BRANDEFENSE COUNTRY REPORT · SOUTH KOREA 2026

Brandefense 대한민국 사이버 위협 현황 보고서 2026

연결된 경제의 신원, 외부 업무 애플리케이션, 복구

Odin by Brandefense

연구 기간: 2026-11-22

버전 1.0 · 공개 연구판 · TLP:CLEAR · 개정일: 2026-11-23

4

증거·종결 시험과 연결된 경영진 판단

250

통합한 열 개 부문에 속한 후보 도메인

8

서로 다른 증거 한계를 지닌 상세 주장 사례

73

Ransompedia의 대한민국 랜섬웨어 게시

목차

목차

Translated with AI

이 판은 영어 원문에서 AI로 번역되었습니다. 내용에 차이가 있으면 영어판을 기준으로 합니다.

01	경영진 요약	05
	보고서 지도	08
02	대한민국의 디지털·보안 환경	09
03	조직 관련 노출과 외부 공개 서비스의 보안 상태	12
04	다크웹과 포럼 증거	21
05	공개 사고와 부문별 표적 활동	41
06	핵티비즘, DDoS, 서비스 연속성	57
07	공격자, 캠페인, 관계	63
08	사기, 신원, 정보 재사용 문제	73
09	은행과 금융 서비스	78
10	규제와 국가 대응	82
11	전망과 조건부 시나리오	86
12	실행 계획	90
A	부록 A. 범위, 증거, 한계	96
B	부록 B. 증거 목록	99
C	부록 C. 출처	100
D	부록 D. 용어 설명	105
	보고서 소개	107

이사회·경영진	01 05 11 12
CISO·보안 책임자	03 04 05 07 12
SOC·위협 인텔리전스팀	04 06 07 부록 B
사기 대응·고객 운영팀	05 08 09
개인정보 보호·법무·구매팀	05 09 10 12

이 판에 관하여

AI로 번역됨. 의미 차이가 생기면 영어 원문을 기준으로 한다.

AI의 도움으로 작성했다. 관찰, 범죄 주장, 출처의 공격자 평가, 확인된 공개 자료를 구분한다. 범위와 확신도는 부록 A에서 설명한다.

대한민국 관련 증거는 연결된 대응을 요구한다. 신원을 확인하고, 지원 업무 애플리케이션을 검토하며, 영향받은 사람을 보호하고, 핵심 서비스 복구를 입증해야 한다.

73

대한민국 랜섬웨어 게시이며 범죄자의 주장

250

열 개 부문에 걸친 선정 후보 도메인

26

주장과 공개 자료를 포함한 상세 사례

4

책임 있는 완료 증거를 갖춘 경영진 판단

목차와 읽기 경로

장	질문	최초 독자
1 경영진 요약	증거에서 어떤 판단이 나오는가?	경영진
2 환경	어떤 서비스 의존 관계가 중요한가?	CISO·업무 책임자
3 조직 관련 노출	선정 도메인 관찰은 무엇을 입증하는가?	신원·인프라 담당팀
4 지하 시장 활동	무엇이 제안되며 무엇이 미확인인가?	위협 인텔리전스팀
5 부문별 사고	출처는 실제로 무엇을 확인·보고했는가?	사고·부문 책임자
6 가용성	주장과 입증된 영향은 어떻게 다른가?	서비스 운영팀
7 공격자	어떤 공격자 평가와 관계가 뒷받침되는가?	위협 인텔리전스팀·SOC
8 사기	어떤 업무 절차에서 유통 정보가 재사용될 수 있는가?	사기 대응·고객 운영팀
9 은행	애플리케이션·신원·고객 판단은 어떻게 연결되는가?	금융 분야 책임자
10 규제	현행 의무와 이후 조치는 어떻게 다른가?	개인정보 보호·법무팀
11 전망	어떤 조건부 시나리오에 대비해야 하는가?	경영진
12 실행 계획	누가 조치하며 무엇으로 완료를 입증하는가?	모든 책임자
부록 A–D	범위, 증거 목록, 출처, 정의	참고 자료

장 01

경영진 요약

01

이 장에서 답하는 질문

어떤 대한민국 관련 결과가 즉각적인 판단의 근거가 되는가?

4

증거·종결 시험과 연결된 경영진 판단

경영진을 위한 네 가지 판단 07

올해의 수치 07

장 01

경영진 요약

요약

증거는 신원 위험·주변 업무앱·공급업체·복구를 연결한다. Ransompedia에는 게시 주장 73건이 있다. 공개 출처는 애플리케이션 정보접근·랜섬웨어·표적서신을 설명한다. 마감 직전 범위수정치는 고유인원으로 합산하지 않는다. 범죄광고는 미확인이며 국가연계 평가는 출처의 판단이다. 계정증거·민감앱 접근·공급업체 통지경로를 확인하고 업무책임자와 복원을 훈련하라.

게시물, 갈취 게시, 선정 도메인, 출처 공개, 사람은 서로 다른 집단이다. 보고서는 이를 전국 사고 총계로 합산하지 않는다. 사건 발생, 발견, 공개, 이후 제재도 구분한다. [S1][S2][S3]

포함된 사건, 발표, 자체 데이터 스냅샷의 마감일은 해당 날짜가 진행 중이던 2026-11-22 이며, 마감 이전 외부 출처 일부는 2026-11-23 에 다시 확인했다. 최근 활동 절은 2026-11-08–2026-11-22 의 공개·관찰을 다루며 기초 침입이 그때 시작됐다고 가정하지 않는다.

1. 지원 업무 애플리케이션에도 보안 책임자가 필요하다. 금융위원회의 기간별 공개 집단과 금융보안원 사례는 핵심 거래 시스템 밖의 고객·직원·평가 정보가 중요한 이유를 보여준다. 실제 권한과 정보에 따라 객체 접근, 내보내기, 인증 의존 관계를 검토하라. [S5][S6]

2. 가시적 갈취는 복구 투자의 근거지만 모든 결과를 입증하지 않는다. Ransompedia의 대한민국 게시 수는 73 건이며 2025 년 전체는 41 건이다. 가장 큰 산업 분류는 제조업으로 게시 19 건이다.

부분 연도와 전체 연도 총계는 같은 기간의 증가율이 아니다. [S2]

3. 광고 수량은 영향을 판단하기 전에 단위를 확인해야 한다. 사례에는 대출 정보, 의료 테이블, 업무 시스템 묶음, 기술 문서가 포함된다. 행, 계정, 파일, 사람은 서로 대체할 수 없다.

보고서는 광고 파일의 진위를 확인하거나 성공한 거래를 추론하지 않는다. [S1]

4. 최근 공개에는 통합 총계보다 통제된 갱신이 필요하다. 대학·공급업체 설명은 서로 다른 서비스와 변하는 범주를 다룬다. 시스템별 기록 합계가 반드시 고유 인원은 아니다.

프로그램 하위 집단을 공급업체 전체 수에 더해서도 안 된다. 제 5 장은 각 경계를 유지한다.

5. 분석에서 조치로 옮겨도 출처의 확신도를 유지해야 한다. Genians는 연구에서 Kimsuky 연관성을 중간 수준의 확신으로 평가하며 모방 가능성을 열어 둔다.

AhnLab의 별도 국내 검토는 관찰 집단 전체를 한 그룹에 귀속시키지 않으면서 행위에 주의를 기울일 근거가 된다. [S14][S15]

6. 선정 포트폴리오는 확인 업무를 지원하며 전국 발생 비율 추정이 아니다. 후보 도메인 250 개는 통합한 열 개 부문에 각각 25 개씩 속한다.

소유, 관련 기업 집단, 확인 불가 관찰이 해석을 제한한다. 선정 도메인 250 개 중 121 개에 관련된 자격 증명 판매가 확인 시점에 관찰됐다.

국가 Atlas 대표값은 100 점 중 54 다. 활성 계정을 먼저 확인하라. [S3]

경영진을 위한 네 가지 판단

1. **신원 경보 확인 책임을 정하라.** 내부 또는 제공업체 경보 경로를 마련하고 관련 제안을 활성 계정·권한·세션과 대조하라. 각 경보에는 날짜가 있는 처리 결과가 필요하다. 추가 증거가 뒷받침하는 현재의 악용은 즉시 사고 대응으로 넘겨라.
2. **외부 업무 인터페이스를 검토하라.** 고객·협력사·직원·지원 애플리케이션을 목록화하라. 인증된 이용자가 허용된 정보에만 접근하는지 시험하고 모든 민감 인터페이스에 업무 책임자를 지정하라.
3. **공급업체와 고객 보호를 함께 훈련하라.** 공급업체가 보유한 기록, 초기 통지 발신자, 접근 증거 보존자를 확인하라. 정확한 개인정보를 아는 발신자를 가정해 복구와 지급 변경을 시험하라.
4. **복원과 사실 중심 소통을 입증하라.** 독립된 복구 자격 증명으로 핵심 서비스를 복원하라. 주장, 확인된 서비스 영향, 확인된 정보 범위를 구분하는 안내를 연습하라.

올해의 수치

73

요청된 2026 년 기간의 대한민국 게시 주장

측정하지 않는 것

확인된 침입이나 고유 조직

41

같은 시점 데이터의 2025 년 전체 대한민국 게시

측정하지 않는 것

같은 기간 길이의 기준선

12 / 8 / 6

N0n / Qilin / Metaencryptor 게시 명칭

측정하지 않는 것

고유 운영자나 확인된 결과

146 / 122 / 67 / 110

일본 / 대만 / 홍콩 / 싱가포르 게시수

측정하지 않는 것

국가 보안 순위

250

통합한 열 개 부문의 선정 후보 도메인

측정하지 않는 것

전국을 대표하는 표본

26

주장·공개 출처 설명에 걸친 상세 보고서 사례

측정하지 않는 것

전국 사고 건수

24

일부를 가린 출처 게시물 카드

측정하지 않는 것

고유 사고나 진위가 확인된 파일

39,733

확보한 국가 연관 게시물 측정

측정하지 않는 것

공격 빈도나 손실

비교 대상 국가는 맥락을 제공하기 위한 예시로만 선정되었으며, 순위나 정치적 평가를 의미하지 않습니다.

핵심 요점

01

신원·애플리케이션 확인 판단의 책임을 정하라.

02

주장, 공식 공개, 변하는 집단을 구분하라.

03

완료 증거를 갖추고 공급업체 대응, 고객 보호, 복원을 시험하라.

보고서 지도

자신이 책임지는 판단에서 시작해 증거, 한계, 완료 시험을 따라가라.

이사회·경영진	서비스·정보 회복력에 예산 배정	이동 1 5 11 12
CISO·보안 책임자	관련 신호·의존 관계의 우선순위 설정	이동 3 4 5 7 12
SOC·위협 인텔리전스팀	주장과 추가 증거로 뒷받침된 행위 구분	이동 4 6 7 부록 B
사기 대응·고객 운영팀	재사용 정보가 피해 행위의 권한을 부여하지 못하게 방지	이동 5 8 9
개인정보 보호·법무·구매팀	적용 범위·공급업체 책임 판단	이동 5 9 10 12

관찰은 자료나 측정 결과를 보유한다는 뜻이다. **주장**은 게시자나 갈취 게시가 어떤 결과를 내세운다는 뜻이다. **공식 설명**은 조직이나 당국이 보고한 범위 안에서 사실을 밝힌다는 뜻이다.

분석가 추론은 빠진 증거를 채우지 않으면서 증거를 판단에 연결한다. **출처의 공격자 평가**는 확신도와 대안을 포함한 인용 연구자의 판단으로 유지한다.

장 02

대한민국의 디지털·보안 환경

02

이 장에서 답하는 질문

대한민국의 연결된 경제에서 어떤 특성을 보안 의사결정에 반영해야 하는가?

96.9%

DataReportal 연말 추정치의 인터넷 이용률

2.1 연결성은 의존 관계를 만든다 10

2.2 주변 업무 시스템에도 명확한 책임이 필요하다 10

2.3 사이버 첩보와 범죄 활동은 별도로 설명해야 한다 10

2.4 정치적 맥락은 공격자 식별의 증거가 아니다 11

2.5 여러 감독 기관에는 각각의 신고 판단이 필요하다 11

장 02

대한민국의 디지털·보안 환경

요약

공통 인증·업무 소프트웨어·통신은 조직들을 연결한다. 공개 사건은 결제시스템이 관련되지 않아도 주변 업무앱이 중요함을 보여준다. 첩보 연구는 업무서신·문서 미끼를 설명한다. 서비스 의존성·개인정보 의무·출처별 공격자 평가를 구분하라. 인증·정보반출·지급변경·핵심서비스 복구 권한자를 파악하라.

2.1 연결성은 의존 관계를 만든다

DataReportal의 Digital 2027 판은 대한민국의 인터넷 이용자를 5,000만 명, 이용률을 96.9% 로 제시한다. 기초 인터넷 추정치는 2026 년 시월 기준이다.

모바일 회선은 6,140만 개, 소셜 미디어 이용자 계정은 4,960만 개로 보고한다. 회선과 계정은 고유한 사람 수가 아니다. [S8]

이 수치는 공격 빈도가 아니라 조직이 활동하는 환경을 설명한다. 조직은 모바일 애플리케이션, 메시지, 웹사이트, 외부 고객 지원을 통해 고객과 접촉한다. 보안 경계는 이러한 관계를 따라 기업 네트워크 밖으로 이어진다.

따라서 유용한 목록은 각 주요 서비스를 인증 제공자, 데이터 책임자, 공급업체, 복구 채널과 연결해야 한다. 누가 문서를 조회하거나 이용자의 접근 권한을 재설정할 수 있는지도 보여줘야 한다. 서버 목록만으로는 이 질문에 답할 수 없다.

은행의 영업 지원 애플리케이션은 예금을 처리하지 않더라도 민감한 고객 정보를 보유할 수 있다. 대학의 교육 포털은 모든 교내 서비스를 중단시키지 않고도 신원 정보를 노출할 수 있다. 각 애플리케이션의 실제 권한과 데이터를 대응의 기준으로 삼아야 한다.

2.2 주변 업무 시스템에도 명확한 책임이 필요하다

금융위원회의 십일월 대책은 외부 인터페이스, 직원용·내부 업무 애플리케이션, 개발 환경, 연계 업무 시스템을 명시적으로 포함한다. 핵심 거래 플랫폼 밖의 시스템도 가치 있는 정보를 보유할 수 있다는 점에서 이 범위는 중요하다. [S5]

방어 관점의 시사점은 이러한 애플리케이션에도 운영 시스템과 같은 업무 책임을 부여하는 것이다. 각 시스템에는 책임자, 지원되는 소프트웨어, 접근 권한 검토가 필요하다. 인증되지 않은 이용자가 다른 사람의 기록을 얻을 수 없다는 증거도 필요하다.

중앙 보안 정책이 있어도 구매는 부서별로 이뤄질 수 있다. 부서는 행사, 교육, 마케팅, 평가 서비스를 발주할 수 있다. 계약에는 필요한 정보, 이용 가능한 기간, 사고 후 접근 기록을 보존할 주체를 명시해야 한다.

이는 공개된 사건의 작동 방식에서 도출한 계획상의 시사점이다. 모든 한국 조직이 같은 구조를 갖거나 이러한 통제를 빠뜨렸다는 조사 결과가 아니다.

2.3 사이버 첩보와 범죄 활동은 별도로 설명해야 한다

Genians의 십일월 연구는 세미나 참석자를 겨냥한 표적 서신 교환을 다룬다. AhnLab의 시월 국내 활동 검토는 악성 바로가기와 문서를 미끼로 한 전달 방식을 설명한다.

이 자료는 신뢰하는 업무 절차와 단말 행위에 주의를 기울일 근거가 된다. 국내 사이버 첩보의 발생 비율을 입증하지는 않는다. [S14][S15]

지하 시장 광고는 다른 역할을 한다. 누군가 정보를 제안하거나 접근 권한을 요청했다는 사실은 보여줄 수 있다. 파일의 출처, 성공한 침입, 운영자의 신원을 독립적으로 입증하지는 않는다.

랜섬웨어 게시 역시 범죄자의 주장이다. 출처가 부여한 국가·산업 분류는 게시물 집단을 설명한다. 기업 소유 관계, 모든 운영 지역, 해당 조직의 암호화 피해 여부를 확정하지는 않는다.

2.4 정치적 맥락은 공격자 식별의 증거가 아니다

작성자는 정부, 정당, 정치인, 선거, 대외 관계에 대해 입장을 취하지 않는다. 정치적 소재, 한국어 문장, 익숙한 악성코드 이름만으로 운영자를 식별할 수 없다.

이 보고서는 2024 년 십이월 계엄령 사태와 그 이후 상황, 2025 년 대통령 선거를 사이버 사고의 책임 주체를 추론하는 근거로 사용하지 않는다. 해당 사건은 관찰 기간 이전에 발생했다.

캠페인이 공직을 언급한 경우에는 사칭과 접근 권한 측면의 영향을 검토한다.

북한, 중국, 일본에 관한 설명은 인용 출처가 공격 주체를 지목하거나 지역 비교에 국가명이 필요한 경우에만 등장한다. 출처의 확신도와 대안 설명도 함께 유지한다.

2.5 여러 감독 기관에는 각각의 신고 판단이 필요하다

개인정보 보호, 금융 감독, 기술적 사고 대응은 겹치지만 서로 다른 질문을 다룬다. 개인정보보호위원회의 신고 안내는 일반 개인정보 사고와 금융 분야의 개인신용정보를 구분한다. 금융회사는 신고 경로를 금융감독원과 협의하도록 안내된다. [S9]

실무적으로는 사고 전에 의사결정 책임자를 정해야 한다. 법무·개인정보 보호팀은 적용 의무를 판단하고, 기술 대응팀은 증거를 보존하며, 업무 책임자는 서비스 영향을 설명한다. 한 채널로 신고했다고 모든 의무를 이행했다고 가정해서는 안 된다.

핵심 요점

01
각 주요 서비스의 인증, 데이터, 공급업체 관계를 파악하라.

02
주변 업무 애플리케이션이 보유한 정보와 권한에 따라 조사하라.

03
출처의 확신도를 유지하고 사고 전에 신고 책임을 정하라.

장 03

조직 관련 노출과 외부 공개 서비스의 보안 상태

이 장에서 답하는 질문

선정 도메인의 관찰 결과는 무엇을 뒷받침하며, 증거의 한계는 어디에서 시작되는가?

250

통합한 열 개 부문에 속한 후보 도메인

3.1 조사 대상 정보 13

3.2 노출 신호와 한계 13

3.3 이메일과 웹 관찰 결과 17

3.4 자산 책임자를 위한 대응 순서 19

3.5 포트폴리오가 답할 수 없는 질문 20

장 03

조직 관련 노출과 외부 공개 서비스의 보안 상태

요약

선정 도메인 250개 중 121개에서 관련 자격증명 판매가 관찰됐다. 국가 Atlas 대표값은 100점 중 54다. 기기연관·과거기록은 따로 검증하라. 목적표본은 전국 발생률을 추정하지 않으며 도메인들의 소유자가 같을 수 있다. 활성계정·직원기기를 확인하고 책임자와 메일통제 변경을 계획하라.

3.1 조사 대상 정보

항목	정의
선정 대상	열 개 부문에 걸친 대표 도메인 후보 250 개
부문 범위	부문별 도메인 25 개, 관련 활동은 통합
선정 기준	시스템상 역할, 공공 서비스 기능, 부문 범위이며 매출 순위가 아님
단위	선정한 도메인 하나. 전체 포트폴리오의 법인 소유 독립성은 확인되지 않음
관찰일	2026-11-22. 확인할 수 없었던 항목은 미상으로 유지
해석	설정 관찰은 사고나 계정 확인과 구분됨
국가 차원의 추론	포트폴리오로 전국 발생 비율을 추정할 수 없음

포트폴리오는 중앙·지역 행정, 은행·결제, 보험·자본시장, 교육·연구, 산업·기술, 에너지·인프라, 운송·물류, 통신·소비자 서비스, 보건·생명과학을 포함한다.

여러 도메인이 같은 기업 집단이나 서비스 제공업체에 속할 수 있다. 대표 도메인 하나가 여러 이용자 집단에 서비스를 제공할 수도 있다. 예를 들어 대학과 연결된 로그인 정보만으로 이용자가 학생이 아니라 교직원이라고 판단할 수 없다.

3.2 노출 신호와 한계

선정 도메인 250 개 중 121 개에 관련된 자격 증명 판매가 확인일 2026-11-22 에 관찰됐다. 국가 Atlas 대표값은 100 점 중 54 다. 목적에 따라 선정한 포트폴리오이며 전국 발생 비율을 추정하지 않는다. [S3]

121 of 250
관련 자격 증명 판매가 관찰된 선정 도메인

54 of 100
국가 Atlas 대표값

238 of 250
감염 기기 연관 기록이 있는 도메인

236 of 250
과거 자격 증명 기록이 있는 도메인

선정 도메인 121 개에 관련된 자격 증명 판매가 관찰된다

	현재 판매	기기 연관	자격 증명 연관	문서 연관
은행·결제	15/25	24/25	23/25	15/25
통신·소비자 서비스	17/25	25/25	25/25	17/25
교육·연구	14/25	25/25	25/25	24/25
에너지·인프라	2/25	23/25	25/25	12/25
의료·생명과학	10/25	22/25	22/25	6/25
산업·기술	8/25	22/25	22/25	14/25
보험·자본시장	17/25	25/25	24/25	17/25
중앙 행정	9/25	25/25	22/25	4/25
지역 행정	14/25	24/25	23/25	6/25
운송·물류	15/25	23/25	25/25	12/25

현재 판매는 산호색이다. 셀: 신호 관찰 도메인/선정 도메인. 출처: 선정 도메인 노출 관찰 [S3]. 2026년 11월 22일. 후보 도메인 250개, 부문별 25개. 중복·과거 연관 기록을 포함하며 전국 발생 비율이나 확인된 침입이 아니다.

부문	도메인	현재 자격 증명 판매가 있는 도메인	기기 연관 기록이 있는 도메인	과거 자격 증명 기록이 있는 도메인	문서 연관 기록이 있는 도메인
은행·결제	25	15	24	23	15
통신·소비자 서비스	25	17	25	25	17
교육·연구	25	14	25	25	24
에너지·기반 시설	25	2	23	25	12

부문	도메인	현재 자격 증명 판매가 있는 도메인	기기 연관 기록이 있는 도메인	과거 자격 증명 기록이 있는 도메인	문서 연관 기록이 있는 도메인
보건·생명과학	25	10	22	22	6
산업·기술	25	8	22	22	14
보험·자본시장	25	17	25	24	17
공공 행정	25	9	25	22	4
지역 행정	25	14	24	23	6
운송·물류	25	15	23	25	12
전체	250	121	238	236	127

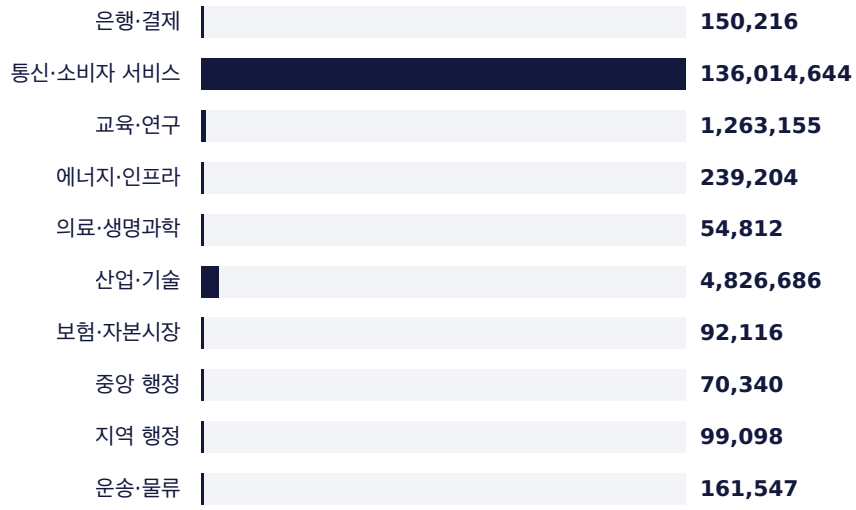
국가 Atlas 대표값만 공개한다. 부문별 항목과 차트 CSV는 법인이나 전체 기록 수가 아니라 각 신호가 있는 선정 대표 도메인 수를 센다.

열 사이에 중복이 있으므로 합산하면 안 된다. 현재 판매는 계정 확인의 근거이며 성공한 침입을 입증하지 않는다. [S3]

기기 연관 기록은 직원 분류 밖에 집중된다



자격 증명 기록 연관(별도 척도)



출처: 선정 도메인 노출 관찰 [S3]. 2026년 11월 22일. 후보 도메인 250개, 부문별 25개. 중복·과거 연관 기록을 포함하며 전국 발생 비율이나 확인된 침입이 아니다.

부문	기기 연관 기록	직원으로 분류된 기기 연관 기록	기타 기기 연관 기록	자격 증명 기록
은행·결제	55,600	152	55,448	150,216
통신·소비자 서비스	164,260	20,402	143,858	136,014,644
교육·연구	24,121	5,637	18,484	1,263,155
에너지·기반 시설	11,136	227	10,909	239,204
보건·생명과학	15,638	77	15,561	54,812
산업·기술	59,314	6,068	53,246	4,826,686
보험·자본시장	21,508	107	21,401	92,116
공공 행정	49,975	101	49,874	70,340
지역 행정	16,146	96	16,050	99,098
운송·물류	59,164	288	58,876	161,547
전체	476,862	33,155	443,707	142,971,818

포트폴리오에는 감염 기기 연관 기록이 476,862 건 있다. 직원 분류는 33,155 건, 기타 분류는 443,707 건이다. 총계는 고유 기기 수가 아니다. 직원 분류 밖 기기의 소유는 미확인이다.

조직 단말이 아니라 고객이나 다른 이용자의 기기가 포함될 수 있다. [S3]

과거 자격 증명 기록은 총 142,971,818 건이다. 유출 데이터베이스 기록 51,019,801 건, 정보 탈취 기록 11,103,468 건, 계정·암호 조합 목록 기록 80,848,549 건으로 구성된다.

관찰일에 보유한 누적 기록이며 2026 년에 처음 노출된 자격 증명 수가 아니다. 사람·출처·조직 사이에 기록이 중복될 수 있다. [S3]

스냅샷에는 문서 연관 기록 1,611 건과 이전 30 일의 유사 도메인 후보 46,750 개도 있다. 악성 출처, 현재 접근, 성공한 침입을 입증하는 수치가 아니다. 실제 내용과 소유를 바탕으로 문서와 후보 도메인을 확인하라. [S3]

조직이 자체 도메인에 영향을 주는 현재의 자격 증명 판매 제보를 받으면 먼저 계정을 확인해야 한다. 해당 계정이 조직 소유이고 여전히 활성 상태인지, 차단해야 할 권한이나 세션이 있는지 확인하라.

과거 기록이나 이미 조치한 관찰 결과는 별도로 기록하라.

기기 연관 기록, 자격 증명 기록, 문서, 언급, 유사 도메인 후보는 서로 다른 집단을 설명한다. 이를 합쳐 피해자 수로 만들어서는 안 된다.

기기 하나에 여러 서비스의 계정이 있을 수 있고, 한 사람이 여러 기록에 등장할 수 있다.

단순한 대화에서도 조직이 언급될 수 있다. 유사 도메인 후보가 해당 브랜드와 무관할 수 있다. 문서가 조직을 언급하더라도 그 조직의 시스템에서 나온 것은 아닐 수 있다.

이러한 한계는 다음 확인 단계를 정하는 기준이며, 관련 경보를 무시할 이유가 아니다.

3.3 이메일과 웹 관찰 결과

관찰	도메인
선정 도메인	250
설정 기록 확보	229
DMARC reject 관찰	5
DMARC quarantine 관찰	14
DMARC 모니터링 정책 관찰	108
DMARC 정책 미확인 (DMARC 미관찰 102 개와 DNS 확인 불가 21 개 포함)	123
SPF 레코드 관찰	205
DKIM 키 관찰	67
상위 영역 DS 관찰	2
CAA 관찰 (부록 D) [S122]	1
인증서 검증 관찰	197
인증서 검증 문제	7
인증서 관찰 불가	46

이 관찰은 선정한 도메인 250 개 전체를 분모로 사용한다. DNS 설정 기록은 도메인 229 개에서 확보됐고 21 개에서는 확인이 불가능했다.

도메인 250 개 중 127 개에서 DMARC 레코드가 관찰됐다(5 개 reject, 14 개 quarantine, 108 개 모니터링). DMARC 정책 미확인 123 개는 DNS 기록이 확보된 도메인 229 개 중 DMARC 미관찰 102 개와 DNS 확인 불가 도메인 21 개를 합한 수치다.

SPF, DKIM, DS, CAA 수치는 DNS 확인이 가능했던 도메인 229 개에서 관찰된 결과다. 인증서 관찰은 도메인 250 개 전체를 대상으로 한다(검증 197 개, 검증 문제 7 개, 관찰 불가 46 개). [S3]

웹 응답 관찰은 도메인 191 개에서 확보했다. 그 응답 중 HSTS 는 58 개, CSP 는 25 개, 프레임 제한은 50 개, 콘텐츠 유형 제한은 58 개에 나타났다.

응답에 관한 관찰이며 모든 애플리케이션의 적용 범위는 아니다. HSTS 와 CSP 의 뜻은 부록 D 에 설명한다. [S3][S120][S121]

부문별 설정 관찰은 등급이 아니라 건수다

	DMARC 거부	DMARC 격리	SPF	DKIM
중앙 행정	0/25	2/25	24/25	4/25
지역 행정	0/25	0/25	16/25	0/25
은행·결제	0/25	0/25	23/25	8/25
보험·자본시장	1/25	1/25	22/25	6/25
교육·연구	1/25	2/25	22/25	14/25
산업·기술	0/25	3/25	17/25	5/25
에너지·인프라	1/25	1/25	19/25	7/25
운송·물류	0/25	1/25	24/25	8/25
통신·소비자 서비스	1/25	4/25	22/25	10/25
의료·생명과학	1/25	0/25	16/25	5/25

출처: 선정 도메인의 공개 설정 관찰, 2026년 11월 22일 [S3]. 선정 도메인을 분모로 사용하며 관찰되지 않았다는 사실이 통제 부재를 입증하지 않는다.

부문	선정	DMARC reject	DMARC quarantine	SPF 관찰	DKIM 관찰
공공 행정	25	0	2	24	4
지역 행정	25	0	0	16	0
은행·결제	25	0	0	23	8

부문	선정	DMARC reject	DMARC quarantine	SPF 관찰	DKIM 관찰
보험·자본시장	25	1	1	22	6
교육·연구	25	1	2	22	14
산업·기술	25	0	3	17	5
에너지·기반 시설	25	1	1	19	7
운송·물류	25	0	1	24	8
통신·소비자 서비스	25	1	4	22	10
보건·생명과학	25	1	0	16	5

각 집단에는 선정 도메인 25 개가 있다. 수치는 신호 건수이며 부문 등급이나 침입 증거가 아니다. [S3]

DMARC 정책은 해당 도메인에서 보낸 것처럼 표시된 인증되지 않은 메일을 수신 시스템이 어떻게 처리할지 지정한다. 정책의 존재는 피싱 성공률을 측정하지 않는다.

모니터링 정책이 관리된 도입 과정의 일부일 수 있으므로, 집행 수준을 바꾸기 전에 정상 발신자를 파악해야 한다. [S94]

SPF 레코드는 허용된 발신 인프라를 설명한다. [S96] 공개된 DKIM 키는 해당 이름에 키가 있다는 증거이며 모든 메시지가 서명된다는 증거는 아니다. 키를 관찰하지 못했다면 도입 여부는 미확인 상태다. [S95]

상위 영역의 DS 레코드는 DNSSEC 검증에 쓰이는 연결 정보를 제공한다. 그 존재만으로 모든 응답에 유효한 신뢰 체인이 있다고 볼 수는 없다.

웹 인증서와 헤더 관찰도 응답한 서비스에 관한 것이며, 조직이 운영하는 모든 애플리케이션에 관한 것은 아니다.

3.4 자산 책임자를 위한 대응 순서

신호	최초 책임자	확인 사항	완료 증거
자격 증명 판매 제보	신원·계정 운영팀	소유, 활성 상태, 권한, 세션 검토	날짜가 있는 계정 처리 결과
기기 연관 기록	단말·신원 담당팀	자산과 계정 대조	관련 세션 차단 또는 관찰 건 종결
불확실한 메일 정책	메시징팀	정상 발신자와 인증 정렬 검토	승인된 정책 집행 계획
웹 인증서 문제	서비스 책임자	인증서 체인과 서비스 의존 관계	유효한 서비스와 갱신 책임 지정
유사 도메인 후보	브랜드 보호팀	소유와 실제 콘텐츠	분류 및 조치 기록
노출된 문서	데이터 책임자	출처, 접근 권한, 민감도	접근 수정과 영향 평가

업무 중요도와 뒷받침하는 증거에 따라 검토 순서를 정하라. 과거 기록 하나만으로 한 부문의 모든 이용자를 차단할 수는 없다. 반면 현재 활성화된 특권 계정이 확인되면 포트폴리오 요약을 기다리지 않고 즉시 차단할 근거가 될 수 있다.

3.5 포트폴리오가 답할 수 없는 질문

관찰 결과는 공격받은 한국 조직 수, 정보를 잃은 사람 수, 사고 중 통제의 작동 성과를 입증할 수 없다. 일치하는 증거 없이 지하 시장 제안과 공식 공개 사이의 관계를 확정할 수도 없다.

경영 보고에서는 검토가 필요한 관찰과 사고로 인정된 건을 구분하라. 완료한 확인 결과와 함께 소유 관계 미확인, 측정 불가 항목을 보고하라. 빈칸을 안심할 수 있는 영으로 바꿔서는 안 된다.

핵심 요점

01
선정 도메인 관찰 결과를 확인 업무 목록으로 다뤄라.

02
확인 불가 항목과 소유 관계의 불확실성을 드러내라.

03
담당 자산·계정 책임자의 증거로 각 경보를 종결하라.

장 04

다크웹과 포럼 증거

04

이 장에서 답하는 질문

보관한 게시물은 무엇을 입증하며, 어떤 주장을 조사해야 하는가?

8

서로 다른 증거 한계를 지닌 상세 주장 사례

4.1 조사 대상 정보 22

4.2 규모, 플랫폼, 언어 22

4.3 여덟 가지 주장 사례 27

4.4 추가 제안과 재유통 자료 35

4.5 최근 활동: 2026-11-08 부터 2026-11-22 까지 40

장 04

다크웹과 포럼 증거

요약

보관 자료에는 데이터·접근권한 광고, 요청, 재게시, 일반 시장대화가 섞여 있다. 게시물의 주장과 근거를 확인하라. 큰 수량은 사람보다 행·파일을 뜻하며 최근 게시도 과거 자료일 수 있다. 차단·공개소통·통지 판단 전에 출처·계정 관련성·주장 단위를 검증하라.

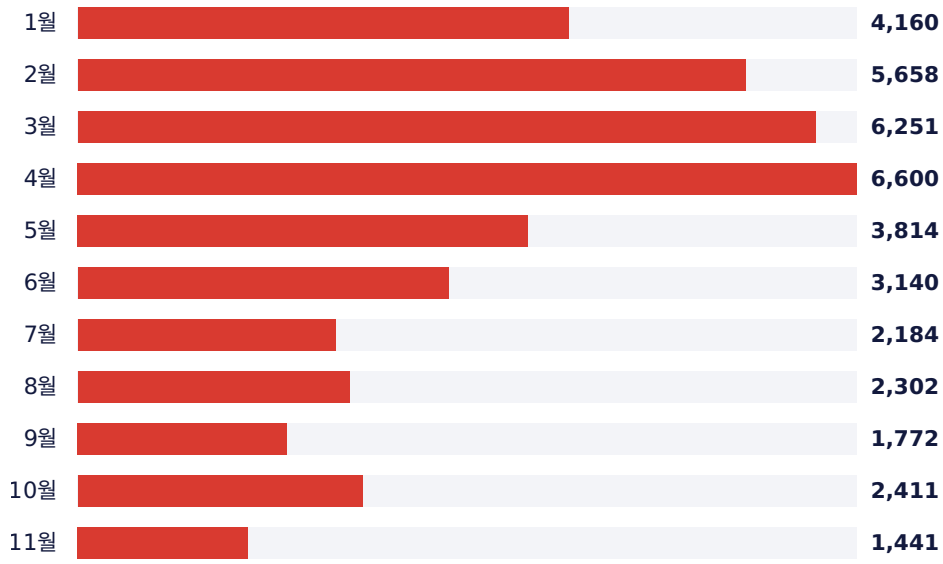
4.1 조사 대상 정보

항목	정의
출처	보관한 Brandefense Blackhole 게시물·광고
기간	게시 시각 2026-01-01 부터 2026-11-22 까지
국가 연관	확보 출처 자료의 대한민국 언급이며 표적화가 확인된 것은 아님
측정 규모	39,733
단위	게시물 하나. 서로 다른 기록이 같은 출처 발언을 반복할 수 있음
미확인 사항	파일 진위, 최초 획득일, 성공한 판매, 지속 접근

4.2 규모, 플랫폼, 언어

보관 증거에는 게시물 기록 39,733 건이 있으며 구체적인 주장과 더 넓은 맥락이 함께 포함된다. 이는 전국 사고 총계나 범죄 활동의 대표 표본이 아니다. 게시 날짜는 침입 시작이 아니라 공개·유통 시점을 설명한다. [S1]

월별 게시물 관찰은 침입 시작이 아니라 유통을 설명한다



출처: Odin by Brandefense의 보관 대한민국 관련 게시물 관찰, 2026년 1월 1일–11월 22일, 마감일 일부 [S1]. 보관 게시물과 국가 태그 게시물은 별도 집단이며 공격 건수가 아니다.

게시 월	보관 기록
2026-01	4,160
2026-02	5,658
2026-03	6,251
2026-04	6,600
2026-05	3,814
2026-06	3,140
2026-07	2,184
2026-08	2,302
2026-09	1,772
2026-10	2,411
2026-11	1,441
합계	39,733

플랫폼별 수치는 보관 증거 집단을 설명한다

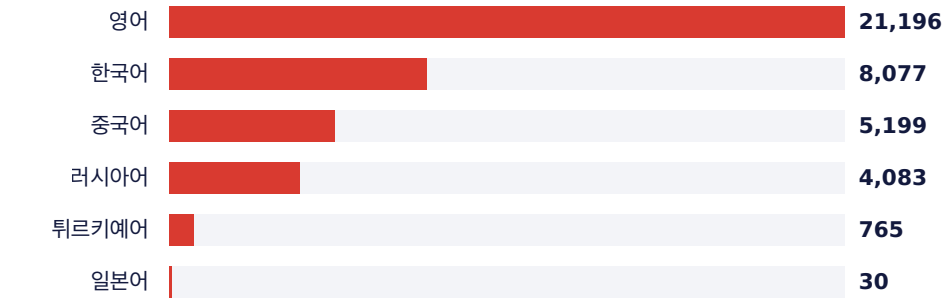


출처: Odin by Brandefense의 보관 대한민국 관련 게시물 관찰, 2026년 1월 1일–11월 22일, 마감일 일부 [S1]. 보관 게시물과 국가 태그 게시물은 별도 집단이며 공격 건수가 아니다.

플랫폼	보관 기록
telegram	38,899
forum	707
discord	72
paste	55

플랫폼별 수치는 확보된 증거 집단을 반영한다. 시장 점유율, 공격 성공, 플랫폼별 안전성을 측정하지 않는다.

언어 표시는 운영자의 국적을 입증하지 않는다



출처: Odin by Brandefense의 보관 대한민국 관련 게시물 관찰, 2026년 1월 1일–11월 22일, 마감일 일부 [S1]. 보관 게시물과 국가 태그 게시물은 별도 집단이며 공격 건수가 아니다.

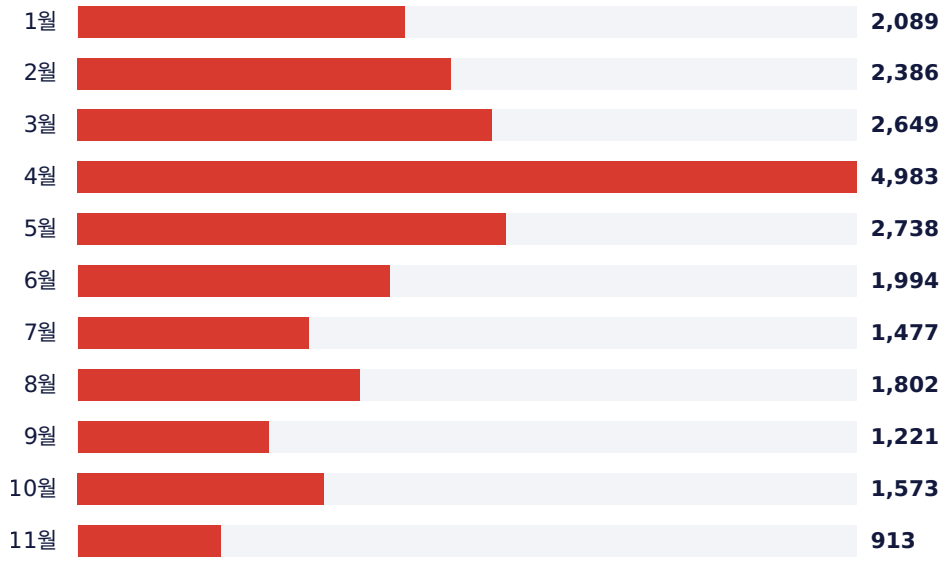
언어 표시	보관 기록
영어	21,196
한국어	8,077
중국어	5,199
러시아어	4,083
튀르키예어	765
일본어	30

언어 표시는 서로 겹칠 수 있고 모든 보관 기록을 포괄하지 않는다. 위 표시 수를 더해 새로운 게시물 총계를 만들거나 운영자의 국적을 추론해서는 안 된다. [S1]

Brandefense Blackhole에는 2026-01-01–2026-11-22 날짜의 국가 태그 게시물 23,825 건이 있다. 태그 게시물 집단이며 관련 사고나 확인된 표적 공격의 수가 아니다. 보관 연구 집단과 겹치므로 합산하면 안 된다. 십일월은 부분 월이다. [S1]

보관 총계는 대한민국 언급을 다루고, 태그 총계는 국가 태그가 있는 게시물을 센다. 범위가 다르므로 보관 총계가 더 클 수 있다. [S1]

국가 태그 월별 수치는 확인된 사고가 아니라 게시를 설명한다



출처: Odin by Brandefense의 보관 대한민국 관련 게시물 관찰, 2026년 1월 1일–11월 22일, 마감일 일부 [S1]. 보관 게시물과 국가 태그 게시물은 별도 집단이며 공격 건수가 아니다.

월	태그 게시물
2026-01	2,089
2026-02	2,386
2026-03	2,649
2026-04	4,983
2026-05	2,738
2026-06	1,994
2026-07	1,477
2026-08	1,802
2026-09	1,221
2026-10	1,573

월	태그 게시물
2026-11	913
합계	23,825

다음 언어 수치는 위 보관 증거 표가 아니라 국가 태그 집단에 관한 것이다. 언어 표시는 서로 겹칠 수 있고 국적을 입증하지 않는다. [S1]

언어 표시	태그 게시물
KO	3,521
EN	11,048
RU	2,013
ZH	5,059
JA	25
TR	646

많은 게시물은 많은 사고를 입증하지 않는다. 세계 시장 목록은 대한민국을 여러 시장과 함께 나열할 수 있다. 새 침입이 없어도 회신, 복제 게시, 갱신된 제안이 이어질 수 있다.

특정 주장을 판단할 때는 사례 증거를 사용하라. 합계 규모는 보관한 출처 집단을 설명하는 데 사용하라. 어느 쪽도 단독으로 대한민국의 피해 규모나 공격자에게 조직이 얼마나 잘 보이는지 입증하지 않는다.

4.3 여덟 가지 주장 사례

사례 A

A

판매 설명이 일치하지 않는 대출 데이터 광고

증거 카드 B01 | 2026년 3월 11일 | 포럼 | 금융 서비스 조직 한 곳

주장 미확인

주장	삼월 게시물은 대출 데이터셋 2 TB를 광고한다. 한국어 본문은 신원, 연락처, 주거, 직장, 대출 관련 필드를 설명하며 삼월의 현행 날짜를 주장한다. [S1]
연대기	2026-03-10 과 2026-03-11 의 관련 게시물은 독점 판매와 공개 배포라는 맥락을 모두 설명한다. 별개의 침입을 입증하지는 않는다.
확인된 증거	보관 자료는 관련 광고의 존재를 뒷받침한다. 정보의 진위나 최초 획득 주체를 확인하지는 않는다.
대안	실제 새 파일, 오래된 자료, 자료 통합, 재판매, 부정확한 광고 가능성이 남아 있다. 서로 다른 판매 설명은 완료된 독점 거래를 입증하지 않는다.
대응	관련 대출업체와 처리업체는 적법하게 확보할 수 있는 증거를 자체 내보내기 형식·접근 기록과 비교해야 한다. 사기 대응팀은 광고된 인적 사항에 의존하는 복구 절차를 검토해야 한다.

결론

차단·통지를 결정하기 전에 출처, 소유, 관련 내부 증거를 확인하라.

증거 카드 B01 — 2026년 3월 11일

FantancyHacker | 포럼 | 포럼 | 한국어

원문

이름, 주민번호, 전번, 집주소, 거주지, 직장직위, 돈 빌린 이유, 동거자 기타 ...

번역

이름, 주민등록번호, 전화번호, 집 주소, 거주지, 직장 직위, 대출 이유, 동거인 및 기타 정보.

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거

보관 게시물은 금융 서비스 조직의 것으로 주장되는 대출 데이터베이스 판매·공개에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

사례 B

B

의료 데이터 행 수는 환자 집단을 식별하지 않는다

증거 카드 B02 | 2026년 1월 14일 | 포럼 | 의료 조직 한 곳

주장 미확인

주장	일월 광고는 병원 관련 데이터베이스를 설명한다. 제목, 전체 본문 수량, 환자 테이블 수량이 서로 다르다. [S1]
확인된 증거	본문은 다른 계정·이벤트·운영 행과 함께 환자 행 34,438 개를 나열한다. 더 큰 150만 수치를 환자나 고유한 사람 수로 볼 수는 없다.
대안	게시물이 겹치는 개인에 관한 여러 테이블, 과거 내보내기 자료, 부정확한 내용을 설명할 수 있다. 제시된 설명만으로 출처와 최신성을 확정할 수 없다.
한계	관련된 관리 접근 권한 제안도 주장이다. 보고서는 임상 서비스에 대한 현재 유효한 접근을 입증하지 않는다.
대응	데이터 책임자는 실제로 어떤 범주와 사람이 포함됐는지 확인한 뒤 임상 연속성과 통지를 별도로 검토해야 한다. 가장 큰 광고 총계로 고객 통지 규모를 정하지 마라.

결론

차단·통지를 결정하기 전에 출처, 소유, 관련 내부 증거를 확인하라.

증거 카드 B02 — 2026년 1월 14일

Solonik | 포럼 | 포럼 | 영어

원문

34,438 records

번역

기록 34,438 건

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거

보관 게시물은 의료 조직의 것으로 주장되는 병원 SQL 덤프 주장에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

고유 환자 총계, 현재 관리 접근, 진위가 확인된 파일, 확인된 침입일.

사례 C

같은 대화에서 이의를 받은 접근 제안

증거 카드 B03 | 2026년 3월 11일 | 포럼 | 공공기관 한 곳

주장 미확인

주장	삼월 판매자는 공공 분야 환경에 대한 것으로 주장하는 특권 접근을 광고하고 제안을 받는다. [S1]
확인된 증거	다른 참여자는 제시된 시스템 정보가 주장된 대상을 입증하는지 의문을 제기한다. 판매자는 제안이 데이터베이스나 트래픽 서비스가 아니라 접근 권한에 관한 것이라고 설명한다.
대안	실제 접근, 잘못 귀속된 인프라, 일반 시연 자료, 허위 광고 가능성이 남는다. 이의 제기는 관련 증거지만 조작을 입증하지는 않는다.
한계	성공한 내부 이동, 데이터베이스 탈취, 운영자 신원은 입증되지 않았다.
대응	관련 가능성이 있는 공공기관은 계정·호스트 소유를 비공개로 확인하고, 접근 증거를 보존하며, 추가 증거가 뒷받침하는 특권 세션을 조사해야 한다. 포럼 주장만으로 공개 침해 발표를 하기에는 부족하다.

결론

차단·통지를 결정하기 전에 출처, 소유, 관련 내부 증거를 확인하라.

증거 카드 B03 — 2026년 3월 11일

zSenior | 포럼 | 포럼 | 영어

원문

i am selling the Full Access Only

번역

전체 접근 권한만 판매한다

참고. 출처 대화에는 접근 증거에 대한 참여자의 이의 제기가 포함된다.

확인된 증거

보관 게시물은 공공기관에 대한 것으로 주장되는 특권 서버 접근에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

정부 소유, 성공한 내부 이동, 정보 탈취, 사용 가능한 접근, 완료된 판매.

사례 D

D ■ 하나의 제안에 등장하는 여러 업무 시스템

증거 카드 B04 | 2026년 4월 26일 | 포럼 | 회원 조직과 연계 고용주

주장 미확인

주장	사월 광고는 회원, 계정, 업무 관리, 인사, 직원 문서 자료를 묶는다. 공유·독점 조건을 제시한다. [S1]
확인된 증거	게시물은 여러 관련 서비스와 서로 다른 주장상 내보내기 날짜를 설명한다. 이는 여러 시스템을 묶은 제안 하나를 뒷받침하며, 이름이 나온 계열사마다 사고가 확인됐다는 뜻은 아니다.
대안	공통 관리, 공통 처리업체, 판매용으로 모은 무관한 파일, 오래된 백업, 부정확한 설명으로 묶음이 생겼을 수 있다.
한계	소유, 파일 진위, 접근의 최신성, 독점성은 미확인이다. 이전에 공개된 적이 없다는 판매자의 말은 독립 증거가 아니다.
대응	설명된 정보 범주를 보유할 수 있는 업무·공급업체 관계를 파악하라. 공통 진입점을 가정하기 전에 관계 전반의 특권 접근과 내보내기 권한을 검토하라.

결론

차단·통지를 결정하기 전에 출처, 소유, 관련 내부 증거를 확인하라.

증거 카드 B04 — 2026년 4월 26일

0xCAFE | 포럼 | 포럼 | 영어

원문

All of the data never exposed to public ever, and never used.

번역

이 데이터는 모두 공개된 적이 없으며 사용된 적도 없다.

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거

보관 게시물은 회원 조직·연계 고용주의 것으로 주장되는 여러 시스템 데이터베이스·직원 문서 판매에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

사례 E

E

가격을 제시한 원격 관리 접근 제안

증거 카드 B05 | 2026년 4월 28일 | 포럼 | 보험 분야 조직 한 곳

주장 미확인

주장	사월 판매자는 보험 분야 조직에 대한 것으로 주장하는 특권 원격 접근을 898 USD 에 제안한다. [S1]
확인된 증거	광고는 원격 근무 환경과 주장된 권한을 설명한다. 보고서가 확인하는 것은 제안이며, 사용 가능한 접근이나 계정 소유가 아니다.
대안	만료된 계정, 공급업체 환경, 잘못 표시한 대상, 실제 활성 세션 가능성이 남는다.
한계	판매자의 운영·사업 설명은 미확인이다. 피해자 프로필로 다시 제시하지 않는다.
대응	관련 보험사는 원격 접근 환경, 특권 계정, 세션을 확인해야 한다. 광고만으로 부문 전체를 재설정하지 말고, 추가 증거가 뒷받침하는 무단 사용을 사고 절차에 따라 차단하라.

결론

차단·통지를 결정하기 전에 출처, 소유, 관련 내부 증거를 확인하라.

증거 카드 B05 — 2026년 4월 28일

TunaFish | 포럼 | 포럼 | 영어

원문

$898 (BTC)

번역

$898 (BTC)

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거

보관 게시물은 보험 분야 조직에 대한 것으로 주장되는 특권 원격 접근 판매에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

사례 F

F

별도의 클라우드 관리자 제안

증거 카드 B06 | 2026년 8월 23일 | 포럼 | 보험 분야 조직 한 곳

주장 미확인

주장	팔월 게시물은 대한민국으로 표시된 보험사에 대한 것으로 주장하는 클라우드 소유자 접근 권한을 광고한다. [S1]
확인된 증거	보관 설명은 클라우드 관리자 권한을 명시한다. 네트워크 규모, 계정 소유, 현재 유효성, 거래는 입증되지 않았다.
관계의 한계	보관 증거에는 이 제안을 사례 E와 연결하는 요소가 없다. 같은 부문이라는 사실은 동일한 대상·판매자·접근 경로를 입증하지 않는다.
대응	클라우드·신원 담당팀은 관련 관리자 계정, 최근 역할 변경, 민감한 API 활동을 확인해야 한다. 내부 증거가 경보를 뒷받침하면 상시 자격 증명과 복구 경로를 검토하라.

결론

차단·통지를 결정하기 전에 출처, 소유, 관련 내부 증거를 확인하라.

증거 카드 B06 — 2026년 8월 23일

HighWayToShell | 포럼 | 포럼 | 영어

원문

Privilege ..... Cloud Admin (Owner)

번역

권한 ..... 클라우드 관리자(소유자)

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거

보관 게시물은 보험 분야 조직에 대한 것으로 주장되는 클라우드 관리자 접근 제안에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

사례 G

■ 마감 전 두 주 동안 광고된 기술 문서

증거 카드 B07 | 2026년 11월 12일 | 포럼 | 방위산업 공급업체 한 곳

주장 미확인

주장	2026-11-12 게시물은 방위산업 공급업체의 것으로 주장하는 기술 문서를 광고한다. 제목의 주장 용량은 536 G 로 제시된다. [S1]
확인된 증거	판매자는 전자전·레이더 관련 정보를 설명하고 사업 관계를 주장한다. 보고서는 광고를 보유하며 문서의 진위를 확인하지 않았다.
한계	주장된 고객 관계가 추가로 확인된 피해자를 만들지는 않는다. 전달, 지속 접근, 국가 연계는 입증되지 않았다.
대응	관련 가능성이 있는 공급업체는 엔지니어링·데이터 책임자를 참여시키고, 통제된 기술 저장소를 확인하며, 접근 증거를 보존해야 한다. 확인된 정보 범주에 따라 계약·공개 의무를 평가하라.

결론

차단·통지를 결정하기 전에 출처, 소유, 관련 내부 증거를 확인하라.

증거 카드 B07 — 2026년 11월 12일

taltikgoo | 포럼 | 포럼 | 영어

원문

We have obtained [a defence-sector supplier's] complete set of technical documents, including data on its electronic warfare and radar equipment.

번역

[방위산업 공급업체의] 전자전·레이더 장비 데이터를 포함한 전체 기술 문서 세트를 확보했다.

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거

보관 게시물은 방위산업 공급업체의 것으로 주장되는 기술 문서 판매 주장에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

진위가 확인된 기술 문서, 고객 침입, 전달, 지속 접근, 국가 연계.

사례 H

H ■ 조달 범주를 사람 수로 합산할 수 없다

증거 카드 B08 | 2026년 11월 19일 | 포럼 | 에너지 분야 조직 한 곳

주장 미확인

주장	2026-11-19 게시물은 에너지 분야 조직의 것으로 주장하는 개인정보, 공급업체, 입찰, 계약 기록을 광고한다. [S1]
확인된 증거	광고는 내부 이용자와 공급업체 관련 기록을 포함한 여러 범주를 설명한다. 범주는 겹칠 수 있으며 사람·회사·거래가 섞인다.
한계	제목의 크기 표현은 모호하다. 수억 명의 사람을 입증하지 않으며 범주별 수치는 고유한 사람 수의 합계가 아니다.
공식 출처와의 경계	에너지 분야 조직에 관한 이후의 공개는 제 5 장에서 별도로 다룬다. 주제나 필드 이름이 비슷해도 광고 파일의 진위나 동일한 획득 경로를 입증하지 않는다.
대응	관련 데이터 책임자는 내부 이용자, 외부 이용자, 공급업체, 조달 기록을 각각 대조해야 한다. 대상 집단 수치를 발표하기 전에 증거가 뒷받침하는 접근을 조사하고 영향받은 사람을 평가하라.

결론

차단·통지를 결정하기 전에 출처, 소유, 관련 내부 증거를 확인하라.

증거 카드 B08 — 2026년 11월 19일

Noiem | 포럼 | 포럼 | 영어

원문

Internal user PII 48,697

번역

내부 이용자 개인정보 48,697

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거

보관 게시물은 에너지 분야 조직의 것으로 주장되는 개인정보·조달 데이터셋 주장에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

고유 인원 총계, 합산 가능한 범주, 파일 진위, 이후 공식 공개와의 입증된 일치.

4.4 추가 제안과 재유통 자료

카드	게시 날짜	관측된 주장	한계
B09	2026-01-13	호스팅 서비스 자료 주장	호스팅 이름과 입주 서비스로 보이는 기록만으로 제공업체 전체 접근을 입증할 수 없음
B10	2026-03-01	인구·거래자 자료 공개 주장	과거 프로필 날짜와 대량 자료 제목이 새로운 국가 등록 시스템 침입을 입증하지 않음
B11	2026-03-10	전문 서비스·제조업 자료 공개 주장	한 글에 두 조직이 나와도 하나의 침입이 입증되는 것은 아님
B12	2026-03-30	대량 행 자료 제안	행은 검증된 고유 인원수가 아니며, 정부 출처는 입증되지 않음
B13	2026-03-31	대규모 커뮤니티 자료 광고	정형화된 설명과 예시성 표본 때문에 규모와 진위는 미확정
B14	2026-04-03	업무 시스템 데이터셋 제안	비슷한 스키마가 같은 백엔드나 거래 성립을 입증하지 않음
B15	2026-05-28	기술 문서 공개 주장	파일 크기 주장이 출처나 국가 귀속을 입증하지 않음
B16	2026-07-06	자동차 관련 자료 제안	출처 날짜가 모호해 새로운 침입이라고 판단할 수 없음
B17	2026-08-23	생명과학 업무 문서 주장	일부 압축파일과 과거 등재의 중복으로 출처와 최초 사고 날짜는 미확정
B18	2026-09-09	통신 자료 제안	추정 수량과 최초 사고 날짜는 미확인
B19	2026-10-07	상거래 고객 자료 유통	뒤늦게 나온 표본도 이어지는 같은 주장 계열에 속함
B20	2026-10-17	대학 채용·교직원 표	과거 표본 날짜와 서로 다른 행 범주 때문에 새로운 고유 인원수를 산정할 수 없음
B21	2026-11-08	최근 고객 관계 관리(CRM) 시스템 관리자 주장 [S123]	내보내기 주장과 제시된 스키마가 활성 접근 권한을 입증하지 않음
B22	2026-11-10	최근 교육 서비스 관리자 제안	플랫폼과 고객 자료에 관한 주장은 미확인

카드	게시 날짜	관측된 주장	한계
B23	2026-11-17	십일월 게시물 속 과거 회원 자료	제목 날짜가 현재 계정 유효성이나 새로운 탈취를 입증하지 않음
B24	2026-11-21	최근 금융 서비스 자료 광고	기록 수, 결제처럼 보이는 표본과 요구 가격은 파일 진위나 피해 인원을 입증하지 않음

증거 카드 B09 — 2026년 1월 13일

Solonik · 포럼 · 포럼 · 영어

원문

82 structured MySQL tables, ~144,000 rows total

번역

구조화된 MySQL 테이블 82 개, 총 약 144,000 행

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거
보관 게시물은 호스팅 서비스 환경의 것으로 주장되는 데이터베이스 덤프 주장에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항
파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

증거 카드 B10 — 2026년 3월 1일

INDOHAXSEC · 포럼 · 포럼 · 영어

원문

514.475 SOUTH KOREAN POPULATION AND TRADER DATA

번역

514.475 대한민국 인구·거래자 데이터

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거
보관 게시물은 전국 소비자·거래자 데이터셋의 것으로 주장되는 대량 개인정보 공개 주장에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항
파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

증거 카드 B11 — 2026년 3월 10일

ZeusHacking · 포럼 · 포럼 · 한국어

원문

[an aerospace organisation]과 [a professional-services organisation]의 데이터를 무료 공개.

번역

[항공우주 조직]과 [전문 서비스 조직]의 것으로 주장되는 데이터를 무료 공개.

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거
보관 게시물은 전문 서비스·제조 조직의 것으로 주장되는 한국어 무료 공개 주장에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항
파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

증거 카드 B12 — 2026년 3월 30일

GlitchX · 포럼 · 포럼 · 영어

원문

Total records: 9 Million Lines

번역

전체 기록: 900만 행

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거
보관 게시물은 소비자 데이터셋의 것으로 주장되는 전국 인구 데이터베이스 제안에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항
파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

증거 카드 B13 2026년 3월 31일

xorcat 포럼 포럼 영어

원문

Records: 15,000,000+ users

번역

기록: 이용자 15,000,000+ 명

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거

보관 게시물은 커뮤니티·토론 서비스의 것으로 주장되는 대형 데이터베이스 광고에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

증거 카드 B14 2026년 4월 3일

Grubber 포럼 포럼 영어

원문

Price: $1000

번역

가격: $1000

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거

보관 게시물은 상거래·교육 서비스의 것으로 주장되는 고객 관계 관리(CRM) 형태 데이터베이스 판매 제안 세 건에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

증거 카드 B15 2026년 5월 28일

포럼 참여자 포럼 포럼 영어

원문

South Korea [...] UAV [...] Documents [...] Size: 3.8 GB

번역

대한민국 [...] UAV [...] 문서 [...] 용량: 3.8 GB

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거

보관 게시물은 방위 관련 데이터셋의 것으로 주장되는 기술 문서 공개 주장에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

증거 카드 B16 2026년 7월 6일

AshleyWood2022 포럼 포럼 영어

원문

Full information [...] Database [...] South Korea 150K

번역

전체 정보 [...] 데이터베이스 [...] 대한민국 150K

참고. 출처의 연대기가 모호하며 표시 날짜가 새 침입을 입증하지 않는다.

확인된 증거

보관 게시물은 자동차 판매 플랫폼의 것으로 주장되는 데이터베이스 판매 주장에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

증거 카드 B17 2026년 8월 23일

updap 포럼 포럼 영어

원문

This is a partial data with dumped files from the company

번역

회사의 덤프 파일을 포함한 일부 데이터다

참고. 광고 또는 출처의 주장이다. 과거 갈취 등재와의 중복으로 최초 사고 날짜는 미확정이다.

확인된 증거

보관 게시물은 제약 분야 조직의 것으로 주장되는 업무·직원 문서 공개 주장에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

증거 카드 B18 2026년 9월 9일

[redacted] 포럼 포럼 영어

원문

Estimated Records: [quantity withheld] (reported)

번역

추정 기록: [수치 비공개](보고된 수치)

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거

보관 게시물은 통신 조직의 것으로 주장되는 가입자 데이터베이스 판매 주장에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

증거 카드 B19 2026년 10월 7일

updap 포럼 포럼 영어

원문

Customers database Total Records: +1m unique records

번역

고객 데이터베이스 전체 기록: +1m 고유 기록

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거

보관 게시물은 전자상거래 조직의 것으로 주장되는 고객 데이터베이스 공개 주장에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

증거 카드 B20 2026년 10월 17일

updap 포럼 포럼 중국어·한국어 주석

원문

[recruitment records] 第 7,806 行 [teaching records] 第 1902 行 [staff records] 第 1,569 行

번역

채용·교원·직원 관련 표본의 행 표시는 7,806, 1902, 1,569 이다.

참고. 행 표시는 전체 기록 수나 고유 인원수를 입증하지 않는다. 과거 표본 날짜도 함께 고려해야 한다.

확인된 증거

보관 게시물은 교육 분야 조직의 것으로 주장되는 채용·직원 데이터베이스 표본에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항

파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

증거 카드 B21 2026년 11월 8일

DataJava 포럼 포럼 영어

원문

this is an admin-side export rather than a scrape.

번역

이것은 스크래핑이 아니라 관리자 측 내보내기 자료다.

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거
보관 게시물은 디지털 서비스 조직의 것으로 주장되는 CRM 관리자·회원 데이터 판매에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항
파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

증거 카드 B22 2026년 11월 10일

DataJava 포럼 포럼 영어

원문

Access: full admin account in [an e-commerce administration environment].

번역

접근: [전자상거래 관리 환경]의 전체 관리자 계정.

참고. 광고 또는 출처의 주장이며 독립적으로 진위를 확인하지 않았다.

확인된 증거
보관 게시물은 교육 서비스 조직의 것으로 주장되는 관리자 접근·고객 기록 판매에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항
파일 진위, 새 침입, 현재 유효한 접근, 완료된 거래, 고유 피해 인원, 공통 운영자.

증거 카드 B23 2026년 11월 17일

thisversace 포럼 포럼 영어

원문

Databases From Korea [a consumer-services organisation] 17.11.2026

번역

한국의 [소비자 서비스 조직] 데이터베이스 17.11.2026

참고. 보이는 표본에는 이전 가입·로그인 날짜가 포함된다.

확인된 증거
보관 게시물은 소비자 서비스 조직의 것으로 주장되는 회원 데이터베이스 유통에 관한 것이다. 광고 내용은 미확인이다.

확인되지 않은 사항
제목 날짜의 새 사고, 현재 계정 유효성, 신뢰할 수 있는 대상 집단 수, 진정한 출처.

증거 카드 B24 2026년 11월 21일

tet 포럼 포럼 영어

원문

Total records : 43.19M Price : 500 $

번역

총 기록 : 43.19M 가격 : 500 $

참고. 정확한 원문 시각이 미확정인 광고다. 반복적인 표본 패턴은 진위에 의문을 제기하지만 조작을 확정하지는 않는다.

확인된 증거
금융 서비스 자료 광고는 기록 43.19M 건과 요구 가격 500 USD 를 제시한다. 이는 광고된 기록 수이며 확인된 사람이나 결제 건수가 아니다.

확인되지 않은 사항
파일 진위, 활성 접근 권한, 유효한 결제, 거래 성립 또는 피해 인원 43.19M 명.

출처: [S1].

표본의 시점으로 포함 자료 일부가 오래됐음을 알 수는 있어도 광고 파일의 모든 행의 시점을 알 수는 없다. 마찬가지로 제목에 2026 년이 있어도 새 사고를 입증하지 않는다. 두 한계를 모두 유지하라.

별도 2026-03-23 게시물은 해운·물류 조직과 관련된 VPN 접근 권한을 10,000 USD 에 광고한다. 신원, 활성 접근 권한, 거래 성립은 미확인이다. 주변 채널명으로 판매자의 소속을 판단할 수 없다. [S1]

2026-10-13 에 관찰한 반복적인 대학 기반 시설 제안은 특권 호스트 접근을 설명하며 300 USD 를 요구한다. 광고된 권한, 자산 관계, 활성 접근은 미확인이다. 반복 게시가 별도 침입이나 거래 성립을 입증하지 않는다. [S1]

구월과 시월에 대중교통 관련 웹사이트 접근 광고가 반복해서 나타난다. 유효한 접근 권한, 항공 운영, 운항 시스템 접근을 입증하지 않는다. 소유자는 범위나 차단을 판단하기 전에 광고된 자산을 해당 웹 애플리케이션과 대조하라. [S1]

더 이른 2026-01-17 해운 관련 제안은 50,000 USD 를 요구한다. 이후 접근 광고와의 관계, 접근 유효성, 거래 여부는 미확인이다. 지방 공공 서비스의 웹사이트 접근 광고도 자산별 확인이 필요하며 정부 전체의 접근 권한을 입증하지 않는다. [S1]

4.5 최근 활동: 2026-11-08 부터 2026-11-22 까지

카드	날짜	역할	증거 상태
B07	2026-11-12	방산 공급업체	광고 또는 유통이며, 내용은 미확인
B08	2026-11-19	에너지 부문 조직	광고 또는 유통이며, 내용은 미확인
B21	2026-11-08	디지털 서비스 조직	광고 또는 유통이며, 내용은 미확인
B22	2026-11-10	교육 서비스 조직	광고 또는 유통이며, 내용은 미확인
B23	2026-11-17	소비자 서비스 조직	광고 또는 유통이며, 내용은 미확인
B24	2026-11-21	금융 서비스 자료	광고 또는 유통이며, 내용은 미확인

관리자 제안, 기술 문서, 조달 기록과 과거 회원 자료는 서로 다른 주장이다. 이를 합쳐 피해 인원을 계산하거나 단일 운영자와 연결하지 않는다. [S1]

2026-11-16 광고는 여러 국가의 항목 중 지방 공공 서비스 웹사이트를 나열한다. 이전 제안과 같은 접근 권한, 새로운 침입 날짜, 운영자 전체의 범위를 입증하지 않는다. 광고된 개별 자산은 별도 검증 업무로 다뤄야 한다. [S1]

최근 활동 절은 게시와 제안을 설명한다. 정보가 처음 획득된 시점은 추론하지 않는다. 게시물의 연대기가 이전 관찰과 일치하지 않으면 해당 구간의 새 공격 증거로 사용하지 않는다.

핵심 요점

01
제안된 접근, 광고된 정보, 확인된 사고를 구분하라.

02
영향을 산정하기 전에 주장 단위와 출처를 확인하라.

03
최근 게시를 최근 침입의 증거가 아니라 확인을 시작할 신호로 다뤄라.

장 05

공개 사고와 부문별 표적 활동

05

이 장에서 답하는 질문

조직과 당국은 실제로 무엇을 보고했으며, 대응은 어떻게 달라지는가?

2

각 사례에 붙는 시간축: 사건과 공개

5.1 부문별 대응 지도 42

5.2 연초 사고와 캠페인 경고 43

5.3 관리자·개발자·소프트웨어 공급망 캠페인 44

5.4 소비자 서비스와 공공 분야 캠페인 보고 47

5.5 범죄적 갈취와 AI 주장 49

5.6 최근 활동: 2026-11-08 부터 2026-11-22 까지 49

5.7 최근 기술 권고는 피해 사고가 아니다 55

5.8 후속 조치와 제외 사항 55

5.9 부문 전반의 판단 56

장 05

공개 사고와 부문별 표적 활동

요약

공개 증거는 랜섬웨어·피싱·업무앱 노출·공급업체 의존성을 다룬다. 캠페인 공지·정책발표는 확인된 사고와 구분한다. 최근 공개에는 실수로 배포된 문서와 십일월에 새로 보고된 이전 활동도 있다. 확인된 방식과 영향받은 정보에 따라 책임자를 정하고 모든 대응판단에 미확인 범위를 명시하라.

5.1 부문별 대응 지도

아래 행은 서로 다른 증거 유형을 함께 보여주되 사고 총계로 합치지 않는다. 미확인 주장에는 표시를 유지한다. 근거 없는 비교를 피하도록 관련 서비스와 작은 부문을 묶었다.

부문	뒷받침되는 사례	증거 유형	최초 대응
공공 행정	QR 미끼, 사칭, 공통 메일 조사	공식 캠페인 공지·공개	업무 흐름·세션·서비스 범위 확인
금융·보험	기간이 명시된 부문 신고, 평가 시스템 노출, 별도 접근 광고	공식 보고와 미확인 주장	인터페이스 검토와 계정 확인
교육·연구	교육·연구·행정 포털 공개	공식 공지와 출처가 명시된 보도	접근 로그 보존과 기록 범주 대조
산업·방위	기술 문서 제안, 개발자·관리자 미끼	주장과 공식 캠페인 경고	엔지니어링·특권 접근 책임자 참여
에너지·인프라	개인정보·조달 데이터 주장과 별도 공개	주장과 공식 설명을 구분	영향 시스템·정보 대조
통신·소비자 서비스	스트리밍 서비스 조사와 가짜 설치 프로그램 배포	감독 기관·CERT 보고	데이터베이스 접근·고객 메시지 검토
보건·생명과학	의료 데이터 제안과 공식 랜섬웨어 경고	미확인 주장과 캠페인 증거	임상 연속성과 정보 영향 구분
운송·여행	지급 메시지에 재사용되는 예약 정보	공식 경고	기존 연락처로 지급 요청 확인
업무 공급업체	교육·공통 서비스 접근 공개	언론이 보도한 회사 설명	개인정보처리자의 기록과 공급업체 증거 파악

5.2 연초 사고와 캠페인 경고

사례 I

데이터 범위가 아직 구체화 중인 교육 기업 집단의 중단

교육·업무 서비스

공식 공개. 범위 한계 유지

공식 설명	2026-01-12 에 게시된 회사 공지는 2026-01-10 에 탐지한 내부 시스템의 비정상 활동을 설명한다. 격리와 랜섬웨어 의심에 대한 조사를 보고한다. [S49][S50]
후속 보도	2026-01-14 보도는 일부 데이터 탈취를 인정한 회사의 후속 설명을 다루지만, 고객 정보 포함 여부는 미확인으로 남겼다. 큰 회원 수가 확인된 데이터 반출 건수는 아니다. [S47]
대응	복원과 고객 데이터 평가를 별도 업무로 시험하라. 최초 발견, 이후 기술 결과, 변하는 대상 집단을 소통에서 구분하라.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

추가 공개: 의료 영상 서비스 가용성

2026-01-27 국내 보도는 영상 판독 업무에 영향을 준 병원의 2026-01-26 랜섬웨어 사건과 당일 오후 복구를 설명한다. 보도 시점에 환자정보 유출이나 수술·진료 중단은 보고되지 않았다고 전한다. 이는 해당 시점 보도의 범위 설명이다. [S104]

사례 J

정부를 사칭한 QR 코드가 판단을 휴대전화로 옮긴다

정부를 사칭한 접근

공식 캠페인 설명. 국내 범위 미확인

공식 설명	KISA의 2026-01-10 공지는 정부·연구기관 관계자를 사칭한 QR 코드 미끼를 설명한다. 의도한 결과에는 악성 모바일 앱 설치나 자격 증명 입력이 포함된다. [S19]
한계	공지는 탐지된 캠페인 행위를 보여주지만 전국 피해 집단을 열거하거나 사칭당한 기관에 침입했음을 입증하지 않는다.
대응	알려진 연락처로 문서·지급 절차를 확인하라. QR 목적지도 이메일 링크와 같은 수준으로 살피고, 모바일 이용자에게 승인된 신고 경로를 제공하라.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

KISA의 2026-01-06 공지는 국내 웹사이트와 관련된 포럼 연관 정황도 설명한다. 이월 경고는 보건·교육·ICT 분야의 랜섬웨어 위험에 초점을 둔다. 이는 캠페인 관찰과 경고이며 서로 다른 확인 조직의 수가 아니다. [S18][S20]

5.3 관리자·개발자·소프트웨어 공급망 캠페인

K

사례 K

유용해 보이는 도구가 특권 이용자를 겨냥한다

관리자·개발자 도구

공식 캠페인 설명. 국내 범위 미확인

공식 설명	KISA의 2026-03-11 공지는 일반적인 관리자·개발자 도구를 사칭한 악성 설치 프로그램을 설명한다. 공개 코드 호스팅 서비스를 통해 배포하고 검색 결과로 유도했다. [S21]
한계	공지는 저장소를 본 모든 이용자가 소프트웨어를 설치했다고 입증하거나 영향받은 한국 조직을 열거하지 않는다.
대응	특권 도구는 승인된 경로로 확보하라. 관리자 업무 단말에서 예상치 못한 설치·스크립트·외부 통신을 검토하고, 추가 증거가 있으면 노출 세션을 확인하라.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

L

사례 L

세계적 개발자 캠페인에 대한 한국의 공식 경고

소프트웨어 공급망

공식 캠페인 설명. 국내 범위 미확인

공식 설명	2026-04-01 경고는 개발 도구와 패키지 공급망을 통한 확산을 다룬다. 2026-05-20 공지는 해당 설명에 추가 활동을 더한다. [S23][S27]
집계 경계	후속 공지는 캠페인의 갱신이다. 세계적 사건에 대한 한국 공식 권고가 한국 피해 총계나 발표일마다 별도 국내 사고가 발생했음을 입증하지는 않는다.
대응	개발 책임자는 관련 의존성, 빌드 자격 증명, 배포 권한을 파악해야 한다. 비밀정보 노출이 확인되면 교체·폐기한 뒤 접근과 빌드 무결성을 확인하라.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

사례 M

M

익숙한 메시징 설치 프로그램 사칭

소비자 소프트웨어 사칭

공식 캠페인 선명. 국내 범위 미확인

공식 설명	KISA의 2026-04-15 공지는 가짜 다운로드 페이지와 정보 탈취 악성코드를 설명한다. 2026-02-10 부터 2026-04-14 까지 악성 다운로드 약 560 건을 추정한다. [S24]
한계	다운로드는 고유한 사람이나 성공한 감염을 식별하지 않는다. 사칭은 정상 제품 제공업체에 대한 침입을 입증하지 않는다.
대응	소프트웨어 입수 경로를 확인하고, 단말 활동을 조사하며, 추가 증거가 뒷받침하는 악성코드 노출 후 세션을 확인하라. 직원에게 알려진 설치 출처를 제공하라.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

사례 N

N

중소기업을 겨냥한 이메일 기반 랜섬웨어

중소기업

공식 캠페인 선명. 국내 범위 미확인

공식 설명	KISA의 2026-04-16 공지는 국내 중소기업의 랜섬웨어 피해 증가를 설명한다. 악성 문서 첨부와 사칭 설치 안내가 포함된다. [S25]
한계	공지는 위협 양상을 제시하지만 전국 분모나 모든 사례의 단일 운영자를 입증하지 않는다.
대응	첨부파일·단말 통제를 격리된 복원 시험과 결합하라. 파일만 시험하지 말고 업무 이메일과 신원 복구도 포함하라.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

사례 Q

AI 도구 사칭과 개발자 자격 증명

개발자 도구

공식 캠페인 선명. 국내 범위 미확인

공식 설명	KISA의 2026-07-16 공지는 악성 다운로드 링크를 포함해 AI 개발 도구를 사칭한 저장소·페이지를 설명한다. 함께 나온 경고는 노출된 개발자 자격 증명을 다룬다. [S30][S31]
보완 맥락	개인정보보호위원회의 유월 안내는 노출된 클라우드·협업 자격 증명의 개인정보 영향을 설명한다. 예방 안내이며 사고 건수가 아니다. [S36]
대응	승인된 개발 도구 출처, 저장소 비밀정보, 클라우드 역할을 검토하라. 파일에서 보이는 비밀정보를 지워도 권한이 폐기되지는 않는다. 노출이 확인되면 교체와 접근 검토가 필요하다.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

추가 공개: 서비스 복구와 이후 랜섬웨어 분류

ActionPower의 Daglo 서비스가 2026-03-27 에 낸 공지는 보안 이상 징후를 2026-03-22 정오 무렵으로 명시한다. 예방적 서비스 중단과 2026-03-23 08:00 까지의 전체 기능 복구를 설명한다. [S98]

연합뉴스의 2026-04-09 보도는 회사가 사건을 이후 랜섬웨어로 분류했다고 전한다. 회사는 조사에서 이용자 개인정보·녹음·핵심 회사 자료의 유출 정황을 발견하지 못했다고 밝혔다. 오래되거나 폐기된 자료와 직원이 개별 보관한 일부 표본 자료는 인정했다. [S99]

이는 명시된 조사 지원을 바탕으로 한 회사의 제한적 조사 결과다. 노출이 전혀 없었음을 입증하지 않는다. 국내 보도는 해당 서비스와 ActionPower의 관계도 확인하지만 추적 서비스의 모든 분류나 주장된 파일 규모를 검증하지는 않는다. [S100]

삼월 모니터링 글들은 Crypto24의 주장을 반복한다. 이 공격자 표시는 회사가 확인한 사건·정보 범위 설명과 구분한다. 여러 채널의 반복은 별도 사고를 만들지 않는다. [S1]

서비스 책임자는 복구 시각을 보존하고 실제 공개된 자료를 식별하며 자체 증거에 따라 관련 접근 권한을 회수하라. 이후의 분류 변경은 최초 공지를 바꾸지 않고 사고 기록에 반영해야 한다.

5.4 소비자 서비스와 공공 분야 캠페인 보고

사례 O

■ 데이터베이스 접근과 별개의 후속 사기 경고

소비자 서비스

공식 공개. 범위 한계 유지

공식 설명	개인정보보호위원회의 2026-06-04 공지는 2026-06-02 에 탐지한 데이터베이스 접근 이후 스트리밍 업체가 제출한 신고를 설명한다. 감독 기관 공지는 영향받은 집단을 확정하지 않는다. [S35][S51]
경계	일부 필드가 암호화됐다고 모든 노출 필드가 보호됐거나 모든 정보를 사용할 수 없었다는 뜻은 아니다.
대응	실제 기록과 암호화 맥락을 확인하고, 접근 경로를 제한하며, 통지를 검토하라. KISA의 별도 보상·환불 미끼 경고는 신뢰 채널을 통한 고객 안내의 근거가 된다. [S28]

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

사례 R

■ 여러 전달 경로를 설명하는 공동 경고

여러 부문에 걸친 캠페인

공식 캠페인 설명. 국내 범위 미확인

공식 설명	한국 사이버·정보·경찰·금융보안 기관의 2026-07-30 공동 공지는 채용·이력서 피싱과 악성코드 배포 발판으로 쓰이는 소규모 웹사이트를 설명한다. [S32]
공격자 평가의 경계	국가 지원이라는 설명은 해당 출처의 평가다. 모든 요소를 특정 그룹에 귀속시키거나 보고서의 범죄 광고에 공통 운영자가 있음을 입증하지 않는다.
대응	채용·문서 절차를 보호하고, 예상하지 못한 웹사이트 변경을 검토하며, 단말 행위를 계정 활동과 대조하라. 한국어 미끼만으로 국가 연계를 추론하지 마라.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

칠월에 보도된 별도 공공 분야 교육 공개는 2025 년에 시작해 2026 년 이월까지 이어진 접근을 다룬다. 부처 설명에서 정확한 노출 내용은 미확인이었다.

튀르키예어 보도는 추가 언어 범위를 제공하며 다른 사고나 최종 대상 집단 총계가 아니다. [S52][S53]

KISA의 구월 경고는 법 위반, 범죄 연루, 침해 보상을 내세운 공공기관·금융회사 사칭을 설명한다. 이는 수신자를 겨냥한 캠페인이며 사칭당한 기관에 침입했다는 증거가 아니다. [S55]

추가 공개: 자산 취급 업무의 민감정보

국세청의 2026-03-01 사과문은 2026-02-26 브리핑 때 제공한 언론용 원본 사진을 다룬다. 기관은 사진에 가상자산 관련 민감정보가 포함됐고 납세자의 지갑에서 코인이 빠져나갔다고 확인했다. 경찰 수사도 요청했다. [S101]

국내 보도는 유동성이 불확실한 토큰 수량과 명목 평가액을 설명한다. 이 보고서는 인용된 평가액을 실현된 순손실로 채택하지 않는다. 채택한 후속 보도에서도 반환 주장은 검증 중이었다. [S102][S103][S105]

이는 우발적인 민감정보 공개와 자산 보관 통제에 관한 사례다. 이전의 다른 압류 자산 보도와는 별개다. 홍보·자산 보관팀은 공개 전 자료에 비밀정보가 있는지 독립적으로 검토하고 승인된 증거 사본을 보존하라.

추가 공개: 두 노출 기간의 업무 문서

국내 보도는 엔터테인먼트 기업 집단이 설명한 2026-09-12–2026-09-13 과 2026-10-03–2026-10-05 의 외부 접근을 다룬다. 설명된 경로는 문서 미리보기 기능과 비용 처리에 관한 것이며 공통 캠페인이 입증된 것은 아니다. [S111][S112]

보도는 일부 내부 문서와 개인정보의 노출을 회사 공지의 설명으로 전한다. 설명된 대상에는 일부 현직·전직 직원과 협력사 관계자가 포함된다. 정보 범주는 개인마다 다르며 피해 인원 총계는 확정되지 않았다.

이 설명은 외부 소프트웨어 공급업체 자체가 공격받았음을 입증하거나 특정 취약점을 식별하지 않는다. 애플리케이션 책임자는 미리보기·내보내기 기능을 목록화하고 접근 가능한 기록을 파악하며 각 노출 기간의 증거를 보존하라.

추가 공개: 별도로 확인된 대학 포털 사건

연세대학교의 2026-10-22 공지는 2026-10-20 과 2026-10-21 의 두 기간에 포털 정보가 노출됐다고 확인한다. 학내 식별자, 연락처·소속 정보, 계정 관리 메타데이터를 설명한다. 항목은 개인마다 다르며 공지는 피해 인원 총계를 제시하지 않는다. [S117]

대학은 접근 경로 차단, 관계 기관 신고, 대상자 통지를 설명한다. 데일리시큐와 뉴스핌 보도는 포털 공개를 뒷받침한다. 정보 범주가 원문 비밀번호 공개나 특권 셸 접근을 입증하지는 않는다. [S118][S119]

확인한 출처는 이 포털 사건을 이전 접근 권한 판매 광고와 연결하지 않는다. 계정 소유자는 확인된 정보 범위와 통지를 따르고 미확인 제안은 별도 검증 업무로 다뤄야 한다.

5.5 범죄적 갈취와 AI 주장

사례 W

W

두 개 연도에 걸친 경찰 협의 설명

여러 부문의 갈취 협의

언론 보도 설명, 범위 한계 유지

보도된 경찰 설명	MBC의 2026-10-26 보도는 2025 년 구월부터 2026 년 시월까지 조직 약 90 곳과 기록 820만 건 이상에 관한 혐의를 설명한다. [S43]
연대기	보도에 따르면 경찰은 생성형 AI의 집중 사용이 팔월 말에 시작됐고, 이후 활동이 빨라졌다는 혐의를 평가했다. 그렇다고 이전의 모든 침입 혐의가 AI를 이용했다는 뜻은 아니다.
관계의 한계	설명은 이 피의자들이 금융 분야 공개 집단 전체나 보고서의 모든 광고를 발생시켰다고 입증하지 않는다.
대응	실제 접근 경로에 따라 권한 통제, 노출 계정, 증거 보존의 우선순위를 정하라. AI 관련 설명 때문에 접근을 막거나 드러내는 일반 통제를 뒤로 미뤄서는 안 된다.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

KISA의 시월 대응 경고도 외부 접근 애플리케이션, 접근 통제, 노출 자격 증명, 정보 전송 감시를 강조한다.

십일월 네트워크 연결 저장장치(NAS) 경고는 별도 백업과 통제된 외부 접근의 근거가 된다. 어느 자료도 완전한 전국 피해 총계를 제공하지 않는다. [S33][S34][S124]

5.6 최근 활동: 2026-11-08 부터 2026-11-22 까지

마감 기간에는 별개 공개와 갱신이 있다. 아래 날짜는 공통 캠페인이 아니라 관련 사건이나 발표를 식별한다.

공개	확인된 범위	사건·발견	경계
금융보안원	평가 서비스 서식·정보	탐지 2026-11-09, 공개 2026-11-10	범주는 고유한 사람이 아님. 제 9 장 사례 P
대학 교육 서비스	보도된 공식 설명의 기록 24,011 건	발견 2026-11-12, 공지 2026-11-13	비밀번호·주민등록번호 제외는 해당 설명의 범위
직원 교육 서비스	무단 클라우드 접근과 잠정 대상 집단	접근 2026-11-09, 신고 2026-11-11	초기 대략적 범위는 잠정 상태
공공 바우처 서비스	API 관련 개인정보 접근	탐지 2026-11-13, 언론 보도 2026-11-16	발표 당시 바우처 탈취는 보고되지 않음
연구중심대학 포털	공개된 세 기록 집단	공격 2026-11-13, 공지 2026-11-19 와 2026-11-20	기록은 겹칠 수 있음. 사례 U
마감일 추가 공개	교육·공통 메일·에너지·공급업체·물류 공개	2026-11-22 까지의 발표이며 기초 사건 날짜는 다름	별개 사례·갱신이며 상세 내용과 한계는 아래에 설명

S

사례 S

제외 범위를 명시한 교육 서비스 정보

교육

언론 보도 설명. 범위 한계 유지

보도된 공식 설명	연합뉴스는 교육 운영 서버에 관한 대학의 사과를 보도한다. 대학은 학생·교직원 식별자와 연락처 관련 기록 24,011 건을 확인했다고 밝혔다. [S40]
한계	당시 대학 설명은 비밀번호와 고유 국가 식별자를 제외했다. 수치는 전체 학생 수나 모든 교내 시스템이 영향을 받았다는 조사 결과가 아니다.
대응	서비스 접근 증거를 보존하고 영향 기록을 대조하며 신뢰 채널로 사칭 주의 안내를 제공하라. 해당 교육 서비스의 권한과 공급업체 관계를 검토하라.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

사례 T

T ■ API 접근은 결제 탈취를 입증하지 않는다

공공 결제 관련 서비스

언론 보도 설명, 범위 한계 유지

보도된 공식 설명	공공 바우처 서비스 운영자는 정보 접근이 API 인증 취약점 때문이라고 설명했다. 십일월 발표는 영향받은 고객을 3,083 명으로 보고했다. [S41]
한계	운영자는 발표 당시 바우처 잔액 탈취나 무단 결제를 확인하지 못했다고 밝혔다. AI 사용에 대한 의심은 운영자의 평가로 유지한다.
대응	실제 권한 통제 경계를 시험하고 정보 조회를 거래 기록과 별도로 검토하라. 결과를 발표하기 전에 정보 접근·결제 증거를 모두 보존하라.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

사례 U

U ■ 추가 포털이 기록 총계를 바꾼다

연구·교육

공식 공개, 범위 한계 유지

공식 설명	연구중심대학의 2026-11-19 공지는 2026-11-13 침입을 설명한다. 계정 ID·암호화 비밀번호 기록 19,500 건과 계정 ID·이메일·소속 기록 478 건을 제시한다. [S44][S76]
갱신	2026-11-20 공지는 행정 포털 기록 25,551 건을 추가한다. 산술 합계는 기록 45,529 건이며 확인된 고유 인원 수가 아니다. [S48]
대응	애플리케이션 간 사람을 대조하고 자격 증명 보호를 평가하며 연속된 공지를 보존하라. 이후 범위 수정은 최초 공개의 증거·시점을 지우지 않으면서 대응을 갱신해야 한다.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

V

사례 V

직원 교육이 드러낸 공급업체 의존 관계

직원 교육

언론 보도 설명, 범위 한계 유지

보도 설명	아시아경제는 회사의 무단 클라우드 접근 확인과 개인정보 감독 기관의 신고 접수를 보도한다. 기사에서 접근일은 2026-11-09, 감독 기관 신고일은 2026-11-11 이다. [S45]
한계	이용자 약 70,000 명 수치는 잠정적이었다. 최종 고유 인원 수나 기업 교육 고객마다 발생한 별개 사고로 바꿔서는 안 된다.
대응	고용주는 교육 제공업체가 보유한 기록을 파악하고 관련 고객 환경을 확인하며 자체 개인정보 보호·직원 보호 판단을 위한 증거를 확보해야 한다.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

X

사례 X

새 인원 수 없이 범주를 넓힌 대학의 추가 공지

교육

공식 공개, 범위 한계 유지

공식 설명	대학의 2026-11-18 공지는 기록 약 180,000 건을 설명하며, 주민등록번호가 있는 약 25,000 건을 포함한다. 사건일은 2026-11-16, 발견일은 2026-11-17 로 명시한다. [S57]
갱신	2026-11-22 공지는 학사·강사 관련 정보를 추가한다. 추가 대상 집단이나 중복 제거 총계는 제시하지 않는다. 국내 보도는 이전 공지를 뒷받침한다. [S56][S73][S74]
대응	새로 식별된 범주를 이전 집단과 대조하고 실제 관련 정보에 대한 안내를 갱신하라. 수량이 명시되지 않은 확대를 가공의 총계에 더하지 마라.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

사례 Y

Y

공통 이메일 접근과 공개 설명의 날짜

공공 서비스

공식 공개. 범위 한계 유지

공식 설명	공공 서비스 운영자의 설명은 행정 이메일 계정 약 300 개에 대한 비정상 접근을 다룬다. 지방자치단체 네트워크와 통합 로그인 취약점을 거친 경로를 설명한다. [S60]
연대기	공식 설명에 따르면 행정안전부가 2026-11-09 에 통보받았다. 국내 보도는 2026-11-16 에 나왔고 공식 웹 설명은 2026-11-17 에 게시됐다. 후속 기사의 날짜가 새 공격 날짜는 아니다. [S60][S61]
한계	조사는 계속됐다. 설명은 공공 분야 메일 전체에 접근했음을 입증하거나 무관한 공개 사례들의 공통 공격자를 식별하지 않는다.
대응	인증 의존 관계, 관련 세션, 메일함 접근 기록을 함께 검토하라. 계정 집단을 메시지, 수신자, 이후 확인된 정보 노출과 구분하라.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

사례 Z

Z

중복을 제거한 단일 총계가 아닌 에너지 회사의 두 서비스 집단

에너지·조달

언론 보도 설명. 범위 한계 유지

보도된 공개	2026-11-22 국내 보도는 2026-11-20 에 탐지된 고객·조달 서비스 관련 회사 공개를 설명한다. 보고된 두 시스템 이용자 집단은 650,487 과 869,761 이다. [S58][S78][S79]
집계 경계	산술 합계는 1,520,248 이다. 두 시스템 사이에서 중복을 제거해 확인한 집단이 아니다. 정보 범주는 기록과 사람에 따라 다르다.
주장의 경계	보고서의 별도 조달 데이터 광고는 미확인 상태다. 공개 시점과 겹치는 주제만으로 제안 파일이 공개 정보와 일치한다고 입증할 수 없다.
대응	서비스 간 신원을 대조하고 실제 노출 범주를 평가하며 연속된 설명을 보존하라. 고객 보호는 공격자의 제목이나 가능한 최대 합계가 아니라 이 사실을 따라야 한다.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

아래 추가 공개는 공통 캠페인을 입증하지 않으면서 공급업체·서비스에 대한 관찰 범위를 넓힌다.

공개	뒷받침되는 구분	최초 대응	출처
창업 프로그램 공급업체	프로그램 참여자 818 명은 공급업체 전체 20,028 명의 하위 집단	개인정보처리자의 실제 기록과 수탁자 통지 확인	[S67][S68]
물류 챗봇	비정상 자동 접근을 식별했으며 실제 정보 노출·대상 집단은 미확인	조회를 보존하고 가능한 정보 범위 확인	[S80][S81]
지역 대학 서비스	도서관·취업·문서·연구 행정 서비스가 서로 다른 공개에 등장	특정 애플리케이션·데이터 책임자 파악	[S71]
학교 통학	보호자 연락처 항목 약 9,900 건이 보고됐으며 영향받은 학생·학교는 평가 중	신뢰 채널로 경고하고 대상 집단 대조	[S75]
외부 직원 교육	금융기관 직원 정보가 교육 제공업체를 통해 영향을 받았으며 핵심 은행 접근은 입증되지 않음	공급업체 고객 환경과 직원 보호 조치 확인	[S69]
보험 수탁자	보도는 십일월 공지로 공개된 시월 수탁자 사고의 고객 66 명을 설명	기록·통지 책임 확인	[S70]

물류 공지는 노출 가능성에 관한 설명이다. 확인된 정보 손실 집단으로 제시하지 않는다. 창업 공급업체의 웹 게시와 언론 공개도 날짜가 다르며 설명된 발견은 그보다 앞섰다.

공공 분야 교육 사고의 부처 브리핑은 이월 인지, 후속 분석, 이후 통지를 구분한다. 저장 정보 집단은 반출이 확인된 사람 수가 아니다. 보고서는 이 연대기에서 법 위반을 판단하지 않는다. [S62][S63]

최근 추가 공개: 수탁자의 고객 상담 정보

MBC와 뉴시스는 금융 서비스 업체가 2026-11-15 에 설명한 고객 상담 수탁자의 2026-11-12 접근 사건을 보도했다. 설명된 정보는 고객의 상담 이력에 따라 달랐으며 영향받은 기록과 대상 집단은 조사 중이었다. [S106][S107]

별도 제공업체 보도는 일부 상담 시스템의 이상 활동을 설명하며 정보 범위가 고객사와 개인에 따라 다르다고 전한다. 제공업체와 고객사 설명은 수탁자 공개의 서로 다른 관점을 다룬다.

어느 쪽도 전체 이용자 규모나 실제 피싱 피해에 관한 일반적인 판단을 뒷받침하지 않는다. [S108]

이 설명은 핵심 거래·지갑 시스템에 대한 접근을 입증하지 않는다. 실제 상담 항목과 영향받은 기록을 대조하고 그 사실에 따라 신뢰 채널의 고객 안내와 의심 메시지 처리를 갱신하라.

십일월 보도는 제조업체가 북미 서비스 사업의 광고 데이터 제공업체와 관련된 보안 사고를 인지했다고 전한다. 제공업체의 예비 조사에서는 일부 회사 정보에 영향이 있었을 가능성이 제기됐으며 조사는 계속됐다. 모든 영향을 부인한 설명이 아니다. [S116]

NOn 표시가 있는 등재와 별도 2026-11-22 Hyflock 제조업 주장은 서로 다른 주장이다. 동일한 피해 주체, 공통 사고, 검증된 침입 두 건을 입증하지 않는다. 제공업체 설명은 제조업체 자체 시스템에 대한 접근을 입증하지 않는다. [S1][S2]

5.7 최근 기술 권고는 피해 사고가 아니다

마감 전 두 주 동안 발표된 Java 권고는 자산 검토가 필요하다는 근거다. 한국 조직이 해당 취약점을 통해 공격받았음을 입증하지 않는다. 개인정보보호위원회의 경고는 연계 시스템과 대량 접근을 통한 대규모 개인정보 노출 예방에 초점을 둔다. [S11][S12][S13][S39]

아래 릴리스 문자열은 CVE-2026-114938 에 관한 것이다. 네트워크 주소가 아니라 소프트웨어 버전이다. NVD는 영향받는 Oracle Java·GraalVM 제품과 함께 일부 Siemens 산업용 엣지·보안관제 제품도 기록한다. KISA의 현행 권고는 이에 대응하는 수정 버전과 배포판별 안내를 제공한다.

제품군	나열된 영향 릴리스	나열된 수정 릴리스
Java 8 Enterprise Performance Pack	8u511b33-perf	8u513-perf
Oracle Java SE 17 / GraalVM JDK 17	17.0.21.0.3	17.0.21.1
Oracle Java SE 21 / GraalVM JDK 21	21.0.13.0.3	21.0.13.1
Oracle Java SE 25	25.0.5.0.3	25.0.5.1
Oracle Java SE 27	27.0.1.0.3	27.0.1.1
GraalVM Enterprise Edition	21.3.20.0.3	21.3.20.1

같은 버전 계열의 이전 릴리스도 검토가 필요할 수 있다. 정확한 배포판, 패키지, 하드웨어 조건, 서비스 런타임이 중요하다. 해당 업체의 최신 안내를 따르고 재시작·재배포 후 실행 중인 서비스를 확인하라.

NVD에 실린 Oracle 제공 CVSS 3.1 점수는 8.1 이다. 척도를 밝히지 않고 다른 CVSS 버전의 점수로 대체해서는 안 된다. 심각도 점수는 관찰된 악용이나 특정 조직의 노출을 입증하지 않는다. [S12]

5.8 후속 조치와 제외 사항

발표	올바른 해석	처리
쿠팡·CFS에 대한 유월 제재	기초 침해는 2025 년에 발생했으며 2026 년 일월 접근 확인·로그 삭제·통지 위반을 포함	규제·증거 보존 맥락이며 새 2026 년 침입이 아님 [S126]
세 회사에 대한 칠월 제재	기초 사고는 2024 년 발생	규제 맥락이며 새 2026 년 공격이 아님 [S37]
KT에 대한 유월 제재 결정(2026 년 팔월 게시)	기초 펨토셀 유출과 별도 웹·서버 침입은 2024–2025 년에 발생했으며 2026 년 로그 삭제·제재 결론을 포함	규제·증거 보존 맥락이며 새 2026 년 침입이 아님 [S127]
산업 기업 집단에 대한 십일월 제재	기초 침입은 2022 년 칠월 발생	제재 맥락으로만 사용 [S38]
교육청의 십일월 문서 공지	오월 제출 자료에 관한 실수에 의한 제한 배포	정보 관리 사례이며 해킹이 아님 [S42]
재게시된 과거 소매·회원 자료	2026 년 게시물에 이전 기록이 포함될 수 있음	재유통이며 새 날짜의 침입이 아님 [S1]
세계적 개발자·VPN 권고	한국 경고가 한국 피해자를 열거하지 않음	국내 범위가 미확인인 방어 맥락 [S23][S29]

개인정보보호위원회의 2026 년 유월 쿠팡·CFS 제재 결정은 위조된 인증 토큰으로 이용자 3,300만 명 이상에게 영향을 준 2025 년 유출을 다룬다. [S126] 같은 결정은 이용자 160,000 명에게 영향을 준 2026-01-30 배송지 목록 페이지 접근 확인과 웹 접근 로그의 수동·자동 삭제 및 지연 통지도 포함한다. [S126]

2026-08-07 에 게시된 개인정보보호위원회의 2026-06-29 KT 제재 결정은 가입자 16,647 명에게 영향을 준 2024–2025 년 불법 펨토셀 유출을 다룬다. [S127] 같은 결정은 합산 이용자 수를 제시하지 않은 별도의 웹 서비스·서버 침입과 서버 로그 삭제 및 조사 방해 고발도 다룬다. [S127] 두 결정 모두 2026 년 이전 침입을 다루므로 2026 년 신규 사고 수에서는 제외하되 인증·로그 보존·고객 보호 의무를 뒷받침한다.

일월 교육 기업 집단의 발견 연대기는 회사의 일차 공지를 따른다. 번역·반복 보도가 별도 사고를 만들지는 않는다. [S49]

5.9 부문 전반의 판단

사례는 데이터 침해라는 단일 범주만으로 대응을 계획하기에는 너무 거칠다는 점을 보여준다. 임상 서비스, 문서 저장소, 교육 고객 환경, 평가 포털은 서로 다른 정보를 보유하고 다른 업무를 지원한다.

어디에 접근했는지, 어떤 권한이 이를 허용했는지, 어떤 정보에 접근할 수 있었는지, 같은 신원에 의존하는 서비스는 무엇인지 물어라. 이 질문이 기술적 결과를 차단·연속성·개인정보 보호 판단과 연결한다.

증거를 보존하거나 확인된 접근 경로를 차단하기 위해 최종 공격자 식별을 기다리지 마라. 동시에 광고나 미확인 집단을 회사의 조사 결과로 바꾸지 마라. 실행 계획으로 긴급성과 증거 책임을 함께 지정하라.

핵심 요점

01
사건·탐지·공개·제재 날짜를 구분하라.

02
피해 인원을 추정하기 전에 애플리케이션과 기록 집단을 대조하라.

03
확인된 접근과 업무 영향에 따라 대응 책임자를 정하라.

장 06

핵티비즘, DDoS, 서비스 연속성

이 장에서 답하는 질문

방어자는 중단 주장과 입증된 서비스 영향을 어떻게 구분해야 하는가?

3

접근 가능 여부, 데이터 접근, 운영 영향에 관한 별도 질문

6.1 인과관계를 가정하지 않는 연표 58

6.2 주장과 확인의 대조 59

6.3 확인되지 않았다는 말의 의미는 제한적이다 59

6.4 추가 공격자 주장과 그 한계 60

6.5 증거가 바뀌어도 유효한 소통 61

6.6 대응 책임 61

장 06

핵티비즘, DDoS, 서비스 연속성

요약

웹사이트 주장·순간적인 접속불가·운영중단에는 각각 증거가 필요하다. 보관 자료는 별개의 가용성·데이터 주장을 같은 운영자에게 연결하지 못하며 정치적 구호도 마찬가지다. 공개 주장을 자체 서비스 관측과 비교하고 물리공정 영향은 운영자에게 확인하라. 갱신시각을 명시한 사실 중심 상태안내를 준비하라.

6.1 인과관계를 가정하지 않는 연표

2026년 1월 10일	**KISA** QR 사칭 경고이며, 캠페인 양상이지 피해자 총계가 아님
2026년 3월 20일	**KISA** 핵티비스트의 시도를 설명하며, 모든 주장의 서비스 영향은 미확인
2026년 6월 4일	**PIPC** 스트리밍 서비스 사고 조사이며, 대상 규모는 미확정
2026년 7월 30일	**관계 기관** 국가 지원 캠페인이라는 평가이며, 귀속 판단은 해당 출처의 것
2026년 11월 10일	**금융보안원** 2026-11-09 발견 뒤 평가 시스템 사고를 공개
2026년 11월 12일	**포럼 판매자** 기술 문서 제안이며, 내용은 미확인
2026년 11월 17일	**공공 서비스 운영자** 공통 메일 설명의 웹 게시일. 이전 통보·보도 날짜와 구분
2026년 11월 19일	**포럼 판매자** 조달 자료 제안이며, 진위는 검증되지 않음
2026년 11월 20일	**대학** 포털 기록이 추가됐으며, 중복을 제거한 인원수는 아님
2026년 11월 22일	**전국 언론 보도** 에너지 기업의 공개 내용이며, 두 시스템의 대상 규모이지 중복 제거 총계가 아님

출처: [S1][S6][S18][S19][S22][S32][S35][S48][S58][S60].

연표는 공격자 발언, 제삼자 전달, 공식 공개를 구분한다. 게시일은 접근이 시작된 시점을 입증하지 않는다. 두 항목의 시점이 가깝다고 공통 인프라나 공조가 입증되는 것은 아니다.

6.2 주장과 확인의 대조

질문	공격자 자료	필요한 증거	방어자의 설명
사이트가 이용 불가였는가?	주장 또는 외부 가용성 결과	해당 구간의 서비스·상위망 관측 자료	영향받은 서비스와 확인된 지속 시간을 설명
정보를 얻었는가?	광고한 파일이나 화면 캡처	접근 기록과 검증한 표본	확인된 정보 범주와 남은 불확실성을 설명
물리 공정에 영향이 있었는가?	인터페이스 이미지나 제어 주장	운영자 기록과 공정 측정값	화면 접근과 공정 변경을 구분
책임 주체는 누구인가?	별칭, 국기, 정치적 구호	출처로 뒷받침되는 공격자 식별 증거	평가의 출처와 확신도를 명시

주장자는 많은 대상을 나열하지만 운영자는 더 좁은 서비스 문제를 확인할 수 있다. 이 두 수치를 비율로 만들어서는 안 된다. 가용성 결과로 정보 탈취, 지속 접근, 별개 사고의 책임을 입증할 수도 없다.

6.3 확인되지 않았다는 말의 의미는 제한적이다

KISA의 2026-03-20 경고는 한국의 정부 및 방산 부문 대상을 향한 RipperSec의 시도를 설명한다. 행위자의 표적 목록에 있는 모든 서비스가 실제로 중단됐음을 입증하지는 않는다.

이 경고는 공식적인 캠페인 맥락이며, 주장된 모든 결과를 독립적으로 검증한 것은 아니다. [S22]

RipperSec

KISA가 설명한 핵티비스트 활동

출처의 캠페인 설명이며 독립적인 국가 연계 평가는 없음

대한민국, 2026년

2026-03-20

KISA 경고는 한국 정부·방위 분야 대상을 상대로 한 시도를 설명한다

주장된 표적

출처가 명시한 넓은 정부·방위 분야 역할

공개 출처의 설명

[S22] 공식 캠페인 경고

분석 평가

경고는 보고된 시도를 설명하며 명시된 모든 서비스의 성공한 중단을 입증하지 않는다. 관련 주장은 담당 운영자의 서비스 기록과 비교하라.

확신도

경고의 존재에 대해서는 높음. 구체적 결과는 미확인

주장이 적더라도 실무에 필요한 구분은 같다. 방어자는 공개 웹사이트, 인증 서비스, 고객 거래, 내부 공정 중 어디에 영향이 있는지 판단할 수 있어야 한다. 상태 지표 하나로 네 가지 질문에 모두 답할 수는 없다.

산업 시설의 경우 인터페이스 화면 캡처는 소유자와 비공개로 확인할 이유가 된다. 안전하지 않은 운영 상태를 발표할 근거는 아니다. 운영 장비에 개입할 때는 운영자의 안전·변경 절차를 따라야 한다.

6.4 추가 공격자 주장과 그 한계

RipperSec 표시가 있는 보관 채널에는 예정 표적 공지와 서비스 가용성·계정·제어 인터페이스에 관한 별도 주장이 있다. 표적과 시각을 예고한 글은 의도를 밝힌 것이며 공격 완료를 입증하지 않는다. [S1]

관측 게시 날짜	포괄적인 역할·주제	보관된 주장	증거의 한계
2026-01-15	통신 관련 호스트	공격자가 호스트 접근을 주장	호스트 소유권과 제공업체 전체 접근은 미확인
2026-02-05–2026-02-21	에너지·농업·관리 인터페이스	제어·관리 접근을 주장하며 일부 글은 영상을 언급	보관된 텍스트는 제어 권한이나 물리 공정 영향을 입증하지 않음
2026-02-20	여러 데이터베이스 표적	채널이 데이터베이스 자료 보유를 주장	파일·출처·별도 침입 건수는 미확인

관측 게시 날짜	포괄적인 역할·주제	보관된 주장	증거의 한계
2026-02-22–2026-03-04	여행·금융·상거래·공공 데이터·에너지 웹사이트	채널이 서비스 이용 불가를 주장하거나 상태 링크를 제시	지속적인 접속 불가와 업무 중단은 입증되지 않음
2026-02-24	외부 공개 웹사이트	별도 공격자가 웹페이지 변조를 주장	독립적으로 확인한 페이지나 서비스 영향은 없음
2026-03-17	여러 외부 공개 표적	다른 채널이 상태 링크와 작전 목록을 게시	표적 목록만으로 모든 표적에 대한 공격 성공을 입증하지 못함
2026-04-13–2026-05-23	공공 서비스 웹사이트	추가 채널이 중단을 주장하거나 표적 목록을 반복	전달 글과 상태 링크는 운영 영향을 독립적으로 입증하지 않음

이들은 서로 다른 주장이며 최초 사건 날짜와 영향은 미확인이다. 제어 인터페이스 주장에 제품명이 나와도 제품 공급업체가 공격받았다는 뜻은 아니다. 비슷한 표현도 국가와의 관계를 입증하지 않는다. [S1]

관련 인터페이스 제보를 받은 소유자는 자산과 접근 경로를 비공개로 확인하라. 인증·운영 기록을 보존한 뒤 공개 화면, 관리 기능, 실제 공정 변경 중 무엇에 관한 주장인지 판단하라.

6.5 증거가 바뀌어도 유효한 소통

조사 중인 주장, 확인된 서비스 중단, 확인된 개인정보 사고에 대해 각각의 안내문 양식을 준비하라. 각 양식에는 영향받은 서비스, 확인된 사실, 진행 중인 완화 조치, 다음 갱신 시각을 담아야 한다.

홍보 담당자는 기술 증거 책임자와 개인정보 판단 책임자에게 접근할 수 있어야 한다. 공격자가 제시한 트래픽 규모, 구호, 피해 대상 수를 회사의 조사 결과처럼 반복해서는 안 된다. 공격 주체가 미확인이라면 이를 명확히 밝혀라.

공급업체와 사고 기록 및 완화 조치 관측 자료의 보존 방식을 합의하라. 업무 연속성 훈련에서는 인증 제공자나 고객 메시지 채널을 쓸 수 없을 때의 대체 방안도 시험해야 한다.

6.6 대응 책임

판단	책임자	상위 대응 전 필요한 증거
완화 조치 가동	네트워크·서비스 운영팀	확인된 비정상 트래픽 또는 서비스 저하
계정 제한	신원·사고 대응팀	계정 일치와 의심 활동
데이터 사고 발표	개인정보 보호·홍보팀	적용 의무와 확인되었거나 법적으로 유의미한 의심 범위
물리 공정 변경	담당 운영자	공정 증거와 승인된 안전 조치
공개적인 공격자 식별	지정된 경영진	검토를 거친 출처 기반 평가

목적은 서비스와 정확성을 함께 지키는 것이다. 팀은 자체 관측 자료에 따라 긴급히 조치하면서도 제삼자의 미확인 설명을 사실 중심의 상태 안내에서 제외할 수 있다.

핵심 요점

01

접근 가능 여부, 데이터 접근, 물리적 영향은 서로 다른 명제다.

02

정치적 표현은 책임 주체를 입증하지 않는다.

03

완화 조치, 증거 보존, 정해진 시각의 상태 갱신을 함께 훈련하라.

장 07

공격자, 캠페인, 관계

07

이 장에서 답하는 질문

어떤 공격자 평가가 뒷받침되며, 공격자 식별과 관계없이 어떤 방어 행위가 중요한가?

73

Ransompedia의 대한민국 랜섬웨어 게시

7.1 관계도 64

7.2 회신을 이용한 피싱과 출처가 지목한 사이버 첩보 65

7.3 일괄적인 공격자 지목 없이 국내 캠페인 연구 읽기 66

7.4 최근의 상거래 미끼도 중요하다 67

7.5 랜섬웨어와 갈취 67

7.6 범죄 활동 계정과 증거의 한계 72

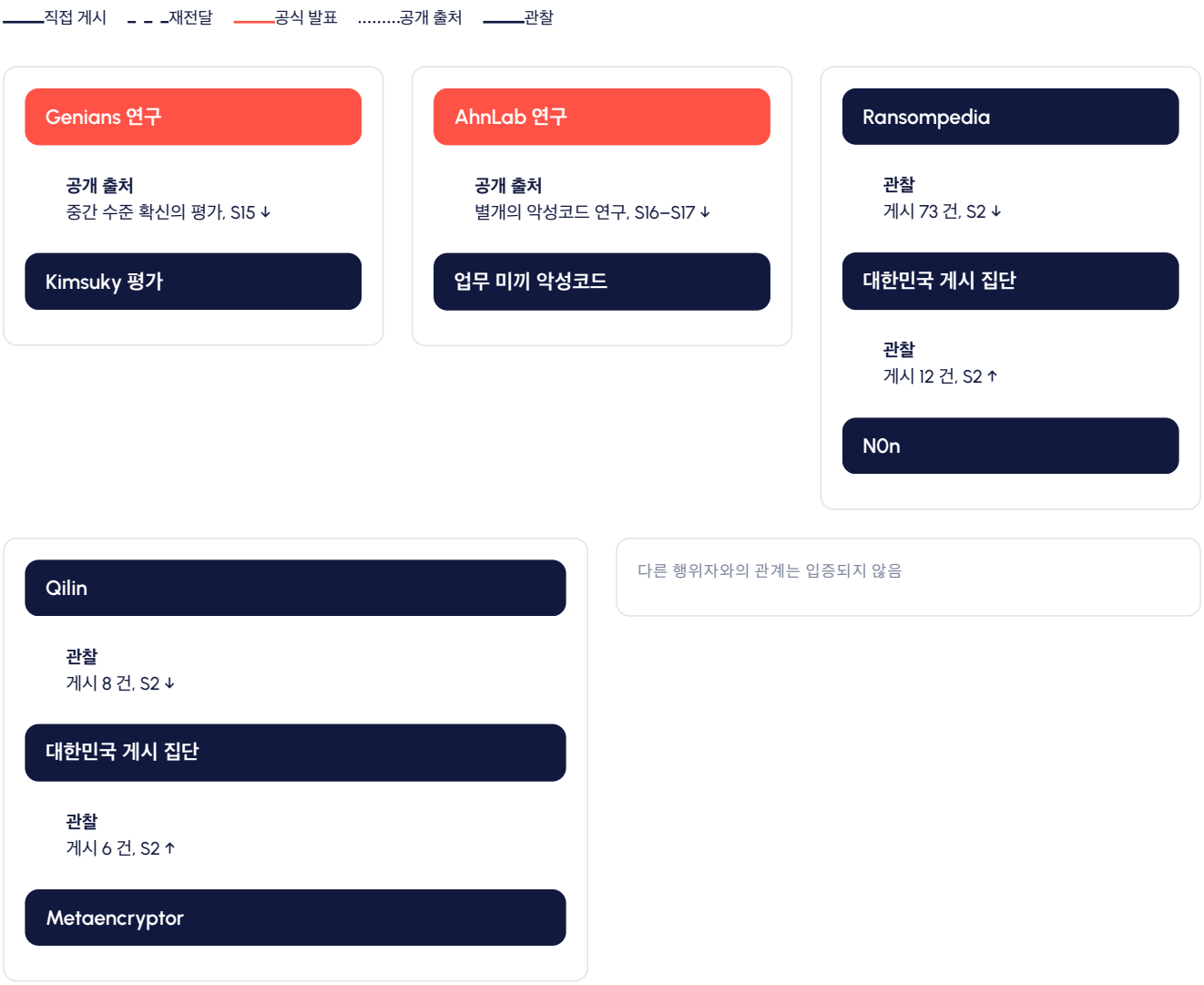
장 07

공격자, 캠페인, 관계

요약

출처가 공격 주체를 지목한 사이버 첩보 연구, 갈취 게시, 범죄 시장의 활동 계정을 구분하라. Genians는 세미나 미끼 연구에서 Kimsuky와의 연관성을 중간 수준의 확신으로 평가한다. Ransompedia에는 여러 주장자 명칭이 기록되지만 서로 다른 운영자임을 입증하지는 않는다. 별칭이 반복돼도 모든 광고의 운영자가 같다는 증거는 아니다. 기록된 행위를 바탕으로 신원·계정, 단말, 복구 통제의 우선순위를 정하고, 대응을 상향할 때마다 공격자 식별의 불확실성을 유지하라.

7.1 관계도



관계도는 발행자, 공격자 명칭, 게시 집단을 구분한다. 출처의 공격자 평가는 이 보고서의 독립적인 조사 결과가 아니다. 자체 데이터의 게시 연결선은 보관 출처의 주장을 기록하며, 해당 조직이 확인한 침입을 뜻하지 않는다.

구체적인 공통 요소 없이 지하 시장 판매자를 국가 연계 캠페인에 연결하지 않는다. 같은 언어, 피해 부문, 게시 주간만으로는 부족하다. 광고 수량이 비슷하다는 사실도 판매자들이 같은 파일을 보유했음을 입증하지 않는다.

7.2 회신을 이용한 피싱과 출처가 지목한 사이버 첩보

Kimsuky

Genians의 사이버 첩보 평가 | Genians가 중간 수준의 확신으로 평가한 북한 연계

대한민국, 2026년

2026-11-16
이전 서신과 도구 변화를 설명한 연구 발표

주장된 표적

출처가 설명한 정책·보안 전문가

공개 출처의 설명

[S15] Genians는 캠페인을 중간 수준의 확신으로 평가하며 모방 가능성을 대안으로 유지한다.

분석 평가

신뢰하는 업무 서신, 단말 행위, 계정 증거를 대조하라. 보고서의 무관한 시장 광고와 연결은 입증되지 않았다.

확신도
출처의 공격자 평가: 중간. 국내 피해 범위는 미확인

Genians는 2026-11-16 에 NodeLinkRAT 연구를 발표했다. 연구는 구월에 국회의원 보좌관을 사칭해 세미나 사례비 서류를 요청한 서신 교환을 설명한다. 첫 메시지에는 첨부파일이 빠졌고, 이후 회신에 악성 압축파일이 포함됐다.

Genians는 중간 수준의 확신으로 이 캠페인을 북한 연계 Kimsuky 그룹의 활동으로 평가한다. [S15]

출처는 모방 가능성을 명시적으로 열어 둔다. 계정, 피싱 키트, 인프라의 겹치는 요소는 연관성을 뒷받침하지만, 흔히 악용되는 서비스만으로 책임 주체를 입증할 수는 없다. 이 보고서는 더 높은 확신도나 더 넓은 피해 집단을 채택하지 않는다.

방어 측면에서는 이메일 대화 맥락과 단말 이벤트를 함께 보존해야 한다. 요청했던 첨부파일은 불시에 온 파일보다 더 정상적으로 느껴질 수 있다. 예상하지 못한 지급·신원 서류는 알려진 채널로 확인하고, 스크립트 해석기를 실행하는 문서 주제의 압축파일을 조사하라.

발표는 최근이지만 설명된 서신 교환은 그보다 앞서 이뤄졌다. 따라서 보고서는 이를 마감 전 두 주 동안에 새로 발생한 공격이 아니라 이전 활동이 최근 공개된 사례로 다룬다.

국가정보원 발간자료 목록은 2026-06-08 에 등록된 2026 국가정보보호백서를 더 넓은 연례 국가 맥락 자료로 기록한다. [S128] 목록 페이지에서 연결된 PDF 본문을 직접 확인할 수 없었으므로 백서의 세부 문장은 이 보고서의 검증 범위 밖에 둔다. [S128]

7.3 일괄적인 공격자 지목 없이 국내 캠페인 연구 읽기

AhnLab이 2026-11-20 에 발표한 국내 시월 활동 검토는 스피어피싱, 바로가기 파일, 한글 문서 미끼를 설명한다. 출처에 따르면 관찰한 시월 집단에서는 바로가기의 비중이 가장 컸다. 공개 글은 전국 단위 분모를 제시하지 않는다. [S14][S97]

글의 공격자 태그는 설명된 모든 전달 과정을 한 그룹에 귀속시키지 않는다. 따라서 보고서는 해당 방식을 방어 계획에 활용하되 전체 집단을 Kimsuky의 활동으로 보지 않는다.

보안 운영에서는 문서·압축파일 이벤트를 자식 프로세스, 지속 실행, 후속 외부 통신과 연결해 살펴야 한다. 정상 원격 관리 소프트웨어나 클라우드 서비스도 악성 과정에 등장할 수 있다. 그 존재만으로 악성 판정을 내릴 수는 없다.

매트릭스와 표는 인용 연구에 대한 분석가의 행위 대응표다. 기법 정의는 MITRE ATT&CK와 대조해 확인했다. 공격자 식별 모델이 아니며, 모든 한국 대상에서 나열된 행위가 각각 발생했다는 주장도 아니다. [S90]

출처 연구에 기술된 기법과 분석가의 대응 관계, 전술별

실행	지속 실행	정보 반출
`T1204.002` 악성 파일: 문서처럼 보이는 바로가기, 분석가 대응표 [S14][S15][S90]	`T1053.005` 예약 작업: 보고된 반복 작업, 분석가 대응표 [S14][S15][S90]	`T1567.002` 클라우드 저장소: 보고된 정보 전송, 분석가 대응표 [S15][S90]
`T1059.001` PowerShell: 보고된 스크립트 흐름, 분석가 대응표 [S14][S15][S90]		

분석가의 행위 대응표. ID는 MITRE와 대조해 확인했으며 보안업체의 공격자 평가나 피해자 수가 아니다. [S90]

행위	방어 관찰 영역	최초 질문	출처
표적 문서 서신	이메일·단말	발신자의 업무 흐름이 알려진 업무 요청과 일치했는가?	[S14][S15]
스크립트를 실행하는 바로가기	프로세스 관측 자료	문서처럼 보이는 파일이 해석기를 시작했는가?	[S14][S15]
예약 작업을 통한 지속 실행	단말 변경	누가 작업을 만들었으며 어떤 행위가 뒤따랐는가?	[S14]
클라우드를 이용한 데이터 전송	프록시·단말	해당 이용자와 프로세스에서 예상되는 전송인가?	[S15]
브라우저 데이터 수집	단말·신원	계정·세션 경보가 프로세스 흐름을 뒷받침하는가?	[S14]

7.4 최근의 상거래 미끼도 중요하다

AhnLab의 십일월 연구는 구매 업무를 미끼로 한 악성코드 전달도 설명한다. 2026-11-12 공지는 SnakeKeylogger와 관련된 견적 압축파일을 다룬다. 2026-11-13 공지는 XLoader와 관련된 구매 주문 문서를 다룬다. 두 사례는 별개의 보안업체 관찰이다. [S16] [S17]

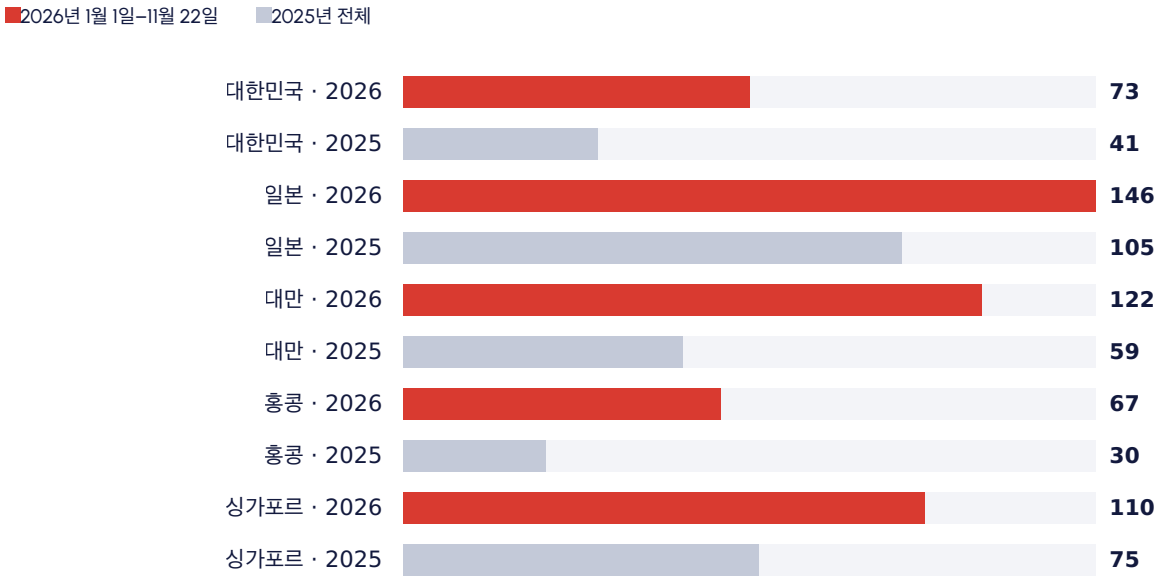
[GROUP commercial-malware]

구매·매입채무 담당팀은 첨부파일이 업무와 관련 있어 보인다는 이유만으로 신뢰해서는 안 된다. 보안 운영팀은 문서·압축파일 애플리케이션이 예상하지 못한 스크립트를 실행하는지 식별할 수 있어야 한다. 이어 같은 단말의 계정·세션 활동을 확인해야 한다.

직원 단말에서 악성코드를 발견했다고 기업 네트워크 침입이 입증되는 것은 아니다. 반대로 데이터 판매 광고가 나타나기 전에도 문서 미끼를 조사할 이유가 생길 수 있다. 외부 시장 관찰과 내부 단말 관찰은 서로 다른 목적을 가진다.

7.5 랜섬웨어와 갈취

대한민국의 가시적 게시 수는 선정한 지역 비교 대상 세 곳보다 적다



출처: Brandefense Ransompedia 게시 주장 [S2]. 2026년은 1월 1일–11월 22일이며 마감일은 일부이고, 2025년은 전체 연도다. 기간과 출처의 가시성이 달라 국가별 위험 순위를 의미하지 않는다.

비교 대상 국가는 맥락을 제공하기 위한 예시로만 선정되었으며, 순위나 정치적 평가를 의미하지 않습니다.

Ransompedia는 요청된 기간에 대한민국 게시 73 건을 기록한다. 2025 년 전체는 41 건이다. 부분 연도와 전체 연도 수치는 같은 시점의 데이터에서 보이는 범위를 설명한다. 같은 기간 길이로 계산한 증가율이 아니다. [S2]

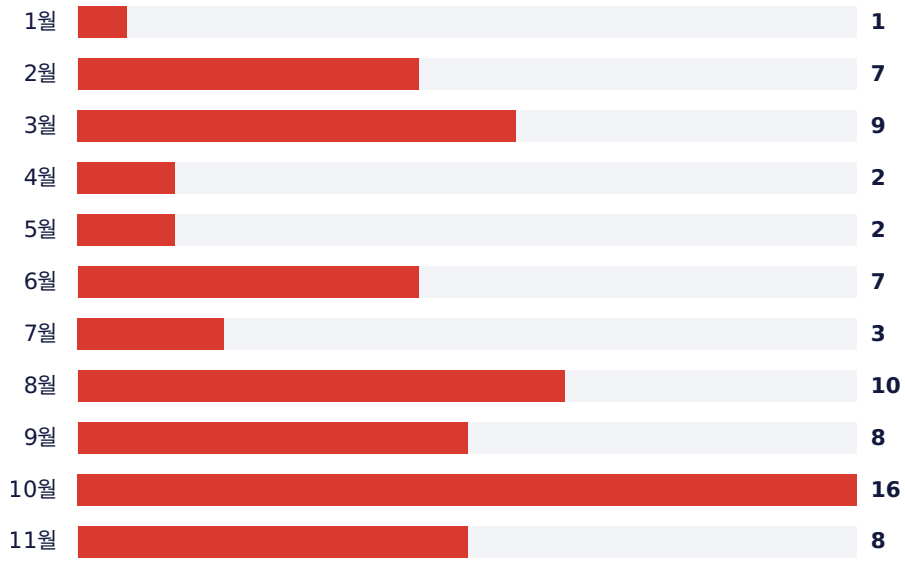
별도의 공식 맥락으로 개인정보보호위원회는 개인정보 유출 신고가 2023 년 318 건에서 2025 년 전체 447 건, 2026 년 상반기 432 건으로 집계됐다고 발표했다. [S125]

개인정보보호위원회의 유출 신고 건수와 Ransompedia의 범죄 갈취 게시는 서로 다른 집단을 측정하므로 합산해서는 안 된다. [S2][S125]

비교 대상	관찰 기간 게시	2025 년 전체	포함 이유
대한민국	73	41	보고서 대상 국가
일본	146	105	인접한 산업·공급업체 경제
대만	122	59	반도체·수출 맥락
홍콩	67	30	지역 금융 서비스 맥락
싱가포르	110	75	지역 금융·무역·디지털 서비스

비교 대상은 규모, 산업 구성, 공개 가시성이 다르다. 수치는 국가 보안 수준의 순위를 매기거나 조직이 공격받을 확률을 추정하지 않는다. 국가·지역 표기는 정치적 추론 없이 비교 목적으로 사용한다.

이 데이터에서는 대한민국의 시월 게시 수가 가장 많다

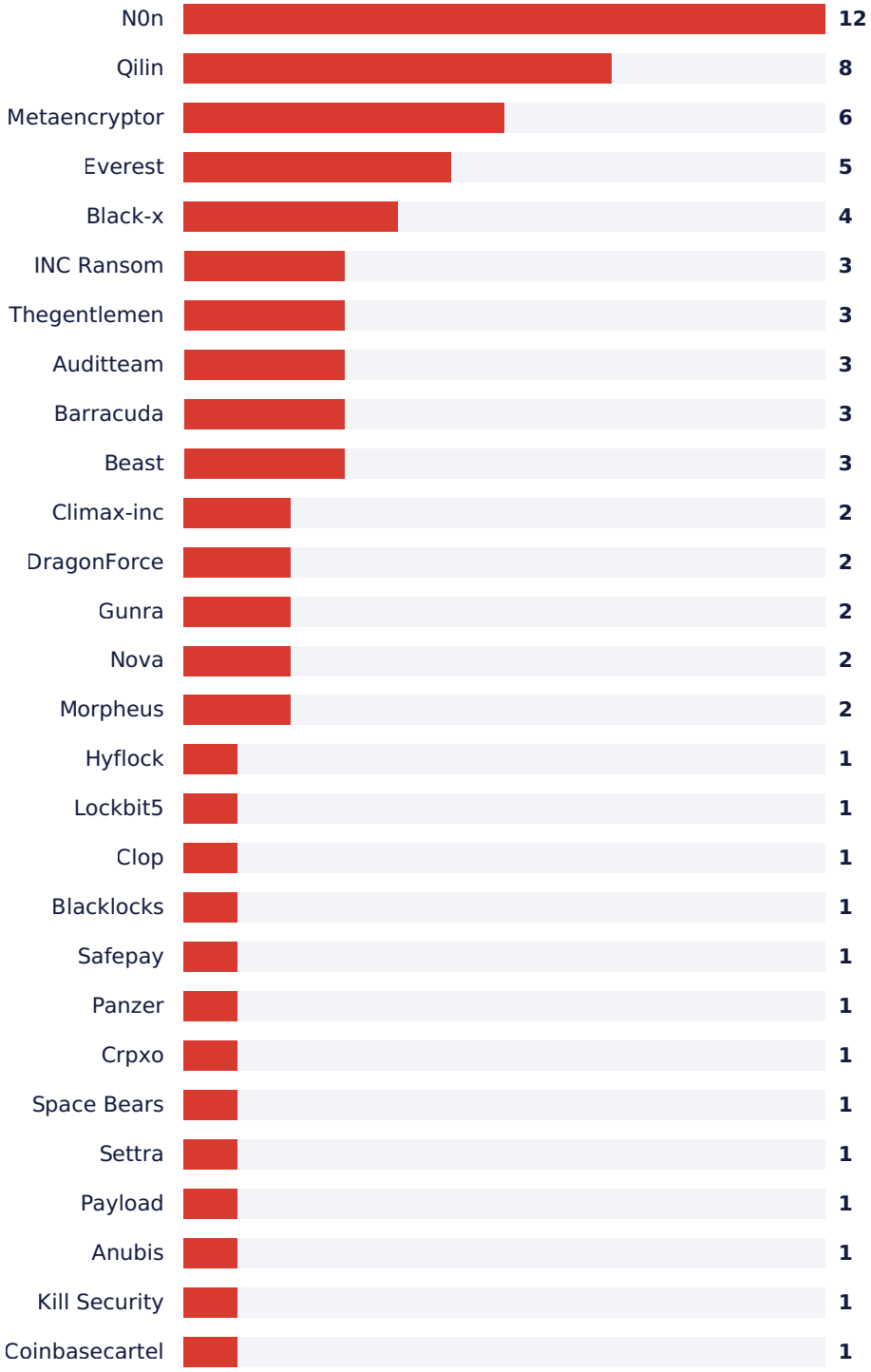


출처: Brandefense Ransompedia 게시 주장 [S2]. 2026년은 1월 1일–11월 22일이며 마감일은 일부이고, 2025년은 전체 연도다. 기간과 출처의 가시성이 달라 국가별 위험 순위를 의미하지 않는다.

월	게시	월	게시
일월	1	칠월	3
이월	7	팔월	10
삼월	9	구월	8
사월	2	시월	16
오월	2	십일월 마감일까지	8
유월	7	합계	73

시월의 게시 16 건은 공개 시점에 관한 관찰이며 침입 시작 건수의 측정이 아니다. 그룹이 오랜 시간이 지난 뒤 자료를 게시할 수 있다. 십일월은 일부 기간이므로 완전한 한 달과 비율을 비교해서는 안 된다.

상위 세 주장자 명칭이 게시 73 건 중 26 건을 차지한다



출처: Brandefense Ransompedia 게시 주장 [S2]. 2026년은 1월 1일–11월 22일이며 마감일은 일부이고, 2025년은 전체 연도다. 기간과 출처의 가시성이 달라 국가별 위험 순위를 의미하지 않는다.

N0n은 게시 12 건, Qilin은 8 건, Metaencryptor는 6 건을 차지한다. 합하면 73 건 중 26 건으로 35.6% 를 차지한다. 나머지 47 건에는 다른 명칭이 붙어 있다.

이 이름은 주장을 식별하며, 고유한 사람이나 독립적으로 확인된 제휴 공격자를 뜻하지 않는다. [S2]

랜섬웨어 주장자 명칭

갈취 게시 집단 | 국가 연계는 평가하지 않음

대한민국, 2026년

2026
요청된 기간의 대한민국 게시 73 건

주장된 표적

게시에 붙은 부문 분류이며 여기서는 피해자를 실명으로 밝히지 않음

공개 출처의 설명

[S2] Ransompedia는 날짜가 있는 게시 집단을 기록한다.

분석 평가

N0n, Qilin, Metaencryptor가 게시 73 건 중 26 건을 차지한다. 복구·공개에 대비하라. 게시 상태가 확인된 사고를 입증하지는 않는다.

확신도
보관 게시 수에 대해서는 높음. 기초 내용은 주장으로 유지

N0n

갈취 게시 명칭 | 국가 연계는 평가하지 않음

대한민국, 2026년

2026
요청된 기간의 대한민국 게시 12 건

주장된 표적

보관 게시 집단에 붙은 분류 기준이며 여기서는 피해자를 실명으로 밝히지 않음

공개 출처의 설명

[S2] 자체 데이터의 게시 관찰 시점 자료

분석 평가

명칭은 갈취·정보 영향 평가·복구에 대비할 근거가 된다. 고유 운영자, 암호화, 완료된 지급, 확인된 정보 전송을 입증하지는 않는다.

확신도
보관 수치에 대해서는 높음. 기초 주장의 결과는 미확인

Qilin

갈취 게시 명칭 | 국가 연계는 평가하지 않음

대한민국, 2026년

2026
요청된 기간의 대한민국 게시 8 건

주장된 표적

보관 게시 집단에 붙은 분류 기준이며 여기서는 피해자를 실명으로 밝히지 않음

공개 출처의 설명

[S2] 자체 데이터의 게시 관찰 시점 자료

분석 평가

명칭은 갈취·정보 영향 평가·복구에 대비할 근거가 된다. 고유 운영자, 암호화, 완료된 지급, 확인된 정보 전송을 입증하지는 않는다.

확신도
보관 수치에 대해서는 높음. 기초 주장의 결과는 미확인

Metaencryptor

갈취 게시 명칭 | 국가 연계는 평가하지 않음

대한민국, 2026년

2026
요청된 기간의 대한민국 게시 6 건

주장된 표적

보관 게시 집단에 붙은 분류 기준이며 여기서는 피해자를 실명으로 밝히지 않음

공개 출처의 설명

[S2] 자체 데이터의 게시 관찰 시점 자료

분석 평가

명칭은 갈취·정보 영향 평가·복구에 대비할 근거가 된다. 고유 운영자, 암호화, 완료된 지급, 확인된 정보 전송을 입증하지는 않는다.

확신도
보관 수치에 대해서는 높음. 기초 주장의 결과는 미확인

가장 큰 산업 분류는 제조업으로, 게시 73 건 중 19 건이다. 분류가 넓거나 부정확할 수 있다. 이를 전국 제조업 사고율 계산에 쓰기보다 생산, 공급업체, 엔지니어링 데이터 시나리오를 훈련에 포함하는 근거로 활용하라.

7.6 범죄 활동 계정과 증거의 한계

페르소나	보관 자료에서의 역할	한계
FantancyHacker	대출 자료 광고	파일 출처, 독점 판매와 대상 규모는 미확인
Solonik	데이터베이스 관련 게시물	행 단위가 섞여 있으며, 호스팅·입주 서비스 귀속은 미확정
zSenior	특권 접근 제안	글 안에서 증거에 대한 이의가 제기됐으며, 데이터베이스 탈취는 입증되지 않음
0xCAFE	여러 시스템의 자료 묶음	여러 서비스가 나온다고 별도 침입이 입증되는 것은 아님
TunaFish	원격 접근 광고	활성 접근 권한과 거래 성립은 미확인
HighWayToShell	클라우드 관리자 제안	다른 보험사 관련 제안과의 연계는 입증되지 않음
taltikgoo	기술 문서 제안	공급 관계가 고객사 사고를 입증하지는 않음
Noiem	개인정보·조달 자료 제안	범주가 겹치며, 공식 공개 파일과의 동일성은 미확인
DataJava	최근 관리자·자료 제안	비슷한 설명은 출처 검토 단서이지 동일한 백엔드의 증거가 아님

실무적인 질문은 보관한 각 게시물이 무엇을 입증하는지다. 판매자는 데이터를 광고하고, 구매자는 접근을 요청하며, 다른 계정은 같은 제목을 전달할 수 있다. 어느 역할도 그 자체로 최초 탈취, 성공한 판매, 지속 접근을 입증하지 않는다.

위협 인텔리전스팀은 활동 계정, 게시 공간, 주장된 데이터셋, 관찰한 게시물을 별도 기록으로 유지해야 한다. 관계를 평가할 때는 구체적인 증거와 한계를 설명해야 한다. 보고서의 사례 카드는 인용 자료 옆에서 이러한 구분을 유지한다.

핵심 요점

01

Genians의 중간 수준 확신도와 모방 가능성을 유지하라.

02

랜섬웨어 명칭을 주장으로 다루고 관련 업무 영향에 맞춰 복구를 시험하라.

03

신뢰하는 업무 절차를 미끼로 한 접근을 단말·신원 증거와 대조한 뒤 사고의 공격 주체를 판단하라.

장 08

사기, 신원, 정보 재사용 문제

이 장에서 답하는 질문

사기 요청을 받은 조직에 새 침입이 없어도 유통 정보가 어떻게 피해를 만들 수 있는가?

4

시험할 업무 절차: 복구, 신규 가입, 지급, 공급업체 연락

8.1 광고는 수요와 공급 주장을 보여준다 74

8.2 결제 카드 자료: 제한된 관찰 74

8.3 공식 경고에 나타난 후속 사기 75

8.4 가격은 거래 증거가 아니라 주장이다 76

8.5 시험할 만한 네 가지 업무 절차 76

8.6 보안팀과 고객 운영팀을 연결하라 76

장 08

사기, 신원, 정보 재사용 문제

요약

범죄시장 자료·공식경고는 신원·관계정보 재사용을 가리킨다. 메시지가 실제 예약·근무지·고객정보를 인용해도 권한의 증거는 아니다. 카드자료는 제한된 관찰이며 전국 손실이 아니다. 개인정보를 아는 상대에 대비해 계정복구·지급변경을 시험하라. 공급업체 메시지는 기존 연락처로 확인하고 증거가 뒷받침하는 사기는 담당팀에 전달하라.

8.1 광고는 수요와 공급 주장을 보여준다

보관된 제안에는 개인정보, 계정 관련 기록, 고객 연락처와 관리자 접근 권한이 등장한다. 여러 서비스의 자료를 한 묶음으로 제시하는 판매자도 있고, 보유를 주장하기보다 자료를 구하는 사람도 있다.

거래 성립을 입증하지는 않지만 업무 절차를 점검할 근거는 된다. [S1]

신원 데이터 제안, 계정 요청, 인증을 약속하는 서비스는 별개 관찰로 유지해야 한다. 서로 보완되는 능력을 설명할 수는 있지만, 한 운영자가 이를 획득하거나 결합했음을 보여주지는 않는다.

방어자에게 유용한 질문은 절차가 알려진 개인정보를 비밀로 취급하는지다. 이름, 연락처, 정확한 업무 관계는 접근을 설득력 있게 만들 수 있다. 위험한 변경의 권한은 추가 인증과 신뢰할 수 있는 재연락 경로로 판단해야 한다.

8.2 결제 카드 자료: 제한된 관찰

카드 수치의 범위

이 수치는 보관 게시물 집단의 결제 카드 기록을 설명한다. 전국 카드 노출, 카드 정보 탈취, 사기 손실을 측정하지 않으며, Brandefense의 더 넓은 카드 관찰 범위를 대표하지 않는다.

보관 게시물 증거에는 서로 다른 결제 카드 기록 365 건이 게시물 424 건에 나타나며 발급사 접두부 187 개와 연관된다. 이는 코퍼스 관찰이며 유효성·출처·사기 피해액은 미확인이다.

전국 카드 노출이나 Brandefense의 전체 카드 탐지 범위를 측정하지 않는다. [S4]

카드 브랜드별 수치는 보관 게시물 증거에만 해당한다



출처: 보관 게시물의 결제 카드 집계 증거 [S4]. 카드 기록은 고유 카드 소지자, 손실, 전국 발생 비율이 아니다.

브랜드 접두부 기준으로는 기록 365 건이 Visa 149 건, Mastercard 116 건, UnionPay 및 국내 제휴 브랜드 94 건, Amex 3 건, 기타·미분류 브랜드 3 건으로 구분된다. [S4]

이 관찰 결과를 공식 침해 총계에 합치거나 특정 은행 침입의 증거로 해석해서는 안 된다. 발급사의 조사는 자체 승인·사기 신호에 근거해야 한다. 재발급이나 고객 이용 제한에는 발급사 정책에 따른 확인이 필요하다.

8.3 공식 경고에 나타난 후속 사기

KISA의 오월 경고는 도난당한 여행 예약 정보가 호텔 사칭과 결제 재확인 메시지에 재사용되는 양상을 설명한다. 유월 경고는 스트리밍 서비스의 사고 공개 뒤 보상·환불 피싱이 발생할 가능성에 대비하도록 한다.

전자는 보고된 재사용이고, 후자에는 예상되는 2 차 악용이 포함된다. 어느 쪽도 전국 사기 피해액 총계를 제시하지 않는다. [S26] [S28]

경찰이 작성한 2026-03-27 재게시 경고는 여행 환불·사칭·투자·연애·기부 유인을 다룬다. 2026-03-23 국내 보도는 보고된 시도와 실제 피해를 구분했다. 이는 예방 시나리오이며 검증된 피해액이 아니다. [S109][S110]

관찰된 후속 악용과 예상되는 후속 악용은 구분해야 한다. 공개 이후 환불 사기가 뒤따를 수 있다는 경고는 대비를 위한 안내다. 경고한 모든 사기가 발생했거나 측정된 손실을 냈다는 증거가 아니다.

고객 안내에는 정상 조직이 불시에 보낸 메시지로 절대 요구하지 않는 정보를 명시하라. 발신자의 링크나 전화번호를 사용하지 않고도 주장을 확인할 수 있는 신뢰 경로를 제공하라.

8.4 가격은 거래 증거가 아니라 주장이다

제안	요구 가격	증거의 한계
원격 관리자 접근 권한, 사례 E	898 USD	광고 1 건이며, 사용 가능한 접근 권한과 거래는 미확인
업무 시스템 데이터셋	900–1,000 USD	일부 판매 제안이며, 파일과 거래는 미확인
최근 관리자·고객 데이터 제안	4,500 USD	주장한 접근 권한과 대상 규모는 미확인
최근 CRM 관련 제안	4,550 USD	관리자 내보내기라는 주장으로, 접근 권한은 검증되지 않음

보관된 게시물에서 따로 광고한 항목들이다. 대표성 있는 가격 분포는 아니다. [S1]

제시 가격은 판매자의 표현 방식과 겨냥한 고객을 설명할 수 있다. 시장 가치, 파일 진위, 그 가격의 수요, 완료된 거래를 입증하지 않는다. 접근 권한, 기록, 구독, 서비스 가격은 서로 대체 가능한 단위가 아니다.

광고 수량도 행, 주문, 파일, 계정을 뜻할 수 있다. 데이터셋에는 한 사람에 대한 여러 기록이나 여러 조직의 정보가 담길 수 있다. 수량을 피해자 수로 바꾸지 말고 판매자가 밝힌 단위와 불확실성을 유지하라.

8.5 시험할 만한 네 가지 업무 절차

절차	시험 조건	책임자	완료 증거
계정 복구	발신자가 정확한 개인정보와 관계 정보를 알고 있음	신원·고객 운영팀	위험한 변경에는 독립 확인이 필요함
신규 가입	신청자가 노출 파일의 그럴듯한 신원 정보를 제시함	사기 대응·준법팀	추가 확인이 실제 위험을 다룸
지급 변경	메시지가 실제 공급업체 청구서나 예약을 인용함	재무·서비스 책임자	변경 전에 기존 연락처로 확인함
직원 지원	요청이 내부 이름과 평가 문서를 인용함	헬프데스크·보안팀	특권 변경에는 승인된 경로가 필요함

합성 사례와 승인된 훈련을 사용하라. 실제 피해자의 정보를 유통하지 않으면서, 정보를 아는 것을 권한으로 오인하는 절차를 찾는 것이 목적이다.

8.6 보안팀과 고객 운영팀을 연결하라

사고 대응팀은 고객 관계를 이해하기 전에 기술 범위를 파악할 수 있다. 고객센터는 보안팀이 일치하는 광고를 보기 전에 의심스러운 접근을 발견할 수 있다. 두 팀 모두 불필요한 개인정보를 퍼뜨리지 않고 관련 사실을 교환할 방법이 필요하다.

고객이나 직원이 무엇을 받았는지, 어떤 관계 정보가 정확했는지, 메시지가 어떤 행동을 요구했는지 기록하라. 정보의 출처에 대한 가정은 이 제보와 구분하라.

새로운 공개로 확인된 정보 범주가 바뀌면 사기 감시와 고객 안내를 갱신하라. 원래 애플리케이션이 복구됐다는 이유로 끝내지 말고, 관련 업무 절차가 여전히 안전한지 확인한 뒤 종결하라.

핵심 요점

01

정확한 개인정보는 권한을 입증하지 않는다.

02

광고 수량과 제한된 카드 관찰을 전국 손실 추정에 포함하지 마라.

03

합성 사례와 책임자를 정해 복구, 지급, 공급업체 업무 절차를 시험하라.

장 09

은행과 금융 서비스

09

이 장에서 답하는 질문

금융회사는 애플리케이션 보안, 신원 확인, 고객 보호를 어떻게 연결해야 하는가?

37

금융위원회가 특정 기간에 공개한 대상 회사

9.1 대상 집단과 구분 79

9.2 기간이 명시된 공식 공개 집단 79

9.3 평가 서비스 증거 80

9.4 업무 인터페이스를 자산 목록에 포함하라 80

9.5 고객과 직원 보호 81

9.6 경영진이 물을 질문 81

장 09

은행과 금융 서비스

요약

금융 증거의 애플리케이션·신고집단·정보범주는 다르다. 금융위원회는 명시된 기간의 37개사 관련 사례 40건을 설명했다. 별도 십일월 공개는 금융보안원 평가서비스를 다룬다. 핵심 은행시스템이나 모든 고객 자격증명에 접근했다는 뜻은 아니다. 외부 인터페이스·지원앱을 검토하고 접근증거를 보존하며 고객보호팀을 사고판단에 참여시켜라.

9.1 대상 집단과 구분

선정 포트폴리오에는 은행·결제 도메인 25 개와 보험·자본시장 도메인 25 개가 있다. 기능이 서로 다르며 관련 기업 집단이 포함될 수 있다. 독립적으로 확인된 은행이나 발급사 50 곳을 뜻하지 않는다.

은행·결제 집단의 도메인 25 개 중 기기 연관 기록은 24 개, 과거 자격 증명 기록은 23 개, 현재 자격 증명 판매는 15 개에서 관찰됐다.

기기 연관 기록은 55,600 건이며 직원 분류 152 건과 기타 분류 55,448 건이다. 과거 자격 증명 기록은 150,216 건이다. [S3]

별도 보험·자본시장 집단의 도메인 25 개 중 기기 연관 기록은 25 개, 과거 자격 증명 기록은 24 개, 현재 판매는 17 개에서 관찰됐다.

기기 연관 기록은 21,508 건이며 직원 분류 107 건과 기타 분류 21,401 건이다. 과거 자격 증명 기록은 92,116 건이다. [S3]

카드 귀속은 도난 출처를 특정하지 않는다. 발급사는 사고를 판단하기 전에 관련 신호를 자체 계정·단말·사기 증거와 대조해 확인해야 한다.

보관 게시물의 결제 카드 자료는 별개의 제한된 관찰이다(§8.2). 전국 카드 노출, 카드 정보 탈취, 사기 손실을 측정하지 않는다. 이를 은행 침입의 근거로 삼거나 광고를 공식 사고와 연결해서는 안 된다.

9.2 기간이 명시된 공식 공개 집단

금융위원회의 2026-11-05 발표는 2026-09-30 부터 2026-11-03 까지 금융회사 37 곳과 관련된 사례 40 건을 보고한다. 개인정보 항목은 약 473,000 건으로 설명한다. 같은 발표는 당시까지 고객 계좌 비밀번호가 탈취됐다는 신고는 없었다고 밝혔다. [S5]

이 경계는 중요하다. 사용 가능한 은행 비밀번호가 없어도 개인정보는 설득력 있는 사칭에 쓰일 수 있다. 고객 안내와 사기 감시는 이 경로를 다뤄야 한다. 기술 조사팀은 어떤 애플리케이션과 계정이 관련됐는지 확인해야 한다.

금융위원회는 예정된 검사와 규정 변경도 설명한다. 예정된 조치는 검사가 완료됐거나 법률이 제정됐다는 증거가 아니다. 제 10 장은 현재 신고 안내와 발표된 정책 작업을 구분한다.

금융위원회의 2026-10-14 발표는 금융회사 사고 중 스트리미 사례를 명시적으로 확인한다. 국내 보도는 스트리미가 고팍스 운영사라고 설명한다. 감독당국은 경로와 사건 간 관계를 조사 중이었으며 집계 결과 전체를 해당 조직에 그대로 적용해서는 안 된다. [S113][S114]

2026-11-18 후속 보도는 영향받은 인원 범위가 확대됐다고 전하며 사건일을 2026-09-08 로 설명한다. 보도는 감독 자료를 근거로 하지만 여기서 그 원문을 확보한 것은 아니다. 최초 추정치를 최종 수치로 제시하지 않으며 자금 손실도 추론하지 않는다. [S115]

9.3 평가 서비스 증거

사례 P

P

평가 데이터와 거래 시스템은 다르다

금융보안 서비스

공식 공개. 범위 한계 유지

공식 설명	금융보안원은 2026-11-09 에 탐지한 상시평가 시스템의 비정상 외부 접근을 공개했다. 접근을 차단하고 조사를 시작했다. [S6]
보고된 범위	금융보안원은 행정 서식 약 200 건, 서식 내 개인정보 항목 300 건, 시스템 이용자 항목 350 건을 설명했다. 이 범주는 겹칠 수 있으며 고유한 사람 수의 합계가 아니다.
경계	금융보안원은 해당 시스템이 일반 고객의 금융 거래를 처리하지 않았다고 밝혔다. 당시 설명한 범위에서는 금융 시스템 구조와 명시된 민감한 고객 정보가 제외됐다.
보도 확인	연합뉴스는 금융보안원의 공개 내용을 보도했다. 이는 공개 사례를 실명으로 다룰 근거가 되지만, 금융보안원 설명을 넘어서는 사실을 입증하지는 않는다. [S7]
대응	금융회사는 평가·지원 서비스에 제출한 문서를 파악하고, 수신자의 접근 권한을 확인하며, 관련 기록을 보존하고, 영향받은 직원의 사칭 위험을 평가해야 한다.

결론

명시된 방식과 정보 범위를 따르고 대응에서 날짜, 대상 집단, 공격자 평가의 한계를 유지하라.

평가 서비스는 결제 플랫폼을 운영하지 않아도 사회공학에 유용한 정보를 보유할 수 있다. 가장 민감한 시스템이 관련됐다고 가정하지 말고 노출 범주와 업무 관계에 따라 대응해야 한다.

9.4 업무 인터페이스를 자산 목록에 포함하라

첫 검토에는 개인정보를 노출하거나 업무 흐름의 상태를 변경할 수 있는 인터페이스를 포함해야 한다. 협력사 접근, 지원 포털, 직원 애플리케이션, 교육·평가 서비스를 포함하라. 이용자가 적은 애플리케이션도 접근이 제한돼야 할 정보를 보유할 수 있다.

각 인터페이스의 책임자, 인증 방식, 허용된 객체, 내보내기 기능을 기록하라. 적절히 승인된 계정으로 접근을 시험하라. 한 이용자가 다른 이용자의 기록을 요청할 수 있다면 로그인 성공 여부만 시험해서는 충분하지 않다. [S92]

사고 대응팀이 계정과 접근한 객체를 모두 식별할 수 있게 하라. 로그 보존은 접근, 내보내기, 관리 변경을 의미 있게 검토할 수 있어야 한다. 정기 순환으로 기록이 사라지기 전에 보존하라.

9.5 고객과 직원 보호

증거	확인할 위험	공동 책임자	최초 조치
직원 연락처 공개	설득력 있는 내부 사칭	보안·인사팀	신뢰 채널로 직원에게 경고
고객 신원 정보 공개	복구·고객센터 사칭	사기 대응·고객 운영팀	위험한 복구 판단 강화
활성 자격 증명이 추가 증거로 확인됨	무단 계정 사용	신원·사고 대응팀	관련 세션을 폐기하고 차단
비정상 수취인·기기 변경	거래 악용	디지털 뱅킹·사기 대응팀	적절한 확인 적용
처리업체의 통지	공유 기록과 통지 의무	구매·개인정보 보호·업무 책임자	범위 확인과 증거 보존

이는 조건부 대응 경로이며, 나열한 피해가 발생했다는 조사 결과가 아니다. 고객 보호 판단은 확인된 정보 범주와 남은 불확실성에 비례해야 한다.

9.6 경영진이 물을 질문

이사회는 외부 업무 인터페이스에 책임자가 있는지, 무단 객체 접근을 탐지할 수 있는지 물어야 한다. 조사에서 최종 수치가 나오기 전에 고객 연락 계획이 준비돼 있는지도 확인해야 한다.

CISO는 미해결 애플리케이션과 증거 공백을 날짜·책임자와 함께 보고해야 한다. 사기 대응 책임자는 알려진 신원 정보만으로 계정 복구나 지급 변경을 승인할 수 없음을 보여줘야 한다.

핵심 요점

01
공식 신고, 선정 도메인 신호, 카드 자료를 구분하라.

02
거래 플랫폼과 함께 지원·협력사 애플리케이션을 검토하라.

03
확인된 정보 범주를 계정, 직원, 고객 보호에 연결하라.

장 10

규제와 국가 대응

10

이 장에서 답하는 질문

한국 조직은 현행 의무와 발표된 대책 중 무엇을 구분해야 하는가?

72 시간

개인정보보호위원회의 조건부 유출 신고 안내에 명시된 기간

10.1 현행 개인정보 유출 신고 안내 83

10.2 구월 변경과 이후 시행되는 인증 조항 83

10.3 금융 분야 발표는 시점이 있는 정책 증거다 84

10.4 시간 계산 전에 적용 범위를 확인하라 84

10.5 신고 절차를 훈련하라 85

장 10

규제와 국가 대응

요약

개인정보 신고·정보주체 통지·부문별 감독을 구분하라. 개인정보보호위원회의 구월 시행변경 설명에는 유출가능성 통지·사고범위 확대가 포함된다. 별도 인증의무는 시행일이 늦다. 금융위원회의 십일월 대책에는 법적 전환을 완료하지 않은 계획도 있다. 개인정보 법률담당자에게 적용여부를 확인받고 판단책임자를 정하며 인지기록·초기증거를 보존하라.

10.1 현행 개인정보 유출 신고 안내

개인정보보호위원회 안내에 따르면 개인정보처리자는 열거된 조건 중 하나에 해당하면 72 시간 이내에 신고해야 한다. 조건에는 정보주체 1,000 명 이상, 민감정보·고유식별정보, 불법적인 외부 접근을 통한 유출이 포함된다. [S9]

마지막 조건은 소규모 사고에도 중요하다. 1,000 명 미만이라는 이유로 모든 신고 의무가 사라진다고 가정해서는 안 된다. 법적 평가는 대상 집단뿐 아니라 사건, 정보 범주, 접근 경로도 다룬다.

안내는 KISA를 지정 신고 기관으로 명시한다. 별도로 금융회사와 관련 신용정보 사업자에게 적절한 경로를 금융감독원에 확인하도록 안내한다. 같은 페이지는 다른 법률의 적용을 받는 개인신용정보도 구분한다. [S9]

이 보고서는 의사결정을 돕는 자료이며 법률 자문이 아니다. 법률 담당자는 해당 조직의 현행 법령, 적용 예외, 부문별 규정, 신고 절차를 확인해야 한다. 관련 사실을 알게 된 시점을 기록하라.

조직의 인지 시점 대신 공격자의 게시일을 사용해서는 안 된다.

10.2 구월 변경과 이후 시행되는 인증 조항

개인정보보호위원회의 2026-09-10 발표에 따르면 개정 법률과 시행 규정은 2026-09-11 에 시행된다. 발표는 유출 가능성 통지, 통지 항목 확대, 랜섬웨어를 포함한 위조·변조·훼손의 포괄을 설명한다. [S10]

발표는 최고경영진과 개인정보 보호책임자의 강화된 관리 책임도 설명한다. 그렇다고 구체적인 시행 조건을 짧은 공개 요약과 모두 같은 것으로 볼 수는 없다. 조직은 자체 적용 여부를 판단할 때 기준이 되는 법령을 확보해야 한다.

별도의 ISMS-P 의무 조항은 2027-07-01 시행으로 설명된다. 이 늦은 시행일을 보고서 마감 시점에 이미 적용되는 의무처럼 제시해서는 안 된다. [S10][S93]

제도	확인된 상태	경영진의 즉시 과제
개인정보보호위원회 유출 신고 안내	조건부 신고 기간과 경로 설명	사건·정보·조직 범위 확인
구월 개인정보 보호 변경	위원회가 명시한 시행일은 2026-09-11	통지·관리 절차 갱신
유출 가능성 통지	구월 체계에서 도입	법률 담당자의 발동 조건·내용 점검표 확보
ISMS-P 의무 조항	명시된 이후 시행일은 2027-07-01	적용 여부와 이행 계획 판단
금융 분야 의무	별도 금융 신고 경로 명시	금융감독원 및 기타 적용 의무 확인

데이터 반출이 확인되지 않았다는 사실만으로 모든 통지 검토를 끝낼 수는 없다. 새 유출 가능성 통지 체계는 불법 접근은 알려졌지만 영향받은 사람을 아직 모두 식별하지 못한 경우에 특히 중요하다.

10.3 금융 분야 발표는 시점이 있는 정책 증거다

금융위원회의 십일월 프로그램은 외부 업무 인터페이스 점검 확대와 명확한 경영 책임을 제안한다. 감독, 정보 공유, 평가 요건의 예정된 변경도 설명한다. [S5]

발표는 디지털금융 안전 법안을 2027 년 첫 분기에 추진할 계획이라고 밝힌다. 이 보고서는 이를 예정된 입법으로 다룬다. 법안이 제정됐거나 발표된 일정이 이행을 입증한다고 설명하지 않는다.

금융회사가 단기에 취할 유용한 대응은 외부에서 접근 가능한 업무 애플리케이션과 책임 임원을 포함한 자산 목록을 유지하는 것이다. 어떤 시스템에 접근했으며 어떤 정보가 영향을 받았는지 설명하는 데 필요한 증거를 보존하라.

10.4 시간 계산 전에 적용 범위를 확인하라

조직	준비할 판단	책임 기능
개인정보처리자	신고 조건, 정보주체 통지, 인지 기록	개인정보 보호·법무·사고 대응
금융회사	금융 신고 경로와 기타 적용 개인정보 보호 의무	준법·개인정보 보호·CISO
수탁자 또는 업무 공급업체	계약상 경보, 증거 보존, 개인정보처리자 지원	구매·법무·서비스 책임자
공공기관	관할 기술·개인정보 보호 채널	보안 부서·개인정보 보호책임자
한국에 서비스를 제공하는 해외 업체	국내 적용 여부와 이용 가능한 신고 절차	법무·해당하는 경우 국내 대리인

공급업체 계약에는 누가 최초 사고 경보를 보내고 누가 접근 기록을 제공할 수 있는지 명시해야 한다. 관련 경보를 개인정보처리자에게 전달할 때마다 최종 포렌식 결론을 요구해서는 안 된다.

인지, 확인된 사실, 불확실성, 법률 검토, 후속 갱신을 담은 판단 기록을 유지하라. 대상 집단 추정치가 바뀌면 최초 기록을 설명 없이 대체하지 말고 통제된 갱신을 해야 한다.

10.5 신고 절차를 훈련하라

지원 서비스가 불법 접근을 알렸지만 영향받은 사람을 아직 모두 식별하지 못한 상황을 사용하라. 개인정보 보호팀은 검토할 의무를 판단하고, 서비스 책임자는 보유 기록을 설명하며, 대응팀은 증거를 보존하게 하라.

이후 두 번째 사실을 추가하라. 암호화된 계정 정보나 내부 평가 문서가 관련됐다는 상황이다. 훈련은 근거 없는 최종 총계를 주장하지 않으면서 고객 보호·신고 판단을 어떻게 바꾸는지 보여줘야 한다.

완료 기준은 날짜가 있는 적용 판단 기록, 채널별 책임자, 시험한 갱신 절차다. 정책 문서에 감독 기관 이름만 적는 것으로는 충분하지 않다.

핵심 요점

01
신고와 정보주체 통지 의무를 별도로 평가하라.

02
현행 요건을 이후 시행일·예정 입법과 구분하라.

03
인지 시점을 기록하고 증거를 보존하며 초기 통지 절차를 시험하라.

장 11

전망과 조건부 시나리오

11

이 장에서 답하는 질문

어떤 평가가 대비의 근거가 되며, 어떤 증거가 그 평가를 바꿀 것인가?

4

발동 조건이 명확한 조건부 계획 시나리오

11.1 핵심 평가 87

11.2 평가를 바꿀 증거 87

11.3 네 가지 계획 시나리오 88

11.4 단독으로는 불충분한 신호 88

장 11

전망과 조건부 시나리오

요약

증거는 신원악용·주변 업무앱 노출·갈취·신뢰하는 업무절차를 이용한 피싱에 대비할 근거다. 전국 공격확률이나 최근 공개 사례의 공통 공격자를 입증하지 않는다. 시나리오는 계획가정으로 다뤄라. 내부증거·공식갱신·검증표본이 판단전제를 바꾸면 우선순위를 바꿔라. 훈련으로 성과를 입증할 통제에 예산을 배정하라.

11.1 핵심 평가

평가	확신도	근거와 한계
주변 업무 애플리케이션을 주요 보안 검토에 포함해야 함	공개된 대응 필요성에 대해 높음	금융·평가 서비스 공개 사례이며 전국 시스템 구조 조사 결과는 아님
신원 정보는 설득력 있는 후속 사칭을 뒷받침할 수 있음	계획 판단으로서 중간	노출 범주와 공식 경고 주제에 근거하며 실제 손실은 여기서 측정하지 않음
갈취 대비에 지속 투자가 필요함	가시적 게시 집단에 대해 높음	게시 73 건이며 비공개 사고와 확인된 결과는 미상
신뢰하는 서신은 여전히 중요한 피싱 접점임	인용 캠페인에 대해 높음	공식·보안업체 설명에 근거하며 전국 빈도 추정은 없음
최근 공개된 사례들의 공격자가 같음	입증되지 않음	시점이 가깝다는 사실은 구체적 연결을 제공하지 않음

확신도는 각각의 명제에 붙는다. 두 사고 모두 한국어 서신과 관련됐다는 이유만으로 한 캠페인에 대한 출처의 확신도를 다른 사고에 옮길 수는 없다.

11.2 평가를 바꿀 증거

현재 입장	새로운 증거	영향을 받는 판단
데이터 광고는 미확인 상태	표본이 보호된 내부 기록 및 접근 증거와 일치함	조사를 상향하고 통지를 검토
자격 증명 연관 기록에는 확인이 필요함	활성 특권 계정과 의심 세션이 일치함	계정과 관련 세션 차단
최근 별개 사고들 사이의 연결은 입증되지 않음	구체적 공통 인프라 또는 출처가 뒷받침하는 캠페인 평가	공조 여부와 탐색 범위 재검토
보안업체가 이전 캠페인을 설명함	조직 자체 관측 자료에 새 활동이 나타남	과거 비교에서 실제 대응으로 전환
공식 대상 집단이 잠정 상태	개인정보처리자가 근거 있는 수정치를 공개함	영향·고객 보호 판단 갱신

이 표는 광고를 예상 손실로 바꾸는 흔한 전망 오류를 피한다. 외부 신호는 피해 가능성이나 규모를 입증하지 않아도 확인 과제를 시작할 근거가 될 수 있다.

11.3 네 가지 계획 시나리오

시나리오 A: 외부 애플리케이션이 정보를 노출한다

조직이 고객·직원·협력사 애플리케이션에서 무단 객체 접근 경로를 발견하면 영향받은 데이터와 권한의 범위를 확인하라. 접근 증거를 보존하고 경로를 안전하게 제한하며 개인정보 보호 담당자를 참여시켜라.

신호는 많은 게시물이 아니라 검증된 접근 통제 실패다.

시나리오 B: 신원 정보가 지급·복구 사기에 재사용된다

고객이 실제 관계 정보를 인용한 메시지를 받으면 정보가 노출됐는지, 해당 연락이 사기인지 확인하라. 신뢰 채널로 경고하고 위험한 복구·수취인 변경의 확인을 강화하라. 정확한 인적 사항만으로 권한을 인정해서는 안 된다.

시나리오 C: 갈취가 연속성과 엔지니어링 정보를 위협한다

신빙성 있는 주장이나 내부 탐지가 생산 지원·엔지니어링 시스템에 관한 것이라면 복구와 정보 영향 검토를 함께 시작하라.

독립된 복구 자격 증명으로 최소한의 안전한 서비스를 시험하라. 공개 게시만으로 암호화나 물리 공정 조작이 입증되는 것은 아니다.

시나리오 D: 신뢰하는 업무 절차가 악성 파일을 전달한다

세미나, 채용, 구매, 지원 요청에 관한 서신에서 예상하지 못한 압축파일·바로가기가 나오면 대화와 단말 행위를 대조하라. 스크립트 실행과 계정 활동을 함께 조사하라.

익숙한 주제나 요청했던 첨부파일이 정상임을 입증하지는 않는다.

11.4 단독으로는 불충분한 신호

국기, 언어, 정치적 구호는 국적을 입증하지 않는다. 별칭 일치는 단일 운영자를 입증하지 않는다. 최근 게시물은 최근 침입을 입증하지 않는다. 많은 행 수는 고유한 피해자 수를 입증하지 않는다.

게시가 없다고 조직이 갈취를 피했다는 뜻도 아니다. 공개적인 공격자 지목이 없다고 캠페인에 후원자가 없었다는 뜻도 아니다. 이러한 공백은 추론을 제한하며 반대 결론을 제공하지 않는다.

경영진은 실제 서비스 의존 관계와 대응팀이 확보할 수 있는 증거에 비춰 시나리오를 검토하라. 측정 가능한 소수의 훈련을 선정하라. 훈련이나 새 사고 사실이 더 중대한 공백을 드러내면 계획을 수정하라.

핵심 요점

01

시나리오를 예측이 아니라 조건부 대비로 다뤄라.

02

기초 명제가 바뀌면 판단을 재검토하라.

03

업무 책임자가 검토할 수 있는 확인, 고객 보호, 복구 증거에 예산을 배정하라.

장 12

실행 계획

12

이 장에서 답하는 질문

앞으로 90 일 동안 누가 조치하며, 무엇으로 완료를 입증할 것인가?

18

책임자와 종결 증거를 갖춘 조치

12.1 90 일 실행 일정 91
12.2 지표별 목표 93
12.3 역할별 과제 94
12.4 Brandefense의 지원 94

장 12

실행 계획

요약

실제로 통제하는 정보·서비스에서 시작하라. 경보책임을 정하고 활성계정 증거·외부 업무인터페이스를 검토하라. 공급업체 통지·고객복구 판단·서비스 복원을 시험하라. 이 계획은 작업순서이며 진행 중인 사고대응을 늦출 허가가 아니다. 90일째까지 완료증거·미해결 의존성·날짜가 명시된 개선조치를 이사회에 보고하라.

12.1 90 일 실행 일정

11–30 일

내부 또는 제공업체를 통해 관련 자격 증명·기기·데이터 제안 경보 경로 마련

책임자

CISO·위협 인텔리전스팀

완료 증거

지정된 출처·수신자와 최초 검토 경보

새 자격 증명 경보를 활성 계정·권한·세션과 대조

책임자

신원·계정 운영팀

완료 증거

경보별 날짜가 있는 처리 결과

지원 서비스를 포함한 외부 고객·협력사·직원 애플리케이션 목록화

책임자

애플리케이션·업무 책임자

완료 증거

서비스·데이터·책임자·인터페이스 목록

승인 계정으로 민감 객체와 대량 내보내기의 권한 통제 시험

책임자

애플리케이션 보안팀

완료 증거

허용·거부된 접근 증거

실제 서비스 런타임과 지원되는 업체 패키지에 비춰 최신 Java 권고 검토

책임자

인프라·애플리케이션 책임자

완료 증거

런타임 목록과 패치·완화 기록

개인정보·부문별 신고 조건, 채널, 인지 기록 확인

책임자

법무·개인정보 보호·준법팀

완료 증거

승인된 적용 판단·초기 통지 점검표

기록이나 관리 접근 권한을 보유한 주요 공급업체 파악

책임자
구매·데이터 책임자

완료 증거
공급업체 증거 담당 연락처와 사고 경보 경로

231–60 일

특권·원격 이용자의 피싱 저항성 MFA 우선 적용 [S91]

책임자
신원·업무 책임자

완료 증거
적용 범위 기록과 시험한 복구 경로

문서·압축파일 절차의 예상치 못한 스크립트 실행과 지속 실행 탐지

책임자
SOC·단말 엔지니어링팀

완료 증거
검토한 승인 모의훈련과 경보 증거

단계적 DMARC 집행 전에 정상 메일 발신자 확인

책임자
메시징팀

완료 증거
인증 정렬 검토, 승인 정책, 되돌리기 경로

정확한 개인정보를 아는 발신자를 가정해 고객 복구·수취인 변경 시험

책임자
사기 대응·고객 운영팀

완료 증거
합성 사례 거부 또는 공백 개선

공급업체 증거 전달과 잠정 통지 시험

책임자
구매·개인정보 보호·사고 대응팀

완료 증거
시간 기록이 있는 훈련 결과와 합의된 갱신

보호된 백업과 별도 자격 증명으로 핵심 서비스 하나 복원

책임자
인프라·업무 연속성팀

완료 증거
무결성 점검과 복구 목표에 따른 업무 승인

361–90 일

서비스 중단과 데이터 주장이 동시에 발생하는 상황 훈련

책임자
CISO·홍보팀

완료 증거
사실 중심 상태 안내, 증거 책임자, 갱신 시각

확인된 사고에서 노출된 특권 토큰·비밀정보 대조

책임자
신원·개발팀

완료 증거
폐기·교체·접근 검토 기록

인증서·갱신·공개 서비스 설정 예외 종결

책임자
네트워크·서비스 책임자

완료 증거
재확인 성공 또는 날짜가 있는 승인 예외

영향받은 사람이 처음에는 불확실한 상황의 통지 훈련

책임자
개인정보 보호·법무·업무 책임자

완료 증거
발동 조건 평가, 초기 내용, 갱신 판단

지표표와 남은 서비스 의존 관계 보고

책임자
CISO가 이사회에 보고

완료 증거
증거와 연결되고 날짜·책임자가 있는 이사회 기록

현재 진행 중인 무단 접근의 새 증거는 즉시 사고 대응으로 넘긴다. 일 단위 구간은 개선 작업을 정리할 뿐이다. 법정 기한이나 조직의 심각도 판단 절차를 대체하지 않는다.

12.2 지표별 목표

아래 목표는 제안하는 경영 약속이다. 서비스, 법률, 내부 정책이 요구하면 더 엄격한 목표를 정하라. 예외에는 보완 통제, 책임자, 검토일을 명시해야 한다.

지표	권장 목표	인정할 증거
관련 경보 경로	30 일째까지 마련	수신자와 최초 경보 검토
새 관련 신원 경보	모든 경보에 날짜가 있는 처리 결과	계정·세션 증거
외부 민감 애플리케이션	모든 애플리케이션에 책임자 지정	검토한 서비스·데이터 목록
특권·원격 이용자	60 일째까지 피싱 저항성 MFA 적용 또는 날짜가 있는 전환 계획	적용 범위와 복구 시험
주요 공급업체 경보 경로	60 일째까지 시험	메시지·증거 전달 시간 기록
핵심 서비스 복원	승인된 복구 목표 충족 또는 날짜가 있는 개선 계획	업무 승인과 무결성 점검
통지 훈련	90 일째까지 완료	인지·발동 조건·갱신 기록

백업 작업의 성공은 복원을 입증하지 않는다. 경보 배포는 적절한 팀이 경보를 받는다는 증거가 아니다. 정책 문서 완성은 시간에 쫓기는 상황에서도 사고 판단을 내릴 수 있다는 증거가 아니다.

12.3 역할별 과제

역할	최초 판단	요청할 증거
이사회	어떤 핵심 서비스·데이터 관계에 훈련이 필요한가?	업무 부서가 책임지는 복구·통지 결과
CISO	지금 확인할 수 있는 외부 신호는 무엇인가?	경보 처리 결과와 미해결 의존 관계
SOC	어떤 업무·신원 이벤트를 연결해야 하는가?	대화·프로세스·지속 실행·세션 증거
신원 담당팀	어떤 활성 계정·토큰이 중요한 권한을 갖는가?	소유·활동·폐기 기록
애플리케이션 책임자	이용자가 허용된 객체에만 접근할 수 있는가?	시험한 접근·내보내기 경계
사기 대응팀	정확한 개인정보로 위험한 변경을 승인할 수 있는가?	합성 복구·수취인 변경 결과
개인정보 보호·법무팀	어떤 사실이 각 의무를 시작시키는가?	적용 범위·인지 판단 기록
구매팀	주요 공급업체가 적시에 증거를 제공할 수 있는가?	시험한 연락처와 계약상 경보 경로
홍보팀	지금 밝힐 수 있는 사실은 무엇인가?	확인된 서비스·데이터 범위와 갱신 시각

12.4 Brandefense의 지원

Brandefense는 Cyber Threat Intelligence, Digital Risk Protection, External Attack Surface Management를 결합한다. 외부 인텔리전스는 검토가 필요한 관련 자격 증명 제안, 사칭 자료, 공개 노출 신호를 파악하는 데 도움을 줄 수 있다.

실무적 가치는 외부 신호를 책임 있는 내부 담당자와 연결할 때 생긴다. 과거 기록과 범죄자의 주장은 여전히 확인이 필요하다. 플랫폼 관찰은 조직의 사고·개인정보 보호·업무 연속성 판단을 대체하지 않는다.

데모 요청을 통해 조직과 관련된 도메인, 브랜드, 서비스, 경보 절차를 논의할 수 있다.

핵심 요점

01
먼저 책임을 정하고 현재 유효한 증거를 확인하라.

02
훈련으로 공급업체 대응, 피싱 저항성, 복원을 입증하라.

03
90 일째까지 종결 증거와 날짜가 있는 예외를 이사회에 보고하라.

부록

부록

A–D

이 장에서 답하는 질문

각 증거 집단에서 독자는 무엇을 결론 내릴 수 있는가?

5

단위와 한계가 서로 다른 집단

부록 A. 범위, 증거, 한계 96

부록 B. 증거 목록 99

부록 C. 출처 100

부록 D. 용어 설명 105

부록 A. 범위, 증거, 한계

비교 대상 국가는 맥락을 제공하기 위한 예시로만 선정되었으며, 순위나 정치적 평가를 의미하지 않습니다.

A.1 관찰 기간

게시물 날짜는 UTC 기준이며, 공개 출처 날짜는 발행자가 표시한 달력을 따른다.

요청된 관찰 기간은 게시 시각 기준 2026-01-01 부터 2026-11-22 까지다. 최근 활동 기간은 2026-11-08 부터 2026-11-22 까지다.

포함된 사건, 발표, 자체 데이터 스냅샷은 해당 날짜가 진행 중이던 2026-11-22 에 마감됐다. 기간 내 발표된 외부 출처는 2026-11-22 또는 2026-11-23 에 확인했다.

공개 자료는 각각의 사건일, 탐지일, 발표일을 유지한다. 최근 공개가 이전 침입을 설명할 수 있다. 정책·수사 동향은 별도 표시하며 새 공격 건수에 더하지 않는다.

A.2 증거 집단

집단	단위	적절한 결론	주요 한계
지하 시장 자료	보관 게시물·광고	무엇을 제안·요청·주장했는가	진위와 결과에는 추가 증거가 필요함
랜섬웨어 게시	공개된 범죄 주장	날짜가 있는 데이터에서 보이는 범위	확인된 침입이나 고유 조직 수가 아님
선정 도메인 관찰	도메인·설정 관찰	확인 또는 설정 과제	독립 법인이나 전국 발생 비율이 아님
공개 자료	출처가 명시한 사건·범위	해당 범위의 확인 사실 또는 출처의 설명	추정치와 조사 결과는 바뀔 수 있음
보안업체 캠페인 연구	연구자가 관찰한 활동	행위와 출처가 지목한 공격자 평가	국내 피해 범위와 공격자 식별이 미확인일 수 있음

이 집단들은 합산하지 않는다. 비슷한 문구나 같은 총계가 겹치는 자료임을 입증하지는 않는다. 대한민국을 언급한 게시물이 세계 가격표, 일상 대화, 다른 국가에 관한 보도일 수 있다.

A.3 노출·설정 관찰

선정한 도메인 250 개 포트폴리오는 통합한 열 개 부문에서 각각 후보 25 개를 포함한다. 목적에 따라 선정했으며 공식 국가 순위를 재현하지 않는다. 법인 독립성과 소유 관계가 확인되지 않은 경우에는 한계로 유지한다.

선정 도메인 250 개의 국가 Atlas 대표값은 100 점 중 54 다. 조직별·부문별 등급이나 등급 분포는 공개하지 않는다. 노출 기록은 2026-11-22 기준 누적 스냅샷이다. 유사 도메인 후보는 이전 30 일을 다룬다. [S3]

DNS, 메일 정책, 웹 관찰은 명시한 서비스와 날짜에 관한 것이다. 확인할 수 없는 관찰은 미상으로 유지한다. 인증서·정책 기록은 성공한 침입을 입증할 수 없다.

설정 요소를 관찰하지 못했다고 다른 곳에도 동등한 통제가 없다는 증거가 되는 것은 아니다.

A.4 범죄 주장과 연대기

사례 카드는 주장, 관찰된 연대기, 확인된 증거, 대안, 비례하는 대응을 제시한다. 실제 인용문에서는 피해자 식별 정보, 개인정보, 연락 수단으로 쓸 수 있는 내용을 삭제한다.

일부 보관 게시물은 날짜 관계가 일치하지 않으며, 과거 글을 인용하거나 이전 연도의 표본 날짜를 보여 주기도 한다. 이런 기록은 주장이 유통됐음을 보여 줄 수 있지만 새로운 침입 시점을 정하는 데 사용하지 않는다.

새 광고는 새 침입을 입증하지 않는다. 재게시, 회신, 최초 탈취는 서로 다른 사건이다. 출처, 최신성, 파일 동일성이 미확인이라면 보고서는 그 불확실성을 유지한다.

A.5 결제 카드 범위

결제 카드 수치는 보관 게시물 집단의 결제 카드 기록에 관한 것이다. Brandefense의 더 넓은 카드 관찰 범위를 대표하지 않으며, 전국 카드 노출, 카드 정보 탈취, 사기 손실을 측정하지 않는다.

A.6 랜섬웨어와 비교

산업·금융·디지털 서비스 맥락을 위해 대한민국을 일본, 대만, 홍콩, 싱가포르와 비교한다. 비교 대상의 규모와 가시성이 달라 위험 순위를 매길 수 없다.

2025 년 전체 수치는 2026 년 일부 관찰 기간의 맥락을 제공한다. 같은 기간 길이의 기준선이 아니다. 산업·국가 분류는 게시 집단을 설명하며 부정확할 수 있다.

A.7 출처 범위

공개 출처 증거에는 한국어·영어 공식 공지, 조직 공개 자료, 국내 보도, 보안업체 연구가 포함된다. 관련성이 있는 경우 러시아어·튀르키예어 보도도 검토했다.

인용한 각 외부 출처는 전체 URL을 제시하거나, 기사 경로가 비공개 피해자를 식별할 경우 발행자의 사이트 루트 주소를 제시한다. 각 항목에는 2026-11-22 또는 2026-11-23 확인일을 함께 기록한다.

관찰 기간 전체의 공식 출처 증거가 고르게 확보된 것은 아니다. 일부 원문 공지는 채택한 증거에 포함되지 않는다. 공식 발표를 전하는 언론 보도에 근거한 경우에는 그 관계를 분명히 밝히고 원문을 직접 확인한 것처럼 단정하지 않는다.

보고서는 대한민국에 영향을 준 사이버 사고를 빠짐없이 집계했다고 주장하지 않는다. 비공개 사건, 접근할 수 없는 원문 공지, 비공개 조사는 확보한 증거로 확인할 수 있는 범위 밖에 남는다.

게시물 단위의 관측에는 공백이 있다. 총계는 보관 증거를 설명하며 전체 관련 게시물의 규모는 확정되지 않았다.

A.8 명칭과 중립성

미확인 대상에는 여러 조직에 해당할 수 있는 넓은 역할명을 쓴다. 공식 확인과 폭넓은 보도가 뒷받침할 때만 조직을 영향받은 당사자로 명명한다. 비공개 당사자를 식별하는 출처 주소는 발행자의 루트 주소와 기사 주소 비공개 안내로 대신한다.

공격자의 수사를 작성자의 표현으로 채택하지 않는다. 국가 연계 평가는 인용 출처의 판단과 명시된 확신도로 유지한다. 정치적 분쟁, 정부, 선거, 대외 관계에 관한 입장을 암시하지 않는다.

A.9 확신도와 조치

보관한 광고의 존재에는 높은 확신을 가질 수 있어도 내용은 미확인일 수 있다. 확인된 공개 자료는 정보 접근을 입증하면서도 공격자나 모든 피해자를 확정하지 못할 수 있다.

증거가 조건부라면 권고도 조건부다. 주장이 확인되기 전에 검증 과제를 시작할 수 있다. 업무를 중단시키는 차단, 공개 발표, 통지 판단은 조직 자체의 증거와 적용 의무를 따라야 한다.

부록 B. 증거 목록

게시물 카드는 4 장에 나온다. 검증된 결과가 아니라 출처의 주장을 옮긴 것이다.

카드	날짜	장소	별칭	언어	위치
B01	2026-03-11	포럼	FantancyHacker	한국어	4 장
B02	2026-01-14	포럼	Solonik	영어	4 장
B03	2026-03-11	포럼	zSenior	영어	4 장
B04	2026-04-26	포럼	0xCAFE	영어	4 장
B05	2026-04-28	포럼	TunaFish	영어	4 장
B06	2026-08-23	포럼	HighWayToShell	영어	4 장
B07	2026-11-12	포럼	taltikgoo	영어	4 장
B08	2026-11-19	포럼	Noiem	영어	4 장
B09	2026-01-13	포럼	Solonik	영어	4 장
B10	2026-03-01	포럼	INDOHAXSEC	영어	4 장
B11	2026-03-10	포럼	ZeusHacking	한국어	4 장
B12	2026-03-30	포럼	GlitchX	영어	4 장
B13	2026-03-31	포럼	xorcat	영어	4 장
B14	2026-04-03	포럼	Grubder	영어	4 장
B15	2026-05-28	포럼	포럼 참여자	영어	4 장
B16	2026-07-06	포럼	AshleyWood2022	영어	4 장
B17	2026-08-23	포럼	updap	영어	4 장
B18	2026-09-09	포럼	□RED✘□	영어	4 장
B19	2026-10-07	포럼	updap	영어	4 장
B20	2026-10-17	포럼	updap	중국어·한국어 주석	4 장
B21	2026-11-08	포럼	DataJava	영어	4 장
B22	2026-11-10	포럼	DataJava	영어	4 장
B23	2026-11-17	포럼	thisversace	영어	4 장
B24	2026-11-21	포럼	tet	영어	4 장

부록 C. 출처

표시되지 않는 출처 번호는 검토 과정에서 제외되었으며 인용하지 않는다. 포함된 사건과 발표의 마감일은 2026-11-22 이다. 외부 출처의 근거 문장은 아래에 표시한 대로 2026-11-22 또는 2026-11-23 에 확인했다.

자체 출처 증거는 공개 다운로드로 제공하지 않는다. 일부 외부 출처는 미확인 피해자를 보호하기 위해 기사 주소를 비공개로 두고 발행자의 사이트 루트 주소로 인용한다.

S1: Odin by Brandefense. South Korea country-tagged post counts and retained research corpus, publication window 2026-01-01–2026-11-22. 확인일 2026-11-22.

S2: Brandefense Ransompedia. Listing snapshot for South Korea and four regional comparators, read 2026-11-22. 확인일 2026-11-22.

S3: Odin by Brandefense. Brandefense Atlas exposure ratings, device and credential associations, current listings and selected-domain configuration observations, dated 2026-11-22. 확인일 2026-11-22.

S4: Brandefense Blackhole. Payment-card aggregate evidence for the retained post corpus. 확인일 2026-11-22.

S5: FSC. Financial-sector incidents and response. 2026-11-05. https://www.fsc.go.kr/eng/pr010101/88092?curPage=1. 확인일 2026-11-23.

S6: FSI. Financial Security Institute assessment-system breach. 2026-11-10. https://www.fsec.or.kr/bbs/detail?bbsNo=12144&menuNo=69. 확인일 2026-11-22.

S7: Yonhap. FSI breach reported nationally. 2026-11-10. https://en.yna.co.kr/view/AEN20261110010651315. 확인일 2026-11-22.

S8: DataReportal. Digital 2027 South Korea; October and late-2026 estimates. 2026-11. https://datareportal.com/reports/digital-2027-south-korea. 확인일 2026-11-23.

S9: PIPC. Personal-data breach reporting guidance. current guidance. https://pipc.go.kr/np/default/page.do?mCode=D030040000. 확인일 2026-11-22.

S10: PIPC. Revised privacy law and decree effective September 11. 2026-09-10. https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=12459. 확인일 2026-11-22.

S11: KISA / KrCERT/CC. Java security update advisory and FAQ. 2026-11-18;updated2026-11-20. https://www.boho.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72313&pageIndex=1. 확인일 2026-11-22.

S12: NIST NVD. CVE-2026-114938 record. 2026-11-17. https://nvd.nist.gov/vuln/detail/CVE-2026-114938. 확인일 2026-11-23.

S13: Oracle. November2026 Critical Security Patch Update;Java risk matrix. 2026-11-17. https://www.oracle.com/security-alerts/cspunov2026.html. 확인일 2026-11-22.

S14: AhnLab ASEC. October2026 domestic APT activity review. 2026-11-20. https://asec.ahnlab.com/ko/96683/. 확인일 2026-11-22.

S15: Genians Security Center. NodeLinkRAT campaign research. 2026-11-16. https://www.genians.co.kr/en/blog/threat_intelligence/nodelinkrat. 확인일 2026-11-23.

S16: AhnLab ASEC. Purchase-order document phishing associated with XLoader. 2026-11-13. https://asec.ahnlab.com/ko/96512/. 확인일 2026-11-22.

S17: AhnLab ASEC. Quotation archive phishing associated with SnakeKeylogger. 2026-11-12. https://asec.ahnlab.com/ko/96494/. 확인일 2026-11-22.

S18: KISA. Forum-linked attacks on domestic websites. 2026-01-06. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=71932. 확인일 2026-11-22.

S19: KISA. Government and think-tank impersonation QR phishing. 2026-01-10. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=71936. 확인일 2026-11-22.

S20: KISA. Ransomware prevention warning. 2026-02-04. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=71960. 확인일 2026-11-22.

S21: KISA. Utilities impersonation targeting IT staff. 2026-03-11. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=71998. 확인일 2026-11-22.

S22: KISA. Hacktivism and geopolitical threat warning. 2026-03-20. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72005. 확인일 2026-11-22.

S23: KISA. Developer supply-chain diffusion warning. 2026-04-01. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72014. 확인일 2026-11-22.

S24: KISA. KakaoTalk installer impersonation. 2026-04-15. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72027. 확인일 2026-11-22.

S25: KISA. Midnight/Endpoint ransomware against SMEs. 2026-04-16. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72028. 확인일 2026-11-22.

S26: KISA. Travel-reservation data reused for phishing. 2026-05-12. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72049. 확인일 2026-11-22.

S27: KISA. Second developer supply-chain warning. 2026-05-20. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72059. 확인일 2026-11-22.

S28: KISA. OTT-breach follow-on fraud warning. 2026-06-03. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72078. 확인일 2026-11-23.

S29: KISA. Firewall/VPN credential-abuse warning. 2026-06-21. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72105. 확인일 2026-11-22.

S30: KISA. AI-development-tool impersonation. 2026-07-16. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72133. 확인일 2026-11-22.

S31: KISA. Developer credential exposure warning. 2026-07-16. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72132. 확인일 2026-11-22.

S32: KISA/NIS/KNPA/FSI joint. State-backed attacks on Korean nationals and businesses. 2026-07-30. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72144. 확인일 2026-11-22.

S33: KISA. Financial and private-sector incident response warning. 2026-10-03. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72207. 확인일 2026-11-22.

S34: KISA. NAS ransomware warning. 2026-11-03. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72267. 확인일 2026-11-22.

S35: PIPC. OTT-service breach investigation. 2026-06-04. https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=12147. 확인일 2026-11-22.

S36: PIPC. Cloud/developer secret-management warning. 2026-06-15. https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C010010000&nttId=12179. 확인일 2026-11-22.

S37: PIPC. Three companies sanctioned for 2024 breaches. 2026-07-08. https://pipc.go.kr/ (article URL withheld). 확인일 2026-11-22.

S38: PIPC. Industrial-group enforcement concerning a 2022 incident. 2026-11-12. https://pipc.go.kr/ (article URL withheld). 확인일 2026-11-22.

S39: PIPC. Java-related mass-leak prevention warning. 2026-11-18. https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=12660. 확인일 2026-11-22.

S40: Yonhap. University teaching-system breach. 2026-11-14. https://www.yna.co.kr/ (article URL withheld). 확인일 2026-11-22.

S41: Yonhap. Regional-voucher platform API authorization incident. 2026-11-16. https://www.yna.co.kr/ (article URL withheld). 확인일 2026-11-22.

S42: Yonhap. Education-office accidental legal-document disclosure. 2026-11-21. https://www.yna.co.kr/ (article URL withheld). 확인일 2026-11-22.

S43: MBC quoting Seoul police. Multi-company extortion arrests. 2026-10-26. https://imnews.imbc.com/ (article URL withheld). 확인일 2026-11-22.

S44: University official. Research-equipment and IT-service portal compromise. 2026-11-19. https://postech.ac.kr/eng/news-center/university_announcement.do?article.offset=0&articleLimit=10&articleNo=56081&mode=view. 확인일 2026-11-23.

S45: Asia Economy. Employee-training platform unauthorized cloud access. 2026-11-12. https://view.asiae.co.kr/ (article URL withheld). 확인일 2026-11-23.

S47: BleepingComputer. Education-group ransomware update. 2026-01-14. https://www.bleepingcomputer.com/news/security/south-korean-giant-kyowon-confirms-data-theft-in-ransomware-attack/amp/. 확인일 2026-11-22.

S48: University official. Second university-portal breach notice. 2026-11-20. https://postech.ac.kr/ (article URL withheld). 확인일 2026-11-22.

S49: Company official. Education-group cyber incident disclosure. 2026-01-12. https://www.kyowon.co.kr/Media/News_detail?iscont=&nttid=1255&page=1&searchcolumn=&searchpreface=+&searchpreface2=&searchpreface3=&searchword=. 확인일 2026-11-22.

S50: Yonhap. Education-group incident nationally reported. 2026-01-12. https://www.yna.co.kr/view/AKR20260112036251030. 확인일 2026-11-22.

S51: Yonhap. OTT provider acknowledges unauthorized-access leak. 2026-06-03. https://www.yna.co.kr/amp/view/AKR20260603014100017. 확인일 2026-11-22.

S52: SBS via Daum. Public-sector training-system access disclosure. 2026-07-20. https://v.daum.net/v/20260720140004721. 확인일 2026-11-22.

S53: TRT Haber / Anadolu. Turkish coverage of public-sector training incident. 2026-07-22. https://www.trthaber.com/haber/dunya/guney-korede-10-bin-disisleri-personelinin-verilerinin-sizdirildigi-iddia-edildi-951857.html. 확인일 2026-11-22.

S55: KISA. Agency and financial-company impersonation mail. 2026-09-29. https://www.boho.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72202. 확인일 2026-11-22.

S56: University official notice. Additional personal-data breach notice. 2026-11-22. https://www.jj.ac.kr/ (article URL withheld). 확인일 2026-11-22.

S57: University official notice. First personal-data breach notice. 2026-11-18. https://www.jj.ac.kr/jj/community/notice01.do?articleNo=535802&mode=view. 확인일 2026-11-22.

S58: Etoday. Utility customer and procurement data disclosure. 2026-11-22. https://www.etoday.co.kr/ (article URL withheld). 확인일 2026-11-22.

S60: National Information Resources Service. Administrative email abnormal-access explanation. 2026-11-17. https://www.nirs.go.kr/ncia_MJS/board/dev/board/board.jsp?id=data_201&idx=4779&mode=view. 확인일 2026-11-23.

S61: Yonhap. Unauthorized access to approximately 300 public-service email accounts. 2026-11-16. https://www.yna.co.kr/ (article URL withheld). 확인일 2026-11-22.

S62: Ministry of Foreign Affairs. Ministry briefing on a public-sector training incident. 2026-07-21. https://www.mofa.go.kr/www/brd/m_4078/view.do?page=1&seq=368855. 확인일 2026-11-22.

S63: Ministry of Foreign Affairs. Ministry briefing on a public-sector training incident. 2026-07-23. https://www.mofa.go.kr/ (article URL withheld). 확인일 2026-11-22.

S67: Ministry of SMEs and Startups. Private AI supplier personal-data breach explanation. 2026-11-20. https://www.mss.go.kr/ (article URL withheld). 확인일 2026-11-23.

S68: Yonhap. Startup-program participants in AI supplier breach. 2026-11-13. https://www.yna.co.kr/ (article URL withheld). 확인일 2026-11-22.

S69: Yonhap. Financial-institution outsourced-training disclosure. 2026-09-28. https://www.yna.co.kr/ (article URL withheld). 확인일 2026-11-22.

S70: Yonhap Infomax. Insurer customer data exposed at a claims processor. 2026-11-22. https://news.einfomax.co.kr/ (article URL withheld). 확인일 2026-11-23.

S71: Yonhap. Regional universities report distinct system exposures. 2026-11-18. https://www.yna.co.kr/ (article URL withheld). 확인일 2026-11-22.

S73: JoongAng Ilbo. University discloses approximately 180,000 records. 2026-11-20 (search metadata; body lacks timestamp). https://www.joongang.co.kr/article/25480425. 확인일 2026-11-22.

S74: Financial News / Newsis. University online liberal-arts service breach. 2026-11-19. https://www.fnnews.com/ (article URL withheld). 확인일 2026-11-22.

S75: Segye Ilbo. University and school-transport disclosures. 2026-11-19. https://m.segye.com/ (article URL withheld). 확인일 2026-11-22.

S76: Dailysecu. Research-university portal breach: initial notice corroboration. 2026-11-20. https://www.dailysecu.com/news/articleView.html?idxno=209629. 확인일 2026-11-23.

S78: Yonhap. Utility customer and procurement disclosure scope. 2026-11-22. https://www.yna.co.kr/ (article URL withheld). 확인일 2026-11-22.

S79: Newsis. Utility confirms customer and procurement data breach. 2026-11-22. https://www.newsis.com/ (article URL withheld). 확인일 2026-11-22.

S80: CJ Logistics. Possible personal-data exposure notice. 2026-11-18. https://www.cjlogistics.com/ko/newsroom/notice/NR_00001412. 확인일 2026-11-22.

S81: Edaily. Logistics chatbot abnormal-access investigation. 2026-11-18. https://www.edaily.co.kr/News/Read?mediaCodeNo=257&newsId=04336166645647032. 확인일 2026-11-22.

S90: MITRE ATT&CK. Technique definitions for the analyst behavioural crosswalk. current reference. https://attack.mitre.org/techniques/T1204/002/ https://attack.mitre.org/techniques/T1059/001/ https://attack.mitre.org/techniques/T1053/005/ https://attack.mitre.org/techniques/T1567/002/. 확인일 2026-11-22.

S91: NIST. Digital identity guidance: phishing resistance. Current reference. https://pages.nist.gov/800-63-4/sp800-63b/authenticators/. 확인일 2026-11-22.

S92: OWASP. Object-level authorisation definition. Current reference. https://api-security.owasp.org/editions/2023/en/0xa1-broken-object-level-authorization/. 확인일 2026-11-22.

S93: KISA. ISMS-P certification overview. Current reference. https://www.kisa.or.kr/1050602. 확인일 2026-11-22.

S94: IETF. RFC 9989 DMARC. Current reference. https://www.rfc-editor.org/rfc/rfc9989.html. 확인일 2026-11-22.

S95: IETF. RFC 6376 DKIM. Current reference. https://www.rfc-editor.org/rfc/rfc6376.html. 확인일 2026-11-22.

S96: IETF. RFC 7208 SPF. Current reference. https://www.rfc-editor.org/rfc/rfc7208.html. 확인일 2026-11-22.

S97: Microsoft. Shell Links overview. Current reference. https://learn.microsoft.com/en-us/windows/win32/shell/links. 확인일 2026-11-22.

S98: Daglo. Service security-anomaly notice. 2026-03-27. https://daglo.ai/page/330ca999-eeb2-8056-ae72-c18f3c954ee4. 확인일 2026-11-22.

S99: Yonhap. Company investigation updates a March service incident. 2026-04-09. https://www.yna.co.kr/view/AKR20260409116200017. 확인일 2026-11-22.

S100: Newsis. Service-provider follow-up and information-scope statement. 2026-04-15. https://mobile.newsis.com/view/NISX20260414_0003591185. 확인일 2026-11-22.

S101: National Tax Service. Official apology concerning sensitive information in press photographs. 2026-03-01. https://s.nts.go.kr/nts/na/ntt/selectNttInfo.do?mi=2201&nttSn=1349387. 확인일 2026-11-22.

S102: Yonhap. Press-photo disclosure and uncertain asset valuation. 2026-02-27. https://www.yna.co.kr/amp/view/AKR20260227180500002. 확인일 2026-11-22.

S103: Newsis. Photo-disclosure explanation and valuation limits. 2026-02-28; updated2026-03-01. https://nwww.newsis.com/view/NISX20260228_0003530566. 확인일 2026-11-22.

S104: Yonhap. Hospital image-workflow interruption and restoration. 2026-01-27. https://www.yna.co.kr/ (article URL withheld). 확인일 2026-11-22.

S105: Yonhap. Investigation of an unverified asset-return account. 2026-03-01. https://www.yna.co.kr/ (article URL withheld). 확인일 2026-11-22.

S106: MBC. Contractor customer-support information disclosure. 2026-11-15. https://imnews.imbc.com/ (article URL withheld). 확인일 2026-11-22.

S107: Newsis. Support-service notice and consultation-dependent scope. 2026-11-15. https://nwww.newsis.com/ (article URL withheld). 확인일 2026-11-22.

S108: Yonhap. Provider account of support-system access and varying client scope. 2026-11-14. https://www.yna.co.kr/ (article URL withheld). 확인일 2026-11-22.

S109: Korean National Police, official Korea.kr republication. Police-authored fraud-prevention warning. 2026-03-27. https://www.korea.kr/multi/visualNewsView.do?newsId=148961591. 확인일 2026-11-22.

S110: Newsis. Police warning distinguishes attempts from realised harm. 2026-03-23. https://www.newsis.com/ (article URL withheld). 확인일 2026-11-23.

S111: CBS NoCut News. Approval and expense-document disclosure across two windows. 2026-11-03 05:00. https://www.nocutnews.co.kr/ (article URL withheld). 확인일 2026-11-22.

S112: Yonhap. Business-document access and reported company response. 2026-11-02 16:07. https://www.yna.co.kr/ (article URL withheld). 확인일 2026-11-22.

S113: Financial Services Commission. Regulator confirms financial-company incidents and unresolved relationships. 2026-10-14. https://www.fsc.go.kr/ (article URL withheld). 확인일 2026-11-23.

S114: NewsPim. Financial intermediary disclosure and remaining scope questions. 2026-10-29 10:35. https://www.newspim.com/ (article URL withheld). 확인일 2026-11-23.

S115: Edaily. Later financial-disclosure scope reporting. 2026-11-18 16:22:38. https://www.edaily.co.kr/ (article URL withheld). 확인일 2026-11-23.

S116: Dailysecu. Manufacturing-related extortion claim and preliminary vendor response. Published2026-11-15 16:02:03+09:00; modified2026-11-16 20:06:57+09:00. https://www.dailysecu.com/ (article URL withheld). 확인일 2026-11-22.

S117: Yonsei University Information and Communications Office. University portal information-exposure notice. 2026-10-22. https://www.yonsei.ac.kr/bbs/sc/58/944433/artclView.do. 확인일 2026-11-22.

S118: Dailysecu. Portal-disclosure scope and response reporting. 2026-11-17. https://www.dailysecu.com/news/articleView.html?idxno=209012. 확인일 2026-11-23.

S119: NewsPim. Portal-disclosure inquiry and separate exposure windows. Published2026-10-22 17:56; modified2026-11-02 14:11. https://www.newspim.com/news/view/20261022001356. 확인일 2026-11-22.

S120: IETF. RFC 6797: HTTP Strict Transport Security (HSTS). 2012-11. https://www.rfc-editor.org/rfc/rfc6797.html. 확인일 2026-11-23.

S121: W3C. Content Security Policy Level 3. 2026-10-27 (Working Draft). https://www.w3.org/TR/2026/WD-CSP3-20261027/. 확인일 2026-11-23.

S122: IETF. RFC 8659: DNS Certification Authority Authorization (CAA) Resource Record. 2019-11. https://www.rfc-editor.org/rfc/rfc8659.html. 확인일 2026-11-23.

S123: IBM. What is Customer Relationship Management (CRM)? https://www.ibm.com/think/topics/crm. 확인일 2026-11-23.

S124: IBM. What is network attached storage? https://www.ibm.com/think/topics/network-attached-storage. 확인일 2026-11-23.

S125: PIPC. The PIPC to Investigate Data Breaches or Infringements in a Faster, Fairer, and More Transparent Manner. 2026-10-02. https://pipc.go.kr/eng/user/ltn/new/noticeDetail.do?nttId=3197. 확인일 2026-11-23.

S126: PIPC. The PIPC Sanctions Coupang and CFS for Data Breaches and Infringements on Privacy. 2026-06-17. https://pipc.go.kr/eng/user/ltn/new/noticeDetail.do?nttId=3071. 확인일 2026-11-23.

S127: PIPC. The PIPC Sanctions KT Corporation for Data Breaches. 2026-08-07 (decision 2026-06-29). https://pipc.go.kr/eng/user/ltn/new/noticeDetail.do?nttId=3133. 확인일 2026-11-23.

S128: National Intelligence Service. 2026 National Cybersecurity White Paper publication listing. 2026-06-08. https://nis.go.kr/AF/1_7_7_1.do. 확인일 2026-11-23.

부록 D. 용어 설명

용어	쉬운 뜻
계정 복구	이용자가 로그인할 수 없을 때 접근을 복원하는 절차
API	애플리케이션이 정보나 동작을 요청하는 소프트웨어 인터페이스
Atlas 대표값	국가 포트폴리오의 노출 수치이며 공격 확률이 아님
인증	이용자·서비스가 제시한 신원을 확인하는 것
접근 권한 부여	해당 신원이 접근할 수 있는 정보·동작을 판단하는 것
Blackhole	보관 게시물 자료에 사용한 Brandefense의 인텔리전스 출처
CAA	Certification Authority Authorization. 도메인의 인증서를 발급할 수 있는 인증기관을 지정하는 DNS 레코드 [S122]
CRM	Customer relationship management. 현재·잠재 고객과의 상호작용을 관리하는 고객 관계 관리 소프트웨어 [S123]
CSP	Content Security Policy. 페이지가 가져오거나 실행할 수 있는 리소스를 통제하는 브라우저 정책 [S121]
클라우드 관리자	클라우드 환경의 관리 권한을 가진 신원
콤보리스트	서로 다른 출처의 로그인 식별자·비밀번호를 모은 자료
개인정보처리자	개인정보 처리 목적과 수단을 결정할 책임이 있는 당사자
자격 증명	계정을 인증하는 데 쓰이는 정보나 토큰
기기 연관 기록	기기의 기록을 서비스·도메인과 연결하는 외부 관찰
DKIM	도메인이 공개한 검증 키를 사용하는 메일 서명 방식 [S95]
DMARC	지정된 인증 확인에 실패한 메일을 처리하는 도메인 정책 [S94]
DNSSEC	DNS 데이터의 진위를 확인하는 서명·검증 연결 정보
DS 레코드	도메인의 DNSSEC 키를 상위 영역과 연결하는 상위 영역 레코드
ERP	업무 절차를 관리하는 전사적 자원 관리 소프트웨어
데이터 반출	통제된 환경 밖으로 정보를 무단 전송하는 것
HSTS	HTTP Strict Transport Security. 브라우저가 보안 연결을 사용하도록 지시하는 웹사이트 정책 [S120]
HWP	한글 워드프로세서 문서 형식. 문서처럼 보이는 이름은 안전한 파일의 증거가 아님
정보 탈취 악성코드	저장된 계정 데이터 등의 정보를 수집하도록 만든 악성코드

용어	쉬운 뜻
ISMS-P	정보보호·개인정보 보호를 포괄하는 한국의 인증 체계 [S93]
LNK	프로그램이나 다른 동작을 시작할 수 있는 Windows 바로가기 파일 [S97]
MFA	여러 유형의 로그인 증거를 요구하는 다중 요소 인증
NAS	Network-attached storage. 네트워크를 통해 파일 저장 공간을 공유하는 네트워크 연결 저장장치 [S124]
객체별 권한 확인	특정 신원이 요청한 특정 기록·객체에 접근할 수 있는지 확인하는 것 [S92]
피싱 저항성 MFA	정상 서비스에 결합돼 자격 증명 중계 위험을 줄이는 인증 [S91]
수탁자	개인정보처리자를 대신해 개인정보를 다루는 당사자
Ransompedia	Brandefense의 랜섬웨어 게시 출처. 게시 항목은 범죄자의 주장을 기록함
복구 목표	복원을 평가하는 업무 승인 서비스·시간 목표
세션	최초 로그인 뒤에도 사용 가능할 수 있는 인증된 상호작용
SPF	메일 발송을 허용한 시스템에 관한 도메인의 선언 [S96]
SSO	하나의 인증 서비스가 여러 애플리케이션 접근을 허용하는 통합 로그인
스틸러 로그	피해 기기에서 악성코드가 기록한 정보
공급업체 고객 환경	공통 서비스 안에서 고객별로 구분된 환경
TLS	네트워크 연결을 보호하는 암호화·인증
토큰	신원·세션·위임 권한을 나타내는 자격 증명
TLP:CLEAR	다른 적용 의무를 전제로 공개 배포를 허용하는 공유 등급

용어 설명은 보고서에서 쓰는 말을 풀이한다. 공격자를 지목하거나 조직이 특정 결과를 겪었다고 입증하지 않는다.

보고서 소개

Odin by Brandefense가 Brandefense Country Report · South Korea 2026 으로 작성했다(최초 발행 2026-11-22, 개정 2026-11-23). 보고서는 보관한 자체 출처 증거와 출처를 확인한 공개 자료를 우선하며 각 집단의 한계를 유지한다.

기준판은 영어 원문이다. 한국어판은 AI의 도움으로 번역했으며 눈에 보이는 안내를 포함한다. 두 판은 같은 수치, 증거 ID, 출처 참조, 방어 판단을 유지한다.

권고는 조건부 방어 조치를 설명한다. 어떤 조직이 통제를 구현했거나 구현하지 않았다고 단정하지 않는다. 이 패키지는 대한민국에 영향을 준 사이버 범죄를 빠짐없이 집계했다고 주장하지 않는다.

© 2026 Brandefense. 모든 권리 보유.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO