AegisAX 사이버보안 뉴스레터 · 주간 종합 분석 리포트

# 2026년 7월 2주차
# 사이버보안 종합 분석 리포트

2026. 07. 12. ~ 2026. 07. 18.

# 문서 정보

| | |
|---|---|
| **문서 종류** | 주간 종합 분석 리포트 |
| **발행** | AegisAX 사이버보안 뉴스레터 |
| **대상 기간** | 2026년 7월 2주차 (2026. 07. 12. ~ 2026. 07. 18.) |
| **분석 기사** | 128건 / 그 주 전체 161건 |
| **분석 근거** | 웹 검색 + 수집 뉴스 |
| **출처** | 3건 |

# 목차

## 핵심 요약

2026년 7월 2주차 사이버보안 동향은 제로데이 및 실제 악용되는 취약점의 급증과 랜섬웨어 공격의 빠른 고도화가 핵심 흐름을 이루었다. 마이크로소프트 셰어포인트(CVE-2026-58644), 포티넷 포티샌드박스(CVE-2026-39808, CVE-2026-25089), 오라클 E-비즈니스 스위트(CVE-2026-46817) 등 다수의 취약점이 CISA KEV 카탈로그에 추가되었으며, 마이크로소프트 7월 패치 화요일에서 622개 취약점이 패치되는 등 AI 활용으로 취약점 연구와 패치 수가 급증했다. 더불어 랜섬웨어 분야에서는 '젠틀맨' 그룹이 최근 3개월간 300건의 공격을 감행하고 '스파이럴스' 랜섬웨어가 24시간 이내에 침투, 데이터 탈취, 암호화를 완료하는 등 이전 대비 빠른 공격 속도를 보였다. 이러한 위협은 코카콜라 자회사 페어라이프의 미국 내 유제품 생산 중단 사례처럼 운영 기술 환경까지 파급되었다. 한편 국내 규제에서는 9월 11일부터 중대한 개인정보 보호법 위반 기업에 전체 매출액의 최대 10%까지 징벌적 과징금을 부과하는 제도가 시행될 예정이다.

최근 가장 심각한 취약점으로는 마이크로소프트 셰어포인트 서버의 원격 코드 실행 취약점인 CVE-2026-58644가 꼽히며, 이는 CVSS 9.8점의 심각 등급으로 인터넷에 노출된 셰어포인트 서버를 사용하는 전 세계 수많은 기업이 영향을 받는다. 또한 포티넷 포티샌드박스의 CVE-2026-39808 및 CVE-2026-25089, 오라클 E-비즈니스 스위트의 CVE-2026-46817도 실제 공격에 악용되어 CISA의 KEV 카탈로그에 추가되었다. 마이크로소프트의 7월 패치 화요일에서는 622개의 취약점이 해결되었으며, F5의 NGINX 및 BIG-IP 제품군에서도 CVE-2026-42533을 포함한 결함이 확인되어 웹 인프라를 운영하는 조직의 빠른 패치가 요구된다. 보안 사고 측면에서는 코카콜라 자회사인 페어라이프가 랜섬웨어 공격을 받아 미국 내 유제품 생산이 일시 중단되는 피해를 입었다. 아울러 침투부터 데이터 탈취 및 암호화까지 24시간 이내에 완료하는 스파이럴스 랜섬웨어와 최근 3개월간 300건의 공격을 감행한 젠틀맨 랜섬웨어 그룹의 급부상으로 기업 및 산업 제어 시스템 환경의 비즈니스 연속성이 크게 위협받고 있다.

조직은 CISA의 KEV 카탈로그에 추가된 마이크로소프트 셰어포인트(CVE-2026-58644), 포티넷 포티샌드박스(CVE-2026-39808, CVE-2026-25089), 오라클 E-비즈니스 스위트(CVE-2026-46817)의 보안 패치를 즉시 적용해야 한다. 더불어 F5 NGINX 및 BIG-IP(CVE-2026-42533 포함), 지멘스 SICAM 8 등의 업데이트와 관리자 계정 다단계 인증(MFA)을 적용하고, 9월 11일 시행되는 매출액 최대 10% 징벌적 과징금제에 대비해 개인정보 보호 준수 상태를 점검해야 한다. 다음 주에는 AI 활용으로 가속화되는 제로데이 취약점의 발굴 및 공격 증가 추세를 집중 주시해야 한다. 또한 24시간 내 공격을 완료하는 스파이럴스나 젠틀맨 그룹 사례처럼 정교해진 랜섬웨어가 페어라이프 생산 중단과 같은 산업 제어 시스템(OT/ICS) 피해로 이어지지 않도록 백업 불변성 확보 및 신속한 침해 탐지·대응 체계 유지에 만전을 기해야 한다.

# 1 2026년 7월 2주차 핵심 지표

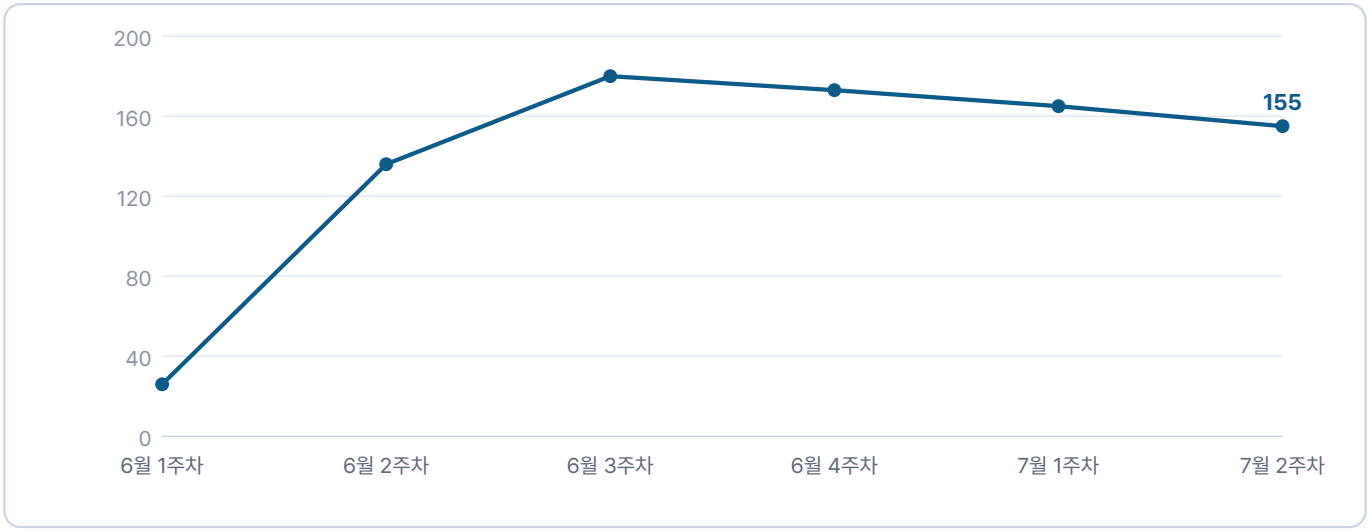


그림 1. 주차별 기사 수 추이

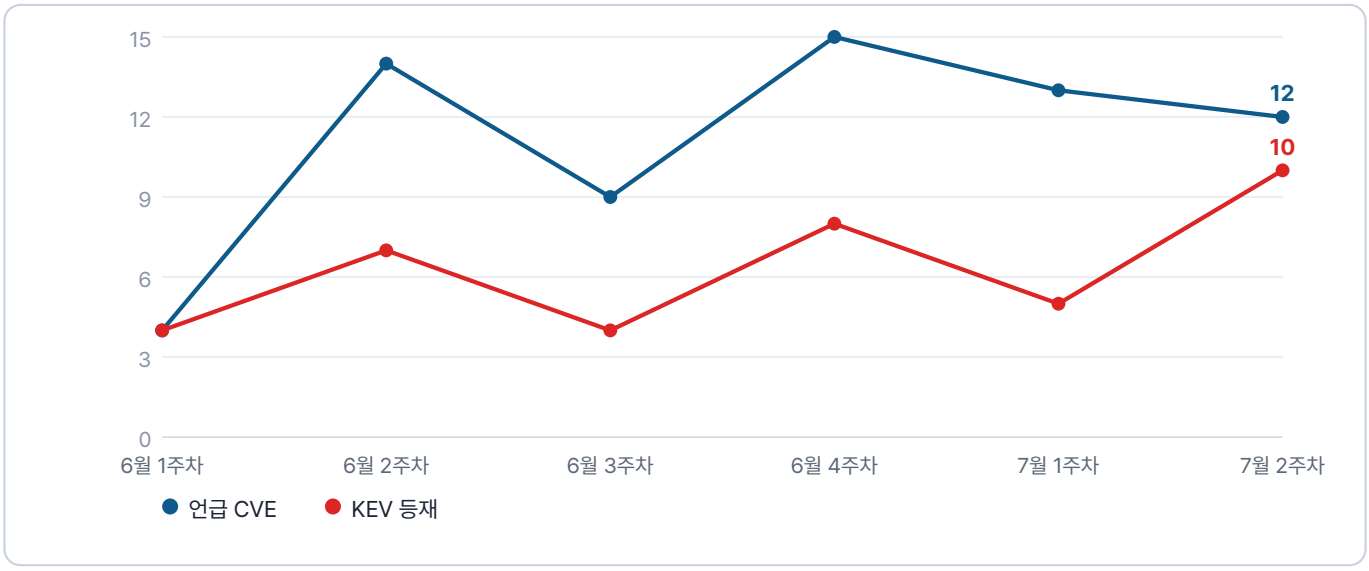


그림 2. 주차별 CVE 언급·악용(KEV) 추이

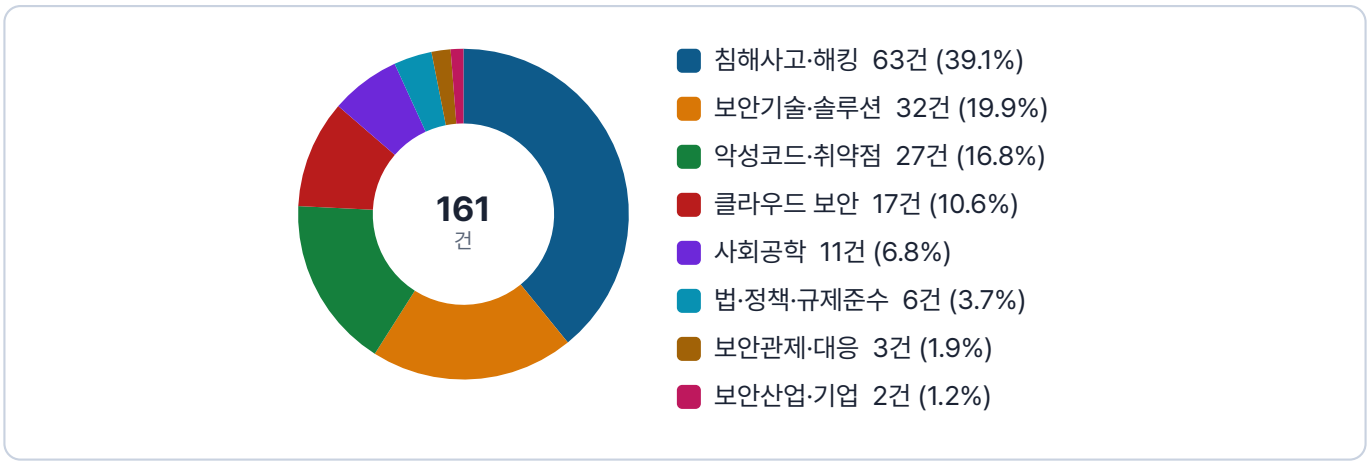


그림 3. 카테고리별 보도 분포

표 1. 조사 개요

| 항목 | 내용 | 관련 정보 |
|---|---|---|
| 분석 기간 | 2026. 07. 12. ~ 2026. 07. 18. | 7일(일~토) |
| 수집 기사 | 161건 | 전주 대비 -2.4% (165건 → 161건) |
| 분석 근거 기사 | 128건 | 수집분의 79.5% · 교차 확인 161건 · 본문 인용 출처 3건 |
| 보도 매체 | 22곳 | 데이터넷, 데일리시큐, 보안뉴스, 전자신문, BleepingComputer, CISA Advisories, Cisco Talos, CSO Online, Cyber Security News, Dark Reading, Hackread, Help Net Security 외 10곳 |
| 언급된 CVE | 14건 | NVD 확정 16건 · CISA KEV 등재 11건 · 치명적 8 · 높음 3 · 보통 3 |
| 분석 모델 | Gemini · 웹 검색 그라운딩 | 웹 근거 3건(검색·벤더 권고) |

표 2. 2026년 7월 2주차 핵심 지표

| 지표 | 값 |
|---|---|
| 주요 취약점 건수 (KEV 등재) | 4건 |
| 2026년 7월 2주차 최고 CVSS | 9.8 (CVE-2026-58644, CVE-2026-39808, CVE-2026-25089, CVE-2026-46817) |
| 주요 사고 수 | 3건 (페어라이프 랜섬웨어, 뉴지스탁 개인정보 유출, 23andMe 데이터 유출 합의) |
| 긴급 패치 발령 여부 | 발령 (CISA, 마이크로소프트, 포티넷, 오라클) |
| 주요 영향 벤더 | 마이크로소프트, 포티넷, 오라클, F5, 지멘스, 스플렁크, Zoom |

## 1.1 2026년 7월 2주차를 관통하는 주제

2026년 7월 2주차는 제로데이 및 활발히 악용되는 취약점의 급증이 가장 두드러진 주제이다. 마이크로소프트 셰어포인트(CVE-2026-58644), 포티넷 포티샌드박스(CVE-2026-39808, CVE-2026-25089), 오라클 E-비즈니스 스위트(CVE-2026-46817)에서 발견된 취약점들은 모두 CISA의 KEV(Known Exploited Vulnerabilities) 카탈로그에 추가되었으며, 이는 해당 취약점들이 실제 공격에 악용되고 있음을 의미한다. 이러한 제로데이 공격의 증가는 공격자들이 벤더의 패치 주기와 무관하게 취약점을 찾아내고 신속하게 악용하는 능력이 향상되었음을 보여준다. Cisco Talos는 7월 패치 화요일에 622개의 취약점이 패치되었으며, 이 중 3개의 제로데이 중 2개가 현재 공격에 악용되고 있다고 언급하며, 이러한 패치 홍수가 AI를 활용한 취약점 연구 가속화 때문일 수 있다고 분석했다. 이는 공격자들이 AI를 활용하여 취약점 탐지 및 익스플로잇 개발 속도를 높이고 있음을 시사하며, 방어자 역시 AI 기반 위협 인텔리전스 및 자동화된 대응 시스템 도입을 고려해야 할 시점

임을 나타낸다.

두 번째 주제는 랜섬웨어 공격의 속도와 규모의 진화이다. '젠틀맨(The Gentlemen)' 랜섬웨어 그룹은 최근 3개월간 300건의 공격을 감행하며 가장 활동적인 위협으로 부상했는데, 이는 공격적인 제휴사 모집과 사용하기 쉬운 침입 키트 제공에 기인하며 AI 도구를 활용해 개발 속도를 높이는 것으로 추정된다. 또한, '스파이럴스(Spirals)'라는 새로운 랜섬웨어는 침투, 데이터 탈취, 암호화를 24시간 이내에 완료하는 빠른 공격 속도를 보여주었다. 이러한 랜섬웨어의 진화는 공격자들이 기업 네트워크에 침투한 후 최대한 빠르게 피해를 극대화하려는 전략을 구사하고 있음을 의미한다. 이는 방어자들이 침해 탐지 및 대응 시간을 획기적으로 단축하고, 백업 및 복구 전략을 더욱 견고히 해야 함을 강조한다. 코카콜라 자회사 페어라이프의 랜섬웨어 공격으로 미국 내 유제품 생산이 일시 중단된 사례는 이러한 랜섬웨어 공격이 실제 산업 운영에 미치는 심각한 영향을 보여준다.

세 번째 주제는 사회 공학 기법과 새로운 공격 벡터의 결합이다. macOS를 표적으로 하는 '클릭락 스틸러(ClickLock Stealer)' 악성코드는 사용자가 시스템 로그인 암호를 입력하도록 강제하기 위해 프로세스를 종료하고 암호 대화상자만 표시하는 사회 공학 기법을 사용한다. 또한, 일반 글꼴 파일(TTF)로 위장한 악성코드를 유포하는 글로벌 피싱 캠페인이 진행 중이며, 이는 고도로 난독화된 자바스크립트와 루아(Lua) 기반 로더를 사용하여 보안 탐지를 회피한다. AI 음성 피싱의 성공 여부가 목소리의 자연스러움이 아닌 스크립트의 설득력에 달려있다는 연구 결과와 금융 부문을 노리는 피싱 공격이 일상적인 업무 이메일을 모방하여 성공률을 높인다는 분석은 공격자들이 기술적 취약점뿐만 아니라 인간의 심리를 이용한 사회 공학 기법을 지속적으로 고도화하고 있음을 보여준다. 이는 사용자 교육의 중요성과 함께, AI 기반의 정교한 피싱 공격에 대응하기 위한 다계층 보안 솔루션의 필요성을 강조한다.

# 2 주요 보안 취약점

## 2.1 마이크로소프트 셰어포인트 원격 코드 실행 취약점 (CVE-2026-58644)

표 3. 취약점 상세 명세 (CVE · CVSS · CWE · 영향 범위 · 악용 현황)

| 항목 | 내용 |
|---|---|
| 취약점 식별·심각도 (CVE·CVSS·CWE) | — |
| 영향 제품·버전 | Microsoft SharePoint |
| 공개일 | 2026-07-14 |
| 악용 현황 | CISA KEV 등재(실제 악용 확인) · 조치 기한 2026-07-19 |
| PoC·익스플로잇 | — |
| 패치·완화 | — |
| 대응 우선순위 | 최우선. CISA KEV 카탈로그에 등재되어 실제 악용이 확인되었으며, 연방 기관에 3일 이내 패치를 촉구했다. |

- 근본 원인: 신뢰할 수 없는 데이터 역직렬화(Deserialization of Untrusted Data) 취약점으로 추정된다. 인증된 공격자가 조작된 데이터를 전송하여 서버에서 임의 코드를 실행할 수 있도록 허용한다.
- 익스플로잇 벡터: 네트워크를 통한 원격 코드 실행. 공격자는 사이트 소유자 권한으로 인증되어야 한다.
- IoC: 비정상적인 셰어포인트 프로세스 동작, 웹 셸 업로드 시도, 비정상적인 네트워크 연결.
- 로그/쿼리 힌트: 셰어포인트 ULS 로그에서 비정상적인 요청 패턴, IIS 로그에서 웹 셸 관련 HTTP 요청, 윈도우 이벤트 로그에서 비정상적인 프로세스 생성.
- 공격 성립 전제조건: 공격자는 셰어포인트 사이트 소유자 권한으로 인증되어야 한다. 네트워크 위치는 인터넷에 노출된 셰어포인트 서버에 접근 가능해야 한다.
- 노출 범위: 셰어포인트는 전 세계 수많은 기업에서 문서 관리 및 협업 플랫폼으로 사용되므로, 인터넷에 노출된 셰어포인트 서버를 사용하는 조직은 광범위하게 영향을 받을 수 있다.
- 악용 관측 여부: 마이크로소프트는 패치 공개 전 제로데이로 악용되었음을 확인했다. CISA KEV 등재는 실제 악용이 확인되었음을 의미한다.
- 패치 후 잔여 위험: 이미 침해된 경우, 패치만으로는 해결되지 않는다. 공격자가 백도어를 설치했거나 추가적인 악성 활동을 수행했을 가능성이 있으므로, 침해 여부 확인 및 포렌식 조사가 필수적이다.
- 오탐 없이 탐지하는 법: 정상적인 셰어포인트 관리 활동과 다른 비정상적인 코드 실행 시도, 웹 셸 업로드 패턴, 비정상적인 파일 생성 및 수정 활동을 모니터링한다. 특히, 셰어포인트 프로세스(w3wp.exe 등)에서 비

정상적인 자식 프로세스가 생성되는지 주시한다.

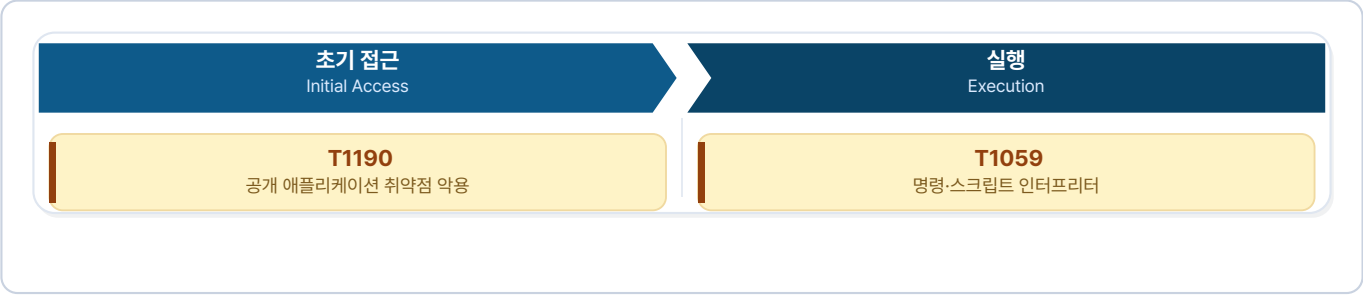


그림 4. MITRE ATT&CK 매트릭스

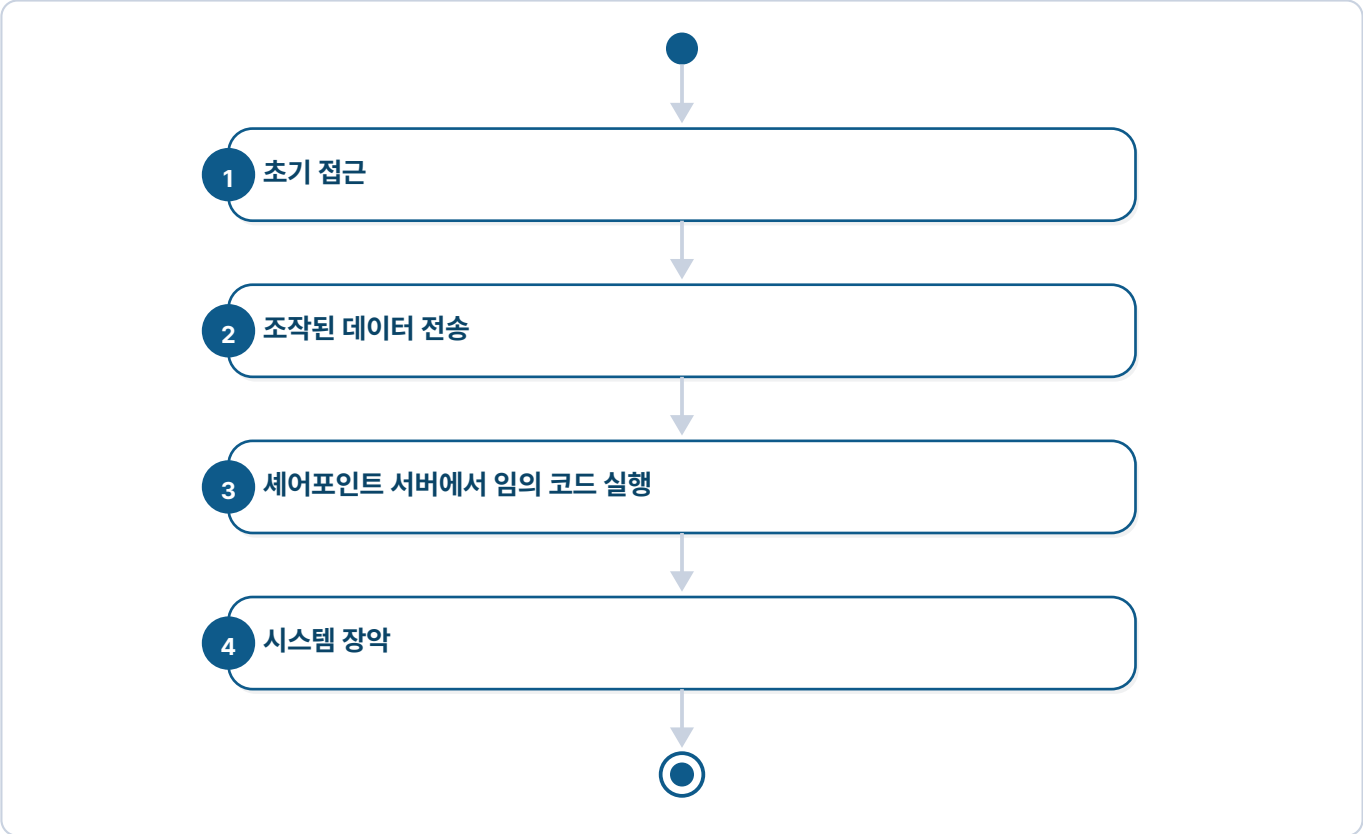


그림 5. 익스플로잇 흐름

- 유사 취약점의 과거 실제 악용 사례: 셰어포인트는 과거에도 원격 코드 실행 취약점으로 인해 여러 차례 공격 대상이 되었다. 예를 들어, 2020년에도 CVE-2020-0646과 같은 셰어포인트 RCE 취약점이 실제 공격에 악용된 바 있다. 이러한 취약점들은 주로 인증 우회 또는 역직렬화 결함을 통해 발생하며, 공격자에게 서버 제어권을 부여하여 민감 데이터 탈취, 웹 셸 설치, 추가 악성코드 배포 등으로 이어진다.
- 유사 CVE와의 비교: CVE-2026-58644는 인증된 공격자가 필요하다는 점에서 인증되지 않은 공격자가 악용할 수 있는 취약점보다는 초기 접근 난이도가 높지만, 일단 인증되면 치명적인 영향을 미친다. CVSS 점수 9.8은 네트워크를 통해 낮은 권한으로도 높은 기밀성, 무결성, 가용성 영향을 줄 수 있음을 의미한다.
- 초래한 피해/교훈: 셰어포인트와 같은 협업 플랫폼은 기업의 핵심 데이터와 업무 흐름을 담고 있어, 이러한 취약점은 데이터 유출, 서비스 중단, 랜섬웨어 감염 등 광범위한 피해를 초래할 수 있다. 교훈은 핵심 시스템에 대한 지속적인 보안 모니터링과 제로데이 공격에 대비한 신속한 패치 관리 프로세스 구축의 중요성이다.

## 2.2 포티넷 포티샌드박스 OS 명령 주입 취약점 (CVE-2026-39808, CVE-2026-25089)

표 4. 취약점 상세 명세 (CVE · CVSS · CWE · 영향 범위 · 악용 현황)

| 항목 | 내용 |
|---|---|
| 취약점 식별·심각도 (CVE·CVSS·CWE) | — |
| 영향 제품·버전 | Fortinet FortiSandbox |
| 공개일 | 2026-04-14 |
| 악용 현황 | CISA KEV 등재(실제 악용 확인) · 조치 기한 2026-07-19 |
| PoC·익스플로잇 | — |
| 패치·완화 | — |
| 대응 우선순위 | 최우선. CISA KEV 카탈로그에 등재되어 실제 악용이 확인되었으며, 연방 기관에 긴급 패치를 촉구했다. |

- CVE-2026-39808: CVSS v3.1 Base Score: 9.8 (Critical). CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.
- CVE-2026-25089: CVSS v3.1 Base Score: 9.8 (Critical). CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.
- 근본 원인: 두 취약점 모두 인증되지 않은 원격 코드 실행을 허용하는 명령 주입(Command Injection) 취약점이다. 입력값 검증 미흡으로 인해 공격자가 악의적인 명령어를 주입할 수 있다.
- 익스플로잇 벡터: 네트워크를 통한 원격 코드 실행. 인증이 필요하지 않다.
- IoC: FortiSandbox 로그에서 비정상적인 시스템 명령 실행, 비정상적인 프로세스 생성, 외부로의 비정상적인 네트워크 연결.
- 로그/쿼리 힌트: FortiSandbox 시스템 로그에서 명령 주입 시도 패턴, 비정상적인 셸 명령 실행 기록.
- 공격 성립 전제조건: 인증이 필요 없으며, FortiSandbox 장비가 네트워크에 노출되어 있어야 한다.
- 노출 범위: FortiSandbox는 기업 네트워크의 보안 솔루션으로 사용되므로, 인터넷에 직접 노출된 경우 심각한 위협이 된다.
- 악용 관측 여부: Defused 등 위협 인텔리전스 기업에서 공격자들이 이 취약점을 악용하기 시작했다고 보고했다. CISA KEV 등재는 실제 악용이 확인되었음을 의미한다.
- 패치 후 잔여 위험: 이미 침해된 경우, 공격자가 백도어를 설치했거나 추가적인 악성 활동을 수행했을 가능성이 있으므로, 침해 여부 확인 및 포렌식 조사가 필수적이다.

- 오탐 없이 탐지하는 법: FortiSandbox의 정상적인 운영 과정에서 발생하지 않는 비정상적인 시스템 명령어 실행 시도, 특히 셸 명령 실행 패턴을 모니터링한다.

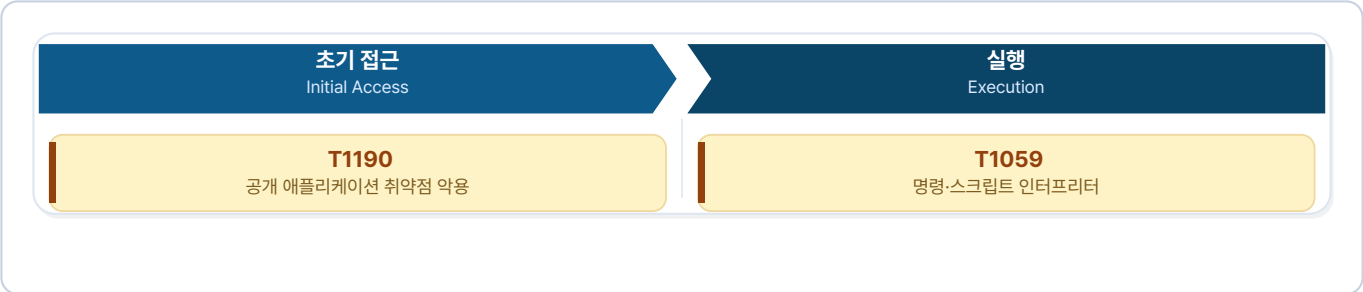


그림 6. MITRE ATT&CK 매트릭스

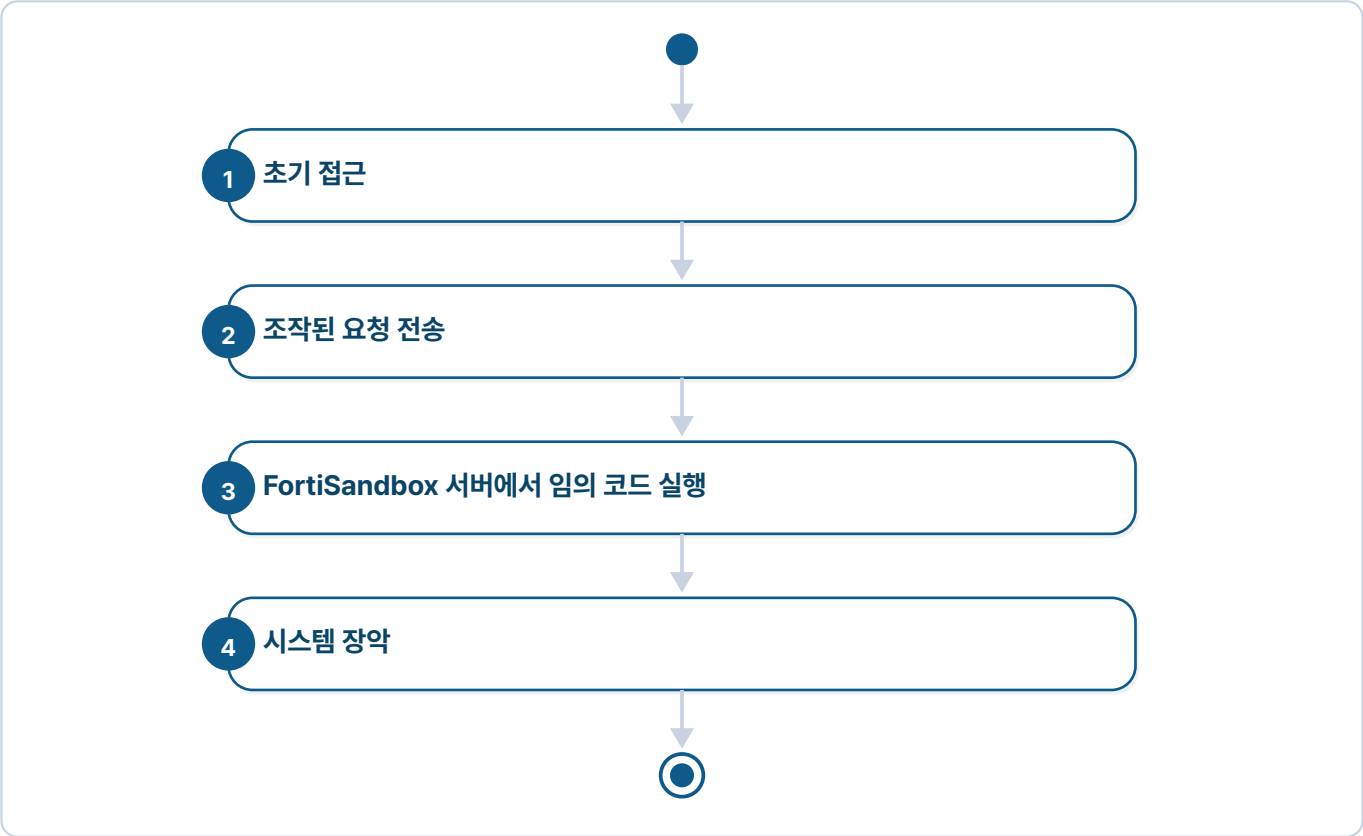


그림 7. 익스플로잇 흐름

- 유사 취약점의 과거 실제 악용 사례: Fortinet 제품은 과거에도 여러 차례 심각한 취약점으로 인해 공격 대상이 되었다. 특히 VPN, 방화벽 등 엣지 장비의 인증 우회 및 원격 코드 실행 취약점은 실제 공격에 자주 악용되어 왔다. 2022년에도 FortiOS SSL VPN의 취약점(CVE-2022-42475)이 제로데이로 악용되어 정부 기관을 포함한 다수의 조직이 피해를 입었다.
- 유사 CVE와의 비교: 두 취약점 모두 CVSS 9.8로, 인증 없이 네트워크를 통해 원격 코드 실행이 가능하여 매우 치명적이다. 이는 공격자가 특별한 사전 지식이나 권한 없이도 시스템을 완전히 장악할 수 있음을 의미한다.
- 초래한 피해/교훈: 보안 솔루션 자체의 취약점은 공격자에게 내부 네트워크 침투의 교두보를 제공하므로, 그 파급 효과가 매우 크다. FortiSandbox는 악성코드 분석을 위한 샌드박스 환경이므로, 이 취약점이 악용될 경우 분석 대상 악성코드가 샌드박스를 탈출하여 실제 시스템에 영향을 미칠 가능성도 배제할 수 없다.

교훈은 보안 장비에 대한 패치 관리 및 보안 강화가 일반 시스템보다 더욱 중요하며, 제로데이 공격에 대비한 위협 인텔리전스 활용이 필수적이라는 점이다.

## 2.3 오라클 E-비즈니스 스위트 취약점 (CVE-2026-46817)

표 5. 취약점 상세 명세 (CVE · CVSS · CWE · 영향 범위 · 악용 현황)

| 항목 | 내용 |
|---|---|
| 취약점 식별·심각도 (CVE·CVSS·CWE) | — |
| 영향 제품·버전 | Oracle E-Business Suite |
| 공개일 | 2026-05-28 |
| 악용 현황 | CISA KEV 등재(실제 악용 확인) · 조치 기한 2026-07-18 |
| PoC·익스플로잇 | — |
| 패치·완화 | — |
| 대응 우선순위 | 최우선. CISA KEV 카탈로그에 등재되어 실제 악용이 확인되었으며, 연방 기관에 토요일까지 패치를 명령했다. |

- 근본 원인: 인증되지 않은 공격자가 HTTP 네트워크 접근을 통해 시스템을 장악할 수 있는 취약점이다. 상세한 근본 원인은 오라클 권고를 통해 확인해야 하지만, 일반적으로 웹 애플리케이션의 입력값 검증 미흡, 접근 제어 우회, 또는 역직렬화 취약점 등이 원인일 수 있다.
- 익스플로잇 벡터: HTTP 네트워크를 통한 원격 코드 실행. 인증이 필요하지 않다.
- IoC: Oracle EBS 서버 로그에서 비정상적인 HTTP 요청 패턴, 비정상적인 프로세스 생성, 웹 셸 업로드 시도.
- 로그/쿼리 힌트: 웹 서버 로그에서 비정상적인 URL 접근, HTTP 요청 헤더/바디에 악성 페이로드 포함 여부 확인.
- 공격 성립 전제조건: 인증이 필요 없으며, Oracle EBS가 HTTP 네트워크에 노출되어 있어야 한다.
- 노출 범위: Oracle E-Business Suite는 전 세계 대기업에서 핵심 업무 시스템(ERP, CRM 등)으로 사용되므로, 인터넷에 노출된 경우 심각한 위협이 된다.
- 악용 관측 여부: 현재 활발히 악용되고 있는 것으로 확인되었다. CISA KEV 등재는 실제 악용이 확인되었음을 의미한다.
- 패치 후 잔여 위험: 이미 침해된 경우, 공격자가 백도어를 설치했거나 추가적인 악성 활동을 수행했을 가능성이 있으므로, 침해 여부 확인 및 포렌식 조사가 필수적이다.

- 오탐 없이 탐지하는 법: Oracle EBS 웹 서버 로그에서 정상적인 사용자 요청과 다른 비정상적인 HTTP 요청 패턴, 특히 시스템 명령 실행을 시도하는 페이로드 포함 여부를 면밀히 분석한다.

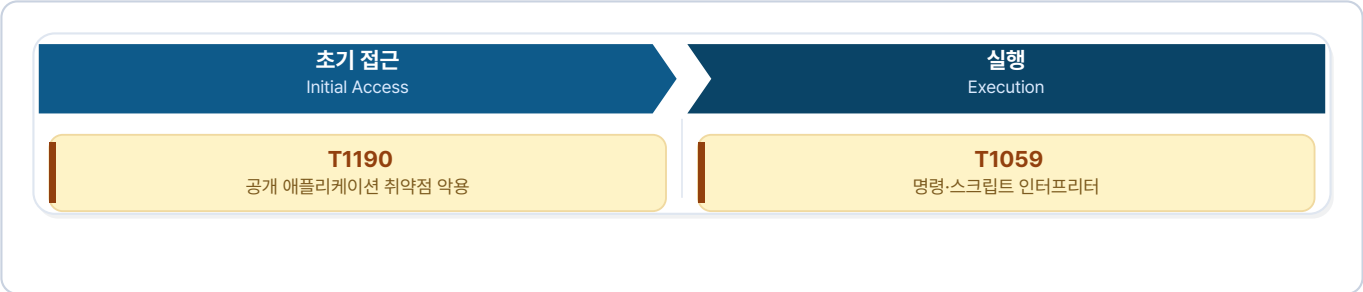


그림 8. MITRE ATT&CK 매트릭스

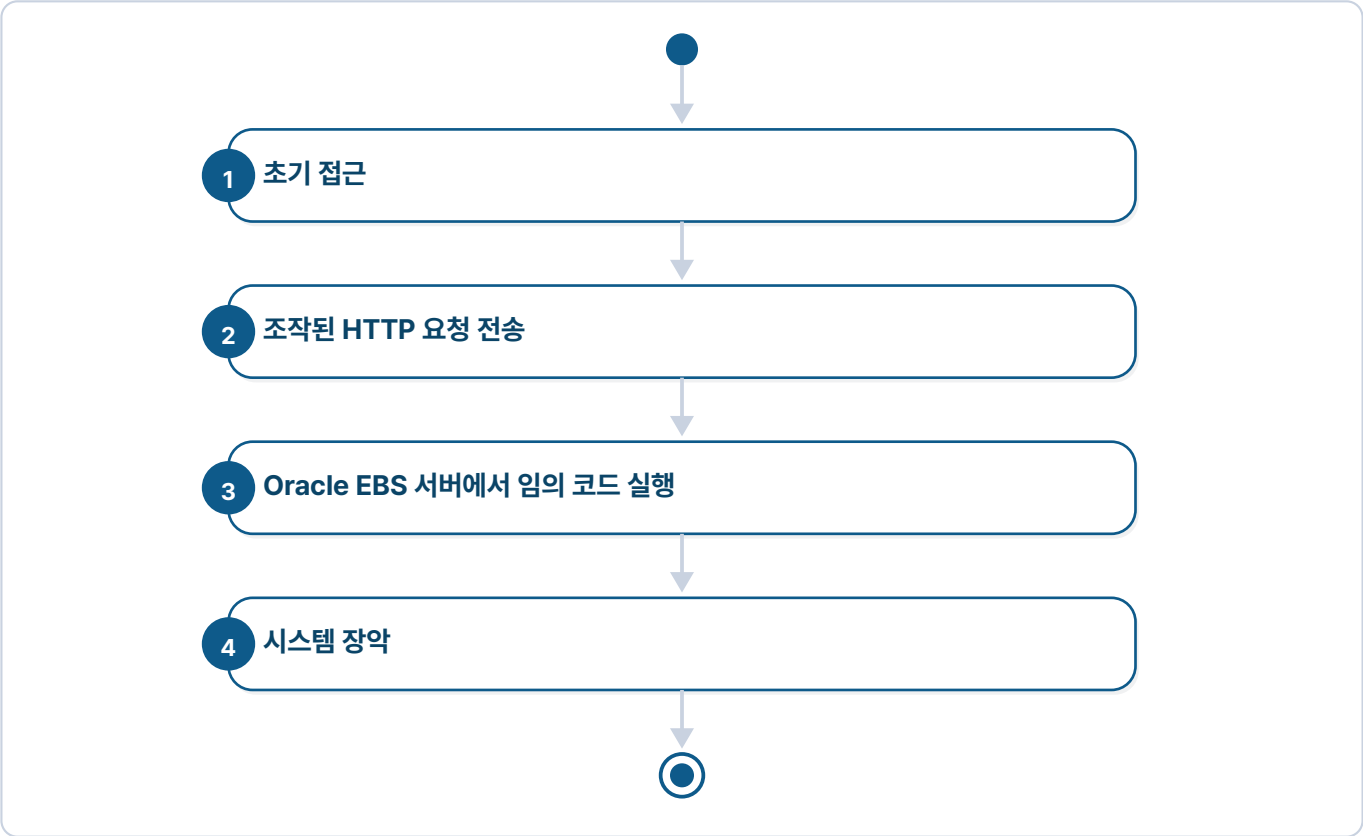


그림 9. 익스플로잇 흐름

- 유사 취약점의 과거 실제 악용 사례: Oracle E-Business Suite는 기업의 핵심 데이터를 다루는 시스템이므로, 과거에도 여러 차례 심각한 취약점으로 인해 공격 대상이 되어왔다. 특히 인증 우회, SQL 인젝션, 원격 코드 실행 취약점 등은 실제 공격에 악용되어 데이터 유출, 시스템 파괴 등의 피해를 초래했다.
- 유사 CVE와의 비교: CVSS 9.8은 인증 없이 네트워크를 통해 원격 코드 실행이 가능하여 매우 치명적이다. 이는 공격자가 특별한 사전 지식이나 권한 없이도 기업의 핵심 업무 시스템을 완전히 장악할 수 있음을 의미한다.
- 초래한 피해/교훈: Oracle EBS와 같은 핵심 업무 시스템의 취약점은 기업 운영 전반에 치명적인 영향을 미칠 수 있다. 데이터 유출은 물론, 업무 마비, 재정적 손실 등으로 이어질 수 있다. 교훈은 핵심 업무 시스템에 대한 보안 취약점 관리 및 패치 적용을 최우선으로 해야 하며, 인터넷에 노출된 시스템에 대한 접근 제어를 강화해야 한다는 점이다.

## 2.4 F5 NGINX 및 BIG-IP 취약점 (CVE-2026-42533 외 다수)

표 6. 취약점 상세 명세 (CVE · CVSS · CWE · 영향 범위 · 악용 현황)

| 항목 | 내용 |
|---|---|
| 취약점 식별·심각도 (CVE·CVSS·CWE) | — |
| 영향 제품·버전 | NGINX Plus, NGINX 오픈소스, NGINX 인그레스 컨트롤러, BIG-IP (정확한 영향 버전은 벤더 권고 참조 필요) |
| 공개일 | 2026-07-15 |
| 악용 현황 | — |
| PoC·익스플로잇 | — |
| 패치·완화 | — |
| 대응 우선순위 | 높음. 실제 악용 사례는 보고되지 않았으나, 웹 서비스의 핵심 인프라 장비이므로 DoS 공격으로 인한 서비스 중단 위험이 크다. |

- CVE-2026-42533: CVSS v3.1 Base Score: 7.5 (High). CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H. (힙 버퍼 오버플로우로 인한 DoS) [2]
- 그 외 다수 고위험 DoS 취약점.
- 근본 원인: CVE-2026-42533은 조작된 HTTP 요청을 통해 힙 버퍼 오버플로우를 유발하여 NGINX 워커 프로세스를 재시작시키는 서비스 거부(DoS) 취약점이다. 다른 취약점들도 DoS를 유발할 수 있는 결함들이다.
- 익스플로잇 벡터: 네트워크를 통한 서비스 거부 공격.
- MITRE ATT&CK 기법 매핑: 가용성 영향 (T1499: 서비스 거부).
- IoC: NGINX/BIG-IP 로그에서 비정상적으로 큰 HTTP 요청, 비정상적인 요청 헤더/바디, NGINX 워커 프로세스 비정상 종료 및 재시작.
- 로그/쿼리 힌트: NGINX/BIG-IP 접근 로그에서 특정 패턴의 HTTP 요청, 시스템 로그에서 NGINX 프로세스 크래시 및 재시작 이벤트.
- 공격 성립 전제조건: NGINX/BIG-IP가 네트워크에 노출되어 있어야 한다.
- 노출 범위: NGINX는 전 세계 웹 서버 시장에서 높은 점유율을 차지하며, BIG-IP는 로드 밸런서 및 웹 애플리케이션 방화벽(WAF)으로 널리 사용되므로, 광범위한 조직이 영향을 받을 수 있다.
- 악용 관측 여부: F5는 이 취약점들이 실제 공격에 악용되었다는 언급은 하지 않았다.
- 패치 후 잔여 위험: DoS 취약점이므로 패치 적용으로 위험이 해소된다.

- 오탐 없이 탐지하는 법: 정상적인 트래픽 패턴과 다른 비정상적인 HTTP 요청 크기, 빈도, 내용 등을 분석하여 DoS 공격 시도를 탐지한다. 특히, NGINX 워커 프로세스의 비정상적인 재시작 횟수를 모니터링한다.

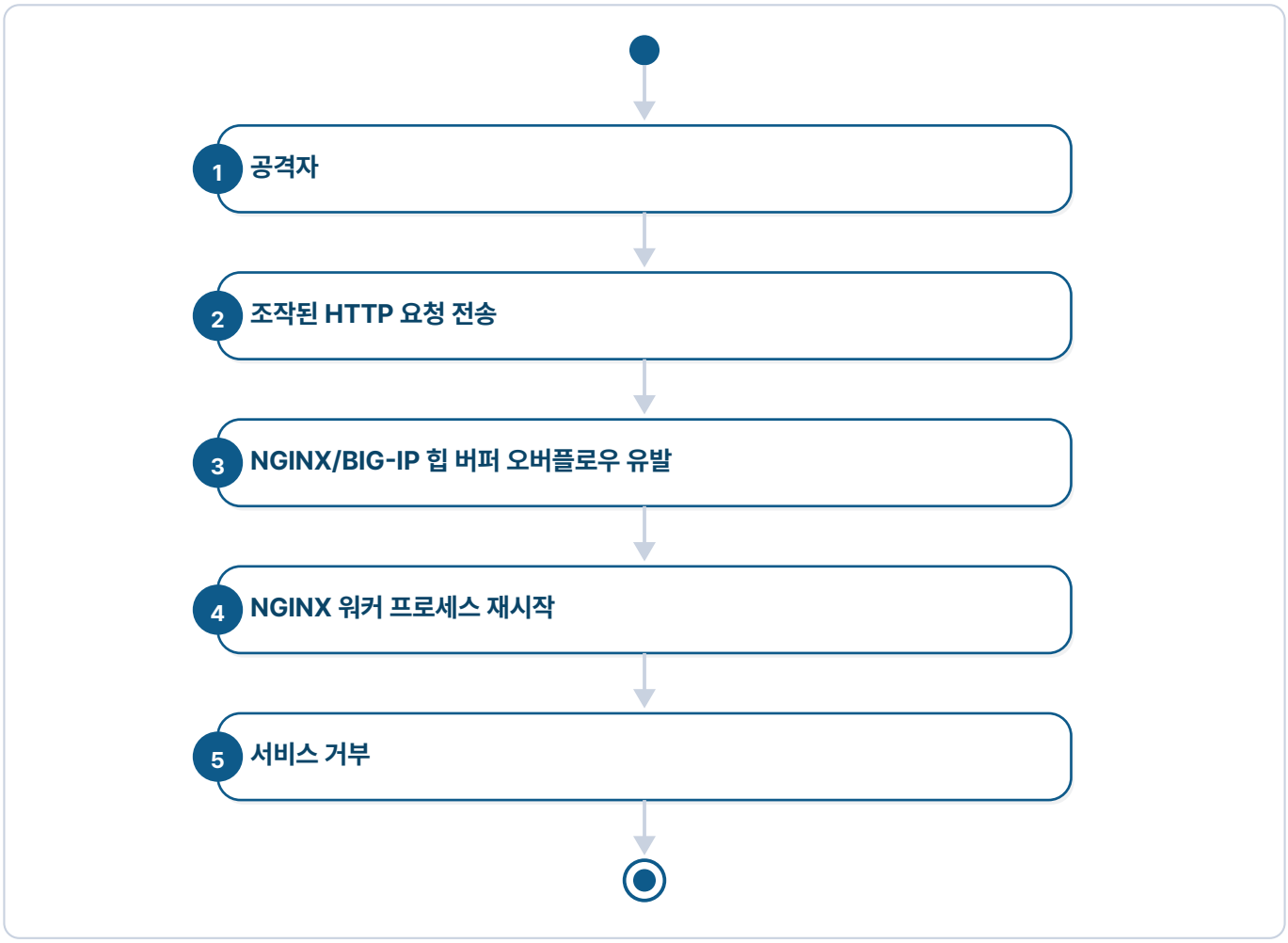


그림 10. 익스플로잇 흐름

- 유사 취약점의 과거 실제 악용 사례: NGINX 및 F5 BIG-IP는 과거에도 DoS 취약점으로 인해 여러 차례 공격 대상이 되었다. 특히 BIG-IP는 2020년 CVE-2020-5902와 같은 심각한 RCE 취약점으로 인해 광범위한 피해를 입은 바 있다. 웹 서비스의 최전선에 위치하는 장비이므로, DoS 공격은 서비스 가용성에 직접적인 영향을 미쳐 기업의 비즈니스 연속성을 위협한다.
- 유사 CVE와의 비교: CVE-2026-42533은 DoS 취약점으로 CVSS 점수 7.5는 높지만, RCE 취약점(9.8)보다는 심각도가 낮다. 그러나 웹 서비스의 핵심 인프라에 대한 DoS 공격은 실제 비즈니스에 큰 피해를 줄 수 있다.
- 초래한 피해/교훈: DoS 공격은 서비스 중단으로 인한 매출 손실, 고객 신뢰도 하락 등 심각한 비즈니스 영향을 초래할 수 있다. 교훈은 웹 서비스의 핵심 인프라에 대한 지속적인 보안 업데이트와 함께, DoS 공격에 대비한 트래픽 필터링, 로드 밸런싱, 캐싱 등 다계층 방어 전략을 구축해야 한다는 점이다.

# 3 주요 보안 사고

## 3.1 코카콜라 자회사 페어라이프 랜섬웨어 공격

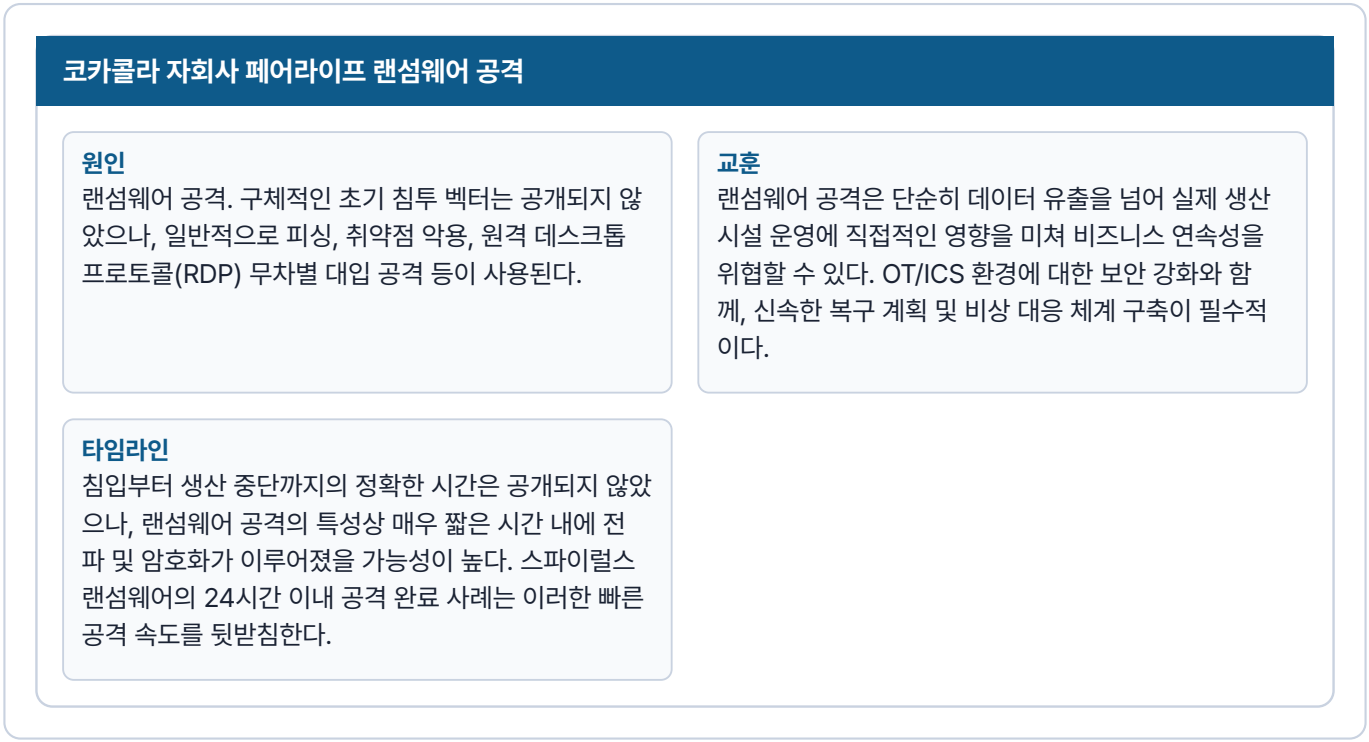


그림 11. 사고 한눈에 보기

- 원인/근본 원인: 랜섬웨어 공격. 구체적인 초기 침투 벡터는 공개되지 않았으나, 일반적으로 피싱, 취약점 악용, 원격 데스크톱 프로토콜(RDP) 무차별 대입 공격 등이 사용된다.
- 피해 규모/범위: 미국 내 유제품 생산 일시 중단. 제품 품질과 안전, 캐나다 생산 시설은 영향을 받지 않았다. 데이터 도난 여부나 공격 배후는 아직 공개되지 않았다.
- 구체적 대응/완화책: 회사는 사고 대응 프로토콜을 가동했으며, 조사가 진행 중이다.
- 교훈: 랜섬웨어 공격은 단순히 데이터 유출을 넘어 실제 생산 시설 운영에 직접적인 영향을 미쳐 비즈니스 연속성을 위협할 수 있다. OT/ICS 환경에 대한 보안 강화와 함께, 신속한 복구 계획 및 비상 대응 체계 구축이 필수적이다.

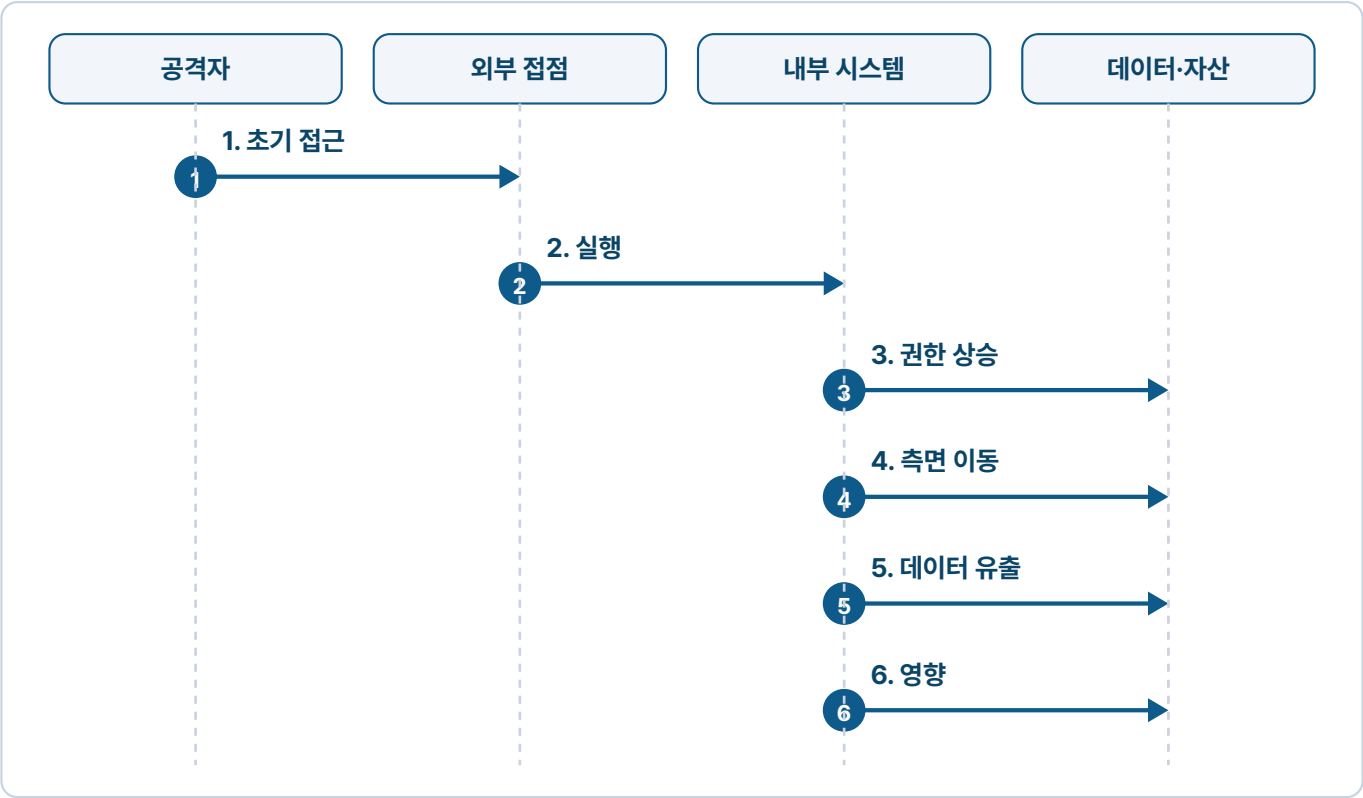


그림 12. 침해 시나리오


그림 13. MITRE ATT&CK 매트릭스

- 타임라인: 침입부터 생산 중단까지의 정확한 시간은 공개되지 않았으나, 랜섬웨어 공격의 특성상 매우 짧은 시간 내에 전파 및 암호화가 이루어졌을 가능성이 높다. 스파이럴스 랜섬웨어의 24시간 이내 공격 완료 사례는 이러한 빠른 공격 속도를 뒷받침한다.
- 탐지 실패 지점: 초기 침투 단계에서 탐지되지 못했을 가능성이 높다. 엔드포인트 탐지 및 대응(EDR) 솔루션, 네트워크 침입 탐지 시스템(NIDS)의 우회 또는 미흡한 설정이 원인일 수 있다.
- 공격자 프로파일: 아직 공개되지 않았으나, 산업 제어 시스템(ICS)을 표적으로 하는 랜섬웨어 그룹이거나, 일반적인 금전적 동기의 랜섬웨어 그룹이 OT 환경까지 공격 범위를 확장했을 가능성이 있다.
- 피해 산정: 생산 중단으로 인한 매출 손실, 복구 비용, 브랜드 이미지 손상 등 막대한 간접 피해가 예상되나, 구체적인 수치는 공개되지 않았다.
- 같은 구조를 가진 조직이 지금 확인할 것: OT/ICS 네트워크와 IT 네트워크 간의 분리(에어갭 또는 강력한 방화벽), OT/ICS 시스템에 대한 취약점 관리 및 패치 적용, 비정상적인 네트워크 트래픽 및 프로세스 모니

터링, 정기적인 백업 및 복구 훈련.

## 3.2 뉴지스탁 관리자 계정 침해 및 개인정보 유출

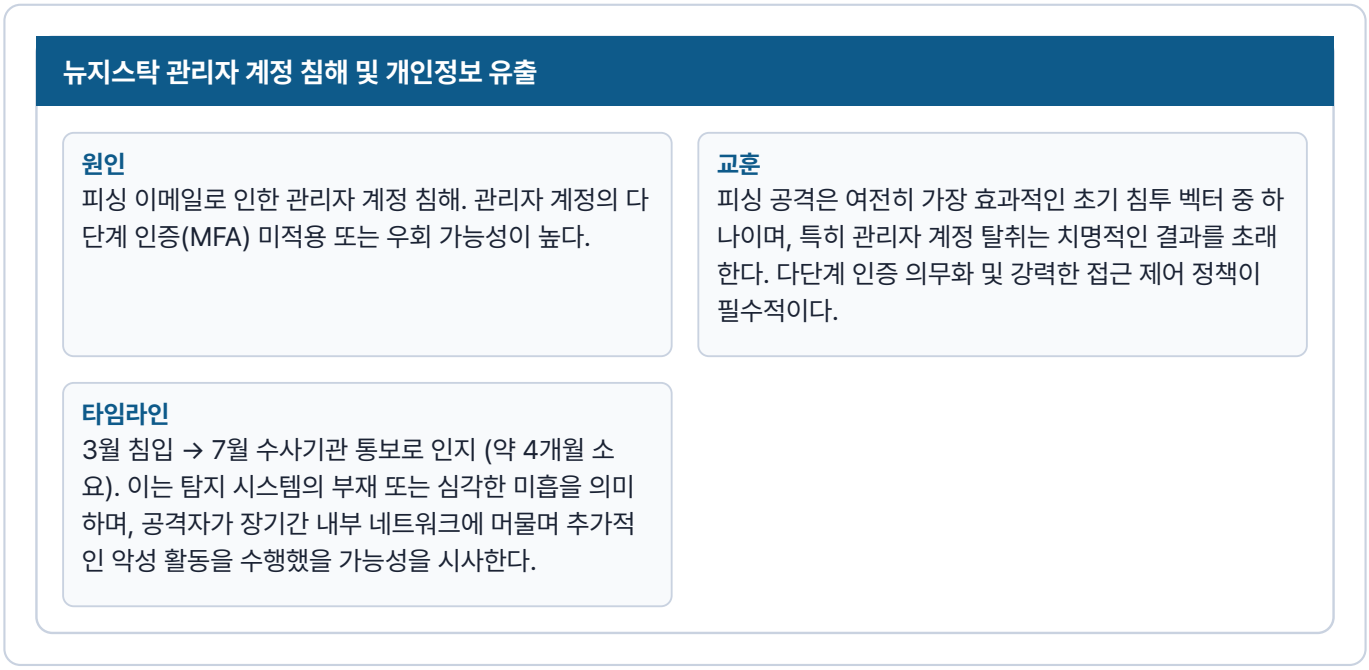


그림 14. 사고 한눈에 보기

- 원인/근본 원인: 피싱 이메일로 인한 관리자 계정 침해. 관리자 계정의 다단계 인증(MFA) 미적용 또는 우회 가능성이 높다 [3].
- 피해 규모/범위: 회원 아이디, 닉네임, 접속 정보 등 개인정보 유출. 이메일 주소와 비밀번호는 포함되지 않은 것으로 확인되었다.
- 구체적 대응/완화책: 수사기관 통보 후 유출 사실 인지 및 대응.
- 교훈: 피싱 공격은 여전히 가장 효과적인 초기 침투 벡터 중 하나이며, 특히 관리자 계정 탈취는 치명적인 결과를 초래한다. 다단계 인증 의무화 및 강력한 접근 제어 정책이 필수적이다. 또한, 침해 탐지 및 대응 시스템의 부재 또는 미흡으로 인해 사고 인지까지 4개월이 소요된 점은 심각한 문제이며, 신속한 탐지 시스템 구축이 시급하다.

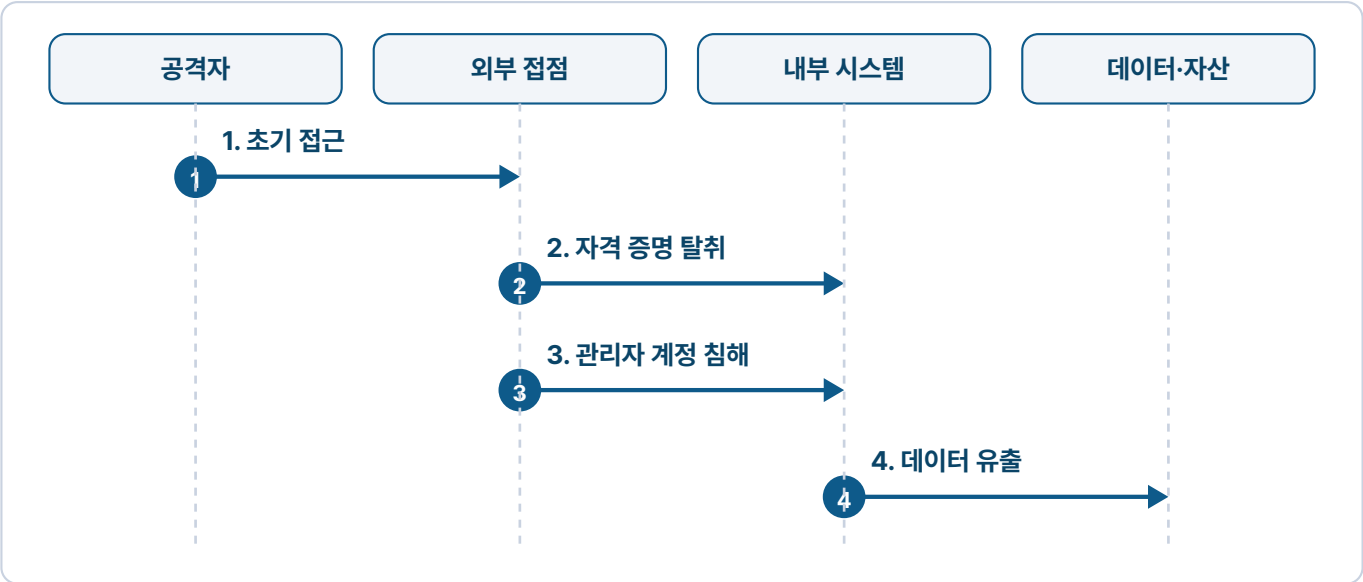


그림 15. 침해 시나리오

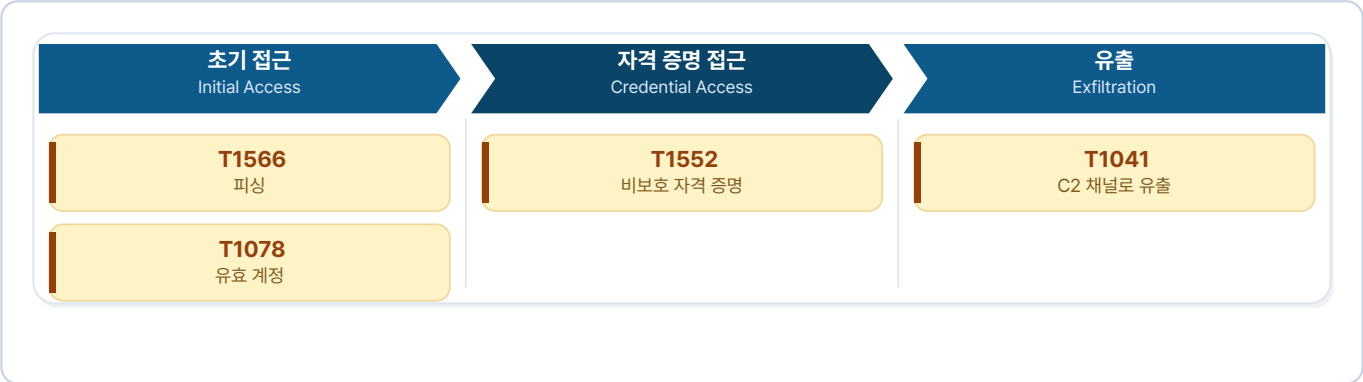


그림 16. MITRE ATT&CK 매트릭스

- 타임라인: 3월 침입 → 7월 수사기관 통보로 인지 (약 4개월 소요). 이는 탐지 시스템의 부재 또는 심각한 미흡을 의미하며, 공격자가 장기간 내부 네트워크에 머물며 추가적인 악성 활동을 수행했을 가능성을 시사한다.
- 탐지 실패 지점: 관리자 계정의 비정상적인 접근 패턴, 데이터 유출 시도 등에 대한 모니터링 및 경고 시스템이 작동하지 않았을 가능성이 높다.
- 공격자 프로파일: 금전적 이득을 노리는 해커 그룹 또는 개인일 가능성이 높다.
- 피해 산정: 유출된 개인정보의 정확한 규모는 공개되지 않았으나, 회원 정보 유출은 기업의 신뢰도 하락 및 법적 제재로 이어질 수 있다. 2022년에도 해킹으로 개인정보가 유출된 이력이 있어, 반복적인 사고에 대한 책임이 가중될 수 있다.
- 같은 구조를 가진 조직이 지금 확인할 것: 모든 관리자 계정에 대한 다단계 인증(MFA) 의무화, 비정상적인 로그인 시도 및 접근 패턴 모니터링, 최소 권한 원칙 적용, 정기적인 보안 감사 및 침투 테스트, 침해 탐지 및 대응(EDR/XDR) 솔루션 도입.

## 3.3 23andMe 유전자 데이터 유출 합의금 지급

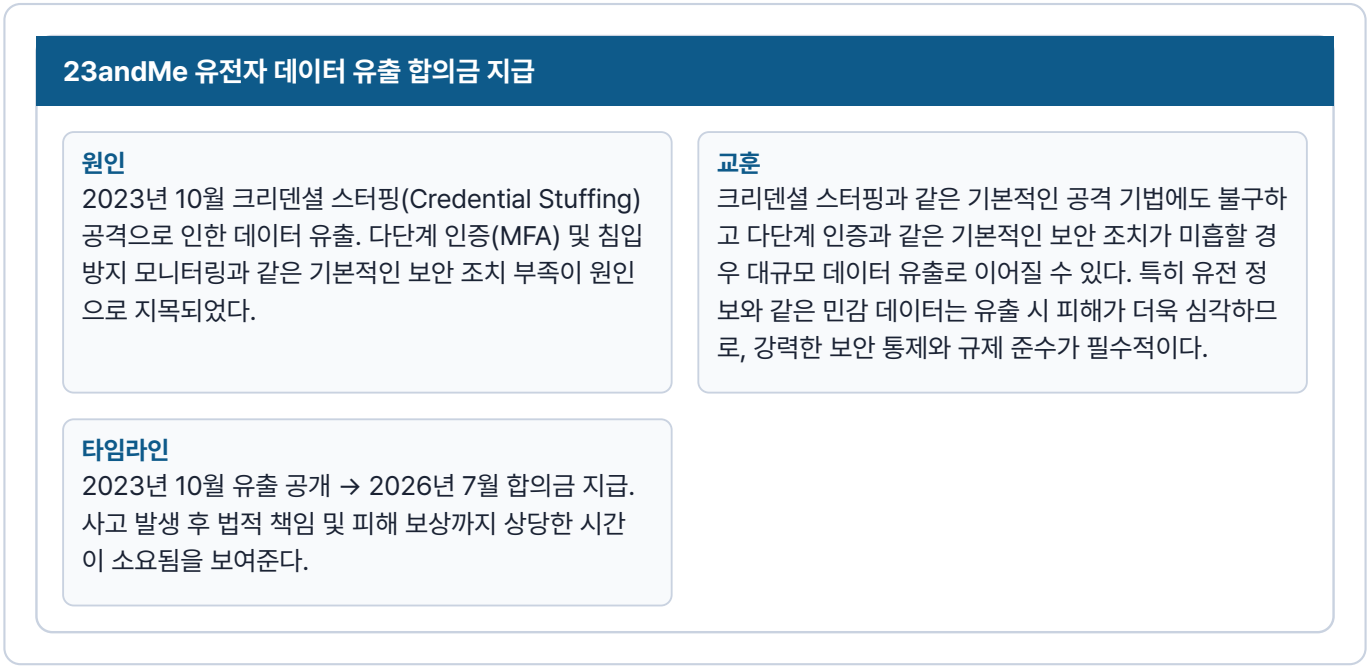


그림 17. 사고 한눈에 보기

- 원인/근본 원인: 2023년 10월 크리덴셜 스터핑(Credential Stuffing) 공격으로 인한 데이터 유출. 다단계 인증(MFA) 및 침입 방지 모니터링과 같은 기본적인 보안 조치 부족이 원인으로 지목되었다 [1].
- 피해 규모/범위: 690만 명 고객의 유전 정보 도난. 43개 주 법무장관 연합과의 합의에 따라 1,800만 달러 지불.
- 구체적 대응/완화책: 1,800만 달러 합의금 지불. 향후 보안 조치 강화가 요구될 것으로 예상된다.
- 교훈: 크리덴셜 스터핑과 같은 기본적인 공격 기법에도 불구하고 다단계 인증과 같은 기본적인 보안 조치가 미흡할 경우 대규모 데이터 유출로 이어질 수 있다. 특히 유전 정보와 같은 민감 데이터는 유출 시 피해가 더욱 심각하므로, 강력한 보안 통제와 규제 준수가 필수적이다.

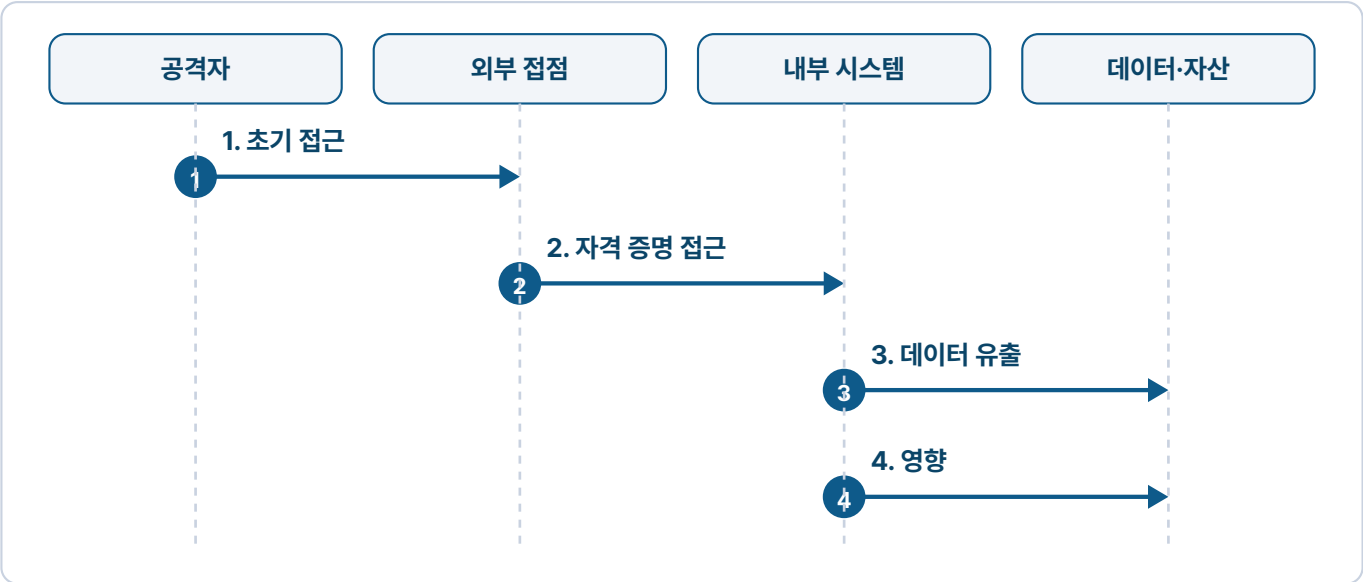


그림 18. 침해 시나리오

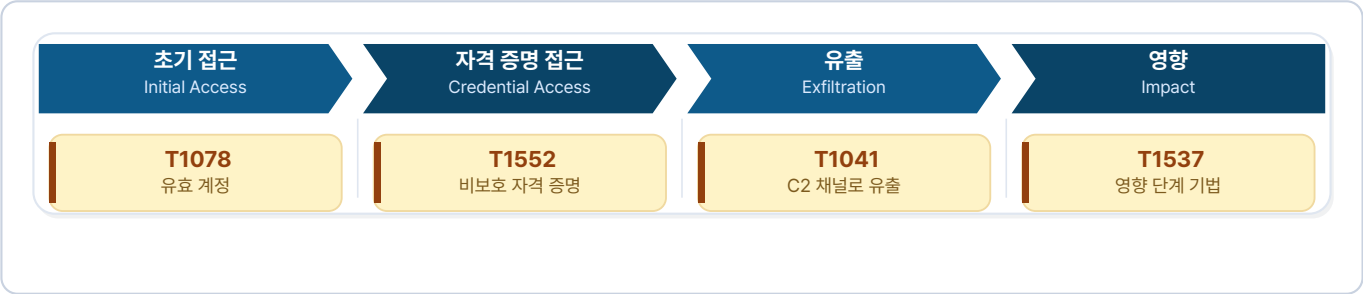


그림 19. MITRE ATT&CK 매트릭스

- 타임라인: 2023년 10월 유출 공개 → 2026년 7월 합의금 지급. 사고 발생 후 법적 책임 및 피해 보상까지 상당한 시간이 소요됨을 보여준다.
- 탐지 실패 지점: 크리덴셜 스터핑 공격에 대한 비정상적인 로그인 시도 탐지 및 차단 시스템이 미흡했거나, 다단계 인증이 적용되지 않아 공격이 성공했을 가능성이 높다.
- 공격자 프로파일: 대량의 유출된 자격 증명을 활용하는 금전적 동기의 해커 그룹일 가능성이 높다.
- 피해 산정: 1,800만 달러의 합의금은 직접적인 금전적 피해이며, 고객 신뢰도 하락, 브랜드 이미지 손상, 향후 소송 가능성 등 간접 피해는 더욱 클 것으로 예상된다.
- 같은 구조를 가진 조직이 지금 확인할 것: 모든 사용자 계정에 대한 다단계 인증(MFA) 의무화, 크리덴셜 스터핑 공격 방어를 위한 봇 관리 솔루션 도입, 비정상적인 로그인 시도 모니터링 및 차단, 정기적인 보안 감사 및 취약점 점검.

## 4 국내외 주요 보안 공지·패치·규제

- CISA KEV 카탈로그 업데이트: CISA는 마이크로소프트 셰어포인트(CVE-2026-58644), 포티넷 포티샌드박스(CVE-2026-39808, CVE-2026-25089), 오라클 E-비즈니스 스위트(CVE-2026-46817)의 4개 취약점을 KEV 카탈로그에 추가하고 연방 기관에 긴급 패치를 명령했다. 이는 해당 취약점들이 실제 공격에 악용되고 있음을 의미하며, 모든 조직이 즉시 패치를 적용해야 함을 강조한다.
- 마이크로소프트 7월 패치 화요일: 622개의 취약점이 패치되었으며, 이 중 62개는 심각한 수준이다. 3개의 제로데이 중 2개는 현재 공격에 악용되고 있다. 이는 AI를 활용한 취약점 연구 가속화로 인해 패치해야 할 취약점 수가 급증하고 있음을 시사한다.
- F5 긴급 보안 업데이트: NGINX와 BIG-IP 제품의 8개 취약점(CVE-2026-42533 포함)을 해결하는 업데이트를 발표했다. 웹 서비스의 핵심 인프라 장비이므로 신속한 적용이 필요하다.
- 지멘스 SICAM 8 취약점 패치: 다수 SICAM 8 제품에서 서비스 거부 등을 유발할 수 있는 여러 취약점이 발견되어 새 버전이 출시되었다. ICS/OT 환경의 보안 취약점은 물리적 피해로 이어질 수 있으므로 즉시 업데이트해야 한다.
- Splunk, Zoom 취약점 패치: Splunk와 Zoom이 자사 제품의 여러 심각 및 고위험도 보안 결함에 대한 패치를 발표했다.
- 국내 개인정보 보호 규제 강화: 이재명 대통령은 개인정보 유출 및 악용에 대한 경제적 제재를 강화하고, 기업이 사전에 개인정보 보호에 투자하도록 제도를 전환해야 한다고 강조했다. 9월 11일부터 반복적이거나 중대한 개인정보 보호법 위반 기업에 전체 매출액의 최대 10%까지 징벌적 과징금을 부과할 수 있는 제도가 시행된다. 또한, 개인정보 유출 증거 은닉·폐기 신고 포상금 도입 및 유출된 개인정보 구매·유포 행위 금지 등 규제가 강화될 예정이다. 이는 국내 기업들에게 개인정보 보호에 대한 투자와 책임 강화를 요구하는 중요한 변화이다.

## 5 실무 권고 · 체크리스트

CISA KEV 등재 취약점 즉시 패치: 마이크로소프트 셰어포인트(CVE-2026-58644), 포티넷 포티샌드박스(CVE-2026-39808, CVE-2026-25089), 오라클 E-비즈니스 스위트(CVE-2026-46817) 취약점은 현재 실제 공격에 악용되고 있으므로, 가장 시급하게 패치를 적용해야 한다. 패치 적용 전후로 시스템 침해 여부를 면밀히 확인하고, 필요한 경우 포렌식 조사를 수행해야 한다.

- 마이크로소프트 셰어포인트, 포티넷 FortiSandbox, 오라클 E-Business Suite의 최신 보안 패치를 즉시 적용한다.
- F5 NGINX/BIG-IP, 지멘스 SICAM 8, Splunk, Zoom 등 2026년 7월 2주차 발표된 모든 벤더의 보안 업데이트를 검토하고 적용한다.
- 정기적인 취약점 스캐닝 및 패치 관리 프로세스를 강화하고, 제로데이 및 활성 악용 취약점에 대한 위협 인텔리전스를 지속적으로 모니터링한다.
- 모든 관리자 계정 및 중요 시스템 계정에 다단계 인증(MFA)을 의무화한다.
- 크리덴셜 스터핑 공격 방어를 위해 봇 관리 솔루션을 도입하고, 비정상적인 로그인 시도 및 접근 패턴을 모니터링한다.
- 최소 권한 원칙을 적용하고, 불필요한 계정 및 권한을 제거한다.
- 정기적인 백업을 수행하고, 백업 데이터의 불변성(immutable)을 보장하며, 오프라인 또는 격리된 환경에 보관한다.
- 랜섬웨어 공격에 대비한 침해 대응 계획을 수립하고, 정기적인 모의 훈련을 실시한다.
- OT/ICS 환경과 IT 네트워크를 분리하고, OT/ICS 시스템에 대한 보안 가시성을 확보한다.
- 사용자들에게 피싱 이메일, 악성 파일(예: 위장된 TTF 파일) 및 사회 공학 기법에 대한 보안 교육을 강화한다.
- 이메일 보안 게이트웨이(SEG) 및 엔드포인트 보안 솔루션을 강화하여 악성 파일 및 피싱 이메일 유입을 차단한다.
- AI 음성 피싱 등 새로운 피싱 기법에 대한 경각심을 높이고, 의심스러운 요청에 대해서는 반드시 다른 채널로 확인하는 습관을 강조한다.
- 9월 11일 시행되는 징벌적 과징금 제도에 대비하여 개인정보 보호법 준수 여부를 재점검한다.
- 개인정보 유출 사고 발생 시 은닉·폐기 행위가 없도록 투명한 보고 및 대응 절차를 수립한다.
- 개인정보 보호를 위한 기술적, 관리적 보호 조치에 대한 투자를 확대한다.

## 6 다음 주 전망

- 제로데이 및 활성 악용 취약점 지속 증가 (신뢰도: 높음): 2026년 7월 2주차 CISA KEV 카탈로그에 다수의 제로데이 취약점이 추가된 것은 공격자들이 새로운 취약점을 빠르게 찾아내고 악용하는 추세가 지속될 것임을 시사한다. AI를 활용한 취약점 연구 가속화는 이러한 흐름을 더욱 강화할 것으로 예상된다. 기업들은 정기적인 패치 주기 외에도 긴급 패치에 대한 신속한 대응 체계를 유지해야 한다.
- 랜섬웨어 공격의 고도화 및 속도 증가 (신뢰도: 높음): '젠틀맨' 그룹의 활동 증가와 '스파이럴스' 랜섬웨어의 빠른 공격 속도는 랜섬웨어 공격이 더욱 정교하고 신속해질 것임을 보여준다. 특히 OT/ICS 환경을 노리는 공격이 증가할 가능성이 있으며, 이는 생산 중단과 같은 물리적 피해로 이어질 수 있다. 백업 및 복구 전략의 재점검과 함께, 침해 탐지 및 대응 시간 단축이 핵심 과제가 될 것이다.
- 사회 공학 및 AI 기반 피싱 공격 진화 (신뢰도: 높음): AI 음성 피싱 연구 결과와 금융 피싱의 일상적인 업무 위장 사례는 공격자들이 AI 기술을 활용하여 사회 공학 기법을 더욱 고도화할 것임을 시사한다. 단순한 기술적 방어뿐만 아니라 사용자 교육 및 행동 변화를 유도하는 것이 더욱 중요해질 것이다.
- IoT 기기를 통한 봇넷 및 내부망 침투 위협 지속 (신뢰도: 중간): 패치 없는 저가형 IoT 기기들이 봇넷의 공격 대상이 되며 '영원한 취약점'으로 작용한다는 경고는 IoT 보안의 중요성을 다시금 강조한다. 스마트 홈, 스마트 오피스 환경에서 미검증 IoT 기기 도입 시 내부망 침투의 위험이 있으므로, 하드웨어 제조 단계부터 보안을 내재화하는 'Security by Design' 접근 방식이 확산될 필요가 있다.
- 개인정보 보호 규제 강화에 따른 기업의 대응 변화 (신뢰도: 높음): 국내 징벌적 과징금 제도의 9월 시행은 기업들이 개인정보 보호에 대한 투자를 확대하고, 사고 발생 시 더욱 투명하게 대응하도록 유도할 것이다. 이는 장기적으로 국내 기업들의 전반적인 보안 수준 향상에 기여할 것으로 예상된다.

# 출처

아래 번호는 본문의 [N] 인용 표기와 대응합니다.

**[1]** 23andMe to pay $18 million in new genetics data breach settlement

**[2]** F5 Patches Multiple NGINX, BIG-IP Vulnerabilities

**[3]** 뉴지스탁, 피싱메일로 관리자 계정 침해…회원 개인정보 유출