

AhnLab

2022년 3분기 보안위협 동향



보안 사고 사례에서 웹 보안의 비중, 사례 등을 차장서 직접적인 시뮬레이션의 필요성을 강조하면 될 듯
 ‘안랩’에서 발표한 2022년 3분기 보안위협 동향에서 공격유형별 통계를 살펴보면, 애플리케이션 취약점이 36%로 1위, 웹기반 공격이 33%로 2위이다.

2023년 7월 17일에 발표된 ‘안랩’의 악성코드 분석, 대응 조직인 안랩시큐리티대응센터가 악성코드 유형별로 분석한 결과인 ‘2023년 상반기 보안위협 동향’을 살펴보면,



위와 같이 악성코드인 공격차가 추가 공격 수행을 위해 주로 사용하는 악성코드인 ‘다운로더’와 ‘백도어’가 각각 1, 2위를 기록하였고 정보유출형 악성코드인 ‘인포스틸러’가 뒤를 이었다. 또한, 피싱 메일 키워드 통계에서는 ‘주문-배송’과 관련된 키워드가 전체의 29.2%로 가장 높은 비중을 차지하였고 ‘결제-구매’가 그 다음으로 14.9%를 차지하며 2위를 기록하였다. 즉, 금전과 연관되어 사용자가 민감하게 반응할 수 있는 키워드들이 높은 순위를 차지하였다.

대부분의 쇼핑몰의 계정이 연결되어 있지 않고 독립적인 로그인 체제를 가지고 있기에, 대부분의 사용자들이 같은 비밀번호를 사용하는 경우가 많다. 2023년 초, 개인정보보호위원회가 온라인쇼핑몰을 중심으로 크리덴셜 스테핑 등 계정 정보 도용 사례가 증가하고 있다며 온라인 쇼핑몰 이용자와 기업들의 각별한 주의를 요구하였다. 여기서 발생하는 ‘크리덴셜 스테핑(Credential Stuffing)’ 공격은 해커가 이미 유출되거나 사전에 탈취한 사용자 계정(ID)과 비밀번호를 다른 웹사이트 등에 무작위로 대입해서 로그인이 성공하면 해당 사용자 정보를 빼가는 공격 수법이다.



(https://www.iitp.kr/kr/1/knowledge/statisticsView.it?masterCode=publication&searClassCode=K_STAT_01&identifier=02-008-230403-000001)

위 사진은 정보통신기획평가원에서 2022년에 발표한 자료이다. 국내 가구 인터넷 접속률은 99.96%에 달해 우리나라 2,136만 가구가 인터넷 접속이 가능하다는 것을 알 수 있다. 국내의 인터넷 이용자 수(이용률)는 최근 1개월 이내 인터넷 이용을 기준으로 약 47,253,345명인 93%에 달한다. 위 통계는 전반적으로 90%가 넘는다는 대부분의 사람들이 웹을 기본적으로 사용하고 있음을 나타내고 있다.

복잡한 위협 환경 다루기

사이버 보안 사고의 주요 원인

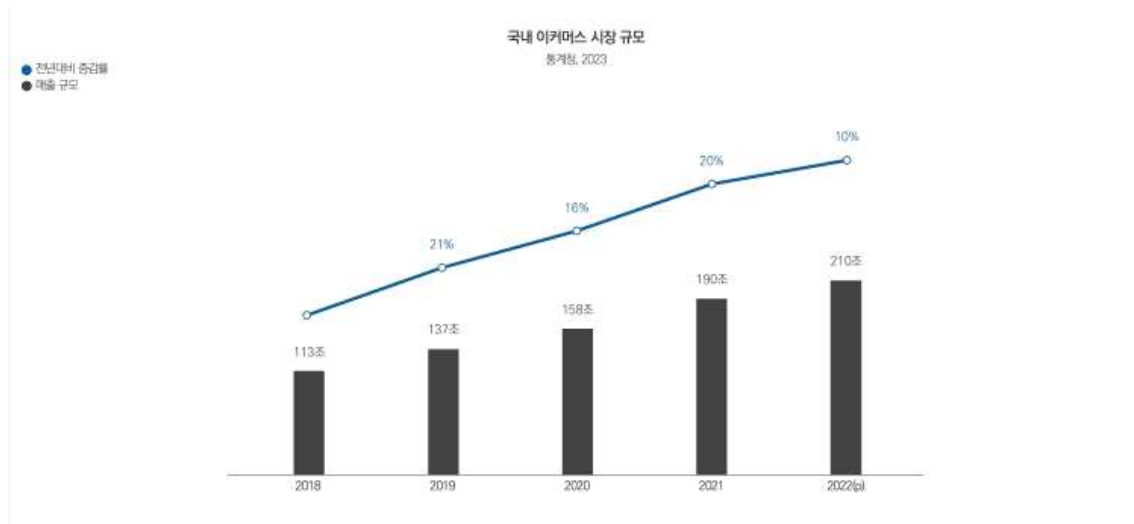


(<https://ddaily.co.kr/page/view/2023091416425212681>)

콘텐츠 전송 및 네트워크(CDN) 및 사이버보안 서비스를 제공 중인 클라우드플레어는 아시아태평양 지역의 사이버보안 현황을 조명한 보고서를 발표하였는데 그 자료의 일부이다. 2023년 9월 기준으로 지난 1년간 한국 응답자 61%는 지난 1년간 사이버보안 사고를 경험하였는데 웹공격/DDoS 공격이 50%를 차지하고 있었다.

(https://www.mezzomedia.co.kr/data/insight_m_file/insight_m_file_1580.pdf)

다음은 온라인 마케팅 분야에서 매체 서비스를 제공하는 인터넷 미디어업사인 메조미디어의 조사 내용이다.



위 통계는 2023년 통계청에서 발표한 국내 이커머스 시장(전자상거래, 인터넷을 통해 이루어지는 모든 거래) 규모를 나타낸 것이다. 2022년 이커머스 시장 규모는 약 210조 원으로 전년 대비 10% 증가하였고, 꾸준히 시장 규모가 커지고 있는 모습을 볼 수 있다.



또한, 고물가-고금리-고환율로 해외직구를 통해 물건을 싸게 구입하려는 소비자가 증가하며 온라인쇼핑 해외 직구 시장 규모가 빠르게 커지고 있는 것을 확인할 수 있는데 2023년 금감원의 발표에 의하면, 해외 온라인 가맹점은 구매와 달리 카드정보를 암호화하지 않은 상태에서 사이트 내 저장해 결제 처리하는 사례가 많아 해킹 등에 의한 카드정보 유출 위험에 노출돼 있다고 설명하기도 하였다.