보안 위협 동향

2020년 결산

2021년 전망

AhnLab

2020년
보안 위협 동향

2020년 보안 위협 동향 결산 **Top 5**

AhnLab

01
랜섬웨어: 이미 익숙해진 공격, 피해는 여전히 심각

랜섬웨어는 몇 년 전부터 보안 위협 결산과 내년도 예측에 빠지지 않고 등장해왔다. 이미 광범위하게 유포되어 사람들이 익숙하게 느끼는 단계에 이르렀지만, 그 피해는 여전히 심각하다. 2020년에는 파일 암호화 전, 내부 정보를 먼저 탈취한 뒤 외부에 공개하겠다는 형태로 '이중 압박'을 가하는 타깃 랜섬웨어 그룹의 확대가 특히 눈에 띄었다. 지난해, 전 세계적으로 주목할만한 랜섬웨어 피해 사례 두 가지는 아래와 같다.

A. 전 세계적인 공격 감행, 메이즈 랜섬웨어

첫 번째로, 메이즈 랜섬웨어(Maze Ransomware)는 전 세계 기업을 대상으로 표적 공격을 수행했다. 공격 조직은 기업의 내부 데이터를 탈취한 후 금전을 요구하며 협박했고, 피해 기업이 응하지 않을 경우 자신의 웹사이트에 탈취한 데이터를 공개했다. 그리고 2020년 11월 초, 은퇴를 선언하면서 자료 삭제 조건으로 기한 내에 본인들에게 연락할 것을 요구했다.

B. 환자의 생명을 앗아간 도플페이머 랜섬웨어

2020년 9월, 독일 뒤셀도르프 대학병원이 랜섬웨어 공격을 받아 의료 시스템이 마비되어, 응급 환자가 사망하는 사건이 발생했다. 병원 서버 30대가 랜섬웨어에 감염되면서 대다수의 의료 서비스 제공이 불가능해졌고, 치료가 지연되면서 응급 환자가 사망하게 된 것이다. 이후, 독일 수사기관은 병원을 공격한 랜섬웨어가 '도플페이머(DoppelPaymer)' 랜섬웨어라고 밝혔다. 공격 조직이 환자 사망을 의도한 것은 아닐지라도, 주요 인프라가 랜섬웨어 등 악성코드에 감염될 경우 자칫 생명을 위협할 수 있음을 시사한 사건이었다.

02
국가 지원 해킹 조직의 **전방위적 공격**

여러 해킹 조직이 작년에도 자국의 이익을 위해 국내외 기업, 정부 기관, 대학교, 개인 등을 대상으로 해킹 시도했다. 일부 기업은 직원의 계정 정보와 내부 자료가 유출됐으며, 개인의 경우, 보유하고 있는 코인을 탈취 당하기도 했다.

코로나19는 국가 지원 해킹 조직의 동향에서 반드시 언급되어야 할 키워드다. 전 세계적으로 코로나 감염자가 폭증하고 다국적 제약 회사들이 앞다퉈 코로나 백신을 개발하고 있는 상황에서, 여러 해킹 조직이 정부 기관 및 제약 회사를 상대로 공격을 시도했다.

유럽의약품청(European Medicines Agency: EMA)은 보관하고 있는 코로나19 백신 관련 문서 탈취를 노리는 해커들의 표적이 되어 왔다. 또한, 특정 국가들의 체계적인 지원을 받는 것으로 의심되는 공격 조직들이 코로나19 백신 기술, 연구 결과, 콜드체인(저온 유통체계)에 불법적으로 접근한 사례들이 계속해서 보고되고 있다.

그동안 지속적으로 글로벌 해킹 조직들의 표적이 되어왔던 한글 문서 취약점은 전년도에 비해 감소했다. 그 이유는 공격자들이 활용했던 한글 문서 내 고스트 스크립트 취약점이 한글 프로그램의 보안 업데이트로 제거됐고, 시간이 지나면서 사용자의 한글 보안 업데이트 설치가 확대되어 더 이상 공격이 효과를 보는 것이 어렵다고 판단한 것으로 추정된다. 다만, 대체 공격 방안으로, 매크로(Macro), 파워쉘(PowerShell), WSF, VBS 등의 스크립트 악성코드 사용이 확대됐다.

03
더 정교해진 **피싱 공격**

작년에 발견된 피싱(Phishing) 유형 악성코드는 사용자가 쉽게 속을 정도로 교묘하게 진화했다. 정상적인 포털사이트를 가장한 악성 웹페이지는 로그인 화면을 정상 사이트처럼 유사하게 만들어 사용자를 속이고 계정 정보 탈취를 시도했다. 과거에는 화면 구성이 다소 어색했던 반면, 현재는 전문가들조차 구분이 쉽지 않을 정도로 정교해졌다. 이러한 피싱형 악성 웹페이지는 사용자가 계정 정보를 입력하면 서버로 정보를 전송한 후, 정상 사이트로 리다이렉트(redirect) 하여 사용자가 의심조차 하지 못하게 한다.

이메일 역시 마찬가지다. 주로 '시스템 점검 안내', '계정 접근 제한', '발주서' 등의 업무 관련 내용으로 사용자가 큰 의심 없이 악성 링크나 메일 내 악성 첨부파일을 실행하도록 했다.
과거에는 불특정 다수를 대상으로 유포되는 영문 스팸 메일 많았다면 최근에는 한글로 작성되고 사용자 맞춤형 내용으로 작성된 내용이 많이 발견되었다. 악성코드 제작자들이 공격 성공률을 높이기 위해 더 정교한 피싱형 악성코드를 제작해 유포하고 있음을 알 수 있다.

04
봇넷 악성코드
글로벌 대량 유포

이모텟(Emotet)으로 대표되는 봇넷 악성코드가 전 세계적으로 대량 유포되었다. 봇넷 악성코드는 많은 사용자를 감염시킨 뒤 공격자의 명령에 따라 동작하는 악성코드로 사용자 정보 유출, 추가 악성 파일 다운로드 등의 기능을 수행한다.

이모텟 악성코드는 금융 정보유출형 악성코드로 시작했지만, 점차 진화하여 트릭봇(TrickBot), 큐봇(QBot) 등 추가적인 금융 정보유출형 악성코드를 다운로드해 실행하는 형태로 바뀌었다. 2020년 확인된 대부분의 봇넷 악성코드는 악성 이메일을 통해 유포됐다. 이메일 첨부 문서 파일에 삽입된 매크로를 실행하면 악성 파일을 다운로드하는 구조로 동작했다.

봇넷 악성코드는 빌더(Builder)를 통해 제작되는 경우가 많아, 첨부 문서 파일과 실행 파일 외형 변경이 몇 시간 단위로 매우 빠르게 진행됐다. 또한 공격자의 명령을 받아야 이후 기능이 동작하기 때문에 악성코드의 최종 목적을 파악하기가 어렵고, 동작 시간대마다 사용자 별 피해 현황이 달라지는 특징도 있었다.

05
구글 플레이 등 공급망을 통한 **악성앱 전파 증가**

2020년에는 구글 플레이(Google Play)를 통해 전파된 악성앱의 유형과 수가 크게 증가했다. 이렇게 배포된 악성앱은 주로 금융정보 탈취, 구독 서비스 가입, 광고 유포 등의 기능을 하는 것으로 확인됐다.

WAP(Wireless Application Protocol) 과금 서비스를 이용하는 국가에서 사용자 모르게 유료 과금 서비스에 가입하는 'Trojan/Android.Joker'는 2020년 최초 확인된 이후 문서 스캐너나 포토 에디터 등으로 위장하여, 구글 플레이를 통해 꾸준히 배포되는 것으로 나타났다. 악성코드 제작자가 소스코드를 공개한 케르베르스(Cerberus)라는 악성앱 역시 구글 플레이를 통해 지속적으로 유포됐다.

광고를 노출하는 유형의 악성앱은 먼저 게임이나 기타 사용자에게 유용한 기능을 제공한다. 그리고 많은 사용자를 모은 뒤, 공격자 서버(C2)에서 전달받은 명령에 따라 일제히 공격적인 광고를 노출시켰다. 이처럼 구글 플레이를 통해 전파된 악성앱은 악의적인 기능이 동작하기까지 일정 기간 대기(잠복)하기 때문에 많은 피해자를 발생시키는 특징이 있다.

2021년 보안 위협 전망

2021년 보안 위협 전망 **Top 5**

AhnLab

01
타깃형 랜섬웨어 확대 및 고도화

그간 활발히 유포되었던 메이즈 랜섬웨어가 2020년 11월 초 은퇴를 선언했다. 하지만, 수많은 랜섬웨어 중 하나가 사라졌을 뿐, 그 빈자리는 분명히 다른 랜섬웨어가 대체할 것이고 피해도 지속될 것으로 예상된다. 특히, 타깃 랜섬웨어 그룹들은 상호 연대를 통해 그 외연을 확장하고 공격을 고도화시켜 나갈 가능성이 높다. 사이버 범죄 조직에게 랜섬웨어는 핵심 돈벌이 수단이기 때문이다.

오늘날 기업들은 자원 관리의 편의성과 효율성 제고를 위해 다양한 소프트웨어를 사용한다. 하지만, 소프트웨어에 취약점이 존재할 경우, 공격자가 이를 악용해 기업의 내부를 장악하고 악의적인 행위를 수행할 수 있는 환경을 만들어 주게 된다. 공격자들은 침투, 장악, 탈취 등 단계 별 공격을 효과적으로 성공시키기 위해 계속해서 그 방법을 고도화 시키고 있다.

과거 언론을 통해 알려진 국내 해킹 사고를 보면, 해커들이 기업용 소프트웨어의 취약점을 사용한 사례들도 존재한다. 랜섬웨어 공격 역시 충분히 가능한 시나리오이며, 2021년에는 보다 고도화된, 그리고 활발한 랜섬웨어 유포를 예측해 볼 수 있다.

또한, 사례들과 같이 랜섬웨어는 언제 어디서든 우리나라 기업들을 공격하고 자칫 사람의 생명을 위협할 수도 있다. 이에 대비할 수 있는 보안 시스템 강화, 보안 수칙 준수 및 인식 개선이 필요하다.

02
코로나19가 바꿔 놓은 업무 환경, 그리고 보안 위협

코로나19가 발병한지 어느덧 1년이 지났다. 지난 2020년, 우리는 코로나19로 인해 생활 패턴에 큰 변화를 겪었다. 예를 들면, 온라인 구매와 배달 서비스 사용이 급격히 증가했고, 비즈니스도 장소의 제한 없이 원격으로 수행하는 '언택트(비대면)' 도입이 크게 늘었다.

비대면 업무 환경에서는 기업의 보안 정책에 의해 보호받을 때와는 달리, 구성원 개개인이 주체가 되어 보안에 신경을 써야 하지만 비용, 인력 등의 이유로 쉽지 않은 것이 사실이다. 보안 측면에서 코로나19는 기업에게 새로운 도전 과제이며, 동시에 공격자에게는 기회일 수 있다. 2021년에는 비대면 업무 환경을 노린 피싱, 표적 공격 등 해킹 시도가 계속해서 발생할 것으로 예상된다.

이에, 기업들은 언택트 환경에서의 보안을 권장이 아닌 필수로 인식하고 해당 환경에서 보안의 우선순위를 명확히 설정할 필요가 있다. 또한, VPN(Virtual Private Network) 사용 시 올바른 정책 설정과 사용자 검증 강화가 필요하며, 별도의 보안 전문 인력 없이도 안전한 업무 환경을 효율적으로 조성할 수 있는 SaaS(Software as a Service)형 보안 솔루션 도입도 고려해볼만 하다.

03
악성코드 제작 언어 **다양화**

2021년에는 EXE, DLL 등 실행 파일 악성코드 제작 방식이 더 다양해질 것으로 보인다. 과거부터 현재까지 상당수의 PE(Portable Executable) 파일들이 C, C++, Visual Basic, Delphi, C# 등의 언어로 제작되고 있지만, 최근 들어 파이썬(Python)이나 고(GoLang) 언어로 제작된 악성코드도 여럿 등장하고 있다.

공격자들은 간편한 컴파일과 바이너리 생성이 가능하고 추가적인 라이브러리나 모듈의 추가가 비교적 쉬운 장점을 십분 활용하는 것으로 보인다. 또한 기존의 안티바이러스 제품의 시그니처 패턴과는 완전히 다른 형태와 구조를 가진 파일이기 때문에 공격자들은 이 점을 노려 악성코드를 제작할 것으로 예상된다.

04
악성코드 동작 방식 **모듈화**

악성코드 동작 방식은 이미 모듈화되고 있다. 한 개의 파일이 공격자 C2 서버 통신, 다운로드, 정보 유출, 파일 생성 등을 모두 하는 것이 아닌 그 기능을 여러 개의 파일로 나눠 동작하는 것이다. 이는 안티바이러스 탐지를 최대한 우회하는 것뿐 아니라 악성 기능을 더 오래 지속하기 위한 목적도 있다. 예를 들면, 공격자 서버에서 인코딩 된 파일을 다운받은 뒤 이를 디코딩하는 파일이 별개로 있을 경우, 단일 파일 정보만 봐서는 정확한 기능과 악성 행위의 흐름을 파악하는 것이 쉽지 않다.

2021년에는 이처럼 모듈화된 악성코드가 더 많아질 것으로 예상된다. 특히, 사용자가 악성 서버에 접속해 파일을 다운로드 받도록 유도하고 심어 놓은 파일을 지속적으로 교체하는 형태로 피해를 가할 것으로 예상된다.

05
악성앱의 공격 대상 국가 확대 **가속화**

모바일 단말기를 대상으로 하는 악성앱은 언어 및 문화적 차이와 결제 시스템의 다양성 등의 이유로 주로 단일 국가만에서만 공격이 효과적으로 이뤄지는 경향이 있다. 국내 스마트폰 사용자를 공격하는 피싱앱(Dropper/Android.PhishingApp)은 택배, 청첩장, 코로나19와 같은 사회적 이슈 관련 피싱 메시지를 통해 전파되었다. 이 악성앱은 사용자의 스마트폰에 저장된 정보를 유출하고 보이스 피싱과 연계해 금전 갈취에 활용되었다.

2020년에는 동일한 제작자가 수행한 것으로 보이는 악성앱 배포 사례가 다양한 국가에서 확인되었다. 공격자는 각 국가의 대표적인 택배 업체를 가장하는 수법을 사용했다. 또한, 넷플릭스와 디즈니 등 유명 콘텐츠 공급자나 인지도 높은 게임 등을 사칭해 전파하고 브라우저 알림 광고를 구독하게 하는 형태의 악성코드도 확인되었다.

이와 같은 악성코드는 광고 제공 업체에서 단말기가 동작하는 국가별 언어에 대한 광고를 제공해 주기 때문에 여러 국가의 사용자를 대상으로 전파될 수 있었다. 과거, 제한된 수익성을 이유로 국지적으로 동작했던 악성앱이 이제 여러 나라의 스마트폰 이용자를 공격 대상으로 삼기 시작했으며 이러한 경향은 점점 가속화될 전망이다.

보안 위협 동향

2020년 결산
2021년 전망

발 행 처 주식회사 안랩

집 필 안랩 시큐리티대응센터(ASEC)

편 집 안랩 콘텐츠기획팀

경기도 성남시 분당구 판교역로 220 | T. 031-722-8000 | F. 031-722-8901

A AhnLab.com B ASEC Blog F 보안정보 Facebook T 보안정보 Twitter

AhnLab