KARA
Korea Anti Ransomware Alliance

2025.1Q

KARA 랜섬웨어 동향 보고서

KARA 랜섬웨어 동향 보고서

EQST Lab 팀 이호석, 정민수, 조효제, 이현아, 이승호

랜섬웨어 트렌드

1. 1 분기 TREND

TREND

- **Clop :** Cleo 사의 취약점(CVE-2024-50623, CVE-2024-55956)을 악용
- **Mora_001 :** Fortinet 의 취약점(CVE-2024-55591, CVE-2025-24472)을 악용

THREAT

- **1 분기 Top5 랜섬웨어 :** Clop, RansomHub, Dragon, Akira, Babuk-Bjorka
- **Babuk-Bjorka 랜섬웨어 :** 유출된 Babuk 랜섬웨어 기반, 실제 침해 여부 확인 불가

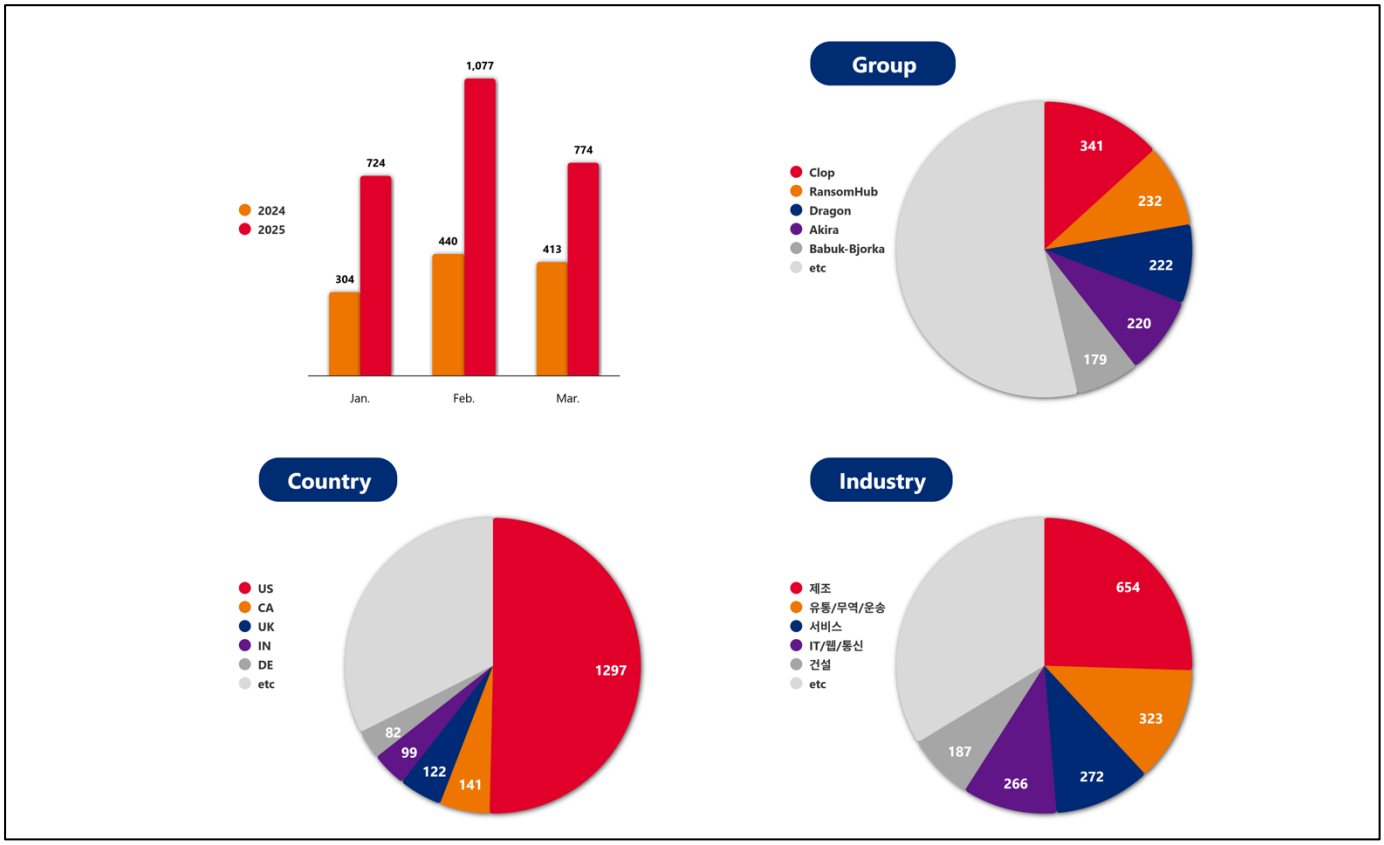
EXPLOIT

- **0-day :** CVE-2025-24472
- **1-day :** CVE-2024-50623, CVE-2024-55956, CVE-2024-55591

TARGET

- **Fortinet 방화벽** 취약점을 통한 초기 침투
- 전체 공격 중 제조 25%, 미국 50%

2. 1분기 랜섬웨어 활동 통계



[그림 1] 랜섬웨어 그룹 활동

2025년 1분기 랜섬웨어 피해 사례는 총 2,575건으로, 2024년 동기 대비 약 122% 증가했으며, 2024년 4분기 대비로도 35% 상승한 수치를 기록했다. 이번 분기에는 한동안 활동을 중단했던 랜섬웨어 그룹들이 다시 활발히 움직이기 시작하면서 전체 공격 건수가 크게 증가했다.

전 분기 Cleo 사의 취약점을 악용해 활동했던 Clop 랜섬웨어는 이번 분기 341 건의 공격을 기록하며 활발한 활동을 이어갔다. 2024 년 4 분기에 240 건으로 가장 활발히 활동한 RansomHub 그룹은 이번 분기에도 232 건으로 유사한 수준을 유지했다. Akira 랜섬웨어는 전 분기 133 건에서 이번 분기 220 건으로 활동량이 약 65% 증가했다. Babuk2 또는 Babuk-Bjorka 로 불리는 랜섬웨어 그룹은 이번 분기 179 건의 활동을 기록하며 활발히 움직이고 있다. 이 그룹은 과거 인도네시아 정부와 공공기관은 물론 미국, 브라질, 인도 등을 공격했던 Bjorka 가 Babuk 의 이름을 차용해 활동하는 것으로 보인다. 다크웹에 공개한 정보는 다른 그룹이 이미 유출한 데이터와 중복되거나 재사용된 것으로 보이며, 파키스탄 정부 웹사이트 공격을 제외하면 다른 구체적인 사례는 확인되지 않았으나 최근까지 랜섬웨어를 유포하며 지속적으로 활동하고 있다.

가장 많은 공격을 받은 국가는 전 분기와 마찬가지로 미국이며, 그 뒤를 이어 캐나다와 영국이 주요 피해국으로 나타났다. 산업별 피해 현황을 살펴보면, 제조와 유통/무역/운송 분야가 여전히 가장 많은 피해를 입었고, 지난 분기에 다섯 번째였던 서비스 분야는 이번 분기 세 번째로 많은 피해를 입은 산업 군으로 상승했다. IT/웹/통신, 건설 분야도 그 뒤를 이었다.

이번 분기 가장 높은 활동량을 보인 Clop 랜섬웨어 그룹은 Cleo 사의 파일 전송 프로그램의 취약점인 CVE-2024-50623, CVE-2024-55956 등을 공격에 활용했으며, 소비재, 제조, 서비스, 운송 등 다양한 분야를 가리지 않고 공격을 수행했다.

이번 분기에도 여전히 높은 활동량을 보이는 RansomHub 그룹은 다양한 취약점을 활용해 초기 침투 및 랜섬웨어 유포를 수행했다. 이들은 FortiGate의 인증을 우회해 시스템에 접속하거나, FortiOS[1], Apache ActiveMQ[2], Citrix ADC [3]등의 취약점을 통해 피해 시스템에 접근했다. 이 외에도 가짜 소프트웨어 업데이트, 자격 증명 탈취를 위한 피싱, 패스워드 초기화 피싱 등을 통해 초기 침투를 수행했다.

Akira 랜섬웨어도 꾸준히 활동하고 있다. 이들은 여전히 MFA[4]가 적용되지 않은 Cisco, SonicWall 등의 VPN 취약점을 악용하고 있으며, 외부 접근이 가능하거나 취약점이 존재하는 RDP[5]를 이용하기도 한다. 1분기 동안 주로 미국, 캐나다, 유럽 등을 공격했으며, 그중에서도 미국을 중심으로 활발히 공격을 수행했다.

[1] FortiOS: Fortinet 사의 보안 플랫폼 Fortinet Security Fabric의 운영체제

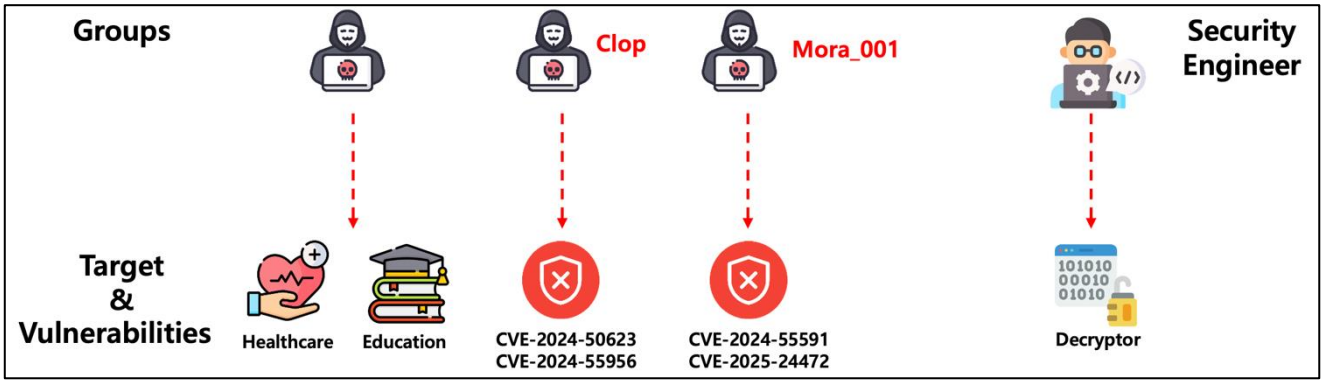
[2] Apache ActiveMQ: 서버와 클라이언트간의 메세지를 주고받기 위한 메시지 브로커

[3] Citrix ADC(Application Delivery Controller): 애플리케이션 트래픽의 로드 밸런싱, 가속, 보안 기능을 제공하는 Citrix의 네트워크 장비

[4] MFA(Multi-Factor Authentication) : 하나의 인증이 아닌 다단계의 인증을 통해 계정을 보호하는 방식

[5] RDP(Remote Desktop Protocol): 원격 제어를 위해 사용하는 프로토콜

3. 랜섬웨어 트렌드



[그림 2] 2025년 1분기 랜섬웨어 트렌드

✓ 고성능 GPU를 통한 Linux용 Akira 랜섬웨어 복호화 키 크랙

2025년 3월, 한 보안 연구원이 Akira 랜섬웨어의 리눅스 변종에 대응하기 위한 복호화 도구를 개발해 공개했다. Akira는 파일 암호화 시 나노초 단위의 4가지 타임스탬프를 시드로 사용해 매번 고유한 키를 생성하고, 이를 1,500회의 SHA-256 해싱을 통해 강화한 뒤 RSA-4096 공개키로 암호화해 각 파일의 끝에 저장한다. 이로 인해 개인키 없이는 복호화가 사실상 불가능하다. 보안 연구원 요하네스 누그로호(Yohanes Nugroho)는 암호화 시점 추정 값, 파일 메타데이터, 시스템 로그 등을 활용해 타임스탬프의 범위를 좁히는 방식으로 RTX 3060 및 3090 GPU를 이용한 복호화 테스트를 진행했다. 그러나 속도에 한계가 있어, 클라우드 GPU 서비스인 RunPod와 Vast.ai를 통해 RTX 4090 GPU 16대를 병렬로 활용한 결과 약 10시간 만에 복호화 키 추출에 성공했으며, 이를 GitHub에 공개했다.

이번 사례는 암호화에 사용된 시드 값을 확보할 경우, 이를 기반으로 고성능 GPU를 활용한 무작위 대입 공격을 통해 암호화 키를 복원할 수 있다는 가능성을 보여주었다.

✓ 헬스케어 분야의 지속적인 피해

지난 분기에 이어, 이번 분기에도 헬스케어 분야의 피해가 지속적으로 이어지고 있다. 캔자스의 Sunflower Medical Group은 2024년 12월 15일경 공격을 받아 220,968명의 환자 정보가 탈취되었으며, 해당 기관은 2025년 1월 7일 침해 사실을 인지했다. 유출된 데이터에는 이름, 주소, 사회보장번호, 운전면허 정보, 진료 기록 및 건강보험 정보 등 다양한 민감 정보가 포함되어 있다.

미국 로드아일랜드주의 Community Care Alliance는 2024년 7월 1일부터 5일 사이에 침해를 당해 114,000명의 환자 데이터가 노출되었고, 이와 함께 SSN[6], 의료 진단, 약물 정보 및 금융 정보도 유출된 사실이 지난 1월 8일 보고되었다. 두 기관 모두 공식 발표에서는 랜섬웨어 공격 여부를 명시하지 않았으나, 악명 높은 러시아계 랜섬웨어 그룹 Rhysida가 두 사건 모두에 대해 자신들의 공격임을 주장하며 자신들의 다크웹 유출 사이트에 수 테라바이트 규모의 탈취 데이터를 공개하고 있다.

1월 말에는 미국의 두 의료 기관인 프레더릭 헬스(Frederick Health)와 뉴욕혈액센터연합(New York Blood Center Enterprises, NYBCe)이 각각 랜섬웨어 공격을 받았다. 두 공격 모두 어떤 랜섬웨어 그룹에 의해 피해를 받았는지 공개되지

[6] SSN (Social Security Number): 미국 시민 및 영주권자 자격을 갖춘 사회보장청이 발급하는 9자리 고유 번호

않았다.

2월에도 헬스케어 분야에 대한 공격이 꾸준히 발생했다. 2월 17일에는 팔라우의 보건복지부(MHHS)가 Qilin 랜섬웨어 그룹의 공격을 받아 의료 시스템이 일시적으로 중단되는 사건이 발생했으며, 이 공격으로 Belau 국립병원을 포함한 보건부의 IT 시스템에 침투해 환자 정보와 병원 청구 내역 등 민감한 데이터를 탈취한 것으로 확인됐다. 탈취된 정보에는 2018년부터 2022년까지의 청구 요약서뿐 아니라 이름, 주소, 전화번호, 진단명, 시술 정보 등도 포함된 것으로 파악되었다.

영국의 민간 의료 및 사회복지 서비스 제공 업체인 HCRG Care Group이 Medusa 랜섬웨어 그룹의 공격을 받았다. 특히 이 공격으로 2.3TB에 달하는 데이터가 탈취당했으며, 데이터 유출을 막기 위해 200만 달러의 몸값을 요구했다. HCRG는 5,000여 명의 직원이 고용되어 있는 대기업으로 이번 사건으로 인해 환자 개인정보, 진료 기록, 여권 사본, 출생증명서, 직원 근무 표 등 광범위한 민감 정보 등이 탈취되었다.

이렇게 헬스케어 분야의 랜섬웨어 피해가 늘어나자, 피해를 줄이기 위해 FBI, CISA, MAISA 등에서 헬스케어 분야에 큰 피해를 입힌 Medusa 랜섬웨어 그룹에 대한 공동 보안 권고문을 발표하며 보건 의료 기관을 포함한 조직들의 주의를 당부했다.

✓ 교육 분야를 대상으로 하는 랜섬웨어 공격의 증가

2025년 1분기에는 헬스케어 분야뿐만 아니라 교육 분야를 대상으로 한 랜섬웨어 공격도 증가했다. 1월에는 영국의 Blacon High School이 랜섬웨어 공격을 받아 IT 시스템이 마비되었으며, 피해를 입힌 랜섬웨어 종류와 탈취된 정보 등은 밝혀지지 않았다. 이로 인해 등교가 중단되었고 Google Class를 통해 수업이 진행되었다.

2월에는 미국 브롱크스 소재 사립학교인 Riverdale Country School이 RansomHub 그룹에 의해 공격당했으며, 학생, 교직원, 학부모 등의 개인 정보와 연락처, 의료 정보 등이 탈취되었다.

3월 20일, Funksec[7] 그룹은 이탈리아의 UNIMORE(Università degli Studi di Modena e Reggio Emilia)를 공격해 1,000여 개의 내부 파일, 재무 거래 및 내부 문서 등 민감한 정보를 탈취했다고 밝혔다. 프랑스 파리의 Sorbonne University 역시 공격을 받았다. 이 그룹은 자신의 DLS[8]에 공격 사실을 게시하며, 설계도, 보고서, 자격 증명 등과 함께 Citrix 접속 흔적 및 웹 브라우저 검색 기록 등을 샘플 데이터로 공개했다. 비슷한 시기, 미국 웨스트버지니아에 위치한 Teays Valley Christian School도 랜섬웨어 공격을 받았다고 발표했다. 이 사건은 어떤 랜섬웨어 그룹의 소행인지는 밝혀지지 않았으며, 학생의 Google 계정 정보와 Discord 등의 데이터가 탈취되었다.

이처럼 전체 랜섬웨어 공격이 증가하는 가운데, 상대적으로 보안이 취약한 병원과 교육 기관이 지속적으로 침해 사고가 발생하고 있다.

✓ 통신 분야를 대상으로 한 랜섬웨어 공격

통신 분야는 국가 기반 인프라의 핵심으로, 그 중요성으로 인해 공격자들의 주요 표적이 되고 있다. 이러한 특성을 반영하듯, 2025년 1분기에는 통신사를 겨냥한 랜섬웨어 공격 사례가 다수 확인되었다.

브라질의 인터넷 제공업체 Hypernova Telecom은 Arcus 랜섬웨어 그룹의 공격을 받아, 관련 정보가 DLS(데이터 유출

[7] Funksec : 2024 년 12 월 처음 발견된 그룹으로, 랜섬웨어 공격과 공격 도구 제공을 통해 활발히 활동 중인 조직

[8] DLS (Dedicated Leaks Sites) : 공격자들이 운영하는 랜섬웨어 PR 및 탈취 데이터 공유 사이트

사이트)에 게시되었다. 이어 3월 16일에는 프랑스의 주요 통신사인 Orange 그룹이 Babuk-Bjorka 그룹에 의해 침해된 사실이 공개되었다. 공격자는 38만 건 이상의 이메일 주소, 결제 카드 정보, 구독 정보, 파트너 및 직원 관련 데이터를 포함한 1TB 분량의 데이터를 탈취했다고 주장했으나, 실제 피해 규모는 약 12,000건의 내부 문서, 총 6.5GB로 추정된다고 밝혔다. 또한 Arkana Security로 알려진 랜섬웨어 그룹은 미국 통신사 Wide Open West를 공격했다고 주장하며, 사용자 이름, 비밀번호, 이메일 주소, 보안 질문과 답변, 로그인 기록, 모뎀 정보 등이 포함된 403,000건 이상의 계정 정보를 탈취했다고 밝혔다. 이들은 해당 정보를 근거로 금전적 요구를 이어가고 있다.

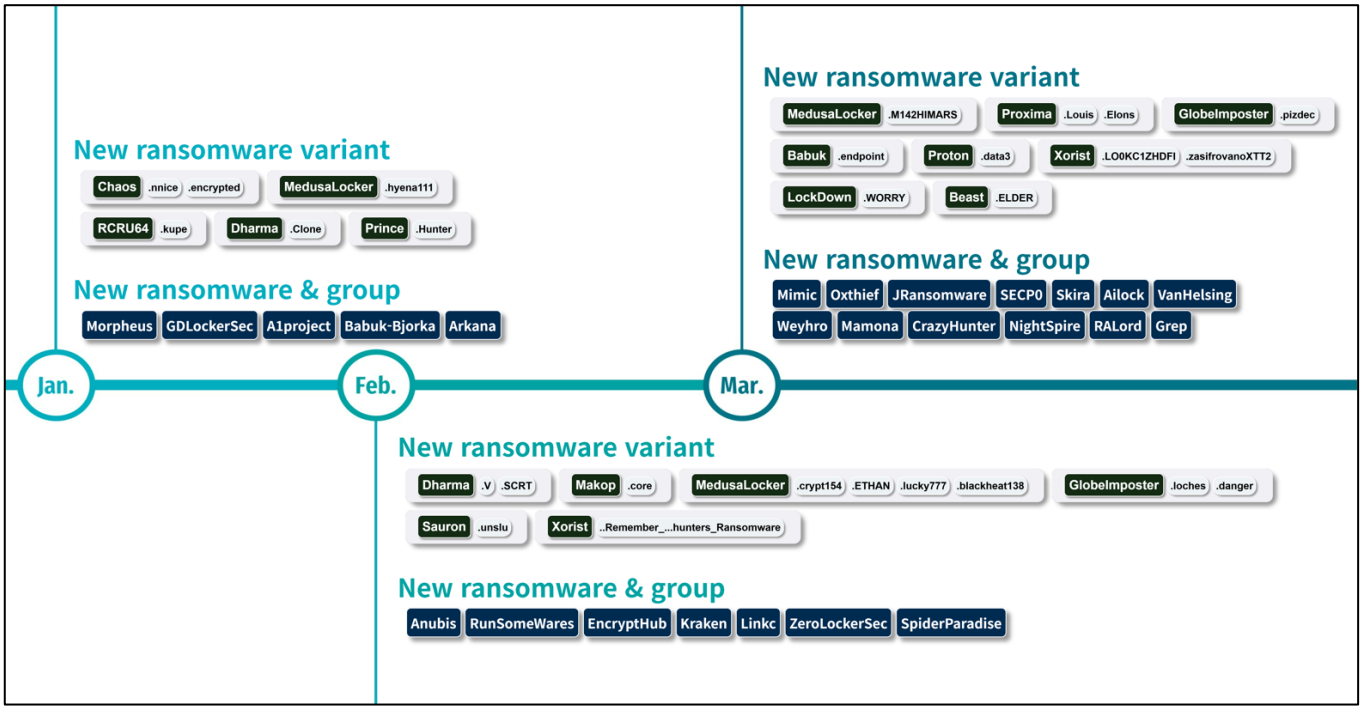
이처럼 통신 인프라를 겨냥한 공격이 지속되자, 덴마크 사이버 보안 센터(CFCS)는 자국 통신 부문에 대한 사이버 위협 수준을 '중간'에서 '높음'으로 상향 조정하며, 해당 분야의 보안 강화를 강조하고 있다.

✓ 취약점을 이용한 랜섬웨어 공격

2025년 3월, Mora_001 랜섬웨어 운영자는 Fortinet 방화벽 제품의 인증 우회 취약점(CVE-2024-55591, CVE-2025-24472)을 악용해 공격을 수행했다. 공격자는 WebSocket 및 HTTPS 요청을 통해 관리자 권한을 획득하고, 지속성을 위해 자동화 작업을 수정하며 추가 관리자 계정을 생성했다. 이후 네트워크를 수평 이동하며 데이터를 탈취한 뒤, LockBit 빌더 기반의 SuperBlack 랜섬웨어를 배포하고 탐지 회피를 위해 맞춤형 와이퍼(WipeBlack)를 사용해 공격 흔적을 제거했다.

지난 분기에 Cleo Harmony, VLTrader, LexiCom 등 Cleo의 파일 전송 설루션을 대상으로 CVE-2024-50623, CVE-2024-55956 취약점을 악용했던 Clop 랜섬웨어 그룹은 이번 분기에도 이 취약점들을 이용해 꾸준히 공격하고 있으며, 전 분기에 비해 높은 활동량을 보였다.

4. 신규 랜섬웨어 및 그룹 활동



[그림 3] 신규/변종 랜섬웨어

2025년 1분기에는 신규 랜섬웨어 그룹의 지속적인 등장이 확인되었으며, 일부 기존 그룹은 새로운 이름과 전략으로 리브랜딩 후 활동을 재개하였다. 특히, 다크웹 유출 사이트 개설과 함께 피해 기업 데이터를 다량 공개하거나, RaaS[9] 파트너를 모집하며 공격 활동을 본격화하는 사례가 증가하고 있다. 또한 일부 그룹은 클라우드 환경이나 리눅스·ESXi 등 다양한 플랫폼까지 공격 대상을 확장하고 있으며, 기존 데이터를 재활용하거나 경매 형태로 판매하는 새로운 수익 모델도 도입하고 있다. 다음은 이번 분기에 등장하거나 활동이 확인된 주요 랜섬웨어 그룹에 대한 설명이다.

- Kraken

  Kraken은 2025년 1월, 기존 HelloKitty(또는 HelloGookie) 랜섬웨어 그룹이 리브랜딩 해 등장한 그룹이다. Kraken의 다크웹 유출 사이트에는 HelloKitty 언급되어 있으며, 과거에 유출한 Cisco의 데이터와 함께 새로운 피해자 데이터가 포함되어 있다. 이들은 윈도, 리눅스, VMware ESXi 시스템을 표적으로 유사한 공격 기법을 계속 사용하고 있으며, 최근 미국과 폴란드에서 여러 건의 새로운 피해자를 발생시키며 활발히 활동 중이다.

- Morpheus

  Morpheus는 2025년 1월에 확인된 신규 그룹으로, 첫 유출 데이터가 2024년 12월 혹은 그 이전에 이미 공격된 것으로 나타나 다크웹 유출 플랫폼의 준비 이후 공개 시점이 지연된 것으로 보인다. 총 3건의 피해자를 게시했으며, 이 중 한 건은

[9] RaaS(Ransomware as a Service) : 서비스형 랜섬웨어의 약어로, 금전을 대가로 랜섬웨어를 서비스 형태로 제공하는 수익 모델

2024년 8월 발생한 공격이었다. 이는 피해 공개 시점과 실제 공격 시점 사이에 상당한 시간차가 발생할 수 있음을 시사한다.

- GDLockerSec

  GDLockerSec는 2025년 1월에 등장해 AWS를 포함한 5건의 피해 데이터를 다크웹 유출 사이트에 게시했다. 이들은 Amazon 클라우드에서 9GB 분량의 데이터를 탈취했다고 주장했지만, 실제 공개된 내용은 Kaggle의 공개 데이터 셋과 동일한 것으로 나타나 허위 데이터 사용 의혹이 제기되었다. 과거 GhostSec-Devil이라는 명칭으로 활동한 전력이 있으며, GhostLocker 기반 랜섬웨어와의 연관성도 있으나 아직 명확히 밝혀지지 않았다.

- A1project

  A1project는 Windows, Linux, ESXi를 아우르는 멀티플랫폼 암호화 기능을 갖춘 랜섬웨어를 기반으로 활동을 개시했다. 이 그룹은 다크웹 해킹 포럼에서 RaaS 파트너를 모집하며, 피해자별 채팅 채널, 데이터 유출 사이트, 파트너 관리 패널을 제공한다. 파트너는 20%의 수수료만 지불하면 독립적으로 활동할 수 있으며, 암호화 기능과 비밀 협상 기능이 포함된 관리 인프라가 이미 구성되어 있다.

- Babuk-Bjorka

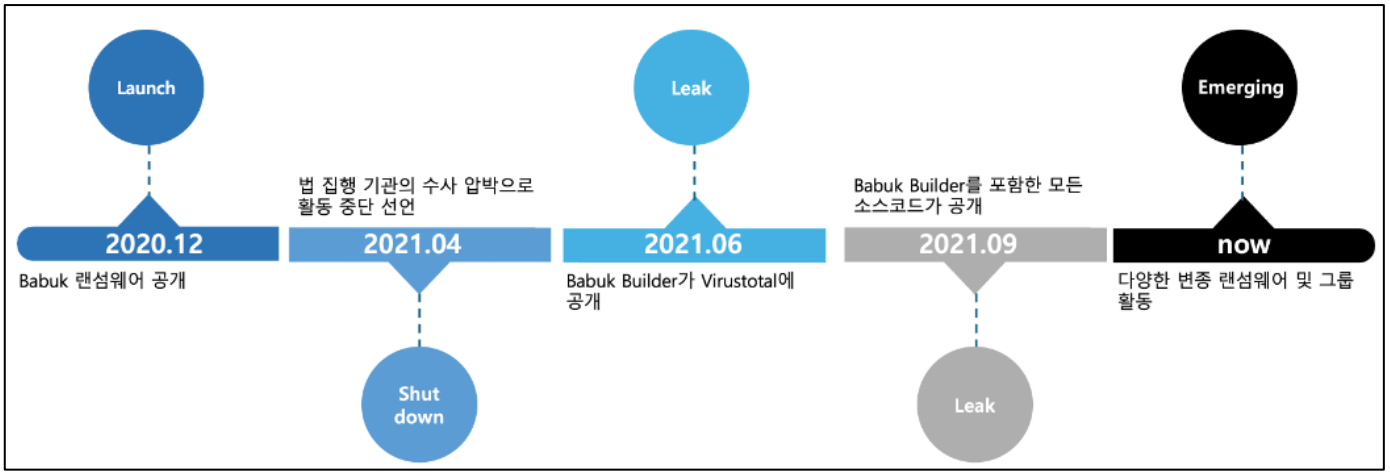
  Babuk2는 해커 Bjorka가 운영하는 것으로 알려진 신규 그룹으로, 기존 Babuk 랜섬웨어와 동일한 명칭을 사용하지만 연관성은 확인되지 않았다. 이들은 총 66건의 피해자 정보를 공개했으나, 상당수가 Funksec, LockBit, RansomHub 등에서 유출된 데이터를 재활용한 것으로 확인됐다. 다크웹 포럼 활동 내역과 피해자 소개 문구도 유사한 사례가 존재해, 독자적인 침해 여부는 불분명하다.

- Anubis

  Anubis는 2025년 2월 러시아 해킹 포럼에 처음 등장한 그룹으로, RaaS 외에도 데이터 협박 서비스, 내부 권한 판매 등을 포함하는 다양한 수익 모델을 운영하고 있다. 협상 전 데이터 공개 없이 민감 정보 노출을 암시하는 형태의 데이터 기반 협박 전략을 구사하며, 다크웹 유출 사이트에 피해 데이터를 공개했다. 각 파트너에게는 수수료 20% 조건이 제공되며, 기존 RaaS보다 구조화된 서비스형 운영 모델이 특징이다.

Babuk Ransomware 그룹 상세 분석

1. 개요



[그림 4] Babuk 랜섬웨어 진화 과정

Babuk 랜섬웨어는 2020 년 후반 처음 등장 후 북미와 유럽의 주요 인프라, 의료·정부 기관을 표적으로 삼으며 빠르게 심각한 위협으로 자리매김했다. 초기에는 단순히 랜섬웨어 페이로드만 발견되었으나, 곧 자체 RaaS(서비스형 랜섬웨어) 모델을 구축하고 제휴 파트너에게 공격 인프라를 제공하며 활동 반경을 확장했다. Babuk 운영자들은 전통적인 파일 암호화·몸값 협박 방식을 넘어, 중요 데이터를 유출한 뒤 협상에 응하지 않을 경우 이를 공개하는 '이중 협박(Double Extortion)' 전술을 사용해 피해자에게 압박했다. 초기에는 협상에 응하지 않은 피해자의 정보를 공개된 해킹 포럼에 올렸으나, 이후 독자적인 데이터 유출 사이트를 구축해 유출 데이터를 관리 및 게시했다.

Babuk 은 감염 시 로컬 드라이브 외에도 네트워크 드라이브까지 파일을 암호화할 수 있으며, C&C 서버와의 연결 없이도 암호화가 가능해 폐쇄망 환경에서도 피해가 발생할 수 있다. 초기 감염 벡터로는 피싱 이메일, 취약한 원격 데스크톱 프로토콜(RDP), 소프트웨어 취약점, 그리고 Cobalt Strike 등 공격 도구가 활용되었다.

2021 년 4 월, 워싱턴 DC 경찰서 공격을 마지막으로 Babuk 운영자들은 랜섬웨어 운영을 중단하고, 데이터 유출 사이트를 Payload.Bin 으로 리브랜딩 해 순수 데이터 강탈 모델로 전략을 전환했다. 그러나 법 집행기관의 수사 압박과 내부 분열로 조직은 결국 해체되었다.

이후 글로벌 악성코드 공유 사이트에 Babuk 랜섬웨어의 빌더가 공개되었고, 이후 이 그룹의 구성원으로 추정되는 인물이 러시아어권 해킹 포럼에 Babuk 전체 소스 코드를 공개했다. 유출된 소스코드와 빌더에는 Windows, NAS[10], VMware ESXi 등 다양한 플랫폼을 지원하는 암복호화기, 키 생성기 등이 포함되어 있었으며, 이로 인해 Rook, RA Group 등 Babuk 기반의 다양한 파생 랜섬웨어가 등장했다. 현재까지도 Babuk 소스코드를 뿌리로 둔 랜섬웨어들이 꾸준히 공격에 활용되고 있다.

'.babuk', '.babyk', '.doydo' 등 다양한 확장자를 사용한 Babuk 은 소스코드가 공개되고 보안업체에서 무료 복호화 툴을 배포하기도 했다. 이번 KARA 에서는 Babuk 랜섬웨어의 출현과 소스코드 공개, 변종 랜섬웨어의 등장과 최근 활동까지의 특징 등을 종합적으로 분석한다.

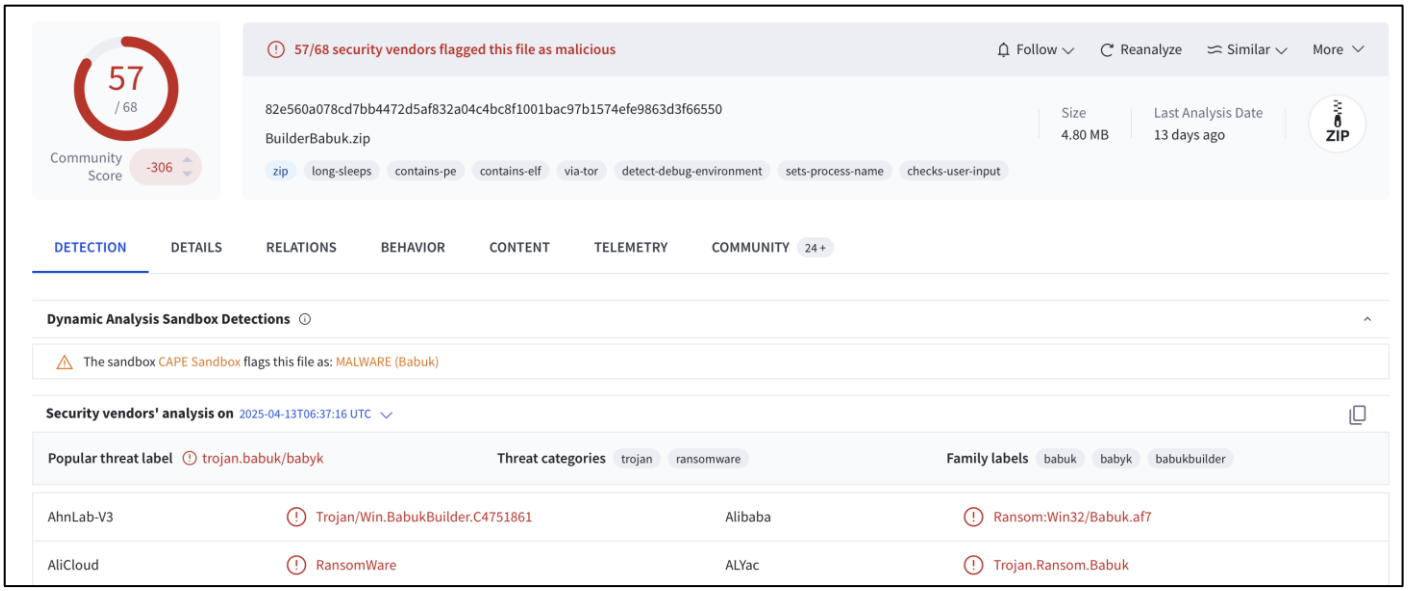
[10] NAS (Network Attached Storage): 네트워크를 통해 데이터를 저장하고 엑세스 하는 저장 장치

2. Babuk 랜섬웨어 활동 변화

2020 년 12 월경 최초로 활동을 시작한 것으로 보이는 babuk 랜섬웨어는 유럽의 소규모 기업을 대상으로 공격을 시작해 미국, 아시아, 아프리카 등 다양한 국가를 대상으로 공격 범위를 넓혔다. 이들은 다른 랜섬웨어 그룹들처럼 병원이나 비영리 재단, 교육기관, 중소기업의 일부를 공격하지 않는다는 예외를 두고 활동했다. 2021 년 상반기 동안 활발히 활동하면서 금전을 갈취했고, 2021 년 4 월에는 워싱턴 DC 경찰서를 공격해 정보를 탈취했다. 이들은 협상이 원활하게 진행되지 않자 워싱턴 DC 경찰서에서 탈취한 민감 정보들을 공개하면서 큰 이슈가 되었으며 이 사건 이후 법 집행 기관의 압박으로 돌연 활동 중단을 선언했다.

활동 중단을 선언하고 얼마 지나지 않아 이들은 랜섬웨어를 직접 운영하고 공격하는 방식이 아닌 자신들의 DLS 사이트를 Payload.bin 으로 리브랜딩 후 타 랜섬웨어 그룹의 탈취 정보 등을 호스팅 하는 방식으로 운영했다.

2021 년 6 월 27 일경 영국의 보안 전문가가 악성코드 공유 플랫폼인 Virustotal 에 babuk 랜섬웨어의 빌더가 업로드된 정황을 확인했다. 업로드된 빌더는 랜섬웨어 제작을 위한 전체 소스코드가 아닌 타깃 운영체제별 템플릿 실행 파일과, 템플릿 실행 파일에 암호화 키 및 랜섬노트를 입력하고, 암호화 키를 생성하는 builder 프로그램, 랜섬노트 구성용 텍스트 파일로 구성되어 있다.



[그림 5] Virustotal 에 업로드된 Ransomware Builder

6 월에 babuk 랜섬웨어의 빌더가 유출된 이후, 별도의 RaaS 없이도 누구나 자신의 babuk 랜섬웨어를 빌드 해 유포할 수 있게 되면서 babuk 랜섬웨어 공격 보고가 늘어났다. 특히 유출된 빌더에는 단순 윈도우 환경뿐만 아니라 ESXi, arm, linux 환경의 바이너리도 포함되어 있어 위협이 높아졌다.

빌더가 공개되고 3 개월 지난 2021 년 9 월, 러시아어를 사용하는 해킹 및 보안 포럼인 vxunderground 에 Babuk 랜섬웨어의 멤버로 활동한 것으로 추정되는 dyadka0220 이라는 사용자가 babuk 랜섬웨어의 전체 소스코드를 공개했다.

[그림 6] 다크웹 포럼에 업로드 된 Babuk Source[11]

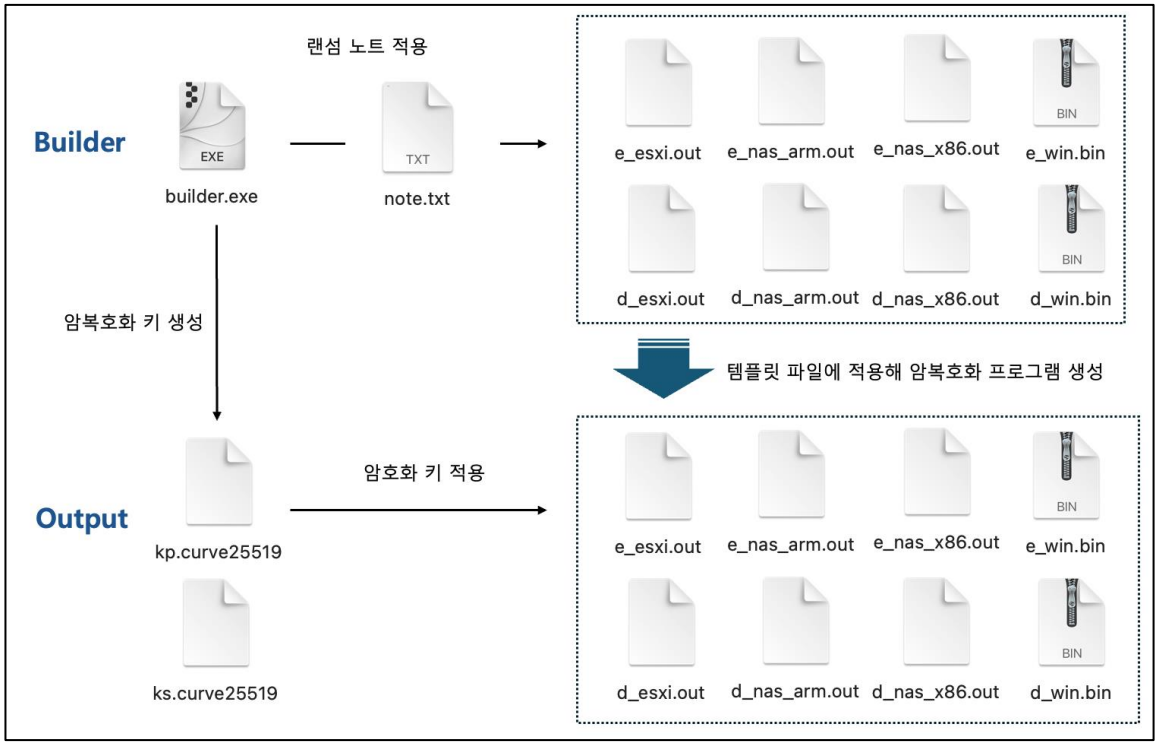
Virustotal 에 업로드된 데이터는 악성코드를 제작하기 위한 빌더와 템플릿 바이너리만 존재했지만, 해킹 포럼에 사용자가 업로드한 소스코드에는 빌더를 포함한 암복호화 소스, 키 생성 프로그램, Windows/NAS/ESXi 를 대상으로 하는 소스코드까지 포함되었다.

소스코드가 공개된 이후 많은 랜섬웨어 그룹들이 babuk 랜섬웨어의 소스코드를 이용해 공격을 수행하거나, 자신들의 랜섬웨어에 기능을 추가해 윈도우 환경을 노리는 랜섬웨어뿐만 아니라 NAS 및 ESXi 기반의 운영체제를 공격하는 계기가 되었다.

[11] https://www.bleepingcomputer.com/news/security/babuk-ransomwares-full-source-code-leaked-on-hacker-forum/

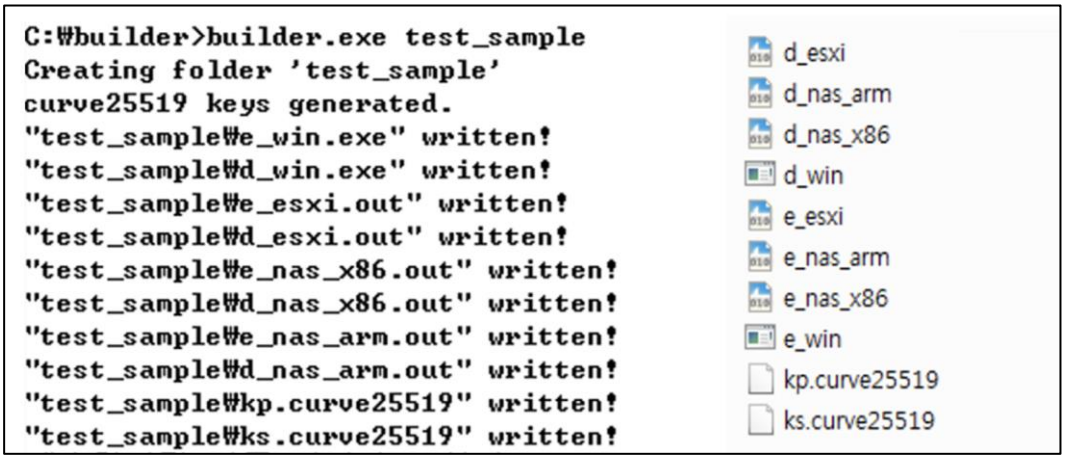
3. Babuk Builder 및 소스코드 분석

2021 년 6 월 바이러스 토탈에 업로드된 Babuk 빌더에는 빌더 프로그램, 랜섬노트가 기록된 note.txt, 타깃별 랜섬웨어 암복호화기로 구성되어 있다.



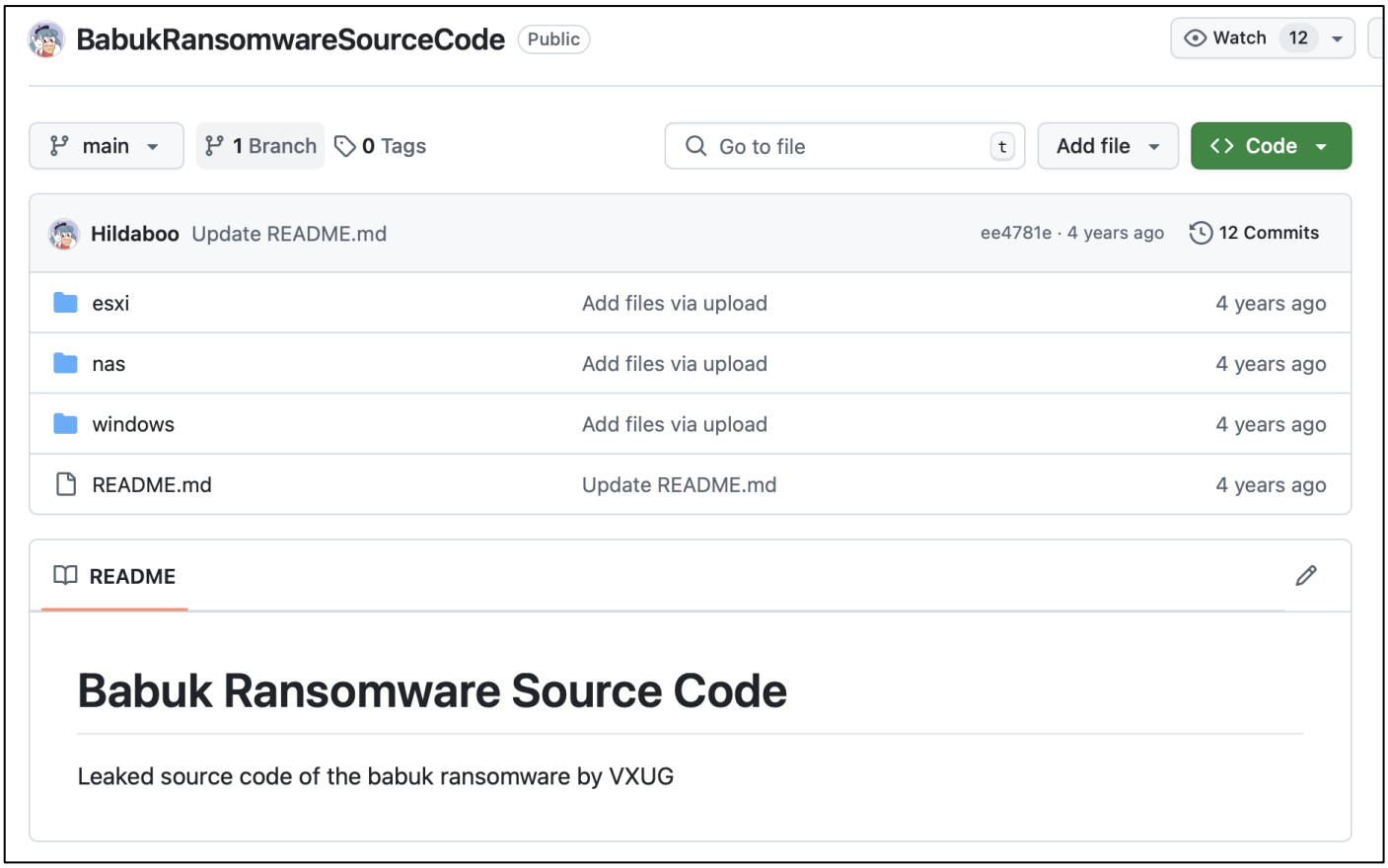
[그림 7] Babuk Builder 구조

빌더 프로그램은 생성한 랜섬웨어 파일이 저장될 폴더를 인자로 받는다. 빌더 프로그램에는 특정 운영체제에서 동작하는 랜섬웨어만 제작하는 옵션이 없어 실행과 함께 암복호화 키를 생성하고, 같은 디렉토리에 존재하는 모든 운영체제 환경의 템플릿 파일들을 메모리에 읽어 note.txt 파일에 기록된 랜섬노트, 암복호화 키를 파일의 특정 영역에 입력해 암복호화 프로그램을 생성한다.



[그림 8] Babuk 랜섬웨어 Builder 동작

빌더가 공개되고 3 개월 뒤인 9 월, 공개된 babuk 의 전체 소스코드에는 기존에 공개된 빌더의 원본 소스코드를 포함해 윈도우, 리눅스, ESXi 및 NAS 를 타깃으로 하는 랜섬웨어 프로그램이 함께 포함되었다. 공개된 랜섬웨어 소스코드는 현재 github 에서도 확인 가능할 정도로 대중적으로 퍼져있다.



[그림 9] Babuk 랜섬웨어 소스코드

공개된 소스코드에는 ESXi, NAS, windows 로 나눠져 있고 이중 NAS 용 소스코드는 go 기반, 그 외 모든 소스코드는 c 로 작성되었다. 또한 ESXi/NAS 용 소스코드에는 en/decryptor 소스코드만 존재하며 이를 기반으로 실행 가능한 템플릿 바이너리를 생성 가능하도록 되어있다. 별도의 키 생성을 통해 ESXi/NAS 용 프로그램을 별개로 만들 수 있지만, 기본적으로는 템플릿 바이너리만 생성하고, builder 를 통해 모든 운영체제용 바이너리를 생성하도록 구성되어 있다.

- Builder 프로그램

  빌더 프로그램이 시작되면 curve25519를 통해 타원곡선 암호화에 사용할 공개키와 비밀키를 생성한다. 생성된 키는 인자로 받은 경로에 공개키와 비밀키를 분리해 저장한다. 이후 파일에 저장된 랜섬노트의 위치와 공개키의 패턴을 찾아온 뒤 랜섬노트와 키 정보를 입력해 암호화 바이너리를 생성한다. 복호화 프로그램 또한 같은 방식으로 복호화 키가 저장될 위치의 패턴을 찾은 뒤 비밀키를 입력해 복호화 프로그램을 생성한다.

패턴 및 파일명	정보
notepattern	암호화 프로그램의 랜섬노트가 저장되는 영역의 패턴
curvepattern	암호화 프로그램의 공개키가 저장되는 영역의 패턴

curvepattern	복호화 프로그램의 비밀키가 저장되는 영역의 패턴
kp.curve25519	암호화에 사용될 공개키가 저장되는 파일명
ks.curve25519	복호화에 사용될 비밀키가 저장되는 파일명

- NAS

NAS를 대상으로 하는 랜섬웨어 프로그램은 Go 언어로 개발되어 있다. 이 랜섬웨어는 Go 루틴을 이용해 멀티 스레드 기반으로 파일 암호화를 수행하며 파일 크기에 따라 암호화하는 사이즈가 달라진다. 파일의 크기가 4MB 보다 작다면 파일의 전체를 암호화하고, 20MB 보다 작은 경우 파일의 상위 4MB만 암호화를 수행한다. 만약 암호화할 파일의 크기가 20MB보다 클 경우 파일을 10MB 단위로 청크를 생성한 뒤 각 청크의 상위 1MB만 암호화한다.

암호화 작업은 랜덤한 비밀키를 생성하고, 공격자의 공개키와의 연산을 통해 공유 비밀값을 생성한 후, 이 값을 기반으로 스트림 암호화를 수행하는 방식으로 이루어진다. 암호화 완료 후, 파일 끝에는 새로 생성한 공개키(32바이트)와 고정된 식별 플래그(6바이트)가 추가로 기록된다. 모든 암호화 작업은 완료 후 원본 파일 이름에 .babyk 확장자가 추가된 형태로 저장된다. 또한, 암호화 경로의 각 디렉터리에는 README_babyk.txt 라는 이름의 랜섬노트가 생성된다.

- ESXi

ESXi 서버를 타깃으로 하는 랜섬웨어 소스코드는 C 언어로 개발되어 있다 프로그램은 암호화할 대상 경로를 인자로 받아 실행하는 형태로, 인자로 받은 경로를 탐색해 특정 확장자(.log, .vmdk, .vmem, .vswp, .vmsn)를 가진 파일 목록을 가져온다. 암호화 대상 파일이 결정되면, 공격자의 공개키를 기반으로 암호화 정보를 설정하고 스트림 암호키를 생성하며, 스트림 암호 sosemanuk 사용해 파일을 암호화한다. 암호화는 최대 512MB 또는 파일 전체 크기 중 작은 범위까지만 수행된다. 암호화가 완료되면 파일 끝에 생성된 공개키 32바이트를 추가 기록하며, 암호화된 파일의 확장자에 .babyk를 추가해 저장한다. 마지막으로 각 디렉토리마다 복호화 안내가 포함된 랜섬노트 파일이 How To Restore Your Files.txt라는 이름으로 생성된다.

- Windows

Windows 환경에서 동작하는 랜섬웨어는 다른 랜섬웨어에 비해 많은 기능을 가진다. 프로그램이 시작되면 랜섬웨어가 모든 파일을 정상적으로 암호화할 수 있도록 백신 프로그램이나, 일부 백업관련 서비스 등을 중단하고, 문서 작업과 관련된 프로세스를 포함한 일부 프로세스를 종료한다. 이후 윈도우 환경에서 감염 이전 상태로 복구할 가능성이 있는 Volume Shadow Copy를 삭제하고, 휴지통을 비운다.

종료 서비스		
vss	sql	svc$
memtas	mepocs	sophos
veeam	backup	GxVss
GxBlr	GxFWD	GxCVD
GxCIMgr	DefWatch	ccEvtMgr
ccSetMgr	SavRoam	RTVscan
QBFCService	QBIDPService	Intuit.QuickBooks.FCS
QBCFMonitorService	YooBackup	YooIT

zhudongfangyu	stc_raw_agent	VSNAPVSS
VeeamTransportSvc	VeeamDeploymentService	VeeamNFSSvc
veeam	PDVFSService	BackupExecVSSProvider
BackupExecAgentAccelerator	BackupExecAgentBrowser	BackupExecDiveciMediaService
BackupExecJobEngine	BackupExecManagementService	BackupExecRPCService
AcrSch2Svc	AcronisAgent	CASAD2DWebSvc
CAARCUpdateSvc		
종료 프로세스		
sql.exe	oracle.exe	ocssd.exe
dbsnmp.exe	synctime.exe	agntsvc.exe
isqlplussvc.exe	xfssvccon.exe	mydesktopservice.exe
ocautoupds.exe	encsvc.exe	firefox.exe
tbirdconfig.exe	mydesktopqos.exe	ocomm.exe
dbeng50.exe	sqbcoreservice.exe	excel.exe
infopath.exe	msaccess.exe	mspub.exe
onenote.exe	outlook.exe	powerpnt.exe
steam.exe	thebat.exe	thunderbird.exe
visio.exe	winword.exe	wordpad.exe
notepad.exe		

파일 암호화를 수행하기 전 인자로 받은 값을 통해 암호화 옵션을 선택한다.

설정	설정 정보
-debug=[PATH]	디버그 정보 기록 여부 및 정보 저장 경로
-shares=[PATH]	암호화 대상이 되는 네트워크 공유 폴더
-paths=[PATH]	암호화를 수행할 특정 경로
-sf	shared 폴더 탐색

윈도우 환경에서 동작할 경우 실행 중인 환경의 프로세스의 코어 개수에 따라 스레드를 생성해 파일을 찾고 암호화를 수행한다. 암호화를 위한 스레드를 실행하고 난 뒤 프로세스는 paths 옵션과 shares 옵션이 지정되지 않았을 경우 뮤텍스를 생성한다. 뮤텍스 이름에 포함된 Chungdong은 한 보안 연구원의 이름으로 babuk 랜섬웨어를 최초로 공개한 이력이 있다.

- 뮤텍스 이름 : DoYouWantToHaveSexWithCuongDong

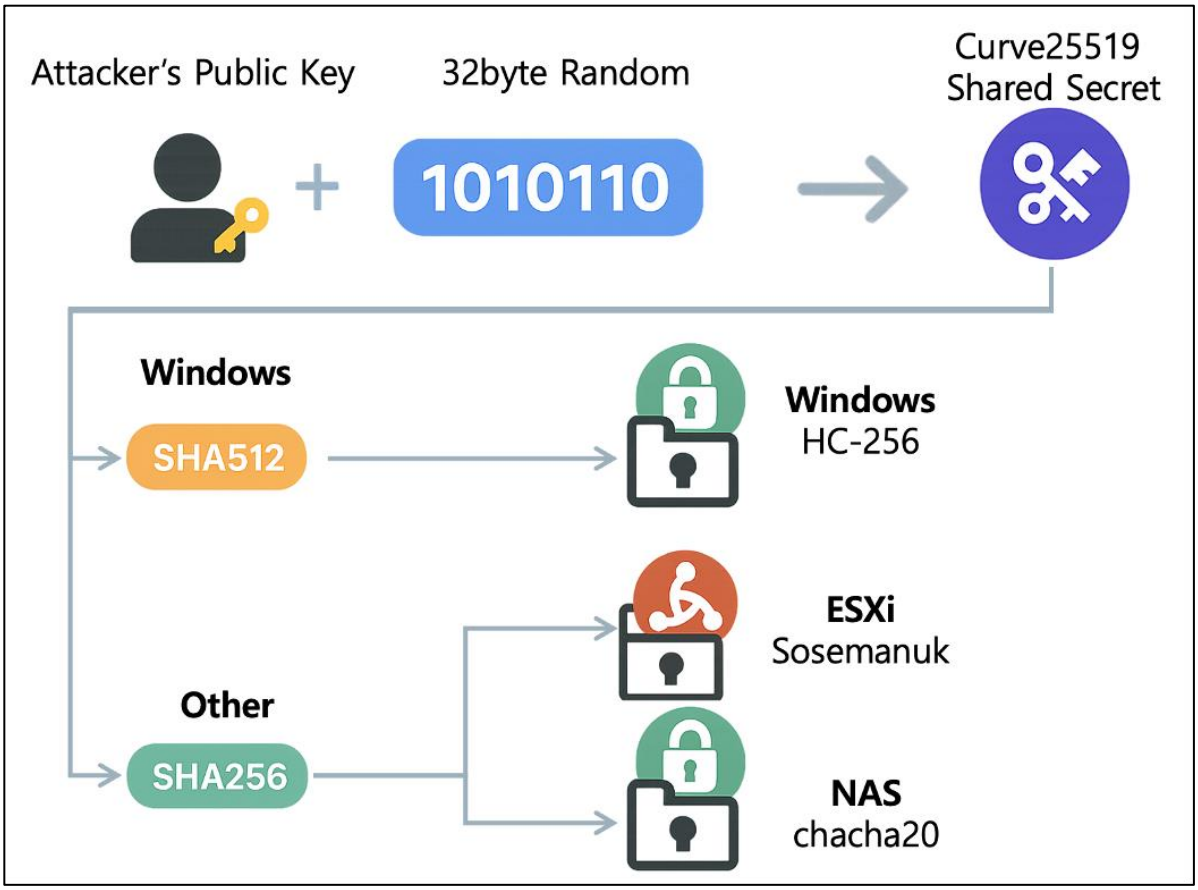
- 암복호화 타깃 폴더 및 파일

NAS, ESXi, Windows에서 동작하는 랜섬웨어는 각각마다 특징을 가지고 있으며 대상 시스템에 따라 암호화 대상 파일명이 존재하거나, 암호화 예외 폴더 등이 존재한다. 암호화를 수행한 뒤 감염 폴더에 Windows, ESXi는 “How To Restore Your Files.txt”, NAS 환경에는 “README_babyk.txt”라는 이름으로 랜섬노트를 생성한다. 각 환경에 따른 랜섬웨어의 암호화 대상 및 예외 대상은 다음과 같다.

ESXi 랜섬웨어 타깃 파일		
.log	.vmdk	.vmem
.vswp	.vmsn	
NAS 랜섬웨어 예외 폴더		
/proc	/boot	/sys
/run	/dev	/etc
/home/httpd	.system/thumbnail	.system/opt
.config	.qpkg	/mnt/ext/opt
.system/opt	.config	
Window 랜섬웨어 예외 폴더		
AppData	Boot	Windows
Windows.old	Tor Browser	Internet Explorer
Google	Opera	Opera Software
Mozilla	Mozilla Firefox	$Recycle.Bin
ProgramData	All Users	autorun.inf
boot.ini	bootfont.bin	bootsect.bak
bootmgr	bootmgr.efi	bootmgfw.efi
desktop.ini	iconcache.db	ntldr
ntuser.dat	ntuser.dat.log	ntuser.ini
thumbs.db	Program Files	Program Files (x86)
#recycle	..	.

- 파일 암호화

  세 가지 프로그램 모두 공격자의 공개키를 기반으로 암호화 키를 생성해 파일 암호화를 수행한다. 랜섬웨어는 실행 시 자체적으로 32바이트 크기의 임의의 개인 키를 생성하며, 이를 이용해 Curve25519 연산을 수행 후 공격자의 공개키와 공유 비밀 값을 계산한다. 이후, 이 공유 비밀 값을 기반으로 Linux와 NAS용 랜섬웨어는 SHA-256 해시 연산을 통해 암호화 키를 생성하고, Windows용 랜섬웨어는 SHA-512 해시 연산을 사용해 암호화 키를 생성한다. 생성된 키는 각 플랫폼별 스트림 암호화 알고리즘에 적용되며, Windows는 HC-256, Linux는 Sosemanuk, NAS 용은 ChaCha20을 이용해 파일을 암호화한다. 암호화가 완료된 파일은 각각 파일 끝에 생성된 공개키를 추가로 기록하며, Windows 용의 경우 공개키 외에도 메타데이터(해시값 및 고정 플래그 데이터)를 함께 저장한다.



[그림 10] Babuk 랜섬웨어 암호화 구조

4. 변종 랜섬웨어 출현

Babuk 외에도 Conti, LockBit 등 여러 랜섬웨어에서 소스코드 유출 사건이 발생한 바 있다. 이러한 유출은 공격자들이 손쉽게 랜섬웨어를 제작할 수 있는 기반을 제공하며, 다양한 파생 랜섬웨어가 제작되고 활동하는 계기가 된다. 특히, 소스코드 전체가 유출될 경우 그 기반을 활용한 변종이 장기간에 걸쳐 지속적으로 등장하며, 이를 바탕으로 새로운 형태로 발전한 랜섬웨어가 나타나기도 한다. Babuk 의 경우, 2021 년 소스코드가 유출된 이후 상당한 시간이 지났음에도 일부 활동 중인 그룹에서 여전히 해당 코드의 흔적이 발견되고 있다. 아래는 해당 소스코드 유출 이후 활동한 주요 랜섬웨어 및 관련 그룹들이다.

- Rook

  2021 년 12 월에 등장한 Babuk 소스코드를 기반으로 만들어진 랜섬웨어이다. 주로 기업들을 대상으로 공격한 이들은 CobaltStrike, 피싱 이메일 등을 통해 유포되고, 간단한 패킹을 통해 코드를 숨기는 특징을 가지고 있다.

- Night Sky

  2022 년 1 월 등장한 랜섬웨어로 Babuk 의 Window 기반 랜섬웨어 소스코드를 통해 악성코드가 제작되었다. 악성코드는 VMProtect 를 통해 패킹해 탐지를 우회했고, 암호화 방식을 AES 와 RSA 로 변경했다.

- RTM Locker

  2022년 하반기 등장한 랜섬웨어로 주로 Window 환경보단 Linux, NAS, ESXi와 같은 서버들을 대상으로 공격을 수행했다.

- RA Group

  2023 년 4 월 처음 발견되었으며 국내에도 많은 피해를 입힌 랜섬웨어 그룹으로 유명하다. 이들은 여러 국가의 제조, 제약, 자산관리 및 보험 등의 분야를 대상으로 공격을 수행했으며 DLS 사이트를 운영했다.

- Babuk2

  Babuk2 는 2025 년 1 월부터 활동을 시작한 신생 랜섬웨어 그룹으로, 기존 Babuk 과는 연관이 없는 별개의 조직이다. 이들은 자체적으로 DLS 를 운영하며 여러 기업의 데이터를 공개하고 있으나, 실제 침해가 없는 기업의 정보를 마치 탈취한 것처럼 위장해 게시하는 사례가 자주 확인된다. 공개된 데이터는 과거에 유출된 자료를 재사용하거나 조작한 경우가 많고, 중복되거나 품질이 낮은 정보도 포함되어 있는 것이 특징이다. 그룹은 LockBit 의 운영 방식과 유사한 제휴 프로그램을 홍보하며 활동 범위를 넓히고 있으며, 허위·과장된 전략을 통해 영향력을 확대하려는 시도를 지속하고 있다. 비록 Babuk 과 직접적인 연관은 없지만, Babuk 의 명성을 이용해 자신들의 활동을 정당화하거나 홍보 수단으로 활용하려는 의도를 보인다.

위에서 언급한 그룹 이외에도 Delta, AstraLocker, Nokoyawa, Cyclops, Knight, Abyss, Mario ESXi, Dark Angels, DarkyLock, Holiday Spider, Daixin, ARCrypter, Gooday, Cheers 등 다양한 그룹들이 등장해 활동하고 사라졌다. 일부 이름이 알려지지 않은 랜섬웨어 그룹의 경우에도 Babuk 랜섬웨어의 소스코드를 기반으로 랜섬웨어를 작성해 공격을 수행했으며, RA Group 의 경우 최근까지도 활발히 활동하고 있다.

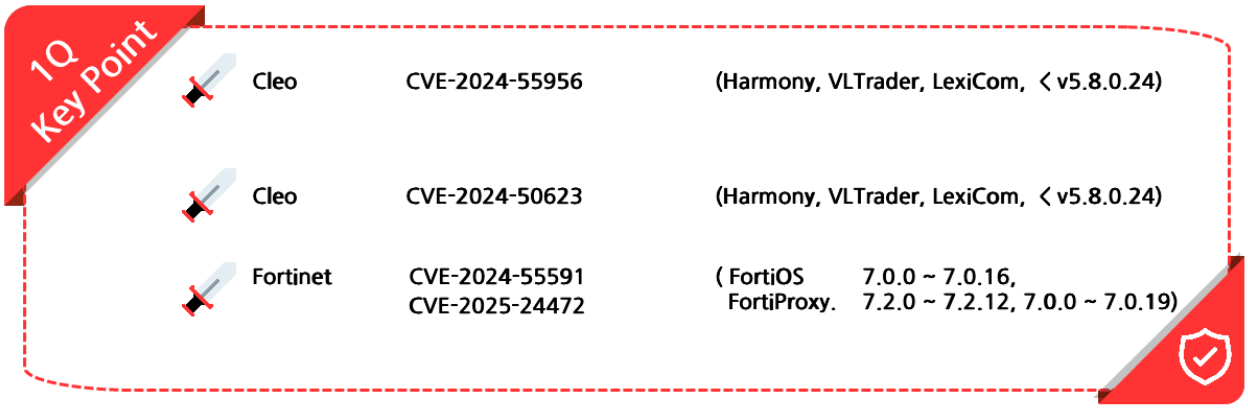
5. IoCs

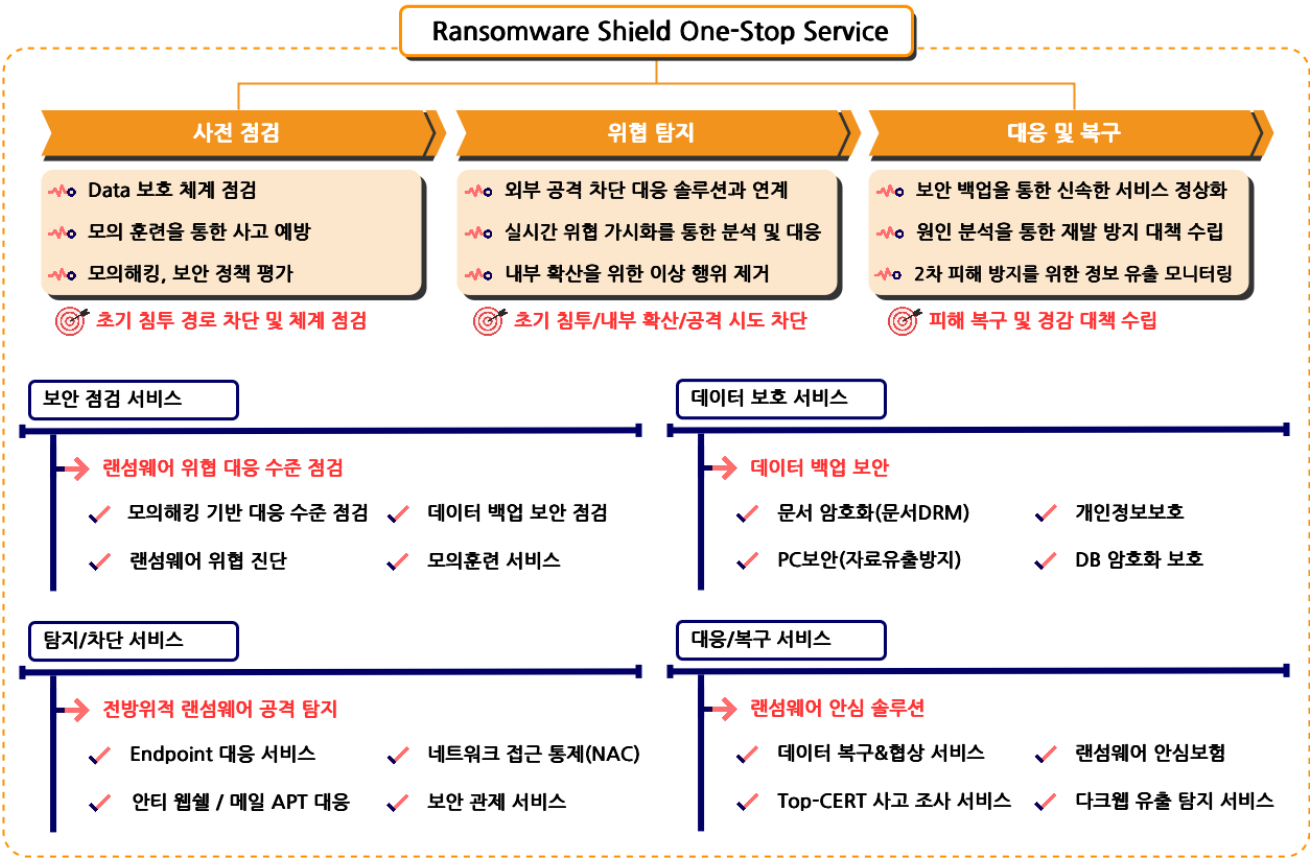
SHA256
3f9349783f0c93cf8c46ab31e96057b9ec364627a28bdf6b187d53696edd8e41

랜섬웨어 Mitigations

1. 랜섬웨어 대응방안 안내

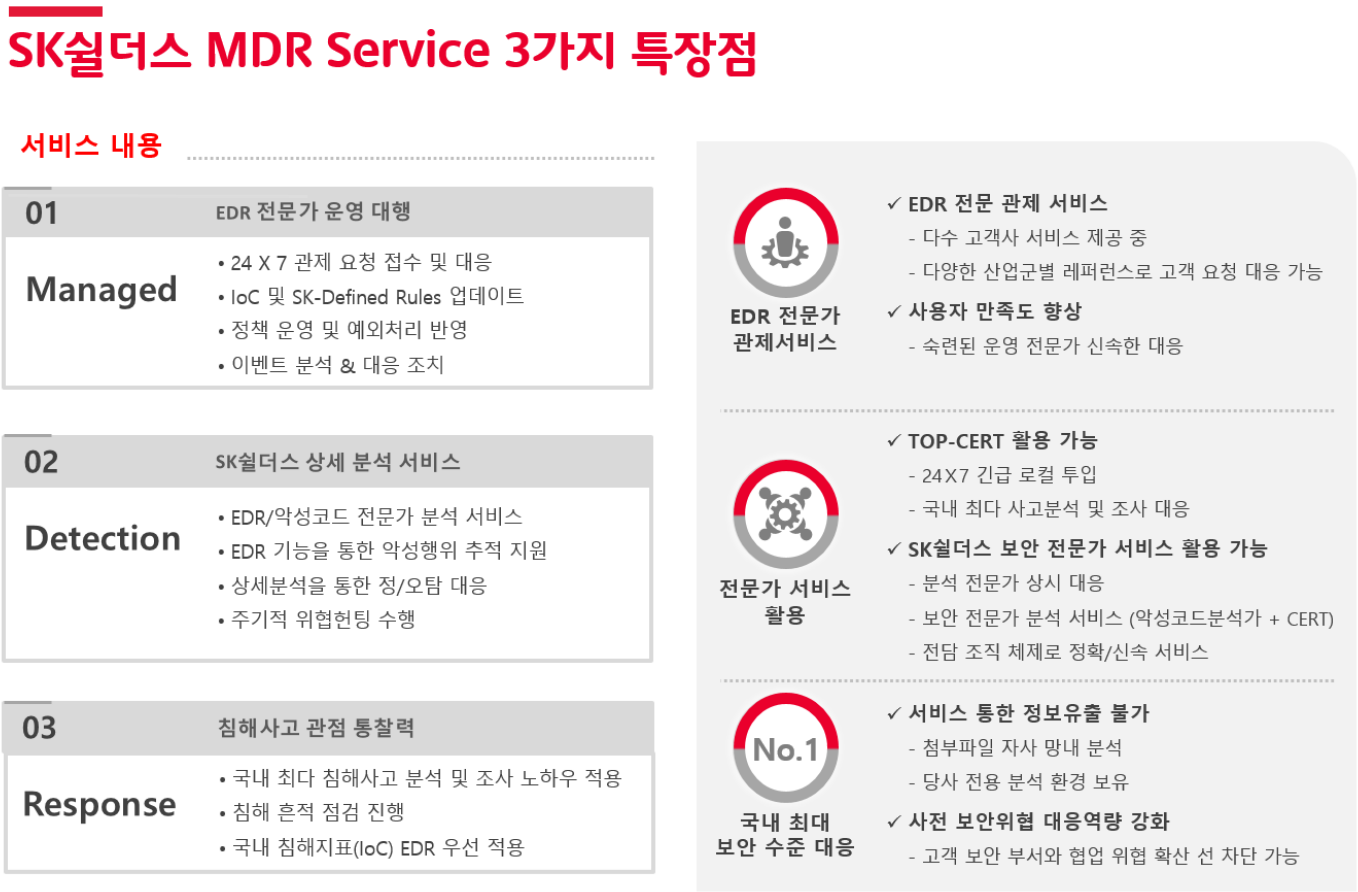
이번 분기 활발히 활동한 Clop 랜섬웨어는 Cleo의 파일 전송 솔루션에 존재하는 CVE-2024-50623, CVE-2024-55956 등의 취약점을 악용해 초기 침투를 수행한다. 다른 랜섬웨어 그룹들은 Fortinet 방화벽의 취약점인 CVE-2024-55591, CVE-2025-24472를 악용해 침투했다. 이후 다양한 산업군을 대상으로 시스템을 장악하고 데이터를 탈취한 뒤, 협상이 결렬되면 다크웹 유출 사이트에 게시하는 이중 갈취 전략을 사용한다. 이런 랜섬웨어의 공격에 대응하기 위해 최신 취약점 패치를 빠르게 적용해야 하며, 내부 시스템에 대한 접근 제어와 로그 모니터링을 강화해야 한다. 또한 공격자는 파일 공유 환경을 노리므로, 내부 자산에 대한 접근 통제를 세분화하고, 전송 이력 모니터링을 통해 비정상적 행위를 조기 탐지해야 한다.



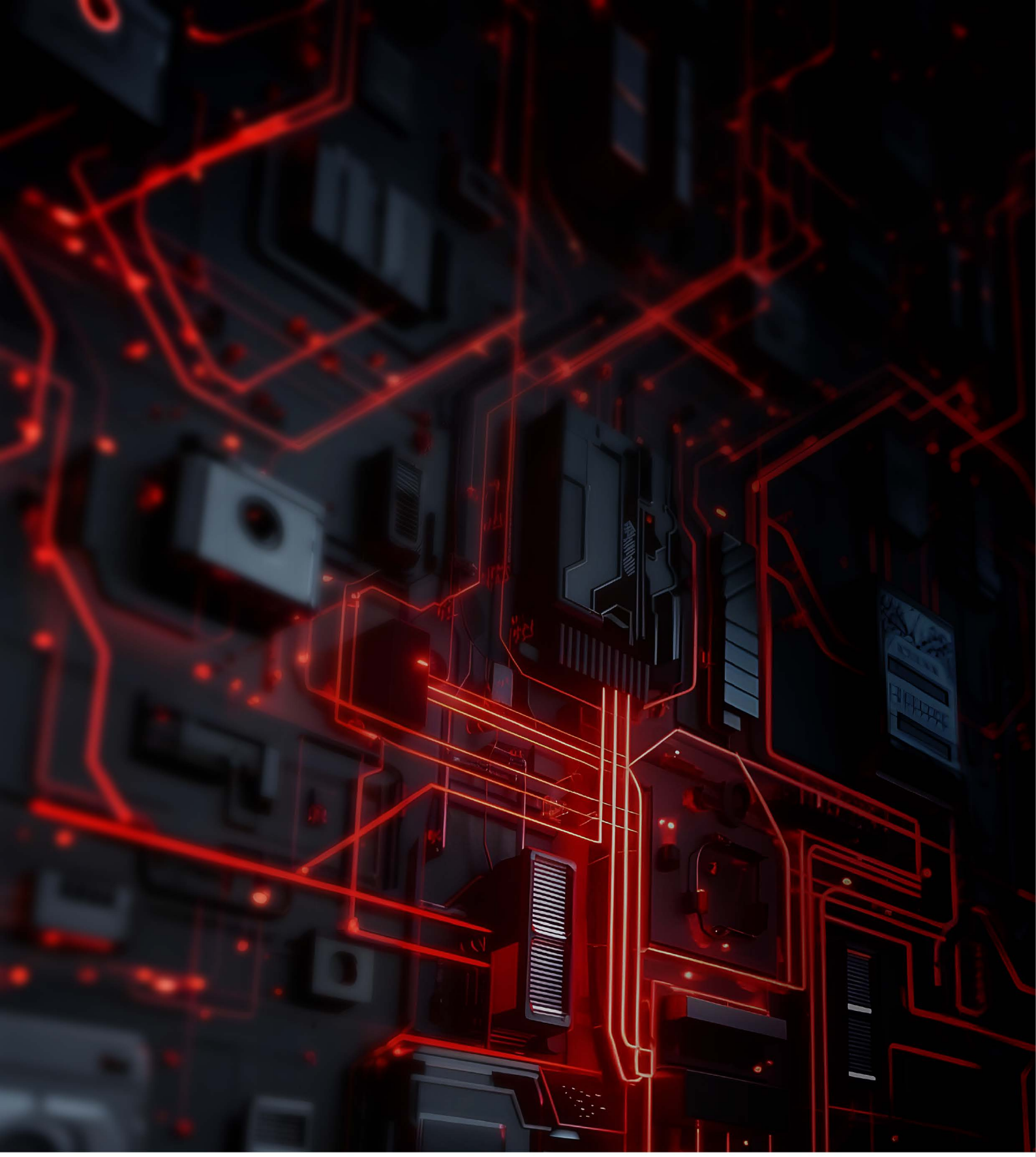


2. SK 쉴더스 MDR 서비스

랜섬웨어에 전문적으로 대응하기 위해서 SK 쉴더스의 MDR(Managed Detection and Response) 서비스[12]를 사용하는 것이 효과적인 방안이 될 수 있다. 최근 랜섬웨어 공격자들의 치밀한 전략과 고도화된 탐지 회피 기법으로 인해 기존의 방어 체계만으로는 위협에서 벗어나기 어려운 상황이다. 이를 해결하기 위해 SK 쉴더스는 실시간으로 네트워크를 모니터링하고 이상 징후를 감지하며 필요시 즉각적으로 대응할 수 있는 MDR 서비스를 제공하고 있다. 랜섬웨어 공격은 사전 예방이 무엇보다 가장 중요하지만, 피해가 발생했을 경우 신속한 조치를 통해 피해를 최소화하는 것 또한 매우 중요하다. 따라서 기업에서는 전담 조직의 신속하고 정확한 사고 조사와 분석을 토대로 맞춤형 보안 솔루션을 제공하는 SK 쉴더스의 MDR 서비스를 고려하는 것을 추천한다.



[12] MDR 서비스: 실시간 위협 감지와 대응을 통해 사이버 공격으로부터 조직을 보호하는 관리형 보안 서비스



안녕을 지키는 기술 | SK 쉴더스

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 EQST/SI솔루션사업그룹 & KARA(Korea Anti Ransomware Alliance)
제　작 : SK쉴더스 마케팅그룹