Keep up with Ransomware

기존 랜섬웨어 코드를 재활용한 BlackField 랜섬웨어

■ 개요

2025 년 10 월 랜섬웨어 피해 사례 수는 지난 9 월(583 건) 대비 약 37% 증가한 799 건으로 집계됐다. 기존 주요 그룹인 Qilin·Sinobi 등의 지속적인 공격 활동에 더해, 10 월 새롭게 등장한 여러 신규 랜섬웨어 조직이 공격에 가세하면서 전체 피해 규모가 확대된 것으로 보인다.

Clop 그룹은 Oracle E-Business Suite 의 신규 취약점(CVE-2025-61882)을 악용해 침투한 것이 확인되었다. 해당 취약점은 인증 없이 페이로드[1] 가 포함된 POST 요청만으로 서버 내부 기능 호출이 가능하며, 이를 통해 공격자는 원격에서 코드를 실행할 수 있다. Clop 은 과거에도 취약점을 악용한 대규모 공격을 반복해왔다. 2023 년도에는 MOVEit Transfer 의 SQL Injection 취약점(CVE-2023-34362, CVE-2023-35036, CVE-2023-35708)을 악용했으며, 2024 년도에는 Cleo 사의 파일 전송 솔루션 제품군에서 발견된 인증 우회 취약점(CVE-2024-55956)을 악용해 대규모 침해를 발생시켰다.

한편, 취약점을 악용한 침투 사례는 Clop 그룹 이외에도 타 랜섬웨어 그룹에서 지속적으로 확인되고 있다. Medusa 그룹은 Fortra GoAnywhere MFT 에서 발생한 취약점(CVE-2025-10035)을 악용한 사례가 보고됐다. 이 취약점은 사용자 인증 없이 특정 요청을 전달할 경우, 서버가 이를 오처리 하도록 유도해 공격자의 명령을 실행할 수 있게 되는 취약점이다. 공격자는 이를 악용해 악성 스크립트 실행과 내부 데이터 탈취를 수행했으며, 최종적으로 랜섬웨어까지 실행했다.

[1] 페이로드(payload): 공격자가 악의적인 실행을 유도하기 위해 첨부하는 데이터/명령

SLSH 그룹은 2025 년 8 월 처음 등장했다. 외부적으로는 Lapsus$와 Scattered Spider 그룹이 ShinyHunters 와 합류해 구성된 연합체인 것처럼 홍보하고 있다. 그러나 실제로는 ShinyHunters 를 중심으로 두 그룹의 일부 구성원만 참여한 형태로, 운영자가 다중 닉네임을 활용해 연합체처럼 보이도록 위장한 것으로 확인된다. 이들은 자체 구축한 다크웹 데이터 유출 사이트와 운영 인프라 등을 EaaS(Extortion-as-a-Service) [2] 형태로 외부 공격자에게 대여하고 있다. 이는 널리 알려진 RaaS(Ransomware-as-a-Service) [3] 모델과 유사하지만, 데이터 탈취와 협박에 중점을 둔다는 점에서 EaaS 와는 차이가 있다. SLSH 는 10 월 초 데이터 유출 사이트를 개설해 탈취한 정보를 게시하였으나, 10 월 11 일 법 집행기관의 압박이 강화되었다는 이유로 2026 년까지 활동을 중단하겠다고 발표했다. 이에 따라 해당 그룹이 운영하던 다크웹 유출 사이트는 현재 비활성화된 상태다.

한편 SLSH 의 운영진 중 하나인 ShinyHunters 는 과거 BreachForums 의 관리자 역할을 수행했던 인물로 유명하다. BreachForums 는 2022 년부터 2024 년까지 법집행기관의 압박으로 여러 차례 폐쇄되었다가, 부활이라는 명목으로 반복 등장한 바 있다. 2025 년 하반기에 다시 모습을 드러낸 BreachForums 는 복구된 것처럼 보였으나, ShinyHunters 는 SLSH 텔레그램 채널을 통해 10 월 이후 해당 포럼은 더 이상 운영되지 않으며 이후 새롭게 개설되는 사이트는 법집행기관이 운영하는 허니팟일 확률이 높다고 주장하였다.

[2] EaaS(Extortion-as-a-Service): 데이터 탈취·협박을 서비스 형태로 제공하는 비즈니스 모델

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

■ 랜섬웨어 뉴스

Clop, Oracle E-Business Suite의 신규 취약점을 악용해 침투

- Oracle E-Business Suite의 신규 취약점(CVE-2025-61882)을 악용해 인증 없이 서버 내부 기능 호출 및 코드 실행을 수행
- 해당 취약점은 인증 없이 원격 코드 실행이 가능
- Clop은 2023년 MOVEit, 2024년 Cleo 파일 전송 솔루션 등 과거에도 제로데이 취약점을 통한 대규모 침해 사례가 확인됨

Medusa의 GoAnywhere MFT 취약점(CVE-2025-10035) 악용 공격

- Medusa 그룹은 Fortra GoAnywhere MFT의 취약점(CVE-2025-10035)을 악용한 것으로 확인됨
- 해당 취약점은 인증 없이 서버에 악의적 요청 가능
- 요청 처리 오류로 인해 공격자의 악의적인 명령 실행이 가능

SLSH, EaaS 기반으로 활동하는 신규 위협 그룹 등장

- Lapsus$, Scattered Spider, ShinyHunters의 연합체를 주장하지만 실제로는 소수 운영자가 다중 닉네임으로 운영함
- 이들은 RaaS 모델이 아닌 데이터 탈취·협박 중심의 EaaS 모델을 사용함
- 10월 초 데이터 유출 사이트 개설 후 활동 시작 이후 법 집행기관의 단속 압박 등으로 현재는 사이트가 비활성화된 상태

BreachForums 재등장에 대해 ShinyHunters는 법집행기관이 운영하는 허니팟이라 주장

- BreachForums은 2022년부터 2024년까지 여러 차례 법집행기관 압박으로 폐쇄되었으나 이후 반복적으로 재등장함
- 2025년 하반기에 다시 등장한 BreachForums은 정상 복구된 것처럼 보였지만 진위에 대한 의혹이 제기됨
- ShinyHunters는 SLSH 텔레그램을 통해 해당 사이트가 법집행기관 운영 허니팟일 가능성이 높다고 주장함

10월, 신생 그룹 9개 등장

- 전체 신규 그룹중 NasirSecurity, BrotherHood, FulcrumSec, Genesis 는 암호화가 아닌 데이터 갈취 중심
- 산업 구분 없이 무차별적 표적 공격이 증가

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

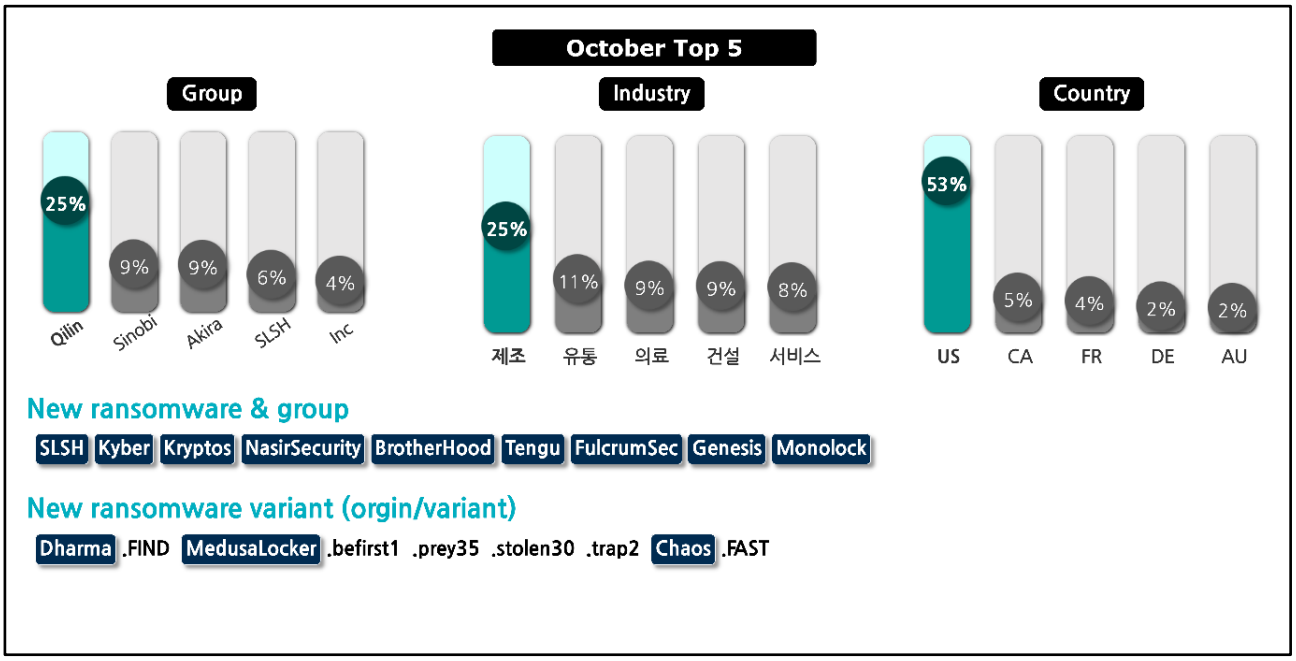


그림 2. 2025 년 10 월 랜섬웨어 위협 현황

새로운 위협

10 월에는 총 9 개의 신규 랜섬웨어 그룹이 등장했다. 이들 중 SLSH, Kyber, Kryptos, Tengu, BrotherHood, FulcrumSec, Genesis 는 자체 다크웹 유출 사이트를 운영하고 있다. 현재 Tengu 와 FulcrumSec 의 다크웹 유출 사이트는 비활성화된 상태로 확인된다.

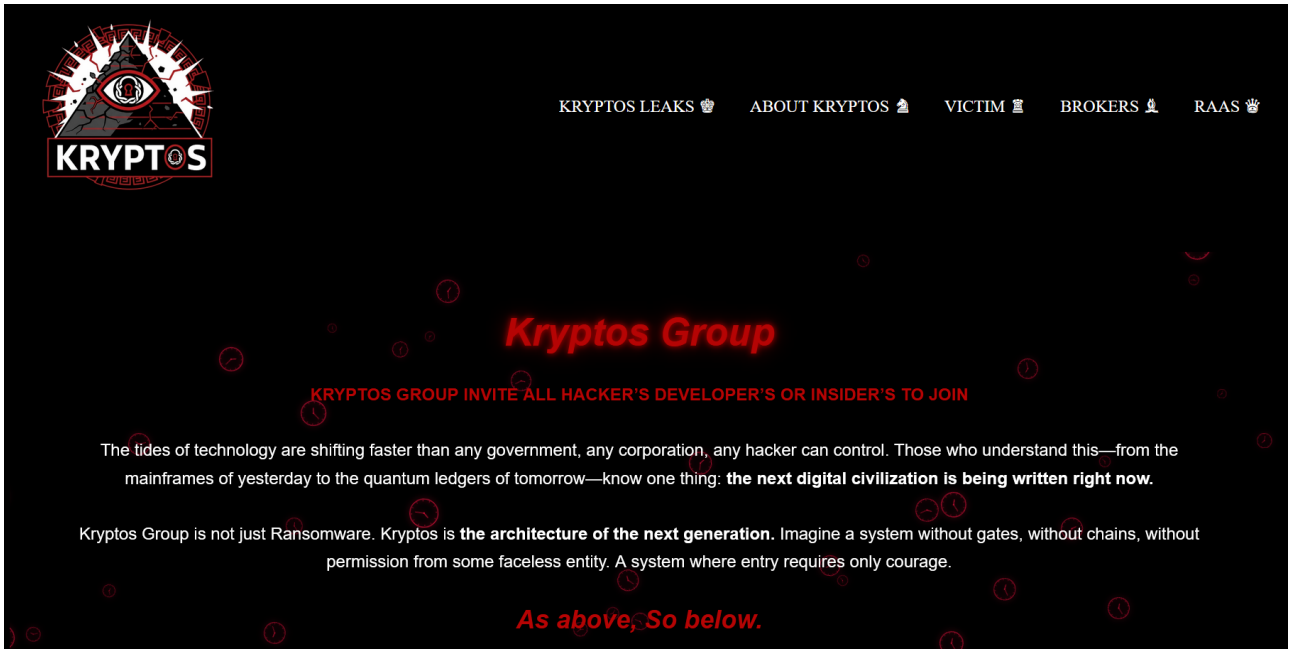


그림 3. Kryptos 의 RaaS 모집글

2025 년 10 월에 발견된 Kryptos 랜섬웨어는 현재까지 총 5 건의 피해 정보를 게시했다. 해당 그룹이 공개한 RaaS 계열사 모집 글에 따르면, 참여자는 매달 50 달러(한화 약 7 만원)의 유지비를 내야 하며 공격 성공 시 수익의 10%를 지불해야 한다고 명시되어 있다. 또한 단순히 가입 의사를 밝히는 것만으로는 계열사로 활동할 수 없으며, 가입 전 반드시 'Attack Phase'라는 테스트 절차를 통과해야 한다. 내부자·브로커·개발자 유형에 따라 서로 다른 검증 기준을 적용하는 등, 엄격한 선발 체계를 통해 운영하고 있는 것으로 분석된다.

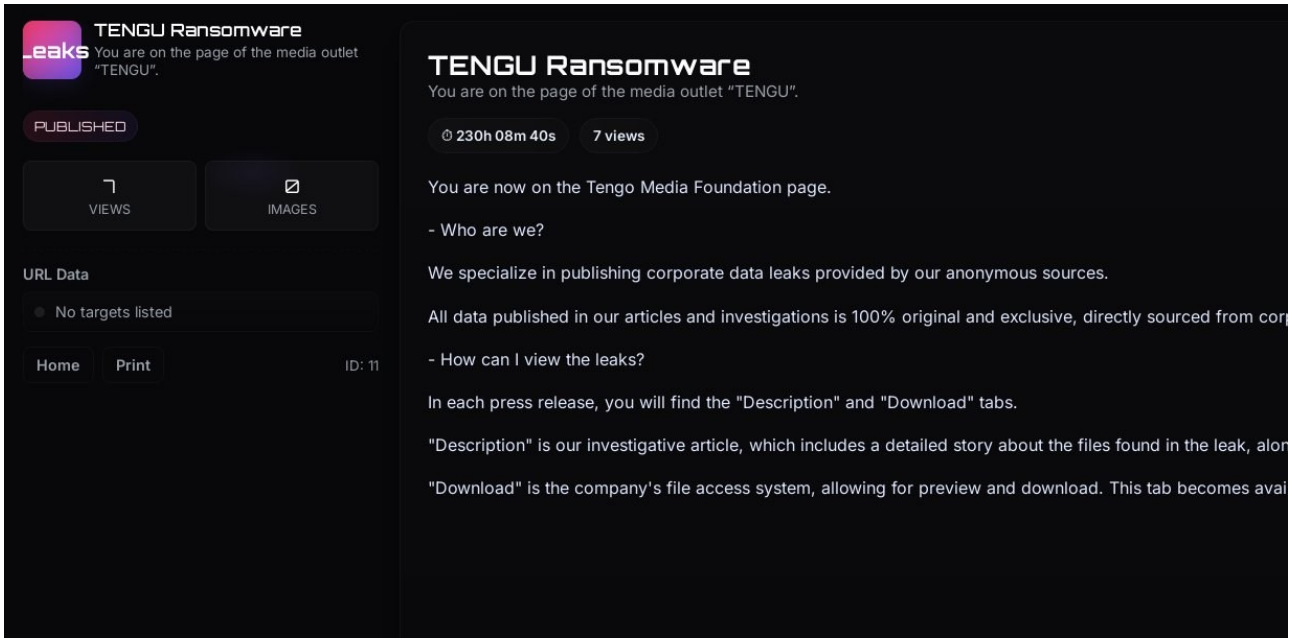


그림 4. Tengu 의 다크웹 유출 사이트

2025 년 10 월에 발견되어 현재까지 총 6 건의 피해 사례가 확인된 Tengu 랜섬웨어는, 등장 초기부터 다크웹 유출 사이트뿐만 아니라 X 에서도 활동을 홍보하며 존재감을 드러냈다. 그러나 현재 Tengu 가 운영하던 다크웹 유출 사이트는 접근이 불가능한 상태다. 이후 추가적인 공격 징후도 확인되지 않고 있다.

Top5 랜섬웨어

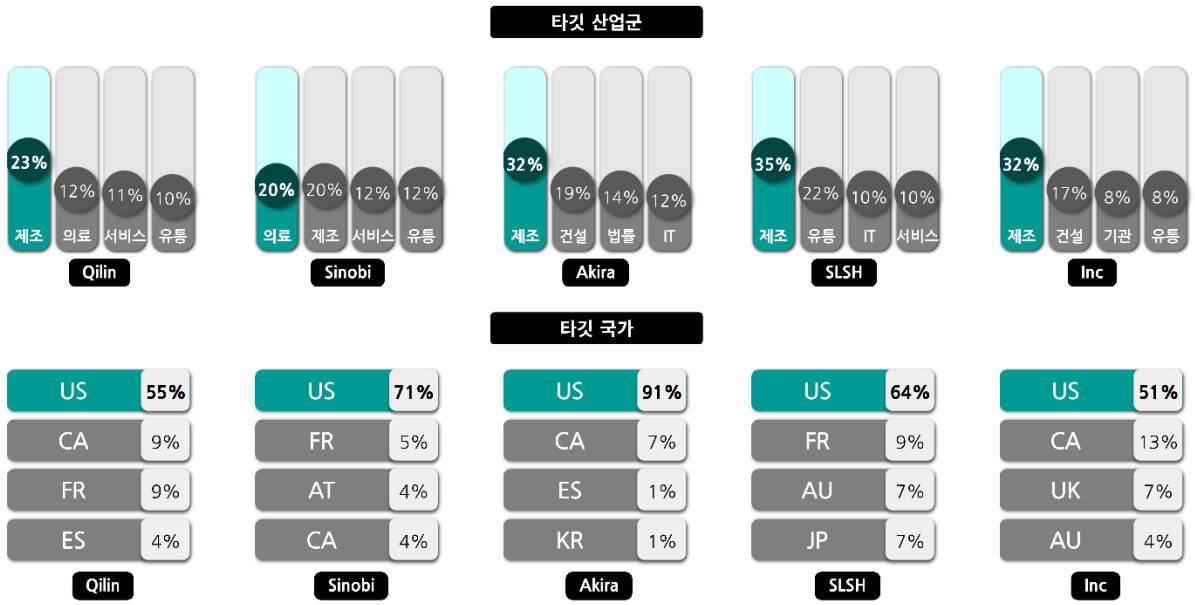


그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

일본의 음료 제조사 아사히는 Qilin 그룹의 공격을 받아 생산 라인이 일시 중단되었다. 내부 재무 문서·공급망 자료·계약 문서 등이 포함된 약 27GB 규모의 데이터가 탈취됐다. 해당 데이터는 이후 Qilin 그룹의 다크웹 유출 사이트에 공개되었다.

Sinobi 그룹은 10 월 13 일 미국 뉴저지주의 의료 센터인 Central Jersey Medical Center 를 공격해 약 930GB 규모의 환자 개인정보를 포함한 데이터를 탈취했다. 이 자료는 다크웹 유출 사이트를 통해 공개됐다. 이어 10 월 28 일 미국 플로리다주의 환경분석 기업인 Florida-Spectrum Environmental Services 를 공격해 기업의 재무제표 및 계약서 등을 포함한 약 500GB 의 데이터를 탈취했다.

Akira 그룹은 10 월 2 일 미국의 컴퓨터 저장장치 제조사 Apricorn 을 공격해 직원 의료기록, 재무 정보, 계약서 등을 포함한 데이터를 다크웹 유출 사이트에 공개하겠다고 협박했다. 같은 날 미국의 디스플레이 제조사인 DisplayIt 도 공격 대상이 되어 기밀 파일과 프로젝트 자료가 유출됐다.

SLSH 그룹은 10 월 초 토요타, FedEx, UPS, Disney/Hulu 등 약 39 개 기업의 정보를 유출 사이트에 게시하며, 10 월 10 일까지 응답이 없을 경우 모든 자료를 공개하겠다고 협박했다. 또한, 같은 시기 Red Hat Consulting 의 내부 GitLab[4] 저장소에서 약 570GB 규모의 소스코드와 고객 리포트를 탈취했다고 주장하며, 이를 다크웹에 게시했다.

[4] GitLab: 기업 내부 개발 소스코드와 CI/CD 설정 등 핵심 개발 자산이 저장된 플랫폼

INC 그룹은 미국의 골프 의류 제조사 Summit Golf Brands 를 공격해 약 47GB 의 데이터를 탈취했다. 회계 자료, 디자인 파일, 인사 자료 등이 포함된 유출 자료는 다크웹 사이트에 공개되었다. 또한, 이들은 프랑스의 IT 기업인 Partitio 를 공격해 약 437GB 규모의 데이터를 유출했다.

SafePay 그룹은 미국 오하이오주 Liberty Township 교육청을 공격해 일부 내부 재무자료, 운영 문서, 교직원 관련 문서가 포함한 48GB 의 데이터를 탈취했다. 또한 독일의 IT 서비스업체 MCSL GmbH 도 공격을 받아 고객 보고서, 프로젝트 문서, 내부 커뮤니케이션 파일이 유출됐다. 미국의 차고 문 제조업체 The Overhead Door Company 역시 공격을 당했다. 해당 기업은 기술 문서, 회계 기록, 고용 계약서 등이 포함된 내부 자료가 노출된 것으로 확인됐다.

한편, Inc 그룹은 독일의 통신기기 제조업체 funktel GmbH 의 3.5TB 가량의 데이터를 탈취했다고 주장했다. 이들은 주요 제품의 설계도, 내부 메일, 급여 명세서, 운영 계획서 등 다양한 문서를 샘플로 공개됐다. 또한 미국의 의료 업체 Medical Center of Marin 도 공격해 환자 개인정보가 포함된 설문지나 의료 소견서, 환자의 신분증 등 환자의 민감 정보가 유출됐다.

■ 랜섬웨어 집중 포커스

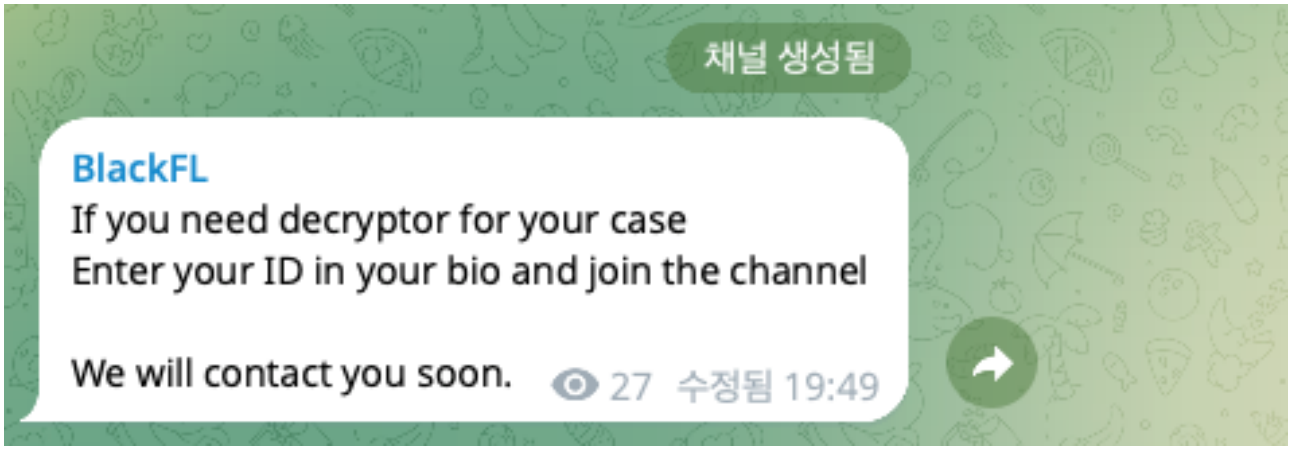


그림 6. BlackField 랜섬웨어 텔레그램 채널

BlackField 랜섬웨어는 2025 년 9 월 악성코드 샘플 공유/분석 플랫폼인 VirusTotal 을 통해 처음 발견되었다. 공개된 2 개의 샘플은 과거 유포된 Cylance 랜섬웨어의 소스코드를 기반으로 개발되었다. 현재 실제 공격 사례는 확인되지 않았으나, 향후 피해 발생이나 데이터 유출 사이트에 활동이 본격화될 가능성이 있다.

```
; int __cdecl main(int argc, const char **argv, const char **envp)
_main proc near

argc= dword ptr  8
argv= dword ptr  0Ch
envp= dword ptr  10h

push    ebp             ; hCrypto
mov     ebp, esp
and     esp, 0FFFFFFF8h
call    HideWindow_407200
call    GetProcessHeap_407290
call    PrivEsc_4055B0
call    ParseCmdLine_401000
call    CreateMutex_4050A0
call    AddScheduleTask_405110
call    CreateLogFile_404CB0
call    CopyRansomNote_405660
call    SetProcessPriv_4051E0
call    DeleteRecycle_405200
call    DeleteShadowCopy_405210
call    VolumeMountAtoZ_4059B0
call    Encrypt_407060
call    DeleteRecycle_405200
call    DeleteShadowCopy_405210
call    RestartDropPE_405450
call    CloseLogFile_404E90
call    DeleteService_4051C0
call    CloseMutex_4050E0
call    SelfDelete_405540
push    0               ; uExitCode
call    ds:ExitProcess
_main endp
```

```
; int __fastcall main(int argc, const char **argv, const char **envp)
main proc near
sub     rsp, 28h
call    HideWindow_140007FB0
call    GetProcessHeap_140008050
call    PrivEsc_140005CB0
call    ParseCmdLine_140001000
call    CreateMutex_140005580
call    AddScheduleTask_140005610
call    CreateLogFile_140005030
call    CopyRansomNote_140005DE0
call    SetProcessPriv_140005740
call    DeleteRecycle_140005770
call    DeleteShadowCopy_140005780
call    VolumeMountAtoZ_140006260
call    Encrypt_140007D50
call    DeleteRecycle_140005770
call    DeleteShadowCopy_140005780
call    Restart_dorpPE_140005AC0
call    CloseLogFile_1400052E0
call    DeleteService_140005700
call    CloseMutex_1400055D0
call    SelfDelete_140005C10
xor     ecx, ecx        ; uExitCode
call    cs:ExitProcess
```

그림 7. Cylance(좌), BlackField(우)

BlackField 랜섬웨어는 Cylance 랜섬웨어와 비교하였을 때 main 함수 내 악성 수행 구조가 완전히 동일하며, PDB[5] 경로에도 'Cylance Ransomware'라는 이름이 명시되어 있다. 이러한 정황으로 볼 때 자체적인 개발 역량을 보유한 그룹이라기보다는 외부에서 소스코드를 구매했거나 공개된 소스를 일부 수정해 활동하는 것으로 판단된다. 또한 BlackField 그룹은 자체 데이터 유출 사이트를 운영하지 않고, 텔레그램 채널·TOX[6] ·이메일 등을 통해 피해자와 접촉하는 것으로 확인되어 실제 활동 및 피해 사례를 직접적으로 확인하기는 어렵다.

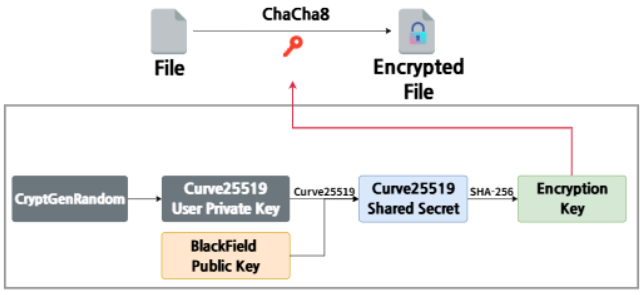
본 보고서는 Cylance 랜섬웨어 기반의 BlackField 랜섬웨어 분석을 진행하여 랜섬웨어 위협에 효과적으로 대비할 수 있도록 하고자 한다.

[5] PDB(Path Database): 프로그램 개발 과정에서 사용된 프로젝트 이름·디렉터리 구조 등이 노출되는 정보

[6] TOX: 중앙 서버 없이 P2P 기반으로 동작하는 익명 메신저

암호화 키

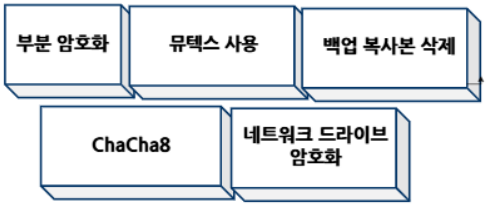
Curve25519 알고리즘으로 암호화 키를 생성하며 ChaCha8 알고리즘으로 암호화



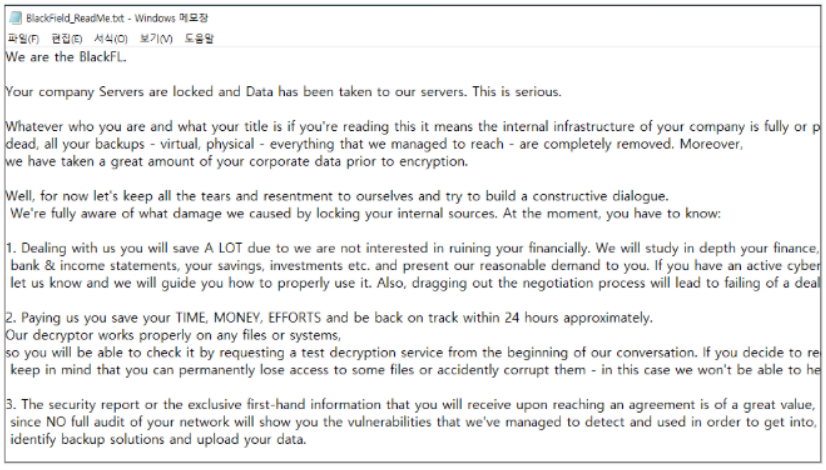
암호화 방식

* Full Mode.
  파일 전체 암호화
* Split Mode.
  -Skip 인자로 전달받은 암호화 간격만큼 스킵하며 1MB 암호화
* Custom Mode.
  파일 크기 ≤ 16MB: 파일 전체 암호화
  파일 크기 16MB ~ 512MB: 256KB 간격마다 1MB 암호화
  파일 크기 512MB ~ 8GB: 4MB 간격마다 1MB암호화
  파일 크기 8GB ~ 128GB: 64MB 간격마다 1MB 암호화
  파일 크기 128GB ~ 2TB: 1GB 간격마다 1MB 암호화
  파일 크기 > 2TB: 16GB 간격 마다 1MB 암호화

특징



랜섬노트


BlackField_ReadMe.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말
We are the BlackFL.

Your company Servers are locked and Data has been taken to our servers. This is serious.

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or p
dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover,
we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue.
We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance,
bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber
let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal

2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately.
Our decryptor works properly on any files or systems,
so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to re
keep in mind that you can permanently lose access to some files or accidently corrupt them - in this case we won't be able to he

3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value,
since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into,
identify backup solutions and upload your data.

BlackField_ReadMe.txt

변경 확장자

.BlackFL

제작 언어

C/C++

그림 8. 랜섬웨어 개요

DireWolf 랜섬웨어 전략

그림 9. 랜섬웨어 공격 전략

BlackField 랜섬웨어는 다양한 실행 인자를 통해 암호화 동작을 정밀하게 제어할 수 있도록 설계되어 있다. 이러한 구조는 공격자가 목표 타겟, 암호화 방식, 뮤텍스 생성 여부를 유연하게 설정할 수 있다. BlackField 의 실행 인자와 기능은 아래 표와 같다.

옵션	보조 옵션	서비스
-path	-	암호화 대상 경로 지정, 옵션이 존재하지 않으면 전체 암호화
-mode	full	파일 전체 암호화
	fast	파일 부분 암호화
	split	특정 크기 간격으로 암호화
	Custom	랜섬웨어 내 정의된 파일 크기에 따라 부분 암호화
-priority	off	프로세스 우선 순위 설정
-skip	-	-split 암호화에서 skip 크기 지정
-power	restart	파일 시스템 덮어쓰기 이후 재시작
	shutdown	파일 시스템 덮어쓰기 이후 시스템 종료
-console	-	암호화 진행 과정 창 활성화 여부 확인
-nomutex	-	중복 실행 방지를 위한 뮤텍스 생성 여부 확인
-nonetdrive	-	네트워크 드라이브 암호화 여부 확인
-nodel	-	암호화 이후 자기자신 삭제 여부 확인

표 1. 랜섬웨어 실행인자

랜섬웨어 실행 시 path 인자와 함께 암호화 대상 경로가 지정되면 시스템 전체 암호화를 하지 않고 지정된 경로에만 암호화된다. 다른 랜섬웨어들이 옵션에 따라 분기해 부분 암호화하는 것과 달리, BlackField 는 path 옵션이 활성화되면 작업 스케줄러에 관리자 권한으로 실행되도록 스스로 등록한 후 즉시 실행한다. 또한 nomutex 옵션이 활성화되지 않은 경우, 랜섬웨어의 중복 실행을 방지하기 위해 "Global\\BlackFLMutex" 문자열로 뮤텍스[7] 를 생성한다. 이후 랜섬웨어 동작을 기록할 로그 파일을 생성하고, 복호화를 방해하기 위해 휴지통을 비우며 WMI[8] 를 통해 볼륨 섀도 복사본을 삭제한다. 이후 감염 PC 에 연결된 모든 네트워크 드라이브를 시스템에 마운트하여 목록을 로그에 남기고, 이들을 대상으로 암호화하기 위한 초기 절차를 완료한다.

이후 시스템 전체 드라이브를 순차적으로 탐색해 모든 디렉토리를 확인한 뒤, 해당 위치에 랜섬노트를 생성하고, 암호화 대상을 판별한다. 이때 특정 경로와 확장자 및 파일명은 암호화 대상에서 제외한다. 확인된 예외 대상은 아래 표와 같다.

암호화 제외 경로	확장자 및 파일명
Windows, $Windows.~bt, $windows.~ws, windows.old, windows nt, All Users, Public, Boot, Intel, PerfLogs, System Volume Information, MSOCache, $RECYCLE.BIN, Default, Config.Msi, tor browser, microsoft, google, yandex, DropBox	dll, exe, sys, drv, efi, msi, lnk, BlackFL, ntldr, ntuser.dat, bootsect.bak, ntuser.dat.log, autorun.inf, thumbs.db, iconcache.db, bootfont.bin, boot.ini, desktop.ini, ntuser.ini, bootmgr, BOOTNXT, BlackField_ReadMe.txt, LPW5.tmp, MSVC150.dll, LLKFTP.bmp

표 2. 암호화 예외 대상

[7] 뮤텍스(Mutex): 하나의 자원에 여러 스레드 혹은 프로세스가 동시에 접근하지 못하도록 하는 동기화 매커니즘으로, 랜섬웨어에서는 흔히 중복 실행 방지를 위해 사용한다.

[8] WMI(Windows Management Instrumentation): 윈도우 운영체제의 구성 요소, 상태, 동작 정보를 표준화된 방식으로 조회·관리할 수 있도록 하는 관리 인터페이스

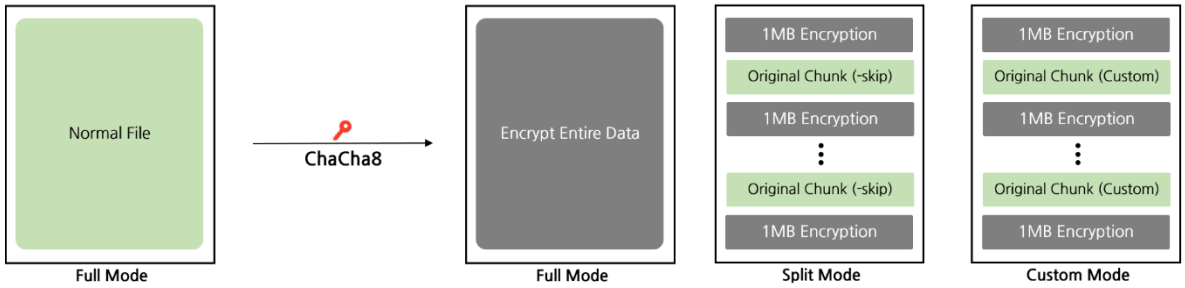


그림 10. BlackField 랜섬웨어 암호화 방식

BlackField 랜섬웨어는 파일 암호화를 수행하기 위해 먼저 키 생성 단계를 진행한다. 난수 생성 함수를 통해 32 바이트 키와 8 바이트 nonce 값을 생성하고, 생성된 32 바이트 키를 기반으로 Curve25519 알고리즘을 이용해 공개키를 만든다. 이후 공격자의 공개키와 연산하여 공유 비밀을 도출하고, 이를 SHA-256 으로 해시해 32 바이트 파생키를 생성한다. 최종적으로 이 파생키를 사용해 ChaCha8 알고리즘으로 파일 암호화를 수행한다.

파일 암호화 방식은 전달받은 -mode 인자에 따라 달라진다. 파일 전체를 암호화하는 full 모드, 일부 구간만 암호화하는 fast 모드, -skip 옵션에 설정된 값만큼 일정 바이트를 주기적으로 건너뛰며 암호화하는 split 모드 그리고 파일 확장자·크기에 따라 암호화 범위가 결정되는 Custom 모드가 존재한다. mode 옵션이 지정되지 않은 경우 기본적으로 Custom 모드가 사용되며, 이 모드에서는 파일 확장자와 크기에 따라 특정 범위만 선택적으로 암호화한다. 각 조건별 암호화 범위는 아래 표와 같다.

파일 크기	암호화 모드	암호화 간격
≤ 16MB	전체 암호화	-
16MB ~ 512MB	부분 암호화	0x40000 (256KB)
512MB ~ 8GB	부분 암호화	0x400000 (4MB)
8GB ~ 128GB	부분 암호화	0x4000000 (64MB)
128GB ~ 2TB	부분 암호화	0x40000000 (1GB)
> 2TB	부분 암호화	0x400000000 (16GB)

표 3. Custom 모드 암호화 범위

파일 크기에 따라 부분 암호화를 수행하는 대상 확장자는 다음과 같다.

암호화 대상 확장자
mdf, ndf, edb, mdb, accdb, db, db2, db3, sql, sqlite, sqlite3, sqlitedb, database, zip, rar, 7z, tar, whim, gz, xld, xls, xlsx, csv, bak, back, backup,

표 4. Custom 모드 적용 대상 확장자

랜섬웨어 대응방안

그림 11. 랜섬웨어 대응방안

BlackField 랜섬웨어는 2025 년 9 월 새롭게 등장했으나, 랜섬노트를 제외한 Cylance 랜섬웨어와 동일한 재활용 코드로 구성되어 있다. 기존에 유출된 소스코드를 기반으로 하거나, 포럼 등에서 코드를 구매해 일부만 변형한 뒤 사용하는 것이다. 이와 같은 사례는 최근 랜섬웨어 생태계에서 매우 흔하게 확인된다. 공개된 랜섬웨어를 재활용한 공격은 보안 솔루션에서 탐지 가능성이 높고 대응 또한 상대적으로 용이하다는 점에서 기술적 위협 수준은 낮아 보일 수 있다. 그러나 최근 공격 경향을 고려했을 때, 공격자는 이미 내부망에 침투해 시스템 구조를 충분히 파악한 후 최종 단계에서 랜섬웨어를 실행하는 경우가 많아 단순한 코드 재사용이라고 해더 위협을 과소평가해서는 안 된다.

또한 BlackField 그룹은 자체 다크웹 데이터 유출 사이트를 운영하지 않으며, 감염 후 텔레그램 채널이나 TOX 를 통해 피해자와 직접 접촉하는 방식을 사용한다. 때문에 실제 피해 사례의 파악이 어렵고, 공격 전술 또한 충분히 공개되지 않았다.

따라서 이미 알려진 변종 기반의 랜섬웨어라 하더라도, EDR 솔루션을 도입하고 최신 보안 패치를 적용하여, 알려진 취약점을 통한 침투나 비정상적인 동작을 신속히 식별·차단할 수 있도록 해야 한다. 이로써 파일 암호화 과정에서 발생하는 행위 기반 패턴을 실시간으로 탐지하고, 악성 프로세스의 실행을 중단시킬 수 있다.

IoCs

Hash(SHA-256)
41c9cd08fff67539525aa413b9199be6e0a4f1a8fc58610a183d77d179d3f282
9f66af5c1e09535d43de5713a3c1d8130e12f8981d1066777f025cf24d963bdc

■ 참고 사이트

• Emsisoft (https://www.emsisoft.com/en/blog/44123/)

• Vulncheck (https://www.vulncheck.com/blog/cve-2025-10035-fortra-go-anywhere-mft)

• Trustwave (https://www.trustwave com/en-us/resources/blogs/spiderlabs-blog/scattered-lapsuss-hunters-anatomy-of-a-federated-cybercriminal-brand/)

• Cybersecuritynews (https://cybersecuritynews.com/breachforums-back-again)