보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

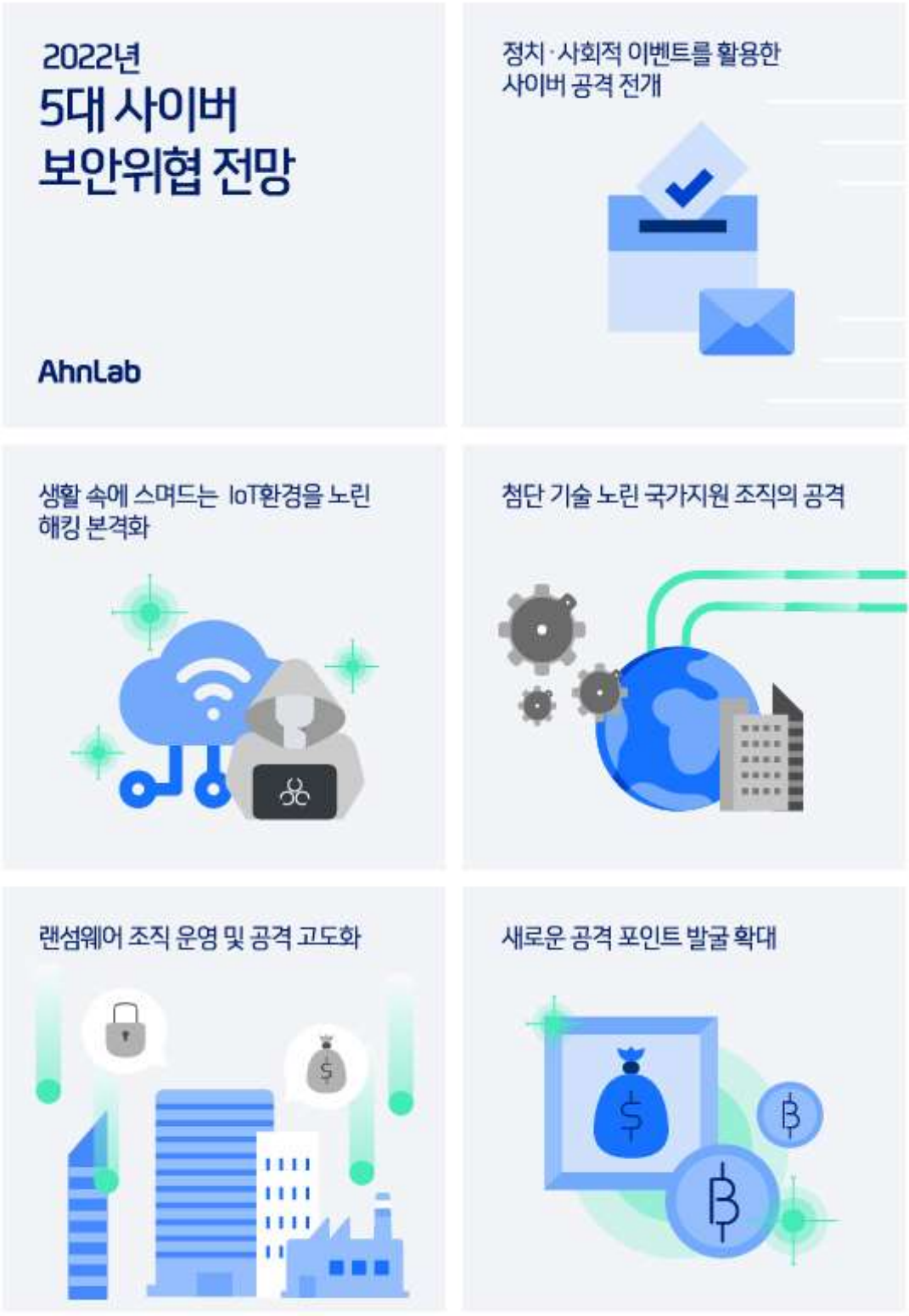
2022 보안 위협 전망 1부: 사이버 보안 주요 화두는?

AhnLab 2022-01-03

사이버 위협 측면에서 2021년은 그 어느때보다 파란만장한 해였다. 미국 콜로니얼 파이프라인을 공격한 '다크사이드 랜섬웨어(DarkSide Ransomware)', 지금까지도 사용자들을 위협하고 있는 'Log4j 취약점' 등 굵직한 글로벌 보안 이슈 뿐만 아니라 국내에서도 월패드 영상 유출, 각종 랜섬웨어 감염 사례가 잇따르면서 사용자들을 직접적으로 위협했다.

2021년을 뒤로하고 새로이 맞은 2022년, 사용자들이 주의해야할 보안 이슈는 무엇이 있을까? 이번 글에서는 안랩이 발표한 2022년 5대 사이버 보안 위협 전망을 살펴본다.

안랩이 '2022년 5대 사이버 보안 위협 전망'을 발표했다. 안랩이 전망한 내년 주요 보안위협은 ▲정치/사회적 이벤트를 활용한 공격 전개 ▲생활 속에 스며드는 IoT 환경을 노린 해킹 본격화 ▲첨단기술 노린 국가지원 조직의 공격 ▲랜섬웨어 조직 운영 및 공격 고도화 ▲새로운 공격 포인트의 가시화 등이다.



[그림] 2022 5대 사이버 보안 위협 전망

안랩 시큐리티대응센터(ASEC) 한창규 센터장은 "다양한 부문에서 디지털 전환이 진행 중인 가운데 공격자들은 급변하는 IT 환경과 이슈를 공격에 악용할 것으로 보인다"며 "특히 IT기술이 생활의 일부가 됨에 따라 새로운 공격 대상이 등장하고 그 방식도 고도화하고 있어, 개인과 조직 모두 나의 일상을 지킨다는 마음으로 생활 속 보안 수칙을 지켜야한다"고 말했다.

다음은 안랩의 2022년 5대 사이버 보안 위협 전망을 정리한 것이다.

1. 정치/사회적 이벤트 활용한 사이버 공격 전개
2022년에는 베이징 동계 올림픽(2월)과 카타르 월드컵(11월) 등 세계적인 스포츠 이벤트와 대통령 선거 등 정치적 이벤트가 많다. 이러한 사회 주요 이슈는 전통적으로 공격자들이 사이버 공격에 자주 활용하는 소재다. 올해도 공격자들은 주요 이벤트를 위장해 스피어 피싱* 이메일, 랜섬웨어 유포시도, 스미싱 등 사회공학적 공격을 전개할 것으로 보인다.

이외에도 대형 이벤트에 대한 국민적 관심을 노려 사회적 혼란을 발생시키기 위한 사이버 공격 그룹의 공격 가능성도 존재하는 만큼, 수상한 이메일 첨부파일이나 문자를 실행하지 않는 등 상시적인 주의가 필요한 해다.
*스피어 피싱(Spear phishing): 불특정 다수가 아닌 특정인(조직)을 대상으로 악성 메일을 발송하는 표적형 피싱 공격

2. 생활 속에 스며드는 IoT 환경을 노린 해킹 본격화
지난 2년간 원격근무가 보편화됨에 따라 홈오피스족을 노린 공격이 발생했다면, 2022년에는 우리 생활 속에 스며든 IoT 환경을 노린 공격도 본격화할 전망이다. 특히 최근 5G 기반 빠르고 안정적인 네트워크의 보급으로 월패드, 스마트 스피커, 홈카메라 등과 같은 네트워크 연결 지점이 확장되고 있다.

최근 발생한 월패드 영상 유출사례처럼, 2022년에 공격자는 우리의 일상생활에 사용하는 IoT 신제품이나 서비스를 노려 정보탈취 및 원격제어 등의 공격을 수행할 수 있다. 개인 사용자는 IoT 기기에 부여된 기본 비밀번호를 변경하는 등 기본 보안수칙을 실천해야 하며, 기관 및 기업은 변화하는 네트워크 환경을 고려한 보안 정책 수립과 대응방안을 마련해야 한다.

3. 첨단기술 노린 국가지원 조직의 공격
2021년 한 해 주요 국가 연구 기관을 대상으로 한 해킹시도가 이어진 가운데, 다가오는 2022년에도 첨단 기술을 노리는 국가 지원 공격조직의 사이버 공격이 이어질 것으로 예상된다. 국가의 안보를 위한 방위 산업뿐 아니라 사회 기반 시설이나 스마트 공장 등 OT(Operation Technology, 운영기술) 환경, 기계·자동차·바이오 등 기술 집약적 산업 분야를 노린 사이버 공격이 발생할 수 있다.

특히 코로나19 상황에서 중요도가 높아지고 있는 바이오분야나, 한국형 발사체 누리호로 주목을 받은 우주항공 산업 분야는 사이버 공격 조직의 타깃이 될 수 있다. 관련 기관 및 기업은 보안 동향을 주시하고 보안 솔루션 도입 및 보안교육 등으로 전반적인 보안수준을 높여야 한다.

4. 랜섬웨어 조직 운영 및 공격 고도화 (Ransomware Revival)
2021년 랜섬웨어로 인한 피해을 막고자 각국의 국제 공조 수사 등을 펼쳐 소기의 성과를 이뤘지만, 랜섬웨어 공격조직은 이를 피하고자 조직운영과 공격방식 면에서 더욱 고도화될 것으로 보인다. 먼저 공격자들은 조직 가입 조건을 강화하는 등 폐쇄적인 운영 방식을 이어가는 동시에, 사법기관 등의 추적을 피하기 위해 점조직화를 가속화 할 것으로 보인다.

랜섬웨어 공격 양상 또한 다변화되고 있다. 공격 조직은 무차별적인 랜섬웨어 유포로 몸값을 받아내는 고전적 전략을 벗어나, 가치 있는 정보를 보유한 기업을 타깃해 주요 정보를 탈취하고 금전도 노리는 방식을 취하기

시작했다. 이러한 양상이 더욱 증가할 것으로 보임에 따라 기업/기관에서는 위협 인텔리전스 서비스 등을 바탕으로 최신 랜섬웨어 공격 양상을 파악하고 이에 맞춘 대응 방안을 준비해야 한다.

5. 새로운 공격 포인트의 가시화

최근 확인된 'Log4j' 취약점의 사례처럼 일반 사용자에겐 생소하나 거의 모든 온라인 솔루션에 광범위하게 사용된 취약점 발견과 이를 악용한 공격시도가 활발해질 것으로 보인다. 또한, 기존에는 일부 사용자들만 관심을 가지던 암호화폐와 NFT(대체불가능토큰)가 대중의 관심을 받음에 따라, 주된 공격 대상으로 떠오를 것으로 보인다.

특히 PC에 저장된 암호화폐 지갑주소 등을 수집, 유출하거나 아예 공격자가 설빙한 별도의 지갑주소로 암호화폐를 전송하는 기존 악성코드 기능을 악용하여 NFT거래에서 금전적 피해를 유발하려는 시도도 등장하게 될 것이다. 이를 막기 위해서는 메일의 URL과 첨부파일을 함부로 실행하지 말고, 사용하는 SW의 보안패치를 최신으로 유지하는 등 기본 보안수칙의 생활화가 필수다.

AhnLab ASEC