

언택트 원격 환경의 사이버 보안 이슈 및 현황

조상현 Ph.D.

네이버 정보보호최고책임자(CISO)

The Joy of Tech™

by Nitrozac & Snaggy



© 2013 Geek Culture

joyoftech.com

우리 삶 속에 빠르게 다가온 언택트의 시대

언택트 (UN + CONTACT) , NO-CONTACT, ZERO CONTACT

소비 환경, 업무 환경의 변화

언택트 마케팅 : 사람과의 접촉을 최소화하는 비대면 형태의 마케팅 기법

기계로 메뉴를 주문하는 키오스크나 가상현실(VR) 쇼핑, 인공지능(AI) 챗봇

온라인 교육, 화상 회의, 원격(재택) 근무, 온라인 면접의 보편화



COVID-19 위기 상황과 보안 위협

사회적 이슈는 사회공학적 해킹 기법으로 빠르게 진화함

- ❖ 기존의 사이버 공격에 대한 탐지 대응 체계는 약화될 수 있음
- ❖ 원격근무 급증에 따른 네트워크 가용성의 문제와 정보 유출 가능성 증가
- ❖ 언택트 비즈니스에서의 신원 확인 한계와 이를 악용한 사이버 범죄의 급증
악성코드, 피싱 사이트, 금융 사기, 가짜 앱 등



(1) 화상 회의 증가에 따른 해커 공격 집중

- ❖ 줌 폭격 (Zoom Bombing) : 원격수업을 진행하던 중 신원을 알 수 없는 사용자가 입장하여 방해
- ❖ 공식 사이트가 아닌 블로그나 카페 등에서 악성코드가 포함된 설치파일 다운로드 설치
- ❖ 다양한 데이터 유출 가능성 (회의 내용, 캡처, 공유 자료 유출)
- ❖ 딥페이크 (Deepfake : 조작영상)의 확산 위협

Zoom says it has 300 million daily meeting participants, not users

로이터, 2020/04/30



March 30, 2020

FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic

COVID-19 팬데믹 중에 화상회의 및 온라인 강의실 하이재킹 공격에 대한 FBI 경고

Intel report warns Zoom could be vulnerable to foreign surveillance

DHS document urges government users to assess their risk.

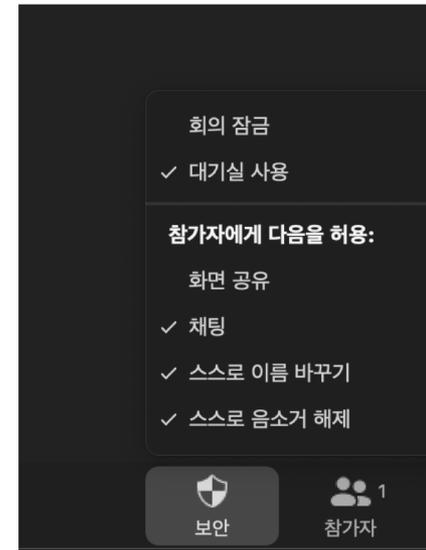
인텔보고서에서는 줌은 외부 감시에 취약할 수 있다고 경고

German government restricts use of Zoom over security concerns - reports

독일 정부는 보안 문제로 줌 사용 제한

화상 회의 보안 대책

1. 안전한 화상 회의 서비스 사용과 신속한 보안 업데이트
2. 회의방 무단 침입 방지를 위한 비밀번호 (PIN) 필수 사용
3. 회의 참여 웹 주소와 비밀번호 외부 공개 금지
4. 회의 참여자의 신원 확인하고 모든 참여자가 회의방에 입장 후에는 회의방 잠금(Locking)
5. 원칙적으로 회의내용 녹화 금지하고 녹화 시 적절한 암호화 조치
6. 회의 주최자만 PC화면 공유 가능하게 하고, 사적인 대화 차단



딥페이크(Deepfake) 위험성 증가

합성 사진의 수준을 넘어서 딥러닝과 같은 AI기술을 활용하여 사람의 얼굴이나 목소리를 흉내내는 기술 사진, 음성, 동영상등 '감쪽같은 가짜'에서 '완전한 가짜' 만들기



'하지도 않은 말이 화면
에'...'딥페이크' 영상 주의보 /
YTN



인공지능스타트업: Generated Photos

(2) COVID-19 키워드 악용 공격 위협 증가

- 피싱 메일 공격, 스미싱 공격, 악성 코드/악성앱 유포 (랜섬웨어 등)
- 코로나19를 주제로 한 피싱 공격 캠페인으로 정부 및 의료 기관을 대상으로 악의적인 공격 출현
- 국내도 2020년 1Q는 전 분기 대비 36%이상 증가했다는 통계

코로나19: 구글 하루 1천8백만 피싱 메일 삭제

🕒 2020년 4월 18일



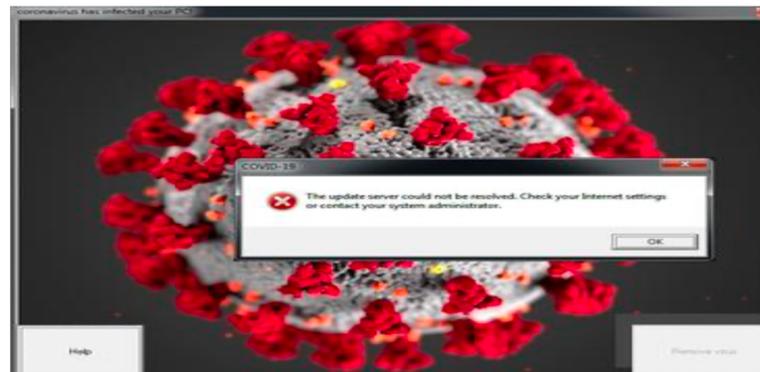
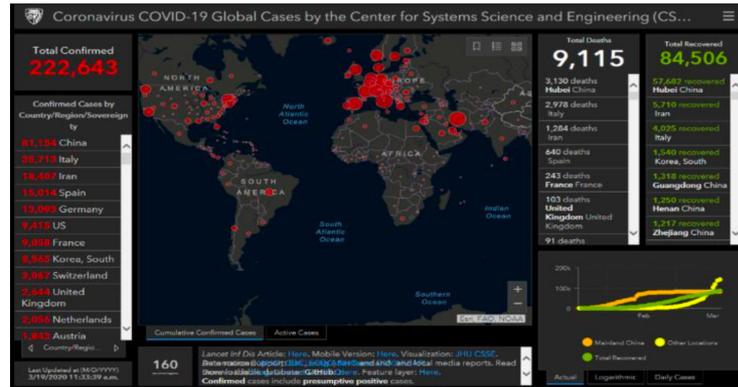
Latest updates on coronavirus disease outbreak

☆ 권아름 @ 2020년 2월 26일 오후 5:39
 코로나 바이러스 관련 이사장님 지사사항 [세부사항](#)
 받는 사람: 참조: 정기호

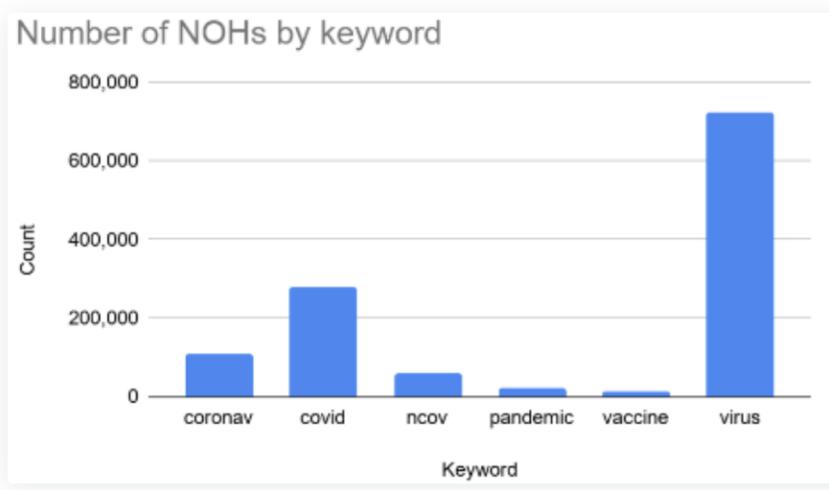
소장님들께,
 안녕하십니까, 경영관리부 권아름입니다.
 코로나19관련 이사장님 지사사항 송부드립니다.
 건강 유의하시길 바랍니다.
 감사합니다.



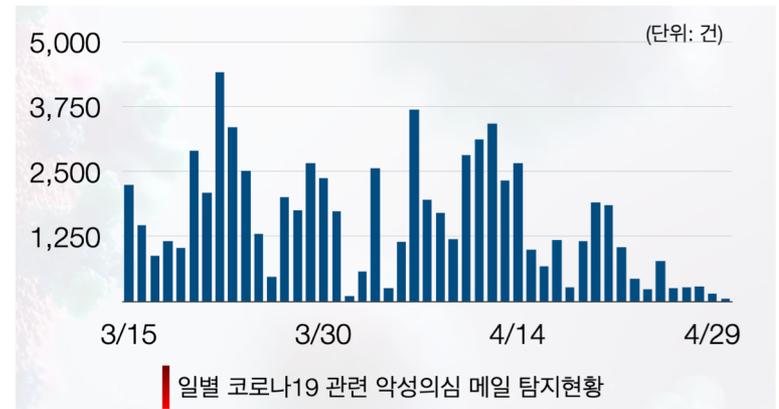
코로나바이러스 대
 용.doc



COVID-19를 키워드로 한 도메인들 생성이 급증하여, 대다수가 피싱 메일 공격 등에 활용됨
 신규 등록된 도메인 중 COVID-19 관련 키워드 도메인이 40% 이상 차지



출처: paloalto (2020/03/09~2020/4/26)



출처: 금융보안원

피싱 사이트 방문 및 악성(가짜) 앱 설치 유도

[Web발신]
 국내 우한폐렴 급속도확산
 감염자및 접촉자 신분정보 확인하기
news.naver.com.____.kr

[Web발신]
 코로나 전염병환자
 휴게소에서 수많은 사람과 접촉 http://___.kr/
 __X 접촉 휴게소 확인

011-9077-9155
 [Web발신]
 [긴급재난자금]
 상품권이
 도착했습니다.확인해
 주세요. <https://>

< 02-318-2458 📞 🔍 ⋮

연락처에 추가 수신 차단

2020년 4월 6일 월요일

[Web발신]
 [제로페이]
 김치냉장고
 모델명: DW-R159DCG
 1,679,000원 승인완료
 요청일:2020/04/06

오후 12:01

전염병 발생 마스크 무료로 받아주세요
http://goo.l/****

[CJ*통운]
 폐렴 바이러스의 영향으로 화물은 도달할 수 없다
http://bi**.net

(광고)
 신종코로나바이러스탐에 배송지연이 됨
 물품확인
http://tic.Comsu/****
 무료거부 080156****

글로벌 전염병 빅데이터 분석 자기방호
 어떻게 잘 할 수 있는지 지도조례 살펴보세요
www.bigp.kj/****



가짜 국세청 앱

사이버 허드렛일 확산

컴퓨터 사기 범죄자들, 자동화 봇이 아니라 값싼 노동력 선호

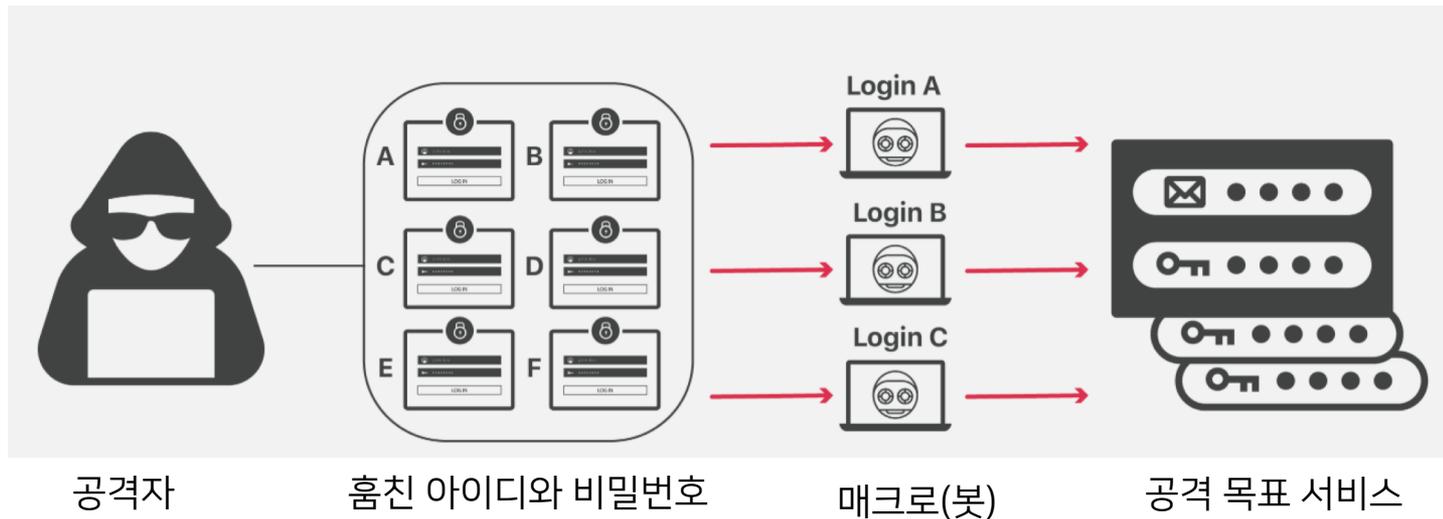
자동화 봇 사용했을 때보다 인간 고용하는 것이 공격 성공율 높아
비용 절감도 되고 공격 효율도 높아지고...유행하면 추적이 힘들어지기도



(3) 크리덴셜 스테핑 (Credential Suffing) 피해 급증

- 한 서비스에서 유출된 자격증명(크리덴셜)을 다른 서비스 로그인에 활용 시도하는 공격
- 약 0.1%는 성공한다는 이야기도 있지만...
- 2017년 11월부터 2019년 4월까지 세계 금융 업계를 대상으로 한 크리덴셜스텅 공격은 35억 건 (출처: Akamai)
“Akamai의 금융 서비스 고객 중 한 명에게 5천 5백만건의 악성 로그인 시도를 가했다”

연예인 폰 해킹 주범 '크리덴셜스텅'...해킹 배후도 밝혀지나



크리덴셜 스테핑 예방 방법

- 2차 인증 활성화
- 서비스 마다 유일한 아이디와 비밀번호 만들기
- 비밀번호는 더 길게 길게 만들기

NAVER

네이버 2단계 인증

통합검색

지식iN

블로그

카페

웹사이트

이미지

동영상

포스트

더보기

검색옵션

정렬

기간

영역

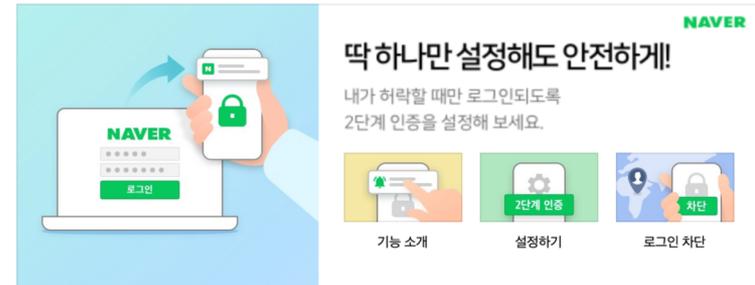
읍선유지

개집

커집

상세검색

브랜드 검색 '네이버2단계인증' 관련 광고입니다.



NAVER

딱 하나만 설정해도 안전하게!

내가 허락할 때만 로그인되도록
2단계 인증을 설정해 보세요.

기능 소개 설정하기 로그인 차단

NAVER 내정보

회원정보

보안설정

비밀번호

네이버 로그인 시 사용하는 **비밀번호**를 변경하거나 안전한 로그인
정할 수 있습니다. 주기적인 비밀번호 변경을 통해 개인정보를 안

비밀번호

[변경하기](#)

2단계 인증

NEW

[관리하기](#)

nid.naver.com 2차인증 로그인

NAVER

2단계 인증 알림이 발송되었습니다.

설정된 기기에서 인증 알림을 확인하세요.

이 브라우저에서는 "2단계 인증" 없이 로그인 합니다.

[알림 다시 보내기](#)

[OTP 인증번호를 입력하여 로그인 하기](#)

7:16

NAVER 2단계 인증

아이디의
2단계 인증 요청을
허락하시겠습니까?

요청 기기 Mac (OS X) Whale

요청 IP

아니오

예

로그인 차단 설정

타지역 로그인 차단

ON OFF

해외 로그인 차단

ON OFF

새로운 기기 로그인 알림

로그인 알림 받기

ON OFF

이전에 사용한 적 없는 PC나 모바일기기(브라우저)에서 로그인 하는 기록을 회원정보에 등록된
메일로 알려드립니다.

크리덴셜 스테핑 예방 방법

Google

구글 2단계 인증

전체 이미지 뉴스 동영상 지도 더보기

검색결과 약 7,160,000개 (0.33초)

www.google.com > landing

Google 2단계 인증

Google 계정을 더욱 안전하게 지키세요. 2단계 인증을 사용하면 비밀번호와 휴대전화 두 가지로 계정을 보호할 수 있습니다. 필요성; 사용 방법; 보호 효과 ... 이 페이지를 20. 6. 1에 방문했습니다.

support.google.com > accounts > answer

2단계 인증 사용 - Android - Google 계정 고객센터

1단계: 2단계 인증 설정. Android 스마트폰 또는 태블릿에서 기기의 설정 앱 다음 Google Google 계정을 엽니다. 상단에서 보안을 탭합니다. 'Google에 로그인'에서 2 ... 이 페이지를 20. 6. 1에 방문했습니다.

Google

Apple 2중 인증

전체 이미지 뉴스 동영상 지도 더보기

검색결과 약 18,000,000개 (0.49초)

support.apple.com > ko-kr

Apple ID의 이중 인증 - Apple 지원

5일 전 - 이중 인증은 다른 사람이 내 암호를 알아도 나만 계정에 접근할 수 있도록 설계된 화 기능입니다.

Google 2단계 인증

홈 기능 도움말

Google 계정을 더욱 안전하게 지키세요.

2단계 인증을 사용하면 비밀번호와 휴대전화 두 가지로 계정을 보호할 수 있습니다.

Apple ID의 이중 인증

이중 인증은 다른 사람이 내 암호를 알아도 나만 계정에 접근할 수 있도록 설계된 Apple ID의 보안 강화 기능입니다.



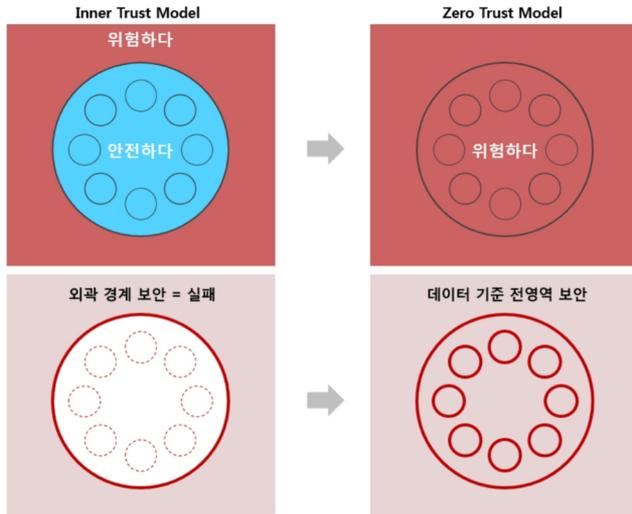
(4) 재택(원격) 근무 환경 보안 위협 증가

- ❖ 회사와 같은 보안 정책의 연속성을 유지하기 어려운 환경
- ❖ 상대적으로 안전하지 않는 네트워크/PC 환경
- ❖ 가정(공공 PC) 에서의 악성코드 감염/ 외부 침입으로 인한 정보 유출
- ❖ 위험 사이트 접근 제한 및 정보 유출 모니터링 차단 한계

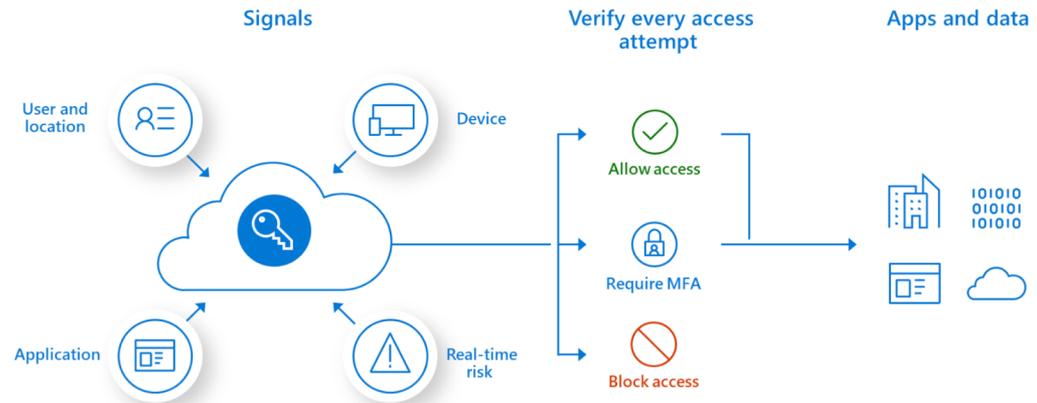


제로트러스트(Zero Trust) 보안 전략의 전환 필요

- ❖ 아무도 믿지 마라
- ❖ 시스템 외부와 내부를 따로 나누지 않고 모든 곳이 위험하다고 가정
- ❖ 누구든 시스템에 접근하려면 권한을 부여하기 전에 한번 더 인증
- ❖ 특히 접근하려는 데이터에 따라 보안 강도(추가 권한 확인 등)를 차별화



출처 : Pentasecurity



출처 : Microsoft

맷음말

1. 주기적으로 안전하게 중요한 데이터를 온라인/오프라인에 백업하기
2. 가정 내 정보 보안에도 신경 쓰기 (예. 공유기 보안 관리)
3. 비밀번호 안전하게 관리하기
4. 의심스러운 이메일, SMS, 메신저 주의하기
5. 항상 최신 소프트웨어로 업데이트
6. 소셜 미디어 프로파일 관리
7. 프라이버시 및 보안 설정 확인
8. 공공 PC 사용 조심하기

KISA 한국인터넷진흥원

과학기술정보통신부



<https://www.kisa.or.kr/covid19/main.jsp>