SPECIAL REPORT

MIDYEAR THREAT REVIEW

2020 상반기 보안 위협 동향

상반기 장악한 보안 위협 Top 5 … 코로나19 영향 컸다

도쿄 올림픽 시즌을 전후로 국가적 사이버 보안 위협이 등장할 것이라고 전망하며 시작했던 2020년. 그러나 그 어느 누구도 예측하지 못한 생체 바이러스인 '코로나 바이러스 감염증 19(COVID-19, 이하 코로나19)'의 등장으로 인해 전세계가 급격한 변화를 맞이했다. 이 감염증은 우리 생활의 모든 것들을 송두리째 바꿔 놓았다고 해도 과언이 아니다. 황사와 미세먼지를 피하기 위해 사용하던 마스크가 매일 매 순간 착용해야 하는 필수 도구가 되었다. 대외 활동 시에는 상대방과 마주 앉아 식사를 하거나, 대화를 하는 것을 최소화하는 사회적 거리 두기와 생활 속 거리 두기를 실천해야만 건강을 보존할 수 있는 시대에 살게 된 것이다. 원격 수업과 원격 근무를 통한 비대면, 비접촉은 일상이 되어 버렸고, 이로 인한 생활의 변화는 불가피해졌다. 사회적 거리 두기와 생활 속 거리 두기의 실천이 사회 여러 부분에서 불편의 요소들로 작용하고 있지만, 서로의 건강을 지키기 위해 불편을 감내하는 기간이기도 했다. 우리의 일상이 불편해진 만큼, 사이버 공간에서의 우리의 생활은 어땠을까.

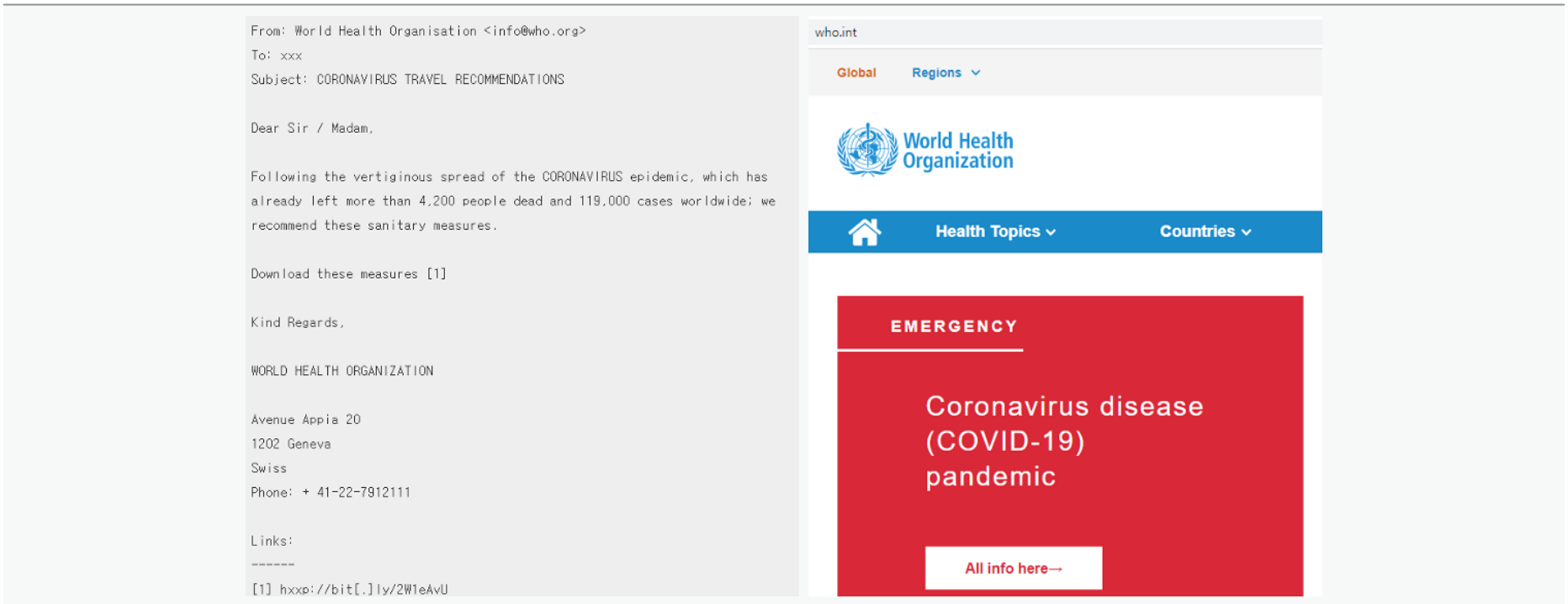
이 글에서는 코로나19로 급격한 변화를 맞이한 2020년 상반기 IT 보안에 있어서 어떤 위협들이 이슈가 되었는지 살펴본다.

1. 코로나19 정보로 위장한 사이버 공격

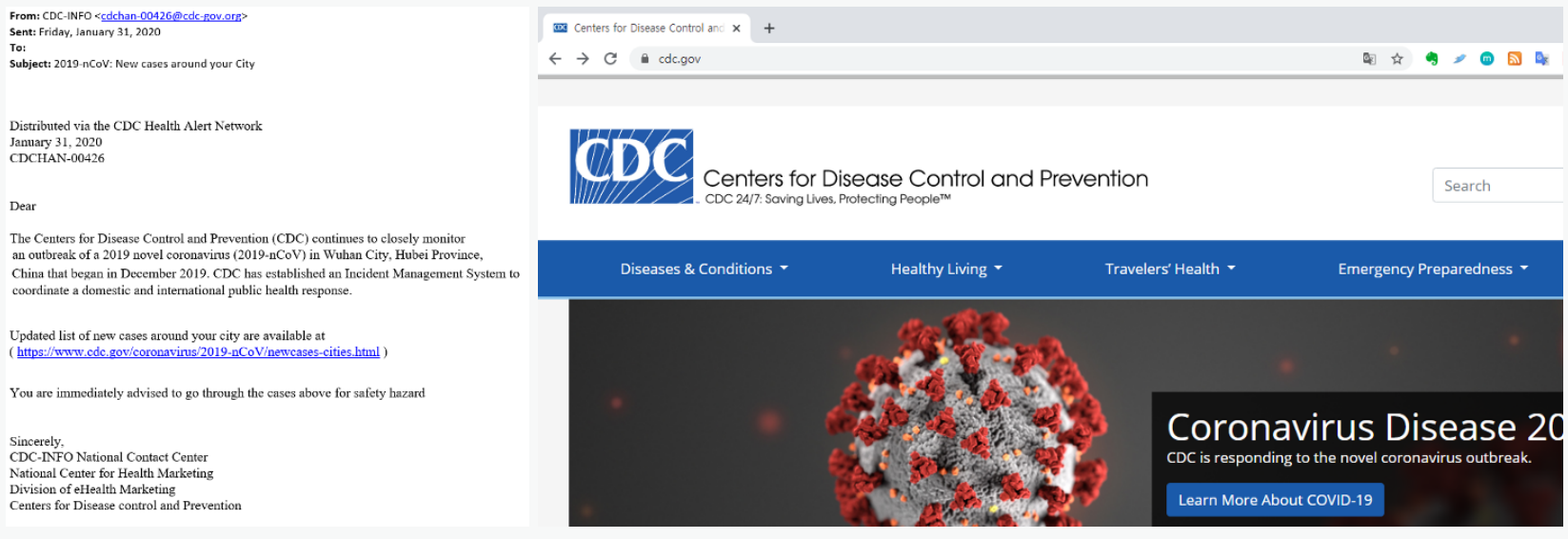
세계보건기구(The World Health Organization, 이하 WHO)는 2020년 3월 12일, 코로나19가 전염병 경고 6단계 팬데믹(Pandemic)임을 공식 선언했다. 덧붙여 공중 보건의 영역을 넘어 사회, 경제를 포함한 모든 영역에 악영향을 끼칠 수 있는 혼란의 시기를 개인과 국가들이 이 위협에 맞서 적극적으로 싸워 줄 것을 촉구했다. 이 혼란의 시기를 틈 타 사이버 공격 세력들은 교묘하게 우리 주변을 파고 들었다. 그 중 가장 대표적인 사이버

위협이 바로 코로나19 정보로 위장한 사이버 공격이다. 코로나19 관련 정보를 담고 있는 것으로 위장한 이메일 악성코드는, 이메일 발신자 주소를 세계보건기구(WHO) 혹은 미국 질병통제예방센터(CDC)와 유사하게 기록하여 메일 수신자의 눈을 속였다.

사실 세계보건기구나 질병통제예방센터의 정확한 URL을 인지하고 있는 이는 그리 많지 않을 것인 관계로, 공격자들이 유사하게 만들어 낸 URL 및 이메일 주소를 보고, 사이버 공격임을 눈치 채거나 의심하는 일은 거의 없었을 것으로 추정된다. [그림 1]의 WHO 위장 메일은 발신자의 메일 주소가 who.org로 사용하였으나, 실제 존재하는 WHO 공식 홈페이지의 주소는 who.int인 것을 알 수 있다. 정상적인 홈페이지 주소가 되려 비정상적인 이메일 주소보다 조금 더 가짜 주소인 것 같은 느낌을 받는다 해도, 결코 이상하지 않을 정도이다.



[그림 1] 세계보건기구(WHO) 메일 주소로 위장한 이메일과 홈페이지 주소



[그림 2] 미국 질병통제예방센터(CDC) 주소로 위장한 이메일

2. 스미싱과 보이스피싱

개인 휴대기기인 스마트폰에 대한 스미싱 공격(Smishing Attack)과 사용자를 속여 금전적 피해를 입히는 보이스피싱 공격(Voice Phishing Attack)이 지속적으로 증가하고 있다. 설날, 추석, 성탄절 등 지인들에게 안부를 전해야 하는 시즌이나 택배 물량이 넘치게 되는 시즌을 즈음하여 유행하게 되는 것이 문자 메시지를 통해 전파되는 모바일 악성코드인 스미싱이다. 그러나 라이프스타일의 변화에 따라 특수한 시즌에만 이용하는 것이 아니라 일상에서도 온라인 쇼핑몰을 통한 주문이 일반화된 요즘, 배송 상황을 알려주는 다양한 문자 메시지 수신은 꽤나 자연스러운 일 중의 하나가 되었다. 특히 코로나19의 여파로 오프라인 활동을 제대로 할 수 없어 온라인 배송 요청이 폭증하게 되는 이 시기를 틈타 스마트폰 이용자를 타깃으로 하는 스미싱 공격이 증가했다.

가장 쉽게는 택배 배송 안내 문자 메시지로 위장하여 사용자의 접속을 유도했다. 과거 스미싱 공격 그룹들은 스마트폰 문자 메시지를 단축 URL로 구성해 스마트폰 이용자의 의심을 최소화 한 후, URL 접속을 유도했다. 문자 메시지의 단축 URL을 누르게 되면, 공격자들이 사전에 제작해 둔 안드로이드 스마트폰 앱의 확장자인 APK 파일을 다운로드하게 된다. 안드로이드 스마트폰 앱의 정식 유통 창구인 구글 플레이스토어를 거치지 않고 직접 악성 APK 파일을 설치하도록 유도했었으나, 지난 해부터 왕성한 활동을 하고 있는 스미싱 공격 그룹들은 자신들의 공격 대상자로부터의 앱 다운로드 시도를 구분하는 목적의 로직을 추가하는 치밀함을 보였다. 자신들이 만든 악성 앱 다운로드용 페이지를 스마트폰에서 접속했는지 PC에서 접속했는지 1차적으로 확인한다. 이어 자신들이 확보한 스마트폰 번호인지 2차적으로 검증한 후 악성 앱을 다운로드하게 한다. 이는 자신들이 의도하지 않는 곳에 자신들의 앱이 노출되는 것을 최소화하기 위한 것으로 짐작된다. 이 과정을 통해, 악성 앱 다운로드 URL이 악성코드 분석가나 보안 업체에 노출된다 하더라도 공격자들이 만든 피싱 페이지가 아닌 정상 택배 회사의 웹 페이지가 열리고, 악성 APK 파일을 다운로드할 수 없어 아무런 방해를 받지 않은 채 공격을 수행할 수 있게 되었다. 이러한 스미싱 앱에는 일반적인 안드로이드 스마트폰 앱에 부여되는 권한보다 더 과도한 권한이 부여된다. 이것은 스미싱 앱을 통해 스마트폰 내부에 존재하는 사용자 정보를 수집하겠다는 의도를 가지고 있음을 드러내는 부분이다.

코로나19 상황을 효과적으로 극복하기 위해 정부가 실시한 '정부 긴급재난지원금'에 대한 내용을 악용하여 '정부 긴급 재난지원 대출 안내'를 빙자했다. KB국민지원, 우리금융지원 등 제도권 은행의 상호를 사칭하거나 서민금융진흥원, 국민행복기금 등 공공기관 상품인 것처럼 사칭하여 이용자들이 공신력 있는 기관에서 발송한 문자 메시지로 오인하도록 유도하였다. 여기에 더하여 선착순 지급, 한도 소진 임박 등의 자극적인 표현으로 긴급 자금이 필요한 이들의 불안한 심리를 악용하는 유형까지 확인되었다. 이런 피해를 입지 않기 위해서라도 문자 메시지와 스마트폰 앱을 이용한 악의적인 공격들을 잘 알고 있어야 한다.

3. 기반시설 타깃 사이버 공격

사이버 영역에서 전략적 우위를 점하기 위한 노력은 끊임없이 시도되고 있다. 특히 국가의 주요 기반시설에 타깃 공격을 통해 기반시설의 내부를 장악하고, 추후 자신들의 목적에 맞게 활용하려는 시도들을 확인할 수 있었다. 국내 특정단체 소속의 실제 직원 이름을 사용한 발신자로부터 관련 직책자들만을 수신자로 제한한 후, 문서 파일로 위장한 악성코드가 첨부된 타깃 메일을 발송하는 스피어 피싱 공격도 발견되었다.

Microsoft 워드 문서로 만들어진 이 악성코드는 내부 매크로 파일을 통해 악의적인 동작을 수행한다. 따라서 사용자가 최초로 문서를 여는 순간 보안 경고창을 통해 '매크로 실행 여부' 선택 메뉴를 보여 주도록 되어 있다. 해당 단체의 직원 리스트를 보면 발신자가 실제 근무자의 이름인 것을 알 수 있었다. 공격자가 공격에 유리하도록 사전에 정보를 수집하고, 이를 적재적소에 활용하는 치밀함을 보여 준 사례라 할 수 있다. 이메일에 첨부된 문서 파일을 열게 되면 실제 코로나19 관련 내용이 펼쳐지게 되므로, 의심할 만한 부분을 발견하기는 어려우나 해당 문서는 보안 취약점을 통해 공격자가 의도한 악성코드를 설치하도록 만들어진 상태였다. 설치된 악성코드의 목적에 따라, 해당 문서를 열람한 사용자 PC 내부에 저장 중이던 주요 정보를 수집 및 유출하도록 동작한다.

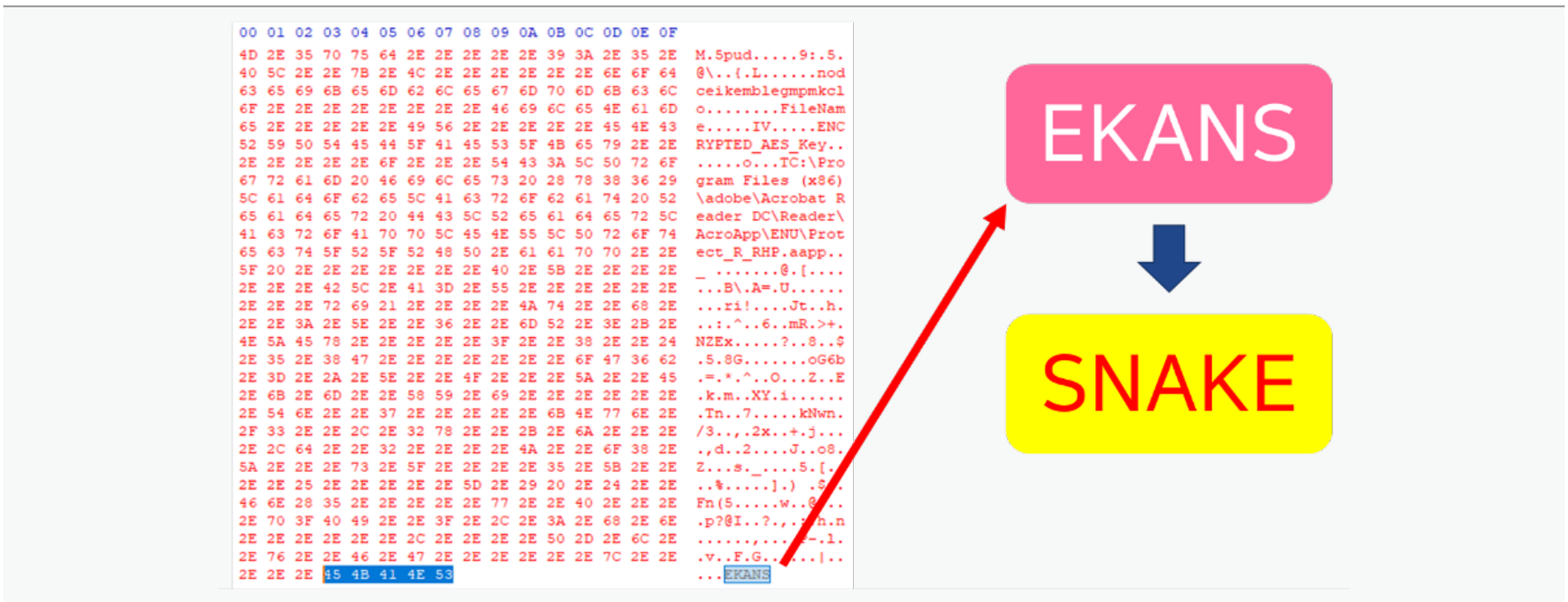
코로나19의 국내 대규모 확진자가 등장하기 시작한 시기에 주목받은 '신천지' 관련 자료로 위장된 문서 파일이 등장하여, 사용자들의 문서 열람을 유도했던 사례도 있었다. 문서는 두 종류의 내용을 담고 있어 사용자들의 의심을 교묘히 피할 수 있는 구조였다. 문서를 열어보게 될 경우에는 레지스트리 키 등록을 통해 PC 재부팅 후에도 공격자가 의도한 백도어가 지속적으로 동작하여 프로세스 목록, 컴퓨터 이름, OS 버전 정보 전송과 파일 실행 및 종료, 추가 파일 다운로드가 진행되어 주요 정보 수집 및 유출이 가능함을 알 수 있었다. 코로나 마스크 관련 중국 내 상황을 브리핑하는 내용의 타깃 이메일이 국내 특정 기업에 유입된 사례 또한 확인되었다. 첨부된 압축 파일을 열고 실행하게 되면 PC 내부 주요 정보 수집 및 유출을 수행하는 원격 명령 수행 악성코드인 나노코어(NanoCore) RAT가 설치 및 동작하게 된다. 2013년 처음 발견된 나노코어 RAT는 PC에서 데이터를 수집하여 공격자에게 전달하는 키로거와 같은 다양한 기능을 가지고 있었다. 원격에서 PC를 켜거나 끄는 것에서부터 파일을 실행하고, 키보드 입력값을 기록하는 것은 물론 컴퓨터를 쓰지 못하도록 잠그거나 웹캠을 통한 녹화까지도 가능한 것이 바로 나노코어 RAT이다. 앞에서 설명한 타깃 공격들은 모두 국가 주도의 사이버 공격 집단 및 그들과 이념을 같이하는 조직들에 의해 진행된 것으로, 특별히 국내 기간산업 및 방위산업체를 타깃으로 진행된 공격이었다.

이들 공격 그룹이 노리는 것은 기본적인 보안 체계의 붕괴를 통한 내부 접근과 인프라 장악 및 주요 기밀 정보 수집과 유출이며, 결정적으로는 '핵심 기술의 유출'과 '정찰을 통한 대비책 수립'을 목표로 하고 있다.

우리가 이미 과거의 수많은 타깃 공격 사례를 통해 학습하고 있는 바와 같이, 파괴를 통한 무기 체계 무력화 및 사회 기반시설 마비는 이들 공격자들이 언제든 선택할 수 있는 옵션 중 하나일 뿐 반드시 필수 항목은 아니다. 국내 기간산업 및 방위 산업체를 타깃 공격하는 사이버 공격 그룹의 공격으로부터 기업과 조직의 안전을 지키기 위한 첫 걸음으로는 내부에서 사용하는 이메일의 첨부 파일을 주의하는 것이다. 이는 여러 번 강조해도 지나치지 않을 만큼 가장 기본적이면서도 중요한 부분이다. 최근 4~5년 전에 사용했던 국산 워드 프로세서 공격 기법을 재사용하는 것이 확인 된 바, 국산 워드 프로세서의 최신 버전 업그레이드와 보안 패치 설치는 반드시 수행해야 한다.

4. OT 환경까지 파고든 랜섬웨어

수많은 IT 보안 사건과 사고들 속에 파묻혀 있지만, 여전히 큰 위협으로 자리하고 있는 것이 바로 랜섬웨어(Ransomware)다. 그 중 산업 제어 시스템을 타깃으로 한 랜섬웨어 공격에 대해서도 주목할 필요가 있다. 2019년 3월, 유럽 소재 제조회사를 타깃 공격해 파일을 암호화하고, 생산라인의 가동을 멈추게 했던 록커고가(LockerGoga)는 ▲ 30개 확장자만 암호화 ▲ 시큐어 이메일 사용 ▲ 유효한 디지털 서명 사용 ▲ 협상을 통해 지불 금액 조율 ▲ 조직 내부 정보 수집 후 유출 등 5개의 주요 특징을 갖는다.



[그림 3] 산업 제어 시스템을 겨냥한 스네이크 랜섬웨어

올해 초 주목할 만한 랜섬웨어로 스네이크(Snake)가 등장했다. 스네이크 랜섬웨어는 고(Go) 랭귀지를 사용하고, 랜섬웨어에 의해 암호화된 파일 내부의 마지막 부분에 'EKANS'라는 문자열을 추가하는 등 자신만의 고유한 특징을 나타냈다. 스네이크 랜섬웨어는 전형적인 산업제어시스템 타깃 랜섬웨어로, 제어 시스템의 운영체제가 윈도우 기반인 각종 생산기기들을 타깃으로 공격을 수행하는 특징을 보였다. 사용자들의 단순 터치만을 필

요로 하는 윈도우 기반의 HMI 기기, 데이터 보관 서버 등을 공격했으며, 윈도우 운영체제가 아닌 기기들은 공격 범위에 전혀 포함되지 않았다. 록커고가와 유사하게 개인정보를 철저히 보장해 주는 이메일을 사용했으나, 윈도우 백업 이미지를 제거하여 복원을 원천 차단한 것과 암호화 이후에도 원격 계정의 연결을 유지한 것은 상당히 특색 있는 부분이었다. 디지털 서명과 악성코드 확산을 위한 자체 전파 방법을 사용하지 않았고, 조직 내부 전파를 위해 AD(Active Directory) 탈취 등을 진행한 것은 이들이 단순 랜섬웨어 공격자가 아니라는 것의 반증일 것이다. 산업 제어 시스템에 대한 타깃 공격에는 랜섬웨어 뿐만 아니라 다양한 목적의 악성코드가 활용되고 있으며, 공격의 범위가 점차 확장되어 가고 있다. 일반 사용자들로부터 상대적으로 관심이 적은 특수목적의 시스템들에 대한 보안체계 구축 및 관리가 그 어느 때보다 중요한 시기임을 기억해야 한다.

5. 몸캠피싱

올 해 초 n번방 이슈로 전국이 떠들썩했었다. 지난 5월 20일에는 n번방 방지법이 국회를 통과했고, 인터넷 사업자에게는 디지털 성 범죄물을 삭제할 의무가 주어졌다. 비정상적인 방법을 통한 협박은 전 세계인의 공통 해결 과제이나, 여전히 잔존하고 있는 문제일 것이다. 웹캠 블랙메일(Webcam blackmail)이라 불리는 위협은 서로의 신상을 노출하지 않은 상태에서 진행되는 화상 채팅 과정에서 범죄자들이 상대방에게 다소 과한 성적 행동을 하도록 유도하여 그것을 녹화한 후 영상 공개를 빌미로 상대방에게 돈을 요구하는 것을 말한다.

2000년대 중반까지 화상 채팅이 유행했다가 2011년 이후 스마트폰 랜덤 채팅의 영역으로 넘어 오면서 국내에서는 몸캠피싱으로 불리고 있다. 범죄자들은 스마트폰 랜덤 채팅 도중, 랜덤 채팅 도중, 음성 혹은 화면이 잘 보이지 않는다는 이유를 말하며, 특정 앱 설치를 종용하게 된다. 이렇게 설치된 악성 앱에 의해 스마트폰에 저장된 주소록, 문자 메시지, 사진 등이 유출되면서 피해가 발생했다. 공격자들은 앞선 웹캠의 공격에 더하여 '주소록을 통해 알게 된 지인들에게 영상을 유포하겠다'고 협박하여 돈을 요구하니 그 무서움이 증폭되었다. 이러한 사건은 생각보다 많이 그리고 끊임없이 발생하고 있고, 가족과 지인들에게 유포된다는 협박에 못 이겨 극단적 선택을 하는 경우도 꽤 많이 발생하고 있는 아주 심각한 사이버 범죄 중 하나이다.

원격 화상 회의 활성화로 인해 2000년대 중반 이후 사라져가던 웹캠이 다시 등장한 요즘, 섹스토션(Sextortion)의 위협이 더 강력하게 다가올 수 있음을 꼭 기억하고 대비하는 것이 필요하다. 웹캠 블랙메일 형태의 내용이 담긴 이메일을 수신하게 된다면 너무 놀라거나 긴장 말고, 내용에 상관없이 삭제 후 신경 쓰지 않는 것이 중요하다. 혹시라도 신경 쓰이는 부분이 있다면, 메일은 지우고 필요에 따라 사용 중인 계정 삭제, 비밀번호 변경, 서비스 회원 탈퇴 등을 고려하는 것이 필요하다. 이메일 제목에 자신이 사용하는 암호(password)를 넣어서 보내오는 경우, 현재 자신의 개인정보 상태를 재확인하고 동일 비밀번호는 파기할 것을 권한다. 이것

은 클라우드 서비스가 활성화되어 특별히 더 신경 써야 하는 부분이다. 더불어 모든 온라인 서비스들이 페이스북, 네이버, 카카오톡, 트위터 등의 계정을 통해 로그인할 수 있도록 연계되어 있는 만큼, 더욱 각별한 주의가 요구된다. 온라인 서비스 로그인 또는 스마트폰 로그인 시 사용하는 ID와 비밀번호 관리를 철저히 하고, 개인정보 유출이 의심되는 경우에는 즉시 자신이 사용하는 비밀번호를 다른 것으로 바꿔 공격자들이 추가적인 공격을 수행할 수 없도록 하는 것이 중요하다.

지금까지 2020년 상반기에 등장한 ▲ 코로나19를 악용한 사이버 보안 위협의 폭발적 증가 ▲ 스미싱&보이스피싱의 증가 ▲ 기반시설 타깃 악성코드 ▲ OT & ICS 영역까지 들어온 랜섬웨어 ▲ 몸캠피싱 등 5가지 사이버 보안 위협을 살펴 보았다.

보안 위협은 다양한 사회적 이슈를 악용하는 만큼 정부 기관 및 보안 업체에서 제공하는 다양한 형태의 위협 정보에 주의를 기울여야 한다. 더불어 자사의 비즈니스 환경에 맞는 대비책들을 강구함으로써, 보다 안전하고 자유로운 사이버 환경에서의 활동을 영위하기를 바란다.