롯데카드 온라인 결제 서버 침해 사고 발생

▶ 롯데카드, 오라클 서버 취약점으로 해킹 공격 및 데이터 유출 가능성 확인

침해사고 일시	8.26	발생국가	한국
침해사고 유형	해킹	침해사고 규모	-

- 8월 26일, 롯데카드는 내부 점검 중 일부 서버에서 악성코드 감염을 발견해 전수 점검을 진행했고, 3개 서버에서 악성코드 2종과 웹셸 5종을 삭제함. 이어 8월 31일 온라인 결제 서버에서 외부 공격자의 자료 유출 시도를 추가로 확인함. 9월 1일, 롯데카드는 온라인 결제 서버를 대상으로 한 해킹 공격을 금융당국에 신고했고 약 1.7GB 규모의 파일이 반출됐을 가능성을 보고함.
- 금융감독원 조사에 따르면 이번 공격은 오라클 웹로직(Oracle WebLogic) 서버의 원격 코드 실행 취약점(CVE-2017-10271)을 이용한 것으로 분석됨. 해당 취약점은 인증 없이 원격 명령 실행이 가능해 공격자가 서버를 완전 장악할 수 있는 치명적 보안 결함으로, 2017년 이미 패치가 제공됐음에도 관리 부실로 여전히 노출돼 있었음. 이번 사건은 구형 취약점 관리 부실이 주요 원인으로 지적됨.
- 국내 보안기업 분석 결과, 동일한 취약점에 노출된 국내 서버는 6,802대로 파악되며 금융기관과 공공기관, 민간 기업 상당수가 여전히 패치되지 않은 상태임. 전문가들은 이번 사건을 계기로 금융권 전반의 보안 업데이트 체계 미흡 문제가 드러났다고 경고함. 공격자는 침투 후 웹셸을 심어 내부망 장악을 시도했으며, 거래 요청 정보 등 결제 관련 데이터가 포함됐을 가능성이 제기됨.
- 금융감독원과 금융보안원은 합동 현장 조사를 통해 고객 개인정보 유출 여부와 추가 피해 가능성을 조사 중임. 롯데카드는 피해 회원 보호를 위해 개인정보 모니터링을 강화하고 있으며 금융당국은 부정사용 피해 발생 시 전액 보상 방침을 발표함. 보안 전문가들은 향후 보안 패치의 신속한 적용, 외부 노출 서버의 정기 점검, 웹 방화벽(WAF) 및 위협 탐지 시스템 강화가 필수적이라고 강조함.

1) https://www.dailysecu.com/news/articleView.html?idxno=169318
2) https://www.dailysecu.com/news/articleView.html?idxno=200055

브라질 핀테크 기업 신키아(Sinqia), 금융 탈취 해킹 시도 발생

▶ 브라질 에버텍의 자회사 신키아(Sinqia), 약 1억 3천만 달러 금융 탈취 시도 발생

침해사고 일시	8.29	발생국가	브라질
침해사고 유형	해킹	침해사고 규모	약 1억 3천만 달러

- 8월 29일, 브라질 상파울루에 본사를 둔 핀테크 기업 신키아(Sinqia S.A.)의 결제 시스템이 해킹 공격을 받아 약 1억 3천만 달러(약 1,750억 원)에 달하는 자금 탈취 시도가 발생함. 신키아는 미국계 금융 기술 기업 에버텍(Evertec Inc.)의 자회사로, 브라질 중앙은행이 운영하는 실시간 결제 시스템 '픽스(Pix)' 환경을 통해 24개 금융기관에 서비스를 제공함.
- 공격자는 IT 공급업체 계정을 통한 우회 침입 방식을 사용했으며, 과거 여러 랜섬웨어 조직이 활용해 온 자격 증명 탈취 기반 공격 수법과 유사한 것으로 분석됨. 공격자는 외부 IT 공급업체의 계정 정보를 탈취해 신키아의 픽스(Pix) 결제 시스템에 무단으로 접근한 뒤 두 개 금융기관을 대상으로 대규모 무단 자금 이체를 시도함. 이 과정에서 일부 거래가 진행됐으나, 신키아가 비정상적 네트워크 트래픽을 탐지해 즉시 픽스 거래를 중단하고 포렌식 전문가와 함께 대응을 개시함.
- 브라질 중앙은행은 추가 피해를 방지하기 위해 신키아의 픽스 접속 권한을 임시로 차단했으며, 현재까지 고객 개인정보 유출 정황은 확인되지 않았다고 발표함. 다만 정확한 피해 금액과 이체 성공 여부는 아직 조사 중이며 탈취 시도 금액 중 일부는 회수된 것으로 알려짐.
- 브라질 금융당국은 이번 사건을 심각한 금융 인프라 보안 위협으로 규정하고 관련 금융기관을 대상으로 실시간 결제망 보안점검과 추가 규제 강화를 예고함. 에버텍은 사이버 보안 체계를 재점검하는 한편, 공급망 보안 강화를 위해 외부 보안 감사 및 침투 테스트를 확대할 계획임. 이번 공격은 전 세계 금융권에서 반복적으로 문제가 되고 있는 공급망 해킹(Supply Chain Attack)의 전형적인 사례임.

1) https://www.bleepingcomputer.com/news/security/hackers-breach-fintech-firm-in-attempted-130m-bank-heist/
2) https://dailysecurityreview.com/cyber-security/evertec-confirms-130m-fraud-attempt-in-sinqia-pix-cyberattack/

클라우드 플랫폼 클라우드플레어(Cloudflare), 공급망 공격 피해 발생

▶ 클라우드플레어(Cloudflare), 세일즈포스(Salesforce) 공급망 공격 및 초대형 DDoS 공격 발생

침해사고 일시	8.29	발생국가	미국
침해사고 유형	데이터 유출	침해사고 규모	-

- 8월 29일, 미국 기반 글로벌 클라우드 플랫폼인 클라우드플레어(Cloudflare)는 세일즈포스(Salesforce) 환경에서 발생한 공급망 공격의 피해를 공식 확인함. 이번 공격은 세일즈로프트(SalesLoft)와 드리프트(Drift) 통합 환경에서 탈취된 OAuth 토큰을 악용한 방식으로, 8월 12일부터 17일까지 고객 데이터가 유출된 것으로 조사됨. 노출된 정보는 고객 연락처, 지원 티켓, 일부 환경 설정 값과 액세스 토큰 등 민감 데이터를 포함하며 약 700개 이상의 기업이 연쇄적으로 피해를 입은 것으로 파악됨.
- 클라우드플레어는 사건 직후 상세한 침해 조사 보고서를 공개하고 IOC(침해 지표), 보안 권고사항 및 대응 방안을 투명하게 공유함. 회사는 고객에게 자격 증명 교체, SaaS 애플리케이션 보안 강화, 서드파티 통합 관리 정책 점검을 권고했으며, 피해 고객에게 이메일과 대시보드 알림을 통해 개별 통지함.
- 이번 사건은 단일 기업의 보안 침해를 넘어, 세일즈포스 생태계를 타깃으로 한 대규모 공격 캠페인의 일환으로 확인됨. Palo Alto Networks, Zscaler, Cisco, Farmers Insurance, Qantas, Adidas, LVMH 등 다수의 글로벌 기업도 피해를 입었으며, 구글 위협 인텔리전스 그룹은 Drift 이메일 통합을 통한 Salesforce 테넌트 접근이 악용되고 있다고 경고함.
- 한편, 클라우드플레어는 같은 기간 사상 최대 규모인 초당 11.5Tbps UDP 플러드 형태의 DDoS 공격을 차단했다고 발표함. 공격은 약 35초간 지속됐으며, 구글 클라우드 등 다수의 클라우드 인프라가 공격에 악용된 것으로 파악됨. 클라우드플레어는 향후 SaaS 통합 환경 보안을 강화하고, 서드파티 위험 관리 및 도구 체인 보안 표준을 재정립하겠다고 발표함. 업계는 이번 대응을 기술력과 투명성을 겸비한 모범 사례로 평가하고 있음.

1) https://www.cybersecurity-insiders.com/cloudflare-admits-data-breach-following-cyber-attack/
2) https://dailysecurityreview.com/cyber-security/cloudflare-confirms-salesforce-breach-in-growing-supply-chain-attack/

미국 타이어 제조사 브리지스톤(Bridgestone), 생산 공장 일부 운영 중단

▶ 미국 타이어 제조사 브리지스톤(Bridgestone), 북미 생산 공장 일부 사이버 공격 발생

침해사고 일시	9.1	발생국가	미국
침해사고 유형	해킹	침해사고 규모	-

- 9월 1일, 세계 최대 타이어 제조사 브리지스톤(Bridgestone)의 북미 일부 공장에서 사이버 공격으로 운영 중단이 발생함. 피해 공장은 미국 사우스캐롤라이나주 에이컨카운티(Aiken County) 공장 두 곳과 캐나다 퀘벡주 졸리에트(Joliette) 공장으로 약 1,400명의 직원이 일시적으로 업무를 중단한 것으로 확인됨. 회사는 네트워크를 즉시 격리하고 비상 대응팀을 가동했으며, 현재 포렌식 조사를 진행 중이라고 발표함.
- 브리지스톤 아메리카스(BSA)는 이번 사건을 "제한적인 사이버 사고"로 정의하며, 초기 차단에 성공했다고 설명함. 고객 데이터와 외부 연결 시스템은 침해되지 않았다는 입장을 유지하며, 피해 최소화를 위해 예방 정비 작업을 지시함. 공장 근로자에게는 예방 정비 참여 시 전액 임금을 지급하거나 무급 휴가를 선택할 수 있도록 지원책을 마련함. 그러나 졸리에트 시장은 내부 메모를 근거로 북미 전역 공장이 영향을 받았을 가능성을 언급함.
- 공격 배후와 방식은 아직 명확히 확인되지 않았으며 랜섬웨어 여부 또한 공식적으로 발표되지 않음. 보안 전문가들은 공격 양상에서 랜섬웨어 가능성을 배제할 수 없다고 분석하지만, 브리지스톤은 2022년 락빗(LockBit) 랜섬웨어 공격과는 성격이 다르다고 강조함. 한편, 이번 사건과 동일한 날 재규어 랜드로버(Jaguar Land Rover)도 사이버 공격을 받아 두 사건 간 연계 가능성이 제기됨.
- 브리지스톤은 북미에서 50개 생산 시설을 운영하며 그룹 매출의 43%를 차지하는 핵심 조직으로, 장기화 시 타이어 공급망 전반에 큰 영향을 미칠 우려가 있음. 브리지스톤은 보안 프로토콜을 강화하고 외부 기관과 협력해 재발 방지 대책을 마련하겠다고 밝혔음.

1) https://www.bleepingcomputer.com/news/security/tire-giant-bridgestone-confirms-cyberattack-impacts-manufacturing/
2) https://cybernews.com/security/bridgestone-cyberattack-auto-manufacturer-disrupted-jaguar-link/