SK 쉴더스

Technical Analysis

침해사고 조사, 단순 비용인가
자산 보호를 위한 핵심 전략인가?

Technical Analysis

침해사고 조사, 단순 비용인가 자산 보호를 위한 핵심 전략인가?

개요

2025년은 사이버 위협이 우리 일상을 얼마나 깊숙이 침범했는지 여실히 보여준 한 해였다. 과학기술정보통신부와 한국인터넷진흥원(KISA)이 발표한 2025년 침해사고 신고 건수는 2,383건에 달했다. 이는 2023년 1,277건에서 불과 2년 만에 2배 가까이 급증한 것으로, 매년 뚜렷한 상승세를 기록하고 있다. IBM의 '2025년 데이터 유출 비용(CODB) 보고서(Cost of a Data Breach Report 2025)'에 따르면, 전 세계 기업들이 침해사고 당 지불하는 평균 비용은 약 444만 달러에 달하는 것으로 나타났다. 한국 기업들 역시 사고당 평균 42억 원 이상의 막대한 비용을 지불하고 있으며, 이는 개별 기업이 감당하기 어려운 수준의 경제적 타격이다.

침해 사고와 피해 규모가 동반 상승함에 따라, 기업 경영에 있어 보안 투자의 중요성은 그 어느 때보다 강조되고 있다. 많은 기업이 최신 보안 솔루션 도입, 방어 체계 강화 등 사전 예방에 적극적으로 예산을 투입하는 추세이지만, 정작 사후 대응 방식에서는 한계를 노출하고 있다. 방어벽이 뚫렸을 때 원인을 정밀하게 규명하고 재발 방지 포인트를 찾기보다는, 당장의 시스템 복구와 표면적 책임 소재 규명에 편중된 임시방편적 조치에 머무르는 실정이다.

정확한 침투 경로나 취약점을 찾지 못한 채 진행되는 복구는 미봉책에 불과하다. 근본 원인이 해결되지 않은 시스템은 결국 2차, 3차 공격의 표적이 될 수밖에 없다. 이제 침해사고 조사는 사후 수습을 위한 단순 비용으로 여길 것이 아니라 기업의 소중한 자산과 비즈니스 연속성을 지키기 위한 또 하나의 필수 투자로 인식되어야 한다.

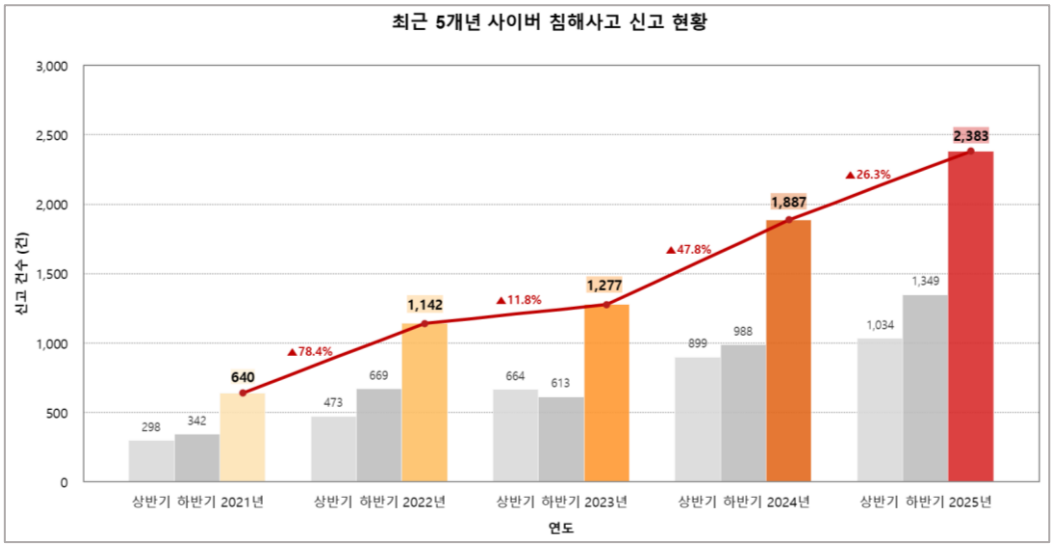

그림 1. 최근 5 개년 사이버 침해사고 신고 현황

침해사고 조사의 중요성

침해사고 조사는 무너진 비즈니스의 신뢰를 복원하고 시스템의 안전성을 증명하는 필수적인 과정이다. 침해사고 조사의 가치는 크게 네 가지로 요약된다.

1. 사고 원인의 명확한 규명: 공격 지점과 침투 경로를 정확히 파악하여 실효성 있는 방어 대책을 세울 수 있다.

2. 비즈니스 가용성과 무결성 보장: 피해 영역과 안전한 영역을 명확히 구분함으로써, 서비스 전체를 중단시키는 극단적 조치 대신 필요한 부분만 통제하여 비즈니스 연속성을 확보한다.

3. 피해 범위의 객관적 확정: 어떤 데이터가 유출되었고 어떤 시스템이 영향을 받았는지 수치로 증명함으로써, 과도한 대응 비용을 줄이고 고객과 이해관계자들에게 정확한 정보를 제공하여 불필요한 혼란을 방지한다.

4. 보안 체계의 실질적 고도화: 사고 조사는 현재 운영 중인 보안 장비와 프로세스의 허점을 발견하는 가장 강력한 기회다. 조사 결과를 보안 전략에 피드백 함으로써, 이론적인 보안이 아닌 실제 공격을 막아낼 수 있다.

데이터와 실전이 증명하는 침해사고 조사의 가치 – 실무 사례 기반

본 보고서에서는 침해사고 조사 실무 사례*를 통해 전문적인 침해사고 조사의 가치를 기술적으로 증명한다.

** 본문에서 등장하는 실무 사례는 당사가 수행한 침해사고 조사 사례를 기반으로 각색한 것임.*

[CASE 1] BitLocker 랜섬웨어 대응: 휘발성 메모리 포렌식 기반 복호화 키 추출 및 데이터 복구

그림 2. CASE 1 침해사고 조사 및 대응 흐름도

1. 상황 개요: 결제 데이터 암호화와 서비스 마비

온라인 결제 서비스 기업 A사의 결제 시스템망이 랜섬웨어에 의해 암호화되어 서비스가 전면 중단되었다. 백업본마저 삭제된 상태에서 공격자는 거액의 대가를 요구했다. 서비스 마비에 따른 즉각적인 매출 손실과 데이터 복구 비용을 고려할 때, 경영상 심각한 타격이 예상되는 상황이었다.

2. 실전 PoC: 휘발성 데이터 내 잔존하는 복호화 키 식별

당사는 시스템 전원이 유지된 상태에서 즉시 메모리 덤프를 획득하고 정밀 분석에 착수했다. 악성 행위 분석을 통해 공격자가 BitLocker를 사용하여 디스크를 암호화하였음을 알아냈고, PoC를 통해 암호화 과정에서 메모리 상에 복호화 키를 남긴다는 점을 이용했다.

▶ **분석 포인트:** BitLocker가 실행되면서 메모리에 잔류하게 된 복호화 키 구조 탐색 / 유효한 키 후보군 선별

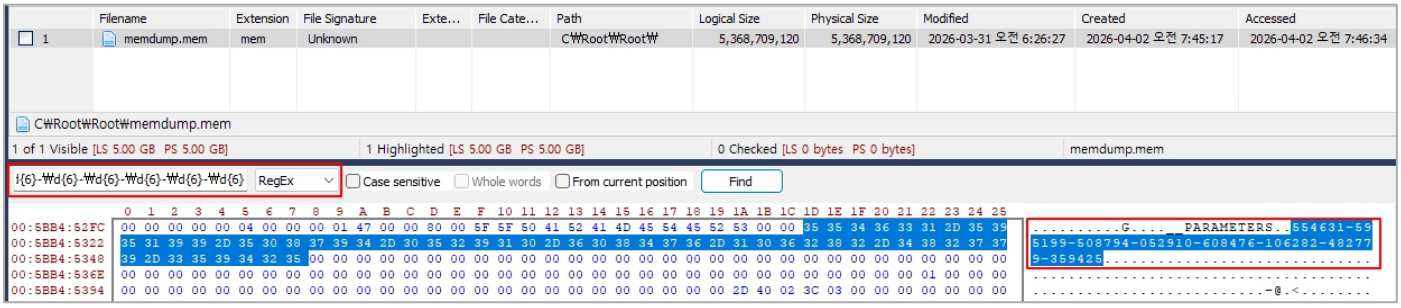

그림 3. 메모리 상에 잔류한 복호화 키 탐색

메모리에 잔류한 BitLocker 디스크 복호화를 위한 48자리 복구 키를 추출하여, 해커에게 별도의 대가 지불 없이 원본 데이터를 모두 복구하는 데 성공하였다.

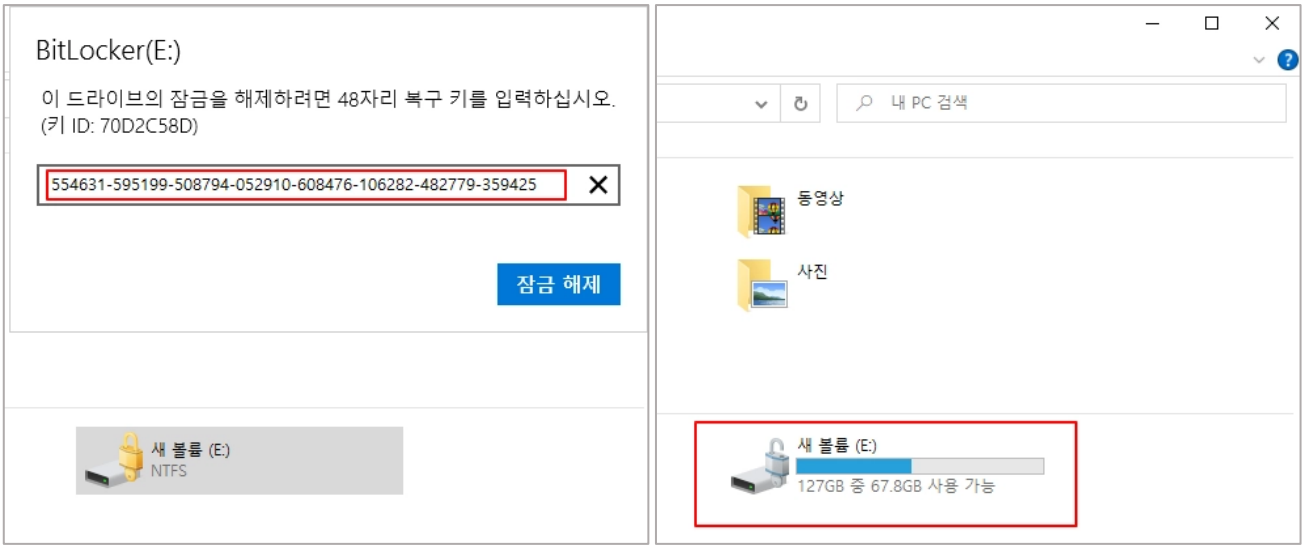

그림 4. 유효한 복호화 키 확인 / 디스크 복구

3. 침해사고 조사의 핵심 역할: 지출이 아닌 '수익형 활동'으로써의 조사 가치

지출이 아닌 수익형 활동으로써의 조사 가치는 다음과 같은 세 가지로 요약된다.

1. 직접적 비용 절감: 해커가 요구한 수억 원대의 협상 비용과 재구축 비용을 전액 보존

2. 가중 손실 방지: 공격자가 사용한 취약점을 동시에 파악하여, 복구와 동시에 재감염 경로를 차단

3. 최종 성과: 조사 비용 대비 수백 배에 달하는 데이터 자산 가치를 온전히 지켜낸 비즈니스 방어의 핵심 사례

[CASE 2] 디스크 포렌식 기반 개인정보 유출 범위 정량화 및 법적 소명 근거 확보

그림 5. CASE 2 침해사고 조사 및 대응 흐름도

1. 상황 개요: 전체 데이터가 유출되었을지도 모른다는 막연한 공포

고객 정보 100만 건을 보유한 이커머스 기업 B사. 관리자 계정 탈취 및 개인정보 유출 정황이 포착되었으나, 공격자가 로그를 치밀하게 삭제한 탓에 유출 규모를 특정할 수 없었다. 유출 규모를 특정하지 못할 경우 기업은 최악의 상황을 가정해 100만 명 전체에 대한 개인정보 유출 통보와 100억 원 ~ 300억 원 가량의 보상 리스크를 검토해야 하는 상황이었다.

2. 실전 PoC: 삭제된 흔적 너머의 데이터 전송 기록 추적

당사는 디스크 포렌식을 통해 삭제된 영역과 임시 파일, 아티팩트(Artifact)를 전수 조사했다. 공격자가 데이터를 압축하거나 외부로 전송할 때 필연적으로 남기는 하드디스크 상의 미세한 흔적을 추적하는 것이 핵심이었다.

▶ **분석 포인트:** 공격자가 탈취 데이터를 모으기 위해 생성했던 압축 파일의 흔적 복구 / 유출 시점의 방화벽 로그와 대조하여 유출된 데이터 규모 및 경로를 파악

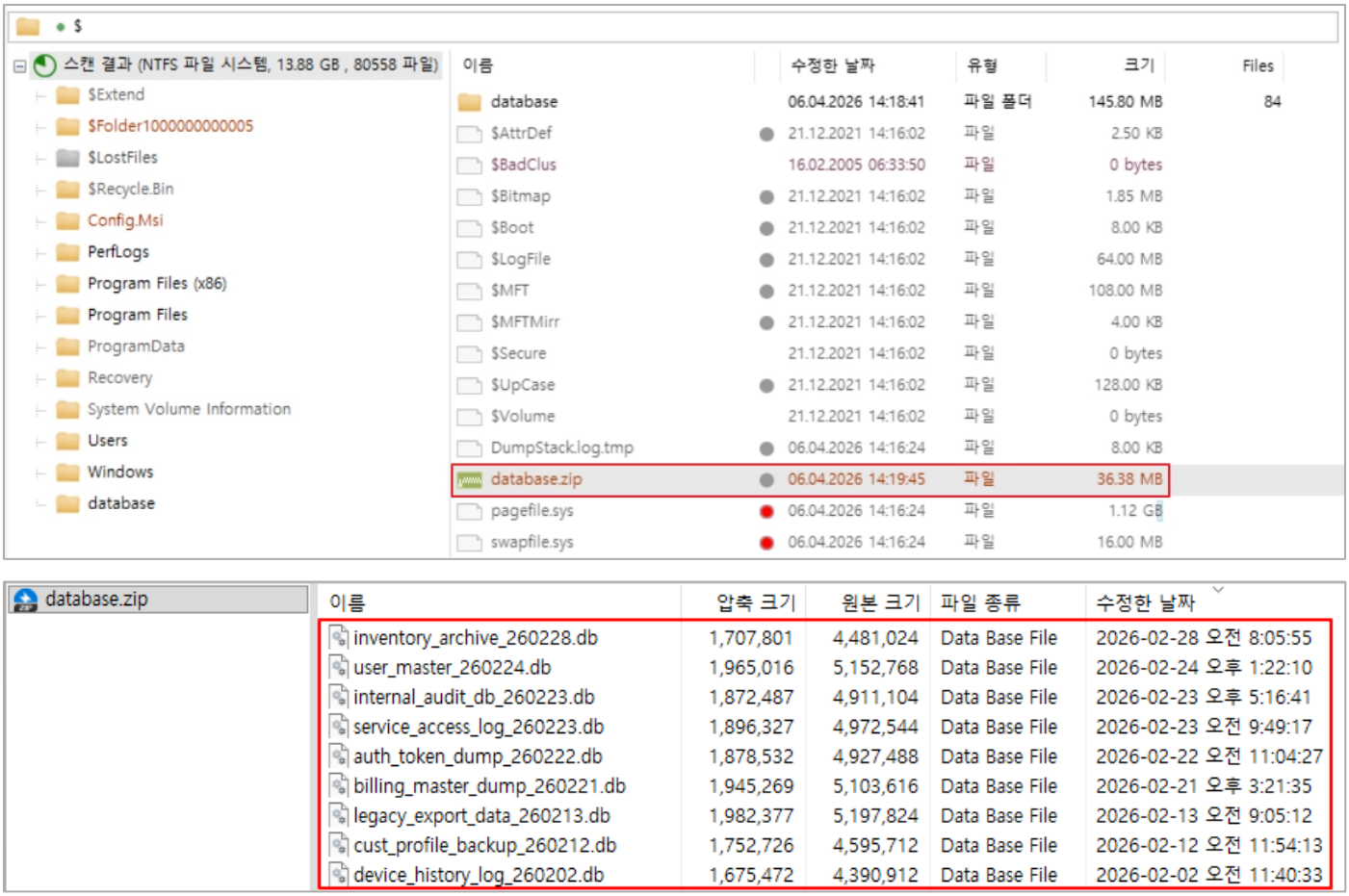

그림 6. 디스크 포렌식을 통한 삭제 파일 복구

디스크 포렌식을 통해 유출 시점에 생성 및 삭제된 압축 파일을 복구하였다. 해당 파일은 암호화되어 직접적인 내용 확인은 불가능했으나, 파일명과 생성 규칙을 통해 해당 파일들이 특정 서버에서 자동 생성되는 로그 파일임을 식별했다. 이후 해당 서버를 정밀 분석하여 공격자가 침투한 기간 동안의 로그파일을 수집 및 탈취하였음을 파악했고, 유출된 데이터는 고객 전체가 아닌 일부 고객 데이터 5천 건이며 개인정보는 마스킹(암호화)처리 되어있음을 증명했다.

3. 침해사고 조사의 핵심 역할: 확정적 리스크 관리로 가중 손실 방어

추측에 의존한 전수 통보 대신, 조사 결과에 기반한 확정적 대응으로 전환하여 기하급수적 손실을 막아냈다.

대응 비용의 최적화: 유출 규모를 명확히 한정함으로써, 불필요한 보상 비용과 브랜드 가치 하락에 따른 가중 손실을 절감

법적 소명 자료 확보: 조사 결과를 수사기관 및 규제 당국에 제출하여, 기업이 침해 사실을 숨기지 않고 적극적으로 소명했음을 증명

신뢰도 높은 사후 조치: 막연한 사과가 아닌, "언제부터 언제까지, 어떤 항목이 유출되었다"는 확정적인 정보를 제공함으로써 고객과 규제 당국에 대한 기업의 신뢰도를 빠르게 회복

최종 성과: 정밀 조사를 통해 리스크의 '불확실성'을 제거하는 것이 기업에 얼마나 큰 재무적 이익을 가져오는지 보여주는 핵심 사례

[CASE 3] 반복된 랜섬웨어 재감염 환경에서의 최초 침투 경로 식별 및 생산 연속성 복구

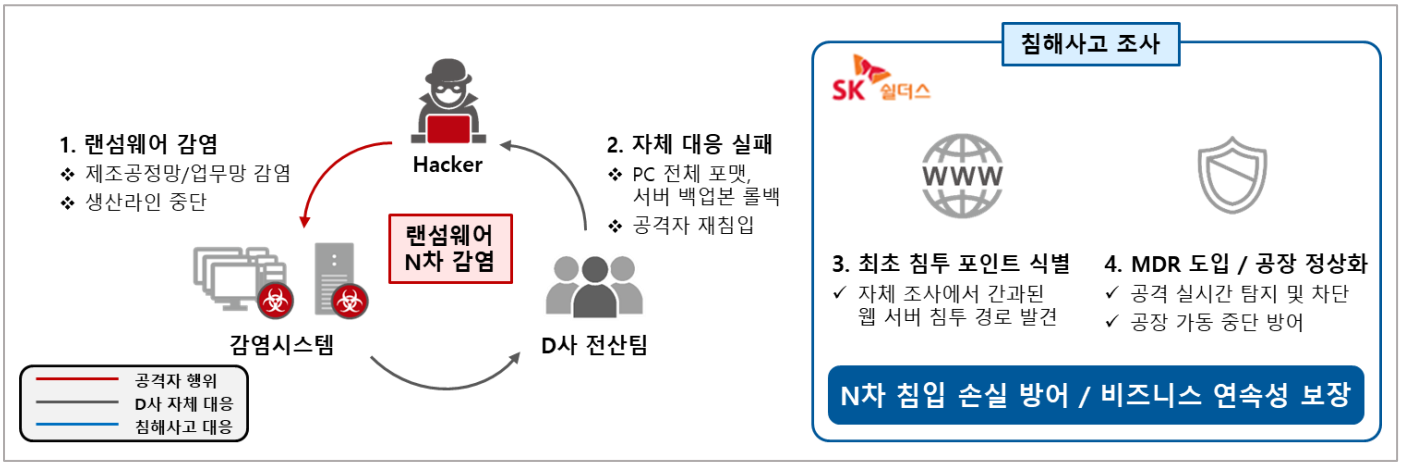

그림 7. CASE 3 침해사고 조사 및 대응 흐름도

1. 상황 개요: 포맷해도 다시 감염되는 2, 3 차 공격의 악순환

제조 기업 D사의 제조 공정망과 업무망이 동시에 랜섬웨어에 감염되며 생산 라인 일부가 가동 중단되었다. 내부 전산팀은 AD(Active Directory) 서버를 감염 매개체로 파악하고, 신속한 가동을 위해 PC 포맷과 핵심 서버의 백업본 롤백을 단행했다. 하지만 근본 원인을 제거하지 않은 성급한 정상화는 더 큰 화를 불렀다. 서비스 재개 직후, 공격자는 다시 AD 관리자 계정을 탈취해 다른 계정들을 잠그며 5일간 4회에 걸쳐 2차, 3차 공격을 이어갔고, 반복되는 감염으로 공장 가동이 수시로 중단되면서 시간당 수억 원에 달하는 막대한 손실이 발생했다.

2. 실전 PoC: 현상 복구가 아닌 침투 근거를 타격하는 정밀 분석

당사는 감염된 시스템을 정상화하는 표면적인 대응을 넘어, 공격자가 지속적으로 재침입할 수 있었던 최초 유입 경로를 식별하는 데 집중했다.

▶ **분석 포인트:** 내부 이동 및 확산 분석을 통한 최초 침투 포인트 식별

Client_IP	Timestamp	Method	Request_URL	StatusCode	Response_	Referer
		GET	/../../../etc/shadow	403	181	com
		GET	/api/v1/product?id=123 AND (SELECT 2234 FROM (SELECT(SLEEP(5)))a)--	200	453	com/produc
		GET	/board/view.php?no=10 AND (SELECT 1 FROM (SELECT COUNT(*),CONCAT(0x71707670	500	192	com/board/
		GET	/view.php?idx=1' OR 1=1 LIMIT 1--	404	181	com/list.php
		GET	/admin/index.php	401	181	com/
		GET	/etc/passwd	404	181	com
		POST	/board/upload_avatar.php	200	652	com/mypag
		GET	/fileupload/	200	325	com/mypag
		GET	/fileupload/avatar_9921.php?c=id;whoami;uname%20-a	200	54	com/fileuplo
		GET	/fileupload/avatar_9921.php?c=ls%20-R%20/var/www/html/config/	200	4243	com/fileuplo
		GET	/fileupload/avatar_9921.php?c=cat%20/etc/passwd	200	4265	com/fileuplo
		GET	/about.php	200	546	com/
		GET	/config/db.php.bak	200	135	com

그림 8. 외부 웹 서버에 노출된 최초 침투 포인트

AD 서버의 접속 기록과 인프라 전수 조사를 통해, 기업 자체 조사에서 간과했던 외부 웹 서버가 공격자의 베이스캠프로 활용되어 있었음을 밝혀냈다. 공격자는 AD 서버가 복구될 때마다 웹 서버에 업로드한 웹쉘을 통해 즉시 재침입하여 관리자 권한을 탈취하고 있었다. 당사는 해당 웹 서버의 외부 접근을 즉각 차단하고, 공격자가 이미 피해 시스템 곳곳에 수많은 거점을 확보해두었을 가능성에 대비하여 관리형 엔드포인트 보안 솔루션인 MDR(전문 보안 조직이 365일 상시로 위협을 실시간 탐지·대응하는 관리형 서비스)을 도입했다.

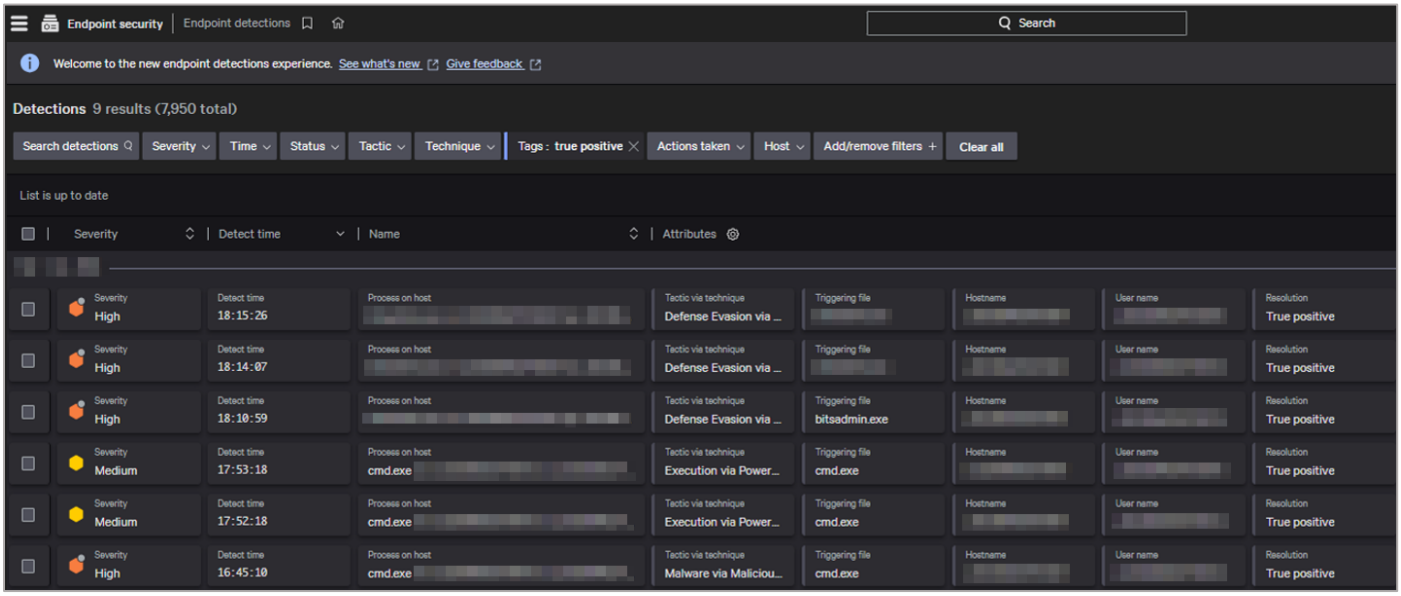

그림 9. MDR 도입을 통한 실시간 공격 행위 차단 및 가시성 확보

D사 네트워크 환경은 IT망과 OT망이 단일 AD로 묶여 있어, AD 권한이 탈취될 경우 망분리가 무용지물이 되는 세그멘테이션 미흡 상태였다. MDR은 공격자가 이러한 구조적 약점을 파고들어 내부망에서 횡적 이동하는 순간을 실시간으로 탐지 및 차단하였고, 일반 백신이 탐지하기 어려운 관리자 계정 오용과 악성 스크립트 실행을 즉각 차단하여 핵심 OT망으로 랜섬웨어가 확산되는 것을 원천 봉쇄했다.

3. 침해사고 조사의 핵심 역할: 비전문적 수습이 키운 손실, 전문 조사가 종결하다

단순 복구에 그쳤던 자체 대응과, 사고의 근본 원인을 규명한 전문 조사의 결과는 비즈니스 연속성에서 극명하게 갈렸다.

손실의 기하급수적 방어: 어디가 문제인지 모른 채 반복했던 시스템 포맷 비용과 공장 가동 중단에 따른 매몰 비용 절약

보안 체계의 실질적 강화: 외부에 방치된 웹 서버 취약점을 패치하고 부실했던 계정 관리 정책 및 네트워크 세그멘테이션을 재설계함으로써 지속 가능한 방어 체계 구축

최종 성과: 전문적인 침해사고 조사가 단순한 수습을 넘어, 기업의 생산성과 직결된 재무적 리스크를 해결하는 경영 전략임을 입증한 사례

[CASE 4] 공급망 연계 데이터 유출 조사: 공격자 인프라 역분석을 통한 피해 범위 확정 및 사각지대 가시성 확보

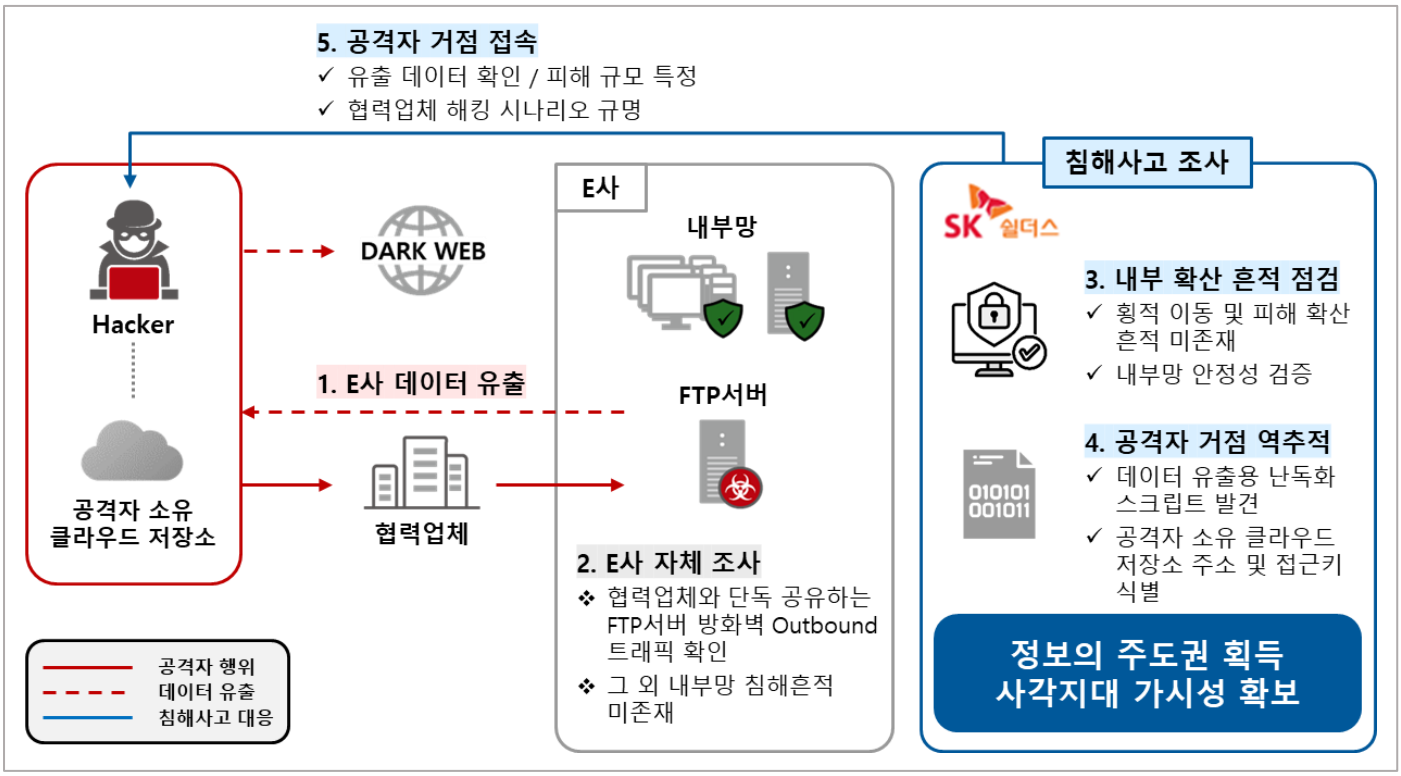

그림 10. CASE 4 침해사고 조사 및 대응 흐름도

1. 상황 개요: 다크웹에 유출된 데이터, 조사 권한 밖의 사각지대에 갇히다

다크웹에 물류 기업 E사의 데이터 탈취 게시글이 올라왔다. E사의 자체 조사 결과, 방화벽 로그와 유출 데이터를 대조해 보니 협력업체와 단독으로 공유하던 FTP 서버가 유출 통로로 확인되었다. 하지만 E사 내부의 다른 시스템에서는 공격자 침해로 보이는 이상 행위나 공격자 서버와의 통신 이력이 전무했다. 정황상 협력업체의 계정 탈취가 의심되었으나, E사는 협력업체 시스템의 직접적인 조사 권한이 없어 사고의 전모를 파악할 수 없었다. 이에 E사는 자사 내부망의 피해 확산 여부를 확실히 검증하고 유출의 실체를 파악하고자 당사에 침해사고 조사를 의뢰했다.

2. 실전 PoC: 해커의 거점을 역추적해 정보 비대칭의 벽을 넘다

당사는 우선 E사의 FTP 서버를 조사하여 내부망으로의 횡적 이동이나 추가 피해 확산이 없음을 최종 확인했다. 이후 수동적 점검을 넘어 데이터 유출 행위 자체를 역추적하는 정밀 분석에 돌입했다.

▶ **분석 포인트:** 탈취 스크립트 역분석 / 공격자 클라우드 저장소 확보

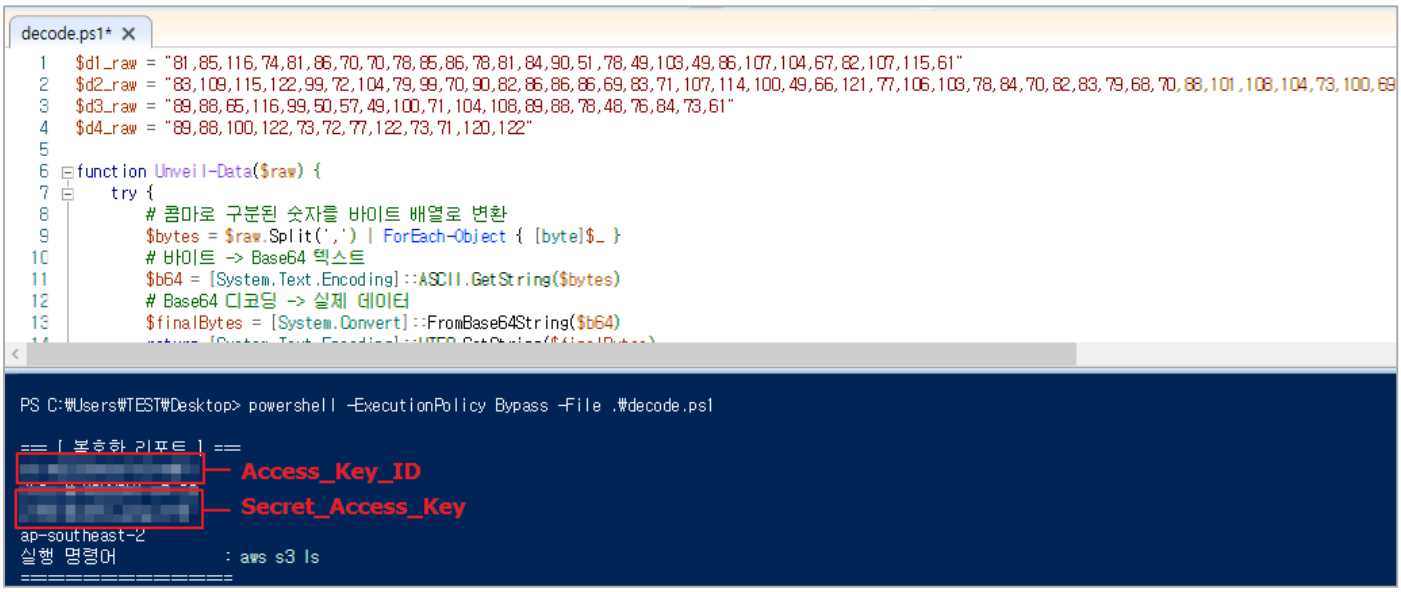

그림 11. 난독화 스크립트 복원 및 클라우드 접근 키 식별

당사는 FTP 서버에 남아있던 공격자의 미세한 흔적을 추적하던 중, 데이터 외부 반출 시 일회성으로 구동된 난독화 스크립트를 찾아냈다. 이를 리버스 엔지니어링(역분석)한 결과, 스크립트 내부에 하드코딩된 공격자 소유의 클라우드 저장소 주소와 접근 키(Access Key)를 추출해냈다.

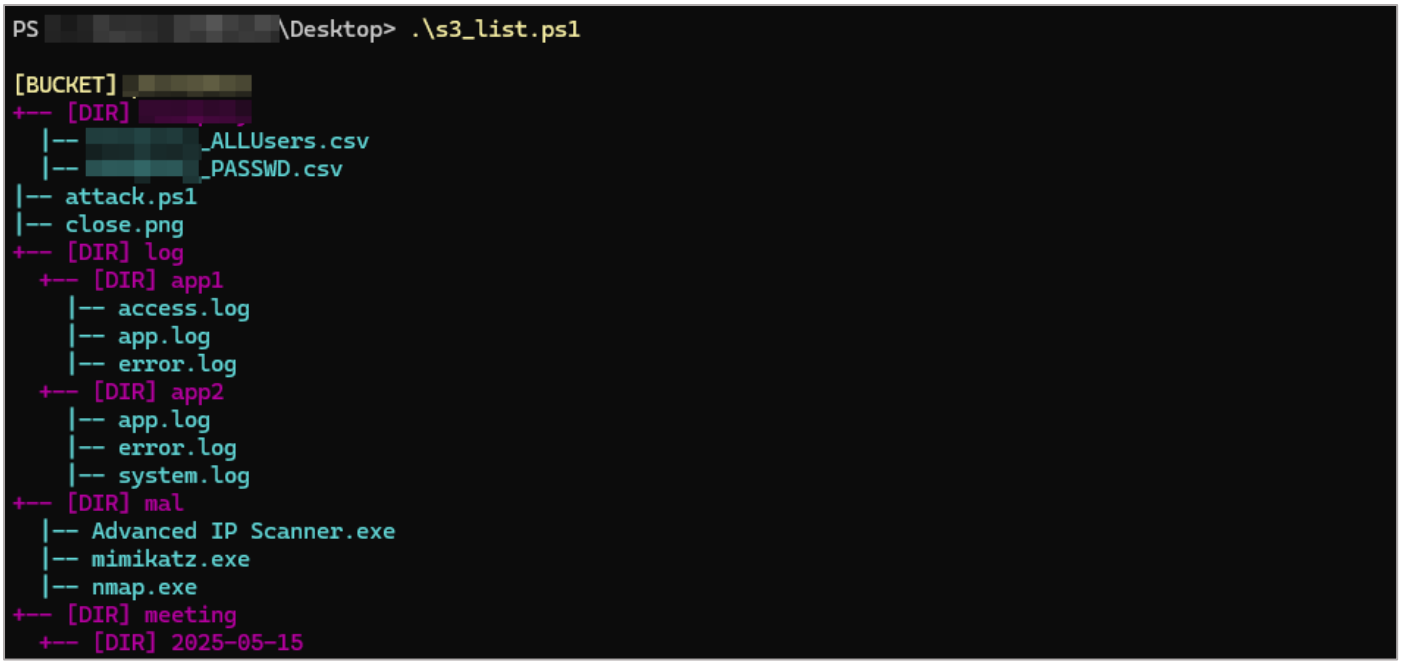

그림 12. 역분석을 통해 드러난 해커의 클라우드 저장소

당사는 확보한 키를 이용해 해커의 클라우드에 직접 접속했다. 그곳에는 탈취된 E사의 데이터와 함께, 공격자가 사용한 악성코드와 해킹 도구들, 협력업체의 내부망 스캐닝 결과 파일과 탈취된 계정 정보가 고스란히 남아있었다. 당사는 E사의 유출 데이터를 즉각 다운로드하여 피해 규모를 특정한 뒤, 법적 검토를 거쳐 클라우드 내 자료를 전량 삭제 조치했다. 동시에 확보한 해커의 도구와 로그를 분석하여, 조사 권한이 없어 알지 못했던 협력업체의 해킹 시나리오와 공격자의 TTPs(전술·기법·절차)를 일부 규명할 수 있었다.

3. 침해사고 조사의 핵심 역할: 정보의 주도권을 되찾고 객관적 증거로 방어하다

전문 조사를 통해, 권한의 한계로 조사가 불가능했던 협력업체 연계 사고를 완벽히 통제 가능한 영역으로 끌어온 사례다.

피해 규모의 정확한 특정: 막연한 공포에서 벗어나 공격자의 저장소에서 실제 유출된 데이터를 직접 확인하고 수치화함으로써 혼란을 막고 사후 대응 근거 마련

내부망 안전성의 100% 검증: FTP 서버 밖으로 다른 시스템에 피해 확산이 없었음을 객관적 포렌식 데이터로 입증

사각지대 가시성 확보: 직접 조사할 수 없었던 파트너사의 피해 양상을 공격자의 악성도구 분석을 통해 추정, 향후 협력업체 보안 연동 정책을 어떻게 강화해야 하는지 핵심적인 인사이트 제공

■ 결론 및 제언: 위기 극복을 위한 최선의 선택

지금까지 살펴본 사례들은 하나의 공통된 사실을 분명하게 보여준다. 침해사고는 단순히 '발생 여부'가 중요한 것이 아니라, 사고 이후 '어떻게 대응하느냐'에 따라 피해의 크기와 기업의 미래가 결정된다는 점이다. 그럼에도 불구하고 여전히 많은 기업은 침해사고 조사를 추가 비용으로 인식하며 최소한의 대응에 그치고 있다. 그러나 이는 단기적인 비용 절감일 뿐, 장기적으로는 더 큰 손실을 초래할 수 있는 위험한 선택이다.

이제는 관점을 바꾸어야 한다. 침해사고 조사는 비용이 아니라, 기업의 핵심 자산과 브랜드 신뢰를 지키는 핵심 전략이자 필수적인 투자다. 사고 발생 직후의 짧은 대응 시간 동안 얼마나 정확하고 깊이 있는 조사를 수행하느냐에 따라 피해 확산을 차단하고 재발을 방지하는 수준이 근본적으로 달라진다. 이에 기업은 다음과 같은 방향으로 대응 전략을 재정립할 필요가 있다.

1. 사고 대응 체계에 전문 침해사고 조사 역량을 반드시 포함해야 한다.
2. 내부 인력만으로 한계가 있는 경우, 신속하게 투입되어 체계적인 분석과 대응이 가능한 전문 침해사고 조사 조직을 활용 해야 한다.
3. 사고 대응을 단순 복구 중심이 아닌 '원인 규명 및 재발 방지 중심'으로 전환해야 한다.

특히, 고도화되는 공격 기법과 AI 기반 분석 환경에서는 경험과 기술력을 갖춘 전문 조사 조직의 역할이 더욱 중요해지고 있다. 단편적인 로그 분석이나 자동화 도구에 의존하는 대응은 오히려 잘못된 결론을 도출해 상황을 악화시킬 수 있다. 반면, 다양한 실전 경험과 정교한 분석 체계를 갖춘 전문 서비스는 복잡한 공격 시나리오를 입체적으로 재구성하고, 기업이 놓치기 쉬운 핵심 단서를 정확히 짚어낸다.

결국 침해사고 대응의 본질은 '얼마나 정확하게 이해했는가'에 있다. 위기에 끌려갈 것인가, 전략으로 통제할 것인가? 사고가 발생한 그 순간의 결정이 기업의 자산과 신뢰, 그리고 미래를 결정한다.

■ 보고서 작성 및 검수

■ 작성: 장지혜 선임, 이승훈 선임, 김지훈 선임 (Top-CERT팀)
■ 검수: 김성동 그룹장 (Incident Response그룹), 허준 팀장 (Top-CERT팀)