

LockBit 5.0 심층 분석 보고서: 동작 원리와 대응 방안

A asec.ahnlab.com/ko/91834

ATCP

January 4, 2026

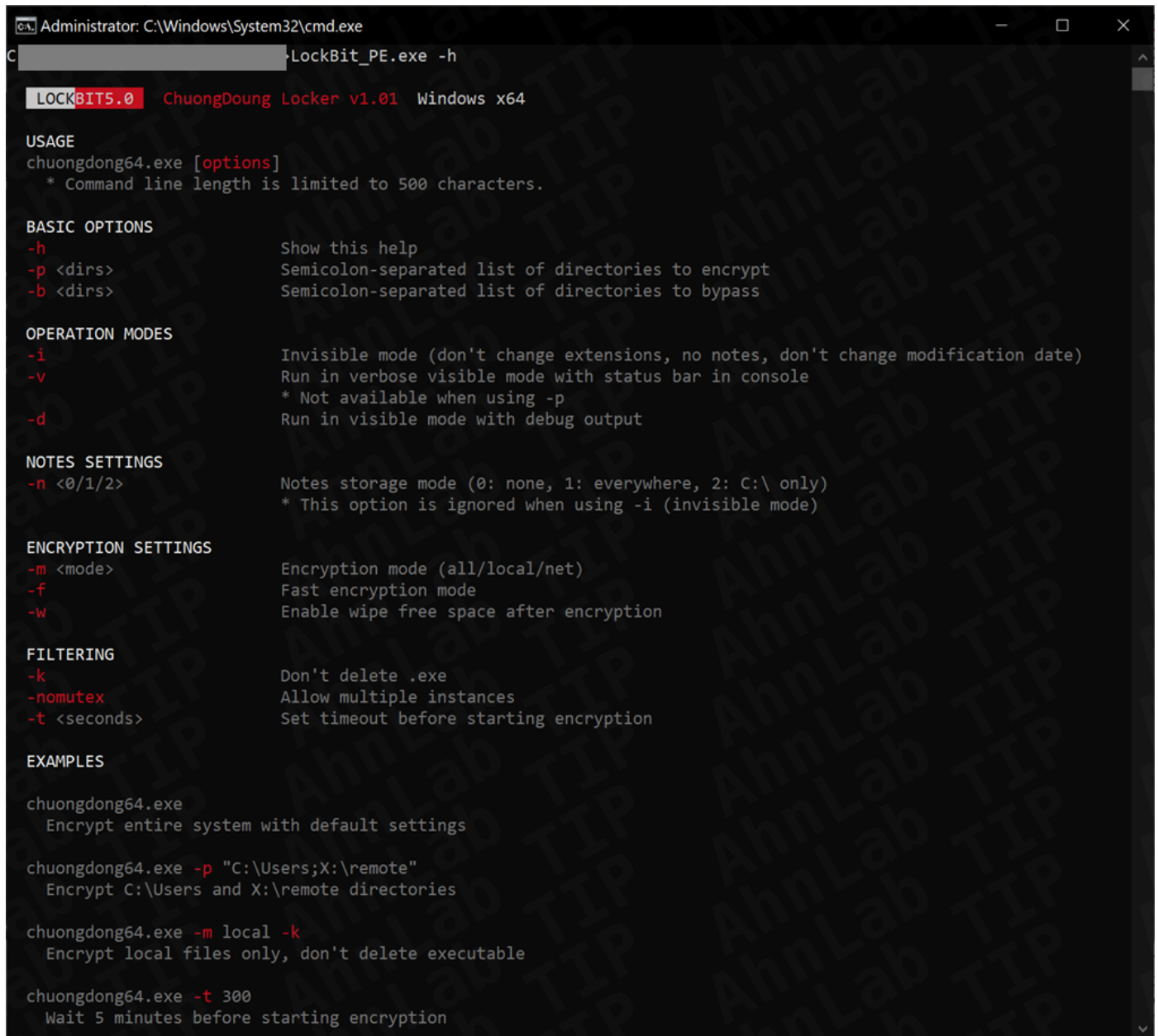


LockBit(락빗, 록빗)은 2019년 9월 처음 등장한 이후 세계에서 가장 악명 높고 활발히 활동하는 Ransomware-as-a-Service(RaaS) 조직 중 하나로 알려져 있다. LockBit은 RaaS 모델로 운영되며 정교한 암호화 기술과 자동화된 확산 능력을 특징으로 한다. 초기 침입은 주로 취약점 공격, 무차별 대입, 피싱, 또는 유출된 로그인 정보를 통해 이루어지며 공격은 초기 접근, 측면 이동 및 권한 상승, 랜섬웨어 배포의 3단계 절차를 따른다. 또한 데이터 유출을 위해 Stealbit 도구를 사용한다. 2021년 8월부터 2022년 8월까지 알려진 랜섬웨어 공격의 30.25%, 2023년에는 약 21%를 차지했으며 이로 인한 몸값 지불과 복구 비용은 수십억 달러에 달한다. 법 집행 기관의 노력에도 불구하고 LockBit은 여전히 전 세계 사이버 보안에 심각한 위협을 가하고 있다.

LockBit 5.0 랜섬웨어 그룹은 DLS 사이트를 운영하고 있으며, 해당 그룹이 침해하여 데이터 확보에 성공한 피해 기업들의 목록이 공개되어 있다. 국내 기업은 포함되지 않았지만, 다수의 해외 기업들이 피해를 입은 것으로 확인된다. IT, 전자, 로펌, 교회 등 분야를 가리지 않고 랜섬웨어 공격을 수행하는 것으로 확인된다.

분석 내용

LockBit 5.0은 실행 시 다양한 인자값을 받을 수 있으나, 인자가 없어도 정상적으로 동작한다. 복구를 방지하기 위해 VSS 관련 서비스를 종료하며, Packing과 난독화를 적용해 정적 분석을 어렵게 한다. 또한 ChaCha20-Poly1305와 X25519+BLAKE2b 기반 키 교환 알고리즘을 사용하고, 암호화된 파일은 로컬 시스템 정보만으로는 복호화가 불가능하며 파일 크기에 따라 암호화 비율이 달라진다.



```
Administrator: C:\Windows\System32\cmd.exe
C:\>LockBit_PE.exe -h

LOCKBIT5.0 ChuongDong Locker v1.01 Windows x64

USAGE
chuongdong64.exe [options]
* Command line length is limited to 500 characters.

BASIC OPTIONS
-h Show this help
-p <dirs> Semicolon-separated list of directories to encrypt
-b <dirs> Semicolon-separated list of directories to bypass

OPERATION MODES
-i Invisible mode (don't change extensions, no notes, don't change modification date)
-v Run in verbose visible mode with status bar in console
  * Not available when using -p
-d Run in visible mode with debug output

NOTES SETTINGS
-n <0/1/2> Notes storage mode (0: none, 1: everywhere, 2: C:\ only)
  * This option is ignored when using -i (invisible mode)

ENCRYPTION SETTINGS
-m <mode> Encryption mode (all/local/net)
-f Fast encryption mode
-w Enable wipe free space after encryption

FILTERING
-k Don't delete .exe
-nomutex Allow multiple instances
-t <seconds> Set timeout before starting encryption

EXAMPLES
chuongdong64.exe
  Encrypt entire system with default settings

chuongdong64.exe -p "C:\Users;X:\remote"
  Encrypt C:\Users and X:\remote directories

chuongdong64.exe -m local -k
  Encrypt local files only, don't delete executable

chuongdong64.exe -t 300
  Wait 5 minutes before starting encryption
```

[그림 1] LockBit 5.0 도움말 정보 표시

암호화 준비

Temp 경로의 파일을 삭제하는데 이는 암호화 대상이 주로 사용자의 가치 있는 파일이기 때문에, 캐시나 임시 데이터로 구성된 Temp 경로의 불필요한 파일을 제거하여 암호화 속도를 향상시키기 위한 목적이다.

삭제되는 Temp 폴더 경로

C:\Users\All Users\AppData\Local\Temp

C:\Users\Default\AppData\Local\Temp

C:\Users\Public\AppData\Local\Temp

C:\Users\{사용자명}\AppData\Local\Temp

[표 1] 삭제되는 Temp 폴더 경로

암호화 과정에서의 충돌을 방지하고 백업 및 보안 솔루션의 동작을 차단하기 위해 시스템 핵심 서비스의 자동 실행을 비활성화하고 즉시 중지한다. 중지 대상 서비스는 해시 값으로 하드코딩되어 있다. 서비스명이 식별된 항목은 [표 2]에, 식별되지 않은 항목은 [표 3]에 정리하였다.

중지 대상 서비스

BackupExecVSSProvider	VSS	vmms
WSearch	EdgeUpdate	AcrSch2Svc
VeeamTransportSvc	MicrosoftEdgeElevationService	BackupExecAgentAccelerator
AcronisAgent	BackupExecJobEngine	GxFWD
VeeamNFSSvc	BackupExecRPCService	edgeupdatem
BackupExecManagementService	GxCVD	

[표 2] 중지 대상 서비스

중지 대상 서비스

0x826AC445, 0x83143F70, 0xFE56F16, 0x10D06066, 0xBEC3470C, 0xC347B317, 0xCA6C4394, 0x5EF504FC, 0x9757464E, 0x9A768D62, 0xA1816235, 0x369D7114, 0xE11A285D, 0xE5C9CC93, 0x732AA0C0, 0x7ABD1404, 0x9439954E, 0x9655130F, 0x23FA53E5, 0x2C1F8E5F, 0xDBECA3C3, 0xDC04E8C, 0x60B29D14, 0x62C32884, 0x6337AD82, 0xA8F16BAB, 0x41278147, 0x4292EDD8, 0xE7AA4057, 0xE7BF305D, 0x7DD43601

[표 3] 중지 대상 서비스

암호화 전 시스템의 주요 파일을 암호화하여 시스템의 안정성이 파괴되는 것을 방지하기 위해 특정 파일과 폴더를 암호화 대상에서 제외한다. 시스템 운영에 필수적인 Windows 폴더와 exe, dll, sys 같은 실행 파일이 제외된다.

암호화 제외 대상 디렉토리

Windows, \$Recycle.Bin, AllUsers, Boot, chocolatey, Microsoft Office, Microsoft Visual Studio, Windows Kits, WindowsApps, VisualStudio, System Volume Information, Microsoft\Windows

[표 4] 암호화 제외 대상 디렉토리

암호화 제외 대상 파일

iconcache.db, thumbs.db

[표 5] 암호화 제외 대상 디렉토리

암호화 제외 대상 확장자

exe, lnk, dll, cpl, sys, 암호화시 변경되는 확장자

[표 6] 암호화 제외 대상 디렉토리

암호화 시 확장자는 고정되어 있지 않으며, 난수를 기반으로 커스텀 해시 함수를 사용해 8바이트 길이의 확장자를 100개 생성한 후 순차적으로 적용한다. 이 확장자 리스트는 LockBit 5.0 랜섬웨어가 실행될 때마다 새롭게 생성된다.

Address	Hex	ASCII
---------	-----	-------

[그림 2] 생성된 확장자 목록

파일 암호화

LockBit 5.0 랜섬웨어는 파일 암호화 시 ChaCha20-Poly1305 알고리즘을 사용하며, 키 교환에는 X25519 + BLAKE2b를 적용한다. 시스템 시간과 메모리 정보를 기반으로 32바이트 난수를 두 개 생성하고, 2번 난수 값의 첫 바이트와 마지막 바이트를 연산하여 개인키로 활용한다. 이후 해당 피해자 개인키로 타원곡선 암호화 알고리즘을 통해 피해자 공개키를 생성하고, 피해자 개인키와 공격자의 공개키와 결합해 공유 비밀(Shared Secret) 값을 도출한다.

이후, 파일 크기가 0x5000000 이하인 경우 난수1을 BLAKE2b 해시 알고리즘으로 처리해 해시 값을 생성하고, 이를 기반으로 ChaCha20 키 스트림을 생성한다. 생성된 키 스트림은 상위 16바이트와 하위 16바이트를 결합해 32바이트 키를 형성하며, 이 키가 파일 암호화 키 스트림 생성에 사용된다. 해당 키를 이용해 64바이트 길이의 ChaCha20 키 스트림을 생성하고, 암호화 대상 데이터와 XOR 연산을 수행하여 최종적으로 파일을 암호화한다.

```

}
sub_1400115B0(&v541, 0x20u);           // 32바이트 난수 생성. 난수1
sub_1400115B0(v442.m128i_i32, 0x20u);   // 32바이트 난수 생성. 난수2
LOBYTE(v439) = v442.m128i_i8[2];
LOBYTE(v526) = v442.m128i_i8[1];
__SET_PAIR__(v441, v440, *(&v442.m128i_i16[1] + 1));

v224 = v445;
v577.m128i_i8[14] = v445;
v225 = v442.m128i_i8[0] & 0xF8;         // 난수2, 첫 바이트 연산
v576.m128i_i64[0] = v442.m128i_i64[0] & 0xFFFFFFFFFFFFFFFF8uLL;
v226 = v446 & 0x3F | 0x40;             // 난수2, 마지막 바이트 연산

v226 = v446 & 0x3F | 0x40;             // 난수2, 마지막 바이트 연산
v577.m128i_i8[15] = v226;             // 공개키 생성
sub_140014500(&v539, &v576, dword_140100230); // 타원곡선 암호화. a1 = 출력 버퍼, a2 = private key, a3 = 9(base point)
v576.m128i_i8[1] = v526;

v576.m128i_i8[0] = v225;
v577.m128i_i8[15] = v226;             // Shared Secret
sub_140014500(&v543, &v576, dword_14010E620); // 타원곡선 암호화. a1 = 출력 버퍼, a2 = private key, a3 = 공격자 공개키
s1128 = _mem_load_size(&mmword_1401001F0,
v576.m128i_i64[1] = s1128.m128i_i64[1];

```

CSPRNG

Private Key Generation

Public Key Generation

Shared Secret Generation

[그림 3] 난수, 개인키, 공개키, 공유 비밀 생성

암호화가 완료된 후, 암호화된 데이터의 끝에 추가 정보를 기록한다. 추가되는 데이터는 파일 크기, 파일 크기를 커스텀 해시로 변환한 값, 난수1을 ChaCha20으로 암호화한 값, Poly1305 값, 그리고 피해자의 공개키이다.

	test.2176b510f1c0f077																
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text

[그림 4] 파일 크기가 0x5000000 이하의 파일 구조

파일 크기가 0x5000000을 초과하는 경우, 데이터를 0x800000 단위로 분할해 암호화한 뒤, 각 조각의 하위 0x80 바이트를 커스텀 해시 함수로 처리해 8바이트 해시 값을 생성하고, 이를 암호화된 파일 데이터 뒤에 추가한다.

[그림 5] 파일 크기가 0x50000000초과시 파일의 구조

랜섬노트

랜섬노트에는 기업 네트워크의 취약점을 악용해 시스템을 침해하고, 접근 가능한 모든 데이터를 암호화했음을 명시하고 있다. 공격자는 자체 복구 시도나 외부 복구 서비스 이용 시 복호화가 불가능해져 영구적인 데이터 손실이 발생할 수 있다고 경고한다. 또한 피해 사실을 외부에 알리거나 법집행기관에 신고할 경우, 복호화 키를 삭제하고 유출된 데이터를 다크웹에 공개하거나 판매하겠다고 위협한다.



[그림 6] 랜섬노트 (ReadMeForDecrypt.txt)

안랩 대응 현황

안랩 제품군의 진단명과 엔진 날짜 정보는 다음과 같다.

V3

Ransomware/Win.LockBit.C5798524 (2025.09.17.00)

Ransomware/Win.LockBit.C5799278 (2025.09.19.00)

EDR

Ransom/EDR.Decoy.M2470 (2022.09.29.03)

MD5

95daa771a28eaed76eb01e1e8f403f7c

97e97e8cde5cc795b4d0a1fb7202b5ed

c15a79d4b3c17bdb01edb097bae53212

c462c6b02b35df2910689947c5090fae

cd6e182fe655724f3d8e711b451a2e93

추가 IoC는 ATIP에서 제공됩니다.

