보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

2021년 보안 위협, 변화에 '민감하게 반응했다'

AhnLab 2021-12-06

지난해 말, 안랩은 2021년 보안 위협 전망 Top 5로 ▲타깃형 랜섬웨어 확대 및 고도화 ▲코로나19가 바꿔놓은 업무 환경, 그리고 보안 위협 ▲악성코드 제작 언어 다양화 ▲악성코드 동작 방식 모듈화 ▲악성앱의 공격 대상 국가 확대 등을 제시한 바 있다. 1년이 지난 현 시점에서 2021 년을 정리하며 어떠한 보안 위협이 실제 이슈가 되었는지 살펴본다.

최근 몇 년간 대세를 굳혀온 랜섬웨어, 국가 지원 해킹 조직, 모바일 악성앱 등이 2021년에도 여전히 기승을 부렸다. 달라진 점이 있다면 새로운 이슈와 새로운 인프라에 더 '빠르고, 민감하게' 반응했다는 점이다. 사회적인 이슈가 발생하면 공격 경로와 대상 플랫폼에 상관없이 곧바로 이를 악용한 사회공학적 공격이 감행되었다. 2021년의 주요 보안 위협들을 다섯 가지로 요약하면 ▲국가 지원 해킹 조직의 활동과 피해 지속 ▲ 타깃형 랜섬웨어 공격과 피해 규모 증가 ▲ 업그레드된 문서형 악성코드 다수 유포 ▲ 사회적 이슈를 활용한 사회공학적 공격 활동 ▲ 금융 모바일 악성 앱의 지속적인 변화 시도 등이 있다.

1. 국가 지원 해킹 조직의 활동과 피해 지속

여러 해킹 조직은 자국의 이익을 위해 국내외 기업, 정부 기관, 교육 기관 등을 대상으로 해킹을 시도해왔다. 2020년에는 국가 지원을 받는 해킹 조직은 코로나 19 백신을 개발하는 제약 회사를 타깃으로 해킹 시도를 집중했다. 2021년에는 의료, 방산, 연구 기관, 정치, 안보 등 다양한 분야를 대상을 확대했다. 특히 연구 기관, 의료, 방산 분야에서는 해킹으로 인해 자료 유출 사고가 발생한 것으로 알려졌다. 이들 국가 지원 해킹 조직은 VPN(Virtual Private Network), 통합 관리 등 기업에 특화된 솔루션의 취약점을 악용해 해킹을 수행했다.

이러한 해킹의 대부분은 메일에서 시작됐으며, 포털을 사칭한 피싱, 악성 스크립트, 악성 매크로가 포함된 오피스 문서 첨부 등이 주를 이뤘다. 일부 사례에서는 Adobe PDF 취약점(CVE-2020-9715), MS Office 취약점(CVE-2021-40444)을 악용한 사례도 보고됐다. 국가 지원을 받는 해킹 조직이 사용한 MS Office 취약점(CVE-2021-40444)은 범용적으로 사용 되었으며, 대표적인 악성코드로는 매그니베르 랜섬웨어를 들 수 있다.

2. 타깃형 랜섬웨어 공격과 피해 규모 증가

악성코드 관점에서는 역시 랜섬웨어가 모든 이슈를 선점했다. 2021년에도 국내외 상관없이 랜섬웨어 공격 건수와 이로 인한 피해액이 크게 증가했다. 특히 단순 개인 PC 공격보다 기업을 표적으로 하는 타깃형 공격이 확대되었다. 미국의 송유관 기업 콜로니얼 파이프라인과 소프트웨어 기업 카세야의 공급망을 악용한 랜섬웨어 공격은 올해 발생한 대형 보안 사고였다. 미국 재무부는 2021년 상반기에 발생한 랜섬웨어 공격 피해액(약 7천억 원)이 2020년 전체 피해액(약 5천억 원)보다도 증가했다고 발표했다.

국내에서도 대기업과 대학병원을 포함해 많은 기업들이 랜섬웨어 공격을 받았다. 2021년 안랩에 접수된 랜섬웨어 공격 사례를 살펴 보면 취약점을 이용한 메그니베르 랜섬웨어부터 이메일에 첨부된 미끼 파일을 이용한 랜섬웨어까지 종류와 유포 방식이 매우 다양했음을 알 수 있다. 이러한 기업 타깃형 랜섬웨어 공격 양상은 2022년에도 지속될 것으로 예상된다.

한편, 법집행기관의 노력으로 랜섬웨어 제작자들을 검거하고 기존 랜섬웨어 그룹 중 활동 중단을 선언하기도 했다. 1월 넷워커(NetWalker) 랜섬웨어, 2월 에그레고르(Egregor) 랜섬웨어, 6월 클롭(Clop) 랜섬웨어, 10월 록커고가(LockerGoga), 메가코텍스(MegaCortex), 다르마(Dharma) 랜섬웨어와 관계된 용의자가 검거 되었다. 하지만, 활동 중단을 선언을 중단한 일부 그룹은 또 다른 이름으로 활동을 이어나가는 경우가 있어, 추적을 피하기 위한 방편으로 해석할 수도 있다.

3. 업그레드된 문서형 악성코드 다수 유포

2021년 한해 동안 기존의 방식에서 업그레이드된 형태의 문서형 악성코드들이 지속 유포되었다. 대표적인 문서 형태는 워드, 엑셀, 파워포인트, PDF로 타깃형과 비타깃형을 막론하고 케이스 별 유포 목적은 다양했다.

피싱의 형태로 메일로 유포되는 경우가 많았으며 특정인을 노린 듯 문서의 내용에 특정 주제를 담아 사용자가 의심없이 실행할 수 있도록 의도한 경우와 불특정 다수에게 유포할 목적으로 매크로 실행 유도를 포함한 문서들이 있었다. 최종적으로 이런 문서들은 사용자 정보를 유출하는 유형의 형태가 많았다. 그 예로는 ▲뱅킹형 정보 탈취 악성코드인 트릭봇(Trickbot), 드라이덱스(Dridex) ▲웹 브라우저, FPT 클라이언트, 메신저 및 암호화폐 지갑에서 데이터를 훔치는 KPOT ▲웹 브라우저, 메일 및 FTP 클라이언트 등에 저장된 사용자 정보를 유출하는 에이전트테슬라(AgentTesla) 등이 있다. 이러한 정보 유출 형태가 아닌 최종적으로 연결된 C&C 서버의 공격자로부터 추가적인 명령을 받을 수 있도록 백도어 혹은 RAT류의 악성코드 감염을 목적으로 했던 케이스도 존재했다.

해당 류들의 문서형 악성코드는 파일 진단과 행위 진단의 우회를 위하여 악성 매크로 코드의 난독화 복잡성을 높이거나 실행 프로세스 상의 단계를 증가시켜 탐지를 피하기 위한 형태로 지속 변화 중이다.

4. 사회적 이슈를 활용한 사회공학적 공격 활동

2021년에는 다양한 사회적 이슈를 키워드로 한 사이버 공격이 꾸준히 발견되었다. 공격에 사용된 주요 이슈는 코로나19 상황과 관련 이슈, 북한 관련 정치 사회적 이슈, 주식 관련 경제적 이슈 등이다.

대다수의 국민들에게 관심이 높은 코로나 확진자 동선, 재난지원금, 소상공인 지원 종합 안내 등의 키워드를 악용한 공격이 감행되었다. 또한 북미정상회담, 중국의 군사전략 분석, 안보 세미나, 남북교류 등 북한 관련 키워드도 역시 유효한 공격 키워드였다. 특히 암호화폐와 주식 시장 상승, 거래 비대면화, 각종 사이버 자산의 출현 등으로 인한 경제적인 이슈를 겨냥한 사이버 공격도 뒤따랐다. 이외에도 넷플릭스를 통해 전 세계적인 인기를 끌고 있는 오징어 게임, 전직 대통령 조문 등의 이슈도 공격자에게 악용되었다.

이러한 사회공학적 공격은 기술적인 공격 방법이 아니라 사람의 심리를 이용한 공격이므로 사용자의 부주의와 실수에 의존하고 있음을 기억해야 한다. 따라서 문자메시지나 메일 속 출처가 불분명한 URL 주소의 연결을 금지하고, 주요 뉴스 기사 및 정보검색 시에는 널리 검증 받은 웹 사이트나 서비스 플랫폼을 이용하는 것이 바람직하다.

5. 금융 모바일 악성 앱의 지속적인 변화 시도

금융 모바일 악성 앱이 공격 대상 및 악성 앱 제작에도 변화를 주었다. 국내 사용자를 대상으로 하는 대표적인 금융 악성 앱인 카이시(Trojan/Android.Kaishi)는 2014년부터 등장 했지만, 최근 들어 앱 제작 방식을 변화하고 공격 대상을 정밀하게 관리하며 피해를 가중시켰다. 보이스 피싱에 악용되는 앱으로 통화를 조작하는 핵심 기능은 유지하지만 코드 난독화, 패킹, 암호화 등 앱 보안 기술을 적용하는 형태가 발견되고 기존과 전혀 다른 구조를 보이기도 했다. 탐지를 회피하며 공격 성공률을 높이려는 움직임으로 해석된다.

일반적으로 금융 악성 앱은 뱅킹 애플리케이션을 공격 대상으로 하게 되나, 최근 해외에서 보고된 금융 악성 앱의 대부분은 암호 화폐 관련 앱과 함께 쇼핑 앱 등 온라인 금융 서비스가 포함된 앱들도 대상으로 삼고 있음을 확인할 수 있었다. 이들 악성 앱은 암호 화폐 서비스의 사용자 계정을 탈취하거나, 인증 키를 탈취하도록 제작 되었다. 실제 정보 탈취에 따른 금전적 피해 사례가 등장하고 있어, 핀테크 서비스 증가 및 확장에 따른 모바일 악성 앱의 새로운 형태들이 등장하는 것에도 주목할 필요가 있다.

AhnLab ASEC 대응팀 박태환 부장