Keep up with Ransomware

확산되는 Gentlemen 랜섬웨어 위협

■ 개요

2025 년 11 월 랜섬웨어 피해 사례 수는 지난 10 월(800 건) 대비 약 8% 감소한 740 건으로 집계됐다.

2025 년 11 월 19 일 미국·영국·호주는 랜섬웨어 그룹들의 인프라를 제공한 러시아 호스팅 업체 Media Land 에 대한 공동 제재를 발표했다. Media Land 는 LockBit, BlackSuit, Play 등 랜섬웨어 그룹에 운영 인프라를 제공한 업체로 지목되었다. 공격에 사용된 서버와 네트워크가 호스팅된 것이 확인됐기 때문이다. 발표 내용에는 Media Land 와 계열사인 ML Cloud 를 비롯한 관련 법인 및 연계된 인물 등의 명단이 포함되어 있었다.

공격자가 직접 침투하는 방식이 아닌 내부자 공모를 통한 접근 방식 사례가 확인됐다. CrowdStrike 는 자사 직원 1 명이 공격자와 공모해 내부 시스템 화면을 외부에 제공한 사실을 확인하고, 해고 조치했다고 발표했다. Scattered Lapsus$ Hunters(SLSH)로 알려진 그룹은 텔레그램 채널에 CrowdStrike 내부 대시보드가 담긴 스크린샷을 공개하며, 내부자로부터 2 만 5 천 달러(한화 약 3,600 만원)를 대가로 SSO 인증 쿠키[1] 등을 제공받았다고 주장했다. 하지만 CrowdStrike 는 조사 결과 해당 직원이 화면 캡처를 외부로 공유한 사실은 인정하면서도, 관련 계정은 탐지 직후 차단되어 사내 시스템 침해나 고객 데이터 유출은 발생하지 않았다고 밝혔다.

내부자 공모는 SLSH 그룹을 통해 2025 년 8 월 처음 확인된 바 있다. 같은 달 텔레그램에서 신규 RaaS[2] 출시를 예고했다. 다만 예고와 달리 10 월까지는 랜섬웨어 배포보다는 주로 데이터 유출·협박 중심의 EaaS[3] 활동이 확인됐다. 이후 2025 년 10 월 11 일, 법 집행기관의 압박이 강화됐다는 이유로 일시적인 활동 중단을 발표했다. 그러나 11 월 랜섬웨어 샘플과 RaaS 모델 공개, 피해자 게시 등 현재까지 활동을 지속하고 있다.

[1] SSO 인증 쿠키: 단일 로그인(Single Sign-On) 환경에서 사용자의 인증이 완료되었음을 나타내는 브라우저 쿠키

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

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

■ 랜섬웨어 뉴스

미국, 영국, 호주 정부의 러시아 기업 Media land 제재

- 2025년 11월 19일 미국, 영국 호주 정부는 러시아 호스팅 업체 Media land를 제재
- Media land는 랜섬웨어 그룹들의 인프라를 호스팅하여 랜섬웨어 그룹들을 지원
- 각 정부는 Media Land의 자산을 동결하고 거래를 금지했으며 전 세계 금융기관에도 이들과의 접촉 중단을 경고

CrowdStrike 직원 SLSH 그룹과 내통

- 2024년 말부터 2025년 초까지 CrowdStrike 위협 인텔리전스팀 직원이 SLSH 해킹 그룹에 내부 자료를 유출하려 한 정황
- 위협 분석 보고서 탐지 규칙 등 민감 자료가 외부 유출 직전 탐지되었으며 해당 계정은 즉시 차단되었고 내부 조사가 실시됨
- 이번 사건은 내부자 위협의 현실성과 권한 관리·사내 보안 정책 강화의 필요성을 부각한 사례

SLSH 그룹의 랜섬웨어 샘플 발견

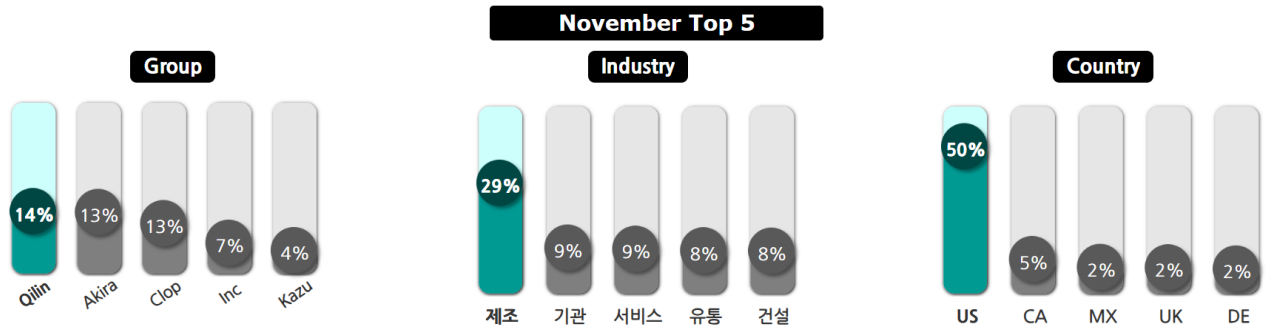
- 2025년 8월 등장 후 텔레그램에서 신규 RaaS 출시를 예고
- 10월까지는 랜섬웨어 배포보다 데이터 유출·협박(EaaS) 중심 활동이 주로 확인
- 중단 선언 이후 11월 샘플이 확인되며 중단 선언과 무관하게 개발이 지속됐거나 활동이 재개됐을 가능성이 제기

11월, 신생 그룹 6개 등장

- 전체 신규 그룹중 QuickLock, Kazu, CipherWolf, Benzona, TridentLocker는 자체 다크웹 유출 사이트를 보유
- 그중 QuickLock과 CipherWolf의 다크웹 유출 사이트는 비활성화된 상태

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협



New ransomware & group

QuickLock Kazu CipherWolf Benzona Root TridentLocker

New ransomware variant (orgin/variant)

HiddenTear .Phantom MedusaLocker .BAGAJAI .BAFAIAI Dharma .zeo

그림 2. 2025 년 11 월 랜섬웨어 위협 현황

새로운 위협

11 월에는 총 6 개의 신규 랜섬웨어 그룹이 등장했다. 이 중 QuickLock, Kazu, CipherWolf, Benzona, TridentLocker 는 다크웹 유출 사이트를 보유하고 있으나, 현재 QuickLock 과 CipherWolf 의 사이트는 비활성화된 것으로 확인된다.

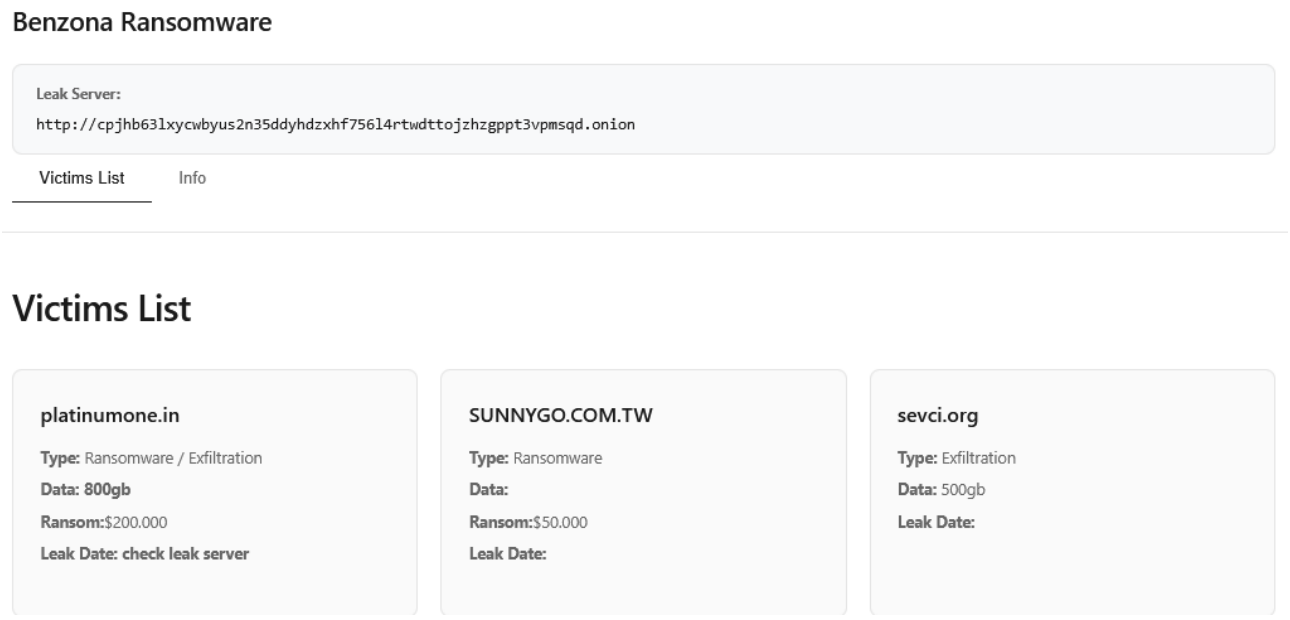


그림 3. Benzona 의 다크웹 유출 사이트

2025 년 11 월에 발견된 Benzona 그룹은 현재까지 총 7 건의 피해 정보를 게시했다. 해당 그룹은 다크웹 유출 사이트에서 피해 건별 공격 유형을 랜섬웨어, 랜섬웨어/데이터유출, 데이터 유출의 3 가지로 구분해 표기하고, 데이터 규모와 요구 금액을 함께 제시하고 있다. 이는 암호화와 데이터 탈취를 병행하는 이중 갈취 모델과, 데이터 유출만을 활용한 협박 방식을 병행해서 운용하고 있음을 보여준다.

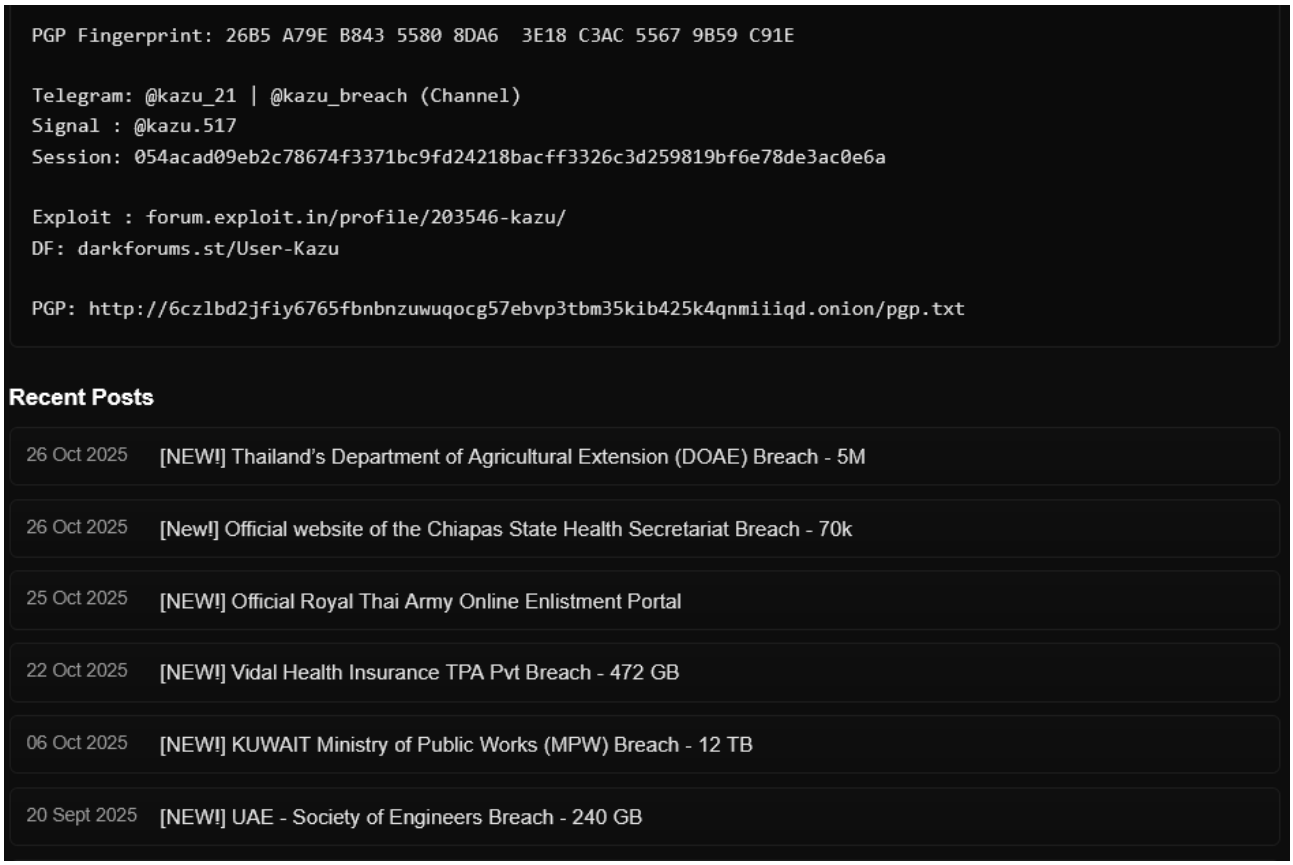


그림 4. Kazu 의 다크웹 유출 사이트

2025 년 11 월에 발견된 Kazu 그룹은 현재까지 총 36 건의 피해 정보를 게시하며, 11 월 기준 활동이 가장 활발한 랜섬웨어 그룹 상위 5 개 중 하나로 확인됐다. Kazu 는 암호화 과정을 거치지 않고, 데이터 탈취와 이를 이용한 협박을 주요 수단으로 삼는 데이터 탈취형 랜섬웨어 그룹으로 알려져 있다.

Top5 랜섬웨어

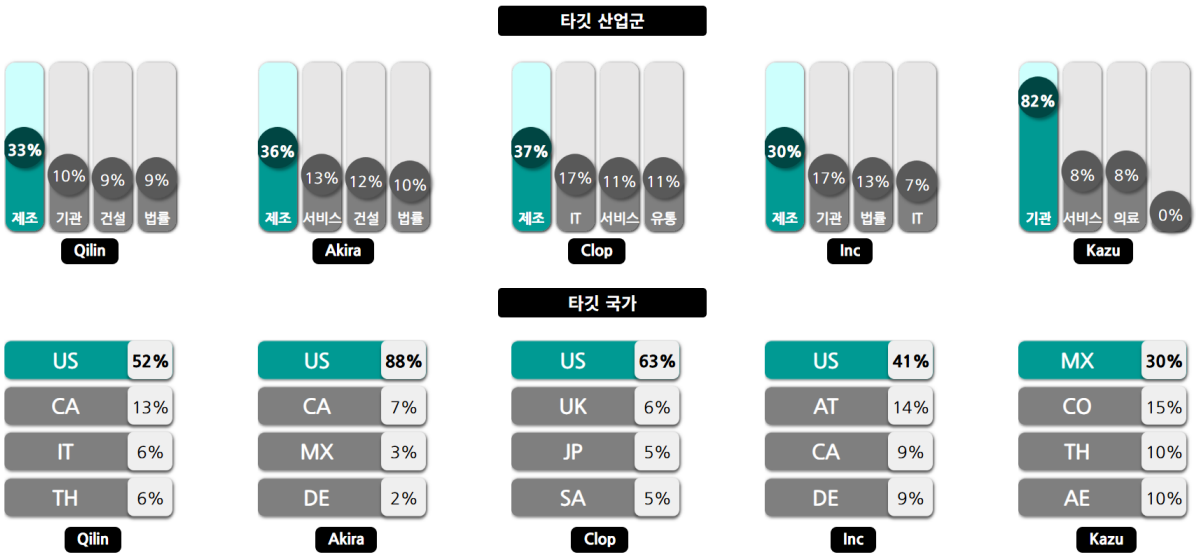


그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

Qilin 그룹은 11 월 25 일 미국 메릴랜드주의 의료 기관인 Columbia Medical Practice 를 공격해 환자 개인정보를 포함한 약 410GB 규모의 데이터를 탈취한 후 Qilin 그룹의 다크웹 유출 사이트에 공개했다.

Akira 그룹은 11 월 28 일 미국의 목재 회사인 Lone Rock Timber 를 공격해 기업 직원의 개인정보, 재무제표 및 계약서 등을 포함한 약 25GB 의 데이터를 탈취했다. 같은 날 미국의 철강 제조 업체인 Crucible Industries 를 공격해 약 10GB 에 달하는 내부 문서와 직원 정보를 유출했다.

Clop 그룹은 오라클의 E-Business Suite 제로데이 취약점(CVE-2025-61882)을 악용해 여러 기업을 공격했다. 대부분의 침해는 2025 년 11 월 이전에 발생했지만 피해 사실과 데이터 유출은 11 월에 공개되었다. 대표적으로 Clop 그룹은 미국의 신문사인 The Washington Post 에 침입해 이름, 은행 계좌, 사회보장번호 등이 포함된 약 180GB 분량의 개인정보를 유출하겠다고 협박했다.

INC 그룹은 11 월 21 일 아랍에미리트의 소방장비 제조사인 NAFFCO FZCO 직원의 개인정보, 내부 재무자료, 운영 문서가 포함된 1TB 의 데이터를 탈취했다. 또한 다음날인 11 월 22 일 오스트리아의 어린이 자전거 제조사인 Woom GmbH 내부 자료도 유출했다.

Kazu 그룹은 11 월 7 일 미국 텍사스주의 의약 플랫폼인 Doctor Alliance 를 공격하여 환자 이름, 의료기록번호 등이 포함된 353GB 크기의 데이터를 탈취하였다고 주장하며, 20 만 달러(한화 약 2 억 9 천만원)를 요구했다. 11 월 10 일에는 콜롬비아의 국가기관인 National Civil Service Commission of Colombia 를 공격해 약 2.9 TB 크기의 데이터를 탈취한 뒤 30 만 달러(한화 약 4 억 4 천만원)를 요구했다.

■ 랜섬웨어 집중 포커스

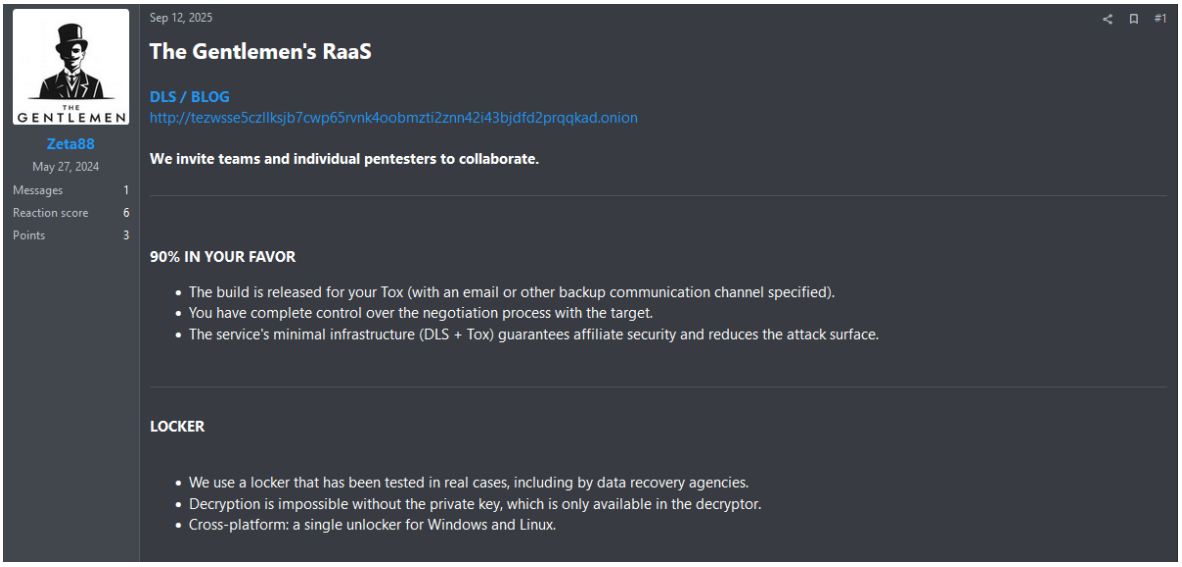


그림 6. Gentlemen 랜섬웨어 그룹의 RaaS 홍보글

Gentlemen 랜섬웨어 그룹은 2025 년 9 월에 활동하기 시작한 RaaS 그룹으로 다크웹 RAMP 포럼에서 구성원을 모집하기 시작했다. 또한 모집 공고에서 독립국가연합(CIS) 소속 국가는 공격 대상에서 제외했는데, 이는 그룹이 러시아와 연관이 있음을 시사한다.

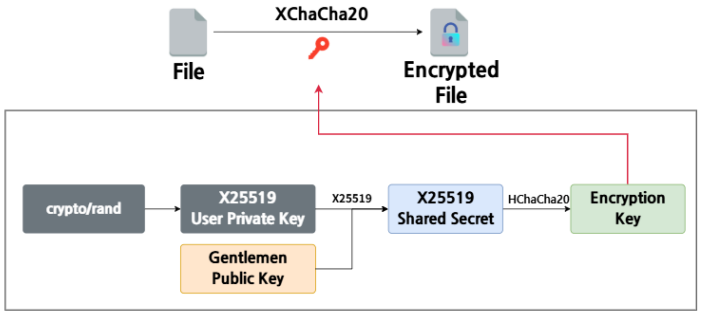
그림 7. Gentlemen 랜섬웨어 그룹의 다크웹 유출 사이트

Gentlemen 랜섬웨어 그룹은 현재까지 다크웹 유출 사이트에 총 64 개 피해 조직 정보를 게시했다. 해당 유출 사이트는 Tor 네트워크에서 운영되며, 각 피해 기업의 명칭과 기업 설명, 유출 자료 게시 일시 등을 함께 공개한다. 또한 Gentlemen 그룹은 Windows, Linux, ESXi 등 다양한 운영 환경을 암호화할 수 있는 기능을 RaaS 를 통해 제공하고 있다. 본 보고서에서는 다가오는 위협에 대비하기 위해 이 중 Windows 버전을 중심의 분석 정보를 공유하고자 한다.

Gentleman Ransomware

암호화 키

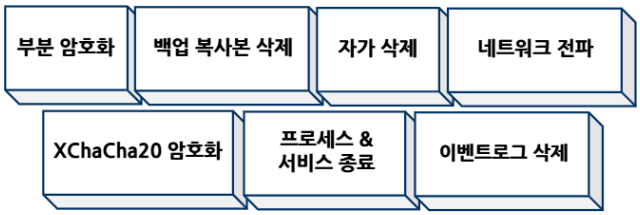
X25519 알고리즘으로 암호화 키를 생성하며 XChaCha20 알고리즘으로 암호화



암호화 방식

Files ≤ 1MB: 전체 암호화
Files > 1MB: 선택한 모드(--fast / --superfast / --ultrafast)에 따라
→ 파일 크기의 9% / 3% / 1%만 부분 암호화

특징



랜섬노트

README-GENTLEMEN.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
7aae8fd9187c88dd0292cce1abd050e2 = YOUR ID

Gentlemen, your network is under our full control.
All your files are now encrypted and inaccessible.

1. Any modification of encrypted files will make recovery impossible.
2. Only our unique decryption key and software can restore your files.
   Brute-force, RAM dumps, third-party recovery tools are useless.
   It's a fundamental mathematical reality. Only we can decrypt your data.
3. Law enforcement, authorities, and "data recovery" companies will NOT help you.
   They will only waste your time, take your money, and block you from recovering your files — your business will be lost.
4. Any attempt to restore systems, or refusal to negotiate, may lead to irreversible wipe of all data and your network.
5. We have exfiltrated all your confidential and business data (including NAS, clouds, etc).
   If you do not contact us, it will be published on our leak site and distributed to major hack forums and social networks.
6. We guarantee 100% file recovery to their original state, bit by bit.
   To demonstrate the quality of our work, you can provide two sample files, and we will restore them free of charge.

TOX CONTACT - RECOVER YOUR FILES
Contact us (add via TOX ID): F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E
Download Tox messenger: https://tox.chat/download.html

COOPERATE TO PREVENT DATA LEAK (48 HOURS BEFORE YOUR COMPANY DATA WILL BE PUBLISHED IN BLOG, WITH 239 H
Check our blog: http://tezwsse5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad.onion/
Download Tor browser: https://www.torproject.org/download/
Follow us on X: https://x.com/TheGentlemen25

Any other means of communication are fake and may be set up by third parties.
Only use the methods listed in this note or on the specified website.
```

README-GENTLEMEN.txt

변경 확장자

.7mtzhh

제작 언어

Go

그림 8. Gentlemen 랜섬웨어 개요

랜섬웨어 전략

그림 9. 랜섬웨어 공격 전략

Gentlemen 랜섬웨어는 다양한 실행 인자를 사용해 암호화 동작을 정밀하게 제어할 수 있도록 설계되어 있어, 공격자는 목표 파일의 위치, 암호화 강도 등을 설정할 수 있다. 이때 사용되는 인자와 기능은 아래 표와 같다.

인자	설명
--paasword	랜섬웨어 실행에 필요한 패스워드
--path	특정 경로 암호화
--T	암호화 시작 전 대기 시간(분 단위) 지정
--silent	파일의 이름과 확장자를 변경하지 않고 암호화 수행
--system	로컬 드라이브 암호화
--shares	네트워크 드라이브 암호화
--full	로컬 드라이브와 네트워크 드라이브 암호화
--fast	파일 크기의 9% 암호화
--superfast	파일 크기의 3% 암호화
--ultrafast	파일 크기의 1% 암호화

표 1. 랜섬웨어 실행인자

Gentlemen 랜섬웨어는 --path 인자를 통해 암호화 대상을 지정한다. --path 가 지정되지 않은 경우 --system, --shares, --full 값에 따라 암호화 대상이 결정된다. 이때 세 인자는 동시에 사용할 수 없다. --system 이 활성화되면 로컬 드라이브 전체를 대상으로 삼고, --shares 가 활성화되면 접근할 수 있는 네트워크 드라이브를 암호화한다. --full 이 활성화되면 로컬 드라이브를 암호화한 뒤, 이어서 네트워크 드라이브를 암호화한다.

랜섬웨어는 실행 시 분석 방해와 탐지 회피를 위해 각종 기록과 흔적을 제거한다. 먼저 실행 중인 Windows 이벤트 로그 관련 프로세스를 종료하고 주요 이벤트 로그를 초기화한 뒤, Windows Defender 기능을 무력화한다. 이어서 VSS(Volume Shadow Copy Service)를 비롯한 백업 데이터를 삭제하며, 파일 암호화가 완료된 이후에는 랜섬웨어 실행 파일 자체도 자가 삭제한다. 아래는 사용되는 명령어 목록이다.

VSS 삭제
vssadmin delete shadows /all /quiet

휴지통 비우기
cmd /C "rd /s /q C:\$Recycle.Bin"

RDP 로그 삭제
cmd /C "del /f /q %SystemRoot%\System32\LogFiles\RDP**.*"

Windows Defender 우회 및 탐지 회피
Powershell -Command "Set-MpPreference -DisableRealtimeMonitoring $true -Force"
Powershell -Command "Add-MpPreference -ExclusionPath C:\ -Force"
Powershell –Command "Add-MpPreference -ExclusionProcess C:\Users\User\Desktop\{filename}.exe -Force"

자가 삭제
ping 127.0.0.1 -n 3 > nul\r\ndel /f /q \""

표 2. 복구 방지 탐지 회피 관련 명령어

랜섬웨어는 원활한 파일 암호화를 위해 특정 프로세스와 서비스를 우선적으로 종료한다. 종료 대상 프로세스 및 서비스는 아래 표와 같다.

프로세스 이름
mvdesktopservice.exe, VeeamDeploymentSvc.exe, VeeamTransportSvc.exe, VeeamNFSSvc.exe, EnterpriseClient.exe, DellSystemDetect.exe, avscc.exe, avagent.exe, sapstartsrv.exe, saposco.exe, saphostexec.exe, CVODS.exe, cvfwd.exe, cvd.exe, CVMountd.exe, tv_x64.exe, tv_w32.exe, pgAdmin4.exe, TeamViewer.exe, TeamViewer_Service.exe, SAP.exe, QBCFMonitorService.exe, pgAdmin3.exe, QBDBMgrN.exe, QBIDPService.exe, CagService.exe, vsnapvss.exe, raw_agent_svc.exe, cbInterface.exe, "Docker Desktop.exe", beserver.exe, pvlsvr.exe, bengien.exe, benetns.exe, vxmon.exe, bedbh.exe, IperiusService.exe, sqlceip.exe, xfssvccon.exe, wordpad.exe, winword.exe, visio.exe, thunderbird.exe, thebat.exe, Iperius.exe, psql.exe, postgres.exe, tbirdconfig.exe, synctime.exe, steam.exe, sqbcoreservice.exe, powerpnt.exe, cbVSCService11.exe, postmaster.exe, mysqld.exe, outlook.exe, oracle.exe, onenote.exe, ocssd.exe, ocomm.exe, ocautoupds.exe, SQLAGENT.exe, sqlwriter.exe, notepad.exe, mydesktopservice.exe, mydesktopqos.exe, mspub.exe, msaccess.exe, cbService.exe, sqlbrowser.exe, w3wp.exe, sql.exe, isqlplussvc.exe, infopath.exe, firefox.exe, encsvc.exe, Ssms.exe, DBeaver.exe, sqlservr.exe, dbsnmp.exe, dbeng50.exe, agntsvc.exe, vmcompute.exe, vmwp.exe, vmms.exe

표 3. 종료 대상 프로세스

서비스 이름
crSch2Svc, VSNAPVSS, MVarmor64, MVarmor, VeeamTransportSvc, VeeamDeploymentService, VeeamNFSSvc, AcronisAgent, QBIDPService, QBDBMgrN, QBCFMonitorService, OracleServiceORCL, MySQL, MSSQL, SAPHostExec, SAPHostControl, SAPD$, SAP$, postgresql, SAP, SAPService, GxFWD, GxVsshWProv, GXMMM, GxClMgr, MariaDB, GxCVD, GxClMgrS, GxVss, GxBlr, BackupExecRPCService, SQLAgent$SQLEXPRESS, BackupExecManagementService, BackupExecJobEngine, MSSQL$SQLEXPRESS, BackupExecDiveciMediaService, BackupExecAgentBrowser, SQLWriter, BackupExecAgentAccelerator, BackupExecVSSProvider, PDVFSService, SQLSERVERAGENT, WSBExchange, MSExchange\$, MSExchange, sophos, msexchange, docker, MSSQLSERVER, MSSQL*, Sql, vss, backup, veeam, memtas, mepocs, vmms

표 4. 종료 대상 서비스

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

암호화 제외 경로	확장자 및 파일명
AppData, Boot, C:\Windows, SYSVOL, Tor Browser, Internet Explorer, Google, Opera, Opera Software, Mozilla, Mozilla Firefox, $Recycle.Bin, ProgramData, All Users, bootmgr, system volume information, inte, msocache, perflogs, ntldr, Program Files, Program Files (x86), #recycle, $windows.~bt, ntuser.dat, NTUSER.DAT	README-GENTLEMEN.txt, .exe, .dll, .sys, .drv, .bin, .tmp, .iso, .img,

표 5. 암호화 예상 대상

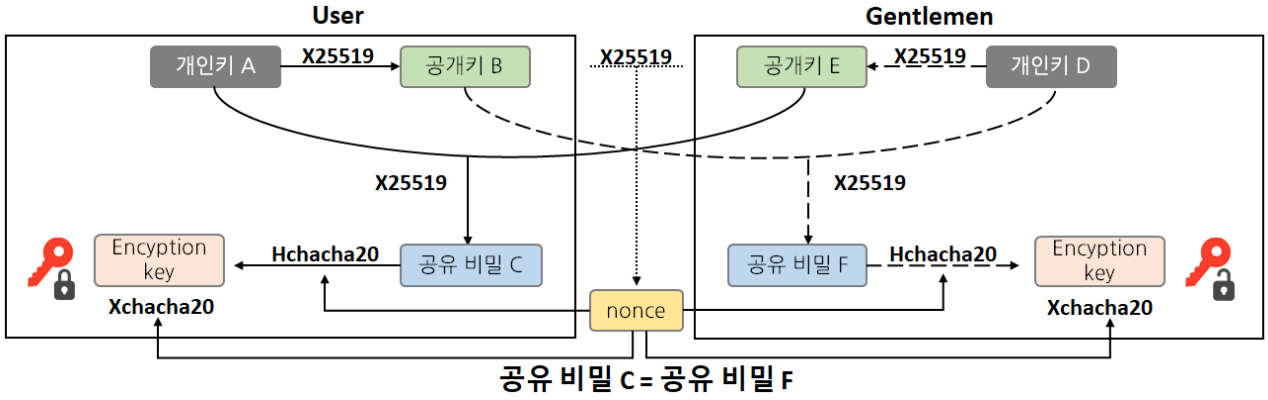


그림 10. 암호화 키 생성 방식

Gentlemen 랜섬웨어는 파일 암호화를 위해 각 파일마다 고유한 32 바이트 개인키를 생성한다. 이 개인키는 하드코딩된 공격자의 공개키와 X25519 연산을 거친 후 공유 비밀을 생성한다. 이렇게 생성된 공유 비밀은 바로 사용되지 않고 HChaCha20 을 통해 32 바이트 암호화 키로 변환되며, 최종적으로 XChaCha20 알고리즘이 이 키를 사용하여 파일을 암호화한다. 또한, 초기 생성된 개인키는 상수 값(0x09)과 조합되어 또 다른 32 바이트 값을 생성하는 데 사용된다. 이 값은 암호화 무결성을 위한 Nonce 구성에 활용되는데, 상위 16 바이트는 HChaCha20 의 Nonce 로, 하위 8 바이트는 XChaCha20 의 Nonce 로 분할되어 각각 적용된다.

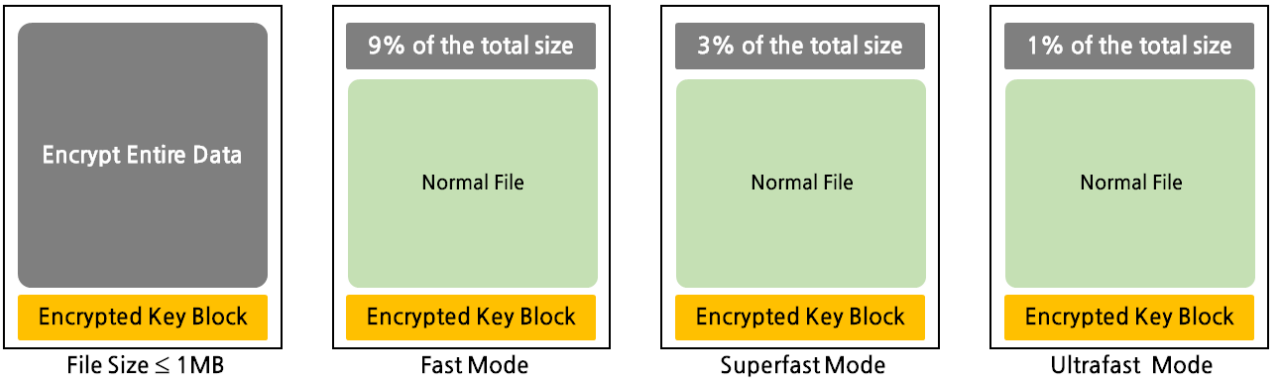


그림 11. 파일 암호화 방식

파일 암호화 범위는 파일 크기와 전달받은 인자에 따라 달라진다. 크기가 1MB 이하인 파일은 인자와 상관없이 전체 데이터가 암호화된다. 1MB 를 초과하는 파일의 경우에는 인자에 따라 파일 크기의 일부만 암호화한다. Fast 모드는 파일 크기의 약 9%, Superfast 모드는 약 3%, Ultrafast 모드는 약 1% 구간만 암호화하는 방식이다. 암호화가 완료되면, 파일 크기나 암호화 모드와 관계없이 모든 파일의 끝에는 고정된 메타데이터 블록이 추가된다. 이 블록에는 키 복구에 필요한 공개키와 해당 파일에 적용된 암호화 모드 정보, 그리고 감염 여부를 식별하기 위한 “GENTLEMEN” 마커가 함께 저장된다.

랜섬웨어 대응방안

그림 12. 랜섬웨어 대응방안

Gentlemen 랜섬웨어는 실행 시 명령 프롬프트와 PowerShell 을 활용해 시스템 내 VSS(Volume Shadow Copy)와 시스템 복원 지점, 이벤트 로그 등 주요 흔적을 삭제하고 Windows Defender 설정까지 변경하는 명령을 연속적으로 실행한다. 이는 ASR[4] 규칙 활성화해 비정상적인 프로세스를 차단해 악성 행위를 막기 위함이다.

또한, EDR 솔루션을 도입과 최신 보안 패치 적용으로 취약점을 악용한 침투나 비정상적인 행위를 신속히 식별·차단할 수 있도록 해야 한다. 백업 복사본을 별도의 네트워크 구간이나 외부 저장소, 오프라인 매체에 주기적으로 분산 백업하는 것도 필수적이다. 시스템이 암호화되더라도 데이터 복구가 가능하기 때문이다.

이때 백업 장치 접근 권한을 최소화하고, 정기적으로 복구 테스트를 실시하여 백업 데이터의 무결성을 보장해야 한다. 추가로 별도의 네트워크나 저장소의 데이터를 분산해 백업하거나 백업 스케줄과 보관 주기를 다양화해 랜섬웨어의 삭제 시도를 피하는 것도 효과적인 방법이다.

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

IoCs

Hash(SHA-256)
EC368AE0B4369B6EF0DA244774995C819C63CFFB7FD2132379963B9C1640CCD2
62C2C24937D67FDEB43F2C9690AB10E8BB90713AF46945048DB9A94A465FFCB8
51B9F246D6DA85631131FCD1FABF0A67937D4BDDE33625A44F7EE6A3A7BAEBD2
025FC0976C548FB5A880C83EA3EB21A5F23C5D53C4E51E862BB893C11ADF712A
9F61FF4DEB8AFCED8B1ECDC8787A134C63BDE632B18293FBFC94A91749E3E454
3AB9575225E00A83A4AC2B534DA5A710BDCF6EB72884944C437B5FBE5C5C9235

■ 참고 사이트

• U.S. Department of the Treasury(https://home.treasury.gov/news/press-releases/sb0319#)

• BleepingComputer(https://www.bleepingcomputer.com/news/security/crowdstrike-catches-insider-feeding-information-to-hackers/)

• BleepingComputer(https://www.bleepingcomputer.com/news/security/meet-shinysp1d3r-new-ransomware-as-a-service-created-by-shinyhunters/)

• The Hacker News(https://thehackernews.com/2025/08/cybercrime-groups-shinyhunters.html#)