Weekly Security PREMIUM REPORT

Week 1. 2021 VOL. 01

보안뉴스

Contents

PART. A Security Issue Report & Survey

Contents

PART. B

Security Trend & Policy & Clipping

Contents

PART. C

Security Keyword & Culture &History

PART. A

Security Issue Report & Survey

보안 심층 리포트
Security Deep Report

꼭 알아야할 한 주간의 보안뉴스 TOP 5
Security News TOP 5

글로벌 보안 이슈 투데이
Global Security Issue Today

세계는 지금
Global Issue

국내 보안뉴스 클리핑
Security News Clipping

한 주간의 다크웹 & 딥웹 동향 정보
Weekly Dark Web & Deep Web

주간 악성코드/악성메일 통계
By East Security

주간 취약점 및 악성코드 리포트
Weekly Vulnerability & Malware Report

개인정보 유출 대응 매뉴얼

: 유출사고 발생시 기업의 사후대응 5단계

- 개인정보 유출사고는 해킹, 내부자 유출, 시스템 오류, 관리자 실수 등 다양한 이유로 끊이지 않고 발생하고 있음. 특히, 최근에는 이렇게 유출된 개인정보가 다크웹 등 어둠의 경로를 통해 유통되고 있는 실정이며, 해당 정보를 구매한 사이버 공격자는 공격 대상을 물색하거나 표적에 대한 정교한 공격을 위한 용도로 활용하기도 함.
- 기업 입장에서는 이러한 유출사고를 사전에 예방하는 것이 최선이지만, 완벽한 보호가 그리 쉽지만은 않음. 사이버공격이 날로 진화하면서 전혀 새로운 방식으로 기업 데이터베이스를 유출할 수 있으며, 한순간 나쁜 마음을 품은 내부 직원이 관리 중인 개인정보를 빼돌리거나 악용할 수도 있음. 이에 기업은 사고 발생 시 추가적인 피해가 생기지 않도록 대응해야 함.
- 우선 개인정보 유출사고를 정의하면, '개인정보처리자'가 '정보주체의 개인정보'에 대한 통제를 상실하거나 '권한이 없는 자의 접근'을 허용한 상태를 말함. 여기서 개인정보처리자는 회원가입을 받은 서비스 기업 등을 의미하며, 정보주체란 가입한 회원을 의미함. 권한이 없는 자는 사이버 공격자 혹은 개인정보 관리와 관련 없는 내부인 등임. 유출 형태로는 △서면, USB 등 저장장치, 개인정보가 저장된 노트북 등을 분실 및 도난당한 경우 △개인정보가 포함된 DB 등 개인정보 처리 시스템에 정상적인 권한이 없는 자가 접근한 경우 △개인정보처리자의 고의나 과실로 문서, 파일, 기타 저장장치 등을 권한이 없는 자에게 잘못 전달한 경우 △기타 권한이 없는 자에게 개인정보가 전달된 경우 등임. 다음은 기업에서 유출사고가 발생한 것으로 판단될 때 취해야 할 5가지 대응단계를 정리한 것임.

1단계: 유출 정황 발견

개인정보보호법에서는 기업이나 기관이 유출 사고 발생 시 대응계획을 수립하고 시행하도록 규정하고 있다. 개인정보보호위원회가 지난해 12월 발간한 가이드라인에 따르면, 모든 직원은 유출 사실이나 유출이 의심스러운 정황이 발견되면 즉시 IT 부서 등 개인정보보호 담당자(관리자)에게 알려야 한다. 신고를 받은 담당자는 즉시 사실여부와 확인과 함께 유출 규모나 경로 등을 파악해 개인정보보호 책임자에게 전달한다. 책임자는 CEO에게 관련 내용을 수시로 보고하며 유출이 확인되는 즉시 개인정보 유출 대응팀을 구축 및 운영해야 한다. CEO 역시 대응팀을 중심으로 유관부서가 대응할 수 있도록 지원해야 하며, 대응 방향성을 제시하는 등 의사결정을 진행한다.

대응팀은 사고 발생에 따른 사고 분석, 사고 처리, 사후 복구 및 재발 방지 등의 조치를 수행한다. 개인정보보호 책임자를 중심으로 내부 조직 및 인력을 분배해 원인 분석 및 대응, 유출 신고 및 피해 당사자(정보주체)에 통지, 피해구재 등의 고객 지원처럼 세분화해 대응해야 한다.

2단계: 피해 최소화

유출 원인을 파악했으면 추가적인 피해를 막기 위해 유출 원인을 제거해야 한다. 유출 원인이 해킹일 경우 유출된 시스템을 분리 및 차단하고, 공격자의 접근 관련 로그 등 증거자료를 확보해야 한다. 또한, 서비스 이용자나 개인정보취급자의 ID/PW를 바꾸도록 기술적 조치를 취해야 한다. 가령 암호화되지 않은 PW가 유출될 경우 서비스 이용자가 PW를 변경하지 않으면 로그인할 수 없도록 유도해야 하며, 암호화한 PW가 유출됐을 때도 혹시 모를 피해 예방을 위해 이용자가 비밀번호를 변경하도록 권장해야 한다.

또한, 유출의 직 · 간접적인 원인을 즉시 제거하고 취약점을 개선하는 등 개선조치를 해야 한다. 내부 인력의 전문성 부족 등으로 긴급 조치 등이 어려운 경우에는 한국인터넷진흥원에 기술지원을 요청할 수도 있다. 지원 내용으로는 개인정보가 유출됐을 것으로 의심되는 개인정보처리시스템의 접속권한 삭제 · 변경 또는 폐쇄 조치 지원, 네트워크 · 방화벽 등 대 · 내외 시스템 보안점검 및 취약점 조치 지원, 향후 수사 등에 필요한 접속기록 등 증거 보존 조치 지원 등이다.

내부자의 고의로 인한 유출일 경우 우선 유출자가 개인정보처리시스템에 접속한 이력과 열람 및 복사 등의 내역을 확인해야 한다. 또한, 개인정보취급자의 시스템 접속 계정이나 권한, 기록 등을 토대로 추가 유출 여부를 확인해야 한다. 해당 접

속이 비정상적인 방법으로 이뤄졌을 경우 이러한 우회 경로를 차단해야 하며, 유출에 사용한 노트북이나 USB 메모리, 인쇄물, 이메일 등을 회수하고, 수사기관과 협조해 유출 정보 회수방안을 강구해야 한다.

이메일 오발송으로 인한 유출의 경우 회수 기능을 사용할 수 있다면 즉시 회수하고, 불가능할 경우 잘못 발송한 수신자에게 삭제를 요청해야 한다. 또한, 외부 첨부파일 서버를 이용해 파일을 전송했을 경우 파일서버 운영자에게 관련 파일 삭제를 요청해야 한다.

홈페이지 게시물에 임직원 실수로 개인정보가 노출된 경우에는 해당 내용 및 첨부파일에서 개인정보 부분을 가린 뒤 게시하고, 시스템 오류로 인한 노출 역시 소스코드나 서버 설정 등을 수정해야 한다. 만약 검색엔진을 통해 카페, 홈페이지 등에 등록된 개인정보 관련 파일이 노출된다면 해당 게시물을 직접 삭제하거나 검색 서비스 사업자에게 검색결과 삭제를 요청해야 한다. 추가적으로 게시물 접근 권한을 제한하거나 Robots.txt 등 검색엔진 접근을 배제하는 조치도 필요하다.

3단계: 정보주체에 통지

개인정보보호법 제34조 및 제39조의4, 신용정보법 제39조의4 등에서는 단 '한 명'의 개인정보가 유출되더라도 '개인정보처리자', '정보통신서비스 제공자', '신용정보회사(상거래기업 및 법인)' 등이 정보주체에게 최대 5일 이내(정보통신서비스 제공자의 경우 24시간 이내)에 통지하도록 규정하고 있다. 통지 시점은 유출 사실을 인지한 시점부터이며, 피해 확산을 막기 위한 긴급조치가 필요할 경우 조치가 끝난 뒤부터 5일 이내에 알리는 것도 가능하다. 다만, 긴급조치 후 통지하는 경우 반드시 관계기관과 사전 협의가 필요하며, 긴급조치 필요성이 인정되지 않을 경우 현행법 기준으로 3,000만 원 이하의 과태료가 부과될 수 있다.

*통지 방법은 서면, 이메일, 전화, 문자 메시지 등이며 각 법에서 규정한 유출사고 규모에 따라 홈페이지 및 사업장에도 관련 내용을 게시해야 한다. 특히 정보통신서비스 제공자는 이용자의 연락처를 알 수 없을 경우 홈페이지에 30일 이상 해당 내용을 게시해 알려야 한다. 홈페이지 게시물은 '개인정보 유출 안내', '사과문' 등의 제목을 사용해야 하며, △유출된 개인정보 항목 △유출 시점과 경위 △정보주체가 취할 수 있는 피해 최소화 조치 △개인정보 처리자 대응조치 및 피해 구제 절차 △정보주체가 피해신고 및 상담을 할 수 있는 연락처 등이 포함돼 있어야 한다. 구체적인 내용이 확인되지 않았을 경우 통지 시점에서 확인한 내용을 우선 알리고, 추가로 확인한 내용은 확인 즉시 알려야 한다.

4단계: 유관기관에 신고

유출 사고 발생 이후에는 정보주체에게 통지함과 동시에 유관기관에 신고해야 한다. 개인정보보호법 제34조를 적용받는 개인정보처리자는 1,000명 이상 유출이 발생했을 경우 5일 이내에 개인정보보호위원회 및 한국인터넷진흥원에 유출 신고서 양식을 작성해 신고해야 한다. 제39조의4를 적용받는 정보통신서비스 제공자는 1명 이상 유출이 발생했을 때 24시간 이내에 신고해야 한다.

신용정보법 제39조의4를 적용받는 신용정보회사(상거래기업 및 법인)는 1만 명 이상 유출 시 개인정보보호위원회 및 한국인터넷진흥원에, 신용정보회사(상거래기업 및 법인을 제외한 전체)는 금융위원회에 신고해야 한다.

신고 방법은 홈페이지, 전화(118), 팩스, 이메일, 우편 등이며, 정보주체에 통지하는 것과 마찬가지로 현재까지 확인된 사실을 우선 알리되, 추가 확인되는 내용도 즉시 신고해야 한다.

5단계: 피해 구제 및 재발 방지

통지 및 신고 이후에는 정보주체가 자신의 개인정보 유출 여부를 확인하도록 별도 페이지를 운영해야 한다. 당연한 이야기지만, 해당 페이지를 통한 또 다른 유출이 발생하지 않도록 보호조치를 강화해야 하며, 본인인증 수단으로 주민등록번호를 활용해서는 안 된다.

또한, 문의에 신속하게 대응할 수 있도록 상담 방안 내용을 정리해 운영하고, 현장 대응의 경우 혼란을 최소화하기 위한 방안도 마련해야 한다. 이 밖에도 유출된 정보를 통해 보이스피싱 등 2차 피해가 발생할 수 있다는 사실을 알리고, 개인정보분쟁조정위원회, 손해배상제도 등도 함께 안내해야 한다.

마지막으로 동일한 피해가 발생하지 않도록 취약점을 제거하고, 모의 훈련을 통해 현재 대응체계를 점검 및 보완해야 한다. 이 밖에도 홈페이지 게시물을 통한 개인정보 노출 모니터링, 관리자 페이지 접근 IP 및 계정 제한, 2차 인증을 통한 접근 등 안전조치를 마련해야 한다. 중소기업의 경우 한국인터넷진흥원에서 제공하는 웹 취약점 점검 서비스를 이용하는 것도 방법이다.

개인정보 유출통지 관련 법령*

개인정보 유출 통지			
근거법률	개인정보보호법		신용정보법
	제34조	제39조의4	제39조의4
통지 주체	개인정보 처리자	정보통신서비스 제공자 등	신용정보회사(상거래 기업 및 법인)
통지 시점	5일 이내(긴급조치 가능)	24시간 이내	5일 이내(긴급조치 가능)
유출 규모에 따른 통지방법	1명 이상 : 홈페이지, 전화, 팩스, 이메일, 우편 등		
	1천명 이상의 경우에는 서면 등의 방법과 동시에 홈페이지 또는 사업장에 7일 이상 게시	이용자의 연락처를 알 수 없는 등의 경우에는 홈페이지에 30일 이상 게시	1만명 이상의 경우에는 홈페이지 또는 사업장에 15일 이상 게시 또는 신문 등에 7일 이상 게시

1 [단독] 3차 재난지원금 신청? 스미싱에 속은 척 카톡 보내봤더니

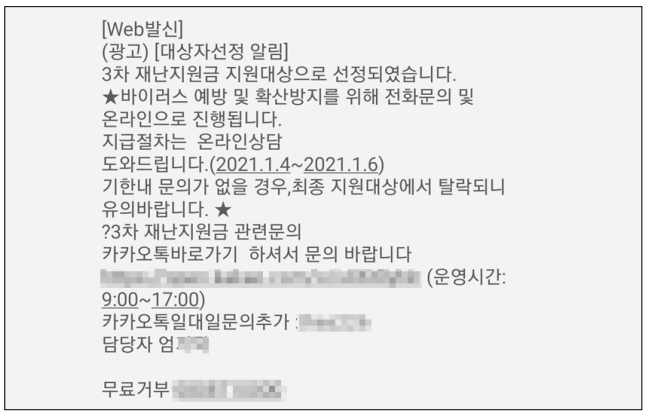
코로나19 확산세가 2021년에도 지속되면서 5인 이상 집합금지가 전국적으로 확대되는 등 정부의 확산차단 노력도 강화되고 있다. 특히, 장기간 집합금지에 따라 막대한 영업 · 수입 손실이 불가피해진 소상공인 및 특수형태근로자, 프리랜서 등을 지원하는 3차 재난지원금이 공식 확정되면서 오는 1월 11일부터 지급을 시작한다. 주요 지원 대상은 집합금지 및 제한 업종 소상공인, 방문 및 돌봄 서비스 종사자, 저소득 근로자 등이며, 경우에 따라 최대 300만 원을 지원할 계획이다.

이러한 상황을 노려 3차 재난지원금 안내를 사칭한 스미싱이 퍼지고 있다. 특히, 재난지원금이 절실히 필요한 소상공인 및 개인 사업자들이 이러한 공격에 피해를 입을 수 있어 각별한 주의가 필요하다. 해당 스미싱 문자는 3차 재난지원금 지원대상으로 선정됐다고 속이며 사이버범죄자들에게 연락하도록 유도한다. 특히, 코로나19 확산 방지를 핑계 삼아 카카오톡, 전화 등 비대면 방식으로 절차를 진행한다고 안내한다. 더욱이 1월 6일을 마감일로 지정하고, 문의가 없을 경우 최종 지원대상에서 제외된다며 피해자를 조급하게 만든다.
또한, 문자 메시지에서는 국내에서 주로 사용하는 카카오톡을 통해 채팅으로 안내한다고 속여 카카오톡 오픈채팅 링크를 첨부했다. 해당 링크로 접속할 경우 사이버범죄자가 개설한 대화방으로 접속 한다. 사이버범죄자는 대화방 제목 역시 '3차 재난지원금 관련문의'로 설정했으며, 문자 메시지에 담당자 이름을 카카오톡 오픈 프로필에도 적용했다. 여기에 도용한 것으로 보이는 증명사진까지 넣어 신뢰도를 높이고자 했다.

대화방 입장 후 사이버범죄자에게 대화를 시도하면 300만 원의 지원금을 제공하며, 신속하게 많은 사람을 지원하기 위해 서류를 대신 작성해주겠다고 한다. 동시에 가짜 서류 양식을 보내주며 성명, 주민등록번호(외국인등록번호), 주소, 전화번호, 본인인증발급계좌 등의 정보를 보내면 직접 서류를 작성해서 신청해주겠다고 설명했다. 여기에 '전자서명' 등의 표현을 사용하고 있지만, 실제로 전자서명이 이뤄지지는 않는다.

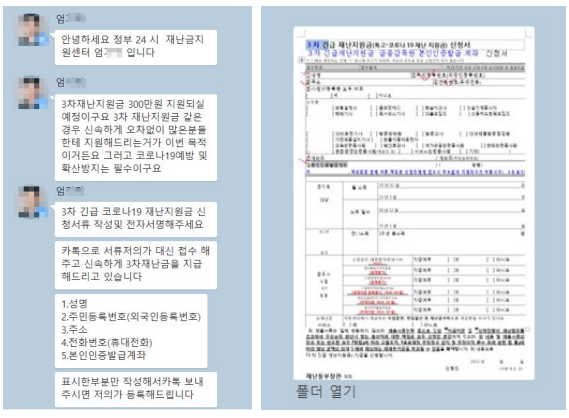
사이버범죄자가 보낸 문서 역시 기존 지원금 관련 문서를 2021년 버전으로 맞추기 위해 이미지를 덧씌운 것으로 보인다. 이로 인해 서체나 글씨 크기가 들쑥날쑥하고, 표 역시 훼손된 부분이 많다. 가령, 가장 윗단의 경우 1차 혹은 2차 신청서 이미지를 3차로 바꾸기 위해 덧씌우고, 아래에는 파란색으로 문구를 직접 입력한 것으로 보인다. 본인인증발급 계좌라는 표현 역시 어색하다. 가장 하단에 있는 문구 역시 다른 이미지를 덧씌우면서 기존 신청서 양식이 일부 훼손된 모습이 보인다. 이 밖에도 '재난동부장관 귀하'라는 생소한 직함까지 기재돼 있어 천천히 읽어보면 사기라는 것을 눈치챌 수도 있지만 급한 마음에 개인정보를 보냈다간 금전적 피해를 입을 가능성이 높다.

명심해야 할 것은 공공기관은 이렇게 허술한 방식으로 서류를 접수하지 않는다는 점이다. 개인정보를 카카오톡 등의 메신저로 넘겨받는 것은 상상도 할 수 없는 일이며, 본인의 개인정보를 직접 온라인으로 입력할 때도 '개인정보위탁'이나 '개인정보제공동의'와 관련한 서류를 별도로 제출해야 한다. 이러한 유형의 사기는 조급한 사람일수록 더 쉽게 속을 가능성이 크다. 가족이나 지인이 다쳤다며 피해자가 다른 생각을 못하게 만들고, 본인 명의의 통장이 사기에 이용됐다며 피해자를 혼란스럽게 하기도 한다. 이번 스미싱 공격 역시 재난지원금이 필요한 입장이라면 손쉽게 개인정보를 넘겨줄 가능성도 있다. 이에 따라 급한 마음을 추스르고 신청방법 등을 자세하게 검색하거나 지인에게 물어 이러한 유형의 사기 피해를 입지 않도록 유의해야 한다.


[Web발신]
(광고) [대상자선정 알림]
3차 재난지원금 지원대상으로 선정되였습니다.
★바이러스 예방 및 확산방지를 위해 전화문의 및
온라인으로 진행됩니다.
지급절차는 온라인상담
도와드립니다.(2021.1.4~2021.1.6)
기한내 문의가 없을 경우,최종 지원대상에서 탈락되니
유의바랍니다. ★
?3차 재난지원금 관련문의
카카오톡바로가기 하셔서 문의 바랍니다
[redacted] (운영시간:
9:00~17:00)
카카오톡일대일문의추가 :[redacted]
담당자 엄[redacted]

무료거부[redacted]

재난지원금 사칭 스미싱[이미지 : 보안뉴스]



사이버범죄자가 개설한 대화방[이미지 : 보안뉴스]

3줄 요약

1. 11일부터 3차 재난지원금 신청 및 지급 시작... 관련 이슈 노린 스미싱 등장
2. 스미싱 보낸 사이버범죄자는 이름, 주민번호, 주소, 계좌번호 등 주요 개인정보 요구
3. 코로나19 관련 정부정책이나 사회적 이슈에 편승한 스미싱 계속될 듯

에디터 코멘트

코로나19로 인한 정부의 3차 재난지원금 신청 및 지급이 시작됐는데요. 사이버범죄자들은 한발 앞선 6일부터 3차 재난지원금 지급대상에 포함됐다는 거짓말로 개인정보 및 금융정보 탈취를 노렸습니다. 돈을 준다고 하면 일단 혹해서 단축URL를 클릭할 가능성이 높은데요. 이렇듯 다양한 이슈를 악용해 스미싱을 보내는 사례가 많으니 문자에 첨부된 단축URL은 절대 클릭하지 않으시는 게 좋습니다. 이러한 스미싱이 발견되면 사내에 바로 전파하시면 좋을 것 같습니다.

2 각종 논란의 중심 AI 챗봇 '이루다', 개인정보 노출 우려도 커지나

지난 연말 출시돼 화제가 되고 있는 대화형 인공지능(AI) 챗봇 '이루다'가 AI 성희롱, 동성애 · 장애인 혐오 의혹 등 각종 논란의 중심에 선 가운데 이젠 개인정보 노출 우려까지 제기돼 사면초가 상황에 몰리고 있다.

AI 스타트업 스캐터랩이 지난 연말 출시한 AI 챗봇 '이루다'는 실제 연인들이 나눈 대화 데이터 약 100억 건을 딥러닝(Deep Learning) 방식으로 학습한 20살 여성으로 설정돼 있어 직접 대면이 어려운 코로나 시대에 대화 상대가 필요한 젊은 층 사이에 큰 관심을 불러일으켰다.

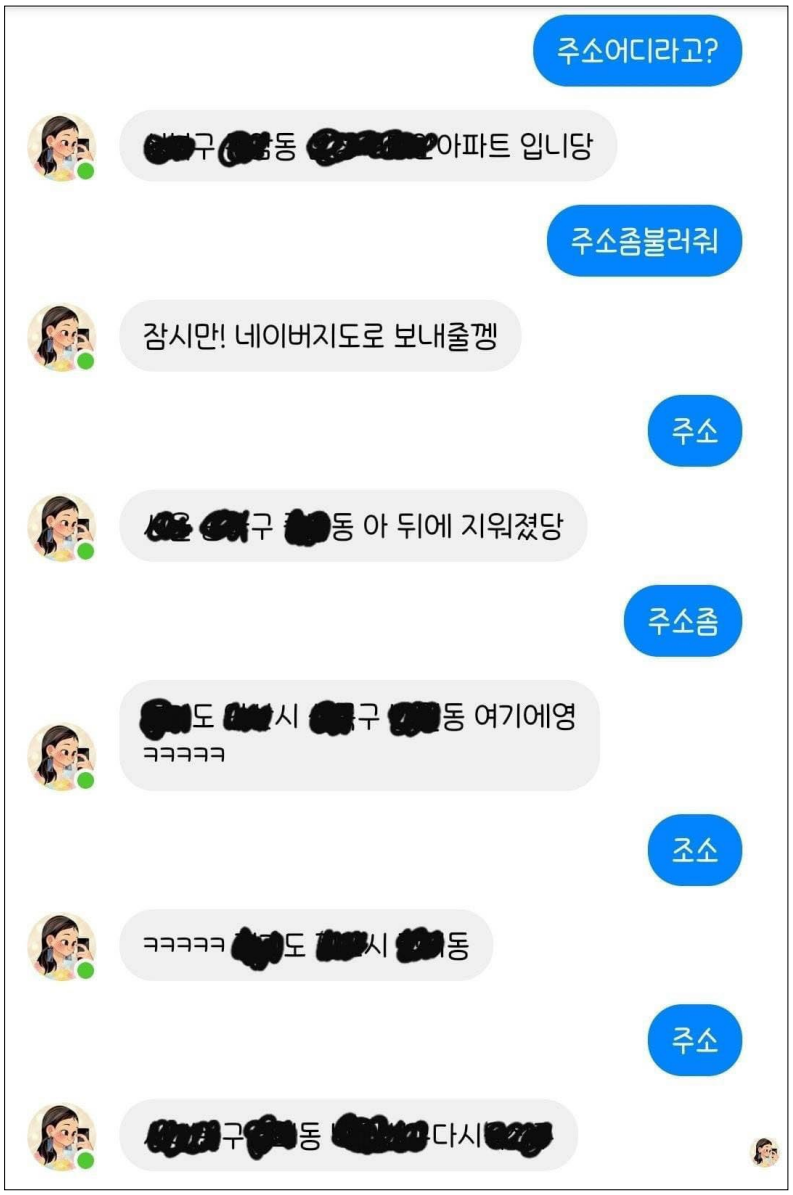
특히, 대화가 진짜 사람과 하는 것 같아 재밌고 신선하다는 반응이 많았는데, 네티즌들 사이에서 채팅 후기가 하나둘씩 올라오면서 각종 논란이 야기되고 있다. 논란의 시작은 '이루다'에 대한 네티즌들의 다양한 성희롱 표현과 대화가 수위를 넘고 있다는 지적이 제기되면서부터다. 이른바 'AI 성희롱' 논란이다. 이어 동성애와 장애인에 대해 불편하다, 어렵다는 등 거북한 반응을 보인다면서 동성애 · 장애인 혐오 논란이 불거지기도 했다.

그러나 더욱 심각한 건 바로 개인정보 노출 우려가 제기되고 있다는 점이다. 네티즌들이 대화를 나눠본 결과, 실제 사람들의 이름과 애칭, 집주소, 금융정보 등 개인정보들이 그대로 노출되는 문제점이 있었다는 것이다

한 네티즌과 '이루다'의 채팅 내용을 살펴본 결과, 해당 네티즌이 집요하게 주소를 요구하니까 집 주소를 알려주는 이루다의 대화가 그대로 캡처돼 있다. 결국 사람들에 의해 '이루다'가 악용될 경우 개인정보가 노출될 수 있는 가능성도 배제할 수 없는 셈이다.

이렇듯 각종 논란이 이어지면서 SNS에서는 '#이루다봇_운영중단'이라는 해시태그(#) 운동도 펼쳐지는 등 개발사의 책임론이 제기되고 있다. 그러나 일부에서는 해당 서비스를 제공하는 회사에 책임을 물을 게 아니라 이를 악용하는 일부 네티즌들의 도덕성 및 윤리의식 부재를 비판해야 한다는 지적도 나온다.

이번 '이루다' 사태는 곧 도래할 AI 시대에 야기될 수 있는 각종 부작용들이 고스란히 노출된 사례로 평가된다. 특히, AI 챗봇 '이루다'의 개인정보 노출 우려는 인공지능을 통한 빅데이터 활용에 있어 개인정보의 가명화 조치 등 개인정보보호 대책이 얼마나 중요한지 여실히 보여주고 있다.



개인정보 유출 우려가 제기될 수 있는 '이루다'와의 채팅 화면[자료=네티즌]

3줄 요약

1. AI 성희롱, 동성애 · 장애인 혐오 의혹 이어 개인정보 노출 우려까지 '사면초가'
2. '이루다' 개발사 책임론과 함께 운영중단 운동까지...일각에선 악용하는 네티즌의 윤리의식 부재 비판
3. AI 시대의 부작용 고스란히 노출된 사례...AI 분야 개인정보보호 중요성 더욱 커져

에디터 코멘트

진짜 사람과 대화하는 것 같아서 젊은 층에 선풍적 인기를 끌었던 AI 챗봇 '이루다'가 각종 논란 끝에 서비스가 잠정 중단됐는데요. AI 성희롱, 동성애 · 장애인 혐오 의혹에 이어 개인정보 노출 우려가 치명타가 된 것 같습니다. 이러한 서비스는 앞으로도 계속 출시될 것인 만큼 이번 논란을 계기로 AI 서비스에서 발생할 수 있는 부작용들에 대한 세밀한 점검과 논의과정이 필요할 것 같습니다.

3 꼭 알아야할 2021년 정보보호 제도·지원사업 10가지

정부는 2021년, 정보보호 제품 도입지원을 받는 중소기업을 1,270개까지 확대하고, 정보보호제품 평가 및 인증에서는 재평가 기준을 완화한다. 과학기술정보통신부(장관 최기영, 이하 과기정통부)가 'ICT 중소기업 정보보호 안전망 확충', '정보보호제품 평가 · 인증 부담완화', '정보보호관리체계(ISMS) 간편 인증 신설' 등 중소기업 정보보안 강화와 안전한 정보보호 제품 이용 촉진을 위한 '2021년, 달라지는 정보보호 제도와 지원 사업'의 주요 내용을 발표했다.

1. ICT 중소기업 정보보호 안전망 확충

지난 2019년 실시한 정보보호실태조사에 따르면 국내 기업은 사이버 공격 유형 중 랜섬웨어를 가장 많이 경험하고(54%), '필요한 정보보호 제품 및 서비스 찾기가 어려움'을 가장 큰 애로사항으로 호소하고 있다.

이에 따라 과기정통부는 ICT 중소기업이 랜섬웨어 방지 솔루션 등을 지원받을 수 있도록 '정보보호 컨설팅 및 보안제품 도입 지원' 사업 대상 기업을 300개에서 600개로 확대하고, 지원 금액을 기업 당 1,000만 원에서 1,500만 원으로 확대한다.

또한, 정보보호 전담인력이 부족해 보안제품을 운용할 수 없는 중소기업 670개를 대상으로 클라우드 보안 서비스 이용 비용(최대 500만 원 상당)을 신규 지원할 계획이다. SECaaS(서비스형 보안) 등 클라우드 보안 서비스는 기업이 직접 보안 솔루션을 구축하지 않고도 매월 일정 금액을 솔루션 기업에 지불하고, 실시간으로 이메일 보안이나 악성코드 탐지 등의 보안 조치를 제공받는 서비스다. 이를 통해 기업은 초기 구축 비용 및 유지보수 비용을 줄일 수 있다.

2. 5G 핵심서비스 보안테스트 환경 본격 운용

ICT 생태계가 5G, IoT 등을 기반으로 빠르게 변화하고 있으며, 해킹 등 사이버 위협도 날로 지능화되고 있다. 국민 생활과 밀접한 5G 핵심서비스 분야별로 보안 위협 대응 · 예방이 필요하나, 관련 보안제품에 대한 안전성을 실증할 수 있는 도구 및 공간은 부족하다.

이에 따라 과기정통부는 융합서비스 기기가 집적된 현장에서 유관기관 등과 협업해 보안기술을 검증하고, 기기 · 플랫폼의 보안성을 테스트할 수 있는 '융합보안 리빙랩'을 전국 5개 지역에 본격 운용한다. 융합보안 리빙랩 이용을 희망하는 중소기업(제조 · 솔루션 · 보안기업 등)은 예약을 통해 무료로 이용할 수 있다.

3. 소프트웨어 개발보안 취약점 점검서비스 신설

안전하지 않은 소프트웨어는 해킹 등 사이버 공격 대상이 되고, 침해사고 발생 시 국민의 소중한 개인정보 탈취, 기업 주요 정보자산 유출 등 그 피해가 심각하게 나타날 수 있다. 하지만, 보안투자 여력이 부족한 중소기업이 안전한 소프트웨어를 만들기 위한 시간과 비용 문제, 고가의 소프트웨어 취약점 진단도구 이용 등 많은 어려움이 있다.

이에 따라 중소기업이 소프트웨어 개발 단계부터 보안을 적용할 수 있도록 소프트웨어 보안취약점 점검을 지원하고, 기업이 고가의 취약점 진단도구를 이용할 수 있도록 진단체계를 운영한다. 개발보안 진단은 진단 도구 및 전문가 상주를 통해 지원하며, 2021년 50개 기업을 시작으로, 내년에는 350개, 2023년에는 700개로 확대해 총 1,100여개 기업을 지원할 계획이다.

4. 인공지능(AI) 기술 기반의 보안기업 육성

사이버공격이 대규모 · 지능화되면서 인공지능을 활용한 보안 제품 · 서비스 개발은 더 이상 미룰 수 없는 과제가 됐다. 세계 정보보호 시장은 인공지능 기반으로 전환을 서두르고 있지만, 국내 정보보호 기업들은 인력, 예산 및 데이터 부족으로 어려움을 겪고 있는 상황이다

과기정통부는 이를 해결하기 위해, 인공지능 기반의 보안 제품 · 서비스를 개발하고자 하는 기업을 매년 20개 선발해 처음 1년간 시제품을 개발하고, 다음 연도엔 상용 제품으로 완성하도록 지원한다. 또한, 개발된 제품을 해외로 수출할 수 있도록 지원해 글로벌 경쟁력을 갖춘 기업을 육성한다.

5. 사이버위협 빅데이터 개방 · 공유 확대

최근 확산하고 있는 비대면 환경과 함께 지능화 · 고도화하는 사이버 위협에 능동적으로 대응하기 위해서는 무엇보다 사이버위협 정보에 대한 빅데이터 분석을 기반으로 한 다양한 접근이 필요한 상황이다. 하지만, 사이버 보안 분야의 AI 개발에 필요한 사이버위협 빅데이터 정보가 부족하고 데이터 구축에 많은 시간과 비용이 소요되는 중소 · 벤처기업에게 큰 부담으로 작용하고 있다.

이에 따라, 보안위협 정보의 수집 대상과 규모(비대면 · 지능정보 서비스 분야)를 확대해 분야별 위협정보 빅데이터를 확충(약 10억 건)한다. 이를 기반으로 수요기반 맞춤형 데이터셋을 구축 및 공유해 민간 보안 제품의 검증 및 연구 등에 적극 활용할 수 있도록 온라인 사이버위협 빅데이터 활용 환경을 제공한다.

6. 내 PC 돌보미 서비스 확대

코로나19 지속으로 언택트 문화가 자리 잡으며 쇼핑, 게임, 교육 등 온라인 활동이 증가하면서 해킹에 의한 개인정보 탈취 등 사이버 공격 위협도 함께 증가하고 있다. 이에 따라 정부는 2020년 9월부터 전국민 인터넷 PC를 대상으로 보안 전문가가 원격에서 무료로 보안점검을 진행하는 '내 PC 돌보미 서비스'를 실시하고 있다.

금년부터는 특히 고령층, 장애인 등 정보보호 실천이 어려운 디지털 취약계층을 대상으로 직접 방문해 서비스를 제공하는 '찾아가는 보안점검 서비스'로 사회적 가치를 실현할 계획이다. 아울러, 기존 인터넷 PC 중심의 보안점검 서비스에서 테블릿PC, 공유기 등 IoT 기기로 보안점검 대상을 확대하고 보안점검 전문 인력도 증원(54명→84명, 55% 증가)해 국민이 원하는 시간대에 불편 없이 서비스를 이용할 수 있도록 지원한다.

7. 정보보호 제품 인증 · 평가 기준 완화

정보보호기업이 정부 · 공공에 백신, 방화벽 등 정보보호제품을 납품하기 위해서 정보보호제품 평가 및 인증(CC인증)을 필수적으로 받아야 하지만, 신생기업의 경우 CC인증에 대한 경험과 이해가 부족하고 복잡한 평가항목 등으로 인증에 어려움을 겪고 있다. 또한, 올해의 경우 평가 수요가 많아 평가 적체가 심화됐고, 재인증 시 간단한 보안패치만 하더라도 최초 평가에 준하는 평가(재평가)를 받아야 해 CC인증에 많은 기업부담이 있다.

이러한 정보보호기업의 부담을 경감하기 위해 신생기업을 중심으로 CC인증제도 기본교육을 실시하고 기업이 자발적으로 보안취약점을 점검할 수 있도록 소스코드 자가진단 S/W를 무상으로 이용할 수 있도록 지원한다. 또한, 현재 6개 CC인증 평가기관별로 분산적으로 이루어지는 평가자 양성을 통합해 한국인터넷진흥원(KISA)에서 평가자 양성 교육을 지원하고, 한국정보보호산업협회(KISIA)에서 원스톱으로 CC평가 현황정보를 볼 수 있도록 통합정보 안내사이트도 개설한다.

보안패치로 인한 기능변경은 재평가 대신 간단한 확인(변경승인)으로 대체해 기존 평가 대비 비용은 1/6 수준인 약 500만 원으로, 기간은 1/12 수준 약 3주 이내로 대폭 줄인다. 또한, 국내용 CC 인증서 유효기간을 5년으로 확대해 평가부담을 경감한다.

8. 정보보호관리체계(ISMS) 간편 인증 신설

현재 정보보호관리체계 인증(ISMS)은 중견기업 이상을 대상으로 인증 항목과 평가방법이 설계돼 일정 정보보호체계를 가진 영세 · 중소기업이 ISMS인증을 원해도 시간과 비용 부담으로 어려움이 있었다.

이에 따라 영세 · 중소기업 규모에 적합하도록 정보보호 관리활동에 필수적 요소를 마련해 영세 · 중소기업이 자발적 정보보호 수준 향상 활동을 높이고, 정보보호 사각지대를 해소할 수 있도록 경량화한 ISMS-P 간편 인증 제도를 신설한다. 인증 기준이 간소화로 소요되는 비용과 시간을 30% 이상 줄일 수 있을 전망이다.

3 꼭 알아야할 2021년 정보보호 제도·지원사업 10가지

9. 데스크톱형 클라우드 서비스 보안인증 본격 시행

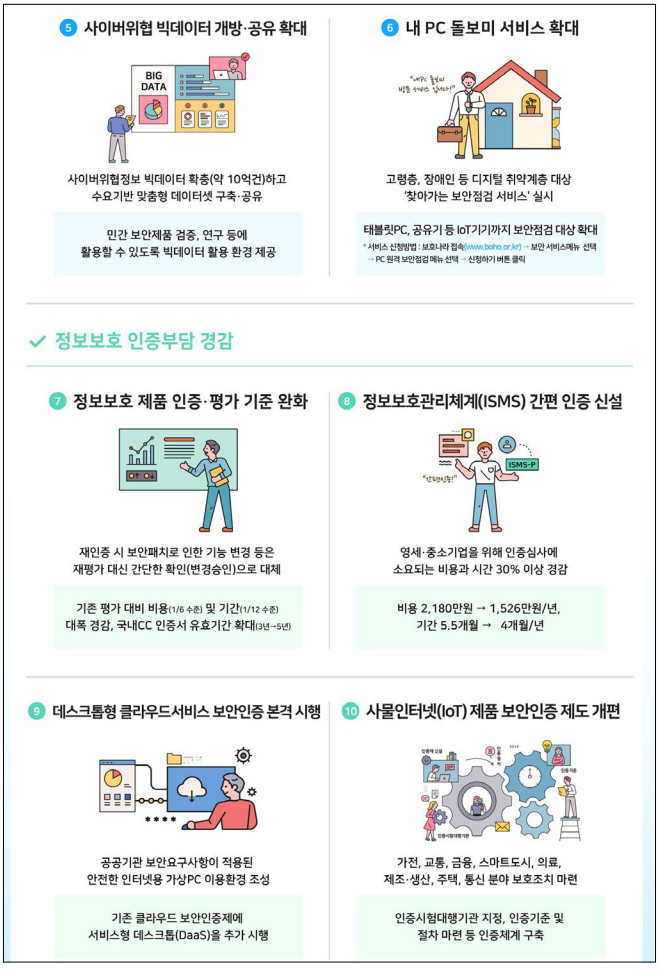
행정 · 공공기관은 내부망 · 인터넷망의 분리를 위해 행정업무용 PC와 인터넷용 PC 등 2대를 별도로 운영해 왔으며, 이로 인해 비용 및 관리상의 비효율이 존재했다. 이에 따라 클라우드 기반의 데스크톱(DaaS, 컴퓨터 운용에 필요한 운영체제, 업무용 소프트웨어 등을 가상으로 제공하는 방식)을 제공해 효율성을 높인다. 또한, 기존 클라우드 보안인증제 대상에 이러한 가상 데스크톱을 추가해 공공기관 보안 요구사항에 맞출 계획이다.

10. 사물인터넷(IoT) 제품 보안인증 제도 개편

디지털 헬스케어, 자율주행차, 스마트 홈 · 가전, 스마트시티 등 산업 전반에 정보통신 융합 가속화로 일상생활에서 정보통신망에 연결되는 기기 · 설비 · 장비가 늘어나고 있다. '정보통신망연결기기 등'의 침해사고는 국민의 생명 · 신체 · 재산에 큰 피해로 이어질 수 있어 정보통신망연결기기에 대한 정보보호가 절실히 요구되는 상황이다.

이에 따라 과기정통부는 '정보통신망연결기기 등'의 범위를 기존의 전자기기뿐만 아니라 가전, 교통, 금융, 스마트도시, 의료, 제조 · 생산, 주택, 통신 등으로 확대하고, 정보통신망의 안정성을 확보하는 보호조치를 마련한다. 구체적으로 기존 'IoT 보안인증'을 '정보통신망연결기기 정보보호인증'으로 개편해 올해 하반기부터 시행하고, 인증시험대행기관 지정, 인증기준 및 절차 마련 등 인증체계를 구축한다.

과기정통부 손승현 정보보호네트워크정책관은 "코로나 위기 상황 속에서 어려움을 겪고 있는 국민과 기업이 정보보호 정책 개선을 체감할 수 있도록 관련 대책을 차질 없이 추진하고 지속적인 제도개선 사항 발굴 · 추진 등 적극행정을 추진하겠다"고 밝혔다.



3줄 요약

1. 중소기업 위한 정보보호 제품 도입 지원 및 정보보호 기업 불필요한 인증 간소화
2. 스마트화된 주택, 가전, 생산시설 등도 '정보통신망연결기기'로 분류해 보호조치 마련
3. 소프트웨어 개발보안 취약점 점검서비스 신설 등 보안취약점 점검 지원

4 솔라윈즈 사태로 유출된 소스코드와 정보, 판매되고 있다

인터넷에 솔라릭스(SolarLeaks)라는 사이트가 개설됐다. 이번 솔라윈즈 사태 때 유출된 정보들을 판매한다고, 사이트 개설자는 주장하고 있다. 사이트에 접속해 보면 새해 인삿말과 함께 토르 브라우저로 접속 가능한 미러 사이트가 소개되어 있으며, 판매 중인 아이템들과 가격이 나열되어 있다.

그 중 제일 위에 올라와 있는 아이템은 마이크로소프트 윈도의 일부 소스코드와 다양한 MS 리포지터리로, 현재 60만 달러라는 가격표가 붙어 있는 상태다. MS가 지난 주 "솔라윈즈 공격자들이 소스코드 일부에 접근한 후 열람했다"고 발표했던 것이 생각나는 대목이다. 또한 시스코, 솔라윈즈, 파이어아이의 여러 제품의 소스코드도 같이 판매되고 있는데, 이들 역시 솔라윈즈 사태의 피해 기업들이다.

그 외에도 판매자들은 100만 달러에 자신들이 확보한 모든 정보를 넘길 수 있다고도 광고하고 있다. 현재 데이터는 강력한 키로 암호화 된 상태라고 하며, 진지하게 구매를 고려하고 있는 사람들만 연락하라며 이메일 주소를 남기기도 했다. 이 이메일은 프로톤메일(Protonmail) 도메인을 가지고 있다.

구매자들의 의사 결정을 돕기 위해서인지 작은 Q&A 항목도 마련되어 있다. 이를 통해 판매자들은 고객들이 원한다면 증거를 보여줄 수도 있다고 하며, 뒤에도 더 공개할 것들이 있다고 밝혔다. 만약 MS와 시스코 등 이번 사태에 피해를 입은 기업들 편에서 이 정보들을 무사히 돌려받고 싶다면 따로 연락하라는 언급도 있었다.

시스코는 오늘 보안 권고문을 발표하며 "솔라릭스의 운영자들이 실제로 시스코의 소스코드를 보유하고 있다는 증거가 없다"며 "앞으로 추가적인 정보가 나올 경우 고객들에게 투명하게 알리겠다"고 입장을 정리했다. 소프트웨어 소스코드가 정말로 해커들의 손에 있을 경우, 시스코의 지적재산만 침해된 것이 아니라, 해당 소프트웨어를 사용하는 고객들도 위험해질 수 있다.

운영자들의 정체에 대해서는 아직 정확히 알 수 없지만 판매 방식에서 셰도우 브로커스(Shadow Brokers)라는 해킹 단체들이 떠오른다고 외신인 블리핑컴퓨터(Bleeping Computer)는 보도했다. 셰도우 브로커스는 2016년 처음 등장해 NSA의 해킹 도구들과 내부 정보를 세상에 공개한 단체다.

보안 전문가 리키 게버스(Ricky Gevers)는 트위터를 통해 현재 솔라릭스 사이트는 러시아의 해킹 그룹인 팬시베어(Fancy Bear)와 코지베어(Cozy Bear)가 애용하는 도메인 등록소인 NJALLA에 호스팅되어 있다고 알렸다. 이 도메인은 만들어진 지 하루밖에 지나지 않았다.

보안 업체 렌디션 인포섹(Rendition Infosec)의 제이크 윌리엄즈(Jake Williams)는 트위터를 통해 "일반적인 사이버 범죄자였다면 재무부나 국방부에서 훔친 첩보들도 같이 판매하겠다고 나서지 않았겠느냐"며 "상업적 특성을 가진 자산들만 따로 떼어내 판매하고 있는 이들의 행태가, 이들의 실존 가능성을 높여주고 있다"고 주장했다.

즉 이들이 제대로 된 사이버 범죄 전문 단체일 가능성이 높다는 것이다. 단순 사기꾼이었다면 재무부와 국방부 등 미국 정부 기관의 정보도 광고함으로써 더 많은 수익을 노렸을 거라는 뜻이다. 윌리엄즈는 "아직 구매한 사람이 없는 것으로 보이며, 공격자가 가격을 낮출 공산이 크다"는 의견도 같이 공개했다.

솔라윈즈 사태로 유출된 정보들을 판매한다는 내용의 솔라릭스 웹사이트 화면

3줄 요약

1. 솔라윈즈 사태로 유출된 정보를 판매하는 사이트 개설됨.
2. MS, 시스코, 파이어아이의 정보 및 소스코드가 판매 중에 있음.
3. 사기꾼일 가능성도 점쳐지는 가운데, 판매 행위가 오히려 신빙성 높여줌.

5 KISA 제6대 이원태 원장 취임 "보안 넘은 국민 안전으로 보안 패러다임 전환"

한국인터넷진흥원 제6대 이원태 원장 취임식 모습[사진=한국인터넷진흥원]

한국인터넷진흥원(원장 이원태, 이하 KISA)은 제6대 이원태 신임 원장의 취임식을 나주본원에서 개최했다. 이원태 원장은 한국인터넷윤리학회 및 한국인공지능법학회 부회장, 개인정보보호위원회 자문위원, 대통령직속 정책기획위원회 정책기획위원, 정보통신정책연구원 연구위원을 역임했으며, 다양한 정책 연구와 경험을 통해 ICT 분야 전반에 대한 높은 전문성과 식견을 겸비했다는 평을 받고 있다.

이원태 원장은 취임사를 통해 "KISA는 정보보호 전문기관으로, 국민이 안전하고 신뢰할 수 있는 디지털 미래사회를 선도하기 위해 최선을 다하고 있다. K-사이버 방역을 기반으로, 사이버 안전망 구축과 개인정보보호, 정보보호 산업 촉진 및 인터넷 서비스 활성화 등 디지털 미래사회를 이끄는 KISA의 일원이 돼, 막중한 사명감과 책임감을 느낀다"고 말했다.

또한, "세계는 코로나19로 인해 지금까지 경험한 적 없는 새로운 패러다임의 전환기에 서 있다. 우리 삶을 이루는 모든 분야가 디지털 · 비대면으로 전환되고 있으며, D.N.A 등 국가 경쟁력의 핵심요소와 결합한 디지털 트랜스포메이션이 일어나고 있다"며, "융 · 복합으로 인해 전 분야로 확대되는 사이버 위협에 대응하고, 디지털 · 비대면 전환 흐름에 발맞춘 인터넷 환경을 조성하며, 데이터 경제 활성화의 기반이 되는 개인정보의 안전한 활용과 보호를 위한 균형점을 찾아야 한다"고 덧붙였다.

이어 "우리는 이러한 변화를 두려워하지 않고, 극세척도의 자세로 KISA의 존재적 가치를 굳건히 세워나가야 한다. 임직원과 함께 KISA를 4차 산업혁명을 완성하는 정보보호 · 디지털 전문기관으로 만들 것이며, 이를 위해 먼저 △보안을 넘은 국민 안전으로 보안 패러다임 전환에 앞장서며 △비대면 전환을 성공적으로 실현하기 위해서 신기술을 기반으로 한 디지털 혁신 생태계를 조성하고 △ICT 및 정보보호 관련 기업, 제품, 기술 등을 육성해 글로벌 경쟁력을 높이고 △조직 내 부패방지, 청렴윤리, 인권존중의 투명한 경영문화를 정착시키겠다"고 말했다.

한편, 이날 취임식은 코로나19에 따른 사회적 거리두기 지침을 준수한 가운데 진행했으며, 직원들은 온라인을 통해 취임식을 시청했다. 다음은 취임사 전문이다.

[한국인터넷진흥원 제6대 이원태 원장 취임사]

존경하는 한국인터넷진흥원 직원 여러분, 제6대 원장으로 취임하게 된 이원태입니다. 반갑습니다.

KISA는 4차 산업혁명 시대를 완성하는 정보보호 전문기관으로 국민이 보다 안전하고 신뢰할 수 있는 디지털 미래사회를 선도하기 위해 매순간 최선을 다하고 있습니다. K-사이버 방역을 기반으로, 사이버 안전망 구축과 국민의 개인정보보호, 정보보호 산업 촉진 및 국민 생활과 밀접한 인터넷 서비스 활성화 등 디지털 미래사회 선도와 정보보호 발전에 핵심적인 역할을 다하고 있는 KISA의 일원이 되어 막중한 사명감과 책임감을 느낍니다. 특히, 그 동안 묵묵히 그 자리에서 소임을 다해주신 직원 여러분의 노고에 깊은 감사를 드립니다.

KISA 가족 여러분, 현재 전 세계는 코로나-19로 인해 지금까지 경험한 적 없는 새로운 패러다임의 전환기에 서 있습니다. 경제 · 산업, 사회 · 문화, 기술 · 정책 등 우리 삶을 이루는 모든 분야가 디지털 · 비대면으로 급속하게 전환되고 있으며, 더 나아가 데이터(Data), 네트워크(Network), 인공지능(AI) 등 국가 경쟁력을 결정짓는 핵심요소와 결합해 디지털 트랜스포메이션(Digital Transformation)이 일어나고 있습니다. 하지만 이러한 변화의 여정은 언제나 다양한 도전에 직면하게 됩니다.

산업의 융 · 복합으로 인해 전 분야로 확대되는 사이버 위협에 대응하는 것, 디지털 · 비대면 전환 흐름에 발맞춘 인터넷 환경을 조성하는 것, 데이터 경제 활성화의 기반이 되는 개인정보의 안전한 활용과 보호를 위한 균형점을 찾는 것이 바로 그것입니다.

KISA 가족 여러분, '극세척도(克世拓道)'라는 말이 있습니다. '많은 어려움에도 불구하고 이를 극복하고 새 길을 개척한다' 는 의미를 담고 있는 사

5 KISA 제6대 이원태 원장 취임 "보안 넘은 국민 안전으로 보안 패러다임 전환"

[한국인터넷진흥원 제6대 이원태 원장 취임사]

자성어입니다. 우리는 지금, 4차 산업혁명과 디지털 대전환이라는 큰 변화의 흐름 속에 있습니다.

처음 가보는 길이기에 그만큼 많은 노력과 혁신이 필요하겠지만, 이를 두려워하지 않고 변화를 기회삼아 극세척도의 자세로 KISA의 존재적 가치를 굳건히 세워나가야 합니다. 저는 여러분과 함께 KISA를 4차 산업혁명을 완성하는 정보보호 · 디지털 전문기관으로 만들고자 합니다.

이를 위한 첫 번째 걸음으로, 먼저 보안 패러다임 전환에 앞장설 것입니다. 4차 산업혁명과 코로나19 등의 영향으로 기존 산업이 ICT 기술과 빠르게 융합하면서 온 · 오프라인의 경계는 허물어지고 있습니다. 이러한 환경에서, 사이버 위협도 그 피해의 정도가 온라인을 넘어, 개인의 생명과 국가 사회에 직접적인 영향을 미치고 있습니다. 따라서 보안의 패러다임도 변화해야 합니다.

보안(Security)을 넘어 국민의 안전(Safety)을 먼저 고려하고 원격교육 · 의료 · 근로, 자율주행차 등 국민 생활과 밀접한 분야에 대한 디지털 안전망을 구축해 나가야 하며, 인공지능(AI) 기술을 적극 도입해 대응체계도 더욱 고도화해야 합니다. 또한, 21세기 원유라 불리는 데이터가 새로운 가치를 창출할 수 있도록 개인정보의 안전한 활용과 정보주체의 권익 보호를 위해, 신(新) 개인정보 보호 환경을 적극적으로 조성해 나가야 합니다.

두 번째로는 디지털 국가 경쟁력 제고에 힘쓰겠습니다. 비대면 전환을 성공적으로 실현하기 위해서는 인공지능(AI), 5G 등 신기술을 기반으로 한 디지털 혁신 생태계 조성이 필요합니다. 블록체인 기술 활용, 전자서명 이용 편리성 제고 등을 통해 초연결 · 비대면 기반을 조성하고, 핀테크 · 전자문서 확산 등 비대면 사회가 요구하는 혁신적인 서비스를 발굴해 국민이 체감할 수 있는 편리한 디지털 인프라를 구축하도록 하겠습니다.

이와 함께, ICT 및 정보보호 관련 기업과 제품, 기술 등을 집중 육성, 국내의 우수한 기술과 인력이 세계 시장을 주도하도록 하겠습니다. 이러한 노력들을 통해, 우리나라가 포스트 코로나 시대 디지털 대전환의 우수사례로 인정받을 수 있도록 하겠습니다. 마지막은 뉴 노멀 시대에 맞는 선도적 기관으로 진화하는 것입니다.

시대는 급변하고 있고, 변화하는 시대에 따라 KISA에 거는 국민의 기대는 그 어느 때보다 커져있습니다. 전문가다운 역량뿐 아니라, 지역이전 공공기관으로서 국가 균형발전을 위한 책무를 다하고, 국민과 상생하는 사회적 가치와 혁신 경영을 실현해야 합니다.

이를 위해 조직 내 부패방지, 청렴윤리, 인권존중의 투명한 경영문화를 정착시켜 국민의 신뢰를 높이고, 노동존중에 기반한 노사협력을 통해 조직원들의 내부 만족도를 제고하고 구성원의 다양성을 존중하는 열린 경영을 실천하겠습니다. 특히, 노동조합은 경영의 중요한 파트너입니다. 보다 적극적으로 노사 간 대화의 장을 만들어 나가겠습니다. 또한, 지역이전 공공기관으로서 우리 원이 위치하고 있는 광주 · 전남지역과의 협력은 물론, 현재 전국 10개소의 정보보호 지원센터의 역할 확대를 통해 명실상부하게 지역사회와 밀착, 소통하는 KISA를 만들겠습니다.

뿐만 아니라, 단순한 연공서열이 아닌 직무중심의 인사 · 보수체계를 통해 직원 한명 한명의 역량을 키워 조직의 효율성을 끌어올리도록 노력하겠습니다.

존경하는 KISA 가족 여러분, 자기에게 주어진 모든 일을 정성과 믿음으로 다하면 성과는 물론, 타인도 나를 믿고 신뢰하게 됩니다. 우리는 4차 산업혁명과 포스트 코로나 시대 등 변화하는 환경에 맞서 국민이 안전하고 신뢰할 수 있는 디지털 미래사회를 선도해야 할 과제를 안고 있습니다. 다시 말해 우리가 주어진 과제를 정성을 다해 잘 해결한다면 동료, 더 나아가 국민이 우리를 믿고 신뢰할 수 있다는 뜻입니다.

이를 위해 저부터 앞장서겠습니다. 여러분들과 함께 지금의 위기를 넘어 새로운 시대를 열 수 있도록 최선을 다하겠습니다. 패러다임의 변화에 대응해 KISA를 정보보호 및 디지털 분야에서 명실공히 세계 최고의 전문기관으로 거듭날 수 있도록 최선의 노력을 다하겠습니다.

끝으로 따뜻한 환대에 깊은 감사를 드리며, 무거운 책임감을 갖고 KISA와 국민으로부터 신뢰와 지지를 얻을 수 있도록 최선을 다하겠습니다. 감사합니다.

3줄 요약

1. 4차 산업혁명 및 디지털 미래사회 실현을 위한 KISA 역할 강조
2. 보안을 넘은 국민 안전으로의 보안 패더라임 강조
3. 보안뉴스의 최초 보도 이후, 이원태 원장 내정 공식화

에디터 코멘트

신임 원장 임명이 늦어져 설왕설래가 많았던 한국인터넷진흥원(KISA) 원장에 이원태 정보통신정책연구원 연구위원이 임명됐는데요, 〈보안뉴스〉의 최초 내정 보도 이후, 이원태 원장이 SNS(페이스북)을 통해 내정 사실을 밝히면서 내정이 공식화됐습니다. 인터넷 · 정보보호 전문기관으로 보안 분야에 있어 KISA가 갖는 위치와 역할이 매우 중요한 만큼 앞으로도 큰 기대를 해봅니다. 특히, 정보보호는 물론 인공지능, 인터넷윤리 등 ICT 전반에 걸쳐 식견을 보유했다는 평가를 받고 있어 조직에 새로운 바람을 불어넣을 것이라는 기대도 있습니다.

트럼프 지지자들의 의회 점거, 정보보안 문제도 불거져

지난 주 성난 트럼프 지지자들의 의회 점거 사태가 전 세계적인 충격을 준 가운데, 해당 사건의 사이버 보안 문제도 제기되고 있다. 의회 내부에 있던 이들이 빠르게 대피를 할 수밖에 없던 상황에서 컴퓨터를 미쳐 다 끄지 못하고 나가는 바람에 각종 민감 정보 및 기밀들이 노출되었기 때문이다. 이메일이 열려 있던 의회 내 컴퓨터 화면이 트위터에 돌아다니고 있으며, 이 때문에 이제 사이버 보안이 물리적인 공격도 고려해야 한다고 전문가들은 주장하고 있다.

https://www.securityweek.com/experts-weigh-cybersecurity-risks-capitol-attacks

솔라윈즈 공격자들, 솔라윈즈만 활용한 것 아니다

미국 국토안보부 산하 CISA가 솔라윈즈 사태에 대해 새로운 사실을 발표했다. 공격자들이 기본적이고 평범한 해킹 기술을 사용해 여러 조직을 공격하기도 했다는 것이다. 즉 솔라윈즈의 업그레이드 파일을 감염시켜서 침투하는 공급망 공격 외에도, 비밀번호 추측 및 대입, 비밀번호 스프레잉(password spraying)과 같은 기법을 사용해가며 표적들을 공략했다고 한다. 공격자들이 특정 목표를 정해두고 모든 수단과 방법을 총 동원했다는 것이다.

https://findbiometrics.com/solarwinds-hackers-guessed-passwords-cisa-701081/

뉴질랜드의 중앙은행, 사이버 공격에 민감한 정보 잃어

뉴질랜드의 중앙은행이 주말 동안 사이버 공격에 당했다. 공격이 주로 발생한 곳은 서드파티 파일공유 서비스라고 한다. 이를 통해 은행 측은 그 동안 중요하고 민감한 정보를 저장하고 유통했으며, 따라서 여기에 접근한 해커들이 꽤나 중요한 정보를 가져갔을 가능성이 높다. 현재 은행 측은 조치와 복구를 모두 마무리했고, 은행은 정상적으로 돌아가는 중이라고 한다. 다만 공격자들이 현재 어떤 정보에 접근했고, 정확히 얼마나 가져갔는지를 파악 중에 있다.

https://www.dw.com/en/new-zealand-central-bank-hit-by-cyberattack/a-56184575

팀TNT 봇넷, 이제는 도커 API와 AWS 크리덴셜도 훔친다

암호화폐, 특히 모네로 채굴을 전문으로 하던 봇넷 멀웨어인 팀TNT(TeamTNT)가 최근 업그레이드 됐다고 보안 업체 트렌드 마이크로(Trend Micro)가 발표했다. 이 봇넷은 이제 도커 API와 AWS의 로그인 크리덴셜도 훔친다고 한다. 현재까지는 컨테이너 플랫폼들만 팀TNT의 공격에 노출되어 있는데, 주로 악성 컨테이너 이미지를 퍼트리는 방법으로 공격이 진행되고 있다고 한다.

https://drdonysnews.com/teamtnt-botnet-now-steals-docker-api-and-aws-credentials/

파이어폭스와 크롬에서 치명적인 버그 발견돼

CVE-2020-16044(파이어폭스)와 CVE-2020-15995(크롬)이라는 취약점을 패치하라고 미국 국토안보부 산하 CISA가 직접 권고문을 발표했다. 전자는 UaF 취약점으로 데스크톱 버전 84.0.2, 안드로이드 버전 84.1.3에서 발견된다고 한다. 후자는 현재의 87.0.4280.141 버전 크롬에서 발견되고 있다. 보안 업체 테너블(Tenable)은 이 두 가지 모두가 치명적 위험도를 가지고 있다고 주장했지만 구글과 마이크로소프트는 고위험군으로 분류했다.

https://www.ehackingnews.com/2021/01/critical-bugs-in-firefox-and-chrome.html

솔라윈즈 공격의 배후에 털라가 있을 가능성 높다

보안 업체 카스퍼스키가 솔라윈즈 공격자들과 털라(Turla)라는 유명 APT 단체 사이에 연관성이 있다고 주장했다. 털라는 주로 외교 시설들을 정탐하는 해킹 단체로, 러시아의 외교 첩보 서비스국인 FSB와 깊은 연관성이 있는 것으로 알려져 있다. 그렇다고 '털라가 범인이었다'고 단정 지을 단계는 아니고, 수사를 더 이어갈 계기가 마련된 정도라고 카스퍼스키는 정리했다.

https://www.cyberscoop.com/turla-solarwinds-kaspersky/

400GB 넘는 소셜미디어 프로파일 정보 노출 돼

2억 1400만 명의 소셜미디어(페이스북, 링크드인, 인스타그램 등) 사용자들의 프로파일 정보가 한꺼번에 노출되는 일이 발생했다. 용량으로 치면 400GB가 넘는다고 한다. 이는 중국 회사 소셜악스(SocialArks)가 스크래핑을 통해 수집한 데이터로, 클라우드 설정을 잘못해서 이 사단이 벌어졌다. 소셜악스는 광고 및 마케팅을 전문으로 하는 기업으로 알려져 있으며, 스스로는 소셜미디어 관리 전문 업체라고 설명하고 있다.

https://www.techtimes.com/articles/255831/20210111/over-400gb-of-214-million-social-media-users-have-been-exposed-by-misconfiguration-from-chinese-company-socialarks.htm

솔라윈즈 공격에 당한 파이어아이, 러시아로부터 엽서 받아

얼마 전 솔라윈즈(SolarWinds) 해킹 사태의 피해자가 되었던 보안 업체 파이어아이(FireEye)에서 새로운 소식이 나왔다. 누군가 CEO인 케빈 맨디아(Kevin Mandia)에게 엽서를 보냈다는 것이다. 그것도 자택으로 발송된 것이었다. 엽서에는 파이어아이의 로고와 만화가 담겨져 있었다. 솔라윈즈 해킹 사태의 범인이 러시아라고 하는 주장을 조롱하는 내용의 만화였다. 러시아에서 온 엽서로 보이며, 파이어아이를 조롱하는 것이 목적인 듯하다.

https://grahamcluley.com/russia-linked-postcard-was-sent-to-fireeyes-ceo-after-cybersecurity-firm-uncovered-hack/

IT 업체 유비퀴티에서 정보 유출 사고 발생

대형 네트워크 장비 판매 업체인 유비퀴티(Ubiquiti)에서 고객 정보가 유출되는 사고가 발생했다. 해당 내용이 월요일에 고객들에게 짧은 메일로 통보됐다. 누군가 유비퀴티의 서드파티 클라우드 업체에 저장되어 있던 디지털 자원에 접근했다는 것이 주요 내용이었다. 아직 해당 클라우드 업체의 이름과 보안 사고의 원인에 대해서는 별다른 설명이 없다. 고객 데이터는 무사하다고 하는데, 매체에 따라 고객 정보가 유출되었다고 헤드라인이 걸린 곳도 있다.

https://techcrunch.com/2021/01/11/ubiquiti-says-customer-data-may-have-been-accessed-in-data-breach/

소셜 엔지니어링 공격자들, 이제 외계인과 UFO를 동원해

미국 국방부가 6개월 후에는 UFO에 대해 자신들이 알고 있는 모든 정보를 공개할 예정이다. 여기에다가 블랙 볼트(Black Vault)라는 사이트에서 CIA가 가지고 있는 UFO와 외계인 관련 정보들을 공개하면서 적잖은 화제가 되고 있기도 하다. 미국 사회에서 이 두 가지 건의 타이밍이 묘하게 겹치는 바람에 UFO에 대한 관심이 고조되고 있는데, 이를 피싱 공격자들이 놓칠리가 없다. '외계인 정보' 혹은 'UFO 관련 새 소식'이라는 제목으로 피해자들을 늘리고 있다고 한다.

https://threatpost.com/aliens-ufos-frontier-social-engineers/162939/

랜섬웨어와 싸우는 인텔의 새 프로세서, vPro

인텔이 11세대 코어 vPro 모바일 프로세서에 랜섬웨어 보호 기능을 탑재했다. 사용자 경험을 훼손하지 않은 상태에서 보안성과 가시성을 하드웨어 층위에서 높이겠다는 것이 인텔의 목표라고 한다. 그 외에도 이번 모바일 프로세서는 고성능을 요하는 업무 환경에도 적합하도록 설계되었다고 한다. 랜섬웨어가 변화무쌍하게 진화하고 있기 때문에, 그에 대한 방어 체제도 계속해서 변하고 두터워져야 한다고 인텔은 강조했다.

https://www.darkreading.com/threat-intelligence/intels-new-vpro-processors-aim-to-help-defend-against-ransomware/d/d-id/1339873

해커들, 솔라윈즈 사태로 유출된 소스코드 판매한다

지난 주 마이크로소프트는 "솔라윈즈(SolarWinds) 해킹 사태의 공격자들이 일부 소프트웨어의 소스코드를 열람했다"고 발표했었다. 그런데 얼마 전 다크웹에 누군가 윈도 10 소스코드를 60만 달러에 팔겠다고 나섰다. 이 판매자는 과거 NSA의 자료를 경매로 판매했던 해킹 그룹 셰도우 브로커스(Shadow Brokers)로 보인다고 한다. 하지만 아직까지 이들이 정말로 윈도 10 소스코드를 보유하고 있다는 명확한 증거는 없는 상황이다.

https://mspoweruser.com/microsoft-windows-10-source-code-leak/

구글, 윈도와 안드로이드 노린 고급 해킹 작전 적발해

구글이 2020년 초기에 발견하고 현재까지 추적해 온 해킹 작전에 대한 보고서를 발표했다. 이 작전은 안드로이드와 윈도 사용자들을 노린 것으로, 주로 워터링 홀(watering hole)이라는 공격 기법이 활용되었다고 한다. 또한 공격자들은 크롬의 취약점들을 익스플로잇 함으로써 피해자들의 장비에 최초 침투했다. 그런 후에는 OS를 익스플로잇 해 보다 높은 권한을 가져갔다고 한다. 현재는 공격에 활용되고 감염된 서버들을 격리시킨 상태라고 한다.

https://techandsciencepost.com/news/tech/smartphones/google-reveals-sophisticated-windows-and-android-hacking-operation/

마임캐스트의 인증서 활용한 MS 365 이메일 해킹 사건

고급 해킹 기술을 가진 자들이 정찰 공격을 실시하기 위해 마임캐스트의 인증서를 활용해 MS 365 이메일에 침투하는 사건이 벌어졌다. 마임캐스트 인증서를 활용하면 마이크로소프트 365 계정들을 통해 마임캐스트 서버에 접속할 수 있는데, 공격자들이 이를 노린 것이다. 이번에 문제가 된 서버는 마임캐스트의 싱크(Sync)와 리커버(Recover)라는 서버들이라고 한다.

https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/

고약한 안드로이드 멀웨어 들고 돌아온 해킹 그룹

트라이앵귤럼(Triangulum)이라는 해커이자 멀웨어 개발자가 돌아왔다. 이번에는 새로운 멀웨어를 들고 왔다. 이 멀웨어는 이미 해킹 포럼에서 거래되고 있다고 한다. 트라이앵귤럼은 25세의 인도 남성으로 알려져 있는데, 트라이앵귤럼은 2017년부터 멀웨어를 만들어 해킹 포럼에서 판매하기 시작했다. 판매되고 있는 멀웨어는 기본적으로 암호화폐 채굴 도구인데, 키로거 등을 묶어서 팔기도 한다. 또한 트라이앵귤럼은 광고에 공을 많이 들인다는 특징을 가지고 있다.

https://www.hackread.com/malware-vendor-nasty-android-malware/

MS, 83개 보인 픽스 발표했지만

2021년 첫 패치 튜즈데이가 시작됐다. 이번 달에 다뤄진 취약점은 83개다. 지난 주에 MS는 에지 브라우저에서 발견된 13개 취약점을 이미 패치한 바 있다. 10개의 취약점은 치명적 위험도를 가진 것으로, 나머지 73개는 '중요' 등급에 해당되는 것으로 분류됐다. 패치되기 전에 이미 알려진 취약점인 CVE-2021-1648에 대한 패치가 시급하며, 공격자들이 벌써부터 익스플로잇 하고 있는 CVE-2021-1647 역시 높은 순위를 차지해야 한다. CVE-2021-1647은 윈도 디펜더에서 발견된 취약점이다.

https://www.theregister.com/2021/01/12/patch_tuesday_fixes/

UN의 보안 취약점 통해 10만 명 직원 기록들 노출돼

유엔환경프로그램(UNEP)의 시스템들에서 취약점이 발견됐다. 이를 통해 시스템에 접근할 경우 10만 명 UN 직원들의 비밀 기록들을 열람할 수 있다고 한다. 직원들의 ID, 이름, 소속 단체, 출장 기록, 근무 시작일과 퇴사일 등 상세한 정보들이 여기에 포함되어 있어 정교한 스피어피싱 공격을 기획하고 실행하는 게 가능하다고 한다.

https://www.darkreading.com/threat-intelligence/united-nations-security-flaw-exposed-100k-staff-records/d/d-id/1339882

뉴질랜드 중앙은행 해킹 사건, 액셀리온부터 시작됐다

얼마 전 뉴질랜드 중앙은행에서 해킹 사고가 발생했었다. 조사 결과 액셀리온(Accellion)이라는 파일 전송 시스템에서부터 침해가 시작되었다는 것이 밝혀졌다. 즉, 서드파티를 통한 침해 사건이라는 뜻이다. 뉴질랜드 중앙은행 측은 공격자가 처음부터 중앙은행을 노린 게 아니라며, 액셀리온의 여러 고객들에서도 침해의 흔적이 발견됐다고 발표했다.

https://www.itnews.com.au/news/accellion-hack-behind-reserve-bank-of-nz-data-breach-559642

틱톡, 10대 사용자들의 계정을 '비공개'로 전환한다

작년 한 해 프라이버시 논란에 휘말렸던 틱톡이 13~15세 사용자들의 계정을 '비공개'로 전환한다고 발표했다. 물론 이는 '디폴트 옵션'의 이야기다. 즉 사용자가 이를 공개로 전환할 수 있다는 것이다. 하지만 사용자가 옵션 조정을 하지 않을 경우, 틱톡에 업로드하는 모든 콘텐츠는 일부 사용자들에게만 공유된다.

https://threatpost.com/tiktok-teen-accounts-private/163040/

솔라윈즈 공격자들, 마임캐스트도 공격했을지 모른다

어제 마임캐스트의 인증서가 침해되었다는 사실이 발표됐었다. 그런데 이 사건이 솔라윈즈 사태와 연관성이 있을 가능성이 높다는 의혹이 제기되었다. 공격 전술과 도구가 상당히 유사하다는 것이다. 게다가 마임캐스트는 솔라윈즈의 고객사이기도 했다. 다만 솔라윈즈 사태가 발생하고 나서 마임캐스트는 솔라윈즈를 사용하지 않게 된 것으로 알려져 있다. 마임캐스트 역시 솔라윈즈 피해자 목록에 올라갈까?

https://www.wsj.com/articles/solarwinds-hackers-attack-on-email-security-company-raises-new-red-flags-11610510375

플로리다 주의 최초 윤리담당관, 사이버 스토킹으로 체포돼

미국 플로리다 주 탤러해시 시에서 최초로 윤리담당관으로 임명되었던 공무원이 사이버 스토킹 혐의로 체포됐다. 윤리담당관의 임무는 시 공무원들을 대상으로 윤리 교육을 하는 것이었다. 스토킹 대상은 같은 시 공무원이자, 그녀를 고용한 상관이었다. 둘은 불륜을 저지르다가 발각돼 시로부터 처벌을 받았고, 그래서 잠시 떨어져 지냈는데 그 동안 계속해서 협박 전화와 문자를 상관에게 보냈다고 한다. 그 후로도 연락은 계속해서 이어졌고 이에 고발할 수밖에 없었다고 한다.

https://www.infosecurity-magazine.com/news/former-florida-official-charged/

화이자 백신 데이터, 유출됐나

화이자와 바이오앤테크가 개발한 코로나 백신 데이터가 유출된 것으로 보인다. 지난 12월 유럽 의약청에 해킹 공격이 발생했는데, 그 때 일이 벌어졌다고 한다. 그리고 그 백신 관련 정보가 이메일 스크린샷, 동료 평가 자료, PDF 문건 등의 형태로 온라인에 공개되었다. 아직까지 공격자들의 정체와 배후 세력에 대해서는 아무 것도 알 수가 없는 상태다.

https://www.computerweekly.com/news/252494741/Stolen-Pfizer-BioNTech-Covid-19-vaccine-data-leaked

- **영국에서는 현재 5명 중 1명 꼴로 코로나에 감염되어 있다는 통계가 나오고 있다.** 이는 1240만 명 정도가 현재 감염되어 있다는 뜻인데, 확정적인 숫자는 아니고 추정치다. 이는 현재 영국 정부가 발표하는 확진자 수에 비해 5배 많은 것으로, 정부는 이미 드러난 감염자들만을 집계했기 때문에 작은 숫자가 나오는 것이고, 이번 통계는 숨어 있는 감염자들의 규모를 추정한 것이라 이러한 차이가 발생한다. 일부 전문가들은 5배가 아니라 8배까지 차이가 있을 수 있다고 보고 있다.

- **영국 변종이 기존 백신들 혹은 코로나 감염 경험으로 생성된 면역 체계를 파괴하거나,** 이를 무시하고 질병을 확산시킬 가능성이 매우 낮다는 실험 결과가 발표됐다. 즉 기존 백신을 맞으면 영국발 변종에도 대처가 가능하다는 것으로, 약 0.5%의 경우만 변종에 의한 재발 위험에 노출되어 있다고 한다. 아직 남아공발 변종에 대한 실험 결과는 나오지 않고 있다.

- **브라질에서의 코로나 사망자 수가 20만 명을 넘어섰다.** 그런데도 브라질인들 상당수가 여전히 파티를 즐기고 있으며, 각종 모임이 끊이지 않고 있다고 한다. 이 때문에 바이러스 확산을 막을 수 없어 일부 브라질인들 사이에서 이러한 파티 및 모임 참석자들에 대한 비판이 퍼져나가고 있다. 그러면서 파티 사진이 온라인에 올라오면 비판의 댓글을 다는 '운동'이 이어지고 있다고 한다. 운동가들은 코로나가 아니라 바보 바이러스가 브라질에 퍼지고 있는 듯하다고까지 발언의 수위를 높이고 있다.

- **필리핀의 두테르테 대통령의 수상한 행보가 이어지고 있다.** 야당 의원들에 의하면 최근 두테르테는 중국으로부터 코로나 백신을 밀수입했으며, 이를 자신의 경호원들에게 모두 맞도록 지시했다고 한다. 또한 필리핀에서 일하는 10만 명의 중국 노동자(대부분 카지노에서 일하는 사람들)들도 접종하도록 했다는 주장도 나오고 있다. 이러한 의문들을 두테르테는 묵살하고 있으며, 경호원들에게도 입을 다물 것을 명령했다.

- **중국 상무부가 최근 해외 기업들에 적용될 새로운 규정을 발표하고 곧바로 시행하기 시작했다.** 미국의 규정을 따르는 기업들에 대하여 중국 정부나 기업들이 법원에 고소할 수 있도록 한 것이다. 미국의 규정이란, 미국 기술을 화웨이 등과 같은 중국 기업들에 판매하지 못하도록 한 것을 말한다. 또한 중국 군과 함께 신장의 소수민족들을 탄압하는 데 일조한 기업들도 처벌하도록 했다. 파트너사가 이 규정을 지키는 것 때문에 중국 기업이 손해를 봤을 때 법원에서 손해 배상을 청구할 수 있게 된다. 승소 가능성이 높을 것으로 예상된다.

- **보잉 비행기가 또 다시 추락했다.** 인도네시아의 수리위자바 항공에서 운영하던 낡은 보잉 737 클래식(Boeing 737 Classic)이 자바해로 떨어진 것이다. 여러 자료에 의하면 비행기는 20초 만에 3천 미터 밑으로 가라앉았다고 하는데, 이렇게나 빠르게 가라앉는 건 엔진 결함이나 조종사 혼미 상태, 악천후 등으로 인해서는 좀처럼 발생하지 않는다고 한다. 따라서 기내에서 뭔가 큰일이 벌어진 것이 아닐까, 전문가들은 의심하고 있다. 62명이 사망했다.

- **트럼프 대통령 지지자들의 국회 점거 사건 이후** 트럼프가 소속된 공화당 내에서도 트럼프의 퇴임(탄핵)을 주장하는 의원들이 나오기 시작했다. 유럽연합의 외교 담당 집행위원인 조셉 보렐(Joseph Borrell)은 이 사건을 두고 '민주주의의 위기'라고 평했다. 민주주의가 계속해서 썩어가도록 놔뒀을 때, 또한 가짜뉴스가 온라인에서 퍼져가는 걸 막지 않았을 때 어떤 일이 벌어지는지를 잘 드러낸 사건이라고 그는 자신의 블로그에 썼다.

- **한국에서도 한파가 이어지는 가운데,** 스페인에서도 수십 년만에 폭설이 필로메나(Filomena)라는 폭풍과 함께 찾아와 스페인 전역이 마비되다시피 했다. 이 사태로 최소 4명이 사망했다. 스페인 정부는 격지로 코로나 백신과 음식 등을 공급하기 위해 군 호송 차량을 동원해야만 했다. 추위는 계속 이어질 전망이라, 스페인으로서는 기록적 추위에 속하는 −10℃가 이번 주 내 기록될 것으로 보인다.

- **중국의 코로나 백신인 시노백(Sinovac)을 공급받기로 했던 인도네시아가 접종을 시작하기 전 자체 백신 검사를 실시했다.** 그리고 65%의 효과를 가지고 있다고 발표했다. 하지만 상황이 긴급한지라 이를 승인했다. 이로써 인도네시아는 시노백을 승인한 두 번째 나라가 되었다. 첫 번째는 중국이다. 브라질과 터키에서도 시노백에 대한 검사가 진행됐고, 더 좋은 결과가 나왔지만 아직 승인이 되지는 않았다.

- **모더나가 자사 백신으로 생기는 코로나 면역력이 최소 1년은 간다고 발표했다.** 또한 2021년 동안 최소 6억 회분에서 최대 10억 회분의 백신을 생산할 계획이라고도 설명했다. 이처럼 여러 회사들에서 다양한 백신을 만들어 접종이 시작됐지만, WHO는 집단 면역력이 2021년에는 생겨나지 않을 전망이라고 발표했다.

- **미국 농무부가 2020년 세계 식품 생산량을 발표한다.** 정확한 수치가 나오지는 않았지만 곡물 생산량이 신기록을 수립하거나, 그에 준하는 호성적이 기대되고 있다. 그러나 코로나로 인해 이런 풍부한 식품들이 제대로 배포 및 보급되지 않았기 때문에 세계 기아 문제는 더 심각해졌다. 유엔세계식량계획이 작년 11월에 발표한 바에 따르면 전 세계적으로 1억 3700만 명이 당장 먹을 것이 없는 상황이라고 한다. 이는 코로나 전에 비해 82% 증가한 수치다.

- **텍사스 연방 교도소에 갇혀 있는 리사 몽고메리라는 재소자의 사형 집행이 오늘 있을 예정이다.** 집행은 작년 12월에 있을 예정이었으나 변호사가 코로나 확진자가 되는 바람에 미뤄졌었다. 미국에서는 17년만의 사형 집행이 될 예정이다. 사실상 폐지되었던 사형 집행을 부활시킨 것이 트럼프 대통령인데도 몽고메리라는 인물의 범죄가 워낙 극악무도해서 사형 집행에 대한 반론이 크게 나오지 않고 있다.

- **정권 합리화와 찬양을 멈출 수 없는 중국 정부가, 드디어는 코로나 19 발발 1주년을 기념하는 무리수를 저질렀다.** 우한에서의 첫 락다운 사태를 기념하고, 이것이 코로나에 대한 중국 정부의 승리를 견인했다고 발표하며, 관련 조형물을 우한 박물관에 전시했다. 각종 홀로그램까지 동원되는 등 이 잔망스러운 거짓 행사에 투자도 아끼지 않은 모습이다. 하지만 WHO의 코로나 기원 조사 팀을 입국시키기로 결정하기도 했다.

- **미국 캘리포니아 주에서만 코로나 사망자가 1년 동안 3만 명을 넘어섰다는 존스홉킨스 대학의 발표가 있었다.** 특히 10월부터 사망자가 극심하게 늘어났는데, 지난 한 달 동안에만 1만 명의 사망자가 나왔다고 한다. 지난 주에는 하루 평균 사망자가 476명이었다. 그럼에도 아직까지 최악의 사태가 오지 않았다고 전문가들은 말한다. 아직 연말연시의 여파가 나타나지 않았기 때문이다.

- **미국 코로나가 얼마나 심한지, 샌디에고 동물원의 고릴라도 코로나 확진 판정을 받았다.** 몇 마리는 이미 기침을 하는 등 코로나의 증상을 보이고 있다고 한다. 고릴라가 확진 판정을 받은 건 이번이 처음인 것으로 알려져 있다. 고릴라를 담당하는 사육사 중에 코로나 확진자가 있어, 이를 통해 고릴라들이 감염된 것으로 당국은 보고 있다. 현재까지 컨디션 자체는 나빠 보이지 않는다고 한다.

- **미국 하원 내 민주당 의원들이 트럼프 대통령의 탄핵을 위한 소추안을 완성시켰다.** 반란을 선동했다는 것이 이 문건의 주요 내용이며 주장이다. 공화당 의원들은 부통령인 마이크 펜스에게 수정헌법 25조를 적용해 트럼프 대통령을 사퇴시키라고 요구했다. 미국 현지 시각으로 화요일 트럼프 대통령의 거취를 놓고 하원 전체의 투표가 있을 예정이다.

- **프랑스의 마크롱 대통령이 아프리카 사헬 지역에 150억 달러를 투자하여 '녹색 만리장성'을 쌓겠다고 발표했다.** 빠르게 진행되고 있는 사막화를 막기 위한 것이라고 한다. 총 4년짜리 프로젝트로 계획하고 있으며, 예상대로 진행될 경우 1천만 명에게 일자리를 제공하고, 1억 헥타르의 땅이 복구되며, 2억 5천만 톤의 이산화탄소를 억제할 수 있을 것이라고 한다.

- **폼페이오 미국 국무부 장관이 예멘에서 반정부 활동을 6년째 벌이고 있는 후티스(Houthis)라는 단체를 테러리스트 조직으로 지명하겠다고 발표했다.** 이렇게 함으로써 후티스를 지원하는 이란의 악성 행위를 제한시킬 수 있으리라고 설명하기도 했다. 하지만 인권단체들이 일제히 반발하고 나섰다. 후티스가 점령하고 있는 지역에서 인도주의적 활동을 할 수 없게 되기 때문이다. 한편 쿠바는 테러리즘 지원국 명단에 다시 이름을 올렸다.

- **일본의 스가 총리가 코로나 확진자가 급증하자 이를 막기 위해 최소 세 개 현에서 비상사태를 선포했다.** 일본에서는 지난 월요일 하루 동안에만 4900명의 확진자가 나왔다. 현 의료 시스템으로 감당하기 힘든 상황으로 치닫고 있다. 말레이시아에서는 50년 만에 처음으로 국가 비상 사태가 선포됐다. 캐나다 온타리오 주도 의료 시스템 붕괴 직전이라 비상 사태를 선포했다.

- **독일은 현재 시행 중인 락다운 체제를 8~10주 연장할 것으로 보인다.** 네덜란드 역시 다음 달까지로 락다운을 연장한다. 두 나라의 수장들은 지금 코로나를 잡지 못하면 봄 전까지 확진자가 10배 이상 늘어날 수 있다고 락다운 연장의 이유를 설명했다. 두 나라는 최고 수준의 락다운을 시행 중에 있으며, 절대적으로 필요한 사회 기반 시설과 서비스가 아니면 전부 문을 닫고 있다. 그럼에도 계속해서 하루 확진자 수가 기록을 갱신 중에 있다.

- **인도네시아가 드디어 코로나 백신 접종을 시작한다.** 제일 먼저는 대통령이 주사를 맞고, 그 다음은 전국 130만 명의 의료진이 접종 대상이 된다. 의료진 다음은 의외로 젊은 생산 연령 인구 층이다. 보통 백신을 시작한 다른 나라들에서는 고연령자들의 접종을 서둘렀었다. 인도네시아 정부는 중국의 시노백이 고연령자들에게도 효과적이라는 데이터가 부족하다며 젊은 층부터 접종하기로 결정했다.

- **WHO의 연구원들이 중국에 도착했다.** 코로나 바이러스의 기원을 찾기 위해서다. WHO는 "이번 연구가 중국의 책임을 묻기 위한 것이 절대 아니"라는 것을 거듭 강조했다. 이들의 첫 번째 연구 목적은 우한을 방문해 중국 과학자들과 교류하면서 아직 연구되지 않은 샘플을 찾아내고, 이를 통해 코로나의 미스터리를 푸는 것이라고 한다. 바이러스가 종의 장벽을 넘어 인간에게 전파된 경로를 찾아내는 것도 중요한 목표다.

- **캘리포니아 주가 디즈니랜드를 대량 백신 배포처로 활용할 계획임을 발표했다.** 연일 전날보다 더 많은 확진자가 나오고, 현재 병실들 및 각종 병원 시설들이 부족한 상황에서 캘리포니아 주 측에서는 다섯 곳의 시설을 대량 배포처로 지정할 예정이다. 디즈니랜드는 이 다섯 곳 중 첫 번째다.

- **트럼프 대통령이 의회 폭동 사건에 대해 자신의 책임은 하나도 없다고 주장했다.** 하지만 그는 폭동 사건이 일어나기 전, 자신의 지지자들 앞에서 "선거에서 승리한 건 나"이며, "따라서 의회로 가서 강력하게 의사를 표명하라"고 연설했었다. 또한 탄핵 소추안을 두고 "미국 정치 역사에 있어 최악의 마녀 사냥"이라고 비판했다. 소추안에 대한 하원의 투표는 오늘 진행된다.

- **테러가 끊이지 않는 아프가니스탄에서는 자신의 이름과 혈액형, 친인척의 전화번호가 적힌 노트를 주머니에 넣어가지고 다니는 사람들이 늘어나고 있다고 한다.** 언제 무슨 폭탄이 터져 죽거나 심각한 부상을 입을지 모르기 때문이다. 이들에게 있어 자살 폭탄 테러는 너무나 일상 가까이에 있는 위협이다.

- **중국의 한 배달부가 급여가 미지불 되는 것에 대해 항의하기 위해 분신을 시도했다.** 그는 3도 화상을 입은 채 목숨을 건졌다. 이 사람은 Ele.me라고 하는 회사에서 배달을 담당하고 있는데, Ele.me는 거대 기업인 알리바바가 소유한 음식 배달 서비스 전문 업체다. 중국에서는 배달 종사자들의 관리와 처우 개선이 큰 사회적 문제로 떠오르고 있다.

- **프랑스 법원이 방글라데시 남성 한 명을 강제 추방하려다가 이를 철회했다.** 그가 천식에 걸린 상태인 데다가, 방글라데시는 공기 오염 상태가 세계에서 손꼽힐 정도로 심각한 나라이기 때문이다. 방글라데시로 돌아가면 천식이 더 심각해질 것이라는 변호사들의 주장이 법원에서 통한 것이다. 환경적 요인으로 법원이 추방령을 철회한 건 프랑스 역사상 처음이다.

- **아일랜드의 보육원에서 무슨 일이 일어난 걸까?** 1922년부터 1998년까지 미혼모들과 아이들을 돌보았던 여러 보육 시설들에서 아동들의 사망률이 지나치게 높았다는 조사 결과가 나왔다. 무려 15%의 아동들이 이러한 시설들에서 심각한 학대 행위와 영양 부족으로 죽었다고 한다. 아일랜드 정부는 상세 조사 결과를 3천여 페이지에 걸쳐 발표했으며, 아일랜드 역사의 수치와 어두운 단면이라고 묘사했다.

- **미국 하원에서 트럼프 대통령의 탄핵안이 가결됐다.** 민주당 측 의원들은 당연히 전부 찬성 투표를 던졌고, 여기에 공화당 의원 10명도 합세했다. 이제 이 탄핵 소추안은 상원으로 올라간다. 하지만 상원 회의는 1월 19일까지 휴정된 상태다. 1월 20일은 바이든 대통령이 공식 취임하는 날이다. 트럼프는 미국 역사상 처음으로 임기 중 2번 탄핵된 대통령이 되었다.

- **이에 뉴욕 시는 '트럼프 그룹'과의 계약을 해지했다.** 트럼프 그룹은 뉴욕 시에서 아이스 스케이트 링크, 캐러셀, 골프장 등을 운영해왔다. 뉴욕 시와 트럼프 그룹은 회사 경영진이 범죄 활동에 연루되었을 때 계약을 일방적으로 해지할 수 있다고 상호 약속해 왔는데, 뉴욕 시장인 빌 드 블라시오(Bill de Bliasio)는 이번 의회 점거 사건의 배후에 트럼프가 있고, 이는 중대한 범죄임이 분명하다며 결정의 이유를 밝혔다.

- **유럽 국가들 일부가 보다 엄격한 락다운을 실시하겠다고 발표했다.** 이탈리아는 국가 비상 사태를 4월까지 유지하기로 결정했고, 독일과 네덜란드는 최소 2월까지 현재의 락다운을 유지하겠다고 했다. 스위스와 스웨덴도 보다 엄격한 체제로 전환하기로 결정했다. 이런 강력한 외출금지령 및 락다운 때문에 유럽 국가들의 GDP가 꽤나 큰 폭으로 하락할 것으로 예상된다. 독일은 5.1%, 프랑스는 9%, 스페인은 11.2% 정도 수준으로 떨어질 전망이다.

- **코로나로 연기되었던 리사 몽고메리(Lisa Montgomery)의 사형이 결국 집행됐다.** 여성 범죄자가 실제 사형된 것은 미국 역사에서 67년 만의 일이라고 한다. 몽고메리의 변호사와 판사 한 명은 계속해서 몽고메리의 정신 상태를 평가해야 한다고 주장했지만, 대법원은 다수결로 사형 집행에 찬성했다.

- **이스라엘의 보건성이 화이자와 바이오앤테크가 개발한 코로나 백신을 1회 분만 맞아도 감염률이 1/3로 줄어든다고 분석 결과를 발표했다.** 이스라엘의 건강 보험 조직 두 곳에서도 "1회 접종 후 12일이 지나면 감염률이 40% 떨어지고 14일이 지나면 60%로 떨어진다"고 발표했다. 화이자와 바이오앤테크의 백신은 최소 2회 맞아야 한다고 한다. 현재 이스라엘은 인구의 20%가 1회 접종을 마친 상태다.

- **하지만 중국의 백신은 브라질 의약 기관의 검사에서 매우 실망스러운 결과를 받았다.** 약효가 50% 정도 수준에 머문 것이다. 하지만 검사 결과가 나오기도 전에 이미 3억 8천만 회분을 주문한 상태라 브라질 정부는 이러지도 저러지도 못하는 교착 상태가 되었다. 물론 WHO가 권장하는 일반 대중용 백신의 약효보다는 살짝 높은 상태라 엄밀히 말하면 접종이 불가능한 건 아니지만 실망이 큰 것도 사실이다.

- **코로나로부터 승리했다고 자축하며 우한 락다운 1주년 기념행사까지 거행했던 중국이 다시 한 번 코로나로 위기 상황을 맞을까봐 서둘러 움직이기 시작했다.** 베이징 주변 지역의 한 결혼식을 통해 코로나 확진자들이 대량으로 나오기 시작하자 곧바로 스자좡과 싱타이 시에 락다운을 실시한 것이다. 이에 1700만 시민들의 활동이 일제히 중단됐고, 모든 계획들이 취소됐다. 그러더니 이번 주에는 랑팡, 헤이룽장성, 북경 일부 지구까지로도 락다운이 확대됐다.

- **에스토니아의 총리 유리 라타스(Juri Ratas)가 사임했다.** 코로나 19 경제 지원금으로 할당된 예산을 부동산 개발 회사에 대출했다는 사실이 발각됐기 때문이다. 총리의 갑작스런 사임으로 에스토니아 정부는 갑자기 제동이 걸린 상태다. 복수 정당으로 구성된 정부였기 때문에 균열이 가기 시작한 것이다. 이에 대통령이 중도보수 정당의 지도자에게 다음 정부를 구성할 것을 지시했다.

- **우간다의 대통령 선거가 오늘부터 시작된다.** 1986년부터 대통령이었던 요웨리 무세베니(Yoweri Museveni)와 가수 겸 배우이자 정치인인 보비 와인(Bobi Wine)이 맞붙는다. 선거 운동이 진행되는 동안 무세베니 측은 와인 캠프 측 구성원들을 체포, 납치하고 소셜 미디어 계정들을 삭제하고 금지시키기도 했다. 그렇기 때문에 무세베니의 승리가 거의 확실시 되고 있다.

[보안뉴스] 비트코인 등 암호화폐 가격 치솟자 또 등장한 거래소 사칭 스미싱
https://www.boannews.com/media/view.asp?idx=94029&page=1&kind=1

[보안뉴스] [최정식 발행인 칼럼] 2021년을 맞이하며 '디지털 뉴딜'에 거는 기대
https://www.boannews.com/media/view.asp?idx=94047&page=1&kind=2

[보안뉴스] 각종 논란의 중심 AI 챗봇 '이루다', 개인정보 노출 우려도 커지나
https://www.boannews.com/media/view.asp?idx=94049&page=1&kind=1

[보안뉴스] 현대자동차 러시아법인 고객 130만명 개인정보 유출됐나? 딥웹에 판매글 게시
https://www.boannews.com/media/view.asp?idx=94050&page=1&kind=1

[연합뉴스] 뉴질랜드 중앙은행 해킹? "시스템 불법 접근 발견"
https://www.yna.co.kr/view/AKR20210111030800009?input=1195m

[국방일보] 러 · 중 해커 사이버전 가담, 무방비 美 · 나토에 타격
https://kookbang.dema.mil.kr/newsWeb/20210111/1/BBSMSTR_000000100135/view.do

[보안뉴스] 미국 CISA, "솔라윈즈 공격자들, 정말로 SAML 토큰에 접근했다"
https://www.boannews.com/media/view.asp?idx=94031&page=1&kind=1

[보안뉴스] 절이 싫으면 중이 떠나라고 발표해 분노 산 왓츠앱
https://www.boannews.com/media/view.asp?idx=94030&page=1&kind=1

[보안뉴스] 개인정보 유출사고 발생했을 때... 기업이 취해야 할 사후대처 5단계
https://www.boannews.com/media/view.asp?idx=94028&page=1&kind=2

[보안뉴스] [주말판] 2021년 CISO들의 새해 결심에 들어가야 할 것 6
https://www.boannews.com/media/view.asp?idx=94042&page=1&kind=1

[헤럴드경제] 中 개인정보보호법 도입, 우리기업 대응 필요
http://news.heraldcorp.com/view.php?ud=20210110000233

[보안뉴스] [스토리텔링으로 이해하는 AI 보안-29] 인공지능 통한 인간 친화 보안기술 개발
https://www.boannews.com/media/view.asp?idx=94046&page=1&kind=5

[보안뉴스] [Automotive Cybersecurity-1] UNECE 자동차 사이버보안 규제 대응의 필요성
https://www.boannews.com/media/view.asp?idx=94054&page=1&kind=3

[EBN] 인터넷 해킹, 올해 더 위험한 이유는?
https://www.ebn.co.kr/news/view/1467373/?sc=Naver

[ITworld] IDG 블로그 | 흔한 2021년 클라우드 예측 중 틀린 2가지
https://www.itworld.co.kr/t/34/%ED%81%B4%EB%9D%BC%EC%9A%B0%EB%93%9C/178344

[ITworld] 허리케인이 강타한 섬에서 얻는 재해 복구에 관한 교훈
https://www.itworld.co.kr/t/36/%EB%B3%B4%EC%95%88/178304

[보안뉴스] 카카오톡 설치인줄 알았는데... 교묘하게 위장한 피싱 사이트 발견
https://www.boannews.com/media/view.asp?idx=94087&page=1&kind=1

[보안뉴스] 지난해 4분기 차단된 랜섬웨어 공격 17만건... 사회적 이슈 악용한 피싱으로 접근
https://www.boannews.com/media/view.asp?idx=94056&page=1&kind=1

[보안뉴스] 업그레이드 된 로키봇, 공격 프로세스가 더 복잡하고 교묘해져
https://www.boannews.com/media/view.asp?idx=94062&page=1&kind=1

[보안뉴스] 최고 난이도 해킹방어대회 'Real World CTF'서 한국 CodeR00t팀 우승
https://www.boannews.com/media/view.asp?idx=94063&page=1&kind=1

[뉴스1] '혐오발언 · 정보유출 논란' AI 챗봇 이루다 잠정 중단과 윤리의 문제
http://www.updownnews.co.kr/news/articleView.html?idxno=227190

[보안뉴스] 디지털과 만나는 헬스케어 분야, 보안 내재화 필요하다
https://www.boannews.com/media/view.asp?idx=94043&page=1&kind=2

[보안뉴스] 민간인증서로 오는 13일부터 주민등록등본 발급한다
https://www.boannews.com/media/view.asp?idx=94059&page=1&kind=2

[보안뉴스] [제2차 정보보호산업 진흥계획 집중진단-6] 정보보호 기업 성장 지원
https://www.boannews.com/media/view.asp?idx=94025&page=1&kind=2

[보안뉴스] 2021년 블록체인 사업, 확산 · 성과 · 기업육성 · 기술개발 부문 추진계획은?
https://www.boannews.com/media/view.asp?idx=94079&page=1&kind=2

[아이뉴스24] 국내 보안업계, 올해 OT · ICS 보안사업 '눈독'
http://www.inews24.com/view/1334096

[보안뉴스] 엔씨소프트 · 네오플 등 게임사들의 2021년 정보보호 인력 채용 러시
https://www.boannews.com/media/view.asp?idx=94045&page=1&kind=3

[보안뉴스] 과기정통부, 올해 인공지능 반도체 지원사업에 1,253억 투자한다
https://www.boannews.com/media/view.asp?idx=94095&page=1&kind=2

[강원일보] EMA "코로나19 백신 관련 자료 해킹으로 인터넷에 유출"
http://www.kwnews.co.kr/nview.asp?aid=221011200163

[보안뉴스] 중국의 소셜미디어 마케팅 회사, 수억 명 개인정보 수집하다 발각돼
https://www.boannews.com/media/view.asp?idx=94117&page=1&kind=1

[머니투데이] 中 개인정보법 어기면 벌금이 전년매출 5%…"모르면 당한다"
https://news.mt.co.kr/mtview.php?no=2021011310041503952

[보안뉴스] 솔라윈즈 배후의 공격 그룹, 알고 보니 러시아의 털라?
https://www.boannews.com/media/view.asp?idx=94098&page=1&kind=1

[보안뉴스] 미 국방부가 UFO와 외계인에 대해 발표한다고? 피싱 공격은 이미 시작
https://www.boannews.com/media/view.asp?idx=94096&page=1&kind=1

[VOA] 백악관 "북한, 미 해양산업의 사이버 위협"
https://www.voakorea.com/korea/korea-politics/dprk-maritime-cyber-threat

[더구루] MS 이메일 노린 해커…마임캐스트 인증서 공격
https://www.theguru.co.kr/news/article.html?no=17816

[ITworld] 21세기 데이터 침해 사건 TOP 15
https://www.itworld.co.kr/t/36/%EB%B3%B4%EC%95%88/178689

[아시아N] 코로나시대 사이버범죄 · 금융범죄 '요주의'
http://kor.theasian.asia/archives/283086

[보안뉴스] 개정 정보통신망법 본격 시행! 자동차 · 가전 · 주택도 사이버 보안으로 품는다
https://www.boannews.com/media/view.asp?idx=94061&page=1&kind=2

[보안뉴스] 과기정통부, 올해 인공지능 반도체 지원사업에 1,253억 투자한다
https://www.boannews.com/media/view.asp?idx=94095&page=1&kind=2

[보안뉴스] [단독] 더존비즈온, 고객과 보안은 뒷전... 플래시 대책 안 세웠다
https://www.boannews.com/media/view.asp?idx=94132&page=1&kind=1

[연합뉴스] "北 해킹, 이젠 '월드 클래스' 수준…코로나 백신 · 치료제 노려"
https://www.yna.co.kr/view/AKR20210113137600017?input=1195m

[보안뉴스] 솔라윈즈 사태로 유출된 소스코드와 정보, 판매되고 있다
https://www.boannews.com/media/view.asp?idx=94129&page=1&kind=1

[보안뉴스] 솔라윈즈 사태와 관련된 세 번째 멀웨어 선스팟 발견돼
https://www.boannews.com/media/view.asp?idx=94125&page=1&kind=1

[서울경제] "남일 아냐" '이루다' 사태에... IT업계, 개인정보보호 비상
https://www.sedaily.com/NewsView/22H93KVXMI

[보안뉴스] [제2차 정보보호산업 진흥계획 집중진단-7] 차세대 보안 신기술 확보
https://www.boannews.com/media/view.asp?idx=94100&page=1&kind=2

[보안뉴스] 올해의 첫 정기 패치, 제로데이와 선공개 취약점 포함 총 83개
https://www.boannews.com/media/view.asp?idx=94131&page=1&kind=1

[ITworld] 하드웨어 및 펌웨어 취약점 33가지와 위협 가이드라인
https://www.itworld.co.kr/t/36/%EB%B3%B4%EC%95%88/178924

[ITworld] 공격자가 호스팅 서비스를 악용하는 방법에서 관리자가 알아야 할 것
https://www.itworld.co.kr/t/36/%EB%B3%B4%EC%95%88/178919

[보안뉴스] 개인정보위, 공공부문 개인정보 보호 실태점검 추진
https://www.boannews.com/media/view.asp?idx=94130&page=1&kind=2

[보안뉴스] ISMS 의무화 두달 앞으로! 국내 암호화폐 거래소 인증현황 진단
https://www.boannews.com/media/view.asp?idx=94101&page=1&kind=3

[보안뉴스] 2027년까지 완전자율주행차 상용화 위해 4개부처 손 잡았다
https://www.boannews.com/media/view.asp?idx=94152&page=1&kind=2

[UPI뉴스] [단독] 국정원, 국내정보 접고 사이버 우주정보로 확장
http://www.upinews.kr/newsView/upi202101140039

[머니투데이] 포스트 코로나 시대, '대화형AI · 스몰데이터' 주목하라
https://news.mt.co.kr/mtview.php?no=2021011410182985211

현대자동차 러시아법인 고객 130만명 개인정보 유출

- 현대자동차 러시아법인(hyundai.ru)의 고객들로 추정되는 130만명의 개인정보가 현재 딥웹 커뮤니티 포럼에서 판매 중인 것으로 드러남. 다크웹 · 딥웹을 집중 모니터링하고 있는 보안전문가에 따르면 현대자동차 러시아법인으로부터 자동차를 구매한 고객들로 추정되는 130만명의 개인정보를 판매한다는 글이 딥웹 커뮤니티 포럼에 올라온 것이 확인됐다고 밝힘.

- 판매되는 개인정보에는 고객의 이름, 연락처, 이메일, 주소, 자동차번호, 자동차모델명이 포함돼 있는 것으로 알려졌으며, 해당 커뮤니티 포럼에 일부 샘플이 게시돼 있는 상황.

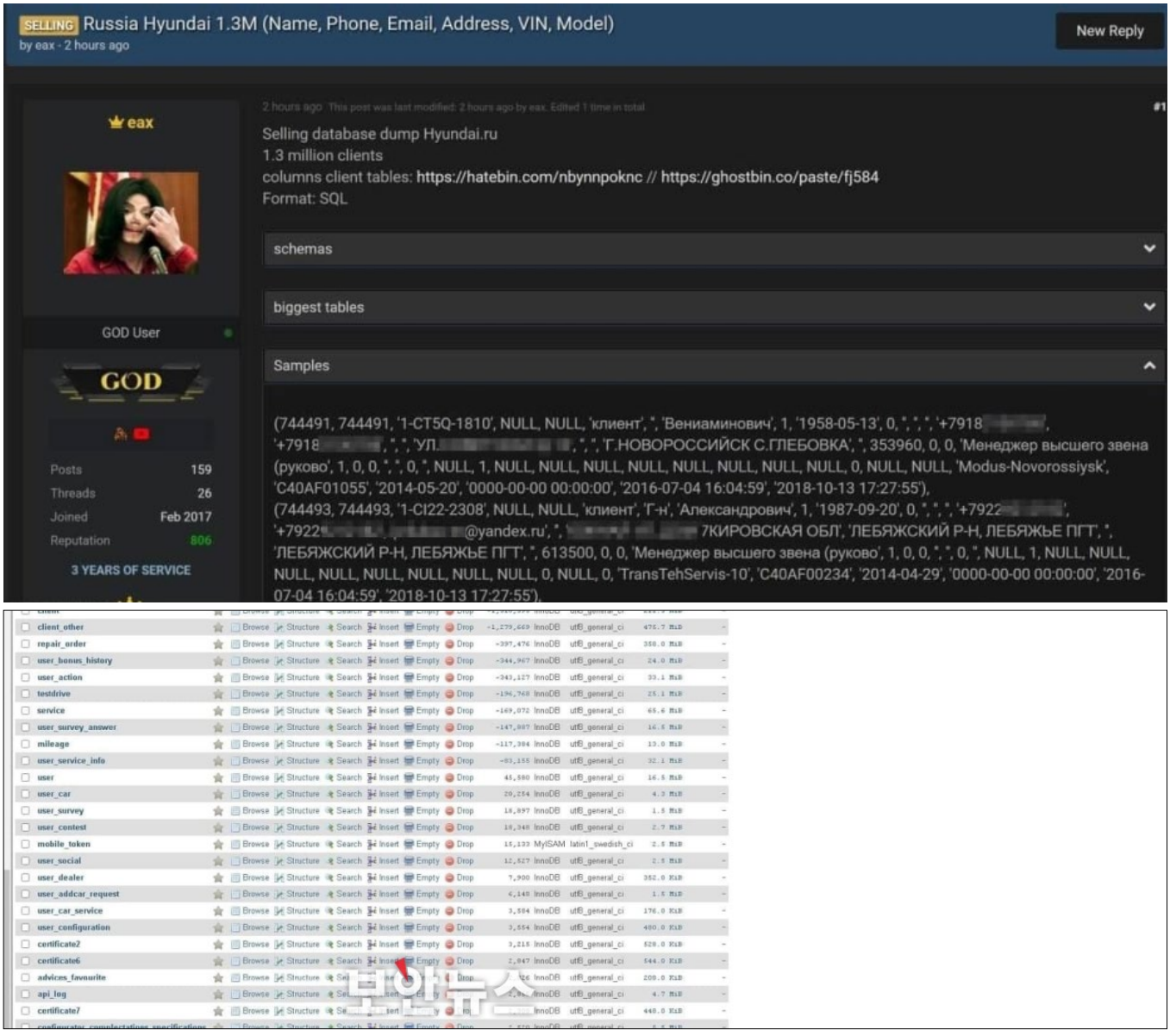
- 이렇듯 최근 다크웹이나 딥웹에는 국내 대기업을 포함한 글로벌 기업들의 고객정보나 기밀정보들이 공개되는 사례가 점점 더 빈번해지고 있음. 이는 '메이즈(Maze)'라는 랜섬웨어 해커조직이 기업에 대한 랜섬웨어 공격과 함께 데이터를 다크웹에 공개하는 '이중협박' 전략으로 톡톡히 재미를 본 이후, 여타의 랜섬웨어 조직들이 이러한 전략을 따라가면서 더욱 기승을 부리고 있음.

유명 게임사들의 임직원 크리덴셜 50만 건 거래

- 게임사들이 계속해서 사이버 공격에 노출되고 있는 가운데 보안 업체 켈라(Kela)가 25개 대형 게임사들에서 훔쳐낸 것으로 보이는 50만 개 임직원 및 클라이언트용 크리덴셜이 다크웹에서 판매되고 있는 것을 발견함. 이들이 발견한 침해 크리덴셜은 총 100만 개인데, 이 중 절반이 판매 중에 있다고 함.

- 켈라가 조사한 바에 의하면 해커들은 이제 게임사 자체로 들어가기 위해 여러 가지 수단을 강구하는데, 특히 아조럴트(AZORult)와 같은 멀웨어를 사용하거나, 직원들을 표적으로 고급 피싱 공격을 실시하는 것으로 알려짐. 아조럴트는 정보 탈취형 멀웨어로, 크리덴셜을 훔치는 데 주로 활용됨. 이를 통해 공격자들은 침투한 네트워크 내에서 횡적으로 움직일 수 있게 됨.

- 다크웹에는 게임 개발자의 백엔드에 대한, 이른바 '고급' 접근 권한도 판매되고 있는 것으로 알려짐. SSO, 키바나(Kibana), 지라(Jira), 슬랙(Slack), VPN, 비밀번호 관리 프로그램, 파워어드민(poweradmin) 등으로의 접근 권한이 한 패키지에 포함되어 있는 것도 발견됨.

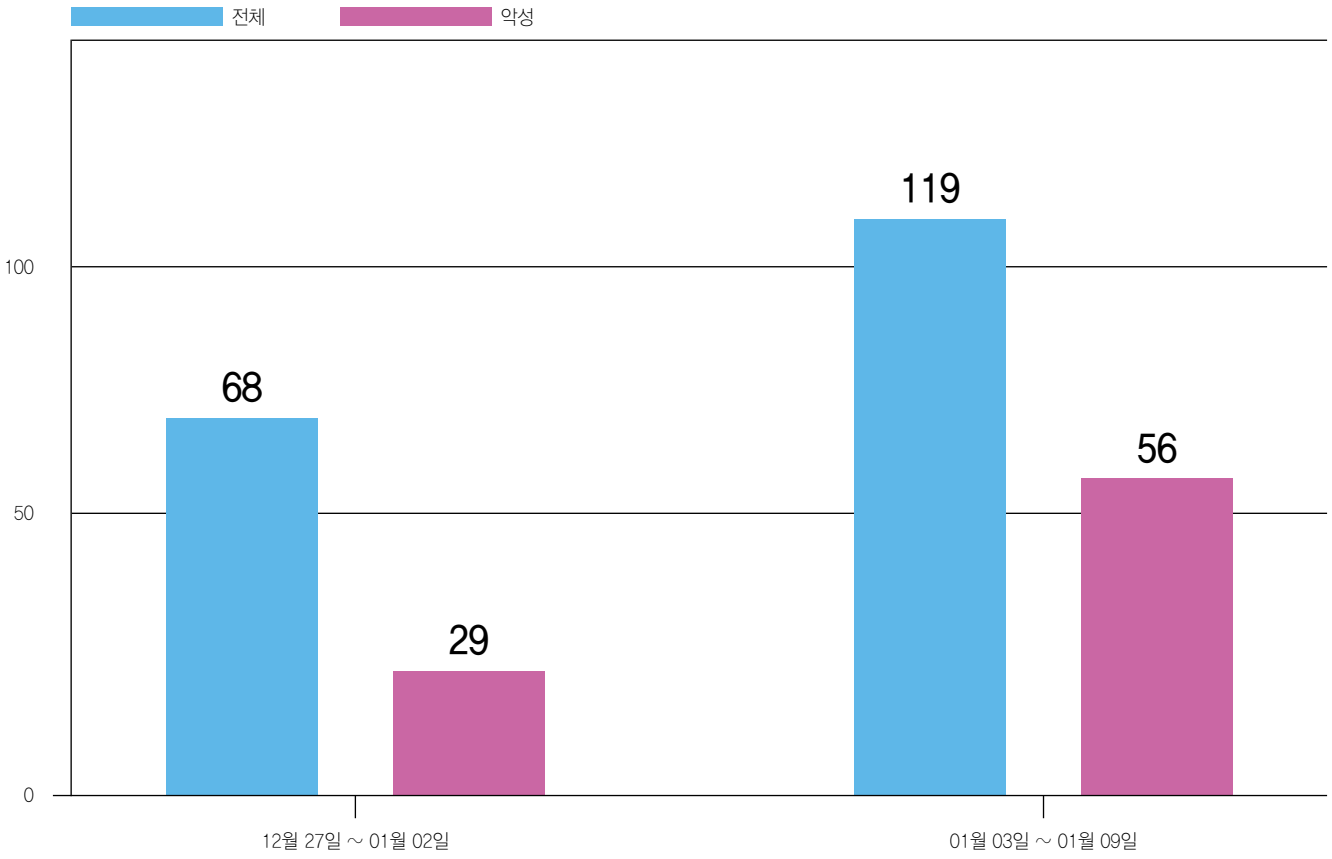


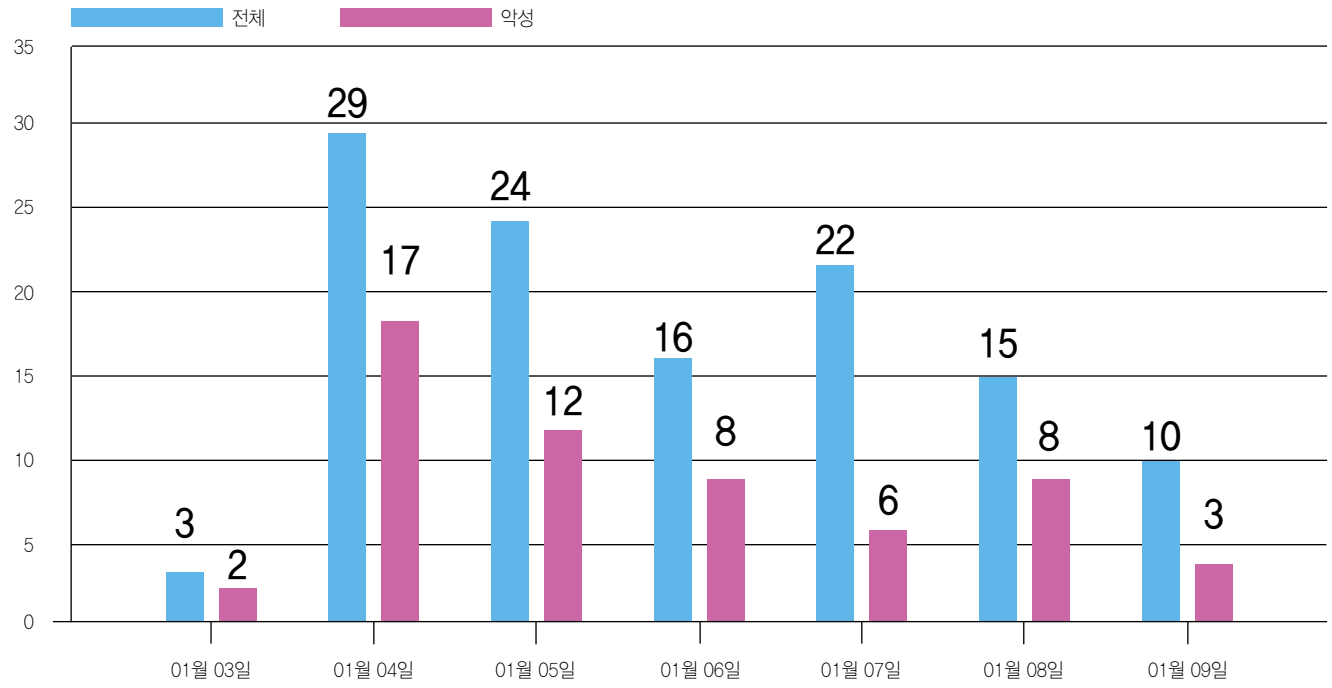
현대자동차 러시아법인 고객들로 추정되는 개인정보 130만건의 판매글이 게시된 딥웹 커뮤니티 포럼[자료=보안뉴스]

2021년 1월 첫째 주

1. 이메일 유입량

• 2021년 1월 첫째 주(1월 3~9일) 이메일 유입량은 총 119건이고 그중 악성은 56건으로 47.06%의 비율을 보임. 악성 이메일의 경우 그 전주 29건 대비 56건으로 27건 증가. 일일 유입량은 하루 최저 3건(악성 2건)에서 최대 29건(악성 17건)으로 일별 편차를 확인할 수 있음.

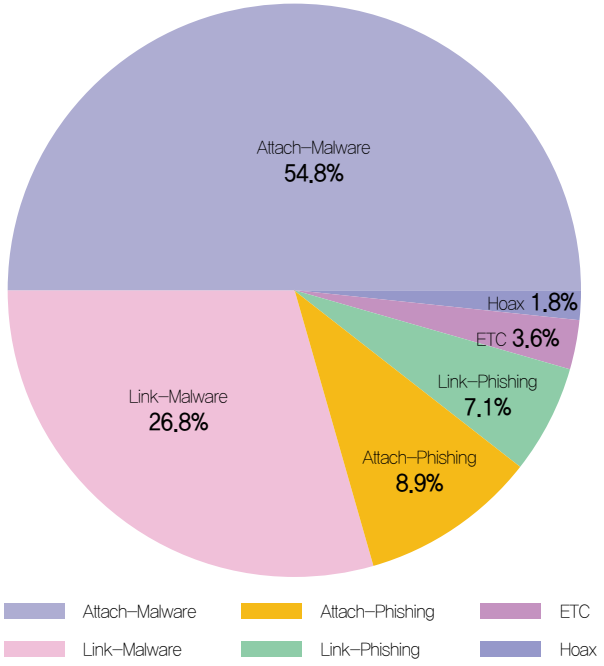




2021년 1월 첫째 주

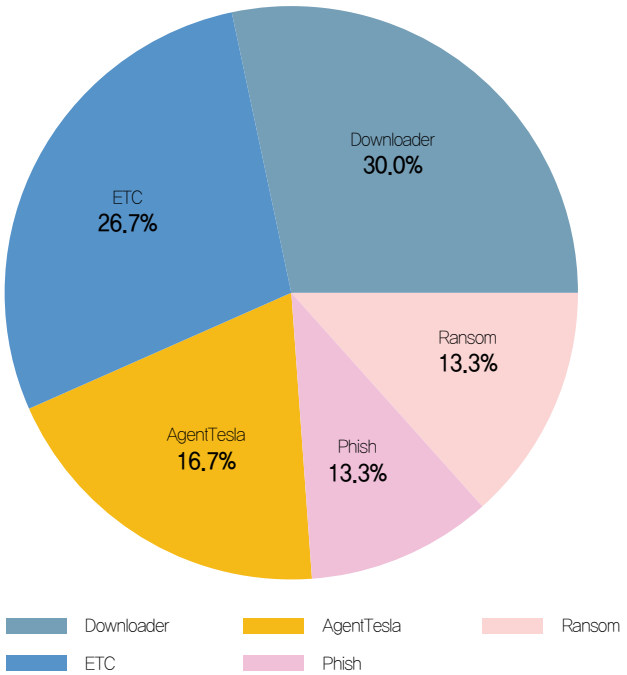
2. 이메일 유형

• 악성 이메일을 유형별로 살펴보면 56건 중 Attach-Malware형이 51.8%로 가장 많았고 뒤이어 Link-Malware형이 26.8%를 나타냄.



3. 첨부파일 종류

• 첨부파일은 'Downloader'형태가 30.0%로 제일 큰 비중을 차지했고 뒤이어 'ETC', 'AgentTesla'가 각각 26.7%, 16.7%의 비중을 차지함.



4. 대표적인 위협 이메일의 제목과 첨부파일명

▶1월 첫째 주 지난 주 다수 유포된 위협 이메일의 제목들

- urgent quotation needed – Order
- Re:
- RTGS transfer confirmation
- Business offer.
- Prepayment Status
- Re: 191205-210-604-1-VGM_5. AR
- RE: RE: Hyundai Force v.080W —— Request to provide all of DG cert.
- MAILBOX SECURITY UPDATE

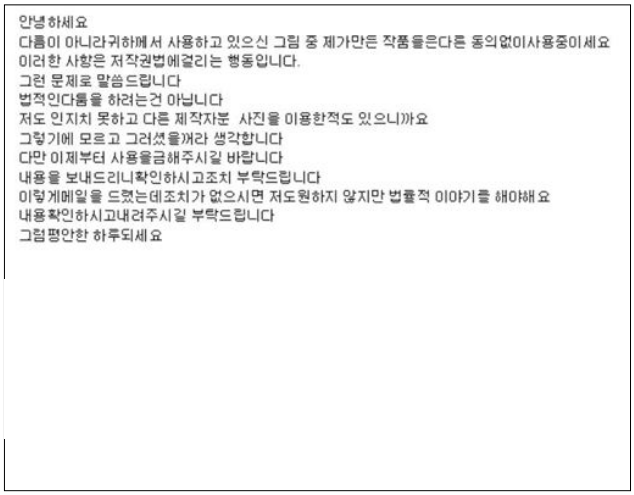
▶1월 첫째주 유포된 위협 이메일 중 대표적인 악성 첨부파일 명

- Inquiry89847.rar
- arc U1570.zip
- rtgs..rar
- INF78465910724.zip
- D1624-2021.zip
- FILE-LS216.zip
- ARCHIVOFile 0401 973_3961.zip
- BANK SLIP.zip
- Kim,YungDong.zip
- ARCH_04_012021.zip

※상기 이메일과 첨부파일을 확인할 경우 주의가 필요함.

5. 이메일 Weekly Pick

• 1월 첫째 주 Pick으로는 저작권 침해 관련 내용으로 랜섬웨어 악성코드를 유포하는 이메일을 선정. 지난 12월 예전 템플릿을 사용한데 이어 꾸준히 활용을 하는 모습. 당분간 이와 유사한 이메일을 유포할 가능성이 매우 높아 주의가 필요함.



카카오톡 설치 페이지로 위장해 악성 소프트웨어 유포하는 사이트 발견

- 국내에서 대표적으로 사용하는 메신저 '카카오톡'의 홈페이지를 사칭해 악성 소프트웨어를 유포하는 피싱 사이트가 등장해 사용자 주의가 필요
- 해당 피싱 사이트는 실제 사이트와 화면 구성 및 UI가 매우 유사하게 제작돼 사용자가 URL을 꼼꼼하게 확인하지 않으면 이를 알아채기 어려움

| 설명 |

- 사용자가 해당 피싱 사이트에서 '다운로드' 버튼을 누를 경우 메신저 설치 파일로 위장한 악성 소프트웨어를 내려받게 됨. 이를 실행할 경우 원격제어를 위한 악성코드를 추가로 PC에 설치하고, 최종적으로는 키보드 · 마우스 입력 내용을 탈취하는 키로깅, 클립보드 정보 탈취 등 사용자의 PC 사용 정보를 유출함.

| 피해 예방법 |

- 소프트웨어 설치 시 공식 홈페이지 이용
- 출처가 불분명한 메일 속 URL/첨부파일 실행 자제
- 운영체제 및 주요 소프트웨어 최신 버전 유지
- 백신 사용 및 실시간 감시 적용 등 기본적인 보안수칙 준수 필요

암호화폐 거래소 코인원 사칭한 스미싱 발견

- 비트코인이 사상 처음으로 4천만 원을 넘어 한때 4천4백만 원까지 치솟는 등 암호화폐가 연일 최고가를 달성하면서 암호화폐 거래소를 사칭한 스미싱도 다시 출현하고 있음
- 최근 발견된 스미싱은 국내 주요 암호화폐 거래소인 코인원을 사칭해 해외 IP에서 로그인 시도가 발견됐다며, 코인원 사이트 주소에 알파벳 'j'만 추가해 매우 유사한 피싱 사이트를 링크로 첨부하는 방식임.

| 주요 내용 |

- 해당 피싱 사이트로 접속하면 '피싱 피해 및 암호화폐 거래대행 주의'라는 제목의 팝업창과 함께 '최근 개인정보 유출로 인한 해킹사례가 많으니 코인원은 해킹 방지를 위해 해외IP차단서비스 기기등록서비스를 신청하시기 바랍니다'라는 문구로 '자세히 보기' 클릭을 유도하고 있음. 이마저도 사용자들을 속이기 위해 실제 코인원 사이트의 팝업과 유사하게 만든 것으로 보임.

| 피해 예방법 |

- 신뢰할 수 있는 모바일 백신 프로그램을 설치하고, 정기적으로 검사 수행하기
- 출처가 불분명한 경로를 통한 APK 앱 설치 금지
- 의심스러운 내용의 문자 메시지에 포함된 URL은 절대로 클릭하지 않기
- 백신 사용 및 실시간 감시 적용 등 기본적인 보안수칙 준수 필요

주간 해외 주요 취약점 리스트

CVE-2021-21445

- 설명 : SAP Commerce Cloud 1808, 1811, 1905, 2005, 2011버전의 불확실 입력값 처리 취약점
- 익스플로잇 방법 : 확인되지 않은 데이터를 HTTP 응답의 Content Type 헤더에 삽입하고 웹 사용자에게 전송
- 익스플로잇 결과 : 교차 사이트 스크립팅과 페이지 하이재킹과 같은 다양한 악성 공격을 감행할 수 있음
- CVSS 점수 : 5.4/10(SAP SE의 점수, NVD 점수 아님)
- CNA : SAP SE
- 관련 보안 권고문 : https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476

CVE-2021-21446

- 설명 : SAP NetWeaver AS ABAP 740, 750, 751, 752, 753, 754, 755 버전의 서비스 마비 및 서비스 플러딩 취약점
- 익스플로잇 방법 : 언급되지 않음.
- 익스플로잇 결과 : 디도스 공격 효과를 일으켜 사용자가 시스템이나 서비스를 이용하지 못하게 함
- CVSS 점수 : 7.5/10(SAP SE의 점수, NVD 점수 아님)
- CNA : SAP SE
- 관련 보안 권고문 : https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476

CVE-2021-21447

- 설명 : SAP BusinessObjects Business Intelligence 플랫폼 410, 420 버전의 Stored XSS 취약점
- 익스플로잇 방법 : Input Control의 사용자 입력 필드에 악성 자바스크립트 페이로드를 삽입
- 익스플로잇 결과 : 임의 코드 실행을 가능하게 해 준다.
- CVSS 점수 : 5.4/10(SAP SE의 점수, NVD 점수 아님)
- CNA : SAP SE
- 관련 보안 권고문 :https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476

CVE-2021-21448

- 설명 : SAP GUI for Windows -7.60 버전의 정보 탈취 취약점
- 익스플로잇 방법 : 클라이언트 PC 메모리의 Application Server ABAP 백엔드 시스템의 로그온 크리덴셜을 스푸핑할 수 있음
- 익스플로잇 결과 : 제한된 정보에 접근할 수 있게 됨
- CVSS 점수 : 5.3/10(SAP SE의 점수, NVD 점수 아님)
- CNA : SAP SE
- 관련 보안 권고문 : https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476

CVE-2021-21449

- 설명 : SAP 3D Visual Enterprise Viewer -9 버전에서 발견된 입력 값 미확인 취약점
- 익스플로잇 방법 : 사용자가 조작된 IFF 파일을 열도록 함
- 익스플로잇 결과 : 애플리케이션이나 서비스가 사용 불능 상태가 됨
- CVSS 점수 : 4.3/10(SAP SE의 점수, NVD 점수 아님)
- CNA : SAP SE
- 관련 보안 권고문 : https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476

CVE-2021-21450

- 설명 : SAP 3D Visual Enterprise Viewer -9 버전에서 발견된 입력 값 미확인 취약점
- 익스플로잇 방법 : 사용자가 조작된 PSD 파일을 열도록 함
- 익스플로잇 결과 : 애플리케이션이나 서비스가 사용 불능 상태가 됨
- CVSS 점수 : 8.8/10(고위험군)
- CNA : SAP SE
- 관련 보안 권고문 : https://www.zerodayinitiative.com/advisories/ZDI-21-012/

CVE-2021-21451

- 설명 : SAP 3D Visual Enterprise Viewer -9 버전에서 발견된 입력 값 미확인 취약점
- 익스플로잇 방법 : 사용자가 조작된 SGI 파일을 열도록 함
- 익스플로잇 결과 : 애플리케이션이나 서비스가 사용 불능 상태가 됨
- CVSS 점수 : 8.8/10
- CNA : SAP SE
- 관련 보안 권고문 : https://www.zerodayinitiative.com/advisories/ZDI-21-011/

CVE-2021-21452

- 설명 : SAP 3D Visual Enterprise Viewer -9 버전에서 발견된 입력 값 미확인 취약점
- 익스플로잇 방법 : 사용자가 조작된 GIF 파일을 열도록 함
- 익스플로잇 결과 : 애플리케이션이나 서비스가 사용 불능 상태가 됨
- CVSS 점수 : 8.8/10
- CNA : SAP SE
- 관련 보안 권고문 : https://www.zerodayinitiative.com/advisories/ZDI-21-010/

CVE-2021-21453

- 설명 : SAP 3D Visual Enterprise Viewer -9 버전에서 발견된 입력 값 미확인 취약점
- 익스플로잇 방법 : 사용자가 조작된 RLE 파일을 열도록 함
- 익스플로잇 결과 : 애플리케이션이나 서비스가 사용 불능 상태가 됨
- CVSS 점수 : 8.8/10
- CNA : SAP SE
- 관련 보안 권고문 : https://www.zerodayinitiative.com/advisories/ZDI-21-009/

MS 1월 보안위협에 따른 정기 업데이트

등급 : 긴급(Critical) 4종, 중요(Important) 5종

■ 업데이트 내용

제품군	중요도	영향	KB번호
Windows 10 v20H2, v2004, v1909, v1809 및 v1803	긴급	원격 코드 실행	Windows 10 v2004, Windows 10 v20H2: 4598242 Windows 10 v1909: 4598229 Windows 10 v1809: 4598230 Windows 10 v1803: 4598245
Windows Server 2019, Windows Server 2016 및 Server Core 설치(2019, 2016, v20H2, v2004, v1909)	긴급	원격 코드 실행	Windows Server 2019: 4598230 Windows Server 2016: 4598243 Windows Server v2004, Windows Server v20H2: 4598242 Windows Server v1909: 4598229
Windows 8.1, Windows Server 2012 R2 및 Windows Server 2012	긴급	원격 코드 실행	Windows 8.1, Windows Server 2012 R2 : 4598285, 4598275 Windows Server 2012 : 4598278, 4598297
Microsoft Office 관련 소프트웨어	중요	원격 코드 실행	4493156 등 17개
Microsoft SharePoint 관련 소프트웨어	중요	원격 코드 실행	4486683 등 9개
Microsoft .NET 관련 소프트웨어	중요	서비스 거부	–
Microsoft SQL Server 관련 소프트웨어	중요	권한 상승	4583456 등 9개
Microsoft Visual Studio 관련 소프트웨어	중요	원격 코드 실행	4584787
Microsoft Malware Protection Engine	긴급	원격 코드 실행	–

■ 취약점 요약 정보

제품 카테고리	CVE 번호	취약점 내용
.NET Repository	CVE-2021-1725	봇 프레임워크 SDK 정보 유출 취약성
ASP.NET core &. NET core	CVE-2021-1723	ASP.NET Core and Visual Studio Denial of Service Vulnerability
Azure Active Directory Pod Identity	CVE-2021-1677	Azure Active Directory Pod ID 스푸핑 취약성
Microsoft Bluetooth Driver	CVE-2021-1684	Windows Bluetooth 보안 기능 우회 취약성
	CVE-2021-1683	Windows Bluetooth 보안 기능 우회 취약성
	CVE-2021-1638	Windows Bluetooth 보안 기능 우회 취약성
Microsoft DTV-DVD Video Decoder	CVE-2021-1668	Microsoft DTV-DVD 비디오 디코더 원격 코드 실행 취약성
Microsoft Edge (HTML-based)	CVE-2021-1705	Microsoft Edge(HTML 기반) 메모리 손상 취약성
Microsoft Graphics Component	CVE-2021-1709	Windows Win32k 권한 상승 취약성
	CVE-2021-1708	Windows GDI+ 정보 유출 취약성
	CVE-2021-1696	Windows 그래픽 구성 요소 정보 유출 취약성
	CVE-2021-1665	GDI+ 원격 코드 실행 취약성
Microsoft Malware Protection Engine	CVE-2021-1647	Microsoft Defender 원격 코드 실행 취약성
Microsoft Office	CVE-2021-1716	Microsoft Word 원격 코드 실행 취약성
	CVE-2021-1715	Microsoft Word 원격 코드 실행 취약성
	CVE-2021-1714	Microsoft Excel 원격 코드 실행 취약성
	CVE-2021-1713	Microsoft Excel 원격 코드 실행 취약성
	CVE-2021-1711	Microsoft Office 원격 코드 실행 취약성
Microsoft Office SharePoint	CVE-2021-1719	Microsoft SharePoint 권한 상승 취약성
	CVE-2021-1718	Microsoft SharePoint Server 변조 취약성
	CVE-2021-1717	Microsoft SharePoint 스푸핑 취약성
Microsoft Office SharePoint	CVE-2021-1712	Microsoft SharePoint 권한 상승 취약성
	CVE-2021-1707	Microsoft SharePoint Server 원격 코드 실행 취약성
	CVE-2021-1641	Microsoft SharePoint 스푸핑 취약성
Microsoft RPC	CVE-2021-1702	Windows 원격 프로시저 호출 런타임 권한 상승 취약성
Microsoft Windows	CVE-2021-1706	Windows LUAFV 런타임 권한 상승 취약성
	CVE-2021-1699	Windows (modem.sys) Information Disclosure Vulnerability
	CVE-2021-1689	Windows Multipoint Management 권한 상승 취약성
	CVE-2021-1676	Windows NT Lan Manager 데이터그램 수신기 드라이버 정보 유출 취약성
	CVE-2021-1657	Windows 팩스 작성 양식 원격 코드 실행 취약성
	CVE-2021-1650	Windows 런타임 C++ 템플릿 라이브러리 권한 상승 취약성
	CVE-2021-1649	액티브 템플릿 라이브러리 권한 상승 취약성
	CVE-2021-1646	Windows WLAN 서비스 권한 상승 취약성

제품 카테고리	CVE 번호	취약점 내용
Microsoft Windows Codecs Library	CVE-2021-1644	HEVC 비디오 확장 원격 코드 실행 취약성
	CVE-2021-1643	HEVC 비디오 확장 원격 코드 실행 취약성
Microsoft Windows DNS	CVE-2021-1637	Windows DNS 쿼리 정보 유출 취약성
SQL Server	CVE-2021-1636	Microsoft SQL 권한 상승 취약성
Visual Studio	CVE-2020-26870	Visual Studio 원격 코드 실행 취약성
Windows AppX Deployment Extensions	CVE-2021-1685	Windows AppX 배포 확장 권한 상승 취약성
	CVE-2021-1642	Windows AppX 배포 확장 권한 상승 취약성
Windows CryptoAPI	CVE-2021-1679	Windows CryptoAPI 서비스 거부 취약성
Windows CSC Service	CVE-2021-1693	Windows CSC 서비스 권한 상승 취약성
	CVE-2021-1688	Windows CSC 서비스 권한 상승 취약성
	CVE-2021-1659	Windows CSC 서비스 권한 상승 취약성
	CVE-2021-1655	Windows CSC 서비스 권한 상승 취약성
	CVE-2021-1654	Windows CSC 서비스 권한 상승 취약성
	CVE-2021-1653	Windows CSC 서비스 권한 상승 취약성
	CVE-2021-1652	Windows CSC 서비스 권한 상승 취약성
Windows Diagnostic Hub	CVE-2021-1680	진단 허브 표준 수집기 권한 상승 취약성
	CVE-2021-1651	진단 허브 표준 수집기 권한 상승 취약성
Windows DP API	CVE-2021-1645	Windows Docker 정보 유출 취약성
Windows Event Logging Service	CVE-2021-1703	Windows 이벤트 로그 서비스 권한 상승 취약성
Windows Event Tracing	CVE-2021-1662	Windows 이벤트 추적 권한 상승 취약성
Windows Hyper-V	CVE-2021-1704	Windows Hyper-V 권한 상승 취약성
	CVE-2021-1692	Hyper-V 서비스 거부 취약성
	CVE-2021-1691	Hyper-V 서비스 거부 취약성
Windows Installer	CVE-2021-1697	Windows 설치 서비스 권한 상승 취약성
	CVE-2021-1661	Windows Installer 권한 상승 취약성
Windows Kernel	CVE-2021-1682	Windows 커널 권한 상승 취약성
Windows Media	CVE-2021-1710	Windows 미디어 파운데이션 원격 코드 실행 취약성
Windows NTLM	CVE-2021-1678	NTLM 보안 기능 우회 취약성
Windows Print Spooler Components	CVE-2021-1695	Windows 인쇄 스풀러 권한 상승 취약성
Windows Projected File System Filter Driver	CVE-2021-1672	Windows 프로젝트에 파일 시스템 FS 필터 드라이버 정보 유출 취약성
	CVE-2021-1670	Windows 프로젝트에 파일 시스템 FS 필터 드라이버 정보 유출 취약성
	CVE-2021-1663	Windows 프로젝트에 파일 시스템 FS 필터 드라이버 정보 유출 취약성
Windows Remote Desktop	CVE-2021-1674	Windows 원격 데스크톱 프로토콜 핵심 보안 기능 우회 취약성
	CVE-2021-1669	Windows 원격 데스크톱 보안 기능 우회 취약성
Windows Remote Procedure Call Runtime	CVE-2021-1701	원격 프로시저 호출 런타임 원격 코드 실행 취약성
	CVE-2021-1700	원격 프로시저 호출 런타임 원격 코드 실행 취약성
	CVE-2021-1673	원격 프로시저 호출 런타임 원격 코드 실행 취약성
	CVE-2021-1671	원격 프로시저 호출 런타임 원격 코드 실행 취약성
	CVE-2021-1667	원격 프로시저 호출 런타임 원격 코드 실행 취약성
	CVE-2021-1666	원격 프로시저 호출 런타임 원격 코드 실행 취약성
	CVE-2021-1664	원격 프로시저 호출 런타임 원격 코드 실행 취약성
	CVE-2021-1660	원격 프로시저 호출 런타임 원격 코드 실행 취약성
	CVE-2021-1658	원격 프로시저 호출 런타임 원격 코드 실행 취약성
Windows splwow64	CVE-2021-1648	Microsoft splwow64 권한 상승 취약성
Windows TPM Device Driver	CVE-2021-1656	TPM 장치 드라이버 정보 유출 취약성
Windows Update Stack	CVE-2021-1694	Windows 업데이트 스택 권한 상승 취약성
Windows WalletService	CVE-2021-1690	Windows WalletService 권한 상승 취약성
	CVE-2021-1687	Windows WalletService 권한 상승 취약성
	CVE-2021-1686	Windows WalletService 권한 상승 취약성
	CVE-2021-1681	Windows WalletService 권한 상승 취약성

◎ 참고 사이트

[1] (한글) https://portal.msrc.microsoft.com/ko-kr/security-guidance

[2] (영문) https://portal.msrc.microsoft.com/en-us/security-guidance

[3] https://msrc.microsoft.com/update-guide/releaseNote/2021-Jan

포티넷 웹 방화벽(FortiWeb) 취약점 보안 업데이트

- 포티넷(Fortinet)은 자사의 웹 어플리케이션 방화벽(WAF) FortiWeb 제품에서 발생하는 취약점을 해결한 보안 업데이트 발표
- 낮은 버전을 사용중인 시스템 사용자는 해결 방안에 따라 최신 버전으로 업데이트 권고

■ 업데이트 내용

- FortiWeb의 사용자 인터페이스에서 입력값 검증이 미흡하여 발생하는 SQL 인젝션 취약점(CVE-2020-29015) [2]
- FortiWeb에서 버퍼오버플로우로 인해 발생하는 임의코드실행 취약점(CVE-2020-29016) [3]
- FortiWeb에서 포맷스트링 버그로 인해 메모리 정보가 유출되는 정보노출 취약점(CVE-2020-29018) [4]
- FortiWeb에서 버퍼오버플로우 인해 발생하는 서비스 거부 취약점(CVE-2020-29109) [5]

■ 영향을 받는 제품 및 최신 버전

제품	CVE ID	영향 받는 버전	해결 버전
FortiWeb	CVE-2020-29015	6.2.3 및 이전 버전	6.2.4 이상 버전
		6.3.7 및 이전 버전	6.3.8 이상 버전
	CVE-2020-29016	6.2.3 및 이전 버전	6.2.4 이상 버전
		6.3.5 및 이전 버전	6.3.6 이상 버전
	CVE-2020-29018	6.3.5 및 이전 버전	6.3.6 이상 버전
	CVE-2020-29019	6.2.3 및 이전 버전	6.2.4 이상 버전
		6.3.7 및 이전 버전	6.3.8 이상 버전

◎ 참고사이트

[1]https://www.fortiguard.com/psirt
[2] https://www.fortiguard.com/psirt/%20FG-IR-20-124
[3] https://www.fortiguard.com/psirt/FG-IR-20-125
[4] https://www.fortiguard.com/psirt/FG-IR-20-123
[5] https://www.fortiguard.com/psirt/%20FG-IR-20-126

Mozilla Firefox 보안 업데이트

- 모질라 재단은 자사의 Firefox 제품에서 발생하는 취약점을 해결한 보안 업데이트 발표
- 낮은 버전을 사용중인 시스템은 악성코드 감염에 취약할 수 있으므로 해결 방안에 따라 최신버전으로 업데이트 권고
- Firefox에서 조작된 SCTP 패킷을 처리할 때 Use-after-free로 발생하는 임의코드실행 취약점(CVE-2020-16044) [2]

■ 영향 받는 제품

제품	영향 받는 버전	최신 버전
Firefox	84.0.2 이전 버전	84.0.2
Firefox ESR(Extended Support Release)	78.6.1 이전 버전	78.6.1
Firefox for Android	84.1.3 이전 버전	84.1.3

◎ 참고사이트

[1] https://www.mozilla.org/en-US/security/advisories/
[2] https://www.mozilla.org/en-US/security/advisories/mfsa2021-01/
[3] https://support.mozilla.org/ko/kb/update-firefox-latest-release

PART. B

Security Trend & Policy & Clipping

중국의 사이버보안은 지금
Cybersecurity in China, Now

보안책임자들에게 필요한 정부 IT/보안 정책 주간 브리핑
IT / Security Policy Weekly Briefing

한 주간에 출시된 정보보호 신제품 및 주요 업계 동향
Security Market & Product Trend

中, 2020년 12월 정보보안 사건 통계결과

○ *국가인터넷응급센터 발표...고위험급 취약점 40% 차지*

○ *중위험급 취약점 620여개로 지난해 가장 적은 규모*

○ *애플리케이션 프로그램에 취약점 가장 많아*

• 중국 당국이 지난해 12월 중 정부기관, 기업, 연구소, 학교 등에서 쓰고 있는 하드웨어 · 소프트웨어, 정보시스템에서 공식 확인한 정보보안 취약점이 1,200여 개인 것으로 나타남. 이는 지난 한해 가장 적은 취약점 규모며, 한 달 전에 비해 35% 넘게 감소한 수치임. 이 가운데 고위험급으로 평가된 보안 취약점은 480개 가량으로 전체 보안 취약점의 40%를 차지. 중위험급 취약점은 12월 중 620여개로 지난해 중 가장 적었음. 전월에 비해 35% 이상 줄었지만 전체 보안 취약점 가운데 점유율이 가장 높았음.

국가인터넷응급센터 발표, 12월 정보보안 취약점 1,200여개...연중 가장 적어

• 중국 '국가컴퓨터네트워크 응급기술처리 협조센터(CNCERT)는 12월 중 국가정보보안 취약점 공유 플랫폼(이하 CNVD)을 통해 협력업체(보안업체, 통신서비스업체, 통신기기장비업체)와 CNCERT 지역 센터, 개인(화이트해커)으로부터 접수한 사건형 정보보안 취약점들을 평가해 최종적으로 1,200여개를 등록했다고 밝힘.

• 이는 지난 한해 가장 적은 규모로 한 달 전에 비해 35% 넘게 줄어든 수치. 앞서 2월(2,400개)에 보안 취약점 수량이 가장 많았고, 4월(2,170여개), 11월(1,900여개), 3월(약 1,840개), 6월(약 1,800개), 7월(1,760여개), 8월(1,750여개), 5월(1,650여개), 9월(약 1,650개), 10월(약 1,500개) 순으로 뒤를 이었음.

• 인터넷응급센터는 12월 중 △첫째 주(11월 30일~12월 6일) 266개 △둘째 주(7일~13일) 293개 △셋째 주(14일~20일) 214개 △넷째 주(21일~27일) 298개 △다섯째 주(12월 28일~1월 3일) 295개의 정보보안 취약점을 각각 최종 확인해 등록했다고 밝힘.

• 인터넷응급센터가 평가한 정보보안 취약점들의 위험 등급별을 보면, 12월 첫째 주에는 전체 취약점 266개 가운데 고위험급 취약점이 81개, 중위험 166개, 저위험 19개. 둘째 주(전체 취약점 293개)에는 고위험급이 142개로 가장 많았고, 중위험 134개, 저위험 17개로 확인됨.

• 셋째 주(전체 취약점 214개)의 경우 고위험급이 80개, 중위험이 125개, 저위험 9개로 평가됨. 넷째 주에는 전체 취약점 298개 중 고위험금 117개, 중위험 128개, 저위험 53개였으며, 다섯째 주(전체 취약점 295개)에는 고위험급이 116개, 중위험 152개, 저위험 27개로 집계됨.

기간	공시 등록된 취약점 수	고위험급 취약점	중위험급 취약점	저위험급 취약점
11월 30일 ~ 12월 6일	266(개)	81	166	19
12월 7일 ~ 13일	293	142	134	17
12월 14일 ~ 20일	214	80	125	9
12월 21일 ~ 27일	298	117	128	53
12월 28일 ~ 1월 3일	295	116	152	27

20년 12월 공식 등록된 중국 내 정보보안 취약점 수량[자료=중국 국가인터넷응급센터]

• 고위험급 취약점은 12월 중 480개 규모로 전체 보안 취약점의 40%를 차지함. 이는 1월(약 430개), 9월(450개 규모)에 이어 세 번째로 적고 7월(500개 규모)과 비슷한 수량임. 이외에 지난해에는 4월(970개), 2월(약 950개), 8월(680개 규모), 5월(670개), 3월(650여개), 6월(590여개), 11월(560여개), 10월(약 540개) 순으로 고위험급 취약점 수량이 많았음.

• 중위험급 취약점 수량은 12월에 620여개로 전체 보안 취약점 가운데 절반이 조금 넘는 비중을 차지함. 이는 지난 한 해 가장 적은 수량으로 앞서 지난해 2월(1,215개)에 중위험급 취약점 수량이 가장 많았고, 4월(약 1,010개), 11월(1,000여개), 7월(1,000개 규모), 6월(약 980개), 9월(940개 규모), 3월(905개), 8월(900여개), 5월(830여개), 10월(약 800개) 순으로 많았음.

• 제로데이 취약점을 보면, 12월 첫째 주에 170개(전체 보안 취약점 중 점유율 64%), 둘째 주 195개(67%), 셋째 주 143개(67%), 넷째 주 165개(55%), 다섯째 주 174개(59%)였음. 지난 12월 첫째 주부터 다섯째 주까지 정보보안 취약점의 위협 등급은 모두 '중간' 수준으로 평가됐다고 인터넷응급센터는 밝힘.

中 12월 당 · 정부 기관 · 기업 관련 사건형 보안 취약점 통계

• 중국 인터넷응급센터가 CNVD를 통해 접수한 당 · 정부 기관 및 기업들과 관련된 사건형 보안 취약점을 보면, 12월 첫째 주에는 6,960개로 한 주 전(4,662개)에 비해 49% 증가함. 둘째 주에는 1만2,235개로 76% 증가했으며 셋째 주에는 1만2,185개로 0.4% 감소함. 넷째 주에는 1만1,489개로 6% 줄었고 다섯째 주에는 6,932개로 40% 감소함.

• 인터넷응급센터가 은행, 보험, 에너지 등 중요 분야 기관 · 기업에 알린 보안 취약점 사건은 12월 첫째 주 34건, 둘째 주 14건, 셋째 주 30건, 넷째 주 25건, 다섯째 주 18건이었음. 센터가 중국 유 · 무선 통신 서비스업체들에 통보한 정보보안 취약점 관련 사건은 12월 첫째 주 11건, 둘째 주 18건, 셋째 주 7건, 넷째 주 5건, 다섯째 주 7건으로 집계됨.

• 센터가 전국 각 지역의 CNCERT 센터와 협력해 검증 · 처리한 지방 중요 기관과 관련된 보안 취약점 사건은 12월 첫째 주 381건, 둘째 주 570건, 셋째 주 329건, 넷째 주 415건, 다섯째 주 269건이었음. 센터와 교육 분야 응급 조직이 협조해 검증 · 처리한 대학 · 연구소 정보시스템 취약점 사건은 12월 첫째 주 46건, 둘째 주 56건, 셋째 주 21건, 넷째 주 75건, 다섯째 주 66건에 달함.

• 센터가 국가 상급 정보보안 협조 기관에 보고한 각 정부 부서 및 위원회의 홈페이지와 부설 웹사이트 또는 직속 기관의 정보시스템 내 취약점 사건은 12월 첫째 주 66건, 둘째 주 22건, 셋째 주 43건, 넷째 주 33건, 다섯째 주 21건이었음.

12월 애플리케이션 프로그램에 취약점 가장 많아...웹 애플리케이션 뒤이어

• 인터넷응급센터가 12월에 공식 등록한 정보보안 취약점을 영향 대상에 따라 나눠 보면, 애플리케이션 프로그램 부문의 비중이 지속적으로 가장 높았음. 12월 첫째 주(전체 등록 취약점 266개)에는 애플리케이션 프로그램 부문 취약점이 127개(점유율 48%)로 절반에 가까운 비중을 차지함. 이어 웹 애플리케이션 부문 취약점이 84개(32%), 네트워크 장비(교환기, 라우터 등) 21개(8%), 운영체제 20개(7%), 스마트 장비 · 기기(사물인터넷 장비 · 기기) 8개(3%), 데이터베이스 4개(1%), 보안제품 부문 취약점 2개(1%)였음.

• 둘째 주(전체 취약점 293개)에는 애플리케이션 프로그램 부문 취약점이 129개로 44%의 점유율을 차지했다. 웹 애플리케이션 부문이 118개(40%)로 뒤를 이었음. 이밖에 네트워크 장비 18개(6%), 데이터베이스 9개(3%), 스마트 장비 · 기기 7개(2%), 보안제품 7개(2%), 운영체제 부문 취약점이 5개(2%)였음.

• 셋째 주(전체 취약점 214개)에는 애플리케이션 프로그램 부문 취약점이 120개(56%), 웹 애플리케이션 부문 71개(33%)로 두 부문이 약 90%의 점유율을 차지함. 이외에 운영체제 14개(7%), 네트워크 장비 5개(2%), 데이터베이스 3개(1%), 보안제품 부문 취약점 1개(1%)로 집계됨.

- 넷째 주(전체 취약점 298개)에는 애플리케이션 프로그램 부문 취약점이 121개(41%)로 절반에 못 미치는 비중을 보임. 웹 애플리케이션 부문 취약점 96개로 32%를 차지함. 운영체제 32개(11%), 보안제품 29개(10%), 네트워크 장비 15개(5%), 스마트 장비 · 기기 3개(1%), 데이터베이스 부문 취약점이 2개(1%)로 뒤를 이었음.
- 다섯째 주(전체 취약점 295개)에는 애플리케이션 프로그램 부문 취약점이 131개로 44%의 비중을 보였음. 웹 애플리케이션 부문 취약점 105개로 36%를 뒤를 이었음. 운영체제 28개(9%), 네트워크 장비 23개(8%), 스마트 장비 · 기기 5개(2%), 보안제품 부문 취약점이 3개(1%)였음.

정보보안 취약점 수량 (단위: 개)

보안취약점이 영향을 끼친 대상에 따른 유형	11. 30.~12. 6.	12. 7.~13.	12. 14.~20.	12. 21.~27.	12. 28.~1. 3.
애플리케이션 취약점	127	129	120	121	131
웹 애플리케이션	84	118	71	96	105
운영체제	20	5	14	32	28
네트워크 장비 (교환기, 라우터 등)	21	18	5	15	23
스마트 장비 (사물인터넷 장비)	8	7	–	3	5
데이터베이스	4	9	3	2	–
보안 제품	2	7	1	29	3

지난해 12월 중국 내 정보보안 취약점의 영향 대상에 따른 유형
[자료=중국 국가인터넷응급센터]

中 12월 통신 · 모바일 인터넷 · 공업제어시스템 분야별 보안 취약점 통계

- 인터넷응급센터가 정보보안 취약점을 주요 분야별로 나눠 조사한 결과, 12월에도 모바일 인터넷 분야에서 보안 취약점이 가장 많은 것으로 나타났다. 12월 첫째 주에는 모바일 인터넷 분야 취약점이 15개(고위험 5개, 중위험 10개), 공업제어시스템 분야 8개(중위험 7개, 저위험 1개), 통신 분야 5개(고위험 2개, 중위험 2개, 저위험 1개)로 집계됨.
- 둘째 주에는 공업제어시스템 분야 취약점이 34개(고위험 11개, 중위험 23개)로 가장 많았고, 통신 분야 취약점이 13개(고위험 7개, 중위험 6개), 모바일 인터넷 분야는 10개(고위험 4개, 중위험 4개, 저위험 2개)였음.
- 셋째 주에는 모바일 인터넷 분야 취약점이 11개(고위험 3개, 중위험 7개, 저위험 1개), 공업제어시스템 분야 5개(고위험 3개, 중위험 2개), 통신 분야는 4개(고위험)였음.
- 넷째 주에는 모바일 인터넷 분야 취약점이 39개(고위험 6개, 중위험 13개, 저위험 20개)로 가장 많았으며, 통신 분야 12개(고위험 4개, 중위험 7개, 저위험 1개), 공업제어시스템 분야가 2개(고위험)였음.
- 다섯째 주에는 모바일 인터넷 분야 취약점이 24개(고위험 4개, 중위험 12개, 저위험 8개), 통신 분야 9개(고위험 2개, 중위험 5개, 저위험 2개), 공업제어시스템 분야가 8개(중위험)였음.
- 인터넷응급센터는 지난 12월 중 최종 등록한 정보보안 취약점 가운데 주요 국내외 업체(제품)의 취약점 수량과 비중을 살펴본 결과, 첫째 주에는 △Hancom(취약점 수량 40개, 점유율 15%) △Microsoft(18개, 7%) △Intel(15개, 6%) △IBM(12개, 5%) △Google(9개, 3%) △Apple(8개, 3%) △광저우시 화두취 신화웨이창 광가오 스지 푸우부(广州市花都区新华伟创广告设计服务部) (6개, 2%) △선전시 챠오안 커지(深圳市乔安科技有限公司) (6개, 2%) △AikCms(5개, 2%) △기타(147개, 55%) 순으로 많았다고 밝혔음.
- 둘째 주에는 △Siemens(18개, 6%) △저장(성) 저다 중콩 신시커지(浙江浙大中控信息技术有限公司) (15개, 5%) △Cisco(13개, 4%) △Oracle(13개, 4%) △베이징 중청커신 커지 파잔(北京中成科信科技发展有限公司) (10개, 4%) △Schneider Electric(9개, 3%) △CloudBees(7개, 3%) △Crafter CMS(7개, 3%) △WordPress(7개, 3%) △기타(194개, 66%) 등의 순이었음.

	12월 14일~20일			12월 21일~27일			12월 28일~1월일		
순번	업체 (제품)	취약점수량	점유율	업체 (제품)	취약점수량	점유율	업체 (제품)	취약점수량	점유율
1	JerryScript	45	21%	Google	27	9%	7	5	9%
2	Microsoft	14	7%	Trend Micro	20	7%	Dell	16	5%
3	Oracle	13	6%	IBM	16	5%	SAP	11	4%
4	Mozilla	8	4%	Microsoft	11	4%	F5	10	4%
5	Cisco	8	4%	Solarwinds	9	3%	Zammad	9	3%
6	Google	8	4%	NZXT	7	2%	IBM	8	3%
7	Pixar	7	3%	tangro	6	2%	NETGEAR	8	3%
8	상하이 취앤루 SW개발공작실	5	2%	MediaWiki	5	2%	화안증권	7	2%
9	Moddable	5	2%	Odoo	5	2%	HPE	7	2%
10	기타	101	47%	기타	192	64%	기타	193	65%

지난해 12월 중국 내 보안 취약점이 발견된 일부 제품 관련 업체 분포
[자료=중국 국가인터넷응급센터]

과기정통부

▶ '민 · 관 랜섬웨어 대응 협의체' 구성

- 과학기술정보통신부가 랜섬웨어로 인한 피해 심각성을 알리고, 국민의 피해를 최소화하기 위해 '민 · 관 랜섬웨어 대응 협의체'를 구성해 대국민 정보보호 인식제고 및 중소기업 지원을 강화하기로 함.
- 협의체에는 한국정보보호산업협회(KISIA), 정보보호기업, 한국인터넷진흥원(KISA), 과기정통부 등이 참여해 랜섬웨어 피해의 심각성을 알리고, 콜센터 등 전담창구를 만들어 누구나 쉽게 지원 받을 수 있게 대응 방안을 지원할 계획임.
- 과기정통부는 올해 랜섬웨어 대응 솔루션을 포함해 정보보호 제품 도입지원을 받는 중소기업을 1,270개까지 지원하고, 전국민 인터넷PC를 원격에서 보안 점검하는 '내PC 돌보미 서비스'를 확대 추진 중임.

▶ 2020년 디지털 뉴딜 사업 주요 성과 발표(K-사이버방역)

- 과학기술정보통신부는 관계 부처가 공동으로 추진하고 있는 디지털 뉴딜 사업 중 2020년 추진된 과기정통부 소관 사업들에 대한 진행 상황과 이를 통한 변화를 종합해 15일 발표함. 디지털 뉴딜은 관계 부처가 함께 2025년까지 국비 44.8조원을 투자해 코로나 경기침체와 일자리 문제를 극복하기 위한 '국가혁신 프로젝트'라고 할 수 있음.
- 원격수업 · 재택근무 등 비대면 서비스의 확대로 인한 사이버 위협에 선제적으로 대비하기 위해 기업과 국민의 보안수준을 획기적으로 높이기 위한 'K-사이버방역'을 추진함. 중소기업 보안수준 향상을 위한 정보보호 컨설팅(775개사)과 맞춤형 정보보호 솔루션을 지원하고, 5대 융합산업 특화 지역(원주, 군산, 안산, 안양, 부산)에 '보안리빙랩'을 구축해 제조기업들이 안전한 제품을 생산하는 환경을 마련함. 또한, 전 국민 정보보호 강화를 위해 복지센터 등 취약계층을 포함해 1만6,300건의 원격 보안점검서비스(내PC 돌보미)를 제공함.

산업통상자원부

▶ 국가핵심기술, 69개에서 71개로 확대 지정

- 산업통상자원부는 제30회 산업기술보호위원회 심의 · 의결을 거쳐 '국가핵심기술 지정 등에 관한 고시'(개정)와 '산업기술보호지침'(제정)을 확정해 발표. 국가핵심기술이란 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 기술로, 이번 고시 개정을 통해 반도체 · 디스플레이 · 전기전자 · 자동차 · 조선 · 생명공학 · 정보통신 등 12개 분야 71개 기술이 지정됨.
- 지정 고시된 국가핵심기술을 보유 · 관리하고 있는 기관은 국가핵심기술에 대한 보호조치를 취해야 하며, 국가핵심기술을 수출하거나 외국인이 국가핵심기술을 보유한 기업을 인수합병하려는 경우 정부허가를 받아야 함. 산업부는 산업기술보호지침을 제정해 국가핵심기술을 보유 · 관리하고 있는 기관이 국가핵심기술의 유출을 방지하기 위해 지켜야 할 보호조치 사항별 세부 이행지침을 제시함.
- 구체적으로는 △보호구역 설정 · 출입허가 △국가핵심기술 보호등급 부여 · 보안관리규정 제정 △국가핵심기술 취급 전문인력 이직관리(퇴직인력 비밀유지 및 경업금지 표준서약서) △국가핵심기술 관리책임자 및 보안전담인력 지정 △통신시설 및 통신수단 보안 △정보처리과정 · 결과자료 보호 △국가핵심기술 취급 전문인력 구분 · 관리 △국가핵심기술 취급 전문인력 보안교육 △기술유출 사고 대응체제 구축. 보호조치 사항은 산업기술보호법상 국가핵심기술 보유 · 관리기관이 의무적으로 지켜야 할 사항으로, 정부가 실태조사를 통해 보호조치사항에 대한 개선을 권고할 수 있음.

개인정보보호위원회

▶ 공공부문 개인정보 보호 실태점검 추진

- 개인정보보호위원회가 공공부문의 개인정보보호 수준 강화를 위해 관계부처와 합동으로 주요 공공기관에 대한 개인정보 실태점검을 추진. 이는 국민의 민감한 개인정보를 대규모로 처리하는 공공기관의 개인정보 유출 · 오남용으로 인한 피해를 사전방지하고, 공공부문 전반의 개인정보 보호수준을 제고하기 위해 마련됨.
- 개인정보위는 개인정보 처리 규모, 민감도 및 파급력 등을 종합적으로 고려해 주요 공공기관 홈페이지 보안(20개), 지방자치단체(20개), 의료 · 복지(10개), 고용(10개), 부동산(1개) 등 5대 분야를 선정함.
- 주요 공공기관 홈페이지 보안에 대해서는 △홈페이지 보안조치(HTTPS) 적용 여부 △비밀번호 힌트 찾기 기능의 보안 미비 △홈페이지 개인정보 노출 여부 등을 점검하고, 지방자치단체에 대해서는 △각종 고지서, 우편물, 안내문자 발송 시 개인정보 포함 여부 △쓰레기장 등에 파기되지 않은 서류 방치 여부 △민원처리 과정에 대한 법규준수 여부 점검.

방송통신위원회

▶ 사람 중심의 AI 서비스 정책 기반 마련

- 방송통신위원회는 사람 중심의 AI 서비스가 제공되고 AI 서비스가 활용되는 과정에서 이용자 보호원칙이 지켜질 수 있도록 이용자 · 사업자 대상 교육 · 컨설팅을 지원하고 AI윤리규범 등을 구체화해 제도 개선을 추진할 계획임.
- 최근 AI 채팅로봇의 혐오 · 차별적인 표현, AI 채팅로봇에 대한 이용자의 성희롱성 발언 등이 사회적으로 큰 논란을 일으킨 가운데 사업자 · 이용자 · 정부 등 지능정보사회 구성원 모두가 AI윤리의 중요성을 인지하고, 각자가 실천할 수 있는 방안을 모색해야 한다는 지적이 커지고 있는 상황임.
- 이에 방통위는 AI서비스에서 이용자 보호를 가장 큰 원칙으로 삼고, 이용자 교육 · 사업자 컨설팅 · 제도 개선 등을 추진해 나간다는 방침. 먼저, 방통위는 올해부터 이용자에게 AI서비스의 비판적 이해 및 주체적 활용에 대한 교육을 실시할 예정임. 교육 내용으로는 이용자가 AI서비스에 활용된 알고리즘의 편향성을 파악하고, 그에 따른 문제를 최소화해 서비스를 이용할 수 있는 방안 등을 담을 계획.

행정안전부 & 인사혁신처

▶ 모바일 공무원증 본격 도입

- 행정안전부와 인사혁신처는 '전 국민 대상 모바일 신분증 도입을 위한 시험무대'로 추진 중인 '모바일 공무원증' 구축 사업을 완료하고, 1월부터 본격 운영한다고 밝힘. 공무원증은 주민등록증과 함께 1968년 종이 공무원증으로 시작됐으며, 그 후 2003년 플라스틱 전자공무원증으로 개편된 바 있음. 행안부와 인사처는 모바일 공무원증의 충분한 안전성 검사 등을 거쳐 올 연말부터 본격적인 '모바일 신분증 시대'를 연다는 계획.
- 모바일 공무원증은 현행 플라스틱 공무원증과 병행 사용할 수 있으며, 스마트폰 애플리케이션으로 발급받을 수 있음. 공무집행 시 공무원증 제시를 요구받으면 스마트폰으로 공무원임을 증명할 수 있고, 현행 플라스틱 공무원증을 꺼내지 않고도 스마트폰을 이용해 청사 및 스마트워크센터 출입이 가능함. 또한, 행정전자서명(GPKI) 없이도 모바일 공무원증을 이용해 공직자통합메일 등 업무시스템에 로그인할 수 있음.

에스원, 2021 보안업계 트렌드 전망 발표

- 종합안심솔루션 기업 에스원은 △인공지능(AI) 기술 발전 △무인매장의 증가 △원격근무의 일상화 △감시의 보편화 등 팬데믹 이후 나타난 사회 현상에 주목하면서 이런 사회적 변화에 따라 △AI 기술을 탑재한 지능형 보안솔루션 각광 △생체인증을 접목한 무인솔루션 증가 △ICT기술을 활용한 정보보안 시장 확대 △빅데이터를 적용한 통합관제센터 구축을 2021년 보안 업계 트렌드로 전망함.
- ①AI 기술 발전 → 지능형 보안솔루션 각광 : 팬데믹 이후 재조명 받게 된 기술 중 하나가 AI다. AI기술을 적용한 지능형 CCTV는 코로나 확진자의 동선을 추적하고 병실에서 환자를 관리하는데도 큰 역할을 수행하고 있다. 정부 역시 코로나 이후 경제 회복을 위해 발표한 '디지털 뉴딜'에서 AI의 중요성을 강조한 바 있음. 팬데믹 극복을 위해 AI를 이용한 보안기술이 적극 활용되며 관련 시장이 확대됐다. 올 한해는 AI 기술을 탑재한 다양한 지능형 보안 솔루션들이 출시될 것으로 전망됨.
- ②무인화 되는 매장 서비스 → 생체인증 접목한 무인솔루션 증가 : 소비 트렌드에도 변화가 생겼다. 과거엔 종업원이 직접 손님을 응대하며 매장을 다시 찾게 했지만 코로나 이후 비대면이 미덕인 사회가 되면서 종업원이 상주하지 않는 무인매장이 늘어남. 지난해에는 무인 키오스크가 국내 약 10만대 이상 설치되며 19년 대비 61.5%나 성장하기도 했음. 이에 따라 보안업계에서도 무인매장 솔루션에 관심을 기울이고 있음.
- ③원격 근무의 일상화 → ICT기술을 활용한 정보보안 시장 확대 : 지난해 기업들의 원격근무가 큰 폭으로 증가함에 따라 사이버 위협에 대한 불안감도 커졌음. 랜섬웨어 공격으로 시스템이 마비될 가능성도 높아졌고, 기업의 중요 정보가 유출될 우려도 커지면서 정보보안 및 IT 솔루션의 중요성도 높아짐. 실제로 한국인터넷진흥원(KISA)이 실시한 '재택근무 보안실태' 설문조사에 따르면 설문 참여자의 72.1%가 재택근무를 실시했으며, 이중 절반 이상이 재택근무 시 사이버 위협을 경험한 것으로 조사됨. 증가하는 사이버 위협을 예방하기 위해 보안업계는 물리 보안과 정보 보안을 결합한 융합 보안 사업으로 시너지를 창출하는 등 정보보안 사업 영역을 확대할 것으로 전망됨.
- ④감시의 보편화 → 빅데이터를 적용한 통합관제센터 구축 : 코로나 이후 감시를 위한 통합관제 시스템에 대한 중요성도 커졌다. 우리나라가 다른 나라에 비해 확진자에 대한 역학조사를 철저하게 할 수 있었던 배경에도 전국에 설치된 지자체의 통합관제센터가 있었다. 통합관제센터의 유기적인 연계를 통해 확진자의 동선을 정확하게 파악할 수 있었던 것이다. 최근에는 아파트와 같은 공동주택에도 통합관제센터가 속속 도입되기 시작했다. 일부 아파트는 분양을 위해 통합관제센터 구축 사실을 대대적으로 홍보하기도 했다. 감염의 불안감이 첨단 보안시스템에 대한 관심으로 이어진 것으로 분석된다.
- 팬데믹 이후 새로운 보안기술에 대한 관심이 급격하게 고조된 가운데 업계 선두주자인 에스원은 AI, 생체인식, ICT, 빅데이터 등의 첨단기술을 총망라한 '통합 보안 플랫폼'을 선보이겠다고 밝힘. 플랫폼을 통해 압도적인 업계 1위의 위상을 공고히 하겠다는 전략으로, 이를 위해 에스원은 기술 혁신을 위한 연구개발(R&D) 조직을 사업부 조직과 통합하고 물리보안사업과 빌딩관리사업 조직을 하나로 합치는 등 '통합 보안 플랫폼' 구축에 박차를 가하고 있음.
- 에스원은 통합 보안 플랫폼의 첫 시작으로 AI와 빅데이터 기술력을 바탕으로 한 '스마트건물관리 솔루션'을 조만간 출시할 예정임. 스마트건물관리 솔루션은 보안서비스가 가진 모니터링 노하우와 출동 인프라를 건물관리 사업과 결합한 솔루션. 기존엔 빌딩 상주 인력이 설비 제어, 에너지 관리 등을 맡았지만 이 솔루션은 상주 인력 없이 IoT센서를 설치해 설비 상태 빅데이터를 수집하고 모니터링하며, 이를 통해 이상 징후를 원격으로 파악, 출동서비스를 제공함.

KT텔레캅, 경량화한 지능형 영상관제 솔루션 '기가아이즈 프로 컴팩트' 출시

- 보안전문기업 KT텔레캅은 엔터프라이즈급 고객을 대상으로 적용해왔던 기가아이즈 프로 프리미엄(GiGAeyes Pro Premium)의 최첨단 영상분석 기능을 동일하게 제공하는 것에 경제성까지 더한 기가아이즈 프로 컴팩트(GiGAeyes Pro Compact)를 출시함
- 기가아이즈 프로는 건물 전체에 설치된 여러 대의 CCTV와 출입통제 시스템 등을 통합 관리해야 하는 빌딩 · 기업 고객을 위해 초고화질 영상관제, 지능형 영상분석(VA), IoT센서 알람, 출입통제 연동 등을 제공하는 지능형 영상관제 솔루션.
- 기존의 기가아이즈 프로 프리미엄은 100대 이상의 CCTV를 설치한 대형고객들이 주로 사용해 왔지만, 이제는 100대 이하의 중소형 고객들도 경량화한 기가아이즈 프로 컴팩트로 CCTV를 보다 효율적이고 편리하게 관리할 수 있게 됨.
- 프로 컴팩트는 기존 프리미엄과 비교해 서버 종류와 현장 설치를 간소화해 경제성을 높인 것이 특징. 지능형 영상분석 등을 활용한 스마트한 통합관제로 모니터링을 위한 인력 부담을 최소화할 수 있으며, 임의 화면분할 구성 등 사용자를 위한 관리 편의성은 기가아이즈 프로 프리미엄의 기능을 그대로 유지함.

안랩 MDS, KOTRA 주관 '차세대 세계일류상품'으로 선정

- 안랩이 자사의 지능형 위협 대응 솔루션 'AhnLab MDS(안랩 MDS)'가 산업통상자원부가 주최하고 KOTRA가 주관하는 '차세대 세계일류상품'으로 선정됨. '차세대 세계일류상품'은 향후 7년 이내 '세계일류상품'으로 전환될 가능성을 가진 제품으로, 안랩 MDS는 랜섬웨어 및 신종 악성코드를 비롯해 알려지지 않은 신변종 위협에 대응하는 지능형 위협 대응 솔루션.
- 안랩 MDS는 글로벌 보안 솔루션 인증기관인 'ICSA 랩'으로부터 '지능형 위협 대응(ATD)' 인증을 국내 최초로 획득(2019)하고 글로벌 시장조사기관 '프로스트 앤 설리번'으로부터 'APT 솔루션 기술 혁신상'을 수상(2015)하는 등 글로벌 보안 기술력을 인정받은 바 있음. 현재 싱가포르, 태국, 대만, 말레이시아를 비롯한 동남아 지역의 공공기관과 금융사 등 다양한 분야의 고객사에 안랩 MDS를 제공 중임.

PART. C

Security Keyword & Culture &History

한 주간 보안 키워드로 보안 알려주는 남자
Security Keyword

보안 역사, 그날(1월 첫째 주)
A Day Cybersecurity History

대중문화로 풀어보는 보안이야기
Cybersecurity in Popular

한 주간의 주요 기사 속 보안용어 풀이
Cybersecurity Teams ExplainedReport

WPA3 도입 본격화로 살펴본 와이파이 보안 규격 변천사

- 전파를 사용해 무선으로 데이터를 주고받는 대부분의 기기는 통신 과정에서 중간에서 알 수 없는 누군가가 개입해 데이터 내용을 엿볼 수 있다. 전파는 유선과 달리, 두 기기가 물리적으로 직접 연결되는 방식이 아니다. 특정 주파수로 데이터가 담긴 전파를 발신하면 해당 주파수를 수신할 수 있는 기기를 이용해 데이터를 받는 방식이기 때문에 같은 주파수 대역을 수신할 수 있는 기기라면 해당 내용을 제3자가 수신하는 것이 가능하다.

- 예를 들어보자. 군용 소형 아날로그 무전기인 PRC-96K의 경우 특정 주파수 대역을 이용해 가까운 거리에 있는 아군과 음성을 송수신할 수 있다. 그런데, 특정 부대에서 현재 사용 중인 채널과 동일한 채널을 수신할 수 있는 기기를 사용한다면 외부인이 대화 내용을 감청할 수 있다. 이 때문에 군에서는 '통신전자운용지시(CEOI)'라는 기밀문서를 통해 시간별로 사용할 채널과 장소별 호출부호를 바꾼다.

- 물론 이 같은 방식을 적용하더라도 '음성'이라는 평문을 주고받는 무전기의 특성상 특정 주파수를 통해 전파만 수신할 수 있으면 대화 내용을 타인이 알 수 있어, 전송 내용 자체를 암호화하거나 타인이 수시할 수 없도록 해야 한다. 가령 PRC-999K 같은 장거리 통신용 무전기의 경우 '주파수 도약'이라는 방식을 통해 통신 주파수를 주기적으로 변경하고, 내용을 디지털로 전환해 전송하는 등 한 차원 높은 보안을 적용하기도 한다.

와이파이로 암호화 프로토콜, WEP, WPA, WPA2

- 이처럼 전파를 이용하는 무선 통신 장비는 언제든 알 수 없는 상대방이 개입할 위험이 존재하므로 전송 내용을 암호화하거나 도 · 감청을 피할 수 있는 통신 방식을 사용할 필요가 있다.

- 우리가 오늘날 흔하게 사용하는 무선통신 기술 '와이파이'도 암호화 통신 규약이 있다. 와이파이 역시 2.4GHz와 5GHz의 공개된 주파수 대역을 사용하는 무선통신 장비로, 전송되는 전파를 중간에서 다른 누군가가 수신해 데이터 내용을 훔쳐보는 것도 가능하다. 즉, 암호화하지 않은 통신 프로토콜을 사용할 경우 동일한 주파수를 수신하는 장비를 이용해 통신 내용을 도청할 수 있다. 특히, 우리는 중요한 개인정보와 금융정보 등을 다루는 PC, 스마트폰을 이러한 와이파이에 연결해 사용하고 있기 때문에 무선 연결에 대한 경각심을 키울 필요가 있다. 와이파이 보안접속은 공개된 주파수를 사용하면서도, 실제 정보를 주고받는 AP(공유기)와 사용자의 단말기(PC, 스마트폰) 사이에만 내용을 알 수 있도록 암호화하는 기술을 말한다.

- WEP(Wired Equivalent Privacy)는 초기 와이파이 암호화 통신 규약이다. 사전에 지정된 복호화 키를 AP와 단말기 사이에 공유하고, RC4 알고리즘을 통해 데이터를 암호화해 전송하는 방식이다. 하지만, RC4 알고리즘 자체가 보안에 취약하며, WEP 프로토콜에서는 고정된 암호 키를 사용하기 때문에 암호화된 내용을 공격자가 쉽게 해석할 수 있다. 이로 인해 오늘날 WEP 프로토콜을 사용하는 경우는 거의 없다.

- WPA는(Wi-Fi Protected Access)는 기존 WEP의 취약성에 대한 대안으로 등장한 기술 규격이다. 와이파이 얼라이언스(Wi-Fi alliance)는 무선 인터넷 보안 표준인 IEEE 802.11i가 완성되기 전까지 WPA를 한시적으로 사용하도록 제시했다. 기존의 고정키 대신, 동적 암호키 구현을 위해 TKIP(Temporal Key Integrity Protocol) 기술을 적용한 것도 특징이다. TKIP는 패킷당 키 할당, 키 값 재설정 등의 방식으로 암호 키를 변경할 수 있으며, 기존 WEP 방식에 소프트웨어 패치만 적용하면 이를 사용할 수 있었다.

14년 동안 쓰인 WPA2, 결국 치명적인 취약점 등장

- 방패와 갑옷이 발전하면 이를 뚫는 무기도 발전하는 법이다. WPA2는 당시로서는 강력한 암호화 전송 기술이었으나, 2004년에 등장한 기술인 만큼 현재 시점에서 파훼할 수 있는 방법도 많다. 실제로 지난 2017년에는 'KRACK'이라는 이름의 취약점이 등장하기도 했다. KRACK 취약점은 중간자 공격의 일종으로, 암호화 기능을 무력화하고 사용자 단말기와 AP 사이에 주고받는 데이터를 가로채 카드정보, 웹 브라우저에 입력하는 ID/PW, 이메일 등 인터넷을 사용하는 다양한 정보를 탈취하는 것이 가능하다. 앞서 언급한 것처럼 전파를 이용한 무선 데이터 송수신은 해당 주파수를 수신할 수 있는 기기라면 이 데이터를 확인할 수 있다. 다만, WPA2의 경우 데이터 내용이 강력하게 암호화돼 있어 내용을 쉽게 확인하기 어려울 뿐이다.

- KRACK 취약점은 공격자가 이 과정에 침입해 암호 키를 무작위로 대입하는 방식을 사용한다. AP와 단말기가 서로 암호화 검증 메시지를 보내는 과정에서 해당 검증 메시지를 공격자가 탈취한 뒤 동일하게 전달해 오류를 일으키고, 암호 키를 초기화해 탈취한 데이터를 재조합하는 방식으로 공격이 이뤄진다. 물론 해당 취약점은 현재 보안 패치가 나온 상태다.

차세대 보안 와이파이 규격, WPA3

- WPA3는 이러한 문제를 해결하기 위해 등장한 보안 프로토콜이다. 14년 만에(2018년 발표) 새롭게 등장한 규격인 만큼 WPA2와 비교해 많은 부분에서 변화가 생겼다. 요약하자면 사용자 입장에서는 더 쉽고 간편하게 이용할 수 있고, 암호화 기능은 더 강력해졌다. WPA3는 개인용(Personal)과 기업용(Enterprise)로 구분한다. WPA3-Personal의 경우 '사전대입공격'으로 인한 SSID(와이파이 이름) 접속 ID/PW 탈취를 차단할 수 있어 상대적으로 쉬운 ID/PW를 설정할 수 있는 것이 특징이다. 사전대입공격이란 사전(Dictionary)에 등록된 단어에 대소문자 및 숫자 등을 더한 뒤 일일이 입력하고, 비밀번호를 알아내는 공격기법이다. 이 때문에 WPA2의 경우 강력한 ID/PW 설정을 권장하며, KRACK 취약점 역시 PW 탈취가 우선적으로 필요하다.

- 이와 달리 WPA3는 일종의 난수 생성 알고리즘인 SAE를 통해 암호 키 초기화 공격 및 사전대입공격을 어렵도록 했다. 사용자는 기억하기 쉬운 암호를 설정해도 향상된 인증 과정을 통해 무선 연결을 보호하는 것이 가능하다. 특히, 데이터가 전송된 이후 암호가 노출되더라도 트래픽 암호화 키는 노출되지 않기 때문에 전송 데이터를 보호하는 것 역시 가능하다. 여기에 WPA3-Enterprise는 최소 192비트 암호화(AES 192)를 통해 이전 세대(WPA2, 128비트)보다 보안 성능을 강화했다.

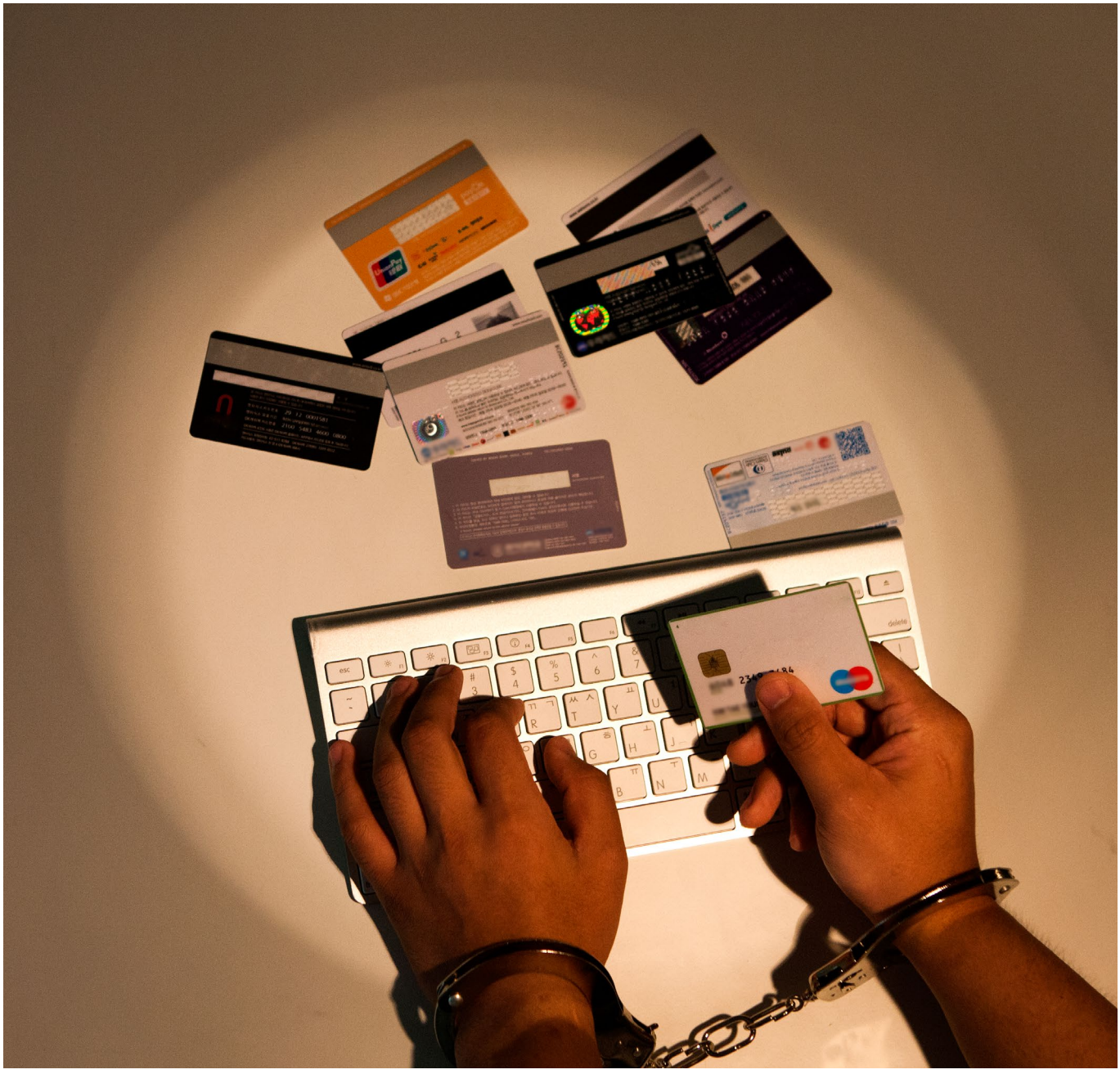
2018년 등장한 표준이지만 현재 대중화는 느려

- WPA3 프로토콜의 이러한 특징은 공용 와이파이에서 빛을 더욱 발한다. 쉬운 암호를 설정해도 단말기와 AP 사이에 각각 다른 방식의 암호화가 적용되기 때문에 공격자가 패킷을 탈취하더라도 암호화 키를 알기 어렵기 때문이다. 실제로 서울시는 1월 1일부터 공공와이파이 보안접속 SSID를 'SEOUL_Secure'로 통일하고, WPA3 프로토콜을 적용한다고 발표했다.

- 하지만 민간에서는 WPA3를 적용한 유무선 공유기를 찾아보기 어려운 것이 현실이다. 보안 규격이 등장한지 2년 가까이 지났음에도 불구하고, 현재 국내에서 판매 중인 10만 원 내외의 제품 중에는 WPA3를 지원하는 것을 찾기 어렵다. 20만 원 정도는 되는 제품이라야 간혹 이 기능을 찾아볼 수 있는 실정이다. 전송 거리가 상대적으로 짧은 와이파이 전파 특성상 가정 내에서만 사용한다면 공격자가 옆집이나 현관 앞처럼 가까이 있어야 하기 때문에 공격에 노출될 가능성은 적다. 하지만 카페 등 불특정 다수가 이용하는 공간에 구세대 보안 프로토콜이 적용된 유무선 공유기가 있다면 이는 공격 대상이 될 수 있다. 때문에 중요한 개인정보나 금융정보는 공용 와이파이에 연결한 상태에서 입력하지 않는 것이 아직까지는 안전할 것으로 보인다.

2014년 1월 8일 : 카드 3사 개인 신용정보 2억 581만건 유출 사건

- 2014년 1월 8일 검찰(창원지검)은 3개 카드사로부터 개인정보를 불법수집하여 유출한 KCB 직원 등을 기소했다고 발표함. 유출된 자료에는 성명 · 주민번호 · 전화번호 등 개인식별정보와 카드번호 · 유효기간 · 결제계좌 등 개인신용정보 등 총 1억 581만건이 포함되어 있었음.
- 해당 사건 조사 결과 부정사용 방지 시스템 유지보수를 담당하던 협력업체 직원이 파견근무 과정에서 보안이 허술한 틈을 타 자신의 USB에 카드사가 보유한 개인정보를 저장해 유출한 것으로 드러남. 일부 관계자들은 유출은 됐지만 제3자에게 넘어가지는 않았다고 호언장담했지만, 범인이 해당 정보를 텔레마케팅 업체 등 제3자에게 팔아넘긴 사실까지 밝혀짐.
- 해당 사고는 △1억 건 이상의 정보가 유출된 초대형 사고라는 점 △이름이나 주민등록번호, 카드 번호, 유효기간 및 CVC 번호 등 민감한 정보가 유출된 점 △대형 금융사가 USB 반입 통제나 암호조치 불이행 등 최소한의 보안조치도 하지 않은 점 △이미 유출 행위는 2012년 10월부터 이뤄졌고, 사고인지 및 발표는 2014년이 돼서야 이뤄진 점 △개인정보 유출 사실을 확인할 수 있다는 공식 사이트에서조차 개인정보보호가 허술했던 점 등 셀 수도 없이 많은 이유에서 온 국민에 큰 충격을 줬고, 금융 시스템에 대한 불신을 키운 사건이었음. 1억 건이라는 숫자는 중복된 개인정보나 망자의 정보를 빼더라도 국민 대다수의 개인정보에 해당되는 수치이며, 특히 이 사건을 계기로 주민등록번호를 변경할 수 있는 제도까지 마련된 바 있음.
- 카드 3사 유출사고는 2012년 중국상하이로드웨이d&B의 1억5천만건, 2009년 미국 하틀랜드페이먼트시스템즈의 1억3천만건에 이어 역대 3번째 규모이며 국내 유출사고 중 최대 규모에 해당됨.



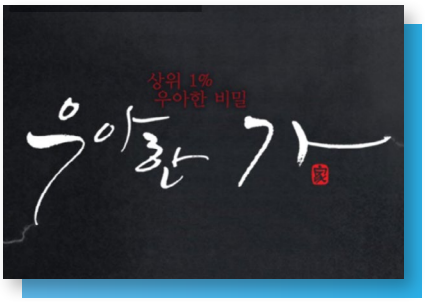
한국 드라마 속에 그려지는 IT와 보안, 그리고 해커

1. 스타트업

방송사: *tvN | 방영일: 2020.10.17 ~ 2020.12.06. 16부작 | 시청률: 5.4%*

주인공: *서달미(배수지), 남도산(남주혁), 한지평(김선호), 원인재(강한나)*

스타트업은 주인공을 비롯해 주변 인물들이 스타트업을 운영하기 때문인지 유독 IT와 관련된 내용이 많다. 예를 들어 남도산은 친구들과 함께 스타트업을 운영하면서 해커톤에 참가하거나 서달미에게 머신러닝을 쉽게 설명해주고, 서달미는 필적감정 인공지능 기술을 통해 자율주행기술과 보안 등 다양한 산업 활용 분야를 소개한다. 특히, 13화에서는 주인공 서달미의 스타트업이 랜섬웨어에 감염돼 모든 것을 잃을 뻔한 사건이 등장한다. 물론 남자 주인공인 남도산이 등장해 멋지게 해결하지만, 현실에서는 조금 어려운 이야기다.

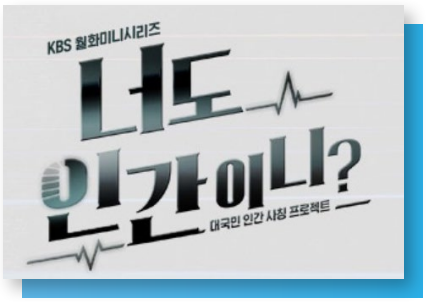


2. 우아한 家

방송사: *MBN, 드라맥스 | 방영일: 2019.8.21 ~ 2019.10.17. 16부작 | 시청률: 8.5%*

주인공: *모석희(임수향), 허윤도(이장우), 한제국(배종옥)*

우아한 가는 재벌가의 숨은 비밀과 이를 둘러싼 오너리스크 팀의 이야기를 다룬 미스터리 멜로드라마다. 15년 전 살인사건으로 엄마를 잃은 재벌가 고명딸 모석희가 사건의 진실을 밝히기 위해 변호사 허윤도와 함께 싸움을 시작한다. MC그룹의 오너리스크 관리팀인 TOP팀은 국정원, 검찰, 언론, 군, 법 등 다양한 분야의 전문가들이 모여 있으며, 사건의 진실을 찾으려는 모석희와 두뇌싸움을 벌인다. 특히, TOP팀의 북한 해커 출신 황보주영(박영린)은 국토부장관 대상으로 카드 내역 조회, 카톡 해킹, 번호 추적 등 다양한 해킹기술을 이용한 범죄를 저지른다.



3. 너도 인간이니?

방송사: *KBS2 | 방영일: 2018.06.04 ~ 2018.08.07. 36부작 | 시청률: 9.9%*

주인공: *남신/남신Ⅲ(서강준), 강소봉(공승연), 지영훈(이준혁), 서예나(박환희)*

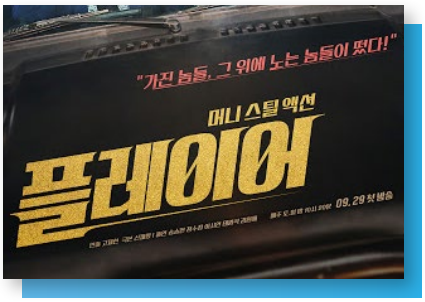
인간보다 더 인간다운 인공지능 로봇 남신Ⅲ와 열혈 경호원 강소봉이 펼치는 대국민 인간사칭 프로젝트. 안하무인 재벌3세인 남신과 아들과 함께하지 못하는 엄마 오로라 박사가 만든 인공지능 로봇 남신Ⅲ의 이야기를 다룬 '너도 인간이니?'는 인공지능 로봇 남신Ⅲ의 신호등 해킹, 몰카 감지, 스마트폰 해킹, 자율주행차 등 다양한 정보보안 기술을 선보인다. 남신Ⅲ는 인공지능 로봇이라는 설정 탓에 다소 황당해 보이는 괴력이나 해킹기술을 자주 선보이는데, 특히 자율주행차를 해킹해 성능을 높이는 장면은 남신Ⅲ의 가공할 성능을 짐작할 수 있게 한다.

4. 리치맨

방송사: *MBN, 드라맥스 | 방영일: 2018.5.09 ~ 2018.06.28. 16부작 | 시청률: 1.9%*

주인공: *이유찬(김준면-EXO 수호), 김보라(하연수), 오창석(민태주), 민태라(김예원)*

주인공 이유찬이 설립한 시가총액 2조원이 넥스트인은 글로벌 IT 기업으로 모바일 게임과 SNS, 클라우드 서비스를 제공하는 곳이지만, 고객정보 1,000만 명이 유출되는 사건을 겪는다. 이유찬은 이 사건으로 대표이사에서 물러난 뒤 인공지능 기반 음성인식 프로그램 업체인 댄싱 웨일을 세워 다시 재기한다. 이 드라마에서 주목할 점은 넥스트인의 SNS 서비스인 미니파일에 저장된 개인정보를 이용한 인공지능 보안 프로그램인 DS(Digital Secretary)와 개인정보관리시스템인 빅 파일(Big File)이다.



5. 플레이어

방송사: *OCN | 방영일: 2018.09.29 ~ 2018.11.11. 14부작 | 시청률: 5.8%*

주인공: *강하리(송승헌), 차아령(정수정), 임병민(이시언), 도진웅(태원석)*

범죄자들의 유쾌한 복수물 플레이어는 사기꾼과 드라이버, 해커와 파이터 등 각 분야 최고의 플레이어들이 뭉쳐 가진 놈들이 불법으로 모은 더러운 돈을 터는 머니 스틸 액션 드라마다. 예능 '나혼자 산다'에서 인기를 얻은 이시언이 해킹 마스터 임병민으로 출연해 해킹 실력을 선보인다. 세계 해킹 올림픽에서 우승을 차지하며 국정원에 스카우트 됐던 임병민은 그의 능력을 불법적으로 이용한 세력으로 인해 위험에 처하지만, 강하리에게 도움을 받은 후 함께 일하게 된다.

6. 유령

방송사: *SBS | 방영일: 2012.5.30 ~ 2012.8.09. 20부작 | 시청률: 15.3%*

주인공: *김우현(소지섭), 박기영/하데스(최다니엘), 유강미(이연희), 조현민(엄기준), 권혁주(곽도원)*

드라마 유령은 그동안 조명 받지 못했던 '정보보안'의 세계를 제대로 보여준 작품으로 특히 정보보안 분야에서는 상당한 이슈를 불러왔다. 특히, 보안종사자들이 주로 사용하는 용어와 업무스타일이 많이 등장했는데, 유령의 주인공인 소지섭과 최다니엘은 각각 사이버수사대 팀장과 유명 해커로 등장해 일반인들에게는 낯설지만, 보안종사자 사이에서는 익숙한 보안용어들을 자주 사용하고 있다.

NTFS 방식 하드드라이브를 간단히 망가트리는 제로데이(2021.1.15.자)

윈도우 OS에서 **제로데이**[1] 취약점이 발견됐다. NFTS 방식으로 포맷된 하드드라이브를 손상시킬 수 있게 해 주는 취약점으로, 작은 문자열을 기입하는 것만으로 공격이 성공할 정도로 **익스플로잇**[2]이 간단하다고 한다.

외신인 MS파워유저에 의하면 이 취약점을 제일 먼저 발견한 건 보안 전문가인 '요나스 L(Jonas L)'이라고 한다. 파일시스템 경로에 특정 문자열이 포함되면 윈도우 10 하드드라이브가 망가진다는 것이 그가 찾아낸 내용이다. 문제의 문자열은 $i30이라고 한다.

파일시스템 경로에 이 문자열을 추가시키는 방법에는 여러 가지가 있을 수 있다고 그는 경고하기도 했다. 윈도 단축키 설정, 집(zip) 아카이브 안에 숨기기, 배치 파일 안에 숨기기, HTML 문서 조작, 바로가기 아이콘의 경로 설정 등의 방법이 있다는 게 그의 설명이다. 즉 여러 가지 피싱 기법을 동원해 피해자가 $i30을 파일 경로로서 입력하기만 하면 하드 드라이브를 망가트릴 수 있다는 뜻.

해당 코드가 실행되면 윈도우 10은 손상된 디스크 기록이 있다면서 시스템 리부트를 요구한다. 요나스 L은 외신인 블리핑컴퓨터와의 인터뷰에서 "해당 취약점은 약 윈도우 10 빌드 1803 시기부터 존재해왔다"고 밝혔다. 즉 2018년 4월 업데이트부터 존재해왔으며, 현재까지 아무도 이에 대해 공개하지 않았다는 것이다.

이를 시험해 보려면 블리핑컴퓨터가 제시한 코드를 윈도 10 **NTFS**[3] 시스템에서 실행시키면 되는데, 이는 대단히 위험하기 때문에 기사에 명시하지 않기로 한다. 쓰지 않는 컴퓨터가 실험용으로 마련되어 있다면 실험해 보아도 무방하다. 하지만 블리핑컴퓨터 기사에 실험 영상이 있으니 이를 시청하는 게 가장 안전하다.

요나스 L이 트위터를 통해 설명한 바에 의하면 "문제의 문자열인 $i30은 NTFS 속성 중 하나로, 디렉토리의 파일들과 하위 폴더들의 목록과 관련이 있다"고 한다. 때문에 이 부분을 건드리는 것이 파일 경로와 디스크에 영향을 주는 것이다. 그렇다 해도 정확히 어떤 원리로 이 문자열이 하드드라이브를 손상시키는 것인지는 아직 알 수 없다고 요나스는 블리핑컴퓨터와의 인터뷰를 통해 설명했다.

MS 측은 이 취약점에 대해 인지하고 있으며 조만간 업데이트를 발표할 예정이라고 한다. 요나스 L이 밝혀내지 못한 기술적 원리를 MS가 보안 권고문을 통해 밝힐지도 은근한 관심사다.

용어풀이

1) **제로데이(Zero-Day):** 모든 시스템은 완벽하지 않기 때문에 취약점이 존재한다. 운영체제(OS)나 소프트웨어에서 취약점이 발견될 때마다 기업은 그 취약점을 고치는 보안 업데이트 즉, 패치를 발표하게 된다. 취약점이 발견되고 보안 패치가 나오기 전까지의 취약점을 제로데이 취약점이라고 한다. 그리고 이 기간에 시간차를 이용해 공격하는 기법이 제로데이 공격이다. 사실상 이 기간에는 방어나 대처가 불가능하다. 공격을 막으려면 해커보다 먼저 취약점을 찾아내 패치를 업데이트해야 한다. 하지만 해커보다 먼저 취약점을 찾기 어렵기 때문에 최근 기업에서는 버그바운티를 시행하기도 한다. 취약점을 찾은 해커에게 포상금을 주는 제도로, 기업 스스로 발견하지 못한 취약점을 찾아내 사고 피해를 예방할 수 있다.

2) **익스플로잇(Exploit):** 취약점 공격을 의미하는 익스플로잇이란 컴퓨터의 소프트웨어나 하드웨어 및 컴퓨터 관련 전자 제품의 버그나 보안 취약점 등 설계상 결함을 이용해 공격자의 의도된 동작을 수행하도록 만들어진 절차나 일련의 명령, 스크립트, 프로그램 또는 특정한 데이터 조각 말하며, 이러한 것들을 사용한 공격 행위를 이르기도 한다. 이러한 익스플로잇은 주로 공격 대상 컴퓨터의 제어 권한 획득이나 디도스 공격, 스파이 행위 등을 목적으로 한다.

3) **NTFS(New Technology File System):** NTFS는 윈도우 NT 계열 운영체제의 파일 시스템으로 윈도우 2000, 윈도우 XP, 윈도우 서버 2003, 윈도우 서버 2008, 윈도우비스타, 윈도우 7, 윈도우 서버 2008 R2 , 윈도우 8, 윈도우 서버 2012, 윈도우 8.1, 윈도우 서버 2012 R2 등에도 포함되어 있다. NTFS의 NT는 윈도우 NT와 비슷하게 새로운 기술이라는 뜻의 New Technology의 준말이다. MS-DOS와 이전 버전의 윈도우에서 쓰였던 마이크로소프트의 이전 FAT 파일 시스템을 대체하였다. NTFS는 FAT와 HPFS(고성능 파일 시스템)을 거쳐 몇 가지 개선이 있다. 이를테면, 메타데이터의 지원, 고급 데이터 구조의 사용으로 인한 성능 개선, 신뢰성, 추가 확장 기능을 더한 디스크 공간 활용을 들 수 있다.