

신사의 가면 뒤에 숨은 협박, Gentlemen 랜섬웨어 분석

A asec.ahnlab.com/ko/91514

ATCP

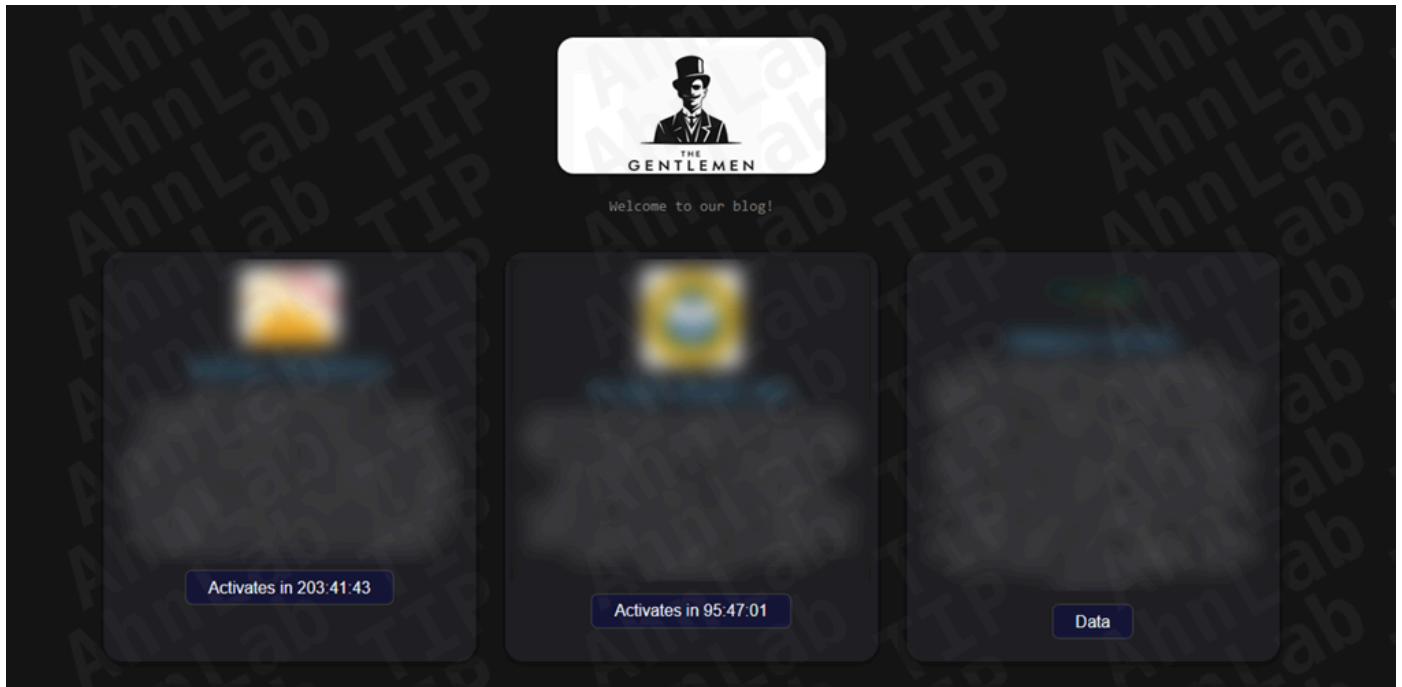
December 10, 2025



Gentlemen 랜섬웨어 그룹은 2025년 8월경 처음으로 식별된 신규 랜섬웨어 그룹이다. 해당 그룹은 기업 네트워크 침투 후 데이터를 외부로 유출하고 암호화한 뒤 이를 협박 수단으로 활용하는 이중 갈취(Double Extortion) 모델을 운영하고 있다. 침해 과정에서는 그룹 정책(GPO) 변조, 정식 서명 드라이버 악용(BYOVD) 등 고도화된 랜섬웨어 그룹에서 확인되는 전형적인 기술들을 활용한다. 현재까지는 Raas 모델로 운영된다는 명확한 증거는 없으며, 기존 랜섬웨어 그룹의 리브랜딩이나 하위 그룹 존재 여부도 확인되지 않았다.

Gentlemen의 공격은 등장 직후 빠르게 확산되었으며, 현재까지 최소 17개국 이상에서 피해 사례가 보고된 것으로 파악된다. 주요 표적 산업은 제조업, 건설업, 의료 및 헬스케어, 보험업 등으로 다양하다. 지역적으로는 아시아 및 태평양(APAC), 북미, 남미, 중동 등 다수의 권역에서 공격이 확인되었으며, 특정 국가나 지역에 국한되지 않는 광범위한 활동 양상을 보이고 있다.

Gentlemen은 등장 이후 비교적 짧은 기간 동안 다수의 지역 및 산업을 공격하면서 2025년 가장 적극적으로 활동하는 신흥 랜섬웨어 조직 중 하나로 평가된다. 특히 표적 공격, 탐지 회피 기술, 정교한 내부 확산 절차 등을 고려할 때 중·대규모 조직을 주요 목표로 삼는 것으로 보이며, 해당 그룹에 대한 지속적인 모니터링이 필요하다.



[그림 1] Gentlemen 데이터 유출 사이트 (DLS)

분석 내용

Gentlemen 랜섬웨어는 Go 언어로 개발된 랜섬웨어로, 실행 인자 내 패스워드 검사를 통해 의도한 환경에서만 정상 동작하도록 제한한다. 암호화 전 초기 루틴으로 Windows Defener 비활성화, 백업 (Veeam) 및 DB(MSSQL, MongoDB) 관련 서비스 중지, 로그 및 시스템 흔적 삭제 작업을 수행한다. 파일 암호화에는 X25519, XChaCha20 암호화 알고리즘을 사용하며, 파일 크기가 클 경우 특정 구간만 선택적으로 암호화하도록 설계되어 있다.

초기 루틴

실행 인자

Gentlemen 랜섬웨어는 실행 직후 명령행(Command-Line) 인자 파싱 루틴을 수행하며, 인자를 통해 암호화 대상, 성능 옵션, 동작 모드 등을 세부적으로 제어하도록 설계되어 있다.

```
The Gentlemen Windows version 0.4.0
Usage: a.exe --password PASS [--path DIR1,DIR2,...] [--T MIN] [--silent] [--full] [--system] [--shares] [--fast] [--superfast] [--ultrafast]

Main Flags
--password PASS    Access password (required)
--path DIRS        Comma-separated list of target directories/disks (optional)
--T MIN            Delay before start, in minutes (optional)
--silent           Silent mode: do NOT rename files after encryption (optional)

Mode Flags (cant be mixed)
--system           Run as SYSTEM: encrypt only local drives (optional)
--shares           Encrypt only mapped network drives and available UNC shares in session context (optional)
--full            Two-phase: --system + --shares. Best practice. (optional)

Speed Flags (cant be mixed)
--fast            9 percent crypt. (optional)
--superfast       3 percent crypt. (optional)
--ultrafast       1 percent crypt. (optional)

Example 1: --password QWERTY --path "C:\W,D:\W,\\nas\share" --T 15 --silent
Example 2: --password QWERTY --system --fast
Example 3: --password QWERTY --shares --T 10
Example 4: --password QWERTY --full --ultrafast

[+]
```

[그림 2] Gentlemen 실행 인자

실행 인자	설명
-password PASS	랜섬웨어 실행을 위한 비밀번호 (필수)
-path DIRS	암호화 대상 디렉터리 및 디스크
-T MIN	암호화 시작 전 지연 시간
-silent	암호화 후 파일 이름을 변경하지 않음
-system	로컬 드라이브만 암호화
-shares	매핑된 네트워크와 사용 가능한 UNC 공유만 암호화
-full	-system 및 -shares 포함
-fast	암호화율 9%
-superfast	암호화율 3%
-ultrafast	암호화율 1%

표 1. 실행 인자 설명

특히, 여러 인자 중 -password 값을 필수로 요구한다. 해당 값이 존재하지 않거나 패스워드가 일치하지 않을 경우 즉시 종료되며, 이는 공격자가 의도한 환경에서만 정상 동작하도록 제한한 것으로, 분석 환경 등 의도되지 않은 환경에서 실행되는 것을 방지한다.

암호화 준비

랜섬웨어 내부에 인코딩된 형태로 존재하는 공격자의 Public Key를 메모리 상에서 디코딩한다. 해당 Public Key는 이후 암호화 과정에서 랜덤하게 생성된 난수와 X25519 연산을 통해 공유 비밀 (Shared Secret)을 생성하고 이를 기반으로 파생된 키를 최종 암호화에 사용하게 된다.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
0013EA00	6F	74	20	63	6F	6E	74	61	69	6E	20	73	6C	61	73	68	ot contain slash
0013EA10	65	73	44	72	32	4F	4C	4E	6D	53	30	7A	4D	48	59	45	esDr2OLNmS0zMHYE
0013EA20	62	63	57	58	72	48	4A	62	69	6F	72	4A	42	7A	36	43	bcWXrHJbiorJBz6C
0013EA30	72	44	69	4C	6C	43	2F	34	49	30	49	32	6B	3D	73	70	rDiLlC/4I0I2k=sp
0013EA40	61	6E	20	6F	6E	20	75	73	65	72	41	72	65	6E	61	2E	an on userArena.
0013EA50	66	61	75	6C	74	4C	69	73	74	20	68	61	73	20	69	6E	faultList has in

[그림 3] 인코딩된 형태로 존재하는 Public Key

암호화 대상 드라이브를 식별하기 위해 Powershell 명령어를 통해 시스템 내 접근 가능한 모든 볼륨 정보를 수집한다. 이 과정에서 Gentlemen 랜섬웨어는 단일 PC 환경 뿐만 아니라, 기업용 클러스터 및 공유 스토리지 환경까지 고려한 것을 알 수 있다.

파일 암호화

암호화 대상 파일이 최종적으로 결정되면 파일 암호화 루틴이 실행된다. Gentlemen 랜섬웨어는 XChaCha20 기반의 스트림 암호를 이용하여 파일을 암호화하며, Key와 Nonce 는 암호화 대상 파일마다 새롭게 생성되며, 생성 과정은 다음과 같다.

먼저, 공격자의 Public key 와 랜덤하게 생성된 난수(32 bytes)를 이용해 X25519(ECDH) 연산을 수행하여 공유 비밀(Shared Secret)을 생성한다. 이 공유 비밀을 기반으로 HChaCha20 연산을 이용해 32 bytes의 SubKey를 생성하며, 최종적으로 해당 SubKey가 파일 암호화를 수행하는 XChaCha20 알고리즘의 Key 로 사용된다. 이후 동일한 난수를 0x9 값과 함께 X25519 연산을 수행하여 또 다른 32bytes 값을 생성하며, 해당 값의 상위 16 bytes는 HChaCha20의 Nonce로 사용되고 하위 영역(0x10 위치의 8 bytes) 은 XChaCha20의 Nonce 구성에 활용된다.

이때 생성된 X25519 결과 값은 Base64 인코딩된 형태로 암호화된 파일에 저장되지만, 임시 Key로 사용된 난수는 저장되지 않는다. 이와 같은 암호화 구조는 공격자가 보유한 Private Key 없이는 공유 비밀을 재생성할 수 없도록 하기 위한 것으로, 결과적으로 피해자가 비용 지불 없이는 복호화 키를 획득하는 것을 차단한다. 또한, X25519 기반의 ECDH와 XChaCha20 암호화를 결합함으로써, 외부로 유출되는 데이터에서 암호화 키가 노출되지 않도록 하고, 매번 새롭게 생성되는 임시 Key 구조를 통해 복호화 불가능성을 극대화한다.

또한, Gentlemen 랜섬웨어는 파일 크기에 따라 암호화 대상 범위가 변경된다. 파일 크기가 0x100000 bytes(약 1MB) 보다 작을 경우에는 전체 파일을 암호화하며, 파일 크기가 0x100000 보다 클 경우 특정 구간만 선택적으로 암호화를 수행한다. 해당 방식은 대용량 파일에 대해 암호화 속도를 향상시키면서도 파일 복구를 어렵게 만들기 위한 목적이다.

00000000008A88EA	48:8B9424 18020000	mov rdx,qword ptr ss:[rsp+218]	file size
00000000008A88F2	0F57C0	xorps xmm0,xmm0	
00000000008A88F5	F248:0F2AC2	cvttsi2sd xmm0,rdx	
00000000008A88FA	F2:0F5905 7E091600	mulsd xmm0,qword ptr ds:[A09280]	file size * 0.09
00000000008A8902	44:0F118C24 98010000	movups xmmword ptr ss:[rsp+198],xmm15	
00000000008A8908	44:0F118C24 A0010000	movups xmmword ptr ss:[rsp+1A0],xmm15	
00000000008A8914	F248:0F2CF0	cvttsd2si rsi,xmm0	
00000000008A8919	48:89B424 D8000000	mov qword ptr ss:[rsp+D8],rsi	first area
00000000008A8921	48:8D3C76	lea rdi,qword ptr ds:[rsi+rsi*2]	
00000000008A8925	48:29FA	sub rdx,rdi	
00000000008A8928	48:89D7	mov rdi,rdx	
00000000008A892B	48:C1EA 3F	shr rdx,3F	
00000000008A892F	48:01FA	add rdx,rdi	
00000000008A8932	48:D1FA	sar rdx,1	
00000000008A8935	48:01F2	add rdx,rsi	
00000000008A8938	48:899424 A0010000	mov qword ptr ss:[rsp+1A0],rdx	second area
00000000008A8940	48:D1E2	shl rdx,1	
00000000008A8943	48:899424 A8010000	mov qword ptr ss:[rsp+1A8],rdx	third area

[그림 4] 암호화 대상 범위 계산

바탕화면 변경 및 랜섬 노트

아래 [그림 5]는 Gentlemen 랜섬웨어 악성코드를 감염시킨 화면이다. 랜섬 노트는 'README-GENTLEMEN.txt' 라는 이름을 가지며, 암호화 작업이 완료된 모든 경로에 생성된다.



[그림 5] 암호화 작업 완료 후 바탕화면

랜섬 노트는 감염 시스템 네트워크 전체를 완전히 통제하고 있다고 주장하며 모든 파일이 암호화되어 접근할 수 없다고 통보하여 피해자에게 심리적 압박을 가한다. 추가로 시스템 내 기밀 정보를 탈취했다고 주장하며, 연락하지 않을 경우 이를 다크웹 및 해킹 포럼에 유출하겠다고 경고하고 있다. 또한, 공격자는 샘플 파일 2개를 보내면 무료로 복호화 해준다는 제안을 통해 피해자의 신뢰를 확보하려는 목적을 확인할 수 있다.



[그림 6] 랜섬 노트 (README-GENTLEMEN.txt)

안랩 대응 현황

안랩 제품군의 진단명과 엔진 날짜 정보는 다음과 같다.

V3

Ransomware/Win.GentlemenCrypt.C5799091 (2025.09.18.03)

Ransomware/Win.GentlemenCrypt.C5825597 (2025.12.11.03)

Ransom/MDP.Decoy.M961 (2016.03.19.00)

Ransom/MDP.Delete.M1105 (2016.05.18.02)

Ransom/MDP.Event.M1784 (2017.11.23.00)

Ransom/MDP.Command.M2255 (2019.06.19.00)

EDR

SystemManipulation/EDR.Event.M2486 (2022.03.31.00)

SystemManipulation/DETECT.T1564.M3965 (2022.04.07.00)

SystemManipulation/EDR.Event.M2506 (2022.09.24.00)

Impact/DETECT.Event.M11078 (2023.05.11.03)

DefenseEvasion/DETECT.T1070.001.M11430 (2023.11.23.02)

MD5

adf675ffc1acb357f2d9f1a94e016f52

de1a114a2c5552387a1bbb61501bf129

