Keep up with Ransomware

Lynx 랜섬웨어의 등장과 INC 그룹과의 연계 가능성 분석

■ 개요

2024년 8월 랜섬웨어 피해 사례는 지난 7월(415건) 대비 약 12% 증가한 464건을 기록했다. 이번 달에는 전체 피해뿐만 아니라 국내 피해도 소폭 증가했다.

8 월 15 일, 해커 그룹 CyberNiggers 에서 활동하는 인텔브로커(IntelBroker)는 해커 커뮤니티 브리치포럼(BreachForums)에 국내 취업정보 사이트 커리어넷의 데이터베이스(DB)를 판매한다는 글을 올렸다. IntelBroker는 약 160만 건의 아이디, 비밀번호, 이메일 등의 회원 정보를 탈취했다고 주장했다. 이후 8 월 23 일, 커리어넷은 개인정보 유출 사실을 인정하고 이를 안내했다. 커리어넷은 유출된 데이터가 2018 년 4 월 이전의 것이며, 아이디를 제외한 이름과 비밀번호 같은 주요 정보는 암호화되어 복호화가 불가능하다고 설명했다.

IntelBroker는 추가적으로 국내 데이터를 공개했다. 8월 24일, 한국 정부가 커리어넷 DB 게시글에 관여하려 했다는 이유로 국방부 데이터를 BreachForums 에 공개했다. 공개된 정보는 재난안전통신망과 관련된 내용으로, 이들은 관리자 대시보드 접속 스크린샷을 증거로 제시하고 경보용 알람 음성 파일을 교체했다고 주장했다. 이외에도, 국내 퍼스널 트레이너 플랫폼 회원 및 트레이너 400 만 명의 회원 정보를 판매한다는 글과 국내 독서 및 학습관리시스템(LMS[1]) 플랫폼 기업 토핑의 회원 정보를 판매한다는 글도 추가로 게시했다.

랜섬웨어 그룹의 다크웹 유출 사이트에도 국내 기업의 피해 사례가 확인됐다. 8 월 11 일, 헌터스(Hunters) 그룹은 국내 자동차 열관리 솔루션 기업 한온시스템의 데이터를 판매한다는 게시글을 업로드 했다. 8 월 14 일에는 직원 정보, 이력서, 재무제표 등 개인정보와 내부 기밀 데이터를 포함한 2.3TB 의 데이터를 전부 공개했다. 한온시스템은 과거 Snatch(22 년 1 월), Egregor(20 년 11 월) 랜섬웨어에 의해 이미 두 차례 유출된 이력이 있어, 사고 발생 후의 적절한 조치가 중요함을 증명하는 계기가 됐다.

[1] LMS(Learning Management System): 학습자의 학습을 지원하고 관리하는 온라인 시스템

8 월 23 일에는 엘도라도(Eldorado) 랜섬웨어 그룹이 국내 소재의 데브옵스(DevOps) 전문 컨설팅 기업을 공격했다고 주장했다. 다크웹 게시글에는 소스 코드가 나열된 파일 리스트를 샘플로 제공하며, 1.5BTC(한화 약 1 억 2 천만 원)에 판매하고 있다.

랜섬웨어 데이터를 여러 차례 중복 게시하는 특징을 보이며 작년부터 활동해 온 디스포제서(Dispossessor) 그룹은 2024 년 8 월 주요 인프라를 압수당했다. 8 월 13 일, 미국 연방수사국(FBI), 미국 법무부(DoJ), 독일 주 형사경찰서(LKA), 영국 국립범죄청(NCA), 독일 밤베르크 검찰청은 Dispossessor 의 데이터 유출 사이트와 공격에 사용된 서버를 압수했다. 미국 서버 3 개, 영국 서버 3 개, 독일 서버 18 개, 미국 기반 도메인 8 개, 독일 기반 도메인 1 개가 압수 대상이었다.

8 월에는 소프트웨어 개발 시 배포 및 통합 서비스를 제공하는 자동화 도구 젠킨스(Jenkins)의 취약점을 악용한 랜섬웨어 공격 시도도 발견되었다. 이 취약점은 2024 년 1 월에 패치된 명령 처리 단계 문제로, 공격자가 내부 시스템의 파일을 임의로 읽을 수 있는 취약점이다. Jenkins 취약점은 3 월부터 본격적으로 악용되었으며, 7 월에는 랜섬엑스(RansomEXX) 그룹이 인도 은행에 기술 서비스를 제공하는 Brontoo Technology Solutions 를 공격할 때 사용되었다. 8 월에는 IntelBroker 가 IT 서비스 제공 업체 BORN Group 공격에 이를 악용한 것으로 밝혀졌다.

7 월 말 새로 등장한 Lynx 랜섬웨어는 INC 랜섬웨어의 소스코드를 구매해 사용하고 있다는 정황이 발견되었다. INC 랜섬웨어는 올해 5 월 다크웹 포럼에 랜섬웨어 소스코드를 30 만 달러(한화 약 4 억 원)에 판매한다는 글을 올린 적이 있다. Lynx 랜섬웨어를 분석한 결과, INC 랜섬웨어와 기능적으로 거의 동일하며, 바이너리 분석 프로그램인 BinDiff 로 비교한 결과 약 45%의 코드 유사도를 보였다.

■ 랜섬웨어 뉴스

infosec

국내 취업 정보 사이트 커리어넷 DB, 해킹 포럼 사이트에서 판매

- 8월 15일, IntelBroker는 커리어넷의 DB 데이터를 판매하는 글을 BreachForums에 게시
- 판매하는 데이터는 총 160만여 개의 규모이며, 공개된 샘플 데이터에 따르면 ID, PW, E-mail 등 회원 정보로 추정

IntelBroker, 국방부 데이터 공개

- 8월 15일 업로드한 커리어넷 DB 판매 글을 한국 정부가 관여하려 했다며, 보복을 목적으로 8월 23일 국방부 데이터 공개
- 공개된 샘플 및 이미지에 따르면 재난안전통신망 관련 데이터로 추정
- 관리자 패널에 로그인 한 스크린샷을 공개했으며, 경보 음성 파일을 임의로 변경

해킹 포럼 BreachForums 관리자 변경

- 24년 5월 FBI, 미국 법무부(DOJ)에 의한 BreachForums 시스템 압수 이후 ShinyHunters가 관리
- 8월 22일 BreachForums의 관리자인 Owner가 ShinyHunters에서 IntelBroker로 변경

LockBit 랜섬웨어, 다크웹 유출 사이트에 연락처 공개

- 해킹 포럼 BreachForums를 통해서 모집
- 자격 요건으로 "백인이며 인종차별주의자"가 있으며, 유출한 데이터를 무료로 공개하는 등 실제 공격 증거를 요구

Dispossessor 랜섬웨어, 공격 인프라 압수

- 8월 13일 FBI, DOJ, 독일 주 형사 경찰서(LKA), 영국 국립 범죄청(NCA), 독일 밤베르크 검찰청에 의해 주요 인프라 압수
- 미국 서버 3개, 영국 서버 3개, 독일 서버 18개, 미국 기반 도메인 8개, 독일 기반 도메인 1개 압수
- FBI는 과거 피해자에게 인터넷 범죄 신고 센터나 유선 연락을 통해 Dispossessor 그룹에 대한 정보 공유 요청

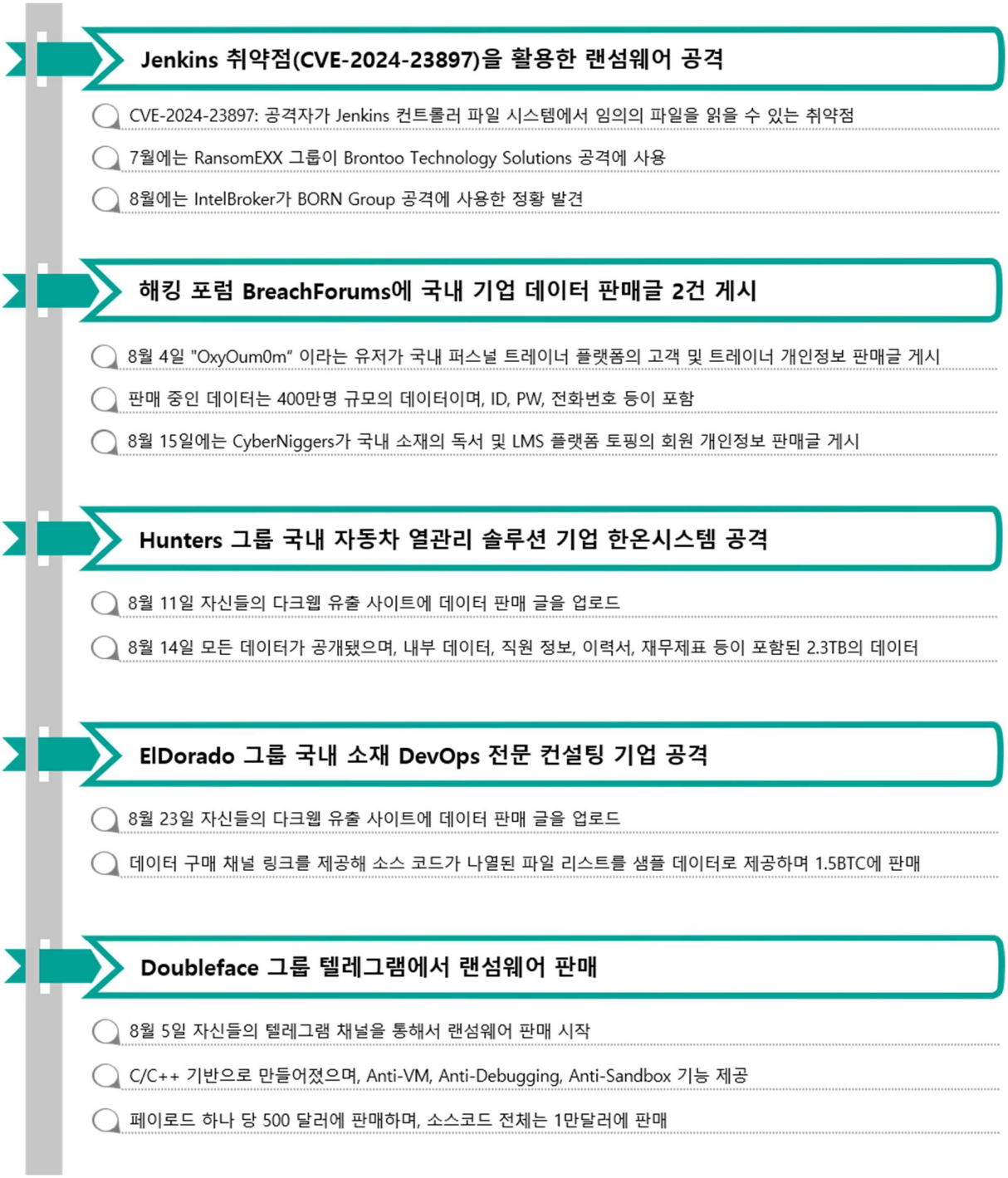

Jenkins 취약점(CVE-2024-23897)을 활용한 랜섬웨어 공격
CVE-2024-23897: 공격자가 Jenkins 컨트롤러 파일 시스템에서 임의의 파일을 읽을 수 있는 취약점
7월에는 RansomEXX 그룹이 Brontoo Technology Solutions 공격에 사용
8월에는 IntelBroker가 BORN Group 공격에 사용한 정황 발견
해킹 포럼 BreachForums에 국내 기업 데이터 판매글 2건 게시
8월 4일 "OxyOum0m" 이라는 유저가 국내 퍼스널 트레이너 플랫폼의 고객 및 트레이너 개인정보 판매글 게시
판매 중인 데이터는 400만명 규모의 데이터이며, ID, PW, 전화번호 등이 포함
8월 15일에는 CyberNiggers가 국내 소재의 독서 및 LMS 플랫폼 토핑의 회원 개인정보 판매글 게시
Hunters 그룹 국내 자동차 열관리 솔루션 기업 한온시스템 공격
8월 11일 자신들의 다크웹 유출 사이트에 데이터 판매 글을 업로드
8월 14일 모든 데이터가 공개됐으며, 내부 데이터, 직원 정보, 이력서, 재무제표 등이 포함된 2.3TB의 데이터
ElDorado 그룹 국내 소재 DevOps 전문 컨설팅 기업 공격
8월 23일 자신들의 다크웹 유출 사이트에 데이터 판매 글을 업로드
데이터 구매 채널 링크를 제공해 소스 코드가 나열된 파일 리스트를 샘플 데이터로 제공하며 1.5BTC에 판매
Doubleface 그룹 텔레그램에서 랜섬웨어 판매
8월 5일 자신들의 텔레그램 채널을 통해서 랜섬웨어 판매 시작
C/C++ 기반으로 만들어졌으며, Anti-VM, Anti-Debugging, Anti-Sandbox 기능 제공
페이로드 하나 당 500 달러에 판매하며, 소스코드 전체는 1만달러에 판매

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

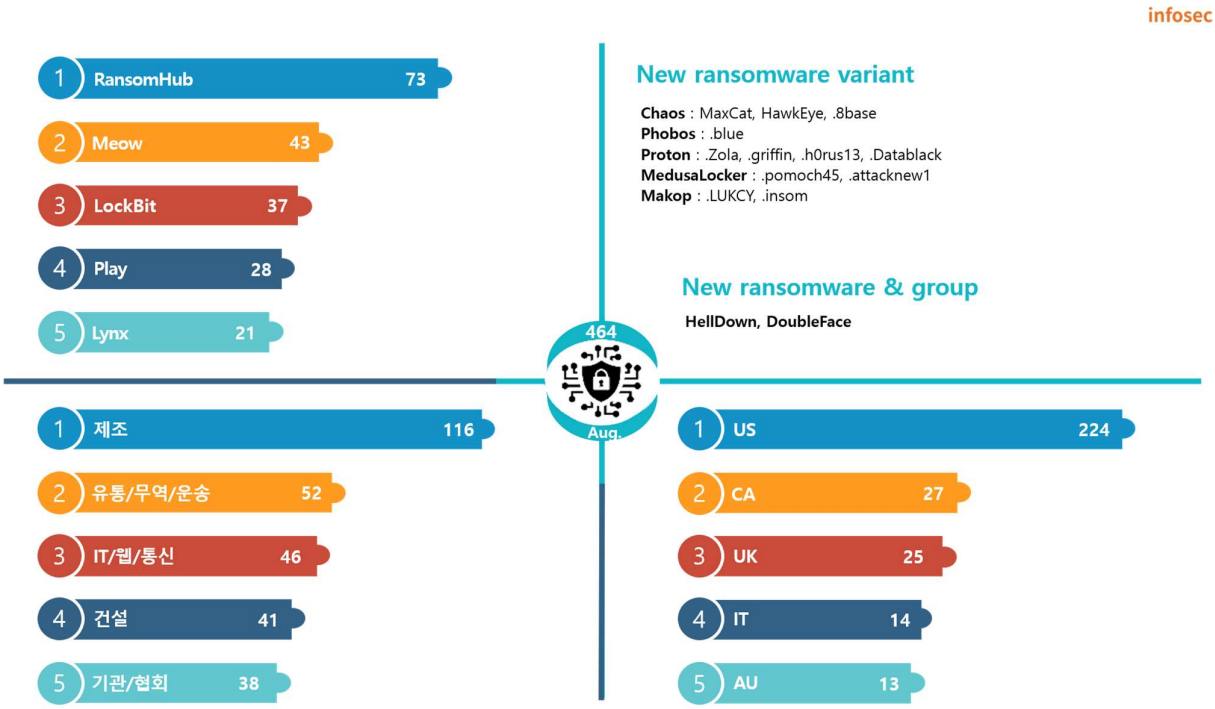


그림 2. 2024 년 8 월 랜섬웨어 위협 현황

새로운 위협

8 월에 발견된 새로운 사이버 위협은 총 2 건으로, 이는 지난달에 비해 크게 감소한 수치다. 특히 8 월 13 일 등장한 HellDown 랜섬웨어 그룹은 다크웹에 데이터 유출 사이트를 개설한 후, 첫날에만 9 건의 피해자를 공개했다. 이후 10 일간 8 건을 추가해, 활동을 시작한 지 10 일 만에 총 17 건의 피해자를 게시했다. 피해자 중에는 대만에 위치한 글로벌 네트워킹 및 보안 솔루션 업체인 Zyxel Networks 도 포함되어 있으며, 이들은 253GB 에 달하는 급여 명세서와 재무제표 등 내부 정보를 탈취했다고 주장했다. 그러나 8 월 24 일 이후로는 다크웹 유출 사이트에 접속할 수 없는 상태가 계속되고 있다.

한편, Doubleface 그룹은 8 월 5 일 텔레그램 채널을 개설하고, 이를 주로 활용해 활동하고 있다. X(구 트위터)에서도 활동하며, 텔레그램 메시지를 통해 자신들이 금전을 목적으로 하는 해커 집단임을 밝히고 있다. 또한 X 의 소개란에서 자신들을 러시아 해커 그룹 APT66 으로 지칭하고 있다. 이들은 랜섬웨어 정보뿐만 아니라 다수의 웹사이트 변조 공격도 감행하고 있으며, HexaLocker, 랜섬허브(RansomHub), God Team, LETGH0ST 같은 공격자 그룹들과 제휴를 맺었다고 발표했다. 다만 RansomHub 와의 제휴 게시글은 현재 삭제된 상태다.

그림 3. Doubleface 랜섬웨어

Doubleface 그룹은 텔레그램 채널 개설 당일, 랜섬웨어 판매 게시글을 올렸으며, 해당 랜섬웨어는 AES 와 RSA 알고리즘을 사용해 파일을 암호화하고 Anti-VM, Anti-Debugging, Anti-Sandbox 기능을 제공한다고 홍보하고 있다. 랜섬웨어 실행 영상에 따르면, 파일 암호화뿐만 아니라 복호화 키 입력 창을 강제로 고정하여 화면을 제어하는 기능도 포함되어 있다. 그러나 복호화 키의 진위를 확인하지 않고 무작정 복호화를 시도하기 때문에, 잘못된 키를 입력할 경우 파일이 영구적으로 손상될 위험이 있다. 해당 랜섬웨어의 페이로드는 개당 500 달러(한화 약 67 만 원)이며, 전체 소스코드는 1 만 달러(한화 약 1,340 만 원)에 판매되고 있다.

Top5 랜섬웨어

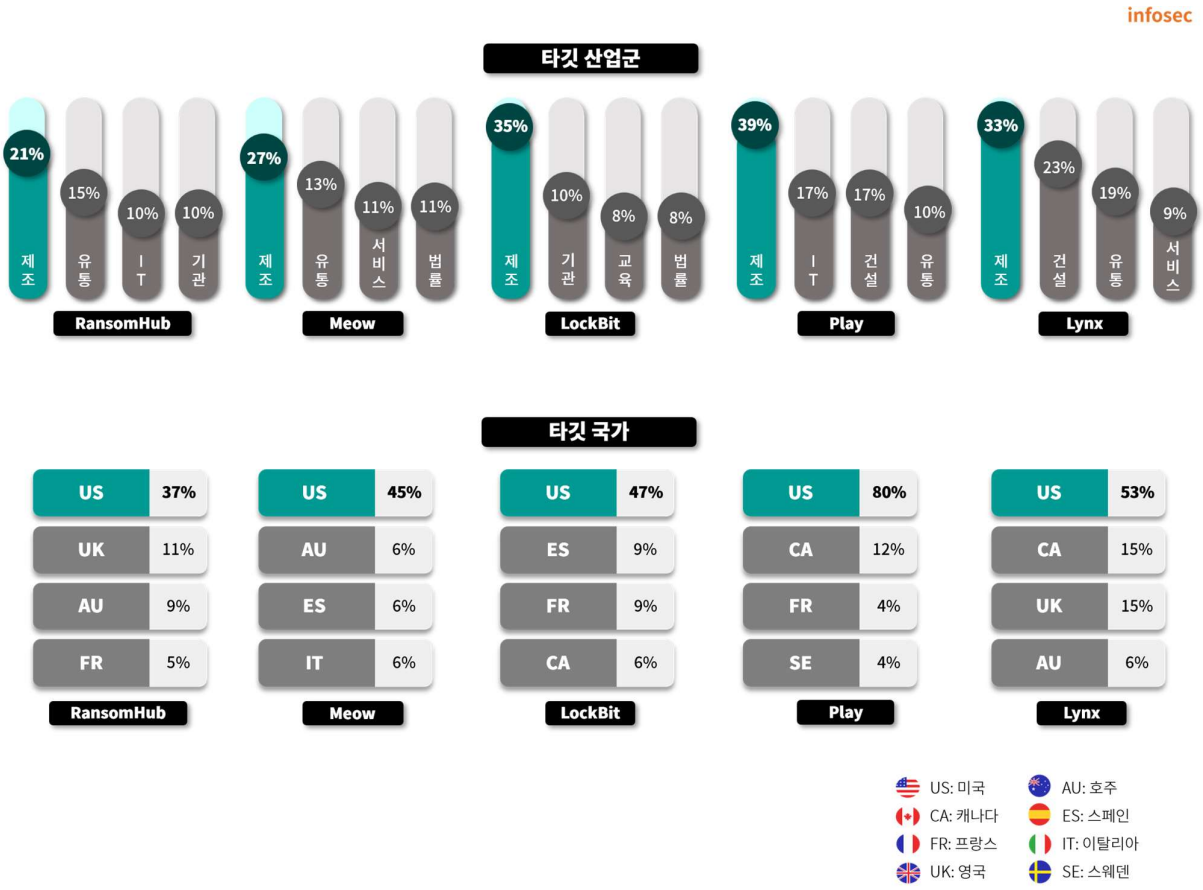


그림 4. 산업/국가별 주요 랜섬웨어 공격 현황

RansomHub 랜섬웨어 그룹은 7 월에만 48 건의 피해자를 게시하며 활발히 활동했으나, 8 월에는 그보다 25 건 더 많은 73 건을 게시하며 위협적인 모습을 보이고 있다. 특히, 8 월에는 EDR(Endpoint Detection and Response) 솔루션을 비활성화하는 악성 도구인 EDRKillShifter 를 사용한 정황이 발견되었다. 이 도구는 실행 시 암호화된 리소스를 복호화하기 위해 특정 키 값이 필요하며, 합법적인 드라이버의 취약점을 이용한 BYOVD(Bring Your Own Vulnerable Driver) 기법을 통해 EDR 솔루션의 보호 기능을 비활성화한다. 해당 악성 도구는 다크웹에서 판매되기 때문에 다른 공격자 그룹도 이를 악용할 수 있다. BYOVD 기법은 신뢰할 수 있는 드라이버를 통해 공격이 이루어지기 때문에, EDR 솔루션과 권한 관리 등의 적절한 대응이 필요하다. RansomHub 그룹에 대한 더 자세한 분석은 2 분기 KARA 랜섬웨어 동향 보고서에서 확인할 수 있다.

Meow 랜섬웨어는 Conti v2 랜섬웨어의 유출된 소스코드를 기반으로 제작된 랜섬웨어다. 2023 년에 다크웹 유출 사이트를 개설한 이후, 매달 10 건 이하의 피해자를 게시해왔으나, 2024 년 7 월부터 피해자 수가 증가하기 시작해 8 월에는 전체 피해자의 51%에 해당하는 43 건을 게시하며 활동량이 폭발적으로 증가했다. 이 그룹은 8 월에 50 개국에 지사를 둔 글로벌 제약회사 Zydus Pharmaceuticals 를 공격해 재무 문서, 고객 데이터, 실험 연구 자료 등 20GB 에 달하는 데이터를 탈취한 것으로 알려졌다.

락빗(LockBit) 랜섬웨어는 8 월 11 일과 12 일, 다크웹 유출 사이트에 약 90 건의 피해자를 일괄적으로 게시했으나, 대부분은 2022 년부터 2024 년 사이에 이미 게시된 피해자들이었다. 그중 신규 피해자는 15 건에 불과했다. 이후 2 건의 피해자만 추가로 게시하며 활동이 저조한 모습을 보이다가, 8 월 30 일에 다시 11 건을 추가로 게시했다.

플레이(Play) 랜섬웨어는 주로 미국 소재 기업들을 표적으로 삼고 있다. 8 월에는 미국의 반도체 제조사인 Microchip Technology 를 공격해 내부 기밀 데이터와 개인 정보, 예산, 급여, 회계 데이터를 탈취했다고 주장했다. 이 그룹은 일부 기밀 문서와 고객사 정보, 회계 정보를 공개했으며, 추가적인 대응이 없을 경우 모든 데이터를 공개할 것이라고 경고했다.

Lynx 랜섬웨어는 7 월에 등장한 신규 그룹으로, 8 월 동안 꾸준히 피해자를 업로드하며 5 번째로 많은 피해자를 게시한 그룹으로 확인되었다. 이 그룹은 자산 관리 전문 기업인 Pyle Group 을 공격해 민감한 기업 정보를 탈취했다고 주장했으며, 예고된 공개 날짜가 한참 지난 후 데이터를 공개했다. 8 월 15 일에는 메두사(Medusa) 랜섬웨어의 다크웹 유출 사이트에도 Pyle Group 이 피해자로 게시되었으며, Medusa 그룹은 TOX Chat 을 통해 데이터를 확인할 수 있다고 알렸다.

■ 랜섬웨어 집중 포커스

Lynx 랜섬웨어 개요

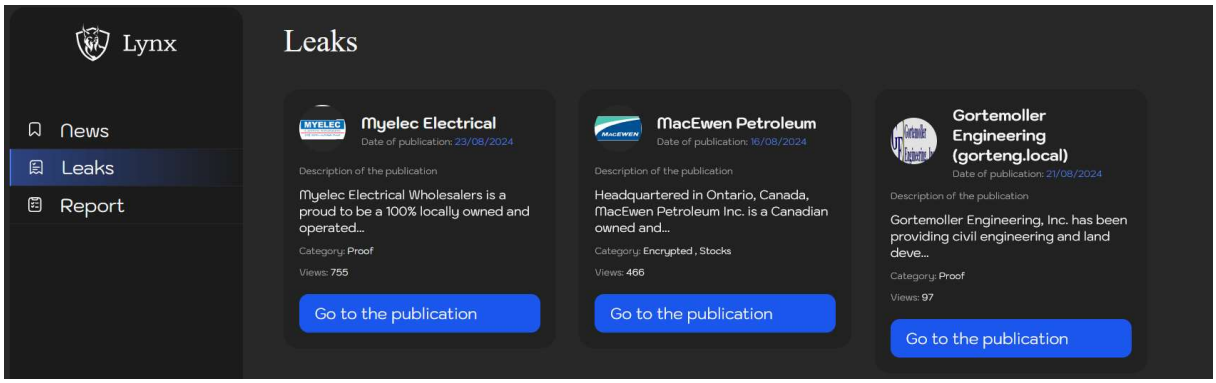


그림 5. Lynx 랜섬웨어 데이터 유출 사이트

Lynx 랜섬웨어는 7 월 29 일 유출 사이트가 발견되면서 본격적으로 주목받기 시작했다. 사이트가 발견되었을 당시 이미 7 월 17 일에 게시된 글이 2 개 존재했으며, 다크웹 기반 사이트뿐만 아니라 클리어넷 사이트도 함께 발견됐다. 현재는 클리어넷 사이트만 접근이 가능한 상태다. 7 월 24 일 다크웹 유출 사이트에 업로드된 그룹 소개글에 따르면, Lynx 는 금전적 목적을 위해 공격을 수행하지만, 정부 기관, 병원, 비영리 조직 등 사회적으로 중요한 역할을 하는 기관에 대해서는 엄격한 공격 제한 정책을 가지고 있다고 소개하고 있다. 실제로 이들은 이들 기관을 제외한 다양한 산업 분야를 대상으로 공격을 수행하며, 활동 시작 한 달 만에 21 건의 피해자를 게시해 새로운 위협으로 부상하고 있다.

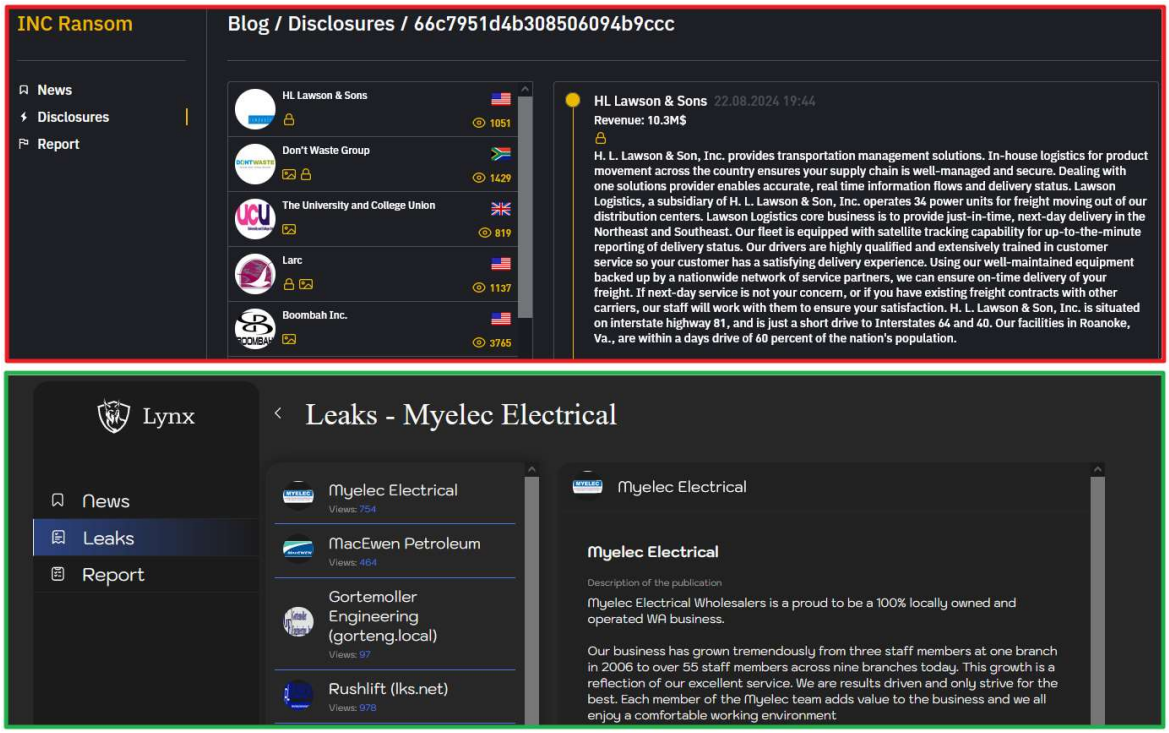


그림 6. 다크웹 유출 사이트 비교(상: INC ransom, 하: Lynx)

Lynx 랜섬웨어와 INC 랜섬웨어 간의 연관성을 시사하는 여러 정황도 발견되었다. 첫 번째 정황으로는, INC 랜섬웨어 그룹이 5 월에 다크웹 유출 사이트의 디자인을 변경한 후, Lynx 랜섬웨어의 다크웹 유출 사이트가 이와 매우 흡사한 디자인을 사용하고 있다는 점이다.

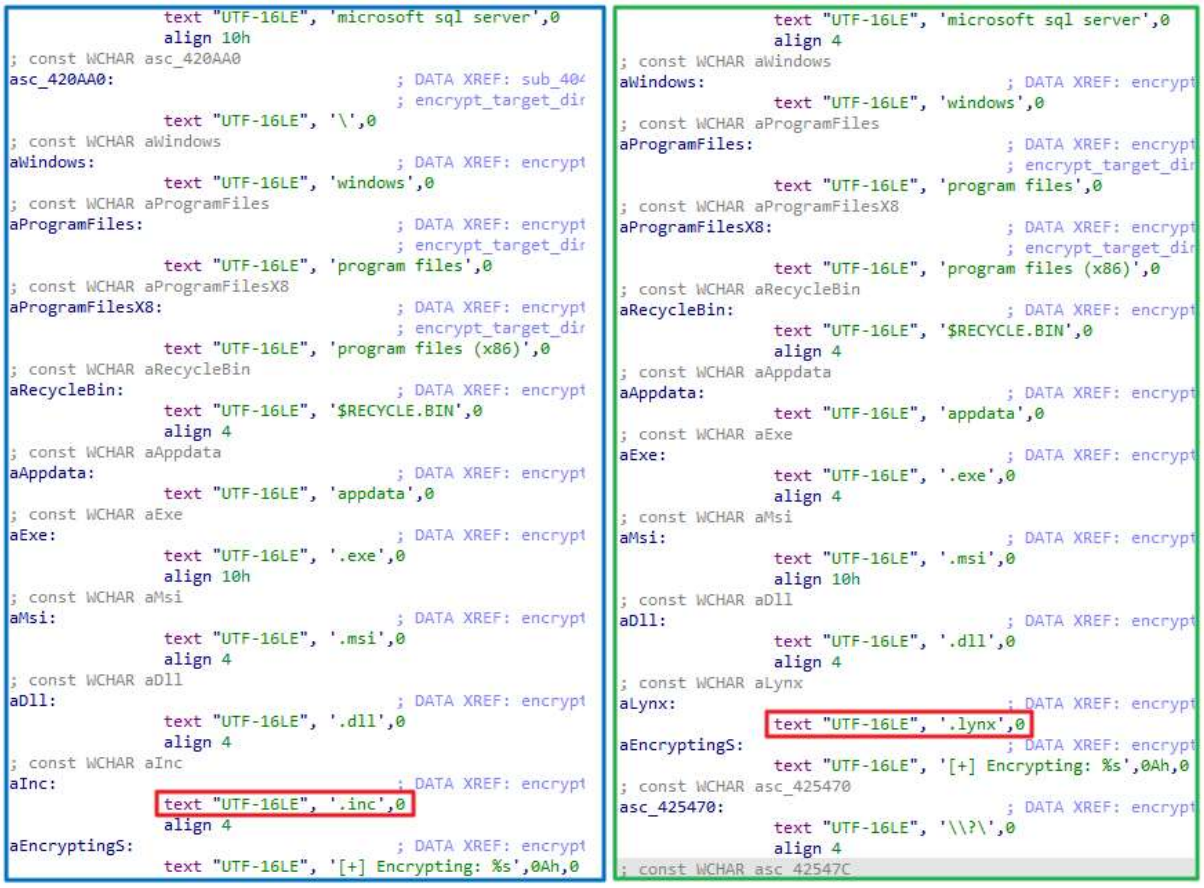


그림 7. 랜섬웨어 문자열 비교(좌: INC ransom, 우: Lynx)

두 번째 정황은 Lynx 랜섬웨어 파일을 분석한 결과, INC 랜섬웨어와 동일한 문자열과 암호화 알고리즘을 사용하고 있으며, 프로그램 실행 흐름 등 기능적으로도 매우 유사한 부분이 확인되었다. 이는 INC 랜섬웨어 그룹이 5 월에 랜섬웨어 소스코드 및 관리 패널 같은 주요 시스템의 소스코드를 해킹 포럼에서 30 만 달러(한화 약 4 억 원)에 판매한 이력이 있는 점과 연관이 있을 것으로 보인다. Lynx 랜섬웨어가 이 소스코드를 구매해 활동을 시작한 것일 가능성이 크다.

따라서 이번 보고서에서는 두 랜섬웨어의 유사점과 차이점을 집중적으로 분석하며, Lynx 랜섬웨어에 대한 상세한 분석 내용을 제공하고자 한다.

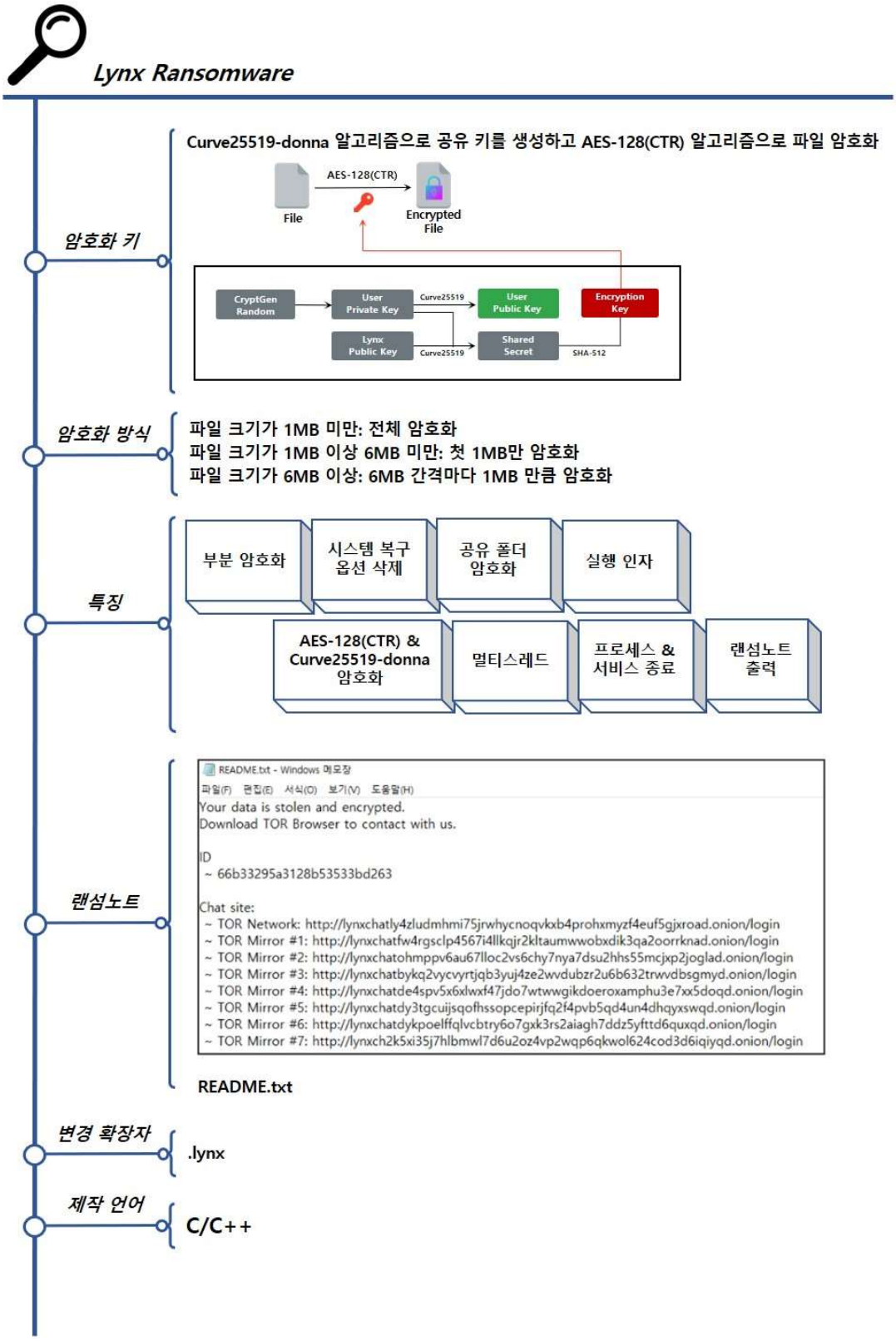


그림 8. Lynx 랜섬웨어 개요

Lynx 랜섬웨어 전략

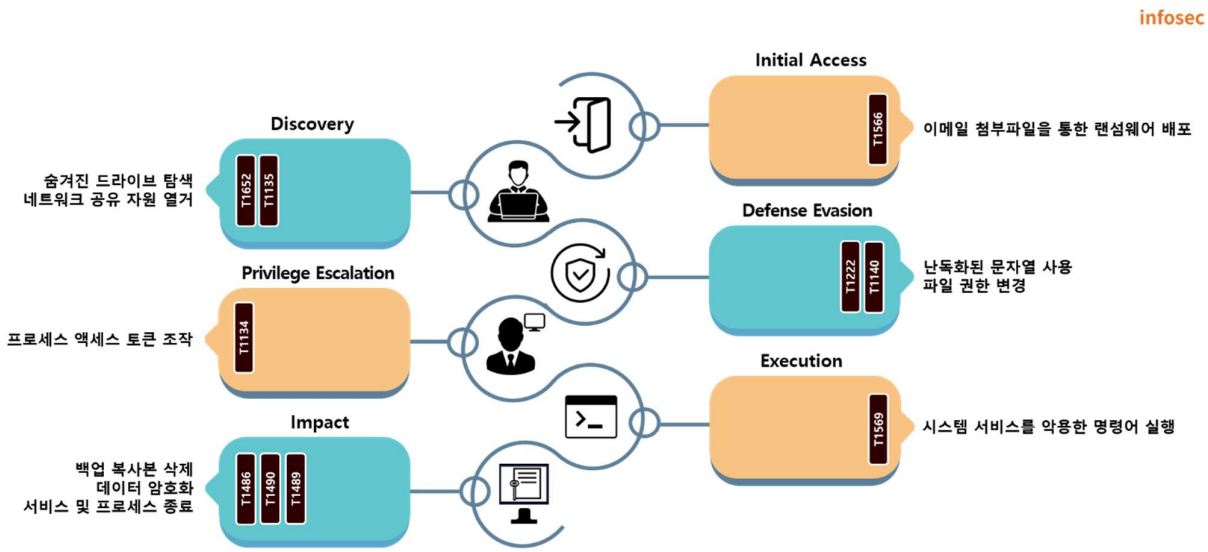


그림 9. Lynx 랜섬웨어 공격 전략

Lynx 랜섬웨어는 실행 시 추가적인 인자 입력을 통해서 숨겨진 드라이브를 마운트하거나, 실행 시 보이는 명령 프롬프트 창을 숨기는 등 여러 기능을 활성화하거나 비활성화할 수 있다. 총 12 개의 옵션이 존재하며, 별도의 실행 인자가 없어도 정상적으로 실행이 가능하다. Lynx 랜섬웨어가 사용하는 실행 인자는 아래 표와 같다.

인자	설명
--file [파일경로]	지정한 파일만 암호화
--dir [디렉토리경로]	지정한 폴더만 암호화
--help	실행 인자 설명 출력
--verbose	디버깅 로그 출력
--stop-processes	파일 암호화 직전, 대상 파일이 실행중인 경우 프로세스 종료
--encrypt-network	네트워크 공유 자원 암호화
--load-drives	숨겨진 드라이브 마운트
--hide-cmd	랜섬웨어 실행 시 보이는 명령 프롬프트 창 숨김
--no-background	배경화면 변경 기능 비활성화
--no-print	랜섬노트 출력 기능 비활성화
--kill	특정 프로세스 및 서비스 종료
--safe-mode	안전모드 부팅(기능 존재하지 않음)

표 1. Lynx 랜섬웨어 실행 인자

랜섬웨어 분석 결과 12 개의 실행 인자 옵션 중 안전 모드로 부팅하는 기능이라고 설명한 “--safe-mode”의 경우, 해당 인자가 입력됐는지 확인하는 코드는 존재하지만 실제로 안전모드로

부팅하거나 재부팅 이후 자동으로 랜섬웨어를 다시 시작하기 위한 코드는 발견되지 않았다. 실제로 실행한 결과 해당 인자를 확인하는 로그만 출력될 뿐, 안전모드로 진입하지 않는다.

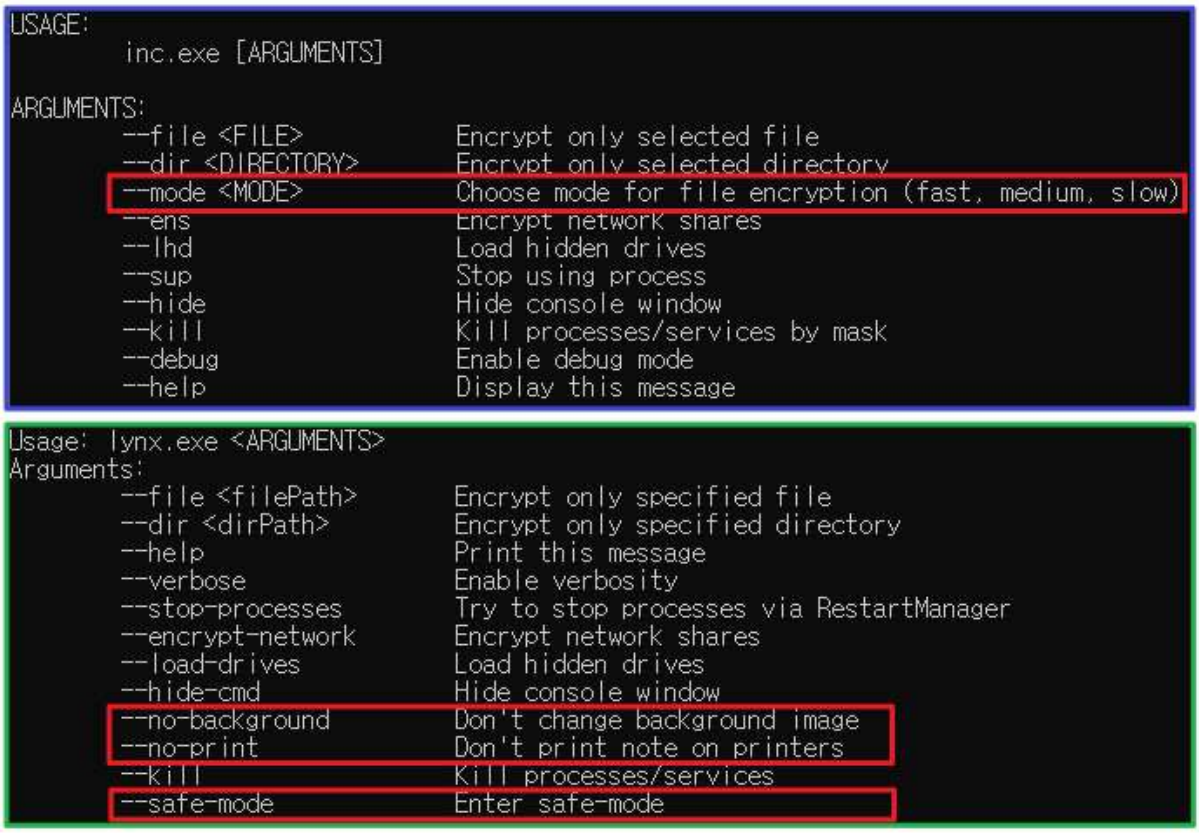


그림 10. 랜섬웨어 실행 인자 비교(상: INC, 하: Lynx)

Lynx 랜섬웨어의 실행 인자는 표기만 다를 뿐 상세한 기능과 작동 방식이 INC 랜섬웨어와 동일하다. 다만 INC 랜섬웨어는 암호화 모드를 설정할 수 있는 “--mode” 인자가 존재하는 반면, Lynx 랜섬웨어는 별도로 암호화 모드를 설정하는 기능이 존재하지 않는다.

또한 배경화면 변경과 랜섬노트 출력 기능을 비활성화 하는 실행 인자가 추가된 것도 확인됐다. INC 랜섬웨어는 랜섬웨어를 시작 서비스에 등록한 뒤 안전모드로 부팅하는 반면, Lynx 랜섬웨어는 해당 기능이 아예 삭제됐으며, 앞서 설명했듯이 “--safe-mode” 인자도 아무런 기능이 없다.

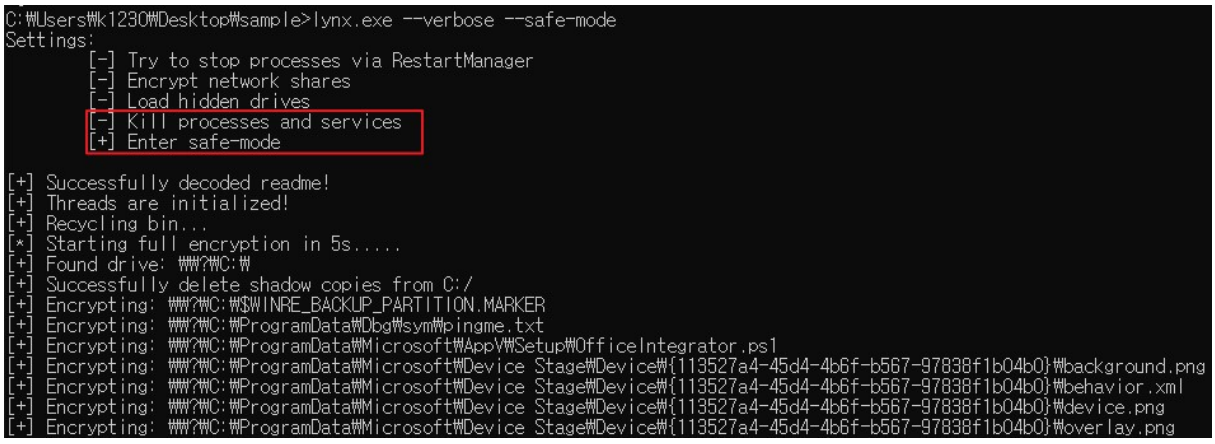


그림 11. Lynx 랜섬웨어 --verbose 입력 결과

Lynx 랜섬웨어는 "--verbose" 실행 인자를 사용하면 랜섬웨어의 설정 값을 보여주고 현재 어떤 작업을 진행하고 있는지를 명령 프롬프트 창에 출력하게 된다. 별도의 실행 인자를 입력해서 기능을 활성화하면 "Settings"에 "[-]" 대신 "[+]" 기호를 통해 활성화를 표시한다. 이러한 디버깅[2] 기능은 INC 랜섬웨어의 "--debug" 실행 인자와 동일한 기능이다.

실행 인자 "--kill"을 입력하면, 랜섬웨어에 하드코딩된 프로세스 및 서비스 목록을 참조해 대상 프로세스와 서비스를 종료시킨다. INC 랜섬웨어의 "--kill" 실행 인자와 동일한 기능이며, Lynx 랜섬웨어에 추가된 텍스트 편집기 notepad 를 제외하고 종료 대상이 모두 동일하다. 확인된 프로세스 및 서비스 종료 대상은 아래 표와 같다.

프로세스	서비스
sql, veeam, backup, exchange, java, **notepad**	sql, veeam, backup, exchange

표 2. Lynx 랜섬웨어 프로세스 및 서비스 종료 대상

[2] 디버깅 (Debugging): 프로그램 개발 단계 중에 발생하는 시스템의 오류를 찾아내 수정하는 과정

```
if ( DeviceIoControl(FileW, 0x53C028u, InBuffer, 0x18u, 0, 0, &BytesReturned, 0) )// delete vsc (change vsc size 1)
                                        // 0x53c028 = IOCTL_VOLSNAP_SET_MAX_DIFF_AREA_SIZE
                                        // resizes the allocated space for shadow copies snapshots cause the deleteion of vsc
```

그림 12. DeviceIoControl 을 이용한 백업 복사본 삭제

전체 드라이브를 암호화하기 전에, 먼저 백업 복사본을 삭제한다. Lynx 랜섬웨어와 INC 랜섬웨어는 다른 랜섬웨어에서 흔히 사용하는 백업 복사본 관리용 Windows 유틸리티(vssadmin, wmic shadowcopy, wbadmin, bcdedit)들을 활용하지 않고 디바이스를 제어하는 함수 DeviceIoControl 를 이용해 백업 복사본을 삭제한다. DeviceIoControl 함수를 이용해 백업 복사본이 저장되는 공간을 아주 작게 재설정하면 시스템은 백업을 저장할 공간이 부족하다고 인식하게 되고, 저장 공간 확보를 위해 이미 저장된 백업 복사본을 삭제하게 된다. Lynx 랜섬웨어에서 해당 기능은 “--file” 인자와 “--dir” 인자를 모두 사용하지 않았을 때만 동작한다.

```
if ( GetVolumePathNamesForVolumeNameW(v5, szVolumePathNames, 0x78u, &cchReturnLength)
  && lstrlenW(szVolumePathNames) == 3 )
{
  szVolumePathNames[0] = 0;
}
else
{
  v7 = lpszVolumeMountPoint[v0--];
  if ( SetVolumeMountPointW(v7, v5) )     // Mount Volume
  {
    if ( param_verbose )
      print_message_with__s(L"\t[+] Mounted % s\n", v7);
```

```
while ( !WNetEnumResourceW(hEnum, &cCount, v4, &dwBytes) )
{
  v5 = 0;
  if ( cCount )
  {
    v6 = v4 + 3;
    do
    {
      if ( v4[2] == 3 )
      {
        lstrcpyW(String1, v6[2]);
        lstrcatW(String1, L"\\");
        if ( param_verbose )
          print_message_with__s(L"[+] Found share: %s\n", String1);
        encrypt_target_directory(String1);
```

그림 13. 암호화 대상 수집(좌: 숨겨진 드라이브 마운트, 우: 네트워크 공유 자원 추가)

파일 암호화를 진행하기 이전에 암호화 대상을 수집하는 과정이 존재한다. “--load-drives” 인자를 사용하면, 파일 암호화 이전에 A 드라이브부터 Z 드라이브까지 모든 드라이브를 확인해 숨겨진 드라이브가 존재하는지 확인하고, 해당 드라이브가 존재하면 마운트 후 암호화 대상에 추가한다. 또한 “--encrypt-network” 인자를 사용하면 네트워크 공유 자원도 암호화 대상에 추가한다. 이는 INC 랜섬웨어의 “--lhd”, “--ens” 인자와 동일한 기능이다.

파일 암호화는 “--file” 인자 입력 시 특정 파일만 암호화하며, “--dir” 인자 입력 시에는 특정 경로에 존재하는 파일들만 암호화한다. 둘 다 입력되지 않았을 경우에는 예외 대상을 제외한 모든 파일을 암호화한다. 암호화 예외 대상 및 폴더 명은 랜섬웨어 내에 하드코딩되어 저장돼 있으며, 확인된 예외 대상은 아래 표와 같다.

예외 확장자 및 파일	예외 폴더
*.exe, *.msi, *.dll, *.lynx, README.txt	Windows, Program Files, Program Files (x86), $RECYCLE.BIN, AppData

표 3. Lynx 랜섬웨어 암호화 예외 대상

Lynx 랜섬웨어와 INC 랜섬웨어의 암호화 예외 대상은 거의 동일하지만 약간의 차이가 존재한다. Lynx 랜섬웨어의 경우, 예외 대상인 “Program Files” 및 “Program Files (x86)” 폴더 하위에 존재하는 “microsoft sql server” 폴더를 암호화하는 코드가 추가됐다. 또한 이미 암호화된 파일을 중복으로 암호화 하지 않기 위해 추가한 “.lynx”가 INC 랜섬웨어에서는 “.inc”로 다르다.

“--mode” 인자를 통해서 총 3 가지의 암호화 모드를 제공하는 INC 랜섬웨어와 달리, Lynx 랜섬웨어는 암호화 옵션을 선택하는 기능이 별도로 존재하지 않는다. INC 랜섬웨어는 파일의 처음, 중간, 끝 세 구간을 1MB씩만 암호화하는 fast 모드와 6MB 마다 1MB 만큼만 암호화하는 medium 모드, 그리고 파일 전체를 암호화하는 slow 모드가 존재한다. Lynx 랜섬웨어는 이 중 medium 모드를 고정으로 사용하고 있다.

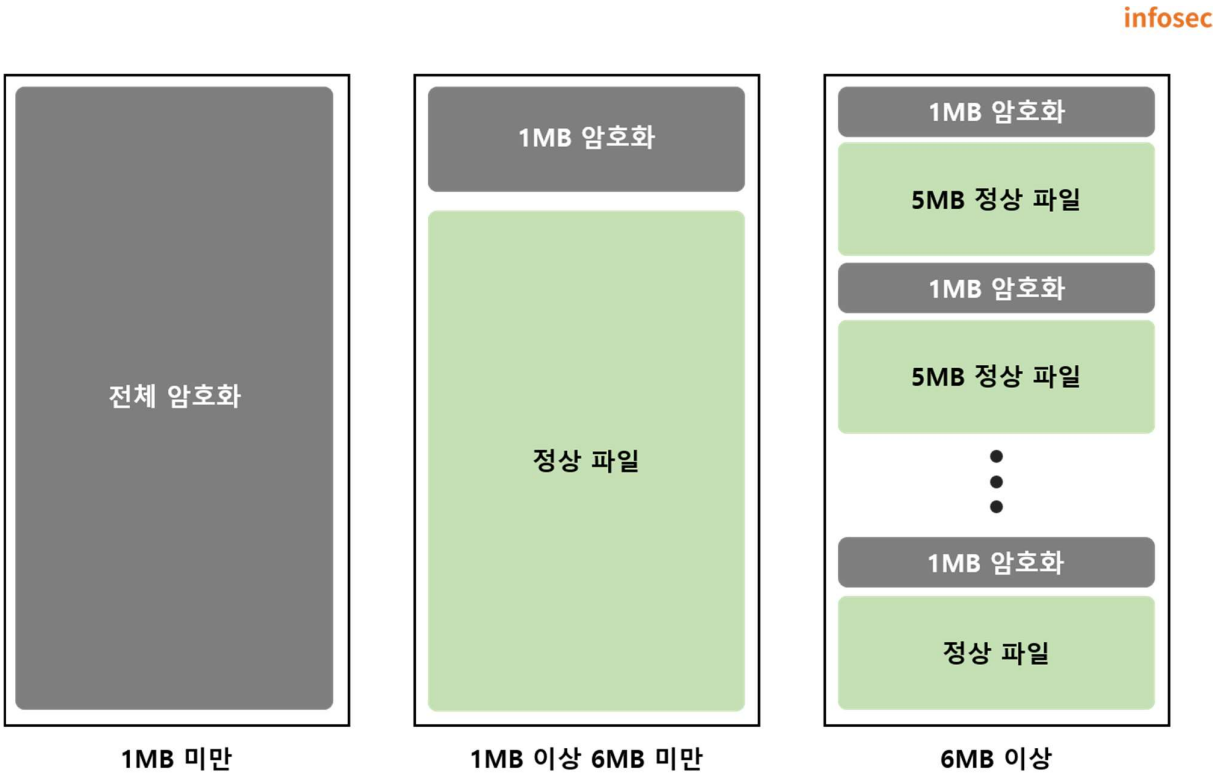


그림 14. Lynx 랜섬웨어 암호화 방식

Lynx 랜섬웨어의 암호화 방식을 좀 더 자세히 살펴보면 위 그림과 같다. 1MB 미만의 파일은 전체 암호화를 진행하며, 1MB 이상 6MB 미만의 파일의 경우 파일의 첫 1MB 만 암호화를 한다. 그리고 6MB 이상의 파일은 6MB 간격으로 1MB 씩 암호화한다. 파일 암호화는 AES-128(CTR) 알고리즘을 사용해 암호화를 진행하며, 키 생성 알고리즘으로 Curve25519-donna 를 사용해 키를 보호한다.

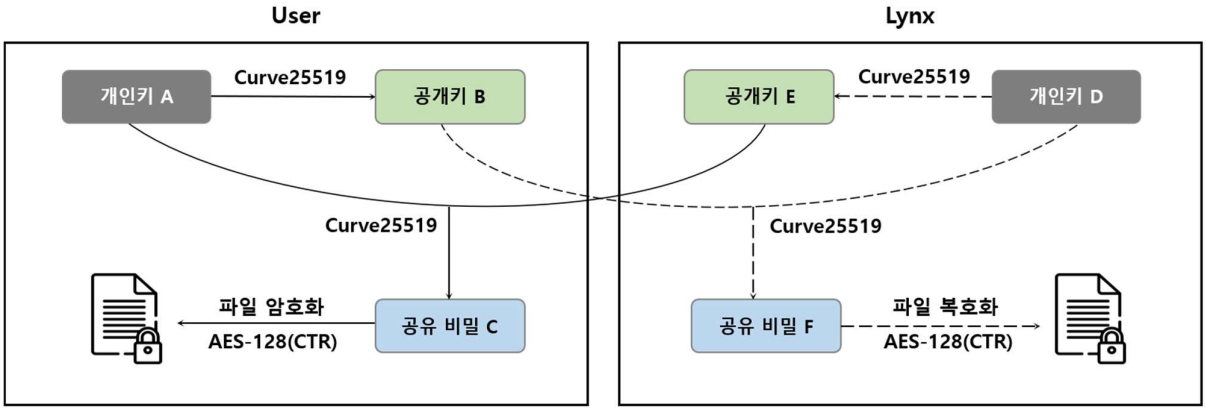


그림 15. Lynx 랜섬웨어 공유 비밀 생성 방식

Lynx 랜섬웨어에서 암호화 키를 생성했을 때, 별도로 키를 암호화하지 않아도 키를 보호할 수 있는 이유는 사용한 Curve25519-donna 알고리즘이 키 분배 알고리즘이기 때문이다. 키 분배 알고리즘을 통해 두 사용자는 각자의 개인키와 상대방의 공개키를 이용해 동일한 대칭키를 생성할 수 있다. 사용자는 본인의 개인키로 공개키를 만들고, 자신의 개인키와 상대방의 공개키로 생성한 키(C)가 상대방의 개인키와 자신의 공개키로 생성한 키(F)와 동일한 값을 가지게 된다. 이 동일한 키(C, F)를 '공유 비밀'이라고 부른다.

Lynx 랜섬웨어는 암호화 대상 파일마다 랜덤한 개인키와 공개키를 생성한 후, 해당 개인키와 하드코딩된 공격자의 공개키로 공유 비밀을 생성해 파일을 암호화한다. 이후, 파일의 끝에 해당 파일의 공개키를 추가하면 공격자는 파일의 공개키와 공격자의 개인키를 사용해 암호화에 사용한 키를 다시 생성함으로써 파일을 복호화 할 수 있다.

```
encoded_ransomnote = decode_base64_string(
                     &dwMessageIda,
                     "WW91ciBkYXRhIGlzIHN0b2xlbiBhbmQgZW5jcnlwdGVkLg0KRG93bmxvYWQgVE9SIEJyb3dzZXIgdG8gY29udGFjdCB"
                     "3aXRoIHVzLg0KDQpJRA0KIH4gJWlkJQ0KDQpDaGF0IHNpdGU6DQogfiBUT1IgTmV0d29yazogaHR0cDovL2x5bnhjaG"
                     "F0bHk0emx1ZG1obWk3NWpyd2h5Y25vcXZreGI0cHJvaHhteXpmNGV1ZjVnanhyb2FkLm9uaW9uL2xvZ2luDQogfiBUT"
                     "1IgTWlycm9yICMxOiBodHRwOi8vbHlueGNoYXRmdzRyZ3NjbHA0NTY3aTRsbGtxanIya2x0YXVtd3dvYnhkaWszcWEy"
                     "b29ycmtuYWQub25pb24vbG9naW4NCiB+IFRPUiBNaXJyb3IgIzI6IGh0dHA6Ly9seW54Y2hhdG9obXBwdjZhdTY3bGx"
                     "vYzJ2czZjaHk3bnlhN2RzdTJoaHM1NW1janhwMmpvZ2xhZC5vbmlvbi9sb2dpbg0KIH4gVE9SIE1pcnJvciAjMzogaH"
                     "R0cDovL2x5bnhjaGF0YnlrcTJ2eWN2eXJ0anFiM3l1ajR6ZTJ3dmR1YnpyMnU2YjYzMnRyd3ZkYnNnbXlkLm9uaW9uL"
                     "2xvZ2luDQogfiBUT1IgTWlycm9yICM0OiBodHRwOi8vbHlueGNoYXRkZTRzcHY1eDZ4bHd4ZjQ3amRvN3d0d3dnaWtk"
                     "b2Vyb3hhbXBodTNlN3h4NWRvcWQub25pb24vbG9naW4NCiB+IFRPUiBNaXJyb3IgIzU6IGh0dHA6Ly9seW54Y2hhdGR"
                     "5M3RnY3VpanNxb2Zoc3NvcGNlcGlyamZxMmY0cHZiNXFkNHVuNGRocXl4c3dxZC5vbmlvbi9sb2dpbg0KIH4gVE9SIE"
                     "1pcnJvciAjNjogaHR0cDovL2x5bnhjaGF0ZHlrcG9lbGZmcWx2Y2J0cnk2bzdneGszcnMyYWlhZ2g3ZGR6NXlmdHRkN"
                     "nF1eHFkLm9uaW9uL2xvZ2luDQogfiBUT1IgTWlycm9yICM3OiBodHRwOi8vbHlueGNoMms1eGkzNWo3aGxibXdsN2Q2"
                     "dTJvejR2cDJ3cXA2cWt3b2w2MjRjb2QzZDZpcWl5cWQub25pb24vbG9naW4NCg0KT3VyIGJsb2c6DQogfiBUT1IgTmV"
                     "0d29yazogaHR0cDovL2x5bnhibG9neHN0Z3pzYXJmeWsycHZoZHY0NWlnZ2hiNHptdGhuem1zaXB6ZW9kdXJ1ejN4d3"
                     "FkLm9uaW9uLw0KIH4gVE9SIE1pcnJvciAjMTogaHR0cDovL2x5bnhibG9nY283cjM3anQ3cDV3cm1meHpxemU3Z2h4d"
                     "zZyaWh6a3FjNDU1cWx1YWN3b3RjaXlkLm9uaW9uLw0KIH4gVE9SIE1pcnJvciAjMjogaHR0cDovL2x5bnhibG9naWp5"
                     "NGpmb2JsZ2l4MmtseG1rYmdlZTRsZW9ldWdlN3F0NGZwZmtqNHpiaTJzanlkLm9uaW9uLw0KIH4gVE9SIE1pcnJvciA"
                     "jMzogaHR0cDovL2x5bnhibG9nbXgzcmJpd2czcnBqNG5kczI1aGpzbnJ3a3B4dDVnYXpuZXRmaWt6NGd6MmNzeWFkLm"
                     "9uaW9uLw0KIH4gVE9SIE1pcnJvciAjNDogaHR0cDovL2x5bnhibG9nb3hsbHRoNGI0NmNmd2xvcDVwZmo0czdkeXYzN"
                     ""3l1eTdxbjJmdGFuNmdkNzJoc2FkLm9uaW9uLw0KIH4gVE9SIE1pcnJvciAjNTogaHR0cDovL2x5bnhibG9ndHdhdGZz"
                     "cndqM29hdHBland4azVibmdxY2Q1ZjdzMjZpc2thZ2Z1N291YW9tamFkLm9uaW9uLw0KIH4gVE9SIE1pcnJvciAjNjo"
                     "gaHR0cDovL2x5bnhibG9neHV0dWZvc3NhZWF3bGlqM2ozdWlrYWxvbGw1a282Z3J6aGt3ZGNscmpuZ3Jmb2lkLm9uaW"
                     "9uLw0KIH4gTWlycm9yICM3OiBodHRwOi8vbHlueGJsb2cubmV0Lw0KIA==",
                     &args_2);
```

그림 16. Lynx 랜섬웨어 랜섬노트 Base64 디코딩

Lynx 랜섬웨어는 Base64 로 인코딩된 랜섬노트 내용을 디코딩하여 사용한다. 디코딩된 랜섬노트는 암호화된 폴더에 텍스트 파일로 저장되거나, 이미지로 변환해 배경화면으로 설정되며, 연결된 프린터로 출력하는데 활용된다. INC 랜섬웨어도 Base64로 인코딩된 랜섬노트를 복구해 사용하지만, Lynx 랜섬웨어와는 달리 텍스트 파일 버전과 HTML 버전의 두 가지 형식의 랜섬노트를 활용한다는 차이점이 있다.

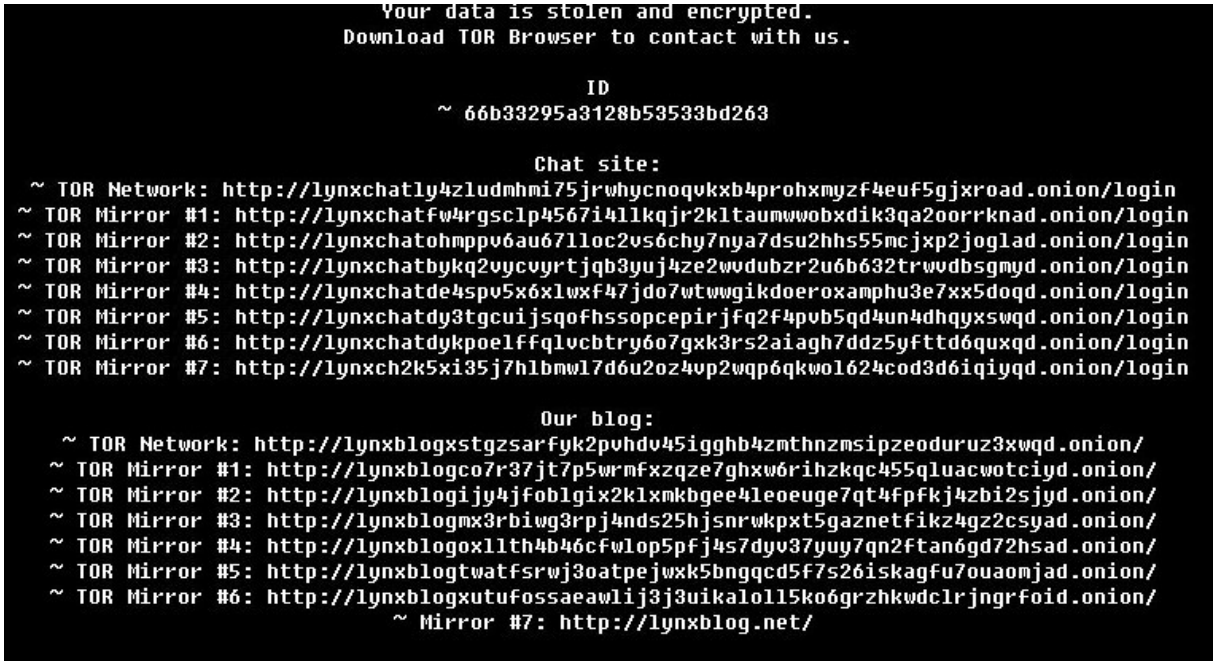


그림 17. Lynx 랜섬웨어 배경화면 변경

Lynx 랜섬웨어 대응방안

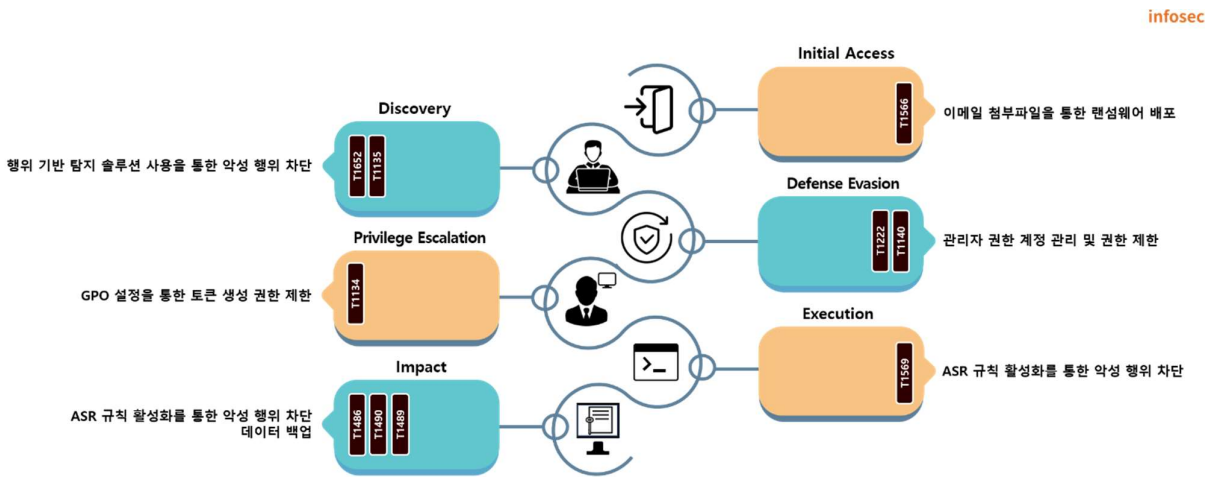


그림 18. Lynx 랜섬웨어 대응방안

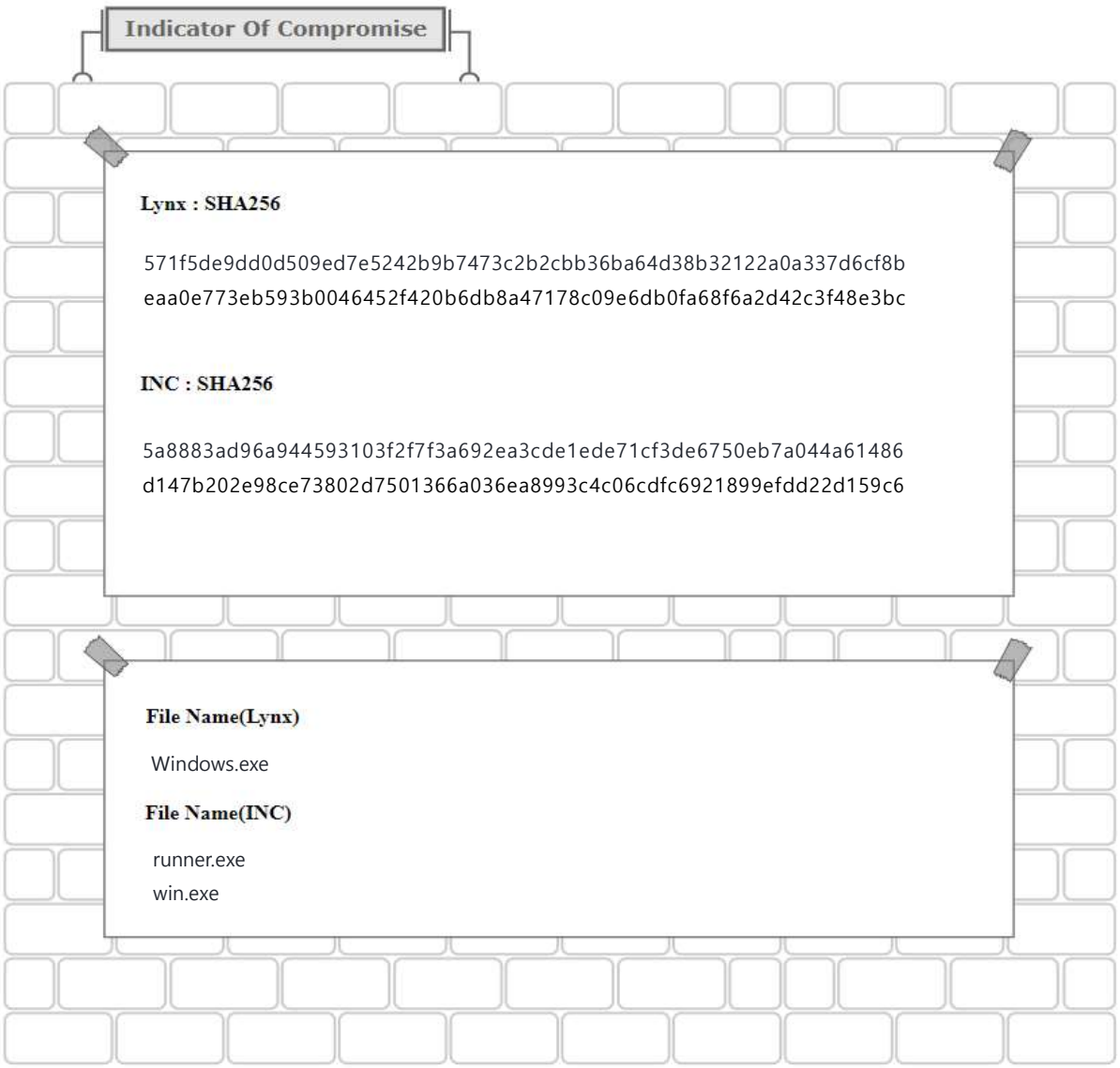
Lynx 랜섬웨어는 이메일 첨부파일을 통해 전파된다. 따라서 의심스러운 이메일이나 확인되지 않은 발신자의 메일 및 첨부파일을 열람하지 않도록 주의해야 한다. 이를 예방하기 위해 가상 환경에서 이메일의 위험을 탐지하고 차단하는 Email Threat Response & Detection 솔루션을 사용하는 것도 효과적이다.

랜섬웨어는 감염된 시스템에서 암호화 대상을 확보하기 위해 연결된 네트워크 공유 자원을 열거하고 숨겨진 드라이브를 탐색하여 마운트한다. 이를 방지하려면 행위 기반 탐지 솔루션을 사용해 이러한 악성 행위를 차단할 수 있다.

또한, Lynx 랜섬웨어는 파일을 암호화하기 전에 파일의 권한을 변경하려 시도한다. 이 과정에서는 관리자 권한이 필요한데, Lynx 랜섬웨어는 별도의 권한 상승 기능이 없기 때문에, 사전에 관리자 계정을 엄격히 관리하고 권한을 최소한으로 부여하는 조치로 파일 암호화를 어느 정도 예방할 수 있다. 추가로, ASR(Attack Surface Reduction)[3] 규칙을 활성화하거나 공격자가 사용하는 특정 프로세스를 차단해 악성 행위를 막을 수 있다.

마지막으로, Lynx 랜섬웨어는 네트워크 공유 파일도 암호화하므로 네트워크 공유 자원의 접근 권한을 최소화하거나 비활성화해 외부 리소스에 접근하지 못하도록 해야 한다. 또한, 랜섬웨어가 윈도우의 기본 복구 기능을 통해 복구할 수 없도록 백업 복사본을 삭제하기 때문에, 별도의 네트워크나 저장소에 데이터를 분산하여 백업하는 것이 중요하다.

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


Indicator Of Compromise
Lynx : SHA256
571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b
eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc
INC : SHA256
5a8883ad96a944593103f2f7f3a692ea3cde1ede71cf3de6750eb7a044a61486
d147b202e98ce73802d7501366a036ea8993c4c06cdfc6921899efdd22d159c6
File Name(Lynx)
Windows.exe
File Name(INC)
runner.exe
win.exe

■ 참고 사이트

• Jenkins 공식 홈페이지 (https://www.jenkins.io/security/advisory/2024-01-24/)

• CISA 공식 홈페이지 (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

• NIST 국립 취약성 데이터베이스 (https://nvd.nist.gov/vuln/detail/CVE-2024-23897)

• Fortinet 공식 블로그 (https://www.fortinet.com/blog/threat-research/stomping-shadow-copies-a-second-look-into-deletion-methods)

• Sophos 공식 홈페이지 (https://news.sophos.com/en-us/2024/08/14/edr-kill-shifter/)

• BleepingComputer 공식 홈페이지 (https://www.bleepingcomputer.com/news/security/fbi-disrupts-the-dispossessor-ransomware-operation-seizes-servers/)