방식
HelloKitty 그룹, Kraken으로 리브랜딩
과거 Cisco, CD Projekt Red 를 공격한 그룹으로, HelloGookie로 리브랜딩 한 뒤 Kraken으로 재변경
기존의 데이터 3건 외에 신규 피해자 3건 추가로 게시

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

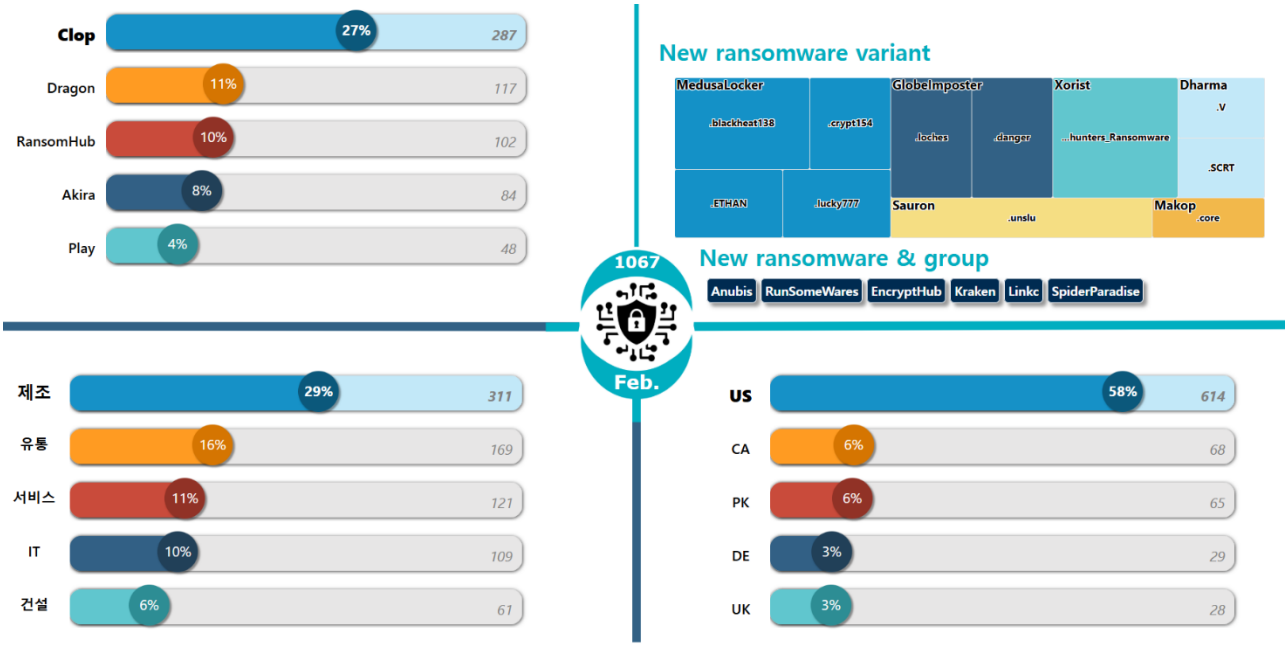


그림 2. 2025 년 2 월 랜섬웨어 위협 현황

새로운 위협

1 월에는 5 개의 신규 랜섬웨어 그룹이 발견됐다. 신규 외에도 기존 HelloGookie(HelloKitty) 그룹이 Kraken 이라는 이름으로 리브랜딩 했으며, 리브랜딩 전에 업로드한 기존 데이터 외에도 신규 유출 데이터 3 개를 추가로 공개했다. 이외에도 신규 RunSomeWares 그룹은 2 월 27 일에 총 4 건의 피해자를 게시했으며, Linkc 그룹은 피해자 1 건을 게시했다.

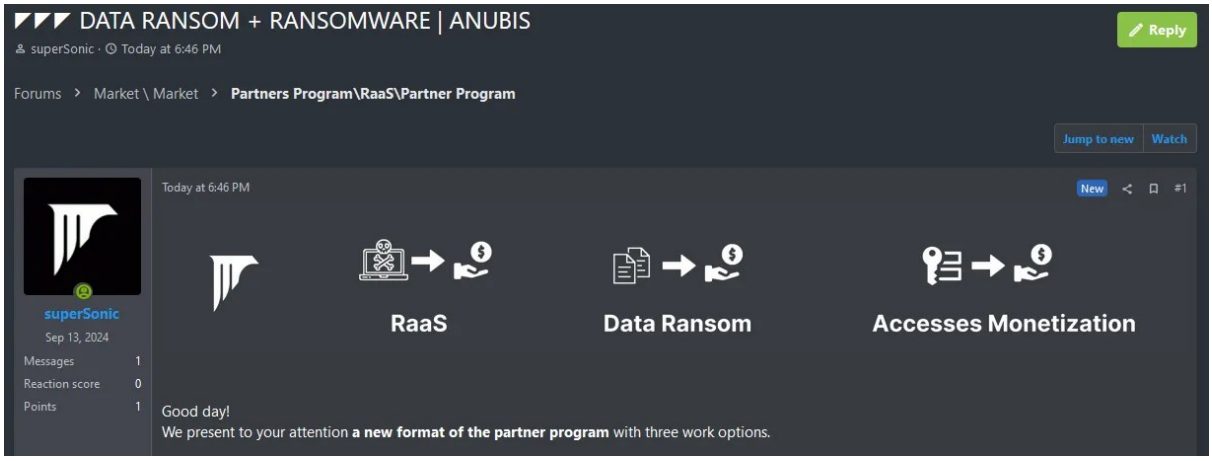


그림 3. Anubis 랜섬웨어 RaaS 파트너 모집 글

2 월에도 신규 파트너를 모집하는 정황이 발견됐다. 새롭게 등장한 Anubis 그룹은 러시아 해킹 포럼에 자신들의 서비스를 이용할 파트너를 모집하는 글을 업로드했다. 이들은 랜섬웨어 서비스 외에도 데이터 서비스, 접근 권한 판매 서비스도 함께 제공한다고 밝혔다. 랜섬웨어 서비스는 일반적인 RaaS 형태로, 랜섬웨어를 제공한 뒤 지불 받은 몸값의 20%에 해당하는 금액만 수수료로 지불하면 된다. 데이터 서비스는 아직 유출된 적 없는 데이터로 협박 후 기업으로부터 협상금을 탈취하는 방식으로, 현재 랜섬웨어 그룹들이 많이 사용하는 이중 강탈 방식에서 데이터 부분만 독립적으로 제공하는 것이다. 이외에도 접근 권한을 판매해 수익화하는 서비스도 제공하는 모습이 확인됐다. 이들은 파트너 모집 이후 25 일부터 다크웹 유출사이트에 데이터를 공개하며 본격적인 활동을 시작했다.

Top5 랜섬웨어

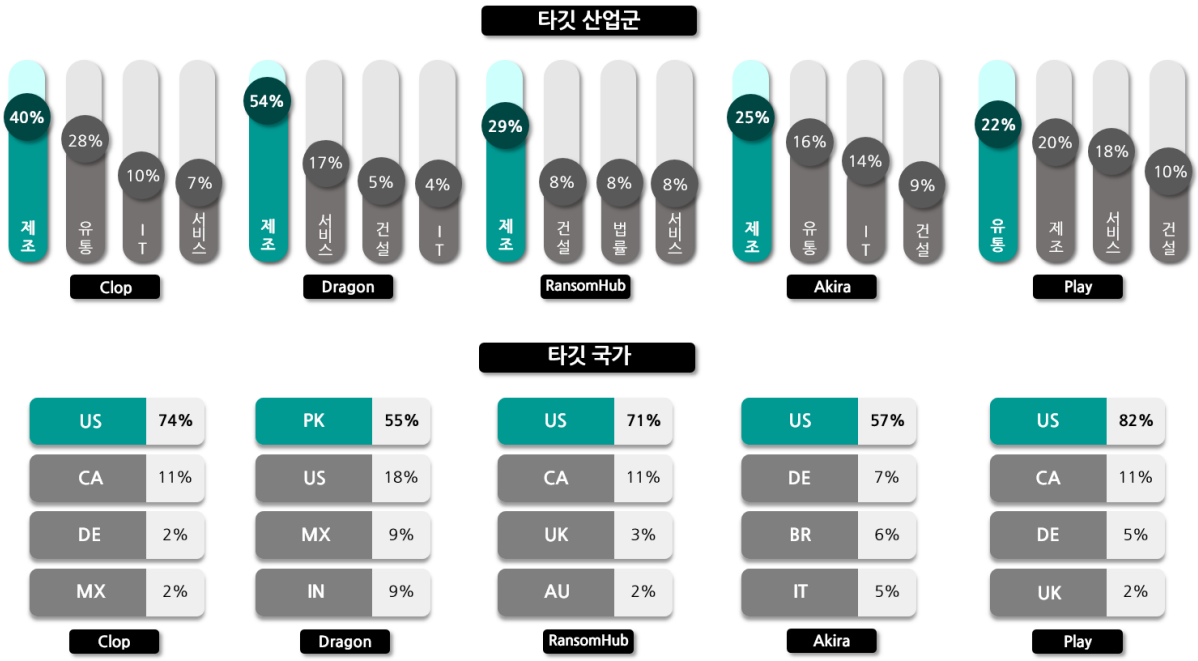


그림 4. 산업/국가별 주요 랜섬웨어 공격 현황

지난 12 월 Cleo 의 파일 전송 솔루션 취약점을 악용해 대규모 공격을 했던 Clop 그룹이 2 월에도 추가 피해자를 공개했다. 이들은 2 월에 총 287 건의 피해자를 추가로 게시했다. 알파벳 순으로 기업명을 순차적으로 공개하고 있기 때문에, 앞으로 더 많은 피해자 명단이 공개될 가능성이 높다.

Dragon 그룹은 지난 10 월부터 텔레그램 채널을 통해 활동하기 시작한 랜섬웨어 그룹으로, 지난달에 이어 2 월에도 100 건이 넘는 피해자를 게시했다. 텔레그램 채널에서 홍보한 내용에 따르면, 자체 Dragon 랜섬웨어 기반의 RaaS 를 제공한다. 랜섬웨어 공격 외에도 DDoS[6]공격과 웹사이트 변조 공격 또한 수행하며 다양한 위협 활동을 하고 있다. 이들은 단일 피해자를 게시하기도 하지만 수십 건에 달하는 피해자를 일괄적으로 게시하기도 한다. 일괄적으로 업로드된 피해자들은 대부분 동일한 웹 호스팅 서비스를 이용하고 있는 특징을 가지고 있다. 또한 피해자 중 일부는 수년 전부터 웹 서비스를 더 이상 운영하고 있지 않는 경우도 많다.

RansomHub 그룹은 미국의 의료 기관 Midwest Vascular, 영국의 파이프 제조 업체 Electro Fusion, 미국의 법률 회사 NOLA Law, 캐나다의 로펌 Withey Addison 등 다양한 분야에 걸쳐 공격을 수행해 총 102 건의 피해자를 게시했다.

Akira 그룹은 2 월에도 84 건의 피해자를 게시하며 활발히 활동하고 있다. 2 월에는 호주 엔지니어링 기업 Thornton Engineering 을 공격해 직원 및 고객의 연락처, 감사 보고서, 결제 세부 사항 등 업무 관련 문서가 포함된 11GB 데이터를 공개했다. 또한 미국 금융 서비스 기업인 Prime Trust Financial 을 공격해 데이터를 탈취하기도 했다. Akira 그룹의 세부 공격 전략과 대응방안은 SK 쉴더스 KARA 랜섬웨어 동향 보고서 2024 4Q 에서 자세하게 확인할 수 있다.

Play 랜섬웨어는 2 월에 미국 캘리포니아주 오클랜드 시를 공격해 대규모의 데이터 유출을 발생시켰다. 초기에 10GB 의 데이터를 공개한 후, 추가로 600GB 에 달하는 시 정부 데이터를 다크웹 유출 사이트에 공개했다. 유출된 데이터에는 시장을 포함한 직원의 개인 정보, 시민의 개인 정보들이 포함되어 있었다.

[6] DDoS: 악의적으로 대상 네트워크, 서버, 온라인 서비스 등에 많은 트래픽을 발생시켜 해당 시스템의 기능을 정상적으로 사용하지 못하도록 하는 공격

■ 랜섬웨어 집중 포커스

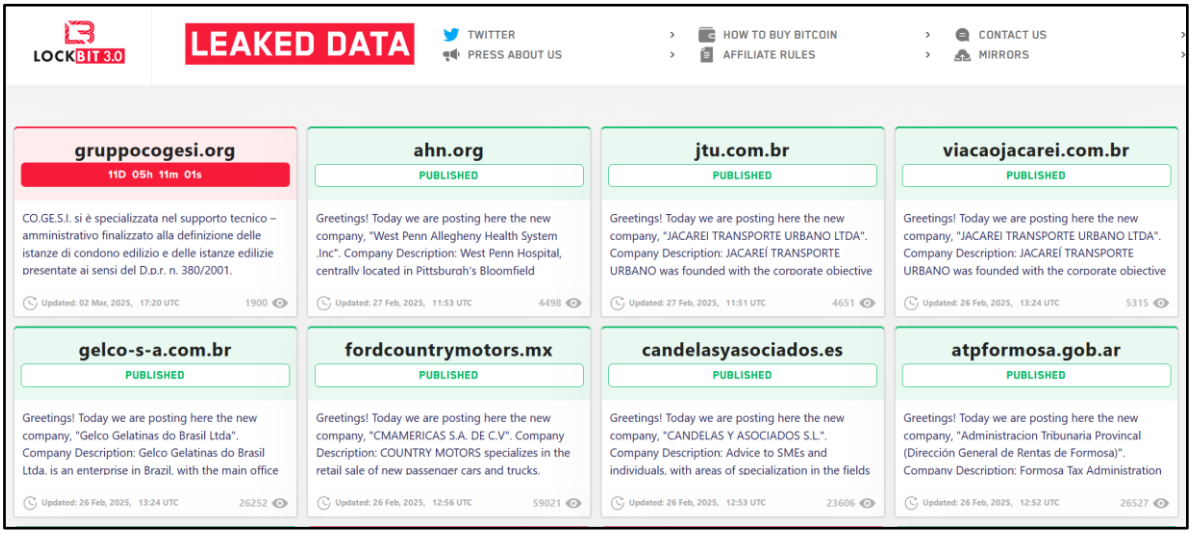


그림 5. LockBit 다크웹 유출 사이트

LockBit 그룹은 2019 년 등장한 이후 꾸준한 업데이트를 진행해왔고, 2022 년에는 LockBit 3.0 을 출시하며 그때부터 왕성한 활동을 보였다. 2024 년에는 FBI 와 유로폴을 비롯한 여러 수사 기관들이 국제 공조를 통해 LockBit 의 인프라를 무력화하는 사이버 작전 Cronos Operation 을 진행했다. 그로 인해 주요 서버 인프라 압수, DLS[7]폐쇄, 복호화 키 공개, 주요 운영자의 신상이 공개되는 등 활동에 큰 영향을 받았다. 이전까지 매달 수십 건의 피해자를 업로드하며 왕성한 활동을 보이던 LockBit 그룹은 Cronos 작전 이후로 활동량이 급격히 줄어들었고, 매달 10 건 내외의 피해자를 업로드 하는 등 운영에 문제가 생긴 모습을 보이고 있다.

그림 6. LockBit 4.0 출시 예고 글

[7] DLS(Dedicated Leak Sites): 특정 대상으로부터 탈취한 정보를 공개해 협박하며, 협상에 응하지 않을 시 데이터를 공개하기 위한 웹사이트

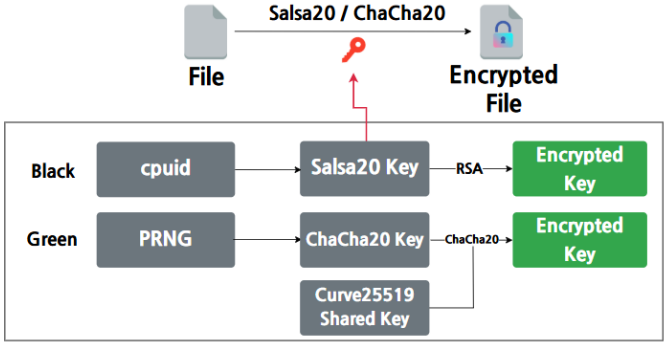
Cronos 작전으로 인해 급격히 무너지던 LockBit 그룹은 다시 재건하기 위한 움직임을 보이기도 했다. 24 년 11 월에는 러시아 해킹 포럼에서 활동하는 LockBit 의 운영자 LockBitSupp 의 메신저 상태 메시지를 통해 LockBit 4.0 에 대해 언급했다. 또한 24 년 12 월에는 다크웹 유출 사이트에 "lockbit4.com" 이라는 글이 업로드 됐는데, 해당 글에는 4.0 버전을 홍보하는 문구와 파트너로 가입할 수 있는 다크웹 페이지 링크 5 개가 공개됐다. 이러한 4.0 버전에 대한 움직임은 예상보다 빠르게 확인됐다. 홍보 글 게시 이후 LockBit 4.0 으로 추정되는 랜섬웨어가 여럿 발견됐으며, 실제 피해 사례도 확인됐다.

확인된 LockBit 4.0 은 2 가지 버전으로 분류된다. 두 버전은 동일한 랜섬노트를 사용하지만 랜섬노트 맨 아래에 Black 과 Green 으로 버전을 표기했다. 기존의 Black 버전은 LockBit 3.0 에서 주력으로 사용하던 랜섬웨어이며, Green 의 경우 23 년에 Conti v3 랜섬웨어를 기반으로 만들어진 버전이다. LockBit 은 매번 버전을 변경하면서 Red·Black·Green 과 같은 이름으로 분류를 진행했지만, 4.0 에서는 기존에 사용하던 버전명을 그대로 사용하는 것으로 확인됐다. 이번 보고서에서는 기존에 사용하던 LockBit 3.0 의 랜섬웨어와 24 년 12 월에 새롭게 발견된 LockBit 4.0 의 랜섬웨어를 비교 분석하는 내용을 다루고자 한다.

LockBit 4.0 Ransomware

암호화 키

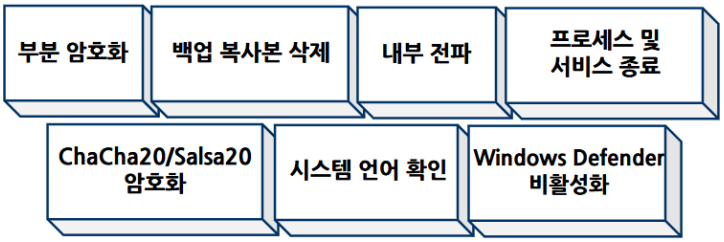
Black: Salsa20 알고리즘으로 파일 암호화를 하고, 해당 키를 RSA로 보호
Green: ChaCha20 알고리즘으로 파일 암호화를 하고, 해당 키를 Curve25519 공유 비밀로 보호



암호화 방식

Black: 512KB 이하: 전체 암호화
512KB 초과 5.5MB 이하: 최초 512KB 암호화
5.5KB 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
Green: 1MiB 이하: 전체 암호화
1MiB 초과: 파일 전체의 27%만 암호화

특징



랜섬노트

```
~~~ You have been attacked by LockBit 4.0 - the fastest, most stable and immortal ransomware since 2019 ~~~~

>>>>> You must pay us.

Tor Browser Links BLOG where the stolen information will be published:
( often times to protect our web sites from ddos attacks we include ACCESS KEY - ADTISZRLVUMXDJ34RCBZFNO6BNKLEYKYS5FZPNNXK4S2RSHOENUA )
http://lockbit3753ekiocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2id.onion/
http://lockbit3g3ohd3katajf6zaehxz4h4cnhmz5t735zpltywhwpc6oy3id.onion/
http://lockbit3olp7oetlc4tl5zydnoluphh7fvdt5oa6arcp2757r7xkutid.onion/
http://lockbit435xk3ki62yun7z5nhwz6jyjdp2c64j5vge536if2eny3gtid.onion/
http://lockbit4lahhluquhoka3t4spqym2m3dhe66d6lr337glmnlgg2nndad.onion/
http://lockbit6knrauo3qafoksvl742vieqbujxw7rd6ofzdtapjb4rrawqad.onion/
http://lockbit7ouvrsdgtojeoj5hvu6bljqtghitekwpdy3b6y62ixtsu5jqd.onion/

>>>>> What is the guarantee that we won't scam you?
We are the oldest extortion gang on the planet and nothing is more important to us than our reputation. We are not a politically motivated group and want

>>>>> Warning! Do not delete or modify encrypted files, it will lead to irreversible problems with decryption of files!
```

Black: [a-zA-Z0-9]{9}.README.txt
Green: Restore-My-Files.txt

변경 확장자

Black: [a-zA-Z0-9]{9}
Green: [a-z0-9]{12}

제작 언어

C/C++

그림 7. LockBit 4.0 랜섬웨어 개요

LockBit 4.0 랜섬웨어 전략

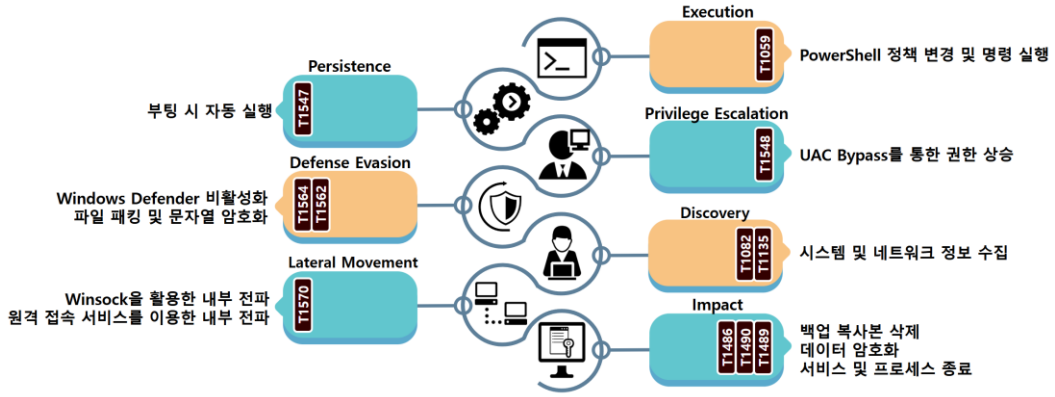


그림 8. LockBit 4.0 랜섬웨어 공격 전략

LockBit Black 4.0

LockBit Black 3.0 과 4.0 은 81%의 유사도를 보이고 있으며, 실제 분석 결과 동일한 기능을 수행하는 것으로 확인됐다. LockBit Black 에 대한 자세한 기능 분석은 24 년 3 월 Keep up with Ransomware 에서 확인할 수 있다. 또한 LockBit Black 4.0 의 경우 PowerShell Script 로 작성된 일부 버전이 확인됐는데, 해당 PowerShell Script 의 경우 최종적으로 인코딩된 LockBit Black 4.0 데이터를 디코딩 후 실행한다.

```
for ($i = 0; $i -lt $args.count; $i++ ){$argument += $args[$i] + ' '}
 $psFile=$PSCommandPath
$global:ProgressPreference = "SilentlyContinue"

# -- thread variables
$script:threadBody = '$data=$threadData;'
$data = @(
@(62416317159553766,6171585555604128,57336399694057504,58471265167106420,54959097326818472
64527480453839471,52536072690480837,52766518087147867,57372294081942048,51370291418535539,
62953253871806504,51638886326030446,57371478650990806,47108824885965523,18209280467040628,
```

그림 9. LockBit Black 4.0 PowerShell Script

PowerShell Script 의 경우 무수히 많은 정수 값들이 배열에 저장되어 있으며, 해당 데이터를 하나씩 가져온 뒤 ASCII 문자로 변환한다. 변환된 문자는 새로운 PowerShell Script 이며 해당 스크립트를 별도의 창 없이 실행하는 코드로 이루어져 있다.

```powershell
function Do-Exec($Payload, $Len) {
    $zipBytes = [System.Convert]::FromBase64String($Payload)
    $ms = New-Object IO.MemoryStream
    $ms.Write($zipBytes, 0, $zipBytes.Length)
    $null = $ms.Seek(0,0)
    $ExeImage = New-Object Byte[]($Len)
    $ds = New-Object IO.Compression.DeflateStream($ms, [System.IO.Compression.CompressionMode]::Decompress)
    $null = $ds.Read($ExeImage, 0, $Len)
    $ds.Dispose()

    Exec -PEBytes $ExeImage
}

# Exe-file image will putted in next line
Do-Exec -Payload '7LVjkC9dsKf7b9u2d9vdu23btm1bu23btm3bxm7bNuY95z13Yu6diDvzcT7ML2pV5qp8amXlqopKGc04AAgAAAD9Z/
```

그림 10. LockBit Black 4.0 PowerShell Script 2

추출된 PowerShell Script 는 Base64 로 인코딩된 LockBit Black 4.0 데이터를 디코딩한 뒤, 파일 형태로 저장하는 것이 아니라 메모리에 로드한 뒤 파일리스 방식으로 랜섬웨어를 실행한다. 메모리에서 실행되는 랜섬웨어 분석 결과, 확장자 변경·아이콘 변경·랜섬노트 등이 기존의 3.0 버전과 동일한 것으로 확인됐다.

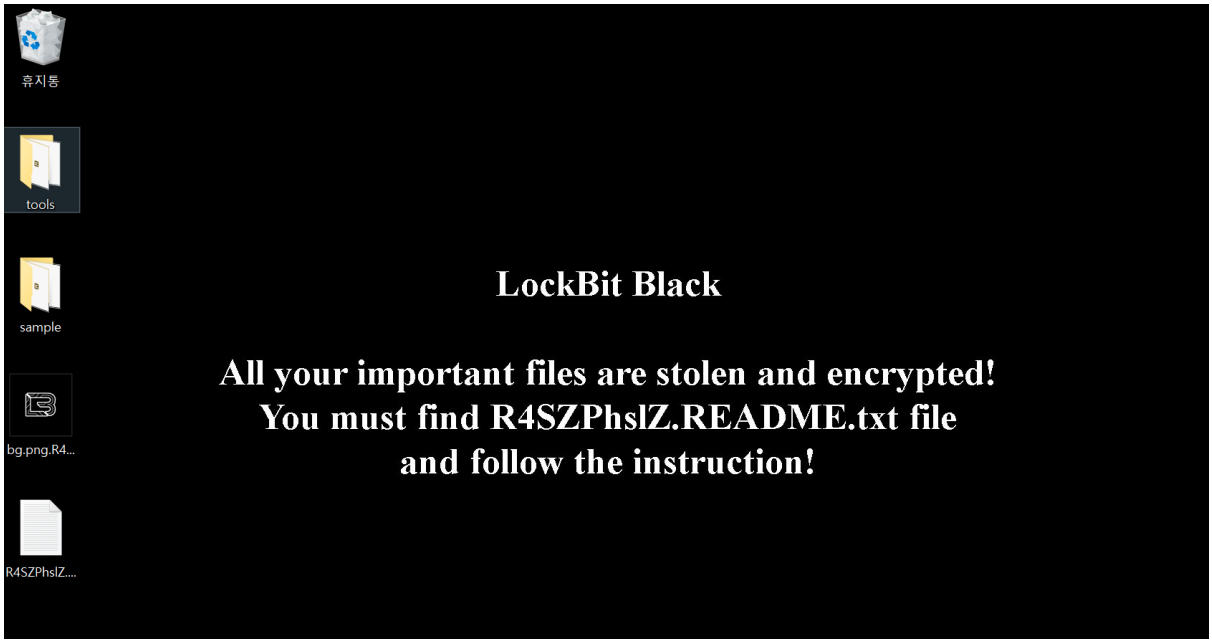


그림 11. LockBit Black 4.0 감염 화면

LockBit Green 4.0

LockBit 그룹은 2023 년에 Conti 랜섬웨어를 기반으로 한 LockBit Green 을 출시했다. LockBit Green 은 Conti v3 와 소스 코드 유사도가 89%나 될 정도로 설정과 디자인만 일부 개량한 버전이다. 과거 Conti 계열사들이 선호해 출시한 것으로 확인됐다. LockBit 그룹이 4.0 버전으로 넘어가면서 LockBit 4.0 Black 뿐만 아니라 과거 Green 버전의 특징을 일부 사용한 LockBit Green 4.0 버전도 발견됐기 때문에, 기존의 Green 버전과의 차이점과 유사점을 분석한 내용을 공유하고자 한다.

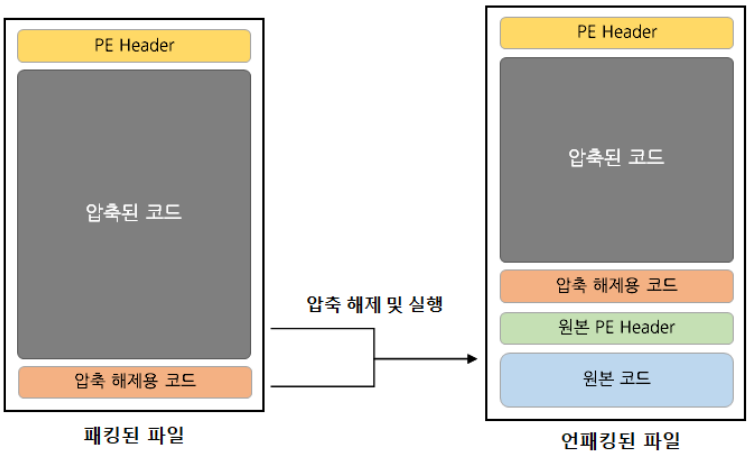


그림 12. LockBit Green 4.0 언패킹

LockBit Green 4.0 은 랜섬웨어 분석 및 탐지를 방해하기 위해 각종 기법을 사용하고 있다. 랜섬웨어 실행파일의 코드 부분을 압축한 뒤 실행할 때 압축 해제하는 방식인 패킹 기법을 사용한다. LockBit Green 4.0 은 오픈소스 기반의 UPX 패커를 사용한다. 또한 주요 문자열들은 모두 인코딩 혹은 암호화된 채로 저장되어 있어 필요할 때마다 디코딩 혹은 복호화 후 사용한다.

```
Decrypted Data (Raw): b"~~~ You have been attacked by LockBit 4.0 - the fastest, most stable and immortal ransomware sin
ce 2019 ~~~~₩n₩n>>>>> You must pay us.₩n₩nTor Browser Links BLOG where the stolen infortmation will be published:₩n( oft
en times to protect our web sites from ddos attacks we include ACCESS KEY - ADTISZRLVUMXDJ34RCBZFNO6BNKLEYKYS5FZPNNXK4S2
RSHOENUA )₩nhttp://lockbit3753ekiocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2id.onion/₩nhttp://lockbit3g3ohd3katajf6zaehxz4h
4cnhmz5t735zpltywhwpc6oy3id.onion/₩nhttp://lockbit3olp7oetlc4tl5zydnoluphh7fvdt5oa6arcp2757r7xkutid.onion/₩nhttp://lockb
it435xk3ki62yun7z5nhwz6jyjdp2c64j5vge536if2eny3gtid.onion/₩nhttp://lockbit4lahhluquhoka3t4spqym2m3dhe66d6lr337glmnlgg2nn
dad.onion/₩nhttp://lockbit6knrauo3qafoksvl742vieqbujxw7rd6ofzdtapjb4rrawqad.onion/₩nhttp://lockbit7ouvrsdgtojeoj5hvu6blj
qtghitekwpdy3b6y62ixtsu5jqd.onion/₩n₩n>>>>> What is the guarantee that we won't scam you?₩nWe are the oldest extortion g
ang on the planet and nothing is more important to us than our reputation. We are not a politically motivated group and
want nothing but financial rewards for our work. If we defraud even one client, other clients will not pay us. In 5 year
s, not a single client has been left dissatisfied after making a deal with us. If you pay the ransom, we will fulfill al
l the terms we agreed upon during the negotiation process. Treat this situation simply as a paid training session for yo
ur system administrators, because it was the misconfiguration of your corporate network that allowed us to attack you. O
ur pentesting services should be paid for the same way you pay your system administrators' salaries. You can get more in
```

그림 13. RC4 Decrypt 예시

문자열의 경우 길이에 따라서 인코딩과 암호화로 구분된다. 랜섬노트 내용, 실행 인자 설명처럼 문자열의 길이가 매우 긴 경우에는 암호화 RC4 알고리즘으로 암호화해 저장한다. 암호화에 사용한 16바이트 키는 랜섬웨어에 저장되어 있으며, 랜섬노트 복호화에 동일한 키를 사용해 복구한다. 그에 반해 랜섬웨어 실행 인자, 암호화 예외 항목 등 랜섬노트에 비해 상대적으로 짧은 20자 내외의 문자열의 경우에는 0x3A와 XOR 연산을 하는 방식으로 인코딩했기 때문에 필요할 때마다 디코딩 후 사용한다.

```
.data:000000014001E910 qword_14001E910 dq 0B63F6BA9h           ; DATA XREF: sub_140013A9F:loc_14001439C↑o
.data:000000014001E918 dq offset kernelbase_GetProcAddress
.data:000000014001E920 dq 2CCBA826h
.data:000000014001E928 dq offset ntdll_NtUnmapViewOfSection
.data:000000014001E930 dq 26AFE3BDh
.data:000000014001E938 dq offset ntdll_NtProtectVirtualMemory
.data:000000014001E940 dq 0C0585A7h
.data:000000014001E948 dq offset ntdll_NtOpenSection
.data:000000014001E950 dq 0A41F0062h
.data:000000014001E958 dq offset ntdll_NtMapViewOfSection
.data:000000014001E960 dq 7329774Ch
.data:000000014001E968 dq offset ntdll_NtSetInformationProcess
.data:000000014001E970 dq 9CB66CE7h
.data:000000014001E978 dq offset ntdll_RtlInitUnicodeString
.data:000000014001E980 dq 0C5FAA7F4h
.data:000000014001E988 dq offset kernelbase_GetSystemDirectoryW
.data:000000014001E990 dq 0BB1877C8h
.data:000000014001E998 dq offset kernelbase_CreateFileW
.data:000000014001E9A0 dq 189B0ED3h
.data:000000014001E9A8 dq offset kernelbase_CreateFileMappingW
.data:000000014001E9B0 dq 3003FE11h
.data:000000014001E9B8 dq offset kernelbase_MapViewOfFile
.data:000000014001E9C0 dq 592687B5h
.data:000000014001E9C8 dq offset kernelbase_UnmapViewOfFile
.data:000000014001E9D0 dq 0BE9F995Fh
```

그림 14. API 동적 호출

랜섬웨어 실행에 필요한 함수인 API를 동적으로 가져온다. 현재 프로세스에서 사용하는 DLL의 함수를 하나씩 순회하며 필요한 함수 혹은 DLL인지 구별한 뒤에 함수나 DLL의 시작 주소를 저장한다. 함수를 비교하기 위해 커스텀 해시 알고리즘을 통해 함수명에 대한 해시 값을 생성하고, 랜섬웨어에 저장된 해시 리스트에 생성된 해시 값이 존재하는지 확인하는 방식을 사용한다. 만약 일치하는 해시가 존재한다면, 해당 해시 값 다음에 API의 주소를 저장한 뒤 사용한다. 기존 LockBit Green에서는 해시 알고리즘으로 MurmurHash2A를 사용했다.

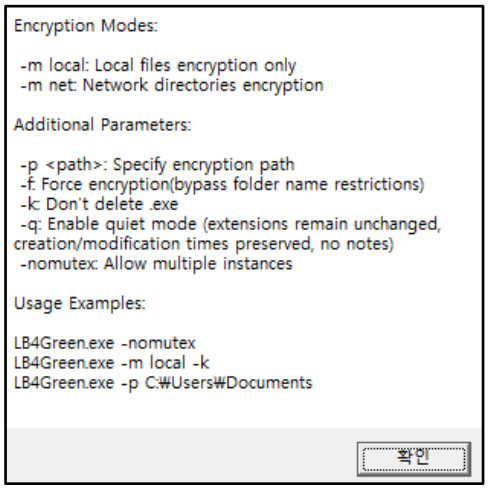


그림 15. LockBit Green 4.0 --help 메시지 박스

LockBit Green 4.0에는 다양한 실행 인자가 존재한다. 실행 인자는 인코딩된 상태로 저장되어 있으며, 비교 직전에 디코딩한 후 랜섬웨어 실행 인자와 비교한다. "--help"를 사용하면 각 실행 인자를 설명하는 메시지 박스를 출력한다. 기존 LockBit Green의 경우, 중복 실행 방지 비활성화 옵션인 "–nomutex"가 항상 활성화되어 있었다. 파일 암호화 경로 지정 옵션인 "–p"는 두 버전 모두 동일한 기능을 제공하지만, 그 외에는 여러 변경점이 확인됐다. 자세한 실행 인자는 아래 표와 같다.

<table>
<tr><th colspan="2">LockBit Green (2023)</th><th colspan="2">LockBit Green 4.0</th></tr>
<tr><th>실행 인자</th><th>설명</th><th>실행 인자</th><th>설명</th></tr>
<tr><td>-p <path></td><td>암호화 경로 지정</td><td>-p <path></td><td>암호화 경로 지정</td></tr>
<tr><td>-m [mode]</td><td>all: 로컬, 네트워크, 백업
local: 로컬 디스크 암호화
net: 네트워크 저장소 암호화
backups: 백업 파일 삭제</td><td>-m [mode]</td><td>all: 로컬, 네트워크
local: 로컬 디스크 암호화
net: 네트워크 저장소 암호화</td></tr>
<tr><td>-nomutex</td><td>중복 실행 방지 비활성화
(인자 상관 없이 항상 활성화)</td><td>-nomutex</td><td>중복 실행 방지 비활성화</td></tr>
<tr><td>-log <path></td><td>로그 파일 생성</td><td colspan="2" rowspan="2">-</td></tr>
<tr><td>-size <percent></td><td>부분 암호화 비율 설정
(입력한 값과 상관 없이 50% 고정)</td></tr>
<tr><td colspan="2" rowspan="4">-</td><td>-f</td><td>암호화 예외 항목 무시</td></tr>
<tr><td>-h / --help</td><td>실행 방식 설명 출력</td></tr>
<tr><td>-k</td><td>자가 삭제 비활성화</td></tr>
<tr><td>-q</td><td>확장자 미변경
랜섬노트 미생성</td></tr>
</table>

표 1. LockBit Green 실행 인자 비교

또한 공격 대상 환경을 파악한 후 프로그램 중단 여부를 결정한다. 우선, 대상 장비의 키보드 언어 식별자를 확인한다. 만약 0x419(러시아어)를 사용하는 장비인 경우 랜섬웨어 실행을 중단한다.

원활한 파일 암호화를 위해서 특정 서비스가 실행 중이라면 해당 서비스를 강제로 종료한다. 서비스 종료 대상은 4Bytes 길이의 해시 값 형태로 총 48개가 저장되어 있다. 현재 시스템의 서비스 목록에 접근한 뒤 모든 서비스의 이름을 하나씩 가져온다. Custom 해시 알고리즘을 사용해 서비스명을 해시 값으로 생성한 다음, 서비스 종료 대상에 저장된 해시 값과 하나씩 비교한다. 만약 해시 값이 리스트에 존재한다면, 해당 서비스의 설정을 변경해 강제로 비활성화를 진행한다. 해시 값은 역산이 불가능해 모든 종료 대상 서비스를 확인할 수 없지만, 백업 복사본을 관리하는 서비스인 VSS를 비활성화하는 것이 확인됐다.

```
iptable = (v1316.m128i_i64[0])(v1010);// _inet_ntoa
v1316.m128i_i8[4] = 0x3A;
v1316.m128i_i32[0] = 0x14080D0B;
v1031 = sub_7FF6EACF1890(&v1316);// decode 172.
v1032 = sub_7FF6EACE3373(iptable, v1031);
v1316.m128i_i8[8] = 0x3A;
v1316.m128i_i64[0] = 0x14020C0B1408030Bi64;
v1033 = sub_7FF6EACF18C0(&v1316);// decode 192.168.
v1034 = sub_7FF6EACE3373(iptable, v1033);
v1316.m128i_i32[0] = 0x3A140A0B;
v1035 = sub_7FF6EACF0950(&v1316);// decode 10.
v1036 = sub_7FF6EACE3373(iptable, v1035);
v1316.m128i_i8[4] = 0x3A;
v1316.m128i_i32[0] = 0x14030C0B;// decode 169.
v1037 = sub_7FF6EACF1890(&v1316);
v1038 = sub_7FF6EACE3373(iptable, v1037);
if ( v1032 == iptable || v1034 == iptable || v1036 == iptable || v1038 == iptable )
```

그림 16. IP 주소 문자열 디코딩

LockBit Green 4.0은 현재 시스템의 네트워크 인터페이스를 확인한 뒤, 특정 IP 대역으로 내부 전파를 시도한다. IP 주소와 MAC 주소가 맵핑된 ARP 테이블을 조회한 뒤 해당 테이블에서 IP 주소 목록만 가져온다. 이후 내부 IP 대역으로 활용되는 172.x.x.x, 192.168.x.x, 10.x.x.x, 169.x.x.x 문자열을 디코딩 후, 가져온 IP 주소 목록에 존재하는지 확인한다. 만일 해당하는 IP 주소가 존재한다면 해당 IP 주소에 소켓 연결을 시도한 다음 전파를 시도한다.

"-m", "-f" 실행 인자에 따라 파일 암호화의 범위를 지정한다. 별도로 인자를 지정하지 않거나 "-m all"을 사용하면 로컬 드라이브와 네트워크 리소스 모두 암호화를 진행한다. "-m local"을 사용하면 로컬 드라이브만 암호화하고 "-m net"을 사용하면 네트워크 리소스만 암호화한다. 이전 버전에서 사용하던 "-m backups"인자는 더 이상 사용되지 않는다. 또한 미리 설정된 암호화 예외 디렉터리와 파일 확장자는 제외하고 암호화를 진행하는데, "-f" 실행 인자를 사용하면 해당 예외 항목도 포함해서 암호화를 진행한다. 각 버전별 예외 항목은 아래 표와 같다.

LockBit Green (2023)	LockBit Green 4.0
Windows, $Recycle.Bin, Boot, **temp, winnt, temp, thumb, Trend Micro, perflogs,** System Volume Information	Windows, $Recycle.Bin, Boot, **All Users**, **Chocolatey**, **Microsoft Visual Studio**, System Volume Information

표 2. 암호화 예외 폴더

LockBit Green (2023)	LockBit Green 4.0
!!!-Restore-My-Files-!!!, CONTI_LOG.txt, *.exe, *.lnk, *.dll, *.sys, ***.msi, *.bat**	**Iconcache.db, thumbs.db,** *.exe, *.lnk, *.dll, *.sys, ***.dpl**

표 3. 암호화 예외 파일 및 확장자

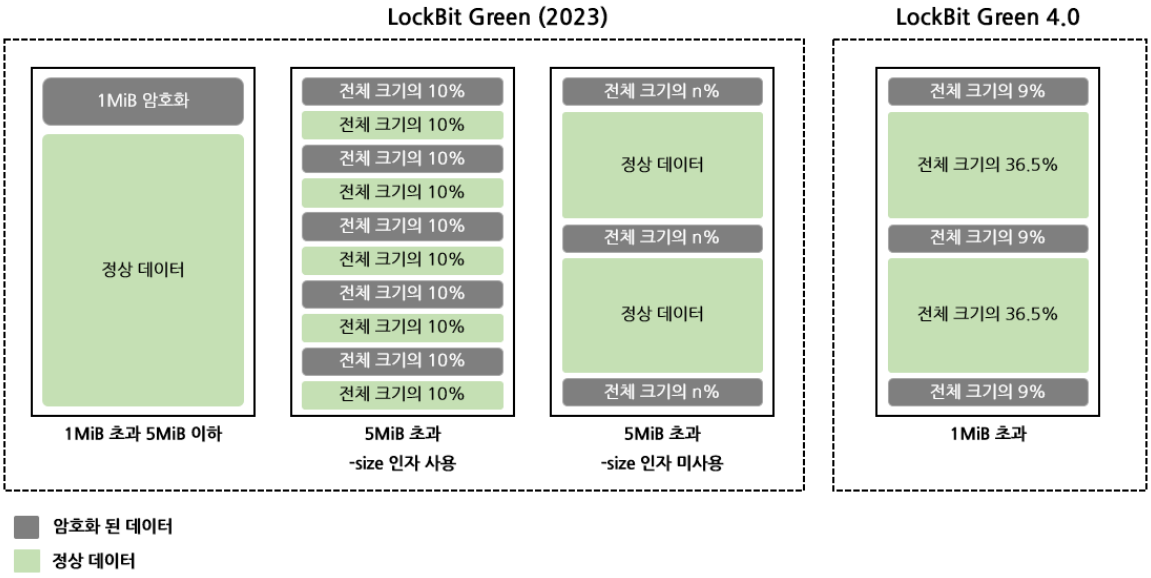


그림 17. LockBit Green 버전별 부분 암호화 방식

암호화 대상 폴더에는 먼저 복호화한 랜섬노트를 저장하고, 그 후 각 파일을 멀티스레드 방식으로 암호화한다. 파일의 암호화는 크기에 따라 전체 암호화와 부분 암호화로 구분되며, 암호화 방식은 버전마다 차이가 있다. 이전 버전에서는 1MiB 이하의 파일은 전체 암호화를 진행하고, 1MiB 초과 5MiB 이하의 파일은 첫 1MiB만 암호화한다. 5MiB 초과 파일은 부분 암호화를 진행하는데, 이때 부분 암호화 방식은 "-size" 인자 사용 여부에 따라 달라진다. "-size" 를 사용하면 파일을 10개의 블록으로 나누고, 전체 파일 크기의 50%에 해당하는 5개의 블록만 암호화한다. "-size" 를 사용하지 않으면 공격자가 사전에 설정한 비율대로 파일의 처음, 끝, 중간 부분만 암호화된다. 최신 버전인 LockBit Green 4.0에서는 1MiB 이하의 파일은 전체 암호화를 진행하고, 1MiB 초과 파일은 전체 파일 크기의 27%만 암호화한다. 부분 암호화는 파일 크기 기준으로 9%씩 총 3개의 영역(처음, 중간, 끝)을 암호화하는 방식으로 진행된다.

두 버전 모두 파일 암호화는 랜덤한 32바이트의 키를 생성한 다음 ChaCha20 알고리즘으로 암호화를 진행한다. 그러나 키 보호 및 저장 방식에는 차이가 있다. 이전 버전은 사용한 키를 RSA 알고리즘으로 보호하고 암호화된 파일의 맨 끝에 저장하지만, LockBit Green 4.0은 Curve25519 알고리즘으로 만든 공유 비밀로 키를 보호한 뒤 암호화된 파일의 맨 앞에 저장한다.

LockBit 4.0 랜섬웨어 대응방안

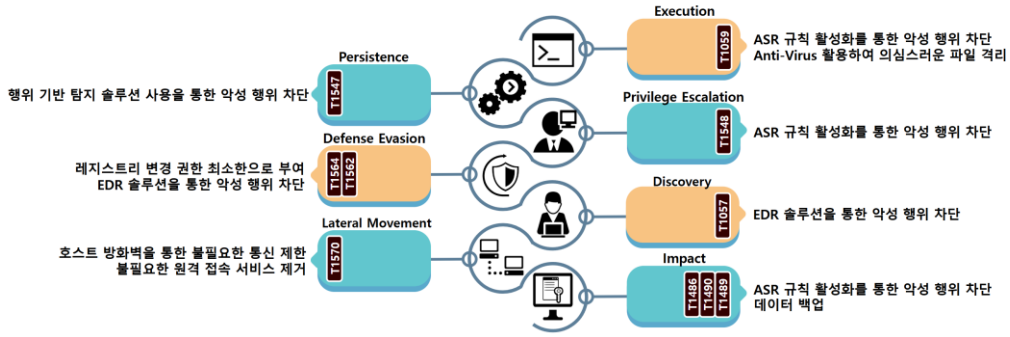


그림 18. LockBit 4.0 랜섬웨어 대응방안

LockBit 4.0 랜섬웨어는 PowerShell Script 를 활용해 랜섬웨어를 실행한다. 별도의 랜섬웨어 파일 생성 없이 메모리 상에서 실행하는 방식을 사용하는 경우도 확인됐다. 따라서 ASR [8] 규칙 활성화를 통해 비정상적인 프로세스를 차단해 악성 행위를 막을 수 있다. 또한 랜섬웨어를 시작 프로그램으로 등록하기 때문에 이를 행위 기반 탐지 솔루션을 사용해 악성 행위를 차단할 수 있다.

Windows Defender 서비스를 비활성화하고 Windows 이벤트 로그 기능 또한 비활성화를 시도한다. 이러한 경우 이벤트 로그를 권한이 있는 사용자만 접근할 수 있도록 사전에 설정해 두거나, 이벤트 로그를 원격 저장소에 별도로 저장해 보존할 수 있다. 이외에도 EDR[9] 솔루션을 통해 공격자가 사용하는 특정 프로세스를 차단해 악성 행위를 막을 수 있다.

랜섬웨어를 내부 네트워크에 전파하기 위해 Windows 의 네트워크 관련 API 인 Winsock 을 활용해서 내부 대역에 전파를 시도한다. 현재 시스템에서 네트워크 IP 주소 테이블을 조회한 뒤 내부 대역으로 사용하는 172.x.x.x, 192.168.x.x, 10.x.x.x, 169.x.x.x 대역의 주소가 발견되면 네트워크 연결 및 랜섬웨어 전파를 시도한다. 때문에 호스트 방화벽을 통해 불필요한 통신을 제한할 수 있다.

파일 암호화에 앞서 사용자가 임의로 복구하는 것을 방지하기 위해 백업 복사본을 삭제하고, 백업 복사본을 관리하는 VSS 서비스를 비활성화한 뒤 파일 암호화를 진행한다. ASR 규칙 활성화를 통해 백업 복사본을 삭제하는 프로세스와 파일을 암호화는 것을 차단할 수 있다. 로컬 디스크뿐 아니라 네트워크 공유 폴더도 암호화를 진행하기 때문에 불필요한 네트워크 공유 기능을 비활성화하고, 백업 복사본의 경우 별도의 네트워크나 저장소에 소산 백업해야 한다.

[8] ASR (Attack Surface Reduction): 공격자가 사용하는 특정 프로세스와 실행 가능한 프로세스를 차단하는 보호 기능

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

IoCs

Hash(SHA-256)
563cd800e80253a7051ea8a1bd690d123cf7820c355addeeaaabaa227984d9cb
82d89a75d80e80e4be42c9eb79e401558c9fa3175648cd0c0467f2de1a07a908
3552dda80bd6875c1ed1273ca7562c9ace3de2f757266dae70f60bf204089a4a
20dd91f589ea77b84c8ed0f67bce837d1f4d7688e56754e709d467db0bea03c9
33376f74c2f071ff30bab1c2d19d9361d16ebaa3dee73d3b595f6d789c15f620
2f5051217414f6e465f4c9ad0f59c3920efe8ff11ba8e778919bac8bd53d915c
48e2033a286775c3419bea8702a717de0b2aaf1e737ef0e6b3bf31ef6ae00eb5
21e51ee7ba87cd60f692628292e221c17286df1c39e36410e7a0ae77df0f6b4b
9733092223c428fc0e44a90b01c7f77a97bb1205def8be1224ac68969182638e
a33f21d28bd83a9501257ee727c46486989bdfea6d5cb9f1c12c9a67296b21b1
0ace4e1158ab5b7723493f39d6949309e00e4a71804f0b09e33d5d48a28cb061
36f48ef3776c01d63a2fd594d52dfb7402ea634162fd079b0d942367a2fbed56

■ 참고 사이트

• 미국 법무부(https://www.justice.gov/opa/pr/phobos-ransomware-affiliates-arrested-coordinated-international-disruption)

• BankInfoSecurity(https://www.bankinfosecurity.com/leaked-black-basta-chat-logs-show-banality-ransomware-a-27573)

• CyberSecurityDive (https://www.cybersecuritydive.com/news/leaked-ransomware-chat-logs-reveal-black-bastas-targeted-cves/741129/)

• CSO Online (https://www.csoonline.com/article/3822338/authorities-seize-phobos-and-8base-ransomware-servers-arrest-4-suspects.html)

• The Record (https://therecord.media/oakland-confirms-massive-second-data-leak)