

2024.4Q

KARA 랜섬웨어 동향 보고서



KARA 랜섬웨어 동향 보고서

EQST Lab 팀 이호석, 정민수, 조효제, 이현아

- 랜섬웨어 트렌드 2
 - 1. 4 분기 TREND..... 2
 - 2. 4 분기 랜섬웨어 활동 통계..... 3
 - 3. 랜섬웨어 트렌드 5
 - ✓ 헬스케어 업체들을 타겟으로 하는 랜섬웨어 공격의 증가..... 5
 - ✓ RansomHub 그룹의 활발한 활동 5
 - ✓ Cleo 사의 제로데이를 악용한 Clop 랜섬웨어의 공격..... 6
 - ✓ Veeam사의 신규 취약점을 악용한 랜섬웨어 공격..... 6
 - 4. 신규 랜섬웨어 및 그룹 활동 7
- Akira Ransomware 그룹 상세 분석..... 9
 - 1. 개요 9
 - 2. Akira 랜섬웨어 공격 시나리오 11
 - 3. Akira 랜섬웨어 분석.....12
 - 4. 암호화 대상 파일 및 폴더 목록 16
 - 5. IoCs17
- 랜섬웨어 Mitigations..... 18
 - 1. Akira 랜섬웨어 대응방안 안내..... 18
 - 2. SK 쉐더스 MDR 서비스..... 19



랜섬웨어 트렌드

1. 4분기 TREND

TREND

- Clop : Cleo 사의 취약점(CVE-2024-50623, CVE-2024-55956)을 악용
- Akira : Veeam 사의 취약점(CVE-2024-40711)을 악용

THREAT

- 3분기 Top5 랜섬웨어 : RansomHub, Akira, Play, KillSec, FunkSec
- Akira 랜섬웨어 : C++/Rust 기반 Akira v1/v2, Megazord

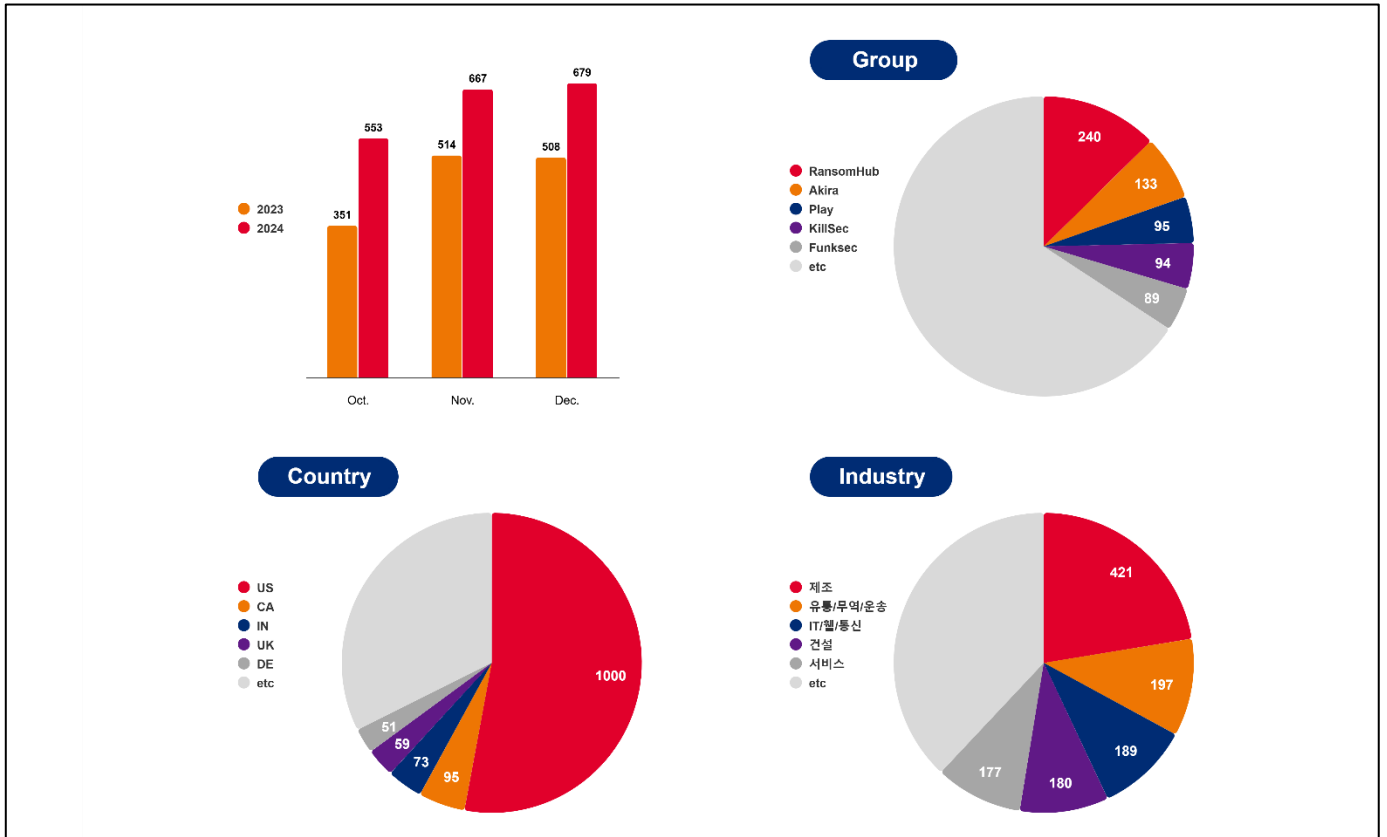
EXPLOIT

- 0-day : CVE-2024-50623, CVE-2024-55956, CVE-2024-40711
- 1-day : CVE-2020-3259, CVE-2023-20269

TARGET

- Cleo (Harmony, VLTrader, LexiCom) 취약점을 통한 초기 침투
- 전체 공격 중 제조 22%, 미국 53%

2. 4 분기 랜섬웨어 활동 통계



[그림 1] 랜섬웨어 그룹 활동

2024년 4분기 랜섬웨어 피해 사례 수는 1,899건으로 2023년 동기 대비 약 38% 증가한 수치를 보이고 있으며, 2024년 3분기 대비 44% 증가한 수치를 보이고 있다. 2024년 3분기에 48건에 그쳤던 Akira 그룹의 활동이 4분기 들어 133건으로 대폭 증가했으며, RansomHub 그룹도 195건에서 240건으로 증가했다. 이 외에도 신규 랜섬웨어 그룹인 FunkSec, Bashe, SafePay 등의 수치가 더해져 4분기 수치가 급등한 것으로 확인된다. 신규 랜섬웨어 그룹의 활동이 확산되는 반면, 악명 높은 랜섬웨어 그룹인 LockBit의 영향력은 갈수록 줄어들고 있다. 대표적인 요인으로 LockBit 랜섬웨어를 개발한 것으로 의심되는 인물들이 체포되고 있으며 인프라가 지속적으로 압수당하고 있어 데이터 유출 건수가 12건에 그친 것으로 보인다.

RansomHub 그룹은 4분기에만 240건의 데이터를 유출하며 가장 많은 활동을 기록했는데, 특히 멕시코 정부와 해외 유명 축구 구단을 공격했으며, 국내 제조 업체를 공격하여 60GB 이상의 내부 데이터를 공개해 영향력을 과시하기도 했다. 주요 전략으로 EDR¹을 무력화 시키는 BYOVD² 전략을 통해 랜섬웨어 공격을 수행하기도 하며, 취약점을 통한 초기 침투와 RMM 도구³ 악용 등의 다양한 전략을 펼치며 활발한 활동을 이어나가고 있다.

¹ EDR(Endpoint Detection and Response) : 엔드포인트에서 발생하는 의심스러운 활동을 탐지하고 대응하는 보안 시스템

² BYOVD(Bring Your Own Vulnerable Driver) : 합법적인 서명이 되어있어 정상 드라이버로 인식되나, 실제로는 취약한 드라이버를 악용하는 공격 기법

³ RMM(Remote Monitoring and Management) 도구 : 원격지에서 시스템을 관리하거나 모니터링 하는 정상적인 도구

Akira 랜섬웨어 그룹도 4 분기에 133 건이라는 다수의 유출 데이터를 게시하며 꾸준한 활동을 이어오고 있다. Akira 랜섬웨어가 10 월에 Veeam Backup & Replication⁴의 취약점인 CVE-2024-40711 를 통해 전파된 정황이 확인되었다. 해당 취약점은 프로그램이 신뢰할 수 없는 데이터를 읽는 과정에서 발생하며, Akira 랜섬웨어 공격자는 이를 통해 랜섬웨어를 실행시킨 것으로 보인다.

Play 랜섬웨어 그룹 또한 4 분기에 95 건의 피해자를 게시하며 지속해서 건재함을 보여주고 있다. 주목할 만한 사항은, 북한 정찰총국 산하 APT 그룹인 Andariel 이 Play 그룹과의 협력을 의심해 볼 만한 활동이 관찰됐다는 것이다. Andariel 이 Play 그룹의 계열사로 활동하는 것이라는 추측도 존재하지만, Play 그룹은 RaaS⁵를 제공하지 않는 것으로 알려져 있어 Andariel 은 단순히 IAB⁶ 역할로 협업을 했을 것으로 보인다.

KillSec 그룹도 Play 그룹과 비슷한 수치인 94 건의 유출 데이터를 게시해 활발한 활동을 보이고 있다. 이들은 국내의 한 부동산 데이터 플랫폼에 대한 공격을 주장하며 유출 데이터를 게시했는데, 해당 데이터에는 각종 개인정보를 포함한 여러 민감한 데이터가 포함되어 있어 2 차 피해가 우려되는 상황이 발생했다.

FunckSec 그룹은 12 월에 발견된 신규 랜섬웨어 그룹으로, 도구 및 피싱 템플릿을 제작하는 것과 같은 특정 작업에 자체 개발한 WormGPT 라는 생성형 AI 를 활용하기도 한다고 밝혔다. 12 월 한 달간 높은 수치인 89 건의 유출 데이터 게시를 기록했으며, 이 중에는 국내의 한 수제품 유통 업체를 공격 후 게시한 유출 데이터가 포함되어 있다.

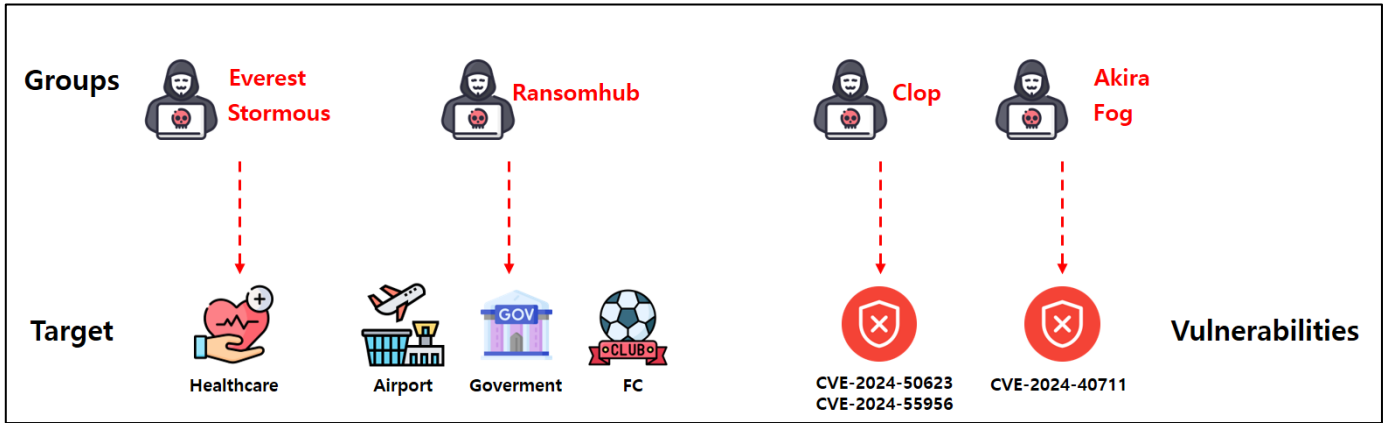
⁴ Veeam Backup & Replicatioin : 데이터를 백업하고 모니터링 하는 솔루션

⁵ RaaS(Ransomware as a Service) : 서비스형 랜섬웨어의 약어로, 금전을 대가로 랜섬웨어를 서비스 형태로 제공하는 수익 모델

⁶ IAB(Initial Access Broker) : 피해자의 시스템에 초기 침투 후 해당 액세스 권한을 판매하는 브로커



3. 랜섬웨어 트렌드



[그림 2] 2024년 4분기 랜섬웨어 트렌드

✓ 헬스케어 업체들을 타깃으로 하는 랜섬웨어 공격의 증가

델러스와 포트워스 지역에서 홈 헬스 및 호스피스 케어 서비스를 제공하는 텍사스의 주요 의료 서비스 제공업체인 Aspen Healthcare Services는 2020년부터 활동해온 Everest 랜섬웨어 그룹의 공격을 받아 내부 데이터가 유출되어 심각한 피해를 입었다. 공격자들은 1,500건 이상의 의료 기록과 개인 정보를 탈취한 뒤, 데이터를 공개하거나 판매하겠다고 협박하며 11월 9일까지를 기한으로 제시했다. Aspen Healthcare는 10월 22일 공격이 시도된 후, 10월 23일 이를 발견하고 즉시 보안 조치를 취했으며, 주 및 연방 당국에 신고하는 등 긴급 대응에 나섰다. 조사 결과, 일부 IT 네트워크에 무단 접근이 있었고, 유출된 데이터에는 환자의 이름, 생년월일, 주소, 보험 ID, 건강 기록, 사회보장번호(SSN) 등 민감한 정보가 포함된 것으로 확인되었다. 이에 따라 11월 18일, Aspen Healthcare는 피해자들에게 데이터 유출 사실을 알리는 공식 통지서를 발송했다.

미국 펜실베이니아와 웨스트버지니아 지역에서 전문 간호 및 케어 서비스를 제공하는 Guardian Healthcare도 랜섬웨어 공격 피해를 입었다. 공격을 수행한 Stormous 랜섬웨어 그룹은 기업 시스템에 침투해 약 3GB의 민감한 데이터를 탈취하고 협상을 시도했으나, 최종적으로 협상은 이루어지지 않은 것으로 확인됐다.

✓ RansomHub 그룹의 활발한 활동

2024년 높은 활동성을 보여온 RansomHub 그룹은 멕시코 정부 기관 및 이탈리아 축구 클럽 등을 공격하며 4분기에도 활발히 활동했다. 이들은 이탈리아 축구 클럽 볼로냐 FC의 내부 시스템에 침투해 선수 계약 정보, 직원 정보, 경기 인프라 및 개인 정보 등이 포함된 200GB 이상의 민감한 데이터를 탈취했다고 주장했다. 이후 볼로냐 FC 측은 공격을 인정하며, 도난된 데이터의 소지 및 유포 금지를 요청하는 공식 입장문을 발표했다.

멕시코 정부 역시 RansomHub의 공격 대상이 되었다. 이들은 멕시코 행정부 법무 사무실을 표적으로 삼아 313GB의 데이터를 탈취했으며, 탈취된 정보에는 계약서, 보험 및 재무 관련 문서가 포함된 것으로 알려졌다. RansomHub 그룹은 자신들의 DLS⁷에 침해 사실을 공개하고 10일간 협상 기간을 부여했으나, 이후 협상 진행 여부는 확인되지 않았다.

이외에도, 멕시코 공항 운영사 Grupo Aeroportuario del Centro Norte에서 3TB의 데이터를 탈취했다고 주장하는 등

⁷ DLS (Dedicated Leaks Sites) : 공격자들이 운영하는 랜섬웨어 PR 및 탈취 데이터 공유 사이트

지속적으로 침해 사실을 공개하며 활발히 활동하고 있다.

✓ Cleo사의 제로데이를 악용한 Clop 랜섬웨어의 공격

최근 Clop 랜섬웨어 그룹이 Cleo 사의 관리형 파일 전송 솔루션에서 발견된 제로데이 취약점을 악용해 공격한 사례가 발견되었다. Clop 랜섬웨어 그룹은 Cleo Harmony, VLTrader, LexiCom 등 Cleo의 파일 전송 솔루션을 대상으로 CVE-2024-50623, CVE-2024-55956 취약점을 악용해 기업 네트워크에 침투하고, 민감한 데이터를 탈취했다. Cleo사는 10월 CVE-2024-50623 취약점을 패치한 버전 5.8.0.21을 출시했으나, 완전한 해결이 되지 않아 추가 패치인 5.8.0.24를 배포했다.

처음에는 다른 랜섬웨어 그룹의 소행으로 추정됐으나, 분석 결과 Clop 랜섬웨어 그룹이 공격을 수행한 것으로 확인됐다. 이번 공격에서는 단순한 파일 쓰기 취약점을 넘어, 리버스 셸⁸을 통한 원격 명령 실행, 내부 이동, 오버패스 더 해시⁹ 기법 등 복합적인 공격 체인이 사용됐다. 특히 새롭게 발견된 CVE-2024-55956 취약점은 Cleo의 "/Synchronization" 엔드포인트에서 발생하며, 이 취약점을 통해 Java 기반 Cleopatra 백도어를 배포한 정황 또한 확인됐다.

CISA는 Cleo 취약점이 랜섬웨어 공격에 악용되고 있음을 확인하고 이를 KEV¹⁰ 목록에 추가했으며, 연방 민간 기관 및 Cleo MFT 솔루션 사용자에게 1월 3일까지 패치 적용을 권고했다. 또한, CyberPanel 등 다른 주요 소프트웨어 취약점이 공격 대상이 되고 있는 점을 고려해, 패치 적용 외에도 Autorun 기능 비활성화, 방화벽 설정, IP 허용 리스트 적용 등의 추가적인 보안 대책을 마련하고, PowerShell 실행 등 의심스러운 활동을 지속적으로 모니터링할 것을 권고했다.

✓ Veeam사의 신규 취약점을 악용한 랜섬웨어 공격

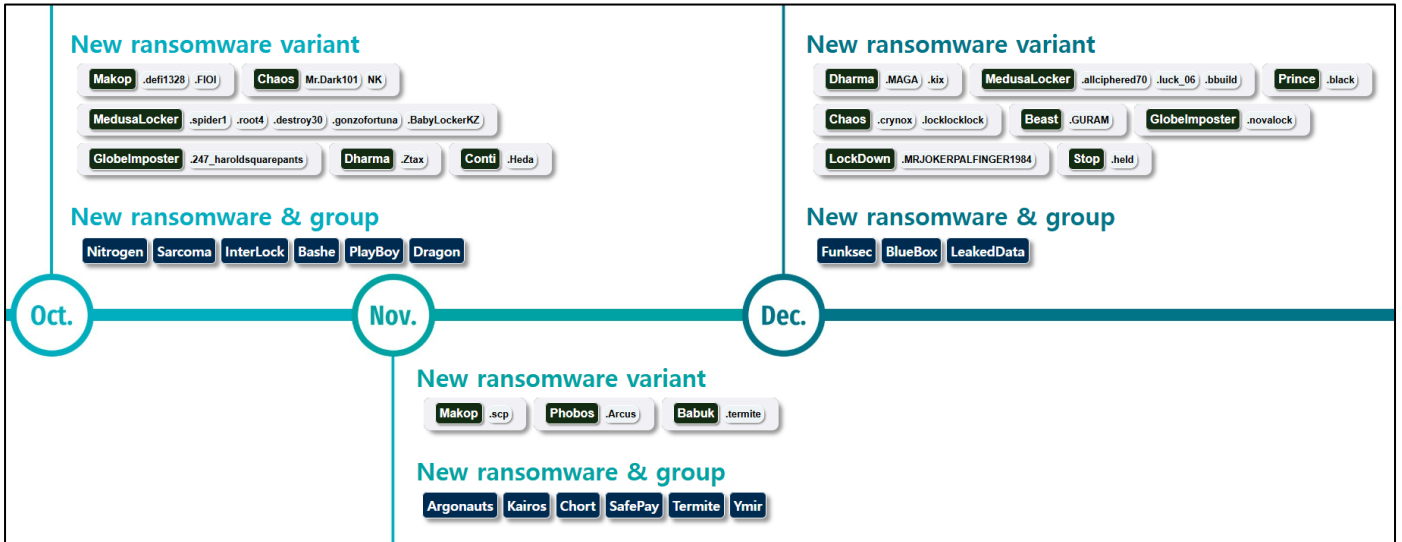
2024년 10월 이후 Veeam 제품에서 치명적인 취약점들이 발견되었고, 이를 기반으로 한 랜섬웨어 공격이 성행하고 있다. CVE-2024-40711 취약점은 CVSS 점수 9.8로 Veeam Backup & Replication 및 Veeam Agent for Linux, Veeam ONE 등의 제품군에서 취약점이 발생했다. Veeam 제품에서 발생한 취약점을 악용할 경우 인증없이 원격으로 코드를 실행할 수 있어 Akira와 Fog 랜섬웨어 그룹이 해당 취약점을 통해 공격을 수행했으며, 다중 인증이 적용되지 않은 취약한 VPN을 통해 침투한 뒤 취약점을 악용해 로컬 관리자 계정을 생성하고 데이터 탈취 및 암호화를 수행했다.

⁸ 리버스 셸 (Reverse Shell) : 피해 시스템이 공격자의 서버로 연결을 생성해 명령을 수행하는 셸

⁹ 오버패스 더 해시 (Overpass-the-Hash) : 해시된 패스워드를 직접 사용해 Kerberos 또는 NTLM 인증을 우회하는 기법

¹⁰ KEV (Known Exploited Vulnerabilities) : 실제 공격에 악용되고 있는 취약점 목록

4. 신규 랜섬웨어 및 그룹 활동



[그림 3] 신규/변종 랜섬웨어

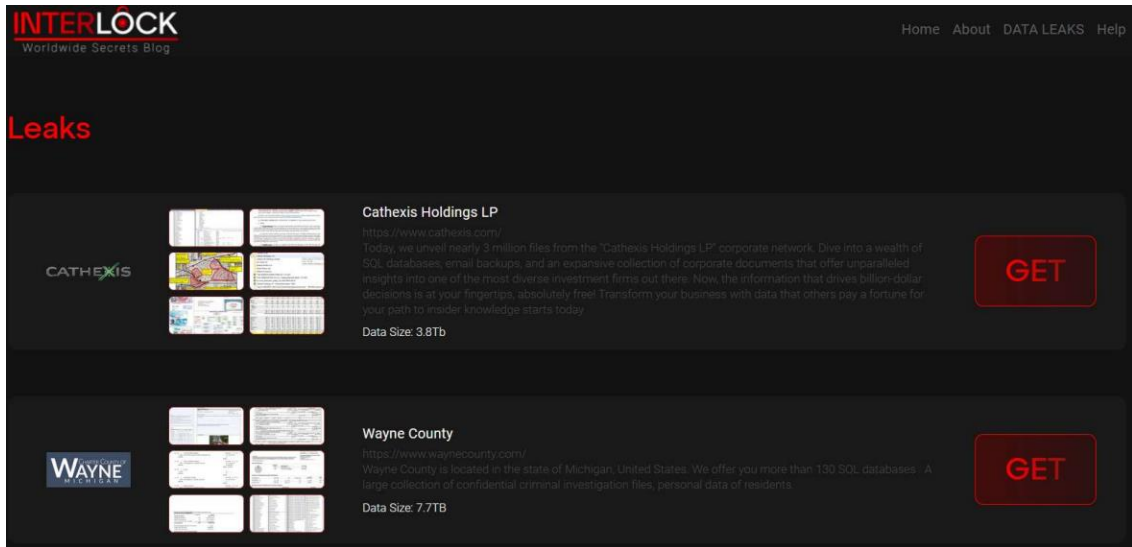
4분기에는 새롭게 리브랜딩된 랜섬웨어 그룹과 신규 랜섬웨어 그룹이 다수 등장했다. 특히, 출범과 동시에 대규모 피해 사례를 공개한 그룹이 증가하는 경향이 나타났다. Sarcoma 랜섬웨어 그룹은 10월에 등장해 한 달 만에 40명 이상의 피해자를 공개했으며, 11월에 활동을 시작한 SafePay 랜섬웨어는 등장과 동시에 40개 이상의 피해 기업을 공개했다. InterLock 랜섬웨어 그룹은 12월 한 달 동안 85개 이상의 피해 사례를 보고하며, 기업들의 피해 규모가 더욱 확대되었다. 8월에 활동을 중단한 APT73 그룹은 Bashe라는 이름으로 리브랜딩해 복귀했으며 이와 함께 20건의 공격 사례를 개시하며 활동을 재개했다. 이외에도 다양한 랜섬웨어 그룹들이 등장했으며 주요 랜섬웨어 그룹의 설명은 다음과 같다.

- Sarcoma

10월 등장한 Sarcoma는 12월까지 총 56개의 기업을 공격해 데이터를 탈취했음을 공개했다. 이들은 미국, 캐나다, 호주 스페인 등의 국가에 소속된 기업들을 공격했으며 데이터 탈취에 성공한 기업들을 대상으로 보안성이 낮은 회사라는 도발적인 문구와 함께 DLS에 샘플데이터를 공개했으며, 협상을 하지 않을 경우 데이터를 다크웹에 판매하는 이중 갈취 방식을 사용했다.

- InterLock

10월 9일 새롭게 발견된 랜섬웨어 그룹으로, 12월까지 활발히 활동하며 공격을 확대하고 있다. 이들은 피싱 웹사이트를 이용해 초기 침투를 시도하며, 내부 시스템에 접근한 후 정보 탈취형 악성코드를 사용해 시스템 정보를 수집한다. 이후 Putty, RDP 등의 정상적인 도구를 악용해 내부 네트워크로 확산한다. 내부 장악 후 InterLock 랜섬웨어를 실행하며, 시스템의 파일들이 암호화되고 .interlock 확장자가 추가된다. 이 후 DLS에 피해 기업 목록을 갱신하고 4일간 협상 기간을 부여한다. 협상이 결렬될 경우 복호화 키를 파기하고 데이터를 판매하거나 공개한다. 이 그룹은 윈도우뿐만 아니라 리눅스 환경도 공격이 가능해 더 많은 기업과 시스템을 표적으로 삼아 공격을 확장하고 있다.



[그림 4] Interlock 랜섬웨어 DLS

- SafePay

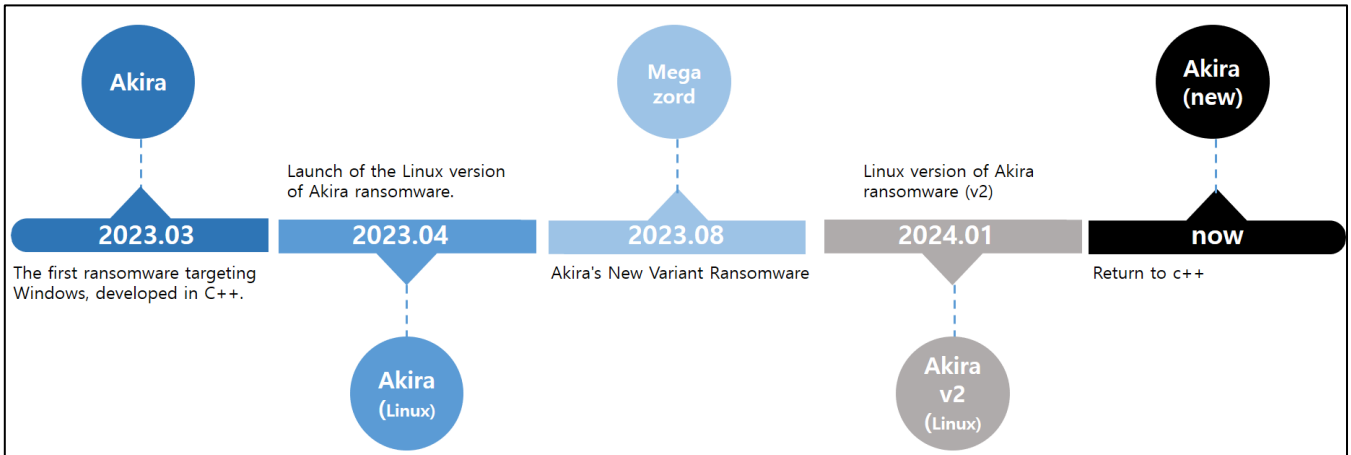
지난 11월 등장한 SafePay 랜섬웨어 그룹은 유출된 LockBit 소스코드를 기반으로 한 변종을 통해 미국, 영국, 캐나다, 브라질 등 여러 국가의 중소기업을 대상으로 공격을 감행하고 있다. 이들은 원격 데스크톱 프로토콜을 이용해 내부 시스템에 침투한 후, 파워셸 스크립트와 윈도우 명령줄을 활용해 공격을 실행한다. 최종적으로 파일들을 암호화하고 확장자를 ".safepay"로 변경한 뒤, 협박 메시지가 담긴 랜섬노트를 남겨 피해자들에게 금전을 요구한다.

- FunkSec

FunkSec 랜섬웨어는 지난 12월 등장 후 DLS에 85개 이상의 피해 기업을 공개하며 활동을 본격화했다. 다만, 이들이 공개한 데이터 중 일부는 이전 핵티비즘 관련 위협에서 유출된 것으로 확인되어, 모든 피해 기업이 실제로 침해를 당한 것으로 단정하기는 어렵다. 이 그룹이 사용하는 악성코드는 Rust 기반으로 개발되었으며, 감염된 시스템의 파일을 ".funksec" 확장자로 암호화하고, 랜섬노트(README-[A-z0-9]{10}.md)를 생성한다. 또한, RaaS(Ransomware-as-a-Service) 방식으로 운영되며, 랜섬웨어 외에도 DDoS 도구, HVNC 클라이언트, 계정 탈취 도구 등의 악성 서비스를 제공한다.

Akira Ransomware 그룹 상세 분석

1. 개요



[그림 5] Akira 랜섬웨어 진화 과정

Akira 랜섬웨어는 RaaS(Ransomware-as-a-Service) 형태로 운영되며, 랜섬웨어 및 DLS 플랫폼의 접근 권한을 판매하고 범죄 수익 일부를 배분하는 방식으로 활동한다. 윈도우 환경에서 동작하는 랜섬웨어가 발견된 이후, 리눅스 환경을 대상으로 한 변종도 확인되었으며, 현재는 운영체제와 관계없이 공격을 수행하고 있다. 주로 북미와 유럽의 기업을 표적으로 삼으며, DLS 사이트에 공개된 피해 기업만 240 곳에 달한다. 협상 후 비공개 처리된 사례나 아직 공개되지 않은 기업을 고려하면 실제 피해 규모는 더 클 것으로 추정된다.



[그림 6] Akira 랜섬웨어 DLS

이들은 단순한 파일 암호화 협박뿐만 아니라, 탈취한 데이터를 이용한 이중 갈취(Double Extortion) 전략을 활용한다. 암호화 대상 및 문자열 암호화 방식이 Conti 랜섬웨어와 유사하지만, Conti 의 소스코드 유출 이후 이를 기반으로 한 랜섬웨어가 다수 등장했기 때문에 직접적인 연관성을 단정하기는 어렵다. 그러나 블록체인 거래 내역 추적 결과, Akira 랜섬웨어 그룹이 Conti 그룹에 암호화폐를 전송한 정황이 확인되었으며, 이를 통해 Conti 그룹 일부가 Akira 에 합류했거나 양측이 공격을 공유하고 있을 가능성이 있다.

Akira 랜섬웨어는 2023 년 3 월 처음 발견되었으며, C++로 작성되어 윈도우 환경에서 동작하도록 제작되었다. 이후 4 월에는 리눅스를 대상으로 한 변종이 등장했고, 2024 년 초에는 Rust 기반의 두 번째 버전이 공격에 사용되었다. 이후 다시 C++ 기반의 랜섬웨어가 제작되었으며, 현재까지 꾸준히 공격에 활용되고 있다.

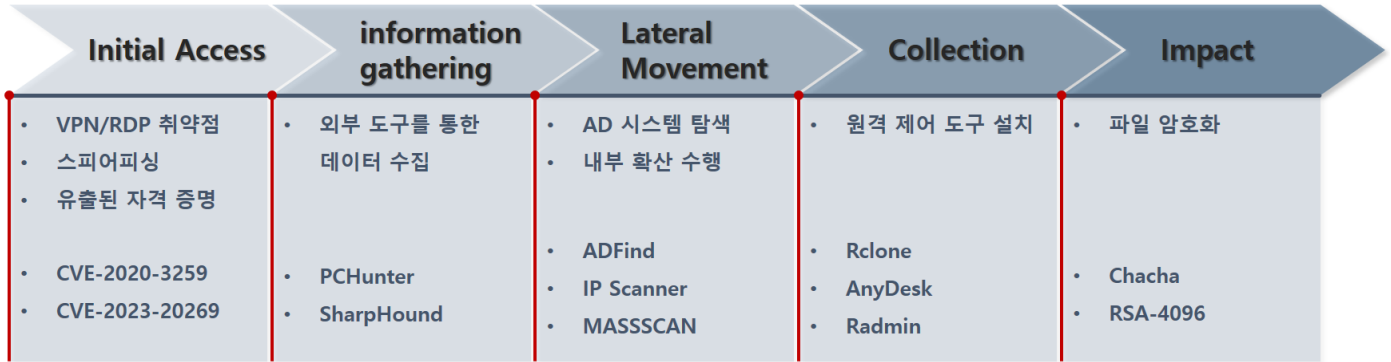
2023 년 8 월 발견된 Megazord 랜섬웨어는 Akira 랜섬웨어와 유사한 코드 및 동작 방식을 보이며, Rust 로 개발되었다는 공통점이 있다. 두 랜섬웨어는 암호화된 파일의 확장자나 랜섬노트 파일명은 다르지만, 초기 접근 방식과 코드 일부를 공유하고 있어 Akira 의 리브랜딩이거나 파생된 변종일 가능성이 보인다.

Akira 랜섬웨어의 데이터 유출 사이트는 일반적인 랜섬웨어 DLS 와 달리, 명령줄(Command Line) 기반 UI 를 제공하는 것이 특징이다. 주요 명령어로는 공격한 기업 목록과 유출 데이터를 다운로드할 수 있는 leaks, 홍보 및 공지사항을 기재하는 news, 협상을 위한 연락처를 제공하는 contact, 명령어 목록을 출력하는 help, 화면을 정리하는 clear 등이 있다.



[그림 7] 피해 기업 정보 및 다운로드 링크

2. Akira 랜섬웨어 공격 시나리오



[그림 8] Akira 랜섬웨어 공격 시나리오

Akira 그룹은 VPN, 스피어피싱, RDP 취약점, 유출된 자격증명 등을 이용해 공격 대상에 침투한다. 특히 Cisco, SonicWall, Fortinet 등의 VPN 소프트웨어를 주요 타겟으로 삼아 CVE-2020-3259, CVE-2023-20269 등의 취약점을 악용한다. 또한, 기존에 유출된 계정 중 다중 인증(MFA)이 적용되지 않은 계정을 통해 네트워크에 침투한 정황이 확인되었으며, 이는 다른 해킹 그룹과 협력했거나 초기 액세스 브로커로부터 계정을 구매했을 가능성을 시사한다.

최초 침투 이후, 공격자는 내부 장악을 위해 PCHunter, SharpHound 를 사용해 시스템 정보를 수집하고, AdFind 및 윈도우 명령어를 활용해 Active Directory(AD) 정보를 파악한다. 이후 IP Scanner, MASSCAN 을 이용해 내부 네트워크를 탐색하며 추가적인 확산 경로를 모색한다. 내부 시스템 정보가 수집되면 취약점을 악용하거나 새로운 도메인 컨트롤러를 등록하여 권한을 상승시키고, 악성 행위를 은폐하기 위해 PowerTool 을 사용해 안티바이러스를 종료한다.

랜섬웨어 실행 전, 공격자는 AnyDesk, Radmin 등 원격 제어 도구와 FileZilla, WinSCP 등의 파일 전송 도구를 설치해 정보를 탈취한다. 이후 랜섬웨어를 실행해 시스템 내 파일을 암호화한 후 공격을 종료한다. Akira 랜섬웨어 그룹은 소프트웨어 취약점뿐만 아니라 유출된 계정을 적극 활용하며, 침투 후에는 공개 도구를 악용해 내부 네트워크를 탐색하고 명령을 주고받는 등 고도화된 공격 기법을 사용하고 있다.

3. Akira 랜섬웨어 분석

- 암호화 문자열 복구

Akira 랜섬웨어는 Conti에서 사용했던 것과 동일한 문자열 암호화 로직을 사용한다. 악성 행위에 필요한 문자열은 암호화된 상태로 저장되며, 프로그램이 실행될 때 Main 함수보다 먼저 initterm에서 복호화된다. initterm의 테이블에는 여러 함수가 저장되어 있으며, 이 함수들은 순차적으로 실행된다. 이 테이블에는 암호화 대상 확장자, 암호화 제외 대상, 예외 폴더 정보, 그리고 악성 행위에 필요한 문자열을 복호화하는 함수들이 포함되어 있다. 프로그램이 실행되면 해당 함수들이 실행되면서 문자열을 복호화하고, 복호화된 문자열은 메모리에 저장된다. 또한, 일부 문자열은 암호화되지 않은 상태로 존재하며, 별도의 복호화 과정 없이 그대로 메모리에 복사된다.

```
memset(v11, 0, sizeof(v11));
wstrcpy_14003E600(v11, L"Trend Micro", 0xBuLL);
memset(v12, 0, sizeof(v12));
wstrcpy_14003E600(v12, L"ProgramData", 0xBuLL);
v1[0] = v2;
v1[1] = &vars0;
sub_14006FE60(&exclude_dir, v1);
`eh vector destructor iterator'(v2, 0x20uLL, 0xBuLL, unknown_libname_4);
return atexit(sub_1400CBBC0);
```

[그림 9] 암호화 되지 않은 문자열 로드

```
00
++v7;
while ( *&v50[2 * v7] );
wstrcpy_14003E600(v71, v50, v7);
v43[14] = 0;
qmemcpy(v44, "c0", 2);
v44[2] = 1;
v44[3] = 48;
v44[4] = 96;
v44[5] = 48;
v44[6] = 17;
memset(&v44[7], 48, 3);
for ( m = 0LL; m < 0xA; ++m )
    v44[m] = (24 * (48 - v44[m]) % 127 + 127) % 127;
memset(v72, 0, sizeof(v72)); // .pvm
```

[그림 10] 암호화된 문자열 복호화

- 로그 파일 생성

Akira 랜섬웨어는 실행 과정에서 로그 파일을 생성하는 특징이 있다. 이 파일에는 랜섬웨어가 설정한 스레드 개수, 파일 암호화 성공 여부 등 실행 중에 기록되는 정보가 저장된다. 로그 파일은 랜섬웨어가 실행된 폴더에 생성되며, 파일명 형식은 "Log-%d-%m-%Y-%H-%M-%S.txt"이다.

```
GetSystemTimeAsFileTime_0(&Time, hPrevInstance, lpCmdLine, nShowCmd);
v4 = localtime64(&Time);
strtime(Buffer, 0x50uLL, "Log-%d-%m-%Y-%H-%M-%S", v4);
v222 = 0LL;
v223 = 0LL;
v224 = 0LL;
v5 = -1LL;
do
    ++v5;
while ( Buffer[v5] );
sub_1400371E0(&v222, Buffer, v5);
sub_14004C6E0(v6, &v222);
```

[그림 11] 로그 파일 생성

```

2025-01-20 10:17:52.373 [file_logger] [info] Number of thread to folder parsers = 1
2025-01-20 10:17:52.373 [file_logger] [info] Number of thread to root folder parsers = 1
2025-01-20 10:17:52.373 [file_logger] [info] Number of threads to encrypt = 2
2025-01-20 10:17:52.373 [file_logger] [error] File handle not found! (C:\BOOTSECT.BAK.MEOW)
2025-01-20 10:17:52.373 [file_logger] [error] File handle not found! (C:\bootmgr)
2025-01-20 10:17:53.107 [file_logger] [error] Get file size failed! (C:\123\Log-05-02-2025-09-24-27.txt)
2025-01-20 10:17:53.123 [file_logger] [error] File handle not found! (C:\Program Files\7-Zip\7-zip.chm)
2025-01-20 10:17:53.123 [file_logger] [error] File handle not found! (C:\Program Files\7-Zip\7z.sfx)

```

[그림 12] 로그파일 내 악성 행위 기록

- 프로그램 실행 인자 파싱

프로그램 실행 시 전달된 인자를 파싱해 플래그 값을 설정하거나 암호화에 필요한 옵션을 지정한다. 인자는 총 다섯 개이며, 입력된 값에 따라 실행 환경이 아래와 같이 구성된다.

설정	설정 정보
-encryption_path, -p	암호화 대상 경로 지정
-share_file, -s	특정 네트워크 드라이브 암호화 지정
-encryption_percent, -n	파일 암호화 비율 지정
-localonly	로컬 드라이브만 암호화 수행
-exclude, -e	암호화 예외 대상 지정
-l	암호화 드라이브 정보를 로그파일에 기록

- 볼륨 새도우 복사본 삭제

파일을 암호화하기 전에, 랜섬웨어는 시스템 복구를 막기 위해 볼륨 새도우 복사본을 삭제한다. 함수가 실행되면 암호화된 PowerShell 문자열을 복호화한 후, 이를 실행하기 위해 COM 객체를 생성하고, 명령줄을 구성해 스크립트를 실행한다. 명령어가 실행된 후, 랜섬웨어는 OpenProcess를 사용해 명령 수행이 완료되길 대기하며, 명령이 완료되면 다음 악성 행위를 시작한다.

```

powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"

```

[Volume Shadow Copy 삭제 명령어]

```

qmemcpy(v6, "c:9{o!Zrc", 10);
v6[10] = 17;
v6[11] = 25;
v6[12] = 50;
for ( i = 0LL; i < 0x4C; ++i )
    enc_str[i] = (42 * (50 - enc_str[i]) % 127 + 127) % 127;
hPowershell = RunPowershell_140078890(enc_str);// Get-WmiObject Win32_Shadowcopy | Remove-WmiObject
if ( hPowershell )
{
    // powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"
    v2 = OpenProcess(0x100000u, 0, hPowershell);
    v3 = v2;
    if ( v2 )
    {
        WaitForSingleObject(v2, 0x3A98u);
        CloseHandle(v3);
    }
}
CoUninitialize();

```

[그림 13] Powershell 스크립트 실행

- 공격자의 공개키 로드

Akira 랜섬웨어는 파일 암호화에 대칭키 암호화 방식을 사용하지만, 암호화에 사용된 대칭키는 공격자의 공개키로 다시 암호화해 저장한다. 랜섬웨어는 악성 행위를 수행하기 전에, 파일에 포함된 공격자의 공개키를 메모리에 로드하고, 파일 암호화가 완료된 후 해당 대칭키를 공개키로 암호화한다.

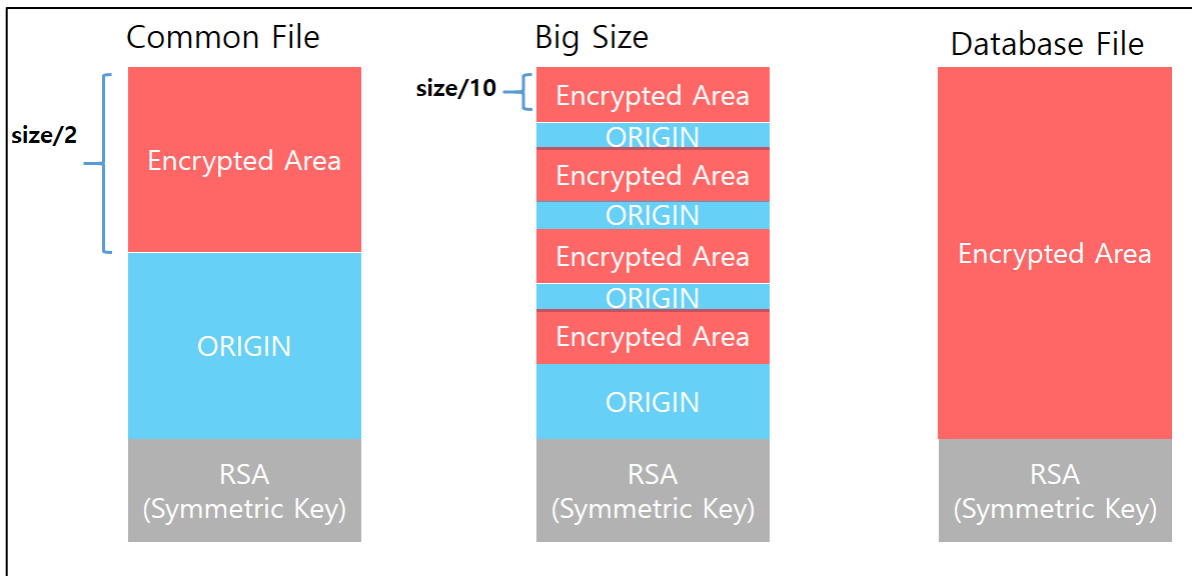
```

30 82 02 0A 02 82 02 01 00 F4 86 C1 AB 44 5F AE 0.....D_
67 A5 4B 9E 56 AB 48 EF FB 83 08 93 A7 87 AB DF g.K.V.H.....
F0 89 27 75 23 76 CE 22 D3 7A 9C 37 75 3E AF 24 ...#v...7u>.$
F9 F2 76 E2 A7 2A 1E A0 6C 80 29 47 33 C3 CD 88 ...*.l.)G3...
A8 40 E9 C6 ED 25 F2 10 63 B9 68 FF F2 E3 59 09 ...@...%...h....
34 1F 42 FF 11 2D B4 24 36 33 87 BF EB AA 2A 58 4.B.-.$63....X
13 E9 F3 7F CF AB 62 D4 0B 89 C0 A3 45 25 2C 93 ...x.b....E%,
6C 03 19 41 79 D4 D0 2A D1 F1 F8 AD A4 D5 31 3B l..Ay...*....;
50 73 2C 8E 61 0F 2F C5 41 4C 0E 0B 53 E2 78 A1 Ps,a./..L.S...
03 0F 27 B5 B4 92 5F 56 4B 53 1F 3D B0 94 BF 43 ...'..._VKS...C
7E B7 5B 41 C0 B2 AF 85 81 6F 08 73 5A B7 71 95 ~.[A.....o.sZ.q.
11 A0 21 DF 6F D8 68 47 14 98 6A AF B1 B9 9F FE .!....G..j....
D4 C9 65 83 A2 75 A7 E0 1B E0 E5 EF BE 9A EF 76 ..e..u.....
16 B2 63 FB BA 76 50 6B 80 2C 06 09 32 B3 AC 95 ..c..vPk,..2...
6D 70 4E 6C 97 7F B8 01 64 D8 8F 2B A0 13 F6 BE mpNl.....d_+....
15 28 18 02 E2 4B 3B FA 3C 71 A5 C1 85 C5 D5 49 .(.....<q....I
5A 93 D4 37 8B 44 E7 23 C7 18 6F D5 DE 27 C3 0C Z...D...o..'...
51 AF AE 67 14 12 92 BF C5 B1 60 04 90 B4 10 D8 Q..g...ü'...
96 4A 4A 81 6E 2F 0F EE 83 2C D9 D7 DA F9 BB 8C .JJ.n/...V....MJ..
17 15 05 5D 94 AA D1 10 56 BF 87 BF 4D 4A 98 88 ...]...oUXT'...!...
DB 8A B0 1E BF 6F 55 58 D0 A2 C1 ED 21 16 80 95 ...I.....
92 B0 FD 9A 49 F6 62 CE B7 B2 DB 5F CD F6 F9 EE ...N}.....s....
D1 00 20 81 4E 7D C7 53 86 04 FA 73 DB 5F F3 F5 ..Z.Y.L>....
A6 10 5A 17 C6 B3 4C 3E F7 B9 36 47 83 E5 77 8D )....sYgy.....
29 F4 05 77 E8 A4 73 59 67 79 0F 89 9B B4 97 F6 p.."...N.....'.
70 0D 17 22 E5 E2 D7 4E BD B7 10 E6 8C 24 27 E4 k...:T...gZ.8'ش.
6B 16 B1 96 3A 54 81 FE 8E 67 5A FC DA 9E 38 9B I.....}.....*%H.
49 B7 00 FF E0 2A 68 7D 03 EF D0 76 2A 25 48 0F @.....vD....A'..
40 AD 12 C4 14 95 76 44 BF A8 CF 48 41 27 EB F2 .I.....D.(a
09 C9 AA D3 E2 8D F8 E7 08 4E 05 B8 44 16 28 61 BB 8B ED 76 B0 97 7F 9D E2 41 E3 E1 BC 0B 0B B6 .....
2C C3 F2 92 CD 18 6A 78 EE 0B 41 57 A8 BA 75 7E ,.....jX...W.u~
A6 1B 45 1A 50 18 D0 32 5B 02 03 01 00 01 00 ..E.P...[.....
  
```

[그림 14] 공격자의 공개키

- 파일 암호화

감염된 시스템에서 파일 구조를 분석해 폴더명과 확장자를 확인한 뒤, 암호화 예외 대상 폴더와 파일은 암호화를 수행하지 않는다. 암호화 제외 대상이 아닌 경우, 확장자를 다시 확인해 암호화 여부를 결정한다. 디스크 이미지나 크기가 큰 파일은 암호화에 많은 시간이 걸리므로 부분 암호화를 수행한다. 반면, 특정 확장자를 가진 비대용량 파일은 크기와 관계없이 전체 암호화가 적용된다. 전체 암호화가 적용되는 파일은 주로 데이터베이스 관련 파일이며, 중요한 정보를 포함하고 있어 암호화 속도와 관계없이 전체 암호화를 진행한다. 암호화 대상 파일은 대칭키 암호화 알고리즘인 ChaCha를 사용해 암호화된다. 일반적인 파일은 절반만 암호화하며, 대용량 파일이나 디스크 이미지는 파일 크기의 1/10 크기의 블록을 설정한 후 네 개의 위치에서 암호화를 수행한다. "암호화 대상 파일 및 폴더 목록" 항목에 기재된 데이터베이스 확장자 파일은 크기에 상관없이 전체 암호화가 적용된다.



[그림 15] 암호화된 파일 구조

- 랜섬노트 생성

암호화가 완료된 폴더에는 토르 브라우저 설치 안내와 협상용 주소가 포함된 랜섬 노트 파일이 생성되며, 이를 통해 피해자에게 감염 사실을 알린다.

- 랜섬노트 파일명 : akira_readme.txt

```

Hi friends,

whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. we're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. we will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidentally corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - https://akira12iz6a7qgd3ayp316yub7xx2uep76idk3u2ko1lpj5z3z636bad.onion.
5. we're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:
1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.
2. Paste this link - https://akira1kzxzq2dsrzsrvbr2xgbbu2wgsxmryd4csgfameg52n7efvr2id.onion/d/0832201915-DMFCY
3. Use this code - 6696-DY-OGIA-UXQX - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.

```

[그림 16] Akira 랜섬 노트

4. 암호화 대상 파일 및 폴더 목록

tmp	winnt	Temp
thumb	\$Recycle.Bin	\$RECYCLE.BIN
System Volume Information	Boot	Windows
Trend Micro	ProgramData	

[암호화 예외 폴더 목록]

exe	Dll	Ink
sys	Msi	

[암호화 예외 파일 확장자]

.accdc	.accdb	.4dl	.4dd	.accft	.accdt	.accdr
.accde	.adp	.adf	.ade	.adb	.ask	.alf
.ora	.arc	.cdb	.cat	.bdf	.btr	.dacpac
.cpd	.cma	.ckp	.db	.daschema	.dadiagrams	.dad
.dbc	.db3	.db-wal	.db-shm	.dbv	.dbt	.dbs
.dbf	.dcx	.dct	.dcb	.dbx	.dqy	.dp1
.dlis	.ddl	.dxl	.dtsx	.dsn	.dsk	.epim
.edb	.ecx	.eco	.fic	.fdb	.fcd	.exb
.fol	.fmpl	.fmp12	.fmp	.fp7	.fp5	.fp4
.fp3	.grdb	.gdb	.frm	.fpt	.ib	.his
.hdb	.gwi	.itw	.itdb	.ihx	.idb	.kexi
.kdb	.jtx	.jet	.lwx	.lgc	.kexis	.kexic
.mas	.mar	.maq	.maf	.mpd	.mdf	.mdb
.mav	.myd	.mwb	.mud	.mrg	.ns2	.nrmlib
.nnt	.ndf	.nv	.nsf	.ns4	.ns3	.odb
.nyf	.nwdb	.nv2	.p96	.owc	.orx	.oqy
.pdm	.pdb	.pan	.p97	.rbf	.qvd	.qry
.pnz	.rpd	.rodx	.rod	.rctd	.scx	.sbf
.sas7bdat	.rsd	.sis	.sdf	.sdc	.sdb	.sqlite3
.sqlite	.sql	.spq	.tmd	.temx	.te	.sqlitedb
.udb	.trm	.trc	.tps	.vis	.v12	.usr
.udl	.wmdb	.wdb	.vvv	.vpd	.xmlff	.xld
.xdb	.wrk	.accdw	.abx	.abcddb	.hjt	.fm5
.db2	.adn	.lut	.kdb	.icr	.icg	.mdt
.mdn	.maw					

[암호화 대상 데이터 베이스 파일]

5. IoCs

SHA256
1ba1ccfacffbb6be9480380f5535a30d3eee1dd7787f3c649ebf8ea2a6a5de51
3720cafdd914d70d5fccf8d61593a66b5bdc400432e687c92e66eb3b5e8a9d9e
78d75669390e4177597faf9271ce3ad3a16a3652e145913dbfa9a5951972fcb0
ccda8247360a85b6c076527e438a995757b6cdf5530f38e125915d31291c00d5
0c662d28268514fab7129fd14d6e3e9d7df29261a861bcf8aab1f318bb8e7d0
f11b60b273e2606e91832edbb014ad229563f5c537ddab11dba80018c11364dd
9f873c29a38dd265decb6517a2a1f3b5d4f90ccd42eb61039086ea0b5e74827e
a5806174261004a0b8b5c0be808a77e5f25b867a4c522813035c2b0dc05d90a2
8c5412298e3c382a1ae3e84fd0ae62bc2d69703e9863ca5478cf3c513e6e232
58e685695afc3a85d2632777a2b54967dc53d6a6fa1b7e2c110b2023b561bfe9
120715377727531a56f32225e196b1536618d224662fa0b3ba6c52dba80f3b29
43b0ac119ff957bb209d86ec206ea1ec3c51dd87bebf7b4a649c7e6c7f3756e7
e10cae894e8873c72ae9e5f3590e2f78f6cc2dcfe01e1a5039c8b6532bfab5f8
aaa7799edfd86b52438a9e0d71f8069cbcbce1988036b95888fcdc553e729b7b9
87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d
442f5b7ae1a60d0cee31290b179b9201902e1f4875c606e6fe58b9ff4907c37e
d323d32cbd906c495a6e9fe7da01bf3e0eca407609a2693c7246346687d59f50
88da2b1cee373d5f11949c1ade22af0badf16591a871978a9e02f70480e547b2
74fbb7885ee486028fe2723f95911474b771f361b2b40ddb77c46f252059c696
1ec34305e593c27bb95d538d45b6a17433e71fa1c1877ce78bf2dbda6839f218
d07b379369e9faea0fed406b9b37652b2fc6453044ab17c1e2189cf61640ab90
74fbb7885ee486028fe2723f95911474b771f361b2b40ddb77c46f252059c696
a6d68214bf78c925b6fe6ab277589bc28c338e7253625925a674f380f3a52102
2d931f6867e7049b450c8ab36e1f8e6a51f0ee95fc2253d0759e3e3b118fe1d1






■ 랜섬웨어 Mitigations

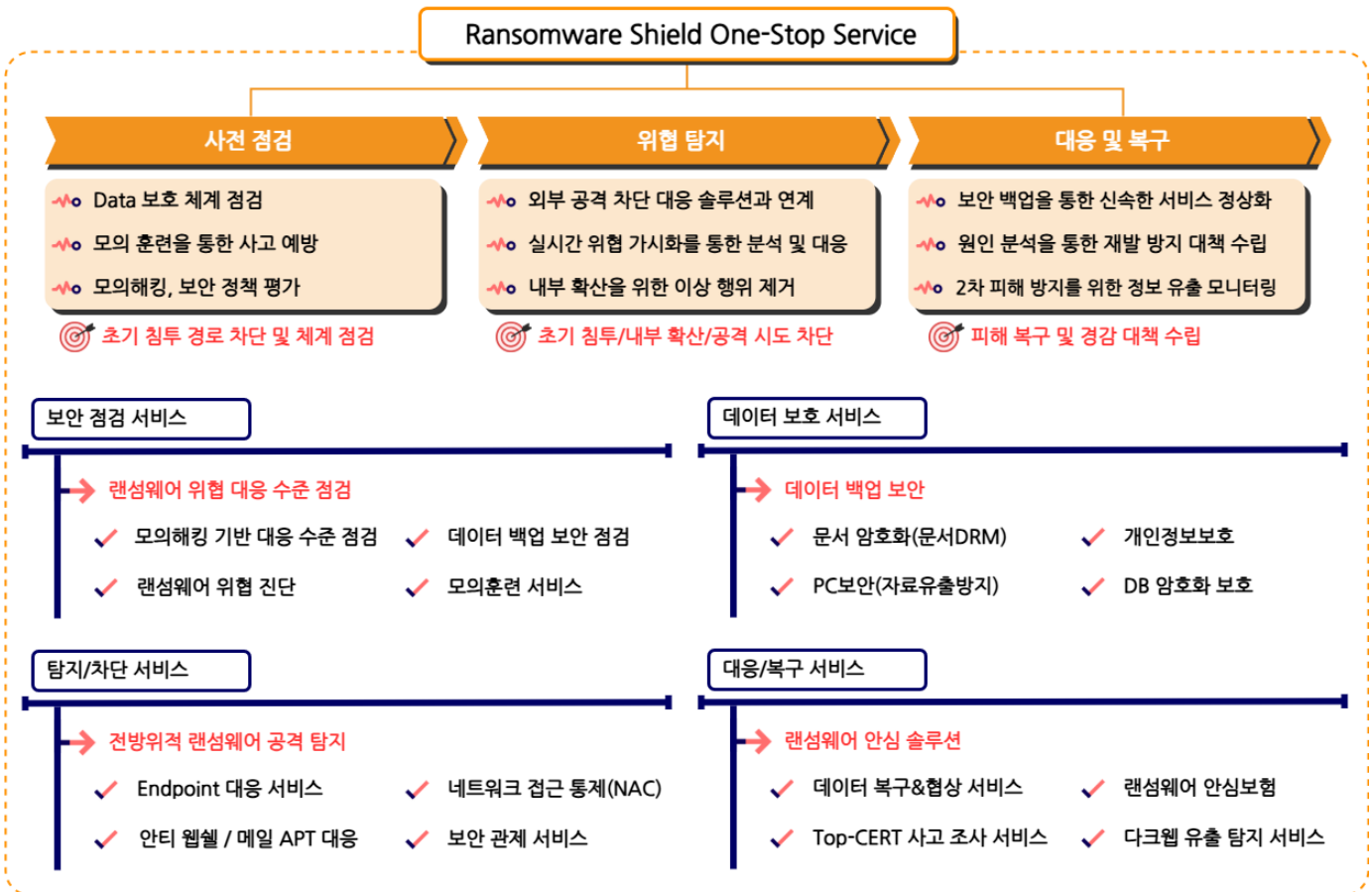
1. Akira 랜섬웨어 대응방안 안내

Akira 랜섬웨어는 피싱과 다중 인증이 적용되지 않은 VPN 취약점을 악용해 초기 침투를 수행하며, 침투 이후 공개된 정보 수집 도구와 원격 제어 도구를 활용해 내부로 확산한다. 내부 시스템이 장악되면 데이터 탈취 후 협상 기간 종료 시 DLS에 공개하므로, 사전 대응이 필수적이다. 이에 따라 외부 접점 보안 패치 적용, VPN의 다중 인증 활성화, 공개된 침해 도구에 대한 지속적 모니터링 등 선제적인 보안 조치를 시행해야 한다.

4Q Key Point

	Cisco	CVE-2020-3259	(Firepower Threat Defense 6.4.0~6.5.0)
	Cisco	CVE-2023-20269	(Adaptive Security Appliance 6.2.3 ~ 9.19.1.18)
	Veeam	CVE-2024-40711	(Backup & Replication 12.0.0.1420 ~ 12.2.0.334)
	Cleo	CVE-2024-55956	(Harmony, VLTrader, LexiCom, < v5.8.0.24)

✓



2. SK 실더스 MDR 서비스

랜섬웨어에 전문적으로 대응하기 위해서 SK 실더스의 MDR(Managed Detection and Response) 서비스¹¹를 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 실더스는 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 실더스의 MDR 서비스를 고려하는 것을 추천한다.

SK실더스 MDR Service 3가지 특징점

서비스 내용

01	EDR 전문가 운영 대행
Managed	<ul style="list-style-type: none"> • 24 X 7 관제 요청 접수 및 대응 • IoC 및 SK-Defined Rules 업데이트 • 정책 운영 및 예외처리 반영 • 이벤트 분석 & 대응 조치
02	SK실더스 상세 분석 서비스
Detection	<ul style="list-style-type: none"> • EDR/악성코드 전문가 분석 서비스 • EDR 기능을 통한 악성행위 추적 지원 • 상세분석을 통한 정/오탐 대응 • 주기적 위협헌팅 수행
03	침해사고 관점 통찰력
Response	<ul style="list-style-type: none"> • 국내 최다 침해사고 분석 및 조사 노하우 적용 • 침해 흔적 점검 진행 • 국내 침해지표(IoC) EDR 우선 적용



EDR 전문가 관제서비스

- ✓ EDR 전문 관제 서비스
 - 다수 고객사 서비스 제공 중
 - 다양한 산업군별 레퍼런스 고객 요청 대응 가능
- ✓ 사용자 만족도 향상
 - 숙련된 운영 전문가 신속한 대응



전문가 서비스 활용

- ✓ TOP-CERT 활용 가능
 - 24X7 긴급 로컬 투입
 - 국내 최다 사고분석 및 조사 대응
- ✓ SK실더스 보안 전문가 서비스 활용 가능
 - 분석 전문가 상시 대응
 - 보안 전문가 분석 서비스 (악성코드분석가 + CERT)
 - 전담 조직 체제로 정확/신속 서비스



국내 최대 보안 수준 대응

- ✓ 서비스 통한 정보유출 불가
 - 첨부파일 자사 망내 분석
 - 당사 전용 분석 환경 보유
- ✓ 사전 보안위협 대응역량 강화
 - 고객 보안 부서와 협업 위협 확산 선 차단 가능

¹¹ MDR 서비스: 실시간 위협 감지와 대응을 통해 사이버 공격으로부터 조직을 보호하는 관리형 보안 서비스





SK실더스(주) 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
<https://www.skshieldus.com>

발행인 : SK실더스 EQST/시솔루션사업그룹 & KARA(Korea Anti Ransomware Alliance)

제 작 : SK실더스 마케팅그룹

COPYRIGHT © 2025 SK SHIELDUS. ALL RIGHT RESERVED.

본 저작물은 SK실더스의 서면 동의 없이 사용될 수 없습니다.