

2021-1

2021년 상반기

사이버 보안 소식

경기교육사이버안전센터(GECSC)



경기도교육정보기록원

■ INDEX

1

알기쉬운 해킹메일 대처법

2

랜섬웨어 예방수칙

3

무선AP 보안위협 및 예방법

4

가상화폐채굴 악성코드 감염

5

‘웹스크래핑’ 사이버공격일까?

6

2021년 상반기 보안 이슈 동향

별첨 1) 경기교육사이버안전센터 사이버침해 대응 현황

별첨 2) 신종피싱사기 예방 / 스마트폰 보안수칙 10



알기쉬운 해킹메일 대처법

해킹메일 수신시 주의사항

1. 발신자 메일주소가 **불분명한 주소**인지 확인
2. 업무 또는 공공기관 관련 메일은 **한번 상세히 확인**
3. 본문 내 삽입된 **URL 링크 의심하기**
4. 메일 내 첨부파일은 한번더 의심하기

:: 해킹메일 판별법 ::



1) 메일주소가 이상하지 않은지 먼저 확인해보세요!

예시

- @naver.com -> naver-com.cc
- @google.com -> @google.com
- @daum.net -> @dauum.net



2) 모르는 사람에게 온 메일 공공해 하지 마세요!

예시

OO이벤트 당첨, 항공권 파격 특가!



3) 사전에 안내되지 않은 메일 열람하지 마세요!

예시

경찰 출석요구서, 국내외 경세 자료, 정책 자료, 각종 업무 메일 등



4) 믿을 수 없는 첨부 파일 절대 열람하지 마세요!

예시

이력서, 송장·Invoice, 연말정산 자료, 연봉계약서 등



5) 클릭 할까? 말까? 함부로 클릭 금지!

예시

본문내용 상세보기, 비밀번호 변경하기, 메일함 용량 초과 등의 내용

해킹메일 열람시 유의사항

1. URL 링크 클릭 후 비밀번호입력 요구 시 입력금지
2. 추가로 수신된 의심스러운 메일 열람 금지
3. 정보유출 시 즉시 비밀번호 변경 및 로그인2단계 설정
4. 첨부파일 실행 시 백신정밀검사 즉시 실시



1) 백신 설치 및 최신업데이트

- 바이러스 백신 소프트웨어 설치 및 최신유지
- 운영체제(OS) 및 업데이트 포함



2) 로그인 보안 강화

- 이메일 비밀번호 수시 변경
- 문자(SMS), 모바일OTP(mOTP) 등 2단계 인증 로그인설정



3) 의심메일 열람금지

- 예정되지 않은 업무 메일, 스팸 메일 등 열람금지
- 의심 메일 수신시 발신자에게 유선 및 문자로 확인



4) 패스워드 입력금지

- 이메일에 링크된 홈페이지를 통한 비밀번호 입력금지
- 패스워드 변경은 해당 홈페이지에 직접 방문



5) 첨부파일 실행주의

- 보안 메일 또는 사전 인지시에만 실행
- 그외의 경우에는 발신자에 확인 후 실행



6) 로그인 이력 수시점검

- '로그인 이력' 조회를 통해 비정상 로그인 수시 확인
- '해위 로그인 차단' 기능 적극 활용

▲ 출처 - KISA 인터넷보호나라&KrCERT ; 해킹메일 (<https://www.boho.or.kr/hackingmail/illustMain.do>)



랜섬웨어 예방수칙



랜섬웨어가 뭐죠?

몸값(Ransom)과 **소프트웨어(Software)**의 합성어로 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 하고 이를 인질로 금전을 요구하는 악성 프로그램



랜섬웨어 감염경로

1. 신뢰할 수 없는 사이트

· 보안관리가 미흡한 사이트 접근(무료게임 사이트, 불법 사이트등)

2. 스팸메일 및 스피어피싱

· 출처가 불분명한 이메일 내 URL링크 열람 및 첨부파일 실행

3. 파일공유 사이트

· 토렌트, 웹하드등 P2P사이트를 통한 파일 다운로드 실행

4. 사회관계망서비스(SNS)

· 페이스북, 인스타그램, 카카오톡등 사회관계망서비스(SNS)에 게시된 단축URL 클릭 실행



랜섬웨어 피해 예방 수칙

KISA 한국인터넷진흥원



나의 소중한 자료를 지키는

랜섬웨어 피해 예방 5대 수칙

랜섬웨어란?
Ransomware

몸값 + 소프트웨어
Ransom + Software

시스템을 잠그거나 데이터를 암호화하여 사용할 수 없도록 하고 이를 인질로 금전을 요구하는 악성 프로그램

1 모든 소프트웨어는 최신 버전으로 업데이트하여 사용합니다.



운영체제 OS



응용 프로그램 SW

> 최신 보안 업데이트



2 백신 소프트웨어를 설치하고, 최신 버전으로 업데이트 합니다.



신뢰할 수 있는 백신



악티 익스플로잇 도구

> 백신 설치, 최신 업데이트



3 출처가 불명확한 이메일과 URL 링크는 실행하지 않습니다.



스팸메일 첨부파일



URL 링크

> 이메일 및 URL 실행 주의



4 파일 공유 사이트 등에서 파일 다운로드 및 실행에 주의합니다.



P2P 토렌트, 웹하드 등 파일공유 사이트



신뢰할 수 없는 사이트

> 파일 다운로드 및 실행 주의



5 중요 자료는 정기적으로 백업합니다.



문서



사진

> 별도 매체 백업



정보보호 안내 | KISA 보호나라 | KrCERT www.krcert.or.kr | KISA 118 센터

▲ 출처 - KISA 인터넷보호나라&KrCERT ; 랜섬웨어 (<https://www.boho.or.kr/ransomware/information.do>)



사이버침해사고신고 : 경기교육사이버안전센터(GECSC) 031-240-6599

E-mail : boan@goe.go.kr



경기도교육정보기록원
Gyeonggi-do Education Information Archive



무선 AP 보안위협 및 예방법



무선AP 보안 위협

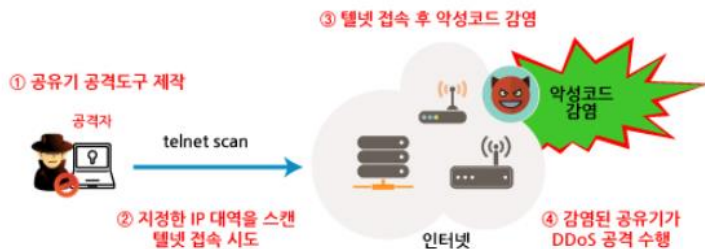
① 통신데이터 정보유출

:무선AP기기의 인증패스워드를 기본 사용하거나 취약한 인증방식(WEP)을 사용함으로 인해 민감정보 유출사고 발생 위험



② DDoS 공격 악용

:무선AP기기의 관리 편의성을 위해 기본계정 및 기본패스워드를 사용하여 DDoS 공격 도구로 사용될 수 있는 위험



③ DNS 변조 (피싱사이트 및 악성사이트접근 피해)

:기본설정으로 인한 무선AP기기의 DNS설정 변조가 발생, AP기기에 연결된 디바이스에 잘못된 DNS정보 전달로 인한 보안위협 및 2차사고 발생



무선 AP 보안관리 가이드

- ✓ **접근통제** : 무선AP 관리자페이지 접근제한, 관리자 ID/PW 초기 설정 사용 금지, 무선인증 취약한 비밀번호 사용금지
- ✓ **서비스 보안관리** : 무선AP 내 불필요한 외부 접속 포트 또는 텔넷 FTP등의 서비스는 비활성화, 필요시 강화된 비밀번호 설정
- ✓ **강도높은 암호화방식** : 무선AP에서 사용할 무선암호화방식은 보안강도가 높은 WPA2 또는 WPA3로 기본설정 필요

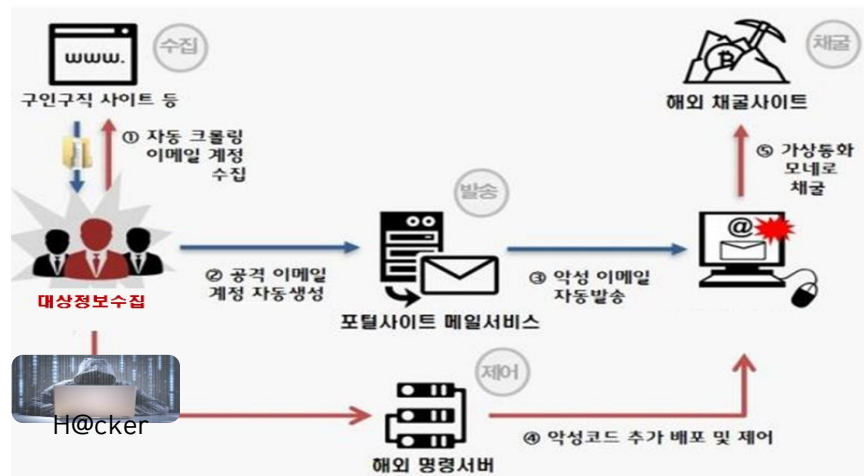
▲ 출처 - KISA 인터넷보호나라&KrCERT ; 인터넷공유기 (<https://www.krcert.or.kr/cyber/internetModem.do>)





가상화폐채굴 악성코드감염

가상화폐채굴 악성코드감염 사례



▲ 이미지출처 - 데일리시큐 (<https://www.dailysecu.com/news/articleView.html?idxno=40854>)

- 가상화폐채굴 악성코드감염 대상자 정보 수집

: 포털, 커뮤니티 사이트등에서 무작위로 감염대상 이메일 정보 수집

- 감염 대상자에게 악성코드 삽입된 메일 발송

: 공공기관 혹은 업무관련 메일로 악성 첨부파일이 삽입된 메일 발송

- 대상자 PC 또는 스마트기기에 악성코드(악성앱) 설치

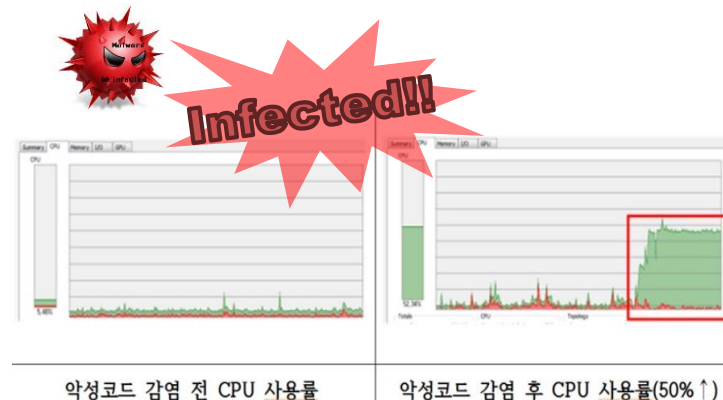
: 자주 사용하는 기기에 악성코드(악성앱) 설치되는 해외 C&C서버로 연결

- 악성채굴그룹(해커)에서 대상자에 추가 악성코드 배포

: 악성채굴집단 혹은 개인이 감염대상자 기기에 추가 악성코드 배포로 채굴 이외 개인정보유출 시도



채굴 악성코드 감염되었다면?



▲ 이미지출처 - 데일리시큐 (<https://www.dailysecu.com/news/articleView.html?idxno=40854>)

✓ 채굴악성코드 감염 시 체크 사항

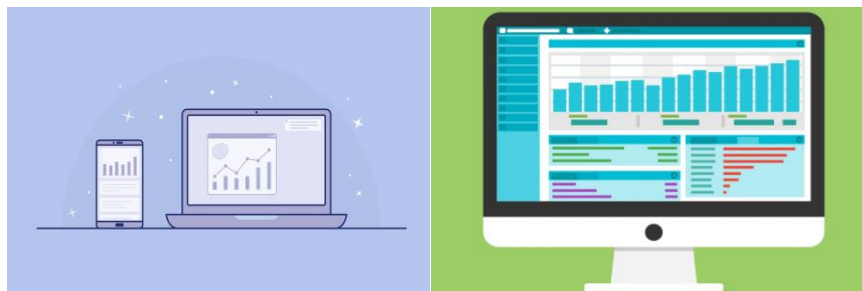
- ❌ 파일(프로그램) 다운로드 후 컴퓨터 성능 저하 체감
- ❌ 인터넷브라우저 실행 시 급격스런 느림 현상 발생
- ❌ 채굴 시 전력소모가 급증하므로 잦은 다운 현상 발생
- ❌ 모바일기기 감염 시 급격한 데이터량 소모 발생



‘웹스크래핑’ 사이버공격일까?



웹 스크래핑이란?



- **개념** : 웹사이트 내 존재하는 특정 데이터를 원하는 부분만을 추출하는 기법
- **목적** : 웹에서 공개되는 데이터를 자동으로 수집하여 추출하고 추출된 데이터를 재가공하여 여러가지 용도로 사용하기 위함
- **동작** : 웹스크래핑을 하기 위한 봇을 설정하고 자동화된 봇은 수집대상 서버에 HTTP GET 요청*을 보낸 후
*URL 형식으로 데이터를 요청함
웹서버에서 전송하는 모든 정보를 복사 저장



웹스크래핑 기법이 사이버공격 ??



- 무분별한 웹스크래핑 등으로 인해 특정 대상을 추정할 수 있는 표적 데이터가 완성되어 공격에 노출
- 수집 추출된 메타데이터들을 재 조합으로 특정 그룹의 사용자 이름, 이메일 등 크리덴셜*한 정보를 획득, 대표적인 웹스크래핑 *정보시스템에서 개인정보를 암호화하는 암호학적 정보를 통틀어 이르는 말
사이버공격 사례에는 페이스북 정보유출 사고가 있음



웹스크래핑 방어책

- ✓ 웹사이트 내 민감 데이터는 공공인터넷에 노출되지 않도록 함
- ✓ (기술적 조치) 웹스크래핑 시 발생하는 오류메시지 최소화
- ✓ (기술적 조치) 무분별한 웹스크래핑을 방어하기 위해 HTTP GET 요청률 제한 설정과 캡차*인증설정 도입

*사용자가 실제 사람인지 컴퓨터 프로그램인지를 구별하기 위해 사용되는 방법



2021년 상반기 보안 이슈 동향

2021년 1월 보안 이슈

- [보안뉴스] [10만개이상 Zyxel방화벽과 VPN에 백도어 발견](#)
- [보안뉴스] [정보유출파일암호화 동시에...타깃형 랜섬웨어 ↑](#)
- [보안뉴스] [모질라 파이어폭스 임의코드 실행 취약점 주의](#)
- [보안뉴스] [시스코 제품 심각한 보안취약점 주의...업데이트 필수](#)
- [보안뉴스] [인터넷 익스플로러 취약점 공격 급증했다는데.](#)

2021년 2월 보안 이슈

- [보안뉴스] [파일공유사이트 위장한 피싱메일 유포](#)
- [보안뉴스] [포티넷, 웹방화벽 보안취약점 주의...패치 필수](#)
- [보안뉴스] [치명적인 리얼텍 와이파이 모듈 취약점 발견](#)
- [보안뉴스] [리눅스 시스템 관리자 권한 획득 취약점...주의](#)
- [보안뉴스] [재택근무 중 보안사고 1위 "정보유출과 이메일 해킹"](#)

2021년 3월 보안 이슈

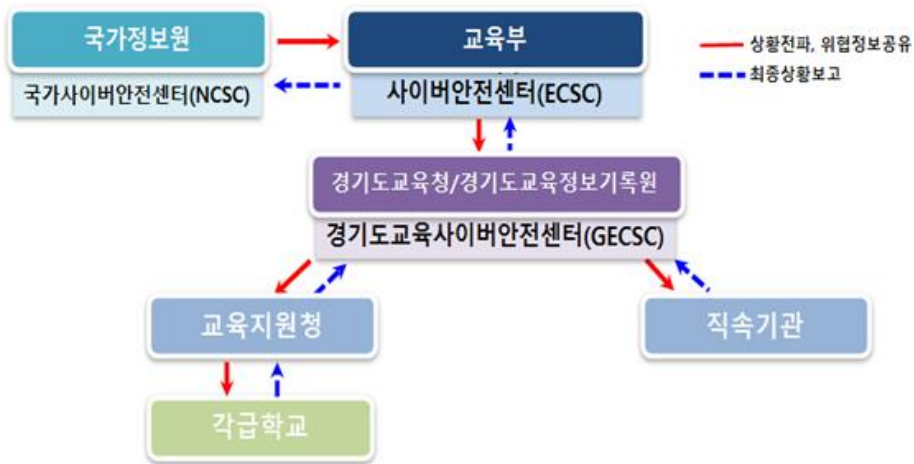
- [보안뉴스] [제주항공·에어서울 탑승객 개인정보 유출됐다](#)
- [보안뉴스] [한국 웹사이트 8곳 해킹? DB 정보 뺏김에 유출](#)
- [보안뉴스] [MS 익스체인지 서버 취약점 이용 랜섬웨어 유포](#)
- [보안뉴스] [구글, 악성플러그인 20개, 악성 도메인 40개 넘게 발견](#)
- [보안뉴스] [OpenSSL 보안취약점 주의...최신 버전 사용 권고](#)

2021년 4월 보안 이슈

- [보안뉴스] [익스체인지 사태로 유명해진 차이나 초퍼, 웹쉘이란?](#)
- [보안뉴스] [페이스북 전세계 5억명 개인정보 유출... 韓 12만명?](#)
- [보안뉴스] [요즘 피싱 메일은, URL 대신 'HTML 첨부파일'](#)
- [보안뉴스] [라자루스, BMP 파일에 악성 요소 숨겨 한국 공격 중](#)
- [보안뉴스] [리눅스 멀웨어 IaC 도구 악용, 암호화폐 채굴 중](#)

[별첨1] 경기교육사이버안전센터 사이버침해 대응 현황

사이버침해 대응 체계



사이버침해 대응 절차

- **사고탐지**: 보안관제시스템에 의한 탐지 및 각급기관으로부터 신고 접수
- **사고분석**: 탐지된 사고 분석(웜·바이러스 등)
- **초동조치**: 해당기관에 침해사고 통보 및 초동 조치 안내
- **사고대응**: 방화벽 등 로그 분석, 악성코드 검사 및 치료
- **사고종결**: 재발방지 대책 수립 및 공유

2021년 상반기 침해사고 유형별 현황(2021.1월 ~ 4월)

구분	침입 시도	해킹 메일	악성코드 감염	웹 해킹	경유지 악용	서비스 거부공격	합계
건수	3,525	13	307	0	33	0	3,878

* 상반기 침해사고 유형 중 **침입시도건**이 가장 많이 발생되었으며, 이는 각 기관 홈페이지를 대상으로 한 공격시도 이벤트가 다수 발생
↳ 이를 대응하기 위해 이벤트 분석 후 관련 IP 차단 및 URL차단을 조치하였습니다.

[별첨2] 신종피싱사기 예방 / 스마트폰 보안수칙 10

과학기술정보통신부 KISA 한국인터넷진흥원

신종 피싱 사기 조심하세요!

휴대폰 문자 · SNS 등으로

- 코로나19 재난지원금 지급
- 대출 상담 / 연말정산 환급금
- 설 택배 배송시간 확인

등을 빙자해

가짜이나 지인을 사칭하여
통화할 수 없는 상황
(폰 고장 등)을 가장해

출처 불명의 인터넷주소(URL) 접속
& 악성앱의 설치를 유도

다른 사람 전화번호로
개인정보를 요구

최근 보이сп이스 · 스미싱 신고 사례

이 Web 발신

[Web 발신]
코로나19 경제지원
신청
nat*.tg*e.chat

※ 주의 해
부르지 마세요

[Web 발신]
설 택배
배송시간 확인
tinyurl.com/
y6m*algt

02. SNS 발신 연말정산 환급금 확인 친구 추가

03. 기타 발신 폰 고장을 이유로 타 전화번호로
부모 신분증 등 개인정보 요구 등

일상에서 지켜주세요

스마트폰 보안수칙 10

- 스마트폰 운영체제와 모바일
백신 최신으로 업데이트하기
- 공식 앱 마켓이 아닌
다른 출처의 앱 설치 제한하기
(출처를 알 수 없는 앱)
- 스마트폰 앱 설치 시
과도한 권한을 요구하는 앱은
설치하지 않기
- 문자 또는 SNS 메시지에
포함된 URL 클릭하지 않기
- 스마트폰 보안 잠금을
설정하여 이용하기
(비밀번호 또는 화면 패턴)
- 스마트폰 WiFi 연결 시
제공자 불분명한 공유기
이용하지 않기
- 루팅, 탈옥 등을 통한
스마트폰 플랫폼의 구조
임의변경 금지
- 스마트폰에 중요정보
저장하지 않기
(주민등록증, 보안카드 등)
- 스마트폰 교체 시 개인정보 등
데이터 완전삭제 혹은
초기화 적용
- 스마트폰, SNS 등 계정 로그인
2단계 인증 설정하기

국가정보원 과학기술정보통신부 KISA 한국인터넷진흥원

◆ 신종피싱사기 예방 / 스마트폰 보안수칙 10 (KISA 인터넷보호나라&KrCERT)
- 출처 (<https://www.krCERT.or.kr/main.do>)