보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

[2023 전망 1부] 안랩이 예측한 5대 사이버 보안 위협

AhnLab 2023-01-02

지난 한 해는 사이버 보안이 그 어느 때보다도 중요한 시기였다. 신/변종 랜섬웨어 공격, 기업 및 정부 기관을 노린 국가 배후 해킹 조직의 활동이 눈에 띄게 증가했다. 이 같은 추세는 2023년에도 지속될 것이다.

이와 관련해 김건우 안랩 시큐리티대응센터(ASEC)장은 "해커가 향후에도 모든 공격 포인트를 활용해 공격 효과를 극대화할 것이기에, 하나의 보안 만능키를 찾기보다는 기업과 사용자의 다면적인 접근이 필요하다"고 조언했다.

이 글에서는 2023년 IT 및 보안 업계에서 꼭 알아둬야 할 2023 5대 사이버 보안 위협의 전망을 살펴본다.

안랩이 전망하는 2023년 5대 사이버 보안 위협은 아래와 같다.

[그림] 2023년 5대 사이버 보안 위협 전망

1. 랜섬웨어 조직, '양보다 질' 전략 추구

최근 신규 랜섬웨어 등장이 주춤한 가운데, 향후 랜섬웨어 조직은 최소한의 공격으로 최대의 수익과 효과를 노리는 '양보다 질(Quantity to Quality)' 전략을 추구할 것으로 예상된다. 이를 위해 공격 단체는 우선 기업의 핵심 인프라를 장악한 다음, 정보유출부터 랜섬웨어 감염, 디도스(Distributed Denial of Service, DDoS) 공격까지 가하는 '다중 협박'으로 하나의 표적을 집요하게 노릴 것이다. 또한, 현재 전 세계적으로 랜섬웨어 조직에 대한 수사와 검거가 이루어지는 상황에서 압박감을 받은 사이버 범죄자가 대규모 공격을 감행한 후 은퇴할 가능성도 있다. 따라서 기업은 기본적인 보안 체계를 구축하는 것 외에 위협 인텔리전스(Threat Intelligence, TI)를 활용해 최신 공격 동향과 취약점 정보를 파악해야 한다.

2. 기업의 핵심 정보를 장기간 유출하는 '기생형' 공격 대세

2022년에는 기술, 개인정보 등 주요 자산을 보유한 가상자산 거래소와 대기업, 공공기관을 노린 공격이 기승을 부렸다. 일부 공격 단체는 자신의 성과를 외부에 공개하기도 했다. 공격자는 투자 대비 효과를 중요시하기에, 올해도 주요 기관 및 기업의 핵심 기술과 자산을 탈취하려는 시도는 계속될 것이며, 그 방식이 더 은밀해지고 고도화될 것으로 보인다. 특히, 과거와 같이 시스템을 파괴하거나 공개하는 보여주기식 공격보다는 인프라를 장악한 후 장기간에 걸쳐 핵심 기술 또는 민감 정보를 유출하는 '기생형' 공격이 주를 이룰 것으로 예상된다. 공격 방식도 계정 정보 수집은 물론, 화면 캡처, 영상 녹화 및 음성 녹음 등 광범위하게 확대될 수 있어 기업은 시스템의 모든 영역에 대응할 수 있는 통합 보안 체계를 구축해야 한다.

3. 파급력 높은 '잭팟' 취약점 발굴 및 지속적인 악용

작년 시스템의 주요 권한에 정상적인 접근이 가능하지만 취약점을 가진 드라이버를 악용하는'BYOVD(Bring Your Own Vulnerable Driver)' 공격 기법이 발견됐다. 올해도 공격자는 PC부터 모바일, 클라우드, 운영 기술(Operational Technology, OT) 환경을 가리지 않고 파급력이 높은 '잭팟' 취약점을 공격에 활용할 것이다. 이들은 보안 패치 지원이 중단된 소프트웨어(SW) 또는 직접 발굴하거나 다크웹(Dark Web)에서 구매한 미패치 취약점을 정보유출 및 랜섬웨어 공격에 악용할 수 있다. 따라서 기업 보안 담당자와 직원은 주기적으로 보안 패치를 적용하고, 미사용 프로그램은 삭제해야 한다.

4. 공급망 공격이 모바일 환경으로 확대

최근 금전 거래와 개인정보 활용 등이 모바일에서도 활발하게 행해지고 있어, 그동안 PC용 소프트웨어 중심으로 발생하던 공급망 공격이 모바일 영역으로 확대될 수 있다. 공격자는 악성코드를 만들어 유포하는 기존 방식보다 정상적인 앱 마켓에 등록할 수 있는 제작사, 제작 툴을 해킹해 앱 제작 초기 단계부터 침투하는 수법을 더 많이 사용할 것으로 보인다. 이 외에도 모바일 앱 배포 또는 업데이트 단계에서 악성코드 주입을 시도하거나, 탈취한 정상 모바일 앱 인증서를 앱 제작 및 배포에 활용할 수도 있다. 모바일 서비스 제공업체는 개발, 배포 과정에서 보안을 반드시 고려하고, 주요 자산에 대한 위협 탐지 및 대응 체계를 갖춰야 한다.

5. 개인의 가상자산 지갑을 노린 공격 심화

대형 암호화폐 거래소, 주요 블록체인 서비스에 대한 해킹 공격이 발생하면서, 코인, NFT(Non-fungible token) 등의 가상자산을 개인 지갑으로 옮기는 사용자가 증가하고 있다. 이에 따라 내년에는 개인의 가상자산 지갑을 노린 공격 시도도 증가할 것으로 예상된다. 예를 들어, 대다수 사용자가 계정 소유권 인증 및 지갑 복구에 사용되는 무작위 단어 조합인 시드 구문이나 12개 또는 24개 단어로 구성된 니모닉 키를 외우지 못해 사진, 이메일, 휴대폰 메모 기능으로 기록, 저장한다. 공격자는 니모닉 키 정보와 지갑 계정 정보를 탈취하기 위해 정보유출 악성코드 또는 유명 가상자산 지갑을 사칭한 피싱 웹사이트, 앱 유포를 확대할 것으로 보인다. 개인 지갑 사용자는 시드 구문 및 니모닉 키를 안전한 곳에 보관하고, 키 분실 위험으로부터 안전한 지갑을 사용해야 한다. 또, 송금하려는 지갑의 범죄 연루 여부도 꼼꼼히 확인해야 한다.

이 같은 보안 위협을 예방하기 위해 기업 차원에서는 △조직 내 PC, 운영체제, SW, 웹사이트 등에 대한 수시 보안 점검 및 패치 적용 △보안 솔루션·서비스 활용 및 내부 임직원 보안 교육 실시 △관리자 계정에 대한 인증 이력 모니터링 △멀티팩터인증(Multi-Factor Authentication) 도입 등 예방 대응책을 마련해야 한다.

개인은 △출처가 불분명한 메일 속 첨부파일·URL 실행 자제 △공식 경로를 통한 콘텐츠·SW 다운로드 △SW·운영체제·인터넷 브라우저에 최신 보안 패치 적용 △ 로그인 시 이중 인증 사용 △백신 최신 버전 유지 및 실시간 감시 기능 실행과 같은 보안 수칙을 철저히 지켜야 한다.