Keep up with Ransomware

Rust 버전의 INC 랜섬웨어 분석 및 위협 대응 방안

■ 개요

2025년 8월 랜섬웨어 피해 사례 수는 지난 7월(485건) 대비 약 13% 증가한 549건을 기록했다. 8월에는 각국의 법집행 활동이 한층 강화되는 동시에, 공격자들의 기술 역시 더욱 정교해지는 양상이 두드러졌다.

미국 법무부는 8 월 11 일, BlackSuit 랜섬웨어 그룹을 겨냥한 국제 합동 작전의 성과를 발표했다. 이번 작전을 통해 수사팀은 해당 조직이 운용하던 서버 4 대와 도메인 9 개를 압수하고, 약 109 만 달러(한화 약 15 억 원) 상당의 암호화폐 자산을 몰수하는 데 성공했다. 미국뿐 아니라 영국, 독일, 프랑스, 캐나다 등 여러 국가의 법집행기관 협력으로 진행됐다. 하지만 암호화 파라미터, 랜섬노트 등에서 확인된 BlackSuit 와 Chaos 랜섬웨어의 연관성으로 인해 BlackSuit 그룹이 완전히 해체되지 않고, 활동을 이어갈 가능성이 제기된다.

8 월초 Akira 랜섬웨어 그룹은 정상 CPU 성능 조정 툴(ThrottleStop)의 드라이버 취약점을 악용해 Microsoft Defender 를 비활성화하는 BYOVD[1] 공격을 수행했다. 공격자는 취약한 드라이버(rwdrv.sys)를 서비스로 등록해 커널 수준의 권한을 확보한 후, 악성 드라이버(hlpdrv.sys)를 로드해 Defender 의 보안 설정을 변경했다. Akira 그룹이 취약한 드라이버를 악용한 공격 기법을 지속적으로 활용하고 있으므로, ThrottleStop 드라이버의 취약점에 대한 보안 조치가 요구된다.

8 월에 등장한 신규 랜섬웨어 그룹인 Cephalus 는 SentinelOne 의 정상 실행 파일(SentinelBrowserNativeHost.exe)을 악용하여 DLL 사이드로딩[2] 방식으로 악성 DLL 을 로드함으로써 랜섬웨어를 실행했다. 이러한 기법은 보안 제품 자체를 역이용해 탐지와 대응을 한층 어렵게 만들며, 랜섬웨어 공격의 복잡성과 정교함을 보여준다.

[1] BYOVD(Bring Your Own Vulnerable Driver): 공격자가 취약점이 존재하는 합법적인 드라이버를 직접 시스템에 설치하여, 운영체제 커널 권한을 탈취한 뒤 보안 솔루션 무력화 등 악성 행위를 수행하는 공격 기법

[2] DLL 사이드로딩: 정상 프로그램이 실행 시 참조하는 DLL 파일을 공격자가 조작하거나 악성 DLL로 교체해, 정상 프로세스를 통해 악성코드가 실행되도록 하는 공격 기법

8 월 말, PromptLock 이라는 이름의 AI 기반 랜섬웨어가 공개되었다. PromptLock 은 뉴욕대 보안 연구팀이 LLM 으로 공격 과정을 자동으로 실행할 수 있는지를 확인하기 위해 제작·공개한 POC[3] 로 알려졌다. 로컬 LLM[4] 을 Ollama[5] 프레임워크로 호출해 실시간으로 Lua[6] 스크립트를 생성한다. PromptLock 은 Windows, macOS, Linux 등 여러 운영체제에서 동작하며, AI 가 파일을 스캔한 뒤 파일 유형, 경로, 내용 등 스캔 정보를 사용자가 사전 작성한 프롬프트에 따라 유출 또는 암호화 수행 여부를 결정한다. 현재 공개된 PromptLock 은 POC 이지만, 실제 공격자가 이 접근법을 악용할 경우 매 실행마다 새로운 코드가 생성돼 해시 등이 바뀌어 정적 탐지의 효용이 낮아질 수 있다. 위험도가 유의미하게 상승하는 것을 고려해 행위 기반 탐지 강화의 필요성이 요구된다.

[3] POC(Proof of Concept): 연구·검증을 위한 시연용 구현으로, 제한된 조건에서 개념의 가능성만 확인하는 코드/설계

[4] 로컬 LLM(Local Large Language Model): 사용자의 시스템에 직접 설치·실행되는 대규모 언어 모델을 의미

[5] Ollama: 오픈소스 기반의 LLM 실행 프레임워크로, 로컬 환경에서 대형 언어 모델을 손쉽게 불러오고 실행할 수 있도록 지원

[6] Lua: 1993 년 개발된 경량 스크립트 언어로, 임베디드 시스템과 게임 엔진 등에서 널리 활용

■ 랜섬웨어 뉴스

BlackSuit 그룹에 대한 국제 합동 작전 결과

- 8월 11일, 미국 법무부가 합동 작전 결과 발표
- 운영 서버 4대·도메인 9개 압수, 암호화폐 $1.09M(약 15억 원) 몰수
- 작전 이후 Chaos 그룹 활동 부각 BlackSuit와의 구조적 유사성에 근거한 연계 정황 제기

일본 경찰청(NPA) Phobos·8Base 무료 복호화기 공개

- 지원 확장자 .phobos·.8base·.elbie·.faust·.LIZARD 등, 복호화 성공 사례 확인
- NPA 홈페이지 및 No More Ransom 등에 공개

Akira 랜섬웨어 BYOVD 기법으로 Windows Defender 비활성화

- ThrottleStop의 취약 드라이버 rwdrv.sys를 서비스로 등록해 커널 권한 획득
- 악성 드라이버(hlpdrv.sys)를 로드해 Microsoft Defender의 보안 설정을 수정하고 기능을 비활성화

신규 그룹 Cephalus, SentinelOne 파일을 이용한 공격

- SentinelOne 정상 실행 파일(SentinelBrowserNativeHost.exe) 악용
- DLL 사이드로딩 기법으로 악성 DLL 실행

AI 기반 PromptLock 랜섬웨어 공개

- 로컬 LLM(Ollama)을 활용해 실시간으로 Lua 스크립트를 생성·실행
- 파일을 스캔한 뒤, 사전 프롬프트에 따라 유출 또는 암호화 여부를 결정
- Windows, MacOS, Linux 등 멀티플랫폼 환경을 지원하며, 공격 자동화와 변종 생성이 더욱 가속화

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

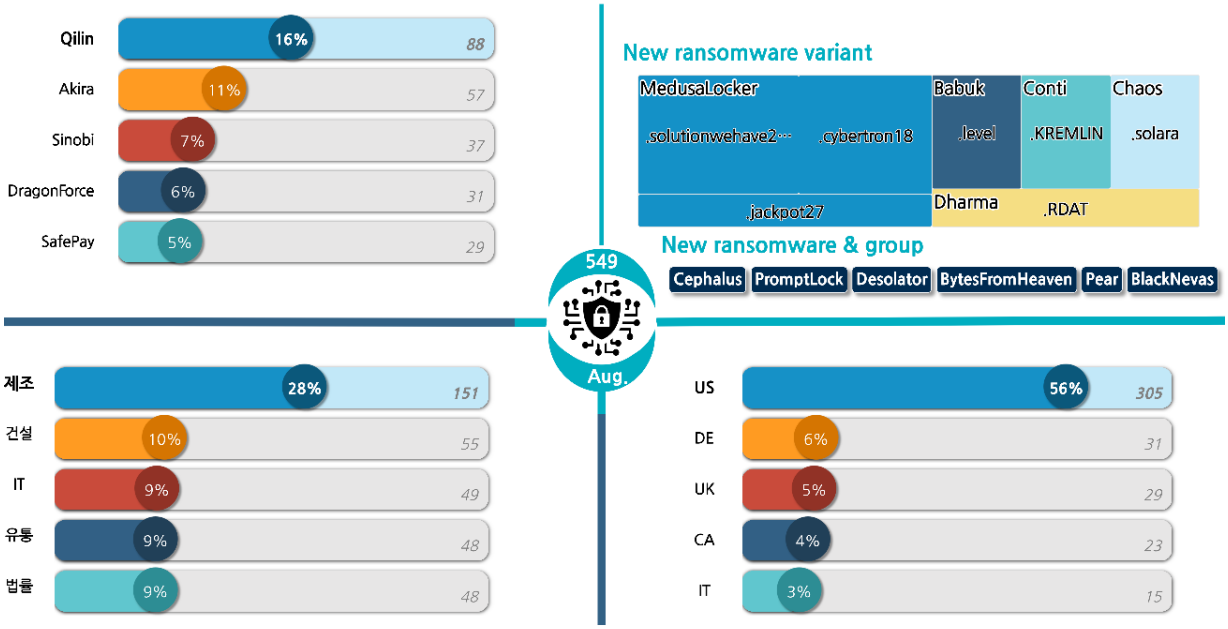

그림 2. 2025 년 8 월 랜섬웨어 위협 현황

새로운 위협

8 월 한 달 동안 총 549 건의 랜섬웨어 피해 사례가 확인됐으며, 이 기간 신규 랜섬웨어 6 개가 새롭게 등장했다. 이 중 Cephalus, Desolator, PEAR, BlackNevas 등 4 개 그룹은 자체적으로 운영하는 데이터 유출 사이트에 피해 사실을 게시했다.

그림 3. Cephalus 의 데이터 유출 사이트

2025 년 8 월에 처음 발견된 Cephalus 랜섬웨어 그룹은 여러 피해 사례를 발생시킨 것으로 확인되었다. 그러나 8 월 말 기준, Cephalus 가 운영하던 다크웹 유출 사이트는 접근이 불가능한 상태로 이후 추가적인 활동은 확인되지 않고 있다.

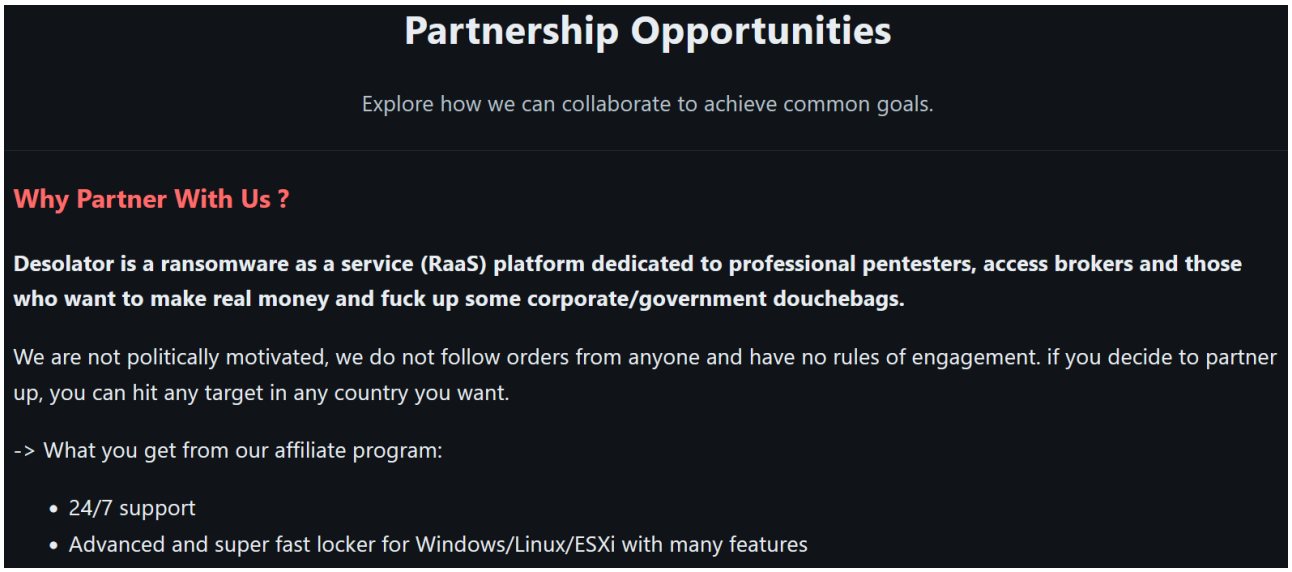

그림 4. Desolator 의 RaaS[7] 모집글

2025 년 8 월 말에 처음 발견된 Desolator 랜섬웨어는 현재까지 총 3 건의 피해 사례가 확인되었으며, 해당 그룹은 RaaS 계열사 모집 글에서 상시 지원을 내세우며, Windows·Linux·ESXi 용 랜섬웨어를 제공하고, 수익의 10%만 지불하면 된다고 명시했다. 또한 피해자가 요구액을 지급하지 않을 경우 탈취 데이터를 공개할 것임을 밝혔다.

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

Top5 랜섬웨어

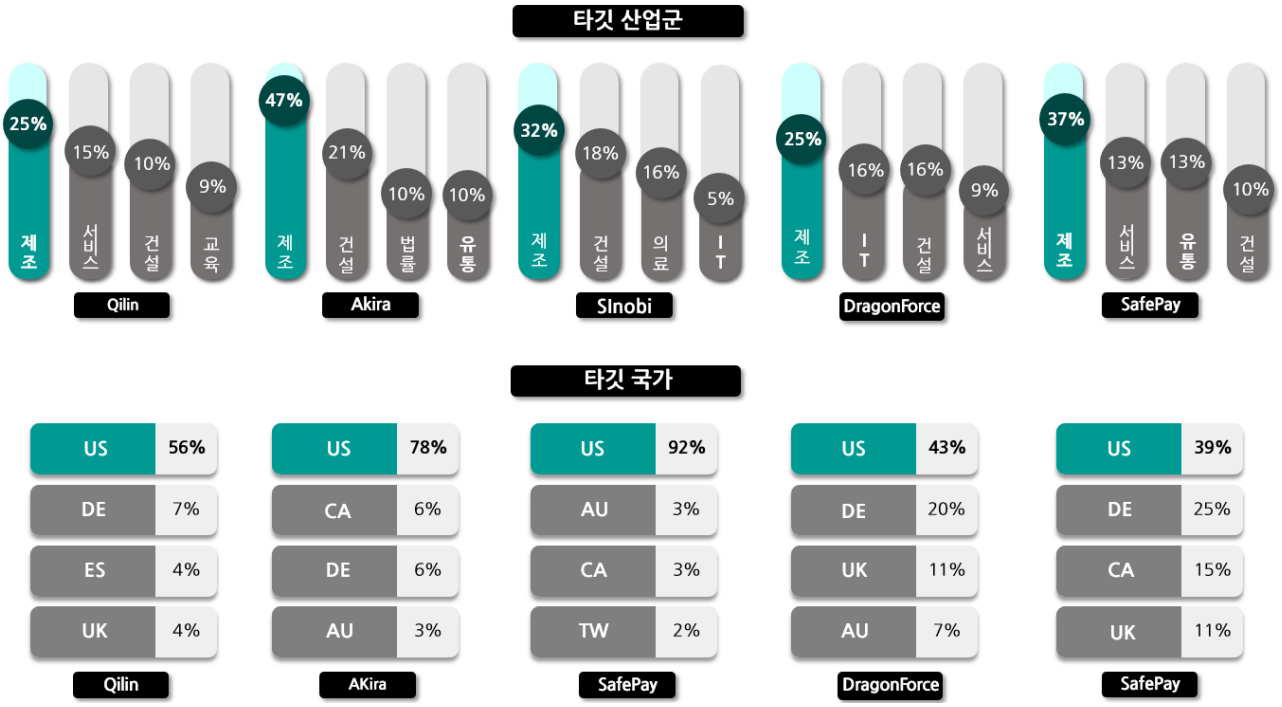

그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

Qilin 그룹은 8 월 20 일 일본의 닛산 디자인 자회사 Nissan Creative Box 를 공격해 약 4TB 분량의 내부 정보를 탈취했다고 주장했다. 이들은 자사 다크웹 유출 사이트에 생산 설계 자료와 각종 내부 문건의 목록을 게시하며, 추가 유출을 예고하는 등 강도 높은 협박을 이어갔다.

Akira 그룹은 8 월 말 미국의 과학 계측기기 제조사 The Fredericks Company 를 공격해 내부 재무자료와 직원·고객 데이터를 탈취했다고 밝혔다. 이들은 다크웹 유출 사이트에 수십 GB 의 정보 유출을 예고하며 피해사를 압박하는 전형적인 전술을 사용했다. 같은 시기, 미국의 교정치료 장비 제조사 RMO Orthodontics 또한 피해 대상으로 등재되었으며, Akira 는 추후 데이터 샘플을 공개하겠다고 경고했다.

Sinobi 그룹은 8 월 중순 호주의 에너지 기업 Energy Developments 를 공격해 운영자료 및 내부 보고서를 탈취했다. 공격자는 다크웹 유출 사이트를 통해 해당 기업의 공급망 및 전력 운영 관련 정보 일부를 공개하며 협박 수위를 높였다. 이외에도 미국의 중견 보험사 Eagan Insurance 와 투자사 Norwest Venture Partners 를 연이어 공격 대상으로 삼아, 고객·계약·내부 재무자료 등 다양한 유형의 정보 탈취를 주장했다.

DragonForce 그룹은 8 월 21 일 독일의 오디오 기기 제조업체 InEar GmbH 를 공격했다고 밝히며, Hear the Difference 브랜드 관련 제품 설계도 및 유통정보 등을 다크웹에 게시했다. 또한 미국의 전자기기 유통기업 ABM Wireless 와 뉴욕 소재 고급 골프클럽 Park Country Club 에 대한 공격도 연이어 게시했다.

SafePay 그룹은 8 월 29 일, 미국 코네티컷 주의 재가 요양 서비스 기관인 Companions & Homemakers 를 공격해 환자 관리 및 내부 인사 기록 등을 암호화하고 탈취했다고 주장했다. 이들은 자사 다크웹 유출 사이트에 피해사를 게시하고 곧 데이터를 전면 공개하겠다며 협상에 응할 것을 강하게 압박했다. 같은 날, 독일의 화장품 제조사 Lipcare.de 에 대해서도, 민감한 제조 문서와 고객 관련 데이터를 암호화했다고 밝혔다.

■ 랜섬웨어 집중 포커스

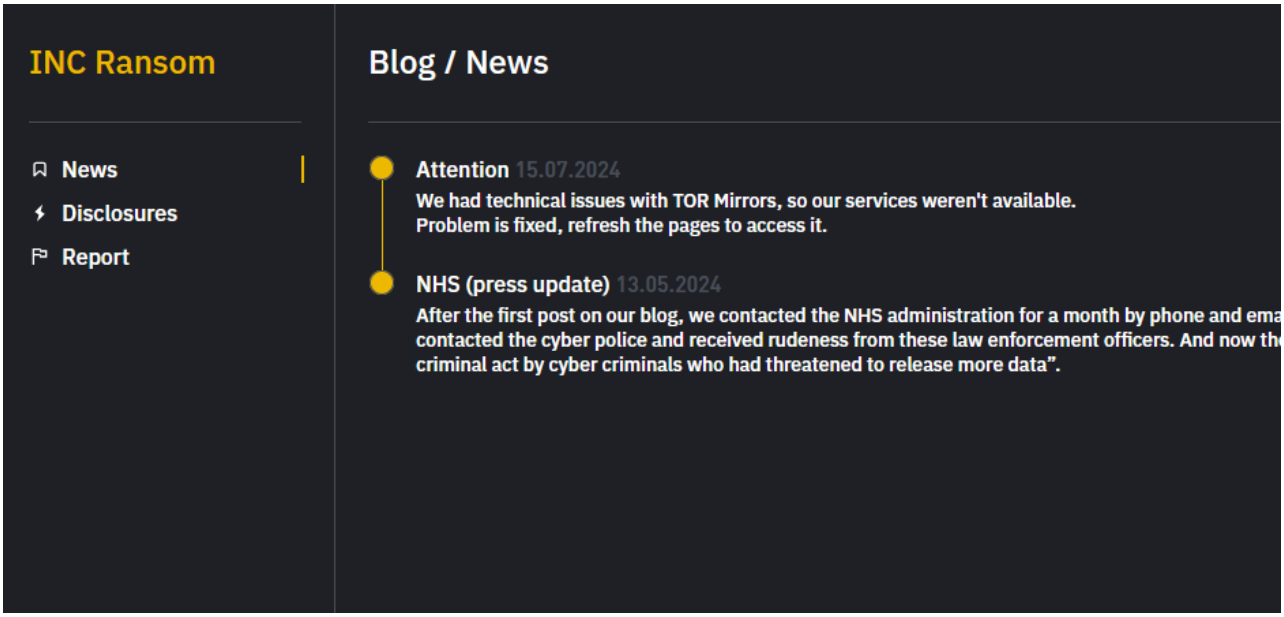

그림 6. INC 랜섬웨어 그룹의 다크웹 유출 사이트

INC 랜섬웨어 그룹은 2023 년 7 월 활동을 시작한 이후 2024 년 4 월 소스코드 판매 정황이 확인된 뒤에도 활동을 중단하지 않았으며, 최근에는 Rust 언어로 제작된 랜섬웨어를 사용해 활동하고 있다. 다크웹 유출 사이트에는 피해 게시가 누적되고, C/C++ 버전 이후 Rust 로 제작된 새로운 버전이 발견되었으며, 다크웹 유출 사이트에는 피해자를 꾸준히 공개했다.

피해 규모는 지속적으로 확대되고 있으며, 의료·제조·교육·공공 등 사회 기반을 구성하는 주요 분야까지 넓히고 있다. 이러한 양상은 INC 랜섬웨어 그룹이 특정 산업이나 지역에 국한되지 않고 폭넓은 대상을 노리며, 전 세계적으로 위협 활동을 확대해 나가고 있음을 보여준다.

본 보고서에는 새롭게 제작된 Rust 버전의 INC 랜섬웨어를 중점으로 분석해 랜섬웨어 위협에 효과적으로 대비할 수 있도록 하고자 한다.

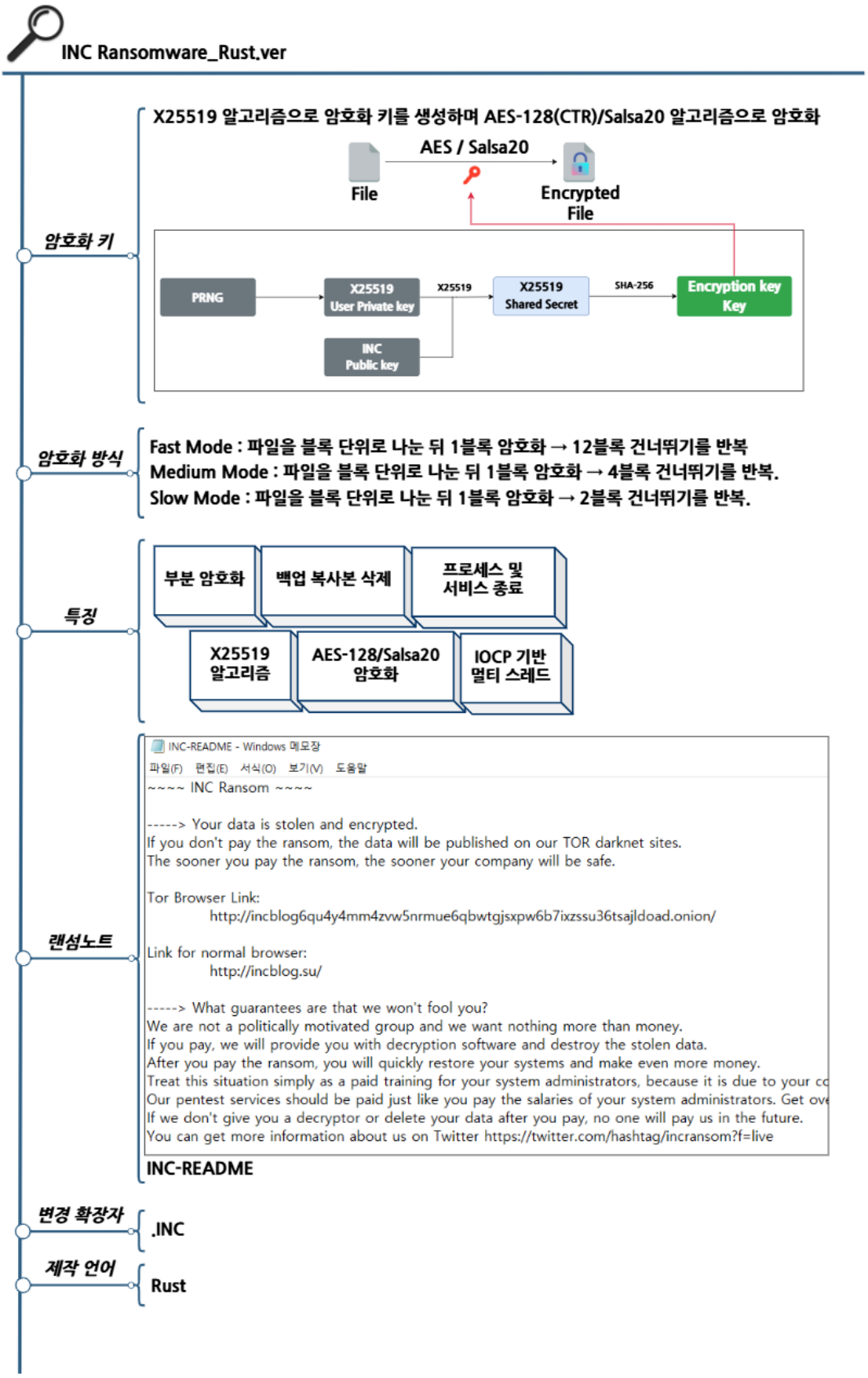

그림 7. INC 랜섬웨어 개요

INC 랜섬웨어 전략

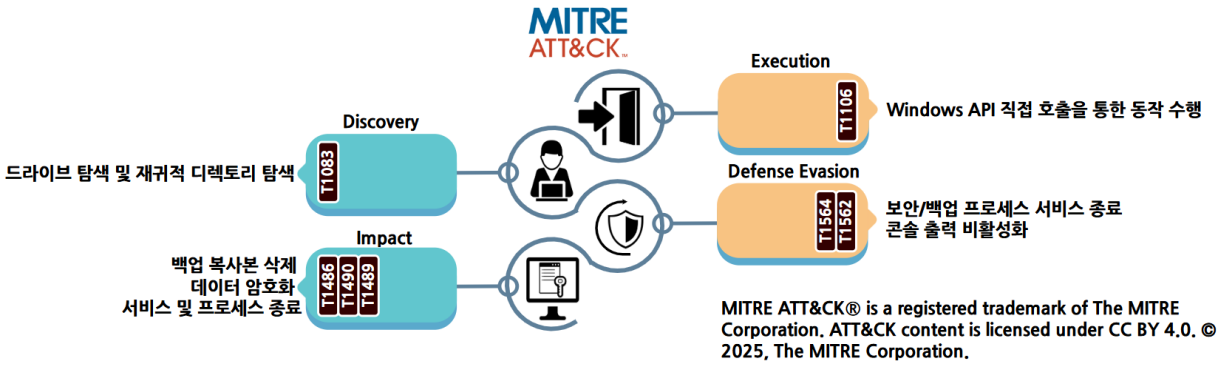

그림 8. INC 랜섬웨어 공격 전략

INC 랜섬웨어 Rust 버전은 실행 시 입력된 인자를 확인하여 기능을 제어한다. 실행에 반드시 필요한 인자는 없으며, 별도의 인자를 지정하지 않아도 랜섬웨어는 정상적으로 동작한다. 확인된 인자와 기능은 아래 표와 같다.

구분	설명
--def	파일 암호화 없이 랜섬노트만 저장
-h / --help	실행 도움 메시지 출력
--hide	콘솔창 숨기기
--sup	암호화 대상이 실행중이라면 해당 프로세스 종료
-v / --version	랜섬웨어 파일명 출력
--dir <directories>	암호화 대상 폴더 지정
--file <files>	암호화 대상 파일 지정
--mode <fast|medium|slow>	암호화 모드 설정 (기본: medium)
--proc <processes>	프로세스 종료 대상 설정
--serv <services>	서비스 종료 대상 설정

표 1. INC 랜섬웨어 실행 인자

INC 랜섬웨어는 실행 시 --proc, --serv 옵션을 통해 지정된 프로세스와 서비스를 종료할 수 있다. 사전에 내장된 고정 목록 대신, 공격자가 상황에 맞게 종료 대상을 유연하게 지정하는 구조다. 또한 --file, --dir 옵션으로 암호화 대상을 명시하지 않으면, 시스템의 모든 드라이브를 열거해 존재 여부와 유형을 확인한 뒤 암호화 대상으로 설정한다.

이때 --dir 인자로 암호화 대상 폴더를 지정한 경우나 전체 드라이브 암호화에서 특정 드라이브를 암호화하는 경우, 지정한 폴더와 그 하위 폴더를 재귀적으로 탐색하며 랜섬노트를 생성한 후 현재 디렉터리의 항목을 열거한다. 이 중 디렉터리는 예외 디렉터리 리스트와 비교해 제외 여부를 결정하고, 제외되지 않으면 탐색 함수를 재귀 호출해 하위 폴더를 계속 탐색한다. 파일은 예외 확장자 리스트와 비교하여 해당하지 않는 경우에만 암호화 대상에 포함한다. 확인되는 리스트는 아래 표와 같다.

예외 확장자 및 파일	예외 폴더
*.exe, *.log, *.dll, *.INC, INC-README.txt	windows, program files, appdata, $recycle.bin, programdata, all users, sophos

표 2. INC 랜섬웨어 암호화 예외 대상

INC 랜섬웨어에서 백업 복사본 삭제는 일반적으로 사용되는 Windows 유틸리티(vssadmin, wmic shadowcopy, wbadmin, bcdedit) 호출 없이, DeviceIoControl 을 직접 사용해 볼륨 섀도 복사본의 저장 공간을 작은 값으로 재설정하는 방식으로 수행된다. 이때 OS 는 저장 공간 부족 상태로 인식해 공간 확보를 위해 기존 백업 복사본을 자동으로 삭제하게 된다.

각 파일에 대해 32 바이트 난수로 X25519 키쌍을 생성하고, 하드코딩된 INC 의 공개키를 사용해 ECDH 공유 비밀을 만들어 암호화에 활용한다. 생성된 공유 비밀은 SHA-256 해싱 과정을 거쳐 파일 암호화 키로 사용한다. 블록 크기는 시스템 클러스터[8] 크기와 동일하게 설정한다. 파일을 해당 블록 단위로 분할한 뒤, 한 번에 1 블록만 암호화하고 이어지는 블록들은 설정된 간격만큼 건너뛰는 절차를 끝까지 반복한다. 설정되는 간격은 옵션에서 설정된 Fast/Medium/Slow 모드에 따라 각각 12/4/2 블록의 간격을 사용한다. 예를 들어 블록 크기가 0x10000 바이트(64KB), 클러스터의 크기가 0x1000 바이트(4KB), 암호화 모드가 Medium(default)인 경우 4KB 크기의 1 블록을 암호화한 뒤 16KB 크기만큼 건너뛰고 다음 4KB 크기의 1 블록을 암호화하는 형태로 반복 동작한다. 암호화 알고리즘은 하드웨어에 따라 선택되며, CPU 가 AES-NI 를 지원하면 AES-128, 미지원 시 Salsa20 을 사용한다.

[8] 시스템 클러스터: 파일시스템이 파일 데이터를 배치·관리할 때 사용하는 최소 할당 단위

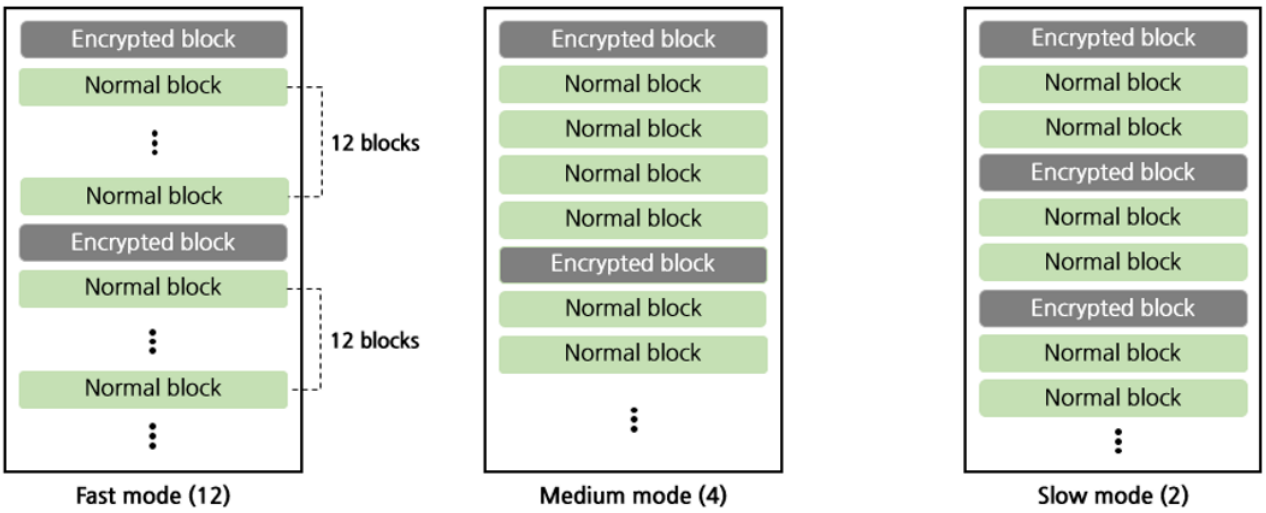

그림 9. INC 랜섬웨어 암호화 방식

파일 암호화가 완료되면 파일 끝에 83 바이트 Footer 를 추가한다. Footer 에는 순서대로 X25519 공개키, 공개키의 SHA-256, 암호화 알고리즘 구분자(0: AES-128, 1: Salsa20), 암호화 블록 크기, 암호화 간격, 암호화된 총 블록 수, "INC" 마커가 저장된다.

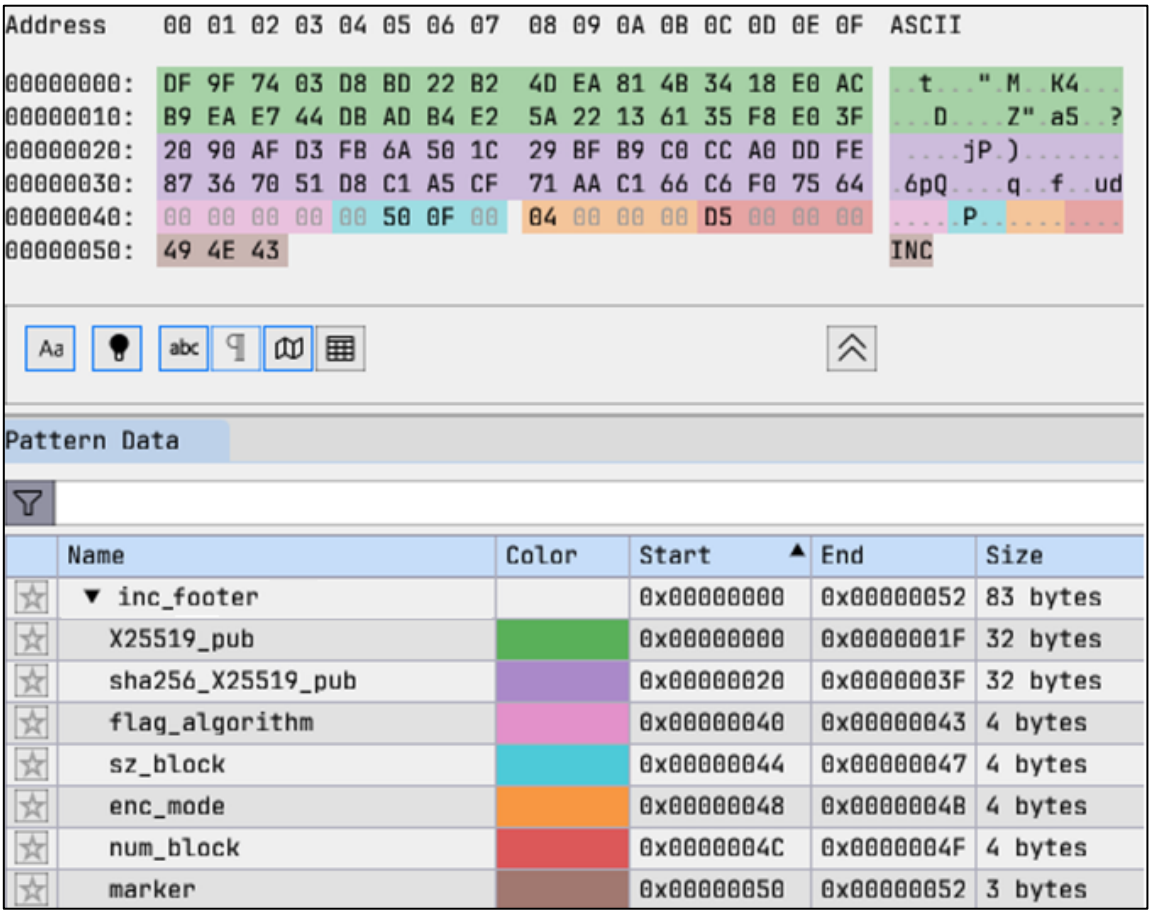

그림 10. 암호화 파일 Footer

INC 랜섬웨어 대응방안

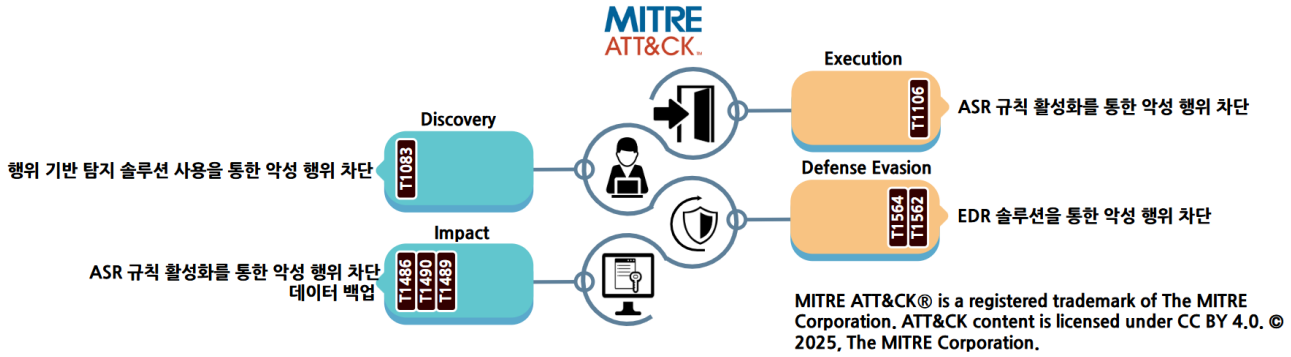

그림 11. INC 랜섬웨어 대응방안

INC 랜섬웨어는 실행 직후 보안 관련 서비스와 특정 프로세스를 강제 종료하고, 볼륨 섀도 복사본을 삭제한 뒤 부분 암호화를 진행한다. 이에 따라 ASR 규칙을 활성화하면, 백업 파괴·서비스 종료·암호화와 연관된 비정상 프로세스를 사전에 차단하여 악성 행위를 효과적으로 억제할 수 있다.

또한 EDR 솔루션을 도입하고 최신 보안 패치를 적용하여, 알려진 취약점을 통한 침투나 비정상적인 동작을 신속히 식별·차단할 수 있도록 해야 한다. 이를 통해 파일 암호화 과정에서 발생하는 행위 기반 패턴을 실시간으로 탐지하고, 악성 프로세스의 실행을 중단할 수 있다.

백업 복사본을 별도 네트워크 구간, 외부 저장소, 오프라인 매체에 주기적으로 분산해 두면 시스템이 암호화되더라도 복구할 수 있다. 이때 백업 장치에는 업무상 필요한 최소 권한만 부여하고, 정기 복구 테스트를 통해 백업 데이터의 무결성과 실제 복원 가능성을 확인하는 것이 중요하다.

IoCs

Hash(SHA-256)
17317ee3c9bd706ef2942a38f55c05176e4abdf377a5b72250d89ebf2a795ca0
fd0dbc6d941ff76e5204df4c644ba0d3241d05995f30e6b837618cd9dcc8b99c
b1815ef993b2649be791f0cf4249e502e7c3763fe69451b8b32508089e15d103
61f70b9a0bde499d764807fe24517e64ea0130a3f6e493ead360058e59854776
be9e1fd4dcf8a644aba70c8e92fa07a54d0ce96fb74217b48991700d281083bd

■ 참고 사이트

• Techradar (https://www.techradar.com/pro/security/the-first-ai-powered-ransomware-has-been-spotted-and-heres-why-we-should-all-be-worried)

• Cyberscoop (https://cyberscoop.com/ai-ransomware-promptlock-nyu-behind-code-discovered-by-security-researchers)

• NYU (https://engineering.nyu.edu/news/large-language-models-can-execute-complete-ransomware-attacks-autonomously-nyu-tandon-research)

• Bankinfosecurity (https://www.bankinfosecurity.com/rise-chaos-ransomware-tied-to-blacksuit-groups-exit-a-29067)

• SC Media (https://www.scworld.com/news/cephalus-ransomware-abuses-sentinelone-executable-for-dll-sideloading)

• Bleepingcomputer (https://www.bleepingcomputer.com/news/security/akira-ransomware-abuses-cpu-tuning-tool-to-disable-microsoft-defender/)

• Justice.gov (https://www.justice.gov/opa/pr/justice-department-announces-coordinated-disruption-actions-against-blacksuit-royal)

• Brinztech (https://www.brinztech.com/breach-alerts/brinztech-alert-partnership-program-of-desolator-ransomware-service-is-detected)