2025년 2분기 랜섬웨어 공격 동향

Qilin, Play, DragonForce 랜섬웨어 분석

요약

1. Qilin Ransomware

의료, 언론 등 사회적 파급력이 큰 분야를 집중적으로 공격

공격 방식: Fortinet 제품의 치명적인 원격 코드 실행 취약점(CVE-2024-21762)을 악용하여 초기 침투를 시도.

2. Play Ransomware

피해자에게 직접 전화로 협박하는 등 과감한 방식을 사용하며 활발한 공격

공격 방식: Microsoft Windows의 제로데이 권한 상승 취약점(CVE-2025-29824)과 SimpleHelp 취약점을 동시에 활용하는 복합적인 공격

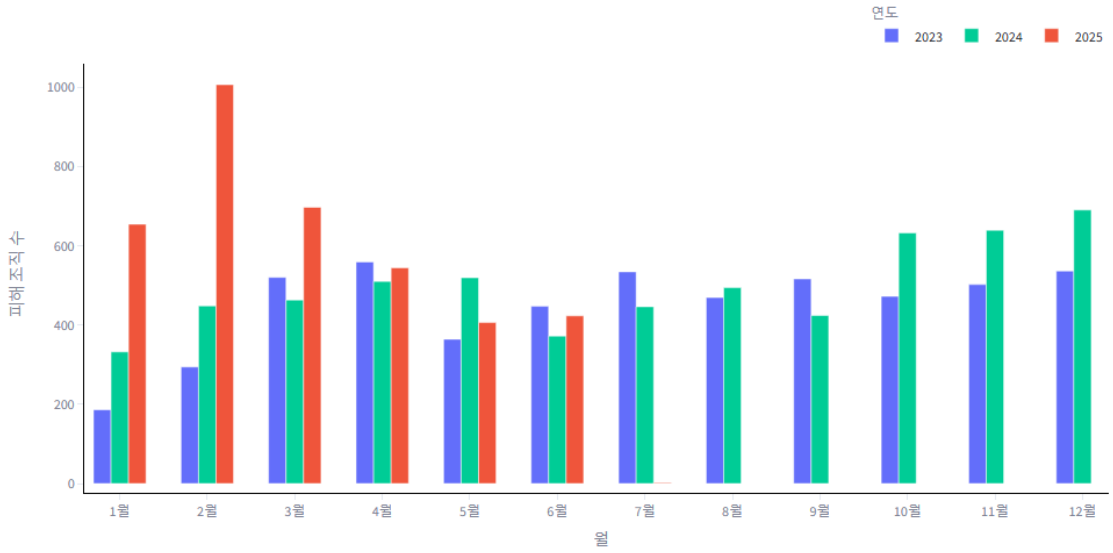
3. DragonForce Ransomware

Conti와 LockBit의 기술을 계승하고,
활동을 중단한 RansomHub의 제휴 조직을 흡수하며 세력 확장

공격 방식: Play 그룹과 마찬가지로 SimpleHelp 원격 관리 도구의 취약점 (CVE-2024-57726 등)을 악용해
MSP(관리 서비스 제공업체)와 그 고객사를 노리는 공급망 공격

목차

1. 개요



[그림 1] 랜섬웨어 피해자 수 월별 추이 (연도별 비교)

2025년 상반기(1분기, 2분기)에 확인된 랜섬웨어 피해 사례는 총 3,730건으로 집계되었다.

1분기는 2,357건, 2분기에는 1,373건이 발생하였으며,
2분기 피해 건수는 1분기 대비 약 42% 감소한 수치이다.

2. 2025년 2분기 랜섬웨어 공격 동향

	4월		5월		6월	
	공격 그룹	피해 조직 수	공격 그룹	피해 조직 수	공격 그룹	피해 조직 수
1	akira	72	qilin	53	qilin	75
2	safepay	51	play	40	akira	37
3	qilin	46	akira	34	incransom	26
4	play	36	safepay	34	dragonforce	24
5	lynx	24	devman	25	handala	23
6	nightspire	22	nightspire	17	play	21
7	killsec	20	lynx	15	lynx	19
8	dragonforce	20	stormous	13	worldleaks	18
9	incransom	19	incransom	13	global	16
10	babuk2	17	medusa	11	sarcoma	16

[그림 2] 월간 TOP 10 Ransomware

2025년 2분기(4월~6월) 랜섬웨어 그룹별 피해 현황을 분석한 결과,
‘akira’, ‘qilin’, ‘play’, ‘incransom’ 등이 상위권을 차지했다.

이 중 ‘akira’와 ‘play’는 1분기부터 활발한 활동을 이어왔으며,
2분기에는 특히 ‘Qilin’과 ‘DragonForce’ 랜섬웨어의 활동이 두드러졌다.

2.1 2분기 랜섬웨어 동향

2025년 2분기 랜섬웨어 동향을 살펴보면, 전 분기 대비 피해 조직 수가 감소하는 양상을 보였다.
물론 피해 조직이 피해 사실을 즉각 공개하지 않는 현실을 고려할 때,
이 수치가 랜섬웨어 위협의 실질적인 감소를 의미한다고 단정하기는 어렵다.
하지만 국제 사회의 공조 강화 등 일정 부분 긍정적인 흐름으로 해석할 수 있다.

이번 분기에는 유럽과 미국 등 주요국이 협력한 '엔드게임 작전(Operation Endgame)'을 통해
수백 개의 서버 및 도메인이 폐쇄되었으며,
여러 국가에서 랜섬웨어 관련 용의자들이 체포되는 등 국제적인 공조가 강화되었다.

공격 그룹 내부적으로는 주요 RaaS(서비스형 랜섬웨어) 그룹 간의 합병, 분열, 활동 중단과 같은
재편 움직임도 나타났다.
특히 DragonForce와 RansomHub 간의 충돌 사례에서 볼 수 있듯이,
조직 간 경쟁 또한 치열해지는 양상을 보였다.

[그림 3] 미국 신장 관리 서비스기업 'Davita' 출처: bleepingcomputer.com

미국 내 주요 신장 관리 서비스 제공업체인 DaVita는 4월 12일에 랜섬웨어 공격을 받아 네트워크 일부가 암호화되고 일부 운영에 차질이 생겼다고 밝혔다.

Yale New Haven Health(YNHHS)는 4월 초 사이버 공격으로 550만 명에 달하는 환자의 개인 데이터가 유출되었다.

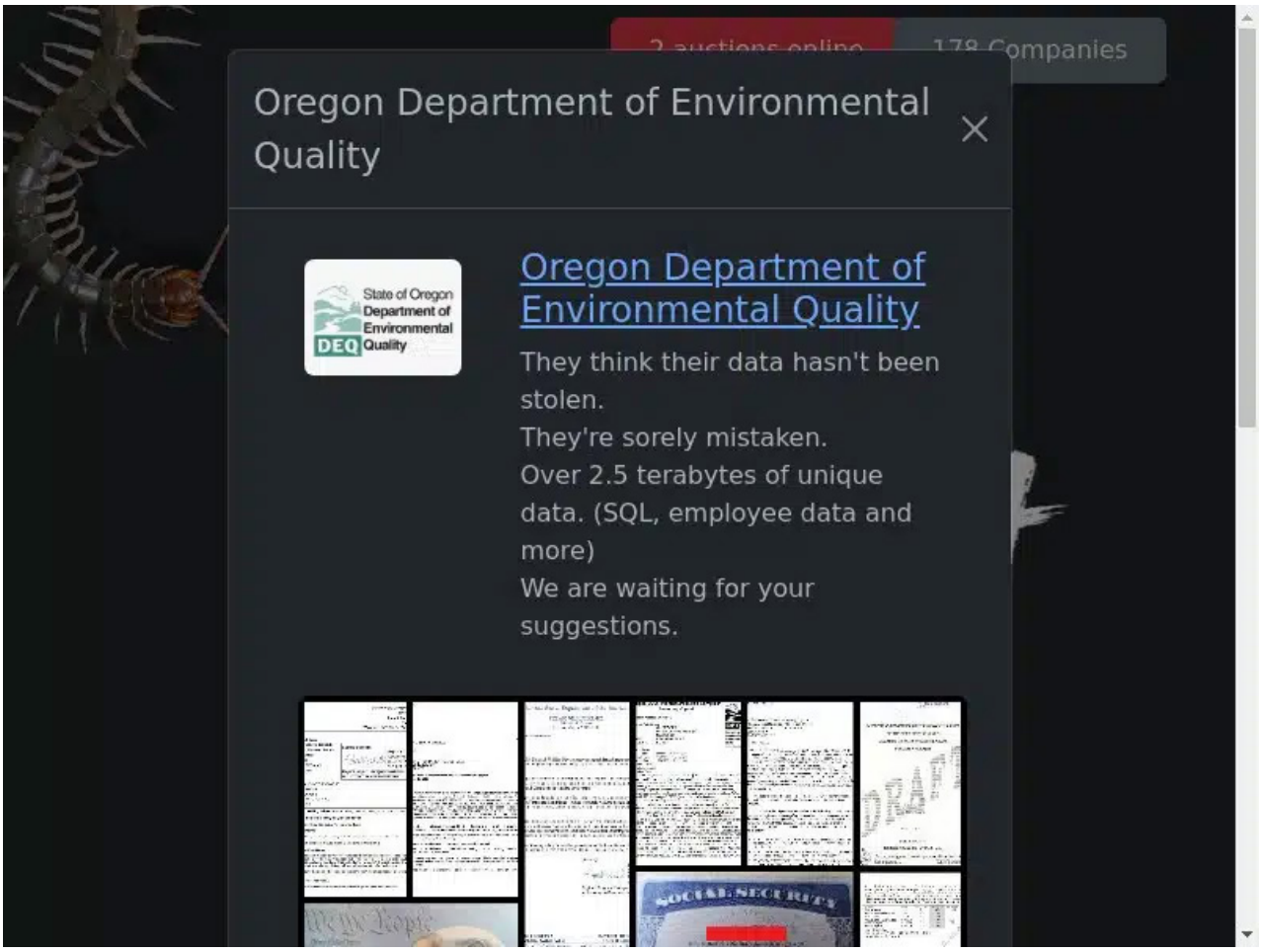
노스캐롤라이나주의 컴패션 헬스케어(Compassion Health Care) 역시 환자 및 직원 정보가 포함된 대규모 데이터 유출 사고를 겪었으며, 이 공격으로 23,282명의 환자 정보가 유출되었다고 통보했다.

또한, 오하이오주의 케터링 헬스(Kettering Health) 시설은 사이버 공격으로 인해 기술 장애가 발생하여 병원 콜센터가 중단되는 등 운영에 차질을 빚었다. 응급 서비스는 유지되었지만 일부 환자 치료 시스템 접근이 제한되었다.

[그림 4] 출처: health-isac.org

Health-ISAC에서 발표한 『2025년 의료 분야 사이버 위협 전망보고서』에 따르면
2024년 한 해 동안 의료 산업을 겨냥한 악성 활동을 분석한 결과
랜섬웨어가 가장 심각한 위협으로 지목되었다.
보고서는 의료 산업군을 대상으로 한 공격이 지속적으로 증가하고 있다고 분석했다.

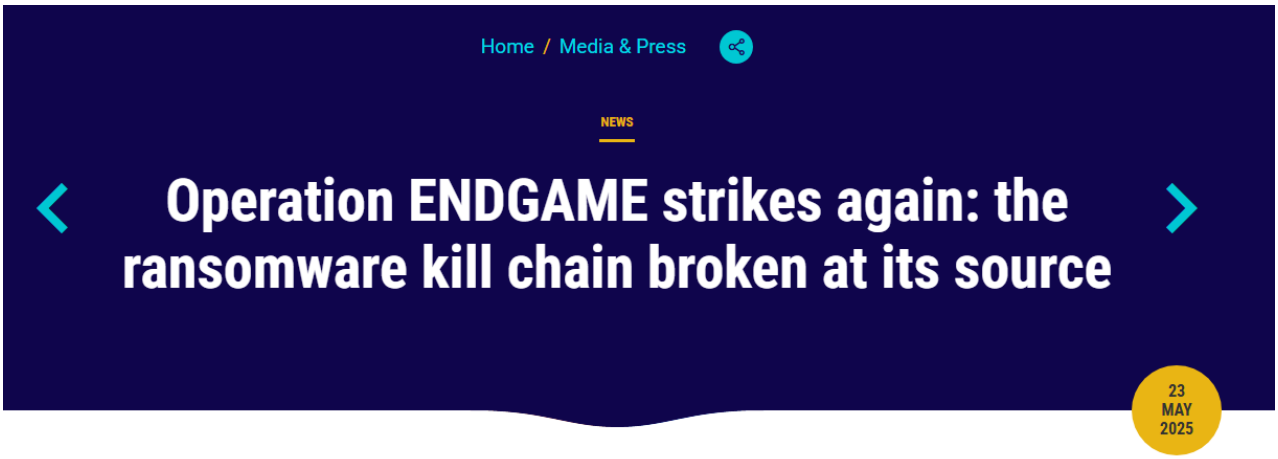
의료 산업에 대한 랜섬웨어 공격은 단순한 금전적 피해를 넘어,
인명 사고로 이어질 수 있는 중대한 위협이다.
실제로 지난해 영국의 진단 서비스 제공업체인 신노비스(Synnovis)가 사이버 공격을 받았고,
이로 인해 런던 병원의 환자가 사망하는 사건이 발생하기도 했다.



[그림 5] 출처: bleepingcomputer.com

오리건주 환경품질부(Oregon Department of Environmental Quality)는 2025년 4월 9일,
랜섬웨어 갱단인 리시다(Rhysida)에 사이버 공격을 받았다.
이 공격으로 인해 이메일 시스템, 컴퓨터 워크스테이션, 헬프 데스크, 차량 검사소가 중단되었다.

리시다(Rhysida) 랜섬웨어 그룹은 지난해 8월 시애틀 항만청을 공격한 이력이 있으며,
2025년 4월 3일 항만청은 데이터 유출로 피해를 입은 개인 약 9만명에게 해당 내용을 통지했다고 밝혔다.



[그림 6] 출처: operation-endgame.com

2024년에 실행된 엔드게임 작전(Operation Endgame)은
랜섬웨어 배포를 담당하는 드로퍼(Dropper)를 단속하며 100개 이상의 서버를 중단시킨 바 있다.
2025년에는 작전 규모를 더욱 확대하여,
랜섬웨어 공격에 사용된 서버 300개와 도메인 650개를 추가로 압수했다.

또한 수백만 달러 상당의 암호화폐를 압수하고,
랜섬웨어 및 다크웹 활동에 연루된 사이버 범죄자 수십 명을 체포하는 성과를 거두었다.

2.2 2분기 주요 랜섬웨어 그룹

2.2.1 Qilin Ransomeware

1) 그룹 개요

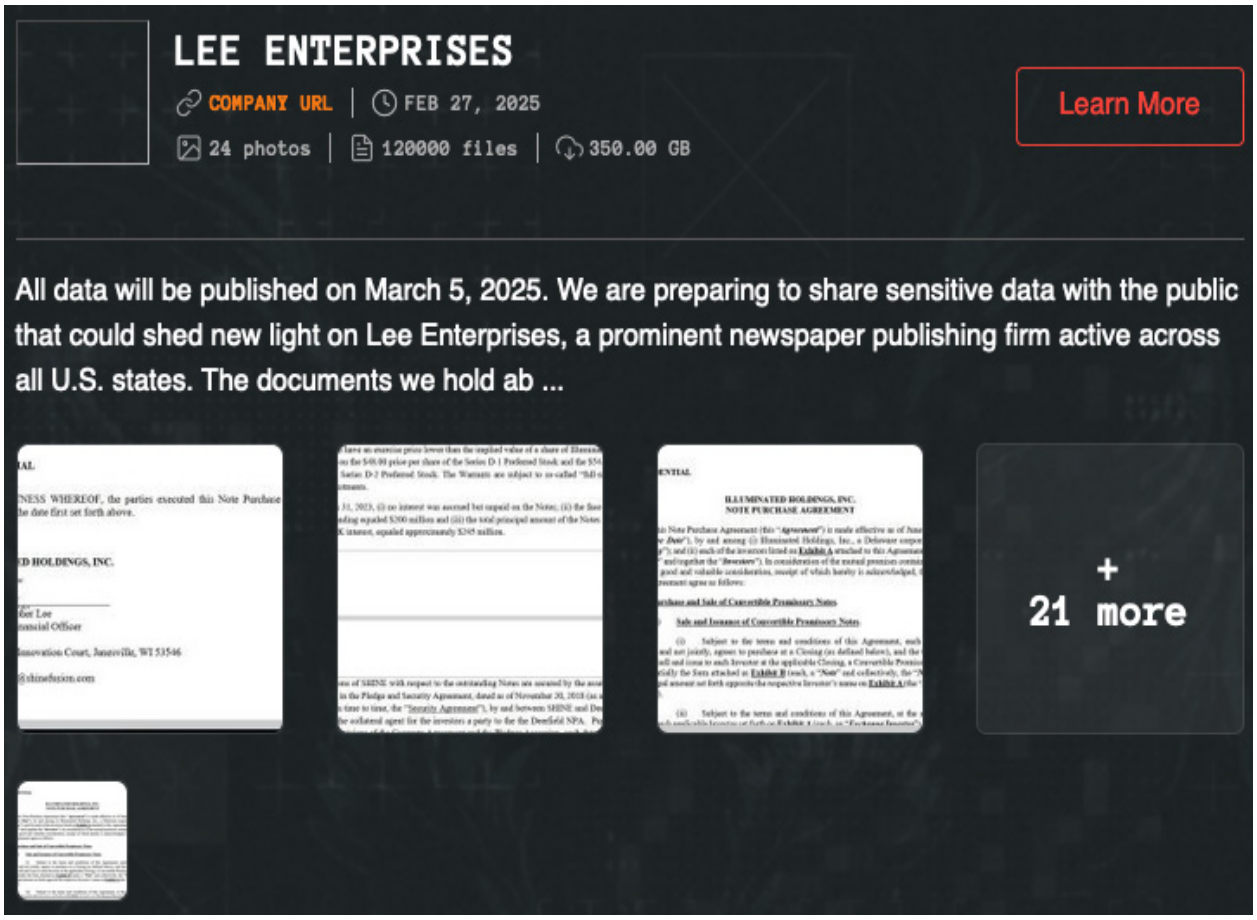
Qilin 랜섬웨어는 2022년 7월 'Agenda'라는 이름으로 처음 등장했으며,
이후 'Qilin'으로 리브랜딩하여 현재까지 활동 중인 RaaS(서비스형 랜섬웨어) 그룹이다.

이들은 전 세계 의료 기관을 비롯한 다양한 산업 분야를 지속적으로 공격하고 있다.
Golang과 Rust 언어로 개발된 멀티플랫폼(윈도우, 리눅스, ESXi) 변종을 제공하며,
데이터를 암호화한 뒤 유출하겠다고 협박하는 이중 협박(double extortion)을 주요 공격 방식으로 사용한다.

2) 최신 이슈

[그림 7] 2분기 Qilin 랜섬웨어 피해자의 월별 분포

2024년부터 활발한 활동을 보인 Qilin 랜섬웨어는 2025년에도 그 기세를 이어갔다.
여러 상위 랜섬웨어 그룹 사이에서 꾸준한 증가세를 보이며,
5월과 6월에는 가장 많은 피해 사례를 기록했다.



[그림 8] 출처: securityweek.com

최근 미국 최대 지방신문사 소유주 중 하나인 Lee Enterprises가
사이버 공격으로 인해 약 4만 명의 주민등록번호가 포함된 개인정보가 유출되었다.

이 회사는 메인주 규제 당국에 제출한 보고서에서 5월 28일에 민감 정보 유출 사실을 발견했다고 밝혔으며,
피해자들에게 1년간 무료 신용 모니터링 서비스를 제공했다.

[그림 9] 출처: comparitech.com

Next Step Healthcare는 지난해 6월 Qilin 그룹의 공격으로 심각한 데이터 유출 사고를 겪었다.
이 사고로 사회보장번호, 의료 기록, 재무 데이터, 운전면허증, 신용카드 정보 등
수천 명의 민감한 환자 정보가 유출되었다.

미국 앨라배마주 버밍엄의 한 피부과에서는 8만 6천여 명의 개인 정보가 유출되는 사고가 발생했다.
유출된 정보에는 이름, 사회보장번호, 주소, 전화번호, 생년월일, 의료 진단 및 치료 정보, 건강보험 정보 등이 포함되었다.
병원 측은 2025년 5월, 피해자들에게 이 사실을 통보했다.
Qilin 랜섬웨어 조직은 이 공격으로 141GB의 데이터를 탈취했다고 주장했다.

3) 최신 악용 취약점

Qilin 랜섬웨어 조직은 최근 공격에서 Fortinet의 취약점을 악용하는 것으로 나타났다.
해당 취약점을 이용하면 인증을 우회하여 원격으로 악성 코드를 실행할 수 있다.

CVE 번호	제품	설명
CVE-2024-21762	Fortinet FortiOS / FortiProxy	원격 코드 실행
CVE-2024-55591	Fortinet FortiOS / FortiProxy	인증 우회

▶ CVE-2024-21762

제품	**FortiOS / FortiProxy (SSL-VPN)**
취약점 유형	원격 코드 실행
공개일	2024년 3월 28일
CVSS 점수	9.8 (Critical)
기술 설명	원격의 인증되지 않은 공격자가 조작된 HTTP 요청을 통해 버퍼 오버플로우를 유발하는 취약점이다. 이로 인해 메모리 손상 및 프로세스 흐름 변경이 발생하여, 결과적으로 임의의 코드나 명령이 실행될 수 있다.
Qilin 사용 사례	Qilin이 이 취약점을 사용해 초기 접근 및 페이로드 실행에 성공
관련 TTPs	**- T1190: Exploit Public-Facing Application:** 인터넷에 노출된 Fortinet SSL-VPN 서비스의 취약점을 이용하여 원격에서 인증 없이 공격을 수행한다. **- T1203: Exploitation for Client Execution:** 악성 HTTP 요청을 통해 원격에서 프로세스 흐름을 제어하고 임의의 코드를 실행한다.

▶ CVE-2024-55591

제품	Fortinet FortiOS / FortiProxy
취약점 유형	인증 우회
공개일	2024년 3월 28일
CVSS 점수	9.8 (Critical)
기술 설명	인증 절차를 우회할 수 있는 문제로, 공격자가 관리 포털에 인증 없이 접근하여 방화벽 설정을 수정하거나 VPN 구성을 변경할 수 있게 한다. 이를 통해 내부 시스템으로의 통로를 확보하거나 제어 권한을 탈취하는 데 활용된다.
Qilin 사용 사례	Qilin이 이 취약점을 사용해 장비 접근 권한 획득에 성공
관련 TTPs	- T1190: Exploit Public-Facing Application: 방화벽 관리 인터페이스에 존재하는 취약점을 악용한다. - T1068: Exploitation for Privilege Escalation: 관리자 권한을 확보한 후 추가 공격 단계로 이어진다.

2.2.2 Play Ransomware

1) 그룹 개요

2022년 6월부터 활동 중인 Play 랜섬웨어 그룹은
데이터 유출 사이트의 성명에 따라 “거래 비밀 유지”를 목표로 하는 폐쇄적인 조직으로 추정된다.
이들은 여러 대륙에 걸쳐 다양한 기관을 표적으로 삼고 있으며,
데이터를 먼저 유출한 뒤 시스템을 암호화하는 이중 갈취(double extortion) 모델을 사용한다.

Play 랜섬웨어 그룹은 2024년에 가장 활발하게 활동한 조직 중 하나로,
북미, 남미, 유럽의 여러 기업과 중요 인프라에 큰 피해를 주었다.

2) 최신 이슈

[그림 10] 2분기 Play 랜섬웨어 피해자의 월별 분포

2분기 피해 현황을 살펴보면 4월과 5월에 활발한 활동을 보이다 6월에는 다소 주춤했지만,
총 97건의 피해를 유발하며 전체 2위를 차지했다.

[그림 11] 출처: cisa.gov

2025년 5월 FBI 발표에 따르면,
Play 랜섬웨어 조직은 전 세계적으로 900건 이상의 공격을 수행하며 활발한 활동을 이어가고 있다.
이들은 민감 데이터를 먼저 탈취하고 시스템을 암호화한 뒤 금전을 요구하는 이중 갈취 전략을 고수한다.
최근에는 SimpleHelp 원격 접속 도구의 취약점을 악용해 초기 침투에 활용한 정황도 포착되었다.

이들의 특징 중 하나는 랜섬 노트에 구체적인 금액이나 결제 수단을 명시하지 않고,
피해자가 특정 이메일 주소(@gmx.de, @web.de)를 통해 직접 연락하도록 유도하는 것이다.
또한, 조직 내 고객 지원 번호 등 외부에 공개된 전화번호를 활용하여
피해자에게 직접 전화를 걸어 협박하는 사례도 다수 보고되고 있다.

[그림 12] 출처: nosh.com

최근 2025년 6월,
Play 랜섬웨어 조직은 **미국 최대 낙농 협동조합인** Dairy Farmers of America(DFA)**를 공격**했다고 밝혔다.

Play 조직은 DFA로부터 예산, 급여, 회계, 세금, 재무 정보 등 기밀 데이터를 탈취했다고 주장하며,
구체적인 액수는 밝히지 않은 채 3일의 협상 시한을 제시하며 몸값을 요구했다.

[그림13] 출처: bleepingcomputer.com

Play 랜섬웨어는 이전에도 식음료 업계를 공격한 사례가 있다.
2024년 11월 크리스피 크림(Krispy Kreme)을 공격하여 161,676명에게 피해 사실을 통지하게 했고,
2025년 2월에는 가농 브라더스(Ganong Bros.)의 침해 사실이 보고되었다.

크리스피 크림은 이 공격으로 인해 1,100만 달러의 매출 손실을 입었고,
복구 비용으로 300만 달러를 지출했다고 밝혔다.

3) 최신 악용 취약점

브로드컴 산하 시만텍 위협 헌터 팀에 따르면,
Play 랜섬웨어 계열 공격자는 최근에야 패치된 Microsoft Windows 보안 취약점을 제로데이로 악용해 미국의 한 조직을 공격했다.

또한, AHA(미국 병원 협회)는 Health-ISAC 및 관련 기관과 협력하여,
SimpleHelp 원격 모니터링 및 관리(RMM) 소프트웨어의 취약점을 악용한
랜섬웨어 공격 정황을 확인했다고 밝혔다.

CVE 번호	제품	설명
CVE-2025-29824	Windows 10 전체 Windows 11 (21H2, 22H2 등) Windows Server 2016/2019/2022 (영향있음)	CLFS.sys 드라이버의 Use-After-Free (UAF) 버그로, 로컬 권한 상승(Local Privilege Escalation, LPE)을 유발한다.
CVE-2024-57726	SimpleHelp 5.5.7 및 이전	API 키를 활용해 관리자 권한 상승
CVE-2024-57727	SimpleHelp 5.5.7 및 이전	인증 없이 경로 탐색 및 파일 탈취
CVE-2024-57728	SimpleHelp 5.5.7 및 이전	Zip Slip 임의 파일 업로드

▶ CVE-2024-5529824

제품	**Windows 10** **Windows 11** **Windows Server 2016/2019/2022** **Windows Server Azure Editions**
취약점 유형	권한 상승
공개일	2025년 4월 8일
CVSS 점수	7.8 (High)
기술 설명	이 취약점은 CLFS.sys 드라이버에 존재하는 Use-After-Free (UAF) 버그로, 로컬 권한 상승(LPE)을 유발한다. 즉, 인증된 비관리자 계정이 SYSTEM 권한을 탈취할 수 있다.
Play 사용 사례	Play가 초기 침입 이후에 Grixba 인포스틸러를 배포하고, 정 API 호출 시점을 조작하여 CLFS UAF 취약점을 유발, SYSTEM 권한으로 권한 상승을 하였다.
관련 TTPs	**– T1068: Exploitation for Privilege Escalation:** CLFS 드라이버의 Use-After-Free 취약점을 악용해 SYSTEM 권한으로 상승시킨다.

▶ CVE-2024-57726

제품	**SimpleHelp 5.5.7 및 이전**
취약점 유형	권한 상승
공개일	2025년 1월 15일
CVSS 점수	9.9 (Critical)
기술 설명	낮은 권한을 가진 사용자가 과 도한 권한을 가진 API 키를 생성할 수 있는 취약점으로, 이를 통해 관리자 권한 획득이 가능하다.
Play 사용 사례	미국 기업을 대상으로 한 공격에서 SimpleHelp 원격 모니터링 및 관리 도구의 세 가지 취약점 (CVE-2024-57726, CVE-2024-57727, CVE-2024-57728)을 악용하는 것으로 확인되었다.
관련 TTPs	– **T1068 Exploitation for Privilege Escalation:** API Key 생성이 관리자 로직을 우회해 권한을 상승시킨다. – **T1098 Account Manipulation:** 새 API Key(자격 증명) 발급 및 권한 부여는 계정 속성 변조 행위에 해당한다.

▶ CVE-2024-57727

제품	SimpleHelp 5.5.7 및 이전
취약점 유형	경로 탐색 및 파일 탈취
공개일	2025년 1월 15일
CVSS 점수	7.5 (High)
기술 설명	인증되지 않은 공격자가 조작된 HTTP 요청을 통해 서버 내 임의 파일(예: 설정, 로그 등)을 외부로 유출할 수 있는 취약점이다.
Play 사용 사례	미국 기업을 대상으로 한 공격에서 SimpleHelp 원격 모니터링 및 관리 도구의 세 가지 취약점 (CVE-2024-57726, CVE-2024-57727, CVE-2024-57728)을 악용하는 것으로 확인되었다.
관련 TTPs	- **T1190 Exploit Public-Facing Application:** 외부 HTTP 요청 하나로 실행되는 무인증 경로 탐색 공격이다 - **T1005 Data from Local System:** 서버 내부 파일을 직접 수집 및 저장한다.

▶ CVE-2024-57728

제품	**SimpleHelp 5.5.7 및 이전**
취약점 유형	임의 파일 업로드
공개일	2025년 1월 15일
CVSS 점수	7.2 (High)
기술 설명	조작된 zip 파일(예: Zip Slip)을 업로드하여 파일 시스템의 어느 곳에나 임의의 파일을 생성할 수 있다
Play 사용 사례	미국 기업을 대상으로 한 공격에서 SimpleHelp 원격 모니터링 및 관리 도구의 세 가지 취약점 (CVE-2024-57726, CVE-2024-57727, CVE-2024-57728)을 악용하는 것으로 확인되었다.
관련 TTPs	- **T1203 Exploitation for Client Execution:** 악성 ZIP 파일이 서버 측 코드 실행을 유발한다 (예: 크론탭, DLL 덮어쓰기). - **T1105 Ingress Tool Transfer:** ZIP 파일 내에 포함된 페이로드를 서버로 옮겨 심는다.

2.2.3 DragonForce Ransomware

1) 그룹 개요

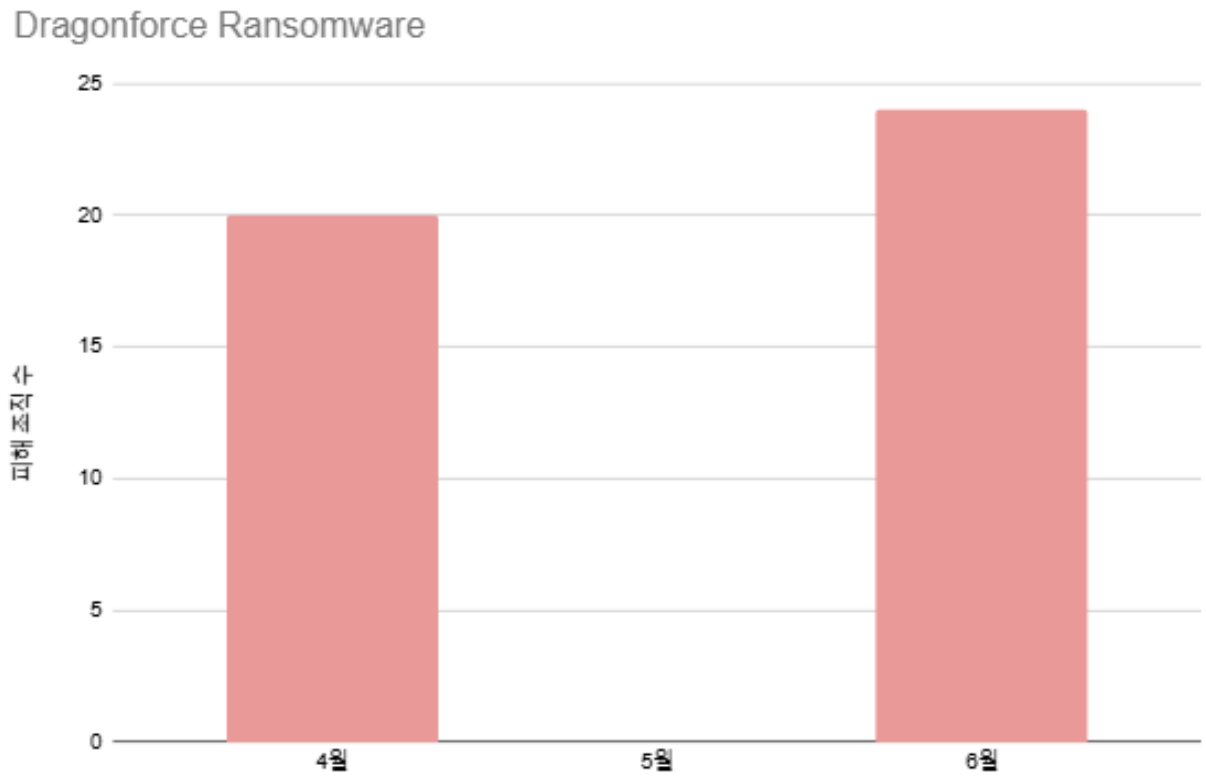
DragonForce는 2023년 중반에 등장한 랜섬웨어 조직으로,
현재 RaaS(Ransomware-as-a-Service) 모델을 기반으로 활발히 활동하고 있다.

최근 급부상하고 있는 위협 그룹 중 하나로,
Conti와 LockBit의 유출된 빌더를 기반으로 개발되어 두 조직의 기술을 계승하며 자체 생태계를 구축했다.

DragonForce는 제휴자(affiliate) 중심의 유포 구조를 통해 변종을 확산시키고 있으며,
최근에는 DragonForce 계열에서 파생된 Devman 랜섬웨어가 등장하는 등
RaaS 생태계 내에서 영향력을 빠르게 확대하고 있다.

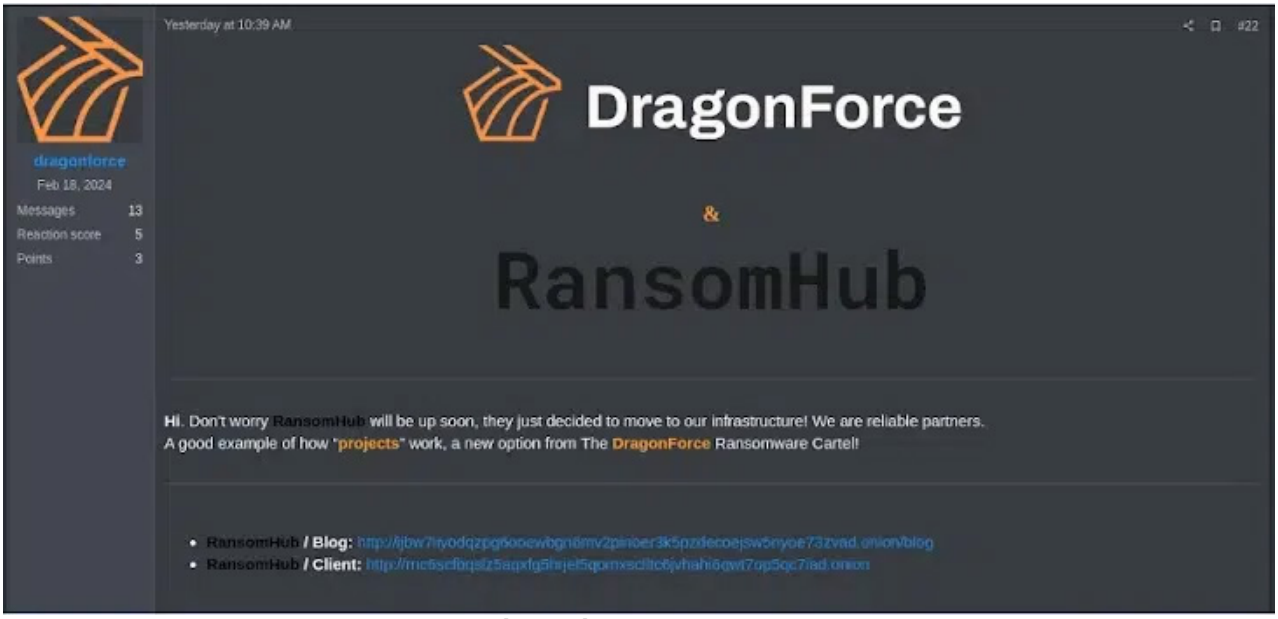
이들은 다양한 산업을 대상으로 민감 정보를 탈취한 뒤 암호화하고
금전을 요구하는 이중 갈취 전략을 사용하며,
원격 관리 도구의 취약점을 이용한 공급망 공격도 수행한다.

2) 최신 이슈



[그림 14] 2분기 Dragonforce 랜섬웨어 피해자의 월별 분포

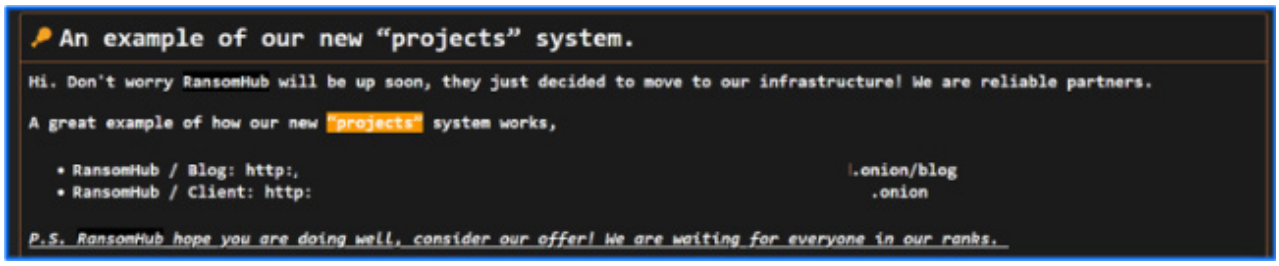
2025년 초, RansomHub가 활동을 중단한 이후
DragonForce는 RansomHub의 일부 제휴자를 흡수하며 자신들의 랜섬웨어 카르텔 구조를 강화했다.



[그림 15] 출처: specopssoft.com

DragonForce는 RansomHub 소속이었던 일부 제휴자들이
자신들의 인프라로 이적했다고 공식 발표했으며,
이 과정이 두 그룹 간의 권력 다툼 양상으로 전개되었다는 정황도 탐지되었다.

5월 초, DragonForce는 자신들의 데이터 유출 사이트에
RansomHub의 블로그 및 인프라 링크를 포함한 게시물을 올렸다.
해당 링크는 “RansomHub R.I.P. (2025년 3월 3일)”이라는 문구가 표시되는 페이지로 연결되었는데,
이는 RansomHub의 인프라가 더 이상 운영되지 않으며
DragonForce가 이를 흡수했음을 과시하는 행위로 해석된다.



[그림 16] 출처: specopssoft.com

해당 게시물은 DragonForce가 RansomHub와의 파트너십을 일방적으로 발표한지
수 주 후에 올라온 것으로,
실제 파트너십이 상호 합의에 의한 것이 아니었음을 뒷받침한다.

[그림 17] 출처: www.drapersonline.com

2025년 4월에서 5월 사이, DragonForce와 그 계열사들은 **영국의 대형 소매 체인**을 연쇄적으로 공격했다.

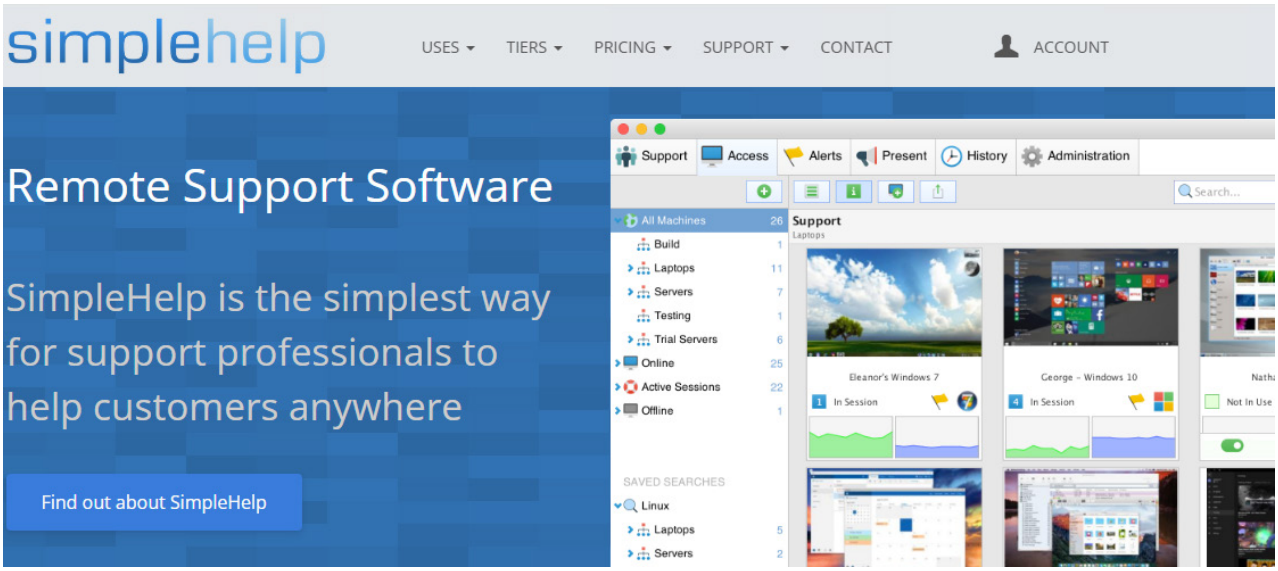
먼저 4월 말, 영국 최대 백화점 체인 중 하나인 M&S(Marks & Spencer)가
대규모 사이버 공격을 받아 광범위한 서비스 중단이 발생했다.
웹사이트와 앱이 마비되면서 회사는 약 일주일간 모든 온라인 의류 및 가정용품 주문을 중단해야 했다.

M&S 공격 발생 며칠 후,
영국의 대형 식료품 및 보험 소매업체인 Co-op Group은 해커가 자사 시스템에 침입하여
모든 직원의 VPN 접속이 중단되고 백오피스와 콜센터 서비스가 격리되는 사건이 발생했다.

이후 2025년 5월 1일, **런던의 고급 백화점인 해러즈(Harrods)에 대한 사이버 공격**이 공식적으로 확인되었다.
해러즈 IT 보안팀은 침해를 감지한 직후 모든 인터넷 접속을 차단하는 선제 조치를 취해,
심각한 피해로 이어지기 전에 사태를 효과적으로 차단한 것으로 알려졌다.

해러즈 백화점 공격의 배후에 DragonForce가 있다는 공식적인 발표는 없었지만,
앞선 M&S와 Co-op 공격과의 시기적 유사성으로 인해
동일 공격자 또는 연계된 캠페인일 가능성에 대한 추측이 제기되고 있다.

3) 최신 악용 취약점



[그림 18] 출처 : simple-help.com

Sophos의 경고에 따르면
DragonForce 랜섬웨어 공격 그룹이 취약한 SimpleHelp 인스턴스를 악용하여
관리 서비스 제공업체(MSP)와 그 고객들을 공격했다.

공격자들은 RMM(Remote Monitoring and Management)을 이용해
MSP의 고객 정보를 수집했으며,
여기에는 디바이스 이름, 구성, 사용자 정보, 네트워크 연결 정보 등이 포함되었다.

CVE 번호	제품	설명
CVE-2024-57726	SimpleHelp 5.5.7 및 이전	API 키를 활용해 관리자 권한 상승
CVE-2024-57727	SimpleHelp 5.5.7 및 이전	인증 없이 경로 탐색 및 파일 탈취
CVE-2024-57728	SimpleHelp 5.5.7 및 이전	Zip Slip 임의 파일 업로드

▶ CVE-2024-57726

제품	**SimpleHelp 5.5.7 및 이전**
취약점 유형	권한 상승
공개일	2025년 1월 15일
CVSS 점수	9.9 (Critical)
기술 설명	낮은 권한을 가진 사용자가 과도한 권한을 가진 API 키를 생성할 수 있는 취약점으로, 이를 통해 관리자 권한 획득이 가능하다.
DragonForce 사용 사례	영국 및 유럽 지역의 IT 관리 업체(MSP) 및 그 고객사 수십 곳을 대상으로, 유출된 자격 증명을 활용해 관리자 권한을 획득한 뒤 침투를 시도함.
관련 TTPs	- **T1068 Exploitation for Privilege Escalation :** API Key 생성이 관리자 로직을 우회해 권한을 상승시킴 - **T1098 Account Manipulation** : 새 API Key(자격 증명) 발급·권한 부여는 계정 속성 변조 행위에 해당

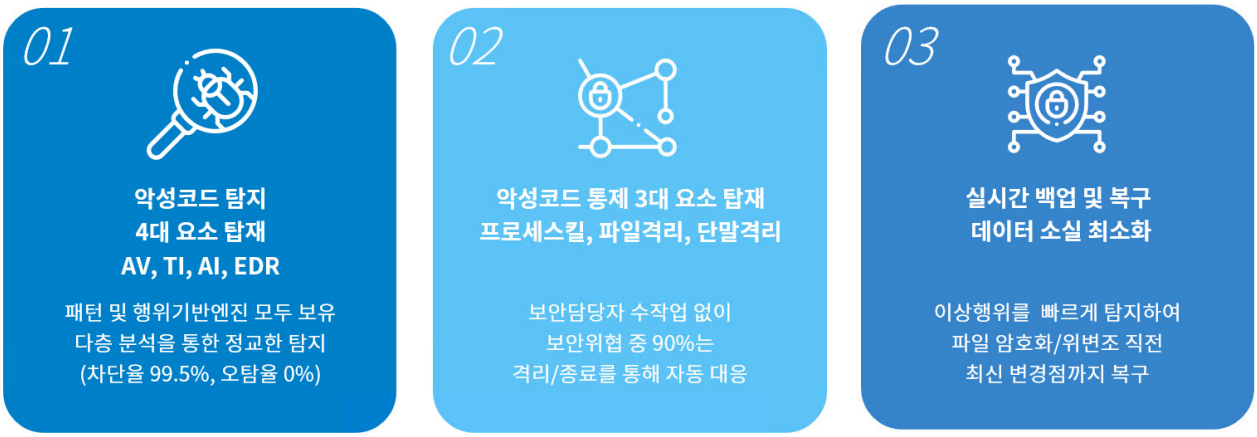
▶ CVE-2024-57727

제품	**SimpleHelp 5.5.7 및 이전**
취약점 유형	경로 탐색 및 파일 탈취
공개일	2025년 1월 15일
CVSS 점수	7.5 (High)
기술 설명	인증되지 않은 공격자가 조작된 HTTP 요청을 통해 서버 내 임의 파일(예: 설정, 로그 등)을 외부로 유출할 수 있는 취약점이다.
DragonForce 사용 사례	영국 및 유럽 지역의 IT 관리 업체(MSP) 및 그 고객사 수십 곳을 대상으로, SimpleHelp의 설정 파일(serverconfig.xml 등)에 무단으로 접근해 정보를 탈취함.
관련 TTPs	– **T1190 Exploit Public-Facing Application** 외부 HTTP 요청 하나로 실행되는 무인증 패스 트래버설 – **T1005 Data from Local System** 서버 내부 파일을 직접 수집·저장 – **T1552 Unsecured Credentials** serverconfig.xml 등에서 평문/해시 패스워드·API Key 획득

▶ CVE-2024-57728

제품	SimpleHelp 5.5.7 및 이전
취약점 유형	임의 파일 업로드
공개일	2025년 1월 15일
CVSS 점수	7.2 (High)
기술 설명	조작된 zip 파일(예: zip slip)을 업로드하여 파일 시스템의 어느 곳에나 임의의 파일을 업로드할 수 있다.
DragonForce 사용 사례	영국 및 유럽 지역의 IT 관리 업체(MSP) 및 그 고객사 수십 곳을 대상으로, ZIP Slip 취약점을 악용해 슬리버(Sliver) 백도어나 초기 페이로드를 업로드함.
관련 TTPs	– T1203 Exploitation for Client Execution 악성 ZIP이 서버 측 코드 실행 트리거(크론탭·DLL 덮어쓰기 등) – T1105 Ingress Tool Transfer ZIP 안에 포함한 페이로드를 서버로 옮겨 심음

3. Privacy-i EDR의 랜섬웨어 대응



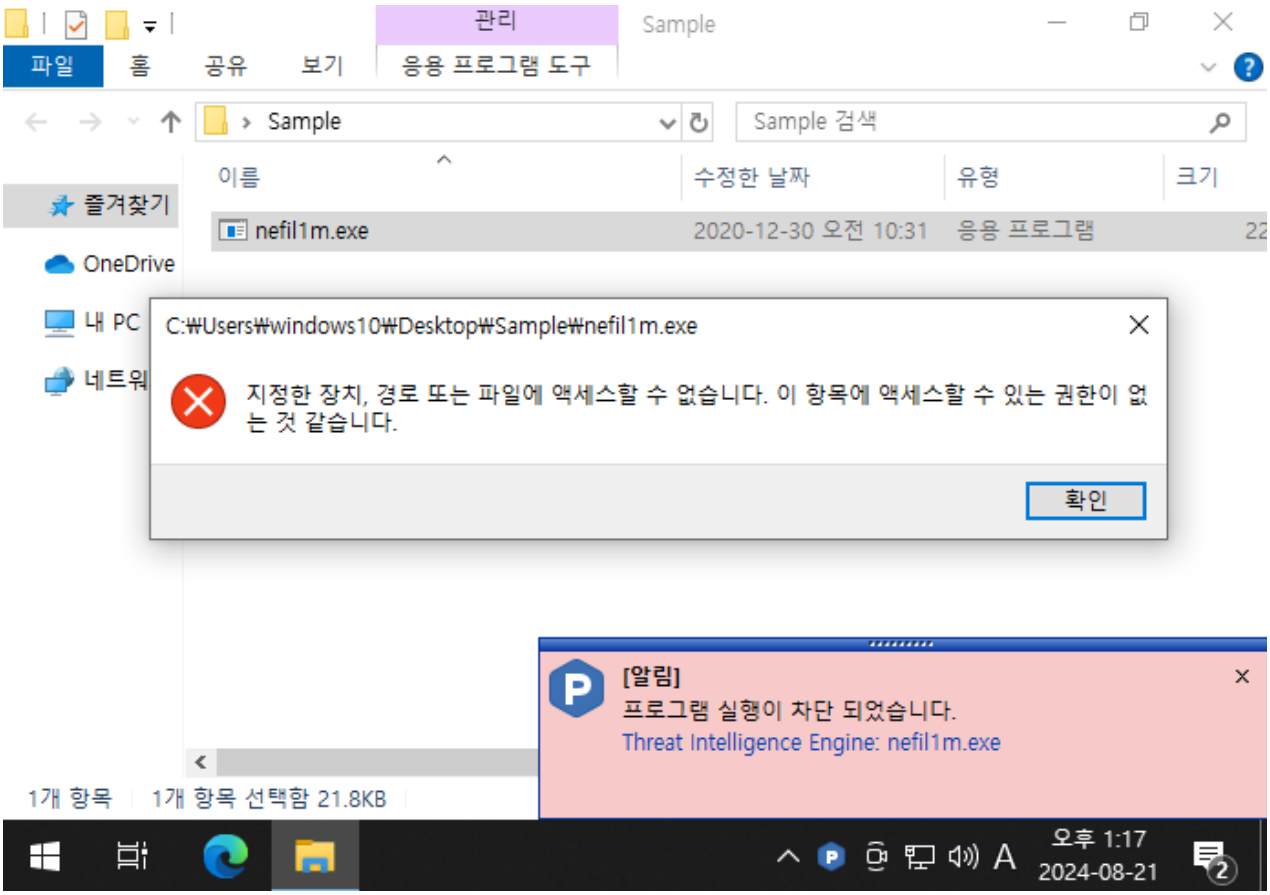
[그림 19] Privacy-i EDR 차별화 기능

Privacy-i EDR은 알려진 랜섬웨어뿐만 아니라
신·변종 랜섬웨어에 대응하기 위해 다계층 보안 기능을 제공한다.

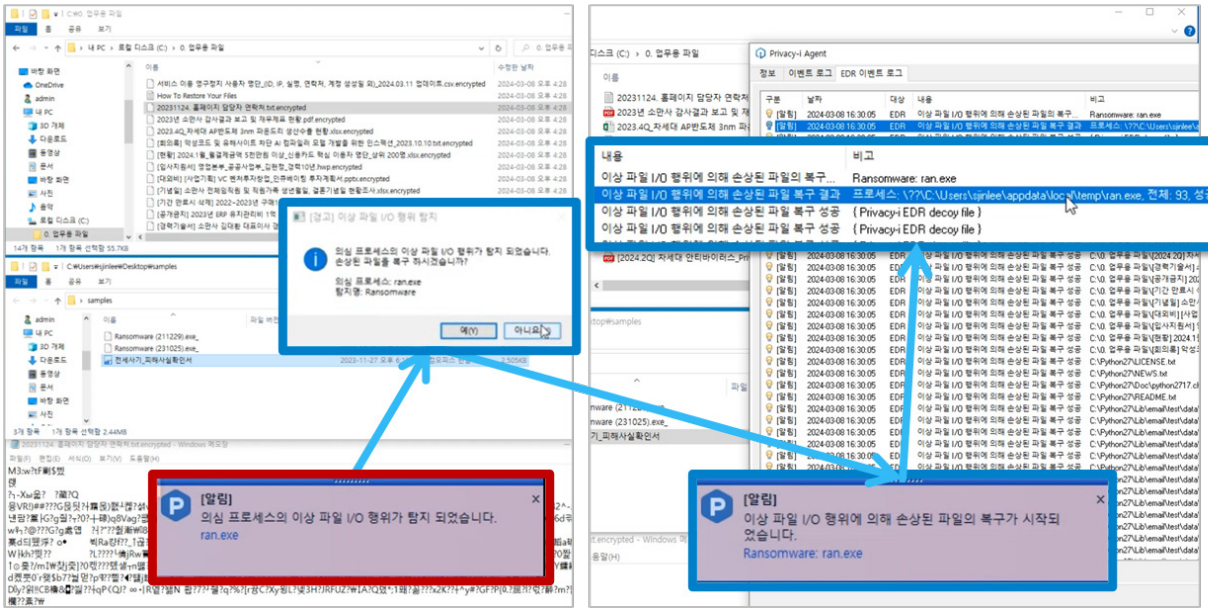
랜섬웨어가 초기 침투할 때,
정적 분석 엔진은 안티바이러스 엔진, 위협 인텔리전스, AI 엔진을 순차적으로 이용해 악성코드를 탐지한다.

정적 분석 엔진으로 탐지되지 않은 신·변종 랜섬웨어는
엔드포인트에서 실행되어 조직 내 자산의 암호화를 시작한다.
이때 동적 분석 엔진은 이러한 암호화 행위를 탐지하고 실시간 백업을 통해 데이터 유실을 방지한다.
또한, 무분별한 데이터 암호화 행위를 기반으로 신·변종 랜섬웨어를 탐지하고
해당 프로세스를 강제 종료하여 데이터 암호화를 중단시킨다.

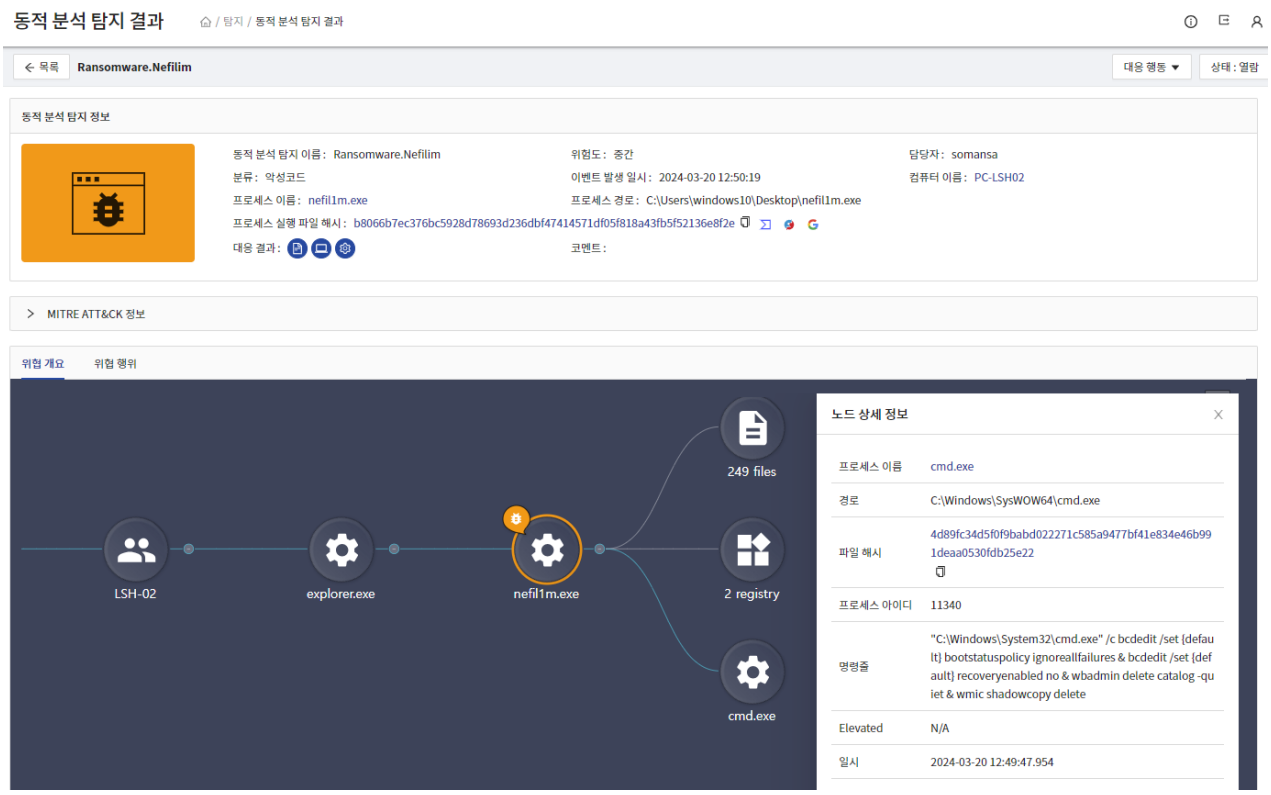
나아가, 실시간 백업 기능으로 저장한 사본을 통해
암호화된 데이터를 원본으로 복원하여 데이터 유실을 방지한다.



[그림 20] Privacy-i EDR 정적 분석 엔진에서 탐지 된 랜섬웨어 실행 차단 화면



[그림 21] Privacy-i EDR 랜섬웨어 탐지 후 복구 완료 화면



[그림 22] Privacy-i EDR 랜섬웨어 로그

궁금하신 점이나 문의사항은 malware@somansa.com 으로 문의주십시오