Keep up with Ransomware

Sinobi 랜섬웨어와 Lynx 그룹과의 연계 정황 분석

■ 개요

2025 년 12 월 랜섬웨어 피해 사례 수는 지난 11 월(740 건) 대비 약 15% 상승한 854 건으로 집계됐다.

프랑스 내무부는 지난 12 월 내부 이메일 서버가 사이버 공격을 받아 다수의 이메일 계정과 기밀문서에 무단 접근이 이루어졌다고 밝혔다. 조사 결과, 해커는 경찰관의 이메일 계정을 탈취해 최초로 침투한 후 평문으로 공유된 비밀번호를 확보한 것으로 밝혀졌다. 확보한 비밀번호로 내부 인증 시스템을 침투하는 과정에서, 경찰 데이터베이스에도 접근한 정황이 확인됐다. 한편 해킹 포럼인 BreachForums 에서 운영자로 추정되는 Indra 계정에 이번 공격을 주장하는 글이 올라왔다. 프랑스 당국이 ShinyHunters 와 연관된 인물들을 체포한 것에 대한 보복을 언급하며, 내무부 침해와 대규모 데이터 접근을 과시하는 내용이 포함됐다. 게시글에는 약 1,640 만 건 규모의 데이터 접근을 시사하는 내부 시스템 검색 결과에 대한 스크린샷과 일부 경찰 기록 관련 신원 정보가 담긴 이미지와 함께 프랑스 정부를 향해 일주일 내로 협상하라는 요구 메시지도 담겼다. 이번 사건은 계정 탈취와 더불어 기본적인 보안 원칙을 준수하지 않아 발생한 것으로 알려졌다. 계정 관리와 인증 체계를 강화하고 접근 권한 최소화 및 인증, 로그인 로그 기반 이상 징후 탐지 체계를 고도화할 필요가 있음을 시사했다.

공격자가 직접 침투하는 방식이 아닌, 보안 사고 대응 분야 종사자가 공격자와 공모한 정황이 사법당국 수사로 드러난 사례가 확인됐다.

미국 법무부는 2025 년 12 월, BlackCat(ALPHV) 랜섬웨어 조직과 공모한 미국인 Ryan Goldberg 와 Kevin Martin 을 미국 내 피해자를 공격해 금전을 갈취한 혐의로 기소했다. 수사 내용에 따르면 Ryan Goldberg 는 사이버 보안 기업에서 사고 대응 업무 담당자였고, Kevin Martin 은 랜섬웨어 사고 대응을 지원하는 기업에서 협상 업무를 맡았던 것으로 확인됐다. 이들은 보안 기업에서 습득한 사이버 보안 훈련과 경험을 바탕으로 기업의 네트워크를 암호화하고 몸값을 요구했다. 수익 분배의 경우 사전에 합의한 뒤 피해자가 지급한 몸값 중 일부를 운영진에게 전달하는 방식으로 공모 관계를 유지한 것으로 밝혀졌다.

2025 년 12 월 5 일 React2Shell 취약점(CVE-2025-55182)을 악용한 Weaxor 랜섬웨어 배포 사례도 있었다. 해당 취약점은 인증 절차 없이 취약한 서버에서 원격 코드 실행이 가능하며, 공격자는 PowerShell 을 통해 CobaltStrike[1] 기반 C&C[2] 서버를 확보한 뒤, Weaxor 랜섬웨어를 실행해 파일을 암호화했다. 공격자는 보안 업데이트가 적용되지 않은 취약한 시스템을 노렸으며, 특히 해당 취약점이 12 월 3 일 공개된 뒤 불과 이틀 만인 12 월 5 일에 악용된 점을 고려하면, 소프트웨어 및 보안 장비에 대한 신속한 취약점 대응이 필수적이다.

[1] Cobalt Strike: 공격자가 원격 명령 실행, 추가 페이로드 투하, 내부 정찰 및 수평 이동을 수행하기 위해 사용하는 C&C 프레임워크

[2] C&C(Command & Control) 서버: 감염된 시스템과 통신하며 명령 전달, 추가 페이로드 배포, 정보 수집 등 공격자의 원격 제어를 수행하는 서버

■ 랜섬웨어 뉴스

프랑스 내무부 이메일 서버 침해 정황

- 프랑스 내무부의 내부 이메일 서버가 공격을 받아 다수의 계정과 기밀 문서에 대한 무단 접근 발생
- 해커는 경찰관 이메일 계정을 탈취한 뒤 이메일로 주고받은 비밀번호를 확보해 내부 인증 시스템을 우회
- BreachForums에 운영자로 추정되는 계정이 침해를 주장하며 대규모 데이터 접근을 과시하고 협상을 요구

미국 법무부 BlackCat 공모 미국인 2명 유죄 인정 발표

- 미국 법무부 랜섬웨어 조직과 공모해 금전을 갈취한 미국인 2명(Ryan Goldberg, Kevin Martin)이 유죄를 인정했다고 발표
- Ryan Goldberg와 Kevin Martin은 미국 기업 네트워크를 암호화하고 몸값을 요구한 혐의를 인정
- 사고 대응, 협상 업무 경험을 악용해 수익 분배를 합의 후 피해자가 지급한 몸값 일부를 운영진에게 전달 정황 확인

React2Shell 악용 Weaxor 랜섬웨어 배포 사례 확인

- React2Shell 취약점(CVE-2025-55182) 악용으로 취약 서버에서 원격 코드 실행 후 랜섬웨어가 실행된 정황 확인
- 공격자는 침투 직후 PowerShell로 Cobalt Strike 기반 C&C 채널을 확보한 뒤 랜섬웨어를 실행해 파일 암호화를 수행

12월 신생 그룹 7개 등장

- 12월에 등장한 신규 랜섬웨어 그룹 7곳 모두 자체 다크웹 유출 사이트를 운영
- 이 중 Osiris, MS13-089, MintEye를 제외하면 현재까지 유출 사이트에 게시된 피해 사례는 확인되지 않음

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

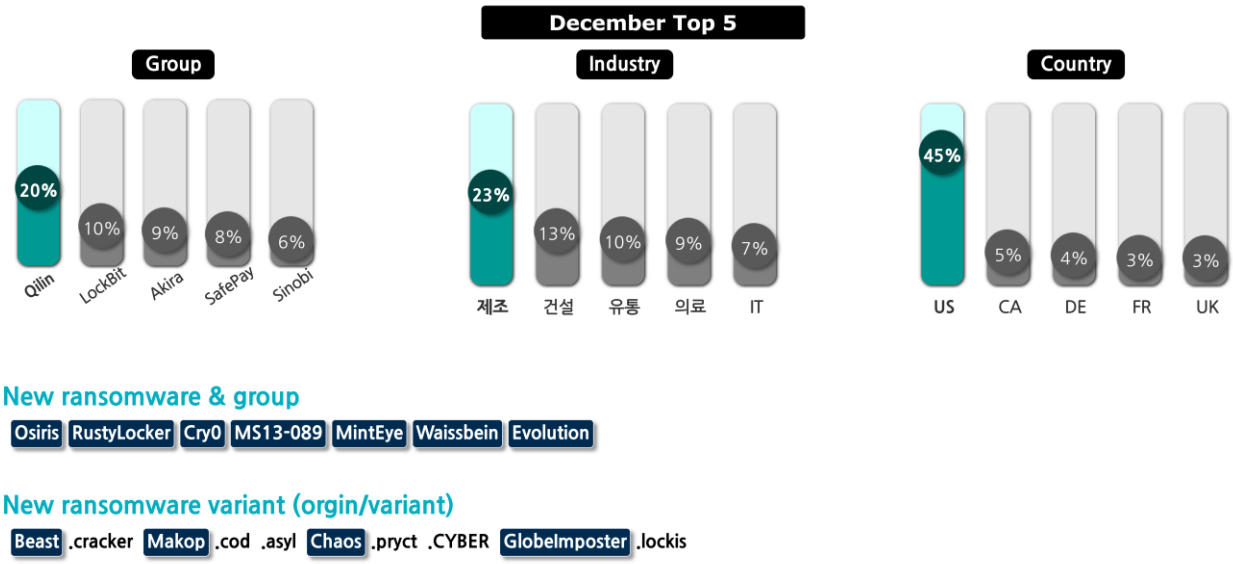


그림 2. 2025 년 12 월 랜섬웨어 위협 현황

새로운 위협

12 월에는 총 7 개의 신규 랜섬웨어 그룹이 등장했다. 이들 모두 다크웹 유출 사이트를 운영하지만, 현재까지 피해 게시물을 업로드한 사례는 일부에 그친다. Osiris 는 1 건, MS13-089 는 2 건, MintEye 는 5 건의 피해 게시물을 유출 사이트에 게시했다. 그 외 나머지 그룹은 다크웹 유출 사이트만 개설해 둔 상태로, 피해 사례는 아직 확인되지 않고 있다.

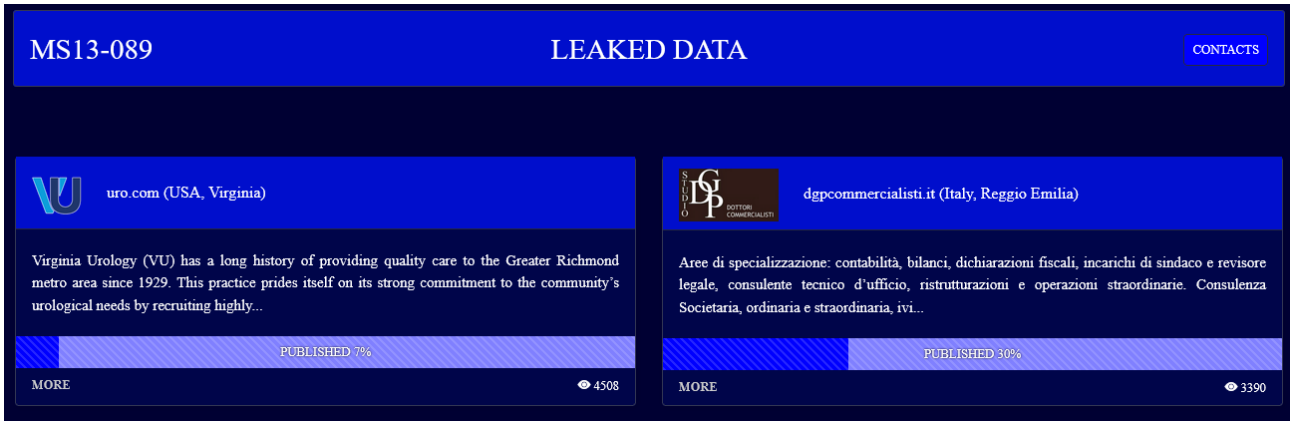


그림 3. MS13-089 의 다크웹 유출 사이트

2025 년 12 월에 등장한 MS13-089 그룹은 현재까지 총 2 건의 피해 게시물을 업로드했다. 또한 데이터를 공개하는 과정에서 공개 진행률을 백분율(%)로 구체적으로 표기해 피해자를 압박하는 특징이 확인된다.

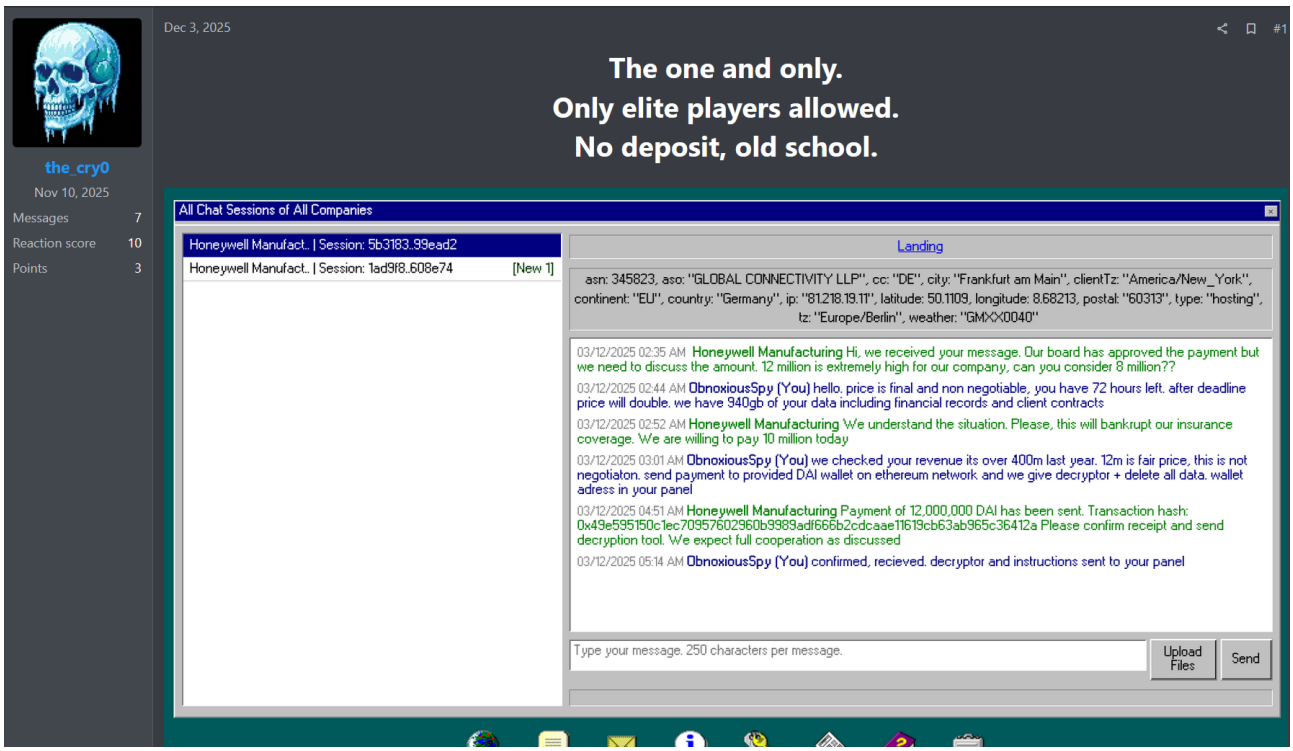


그림 4. Cry0 랜섬웨어 그룹의 RaaS[3] 홍보글

Cry0 그룹은 2025 년 12 월 3 일부터 러시아 해킹 포럼인 RAMP 에서 구성원을 모집하기 시작했다. 이들은 기업별 협상 세션을 관리하는 채팅 패널 화면과 실제 협상 로그를 게시해 운영 능력을 홍보했으나, 현재까지 다크웹 유출 사이트에 게시된 실제 피해자 명단은 확인되지 않고 있다.

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

Top5 랜섬웨어

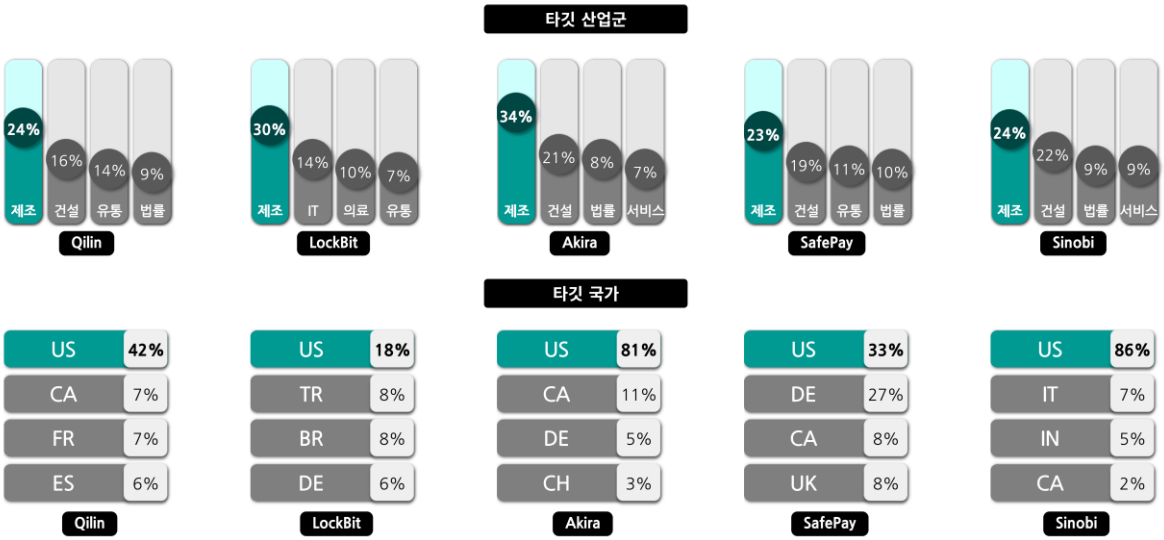


그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

12 월 가장 많은 피해를 발생시킨 랜섬웨어 그룹은 Qilin 그룹이다. 대표적으로 Qilin 그룹은 12 월 29 일 미국 코네티컷주의 Goodwin University 를 공격해 학생 및 직원의 개인정보를 포함한 약 140GB 규모의 데이터를 탈취한 후, 그룹 다크웹 유출 사이트에 공개했다.

LockBit 은 2025 년 9 월 LockBit 5.0 을 출시하며 재정비를 예고했지만, 이후 한동안 뚜렷한 활동은 관측되지 않았다. 그러나 12 월부터는 피해자를 연달아 게시하며 활동 강도를 높였다. 대표적으로 12 월 19 일 미국 아이오와주의 Clarinda Regional Health Center 를 공격한 뒤 환자와 직원들의 개인정보 공개를 예고했다. 12 월 22 일에는 브라질 상파울루의 Colégio Miguel de Cervantes 를 공격해 학생 성적, 행정 서류 등의 정보를 게시했다.

Akira 그룹은 2025 년 SonicWall 방화벽의 접근 제어 미흡 취약점(CVE-2024-40766)을 집중적으로 악용했다. 다수의 사례가 이를 주요 침투 경로로 삼은 것이 확인됐다. 공격자는 해당 취약점을 통해 유효한 VPN 세션을 탈취하거나 자격 증명을 확보해 내부망에 침투한 뒤, 랜섬웨어를 실행하고 데이터를 탈취했다. 이와 별개로 Akira 그룹은 2025 년 12 월 24 일 미국 미네소타주의 전력협동조합인 Agralite Electric Cooperative 를 공격해 사회보장번호와 세금 문서 등 민감정보가 포함된 약 136GB 규모의 데이터를 탈취했다. 또한 12 월 25 일 덴마크의 건축 설계 회사 Friis & Moltke Architects 를 공격해 도면 파일과 계약서 등이 포함된 약 12GB 규모의 데이터를 유출하겠다고 협박했다.

SafePay 그룹은 2025 년 12 월 29 일 영국의 유통 노동조합 Usdaw 를 공격해 조합원의 개인정보와 내부 문건이 포함된 데이터를 탈취했다. 또한 같은 날 아르헨티나의 의료기업 Investigaciones Médicas 를 공격해 환자 검진 데이터와 의료 자료 등의 민감한 정보를 취득했다고 주장했다.

Sinobi 그룹은 2025 년 12 월 7 일 미국의 에너지 산업 서비스 업체 Quality Companies 를 공격해 업무 문서와 계약 정보 등이 포함된 약 40GB 규모의 데이터를 탈취한 뒤, 이를 다크웹 유출 사이트에 공개했다. 또한 미국의 전기 설계 업체 Homestead Electrical Contracting 을 공격해 내부 자료를 유출하겠다고 협박했다.

■ 랜섬웨어 집중 포커스

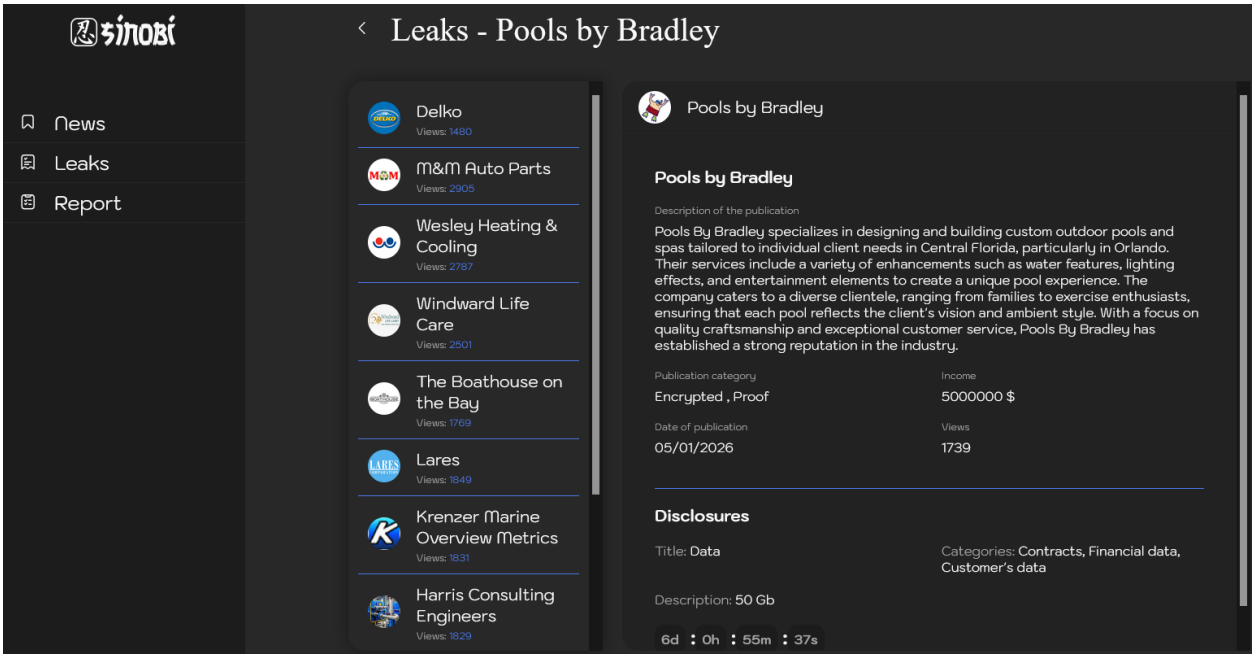


그림 6. Sinobi 그룹의 다크웹 유출 사이트

Sinobi 랜섬웨어 그룹은 2025 년 7 월에 발견되었다. 현재까지 다크웹 유출 사이트에 피해 조직 221 곳을 공개했다. 유출 게시물에는 피해 조직의 이름과 정보, 게시 일자뿐 아니라 탈취 자료의 종류와 샘플 데이터를 함께 제시하고 있다. 파일 암호화와 데이터 탈취 공개를 병행하는 이중 갈취 방식으로 피해 조직을 협박한다. 또한, 피해 조직마다 몸값을 다르게 요구하는데 적게는 500 만(한화 약 72 억) 달러에서 최고 4,400 만 달러(한화 약 640 억)으로 확인돼 평균 약 2,400 만 달러(한화 약 349 억)의 금액 규모다.

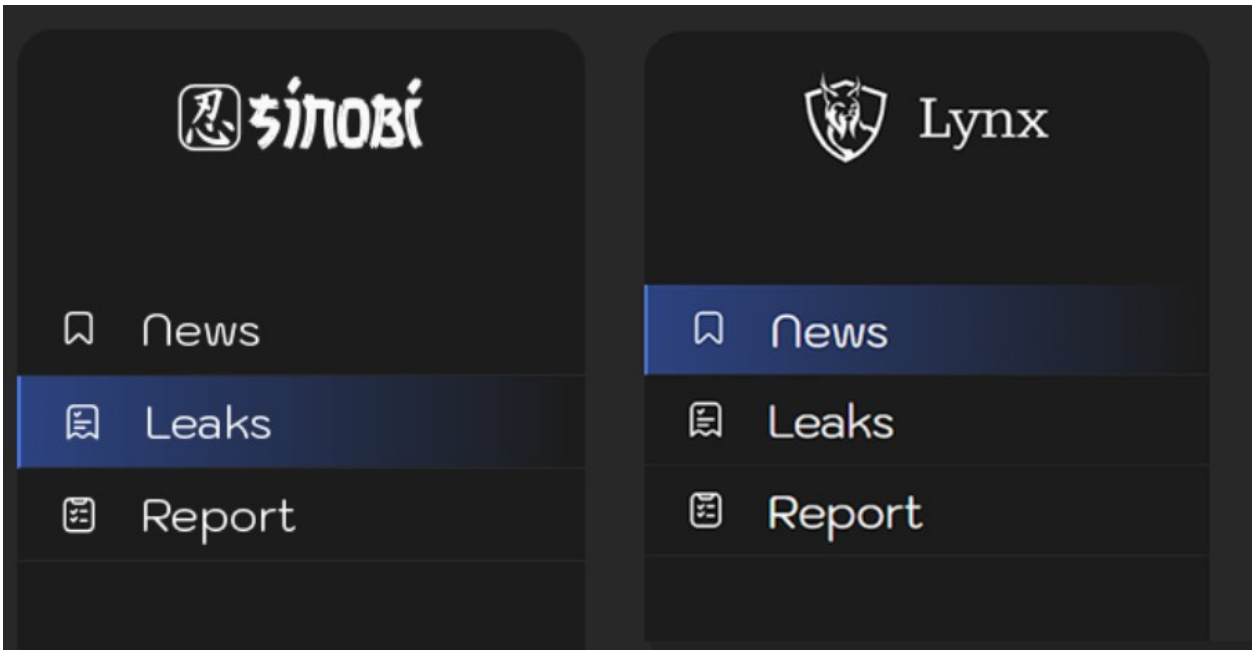


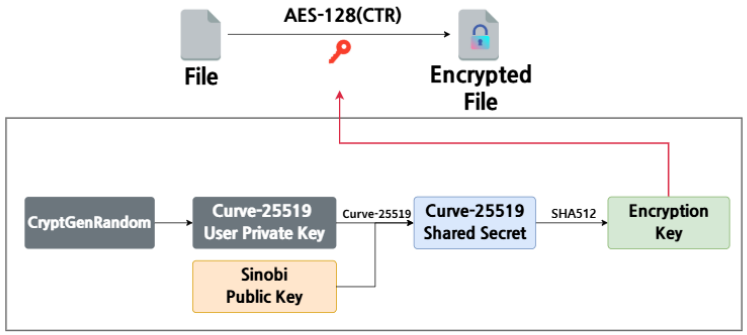
그림 7. 다크웹 유출 사이트 비교(좌: Sinobi, 우: Lynx)

또한 Sinobi 그룹은 INC 소스 코드 거래 정황 이후 등장한 Lynx 계열과 유사성을 보인다. Lynx 는 INC 랜섬웨어에서 확인된 코드 구성 및 기능 흐름과 유사한 특징을 보이며, Sinobi 역시 Lynx 와 암호화 방식 및 실행 인자 구조가 유사한 특징이 확인된다. 즉, INC-Lynx-Sinobi 세 그룹은 코드와 구조적 측면에서 연관성이 있다. 특히, Lynx 와 Sinobi 의 다크웹 유출 사이트는 UI 와 메뉴 구성이 유사해 동일 운영 주체 또는 협력 관계 가능성도 제기된다. 이에 따라 본 보고서는 다가오는 위협에 대비하기 위해 INC–Lynx–Sinobi 간 연관 정황을 종합하고, Sinobi 랜섬웨어의 상세 분석 내용을 공유하고자 한다.

Sinobi Ransomware

암호화 키

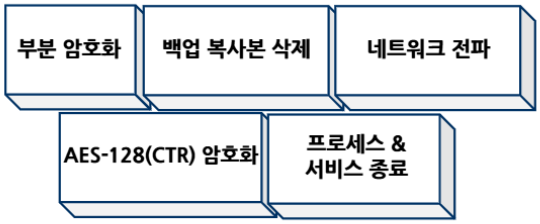
Curve-25519 알고리즘으로 암호화 키를 생성하며 AES-128(CTR) 알고리즘으로 암호화



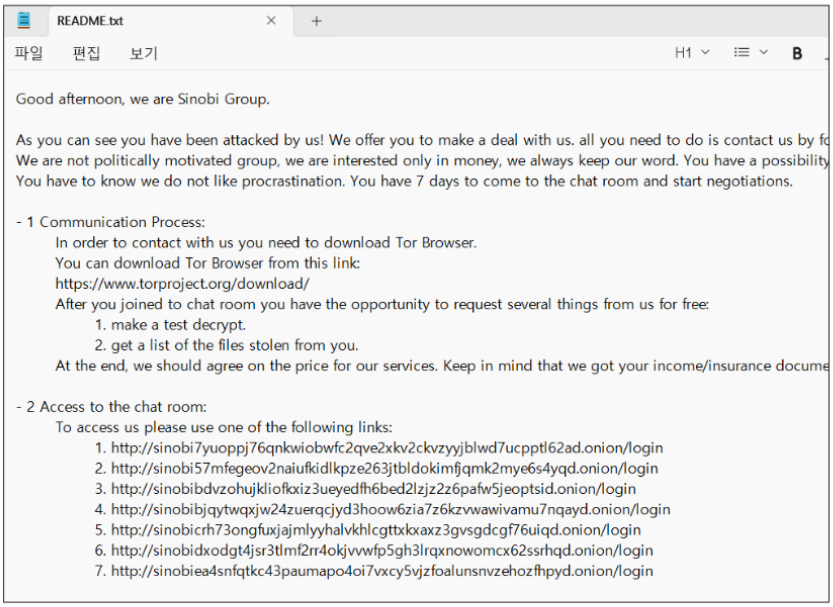
암호화 방식

Files ≤ 1MB: 전체 암호화
Files > 1MB: 선택한 모드(entire / fast / medium / Slow)에 따라
→ 파일 크기의 100% / 5% / 15% / 25%만 부분 암호화

특징



랜섬노트


README.txt

파일 편집 보기

Good afternoon, we are Sinobi Group.

As you can see you have been attacked by us! We offer you to make a deal with us. all you need to do is contact us by fo
We are not politically motivated group, we are interested only in money, we always keep our word. You have a possibility
You have to know we do not like procrastination. You have 7 days to come to the chat room and start negotiations.

- 1 Communication Process:
  In order to contact with us you need to download Tor Browser.
  You can download Tor Browser from this link:
  https://www.torproject.org/download/
  After you joined to chat room you have the opportunity to request several things from us for free:
    1. make a test decrypt.
    2. get a list of the files stolen from you.
  At the end, we should agree on the price for our services. Keep in mind that we got your income/insurance docume

- 2 Access to the chat room:
  To access us please use one of the following links:
    1. http://sinobi7yuoppj76qnkwiobwfc2qve2xkv2ckvzyyjblwd7ucpptl62ad.onion/login
    2. http://sinobi57mfegeov2naiufkidlkpze263jtbldokimfjqmk2mye6s4yqd.onion/login
    3. http://sinobibdvzohujkliofkxiz3ueyedfh6bed2lzjz2z6pafw5jeoptsid.onion/login
    4. http://sinobibjqytwqxjw24zuerqcjyd3hoow6zia7z6kzvwawivamu7nqayd.onion/login
    5. http://sinobicrh73ongfuxjajmlyyhalvkhlcgttxkxaxz3gvsgdcgf76uiqd.onion/login
    6. http://sinobidxodgt4jsr3tlmf2rr4okjvvwfp5gh3lrqxnowomcx62ssrhqd.onion/login
    7. http://sinobiea4snfqtkc43paumapo4oi7vxcy5vjzfoalunsnvzehozfhpyd.onion/login

README.txt

변경 확장자

.SINOBI

제작 언어

C/C++

그림 8. Sinobi 랜섬웨어 개요

랜섬웨어 전략

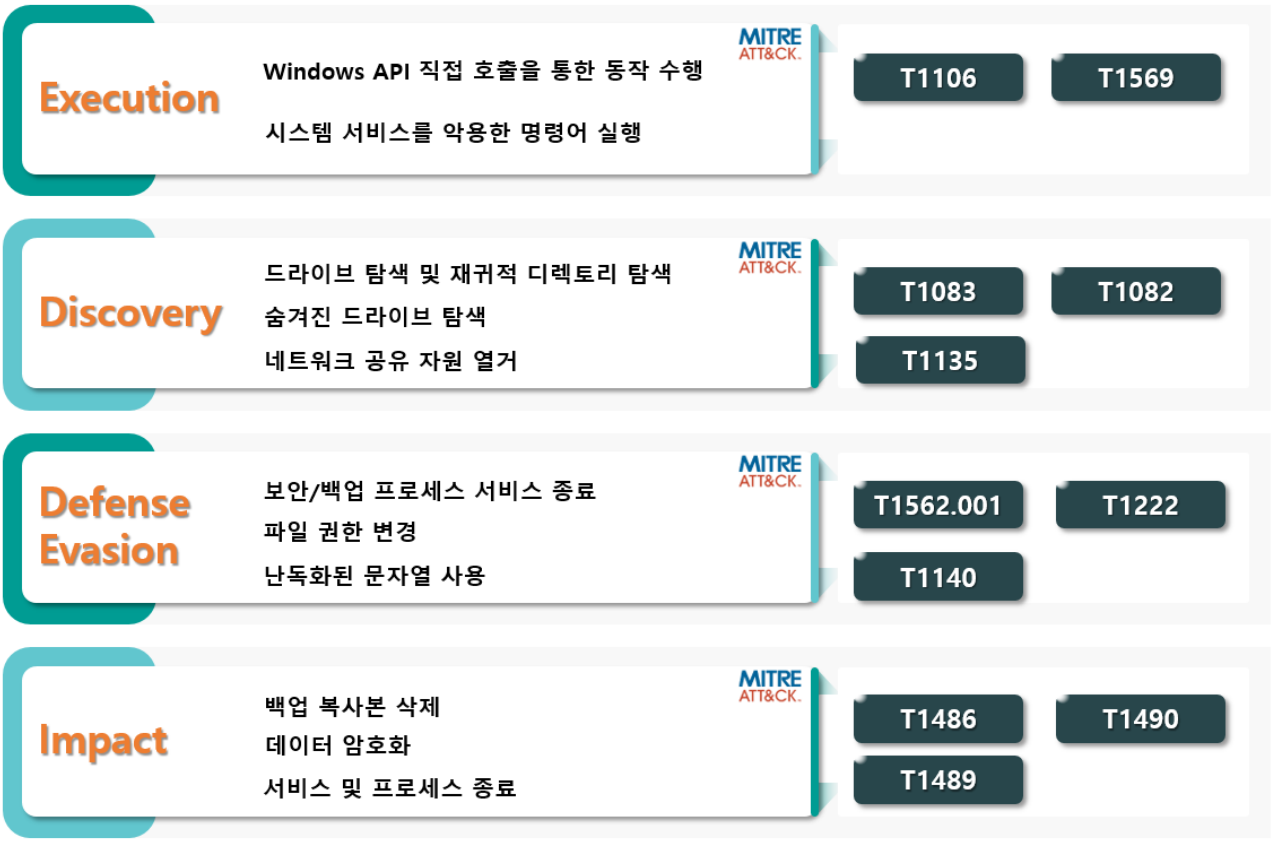


그림 9. 랜섬웨어 공격 전략

Sinobi 랜섬웨어는 다양한 실행 인자를 사용해 암호화 대상이나 방식을 정밀하게 제어할 수 있도록 설계되어 있어, 공격자는 암호화 대상과 전체 혹은 부분 암호화를 수행할 수 있는 모드 등을 설정할 수 있다. 이때 사용되는 인자와 기능은 아래 표와 같다.

인자	설명
--file <filePath>	암호화 대상 파일 지정
--dir <dirPath>	암호화 대상 폴더 지정
--mode <mode>	암호화 모드 설정 (Entire / Fast / Medium / Slow)
--help	실행 도움 메시지 출력
--verbose	로그 출력
--silent	확장자 미변경, 랜섬노트 미생성
--hide-cmd	콘솔창 숨기기
--no-background	배경화면 변경 기능 비활성화
--no-print	랜섬노트 출력 기능 비활성화
--stop-processes	파일 암호화 직전, 대상 파일이 실행중인 경우 프로세스 종료
--kill	특정 프로세스 및 서비스 종료
--encrypt-network	네트워크 공유까지 암호화 대상으로 포함
--load-drives	숨겨진 드라이브 마운트
--safe-mode	안전모드 부팅

표 1. 랜섬웨어 실행인자

Sinobi 랜섬웨어와 INC 및 Lynx 랜섬웨어의 실행 인자를 비교한 결과, 세 랜섬웨어는 상당 부분에서 공통된 기능을 공유하고 있으나 일부 인자 구성에서는 차이가 확인된다. 먼저 암호화 모드 설정 기능은 Sinobi와 INC에서 제공되지만 Lynx에서는 확인되지 않았다. Sinobi는 --mode 인자를 통해 암호화 모드를 설정할 수 있고 INC 역시 --mode 로 암호화 모드를 설정할 수 있다. 반면 Lynx 는 이를 제어하는 인자가 확인되지 않는다. 또한 확장자 변경 및 랜섬노트 생성 생략 기능은 Sinobi 에서만 제공된다. Sinobi 는 --silent 인자를 사용하면 확장자 변경과 랜섬노트 생성을 수행하지 않지만, Lynx 와 INC 에서는 동일한 기능의 인자가 확인되지 않았다. 이러한 차이점을 제외하면, 세 랜섬웨어는 실행 인자 수준에서 제공하는 나머지 주요 기능이 전반적으로 동일한 구성을 보인다.

```
if ( DeviceIoControl(FileW, 0x53C028u, &InBuffer, 0x18u, 0, 0, &BytesReturned, 0) )
{
  if ( byte_140033C78 )
    printf_1(L"[+] Successfully delete shadow copies from %c:/\n", i);
```

그림 10. 백업 복사본 삭제

Sinobi 랜섬웨어는 Lynx 랜섬웨어와 동일한 방식으로, 암호화 작업을 수행하기 전 복구 방해를 위해 백업 복사본을 삭제한다. 이를 위해 DeviceIoControl 함수를 호출해 백업 복사본이 저장되는 공간의 최대 용량을 낮게 재설정한다. 그 결과 시스템은 저장 공간이 부족하다고 판단하고, 공간을 확보하는 과정에서 기존에 생성된 백업 복사본을 자동으로 삭제한다.

또한 랜섬웨어는 --kill 인자를 사용하면 원활한 파일 암호화를 위해 특정 프로세스와 서비스를 종료한다. 종료 대상 프로세스 및 서비스는 아래 표와 같으며, 해당 목록은 Lynx 랜섬웨어에서 확인된 항목과 동일한 것으로 확인된다.

프로세스	서비스
sql, veeam, backup, exchange, java, Notepad	sql, veeam, backup, exchange

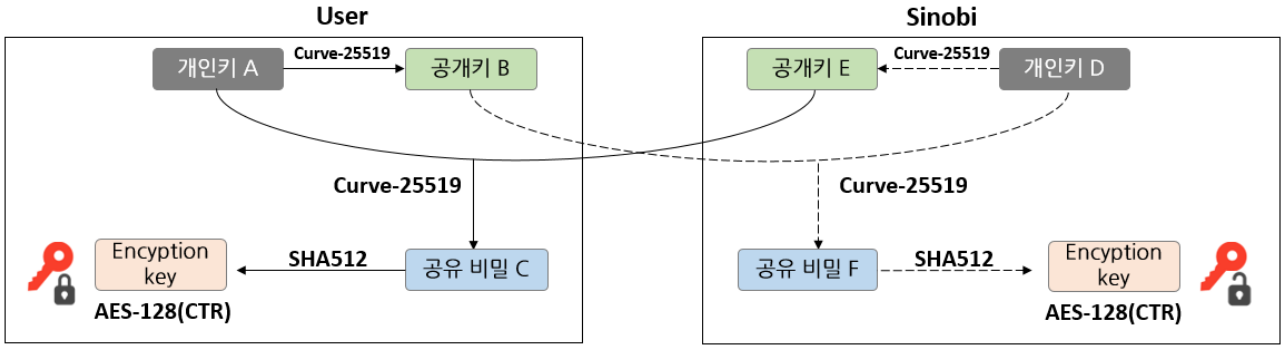
표 2. 프로세스 및 서비스 종료 대상

파일 암호화는 --file 인자 사용 시 특정 파일만 암호화하며, --dir 인자 사용 시에는 지정한 경로에 존재하는 파일만 암호화한다. 두 인자가 모두 입력되지 않으면 예외 대상을 제외한 모든 파일을 암호화하며, 확인된 예외 대상은 아래 표와 같다.

암호화 제외 경로	확장자 및 파일명
Windows, Program Files, Program Files (x86), $RECYCLE.BIN, AppData	.exe, .msi, .dll, .SINOBI, README.txt

표 3. 암호화 예외 대상

Sinobi 랜섬웨어와 Lynx 랜섬웨어의 암호화 예외 대상은 대부분 동일하나, 일부 항목에서 차이가 확인된다. Sinobi 랜섬웨어는 이미 암호화된 파일을 중복으로 암호화하지 않기 위해 ".SINOBI" 확장자를 예외 대상으로 추가한 반면, Lynx 랜섬웨어는 ".lynx" 확장자를 예외 대상으로 사용한다.



공유 비밀 C = 공유 비밀 F

그림 11. 암호화 키 생성 방식

Sinobi 랜섬웨어는 파일 암호화를 위해 파일마다 고유한 32 바이트 개인키(A)를 생성한다. 이후 하드코딩된 공격자의 공개키(B)와 Curve-25519 연산을 수행해 공유 비밀(C)을 생성한다. 이때 공유 비밀이란, Curve-25519 알고리즘에서 양측이 각자의 개인키와 상대방의 공개키만으로 동일하게 계산되는 값을 의미한다. 즉 피해자의 개인키(A)와 공격자의 공개키(B)로 계산한 값(C)은, 공격자의 개인키(D)와 피해자의 공개키(E)로 계산한 값(F)과 동일하며, 이 동일한 값(C, F)을 공유 비밀이라고 한다. 이때 생성된 공유 비밀은 바로 사용되지 않고 SHA-512 로 해시되어 파생키로 변환되며, 최종적으로 이 파생키를 사용해 AES-128(CTR) 알고리즘으로 파일 암호화를 수행한다. 암호화가 완료되면 Sinobi 는 파일의 끝에 피해자의 공개키(E)를 저장한다. 공격자는 이 공개키(E)와 자신이 보유한 개인키(D)를 이용해 공유 비밀을 다시 계산할 수 있으며, 같은 방식으로 해시를 적용해 파생키를 생성함으로써 해당 파일을 복호화할 수 있다.

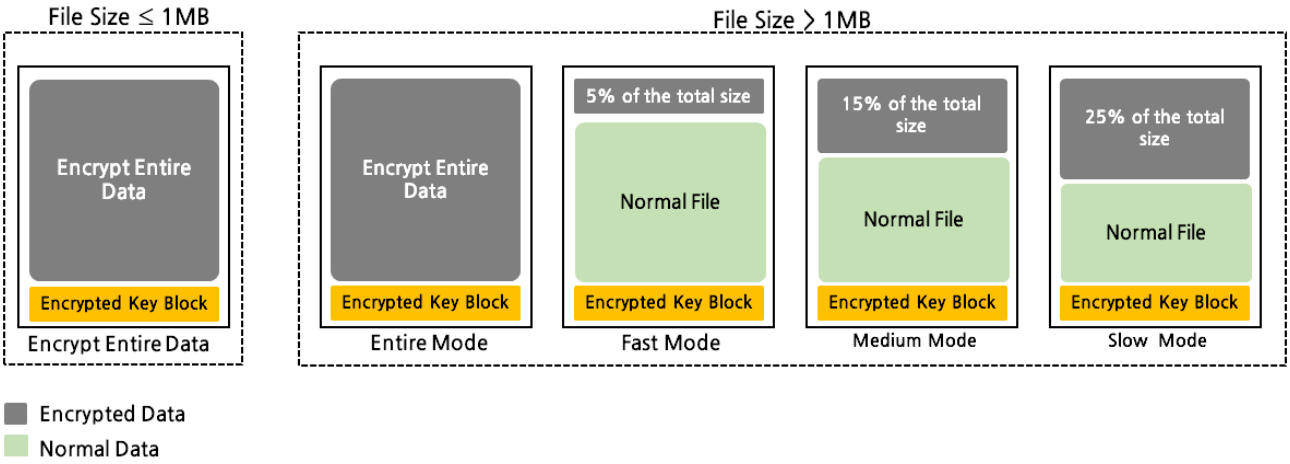


그림 12. 파일 암호화 방식

파일 암호화 범위는 파일 크기와 사용되는 인자에 따라 달라진다. 크기가 1MB 이하인 파일은 인자와 상관없이 전체 데이터가 암호화된다. 1MB 를 초과하는 파일의 경우에는 인자에 따라 파일 크기의 일부만 암호화한다. Entire 모드는 파일 전체가 암호화되고, Fast 모드는 파일의 5%, Medium 모드는 15%, Slow 모드는 25%를 암호화하는 방식이다. 암호화가 완료되면, 파일 크기나 암호화 모드와 관계없이 모든 파일의 끝에는 고정된 메타데이터 블록이 추가된다. 이 블록에는 복호화에 사용되는 공개키와 해당 파일에 적용된 암호화 모드 정보, 그리고 감염 여부를 식별하기 위한 “SINOBI” 마커가 함께 저장된다.

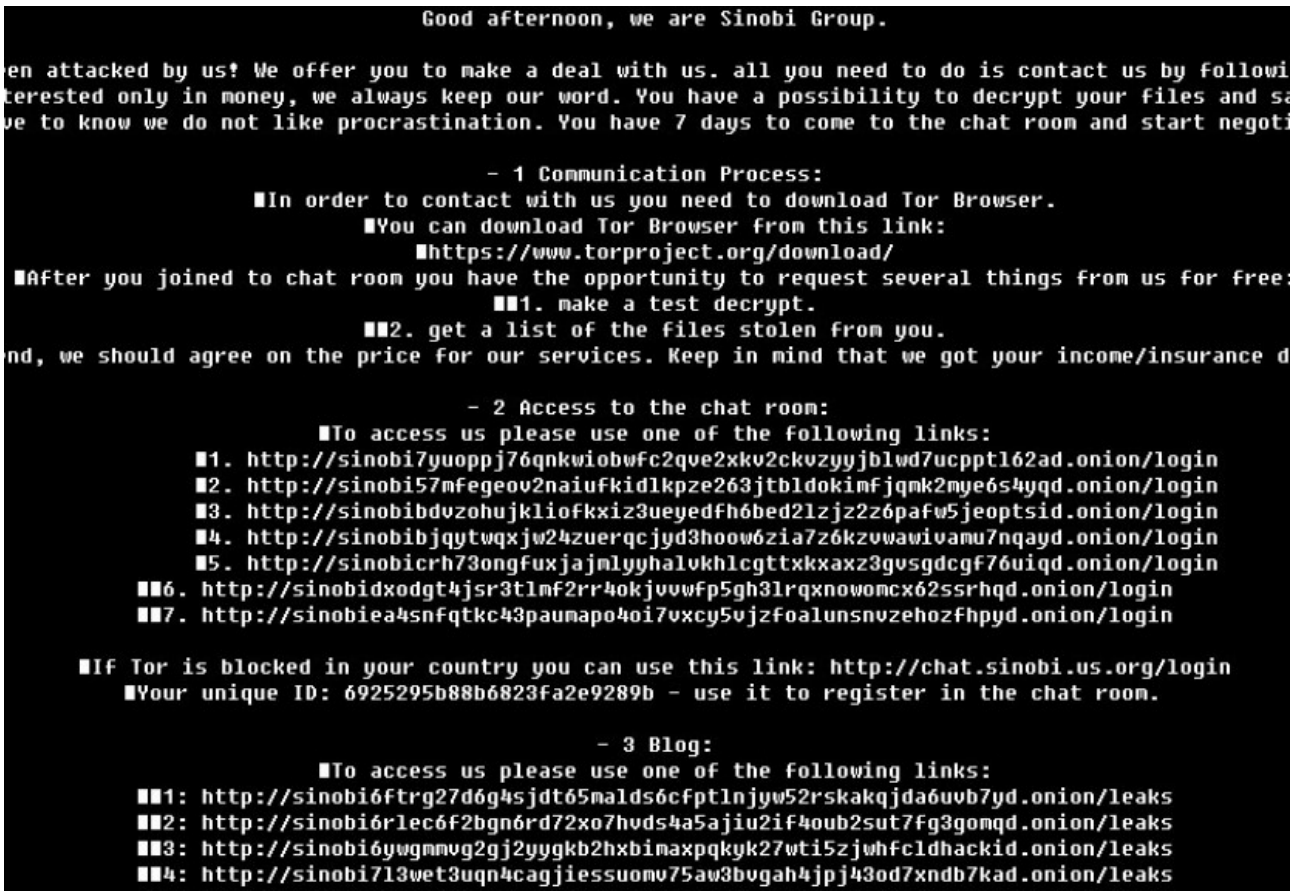


그림 13. 변경된 바탕화면

파일 암호화가 완료되면, 랜섬웨어는 실행 시점에 랜섬노트 텍스트를 포함한 바탕화면 이미지를 생성해 디스크에 저장한다. 이후 해당 이미지 경로를 HKCU\Control Panel\Desktop\Wallpaper 레지스트리 값에 설정하고 바탕화면을 변경함으로써, 피해자가 랜섬노트 내용을 즉시 확인하도록 유도한다.

랜섬웨어 대응방안

그림 14. 랜섬웨어 대응방안

Sinobi 랜섬웨어는 실행 시 복구를 방해하기 위해 VSS 와 백업과 관련된 프로세스 및 서비스를 종료한다. 이에 대비하기 위해 ASR[4] 규칙 활성화를 통해서 비정상적인 프로세스 동작을 차단하고, 랜섬웨어의 악성 행위를 막을 수 있다.

또한, EDR 솔루션 도입과 최신 보안 패치 적용으로 취약점을 악용한 침투나 비정상적인 행위를 신속히 식별하고 차단할 수 있도록 해야 한다. 백업 복사본은 별도의 네트워크 구간이나 외부 저장소, 오프라인 매체에 주기적으로 분산 백업해, 시스템이 암호화되더라도 데이터 복구가 가능하게 해야 한다. 이때 백업 장치 접근 권한을 최소화하고, 정기적으로 복구 테스트를 실시하여 백업 데이터의 무결성을 보장해야 한다.

마지막으로, Sinobi 랜섬웨어는 네트워크 공유 파일도 암호화하므로 네트워크 공유 자원의 접근권한을 최소화하거나 비활성화해 외부 리소스에 접근하지 못하도록 해야 한다.

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

IoCs

Hash(SHA-256)
9432B065C803BAA54F1FEFAC20D97AFFCE212DEC2BB9A597FC010064D391FC24
1B2A1E41A7F65B8D9008AA631F113CEF36577E912C13F223BA8834BBEFA4BD14
D4919A7402D7AE02516589FBDFB3CC436749544052843A37B5D36AC4B7385B18

■ 참고 사이트

• U.S. Department of the Justice(https://www.justice.gov/opa/pr/two-americans-plead-guilty-targeting-multiple-us-victims-using-alphv-blackcat-ransomware)

• Reuters(https://www.reuters.com/world/cyberattack-french-interior-ministrys-email-servers-compromised-more-than-20-2025-12-17/)

• Le Parisien(https://www.leparisien.fr/faits-divers/une-attaque-tres-grave-cinq-minutes-pour-comprendre-la-cyberattaque-qui-a-vise-le-ministere-de-linterieur-17-12-2025-ISX6EVWKDFCLLEZKHA2RBJFECA.php)

• S-RM(https://www.s-rminform.com/latest-thinking/react2shell-used-as-initial-access-vector-for-weaxor-ransomware-deployment)