

글로벌 인터넷 · 정보보호 주간 동향

Global Internet & Security Weekly Trends

CONTENTS

인터넷서비스

- WebRTC(Web Real-Time Communications), 10년 만에 공식 표준 지정
- 2020년 미국 온라인광고 시장, 아마존 점유율 10% 넘어

개인정보보호

- 코로나19 백신여권, 세계 각국에서 차별·프라이버시 논란 직면
- 일본 정부, 마이넘버카드 보급·이용 확대 추진
- 미국, 안면인식을 중심으로 생체인식 관련 규제 확산
- 프랑스 CNIL, 쿠키 등 트래커에 대한 새 지침 발표
- 이탈리아 국무원, Facebook의 불법광고 과징금 관련 상고 기각
- 유럽 인터넷광고협회, '정당한 이익(legitimate interests)' 관련 지침 발행
- AI 이루다 개인정보 유출 피해자, 개발사 상대로 손해배상 청구 소송 제기

사이버침해

- Google Play의 가짜 Netflix 앱이 WhatsApp을 통해 악성코드 전파
- GitHub 서버에서 암호화폐 채굴을 위해 악용되는 GitHub Actions
- 유럽이사회, 신규 EU사이버보안 전략 채택

정보보호산업

- 움디아, 서비스형 통합 물리보안 시장 전망

인터넷서비스

인터넷기반단 인터넷기반조성팀

WebRTC(Web Real-Time Communications), 10년 만에 공식 표준 지정

- W3C와 IETF는 오늘 수많은 서비스를 제공하는 웹 실시간 커뮤니케이션(WebRTC)이 이제 웹상의 모든 곳에서 오디오와 비디오 통신을 제공하는 공식 표준이 되었다고 발표

WebRTC가 W3C 권고 및 IETF의 공식 표준으로 지정**▶ WebRTC는 이미 온라인 커뮤니케이션 및 협업 서비스의 초석 역할**

- WebRTC는 브라우저에서 실시간 통신을 가능하게 하는 웹용 개방형 프레임 워크로, 음성 및 영상 채팅 애플리케이션에 사용되는 네트워크, 오디오 및 비디오 구성 요소와 같은 웹에서의 고품질 통신을 위한 기본 구성 요소가 포함
- 이러한 구성 요소는 WebRTC는 네트워크에 연결된 모든 장치가 웹에서 잠재적인 통신을 할 수 있도록 쉽게 구현이 가능
- W3C CEO인 Jeff Jaffe 박사는 "오늘날의 획기적인 업적은 시기적절합니다. COVID-19 코로나 바이러스의 세계적 유행병에 직면하면서, 세계는 점점 더 가상으로 변해가고 있다. 그것은 정보 공유, 실시간 커뮤니케이션, 그리고 오락 분야에서 웹이 사회에 훨씬 더 중요하도록 만듭니다," "이렇게 중요한 디지털 인프라를 구현하는 데 우리의 기술이 핵심적인 역할을 하는 것을 보니 매우 기쁩니다. 웹의 보편적 영역과 라이브 오디오 및 비디오 대화의 풍부함을 결합함으로써 세계가 소통하는 방식을 재편성했다." 라고 언급
- 2020년은 웹 RTC가 여행 및 물리적 접촉을 제한해야 하는 세계에서 이미 얼마나 중요한지 뿐만 아니라 출현한 새로운 사용법을 해결하기 위해 기술에 가져올 수 있는 많은 개선점을 보여줌
- WebRTC의 이점을 사용하여 서비스 제공 업체가 소비자 및 기업 고객을 위한 새로운 음성, 비디오 및 협업 서비스를 제공 할 수 있는 통신 제품을 만들 수 있도록 솔루션을 개발하기 시작
- 기업과 가계는 웹 RTC에 의존하여 웹 RTC의 채택을 늘리고 있으며, 조직들은 WebRTC를 활용하여 교육, 인터뷰, 전략적인 계획을 수립하거나 직접 미팅하는 대신 기타 사회적 상호 작용을 통해 지속적으로 연결될 수 있도록 지원
- 직접 미팅을 대체할 뿐만 아니라 현재 사무실 내부의 인적 상호 작용도 대체, 학교와 대학이 가상학습 플랫폼으로 전환하였으며, 클라우드 게임과 소셜 네트워크는 라이브 스트리밍과 대화형 방송을 사용
- 엔터테인먼트는 원격으로 관객들을 스튜디오로 불러들이는 방법을 찾고 있으며, 스포츠는 WebRTC를 사용하여 경기장 내 경험을 재현하려고 노력중이고, 가족과 친구들은 WebRTC나 그것의 일부분으로 만들어진 제품을 매일 사용하는 등 WebRTC의 미래는 이미 진행 중

[출처]

- Infoq, "10 Years after Inception, WebRTC Becomes an Official Web Standard", 2021.4.5.

인터넷서비스

블록체인진흥단 핀테크진흥팀

2020년 미국 온라인광고 시장, 아마존 점유율 10% 넘어

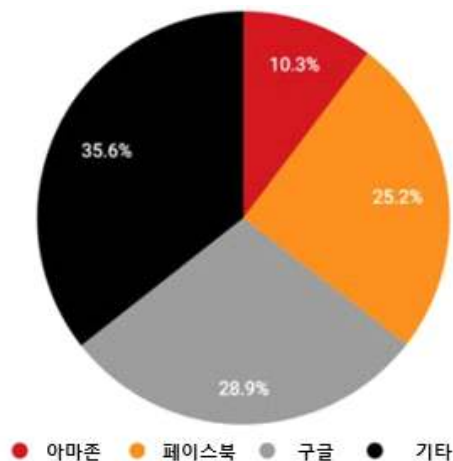
- 아마존의 美 온라인광고 시장 점유율이 7.8%('19년)에서 10.3%('20년)로 증가
- 아직 구글과 페이스북의 점유율에는 못 미치나, 전자상거래 확대, 아마존 검색광고 수익 증가, 쿠키 중단으로 인한 광고주의 전자상거래 플랫폼 의존도 강화 등의 이유로 지속적인 점유율 증가 전망

eMarketer는 美 온라인광고시장 내 아마존의 점유율이 증가하고 당분간 상승세가 계속될 것으로 전망했는데, 이는 코로나19로 인한 전자상거래의 급증과 쿠키 중단으로 인한 전자상거래 플랫폼 의존도 증가에 기인

▶ '20년 코로나19로 인한 전자상거래의 급증으로 아마존의 온라인광고 상승세가 가속화되면서 미국 내 온라인광고 시장점유율이 전년 대비 약 3%p 증가(10.3%)

- 월스트리트저널(WSJ)에 따르면 아마존의 美 광고 수익은 전년 대비 52.5% 증가한 157.3억 달러를 기록
- '20년 美 온라인광고 시장점유율에서 구글은 전년대비 감소(31.6%→28.9%), 페이스북은 소폭 상승(23.6%→25.2%)

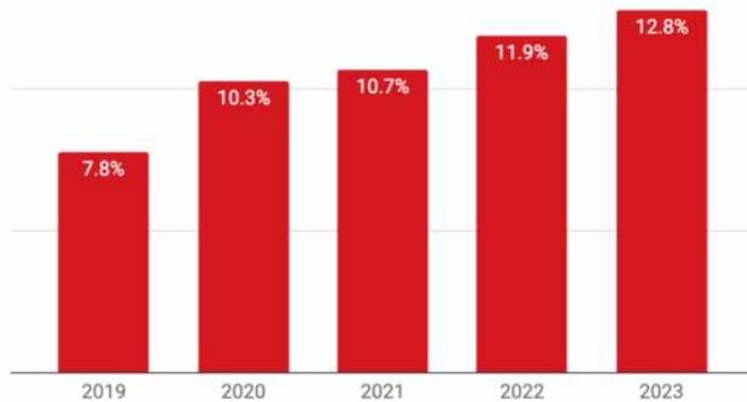
< 미국 온라인광고 시장점유율 ('20년) >



▶ 현재 구글(28.9%)과 페이스북(25.2%)이 여전히 높은 시장점유율을 차지하고 있긴 하지만, 상승 추세에 있어서는 아마존의 점유율이 '22년 11.9%, '23년 12.8%로 지속 상승할 것으로 전망

- 아마존은 페이스북에서도 약간의 점유율을 가져오긴 했지만 검색 광고 등 주로 구글과 경쟁하는 상황
- eMarketer에 따르면 美 온라인광고 지출에서 구글의 점유율은 '20년 28.9%에서 '23년 26.6%로 감소 예상
- '20년 중반, eMarketer는 구글의 美 온라인광고 수익이 '19년 418억 달러에서 '20년 390억 달러로 처음으로 감소를 기록할 것으로 전망

< 美 온라인광고시장 내 아마존 시장점유율 변화 (전망치 포함, '19-'23) >



▶ 아마존의 검색 광고 수익은 올해 145억 달러, 美 전체 검색광고 지출의 19%로 '19년(13.3%)보다 증가할 것으로 예상되며 구글의 '21년 검색 점유율은 56.8%로 예상

- 구글의 서드파티 쿠키 중단으로 인해 광고주들이 아마존 및 기타 자사 데이터 기반 전자상거래 플랫폼에 더 많이 의존하게 되면서 아마존의 이익이 증가할 것으로 전망됨

[출처]

- MediaPost, "Amazon Share Of U.S. Digital Advertising Tops 10%", 2021.4.6.

개인정보보호

개인정보정책단 개인정보정책기획팀

코로나19 백신여권, 세계 각국에서 차별·프라이버시 논란 직면

- ▶ 영국 의회 의원 70명 이상이 공식 성명을 통해 코로나19 백신증명(혹은 백신여권)* 도입에 대한 반대 의사를 표명('21.4.2)
 - * 코로나19에 이미 걸린 적이 있거나, 테스트 결과 음성 판정을 받았거나, 혹은 백신 접종을 받은 사실을 입증
- 영국 정부는 경제 정상화 계획의 일환으로 백신증명을 소지한 사람에 한해 술집, 경기장 등 다중 이용 시설 입장을 허용하는 방안을 검토 중이며, 향후 수 주 내에 스포츠 경기장과 공연장 등을 대상으로 시범 서비스를 시행할 예정
- 반대 성명에 참여한 여야 의원들은 “코로나19 증명서로 시민을 나누고 차별하는데 반대한다”는 입장. 시민사회에서도 같은 맥락의 목소리가 작지 않기 때문에 백신증명이 실제 도입될지 여부는 미지수
- ▶ 미국 플로리다에서는 코로나19 백신여권*의 사용을 금지하는 주지사 행정명령이 발동됨('21.4.2)
 - * 바이든 행정부는 비영리 테크 기업들과 공동으로 백신증명 표준을 개발 중. 그러나 백악관 언론 담당 비서관 Jen Psaki는 ‘(해당 표준이 개발되더라도) 모든 미국 주민에게 백신증명을 의무화하는 연방 차원의 조치는 없을 것’이라고 언급('21.3.29)
- 동 명령에 따르면 주내 어떠한 공공기관도 백신여권을 발급할 수 없으며, 민간 사업장들 역시 그런 종류의 문서를 손님이나 구직자에게 요구할 수 없음
- 이와 관련, 플로리다의 Ron DeSantis 주지사는 ‘백신여권은 백신 접종 여부에 따라 시민을 사실상 두 부류로 나누는 결과를 초래할 것’이라며, ‘백신 증명을 보여주지 못하면 평범한 사회활동조차 불가능해질 상황을 용납할 수 없다’고 강조
- 한편, 미국 인권단체인 ACLU(American Civil Liberties Union)는 백신여권으로 인한 프라이버시 침해 위험도 지적하고 있는데, 예를 들어 중앙 집중형 시스템 기반의 여권일 경우에는 ‘내가 언제 어디서 백신 증명을 내보였는지 정부 기관에 낱알이 보고’될 수 있기 때문
- ▶ 독일 개인정보보호컨퍼런스(DSK)*에서는 코로나19 백신증명 규제를 위한 한시적 연방법 제정을 촉구하는 결의안을 채택('21.3.29)
 - * German Data Protection Conference 혹은 Datenschutzkonferenz: 독일 내의 모든 개인정보 감독기구가 참석해 프라이버시 보호 관련 가이드라인 등을 발표하는 정례회
- 백신증명의 역기능을 최소화하기 위해서는 코로나19 관련 건강정보의 처리 조건 및 처리 주체를 연방 차원에서 법으로 규정해 독일 전역에 일괄 적용할 필요가 있다는 것이 감독기구들의 판단
- 아울러 백신 증명 규제법은 GDPR 제9조제2항(특정 범주 개인정보의 처리 조건 - 동의, 공중보건 분야에서의 공익 등)의 요건에 부합하는 내용이어야 한다는 것이 해당 결의안의 주문

[출처]

- Reuters, “Opposition grows against UK vaccine passports”, 2021.4.2.
- CNN, “Florida governor bans Covid-19 'vaccine passports'”, 2021.4.3.
- LfDI, “Debatte zu Impfpass nimmt Fahrt auf - Datenschützer fordern Bundesgesetz”, 2021.3.31.

개인정보보호

개인정보정책단 개인정보정책기획팀

일본 정부, 마이넘버카드 보급·이용 확대 추진

▶ 일본 디지털개혁법안이 중원본회의에서 통과됨에 따라 마이넘버카드* 이용 확대 추진 예고('21.4.6)

* 일본 마이넘버카드는 사진과 개인고유번호가 포함된 IC칩 내장 플라스틱 카드. 신분증으로 사용 가능하나 의무 발급이 아니며 개인정보 노출에 민감한 일본인들의 정서가 겹쳐 지금까지 실제 활용은 저조한 상태

- 일본 정부는 디지털개혁의 일환으로 '23년 3월까지 마이넘버카드를 전 국민에게 보급해 신원 및 자격 확인 시스템을 일원화할 방침
- **(편리성 향상)** 마이넘버카드에 개인정보를 집약시켜 ▲대학 학생증 및 장애인 증명서('20년) ▲교원증('21년) ▲직업소개소 등록증('22년) ▲직무경력 및 훈련내역 확인증('22년) ▲운전면허증('24년) 등을 포괄적으로 겸하게끔 지원 예정
- **(활용 범위 확대)** 또한 금융·의료 기관 등과 연계하여 마이넘버카드를 통한 ATM 거래 및 주민등록증·인감증명서 발급을 지원하고, 향후 이 카드에 ▲의료보험증('21년 10월) ▲의료 처방 관리 수첩*('23년) ▲요양보험 자격확인서('23년) 등도 통합시킬 예정
- * 처방약의 상세정보 및 환자 알레르기 등의 정보를 저장
- **(국가와 지방 연결 디지털 기반 구축)** 마이넘버카드 관련 시스템 및 각종 지자체시스템을 정부관계 시스템과 묶어 통일된 디지털 시스템 구축
- **(디지털정부 체제 강화)** 해외에서도 마이넘버카드를 사용할 수 있도록 마이넘버카드에 서력, 로마자 표기도 병기하도록 법제화

▶ 일본 마이넘버카드 소지자에게 5만원 상당의 포인트 지원하자 접수 50% 이상 증가

- 일본 국민의 마이넘버카드 보급을 확대하기 위해 미소지자에게 QR코드가 든 신청서를 발송하여 온라인 신청을 장려하고 발급자에게는 마이* 포인트 지급 및 행정수속 우선처리 등의 인센티브 제공
- * 마이넘버의 약칭
- 마이넘버카드 소지자에게 5천엔 포인트*를 지급('20년 9월~'21년 3월)하자 하루 신청자 수가 22만 건으로 폭주하는 등 3월 말 기준으로 4,549만 건(3,590만 장 교부 완료)이 접수되어 전 국민 50% 소지가 가시화
- * 일본정부는 보급률을 높이기 위해 당초 3월 말까지였던 포인트 지급 기한을 4월 말로 연장
- 한 정부 관계자는 에스토니아 등의 전례를 근거로 '국민의 절반이 카드를 보유하면 보급 속도는 더욱 빨라진다'며 전 국민 보급 목표 달성에 기대감을 피력

[출처]

- Yahoo Japan, "デジタル庁法案、衆院通過へ 内閣委が可決", 2021.4.2.
- Yahoo Japan, "デジタル改革法案、衆院通過 マイナンバーの利用拡大", 2021.4.6.
- Yahoo Japan, ""お得期限"延長効果で1日22万件申請!国民の半数取得も見えてきたマイナンバーカードの便利度と課題", 2021.4.6.
- 内閣官房番号制度推進室兼内閣官房情報通信技術(IT)総合戦略室, "マイナンバー制度とデジタル化のこれから", 2020.12.10.

미국, 안면인식을 중심으로 생체인식 관련 규제 확산

▶ 안면인식 등 생체인식 정보의 수집 및 활용을 규제하는 법이 미국 각지로 급속 확산될 전망

- 텍사스, 일리노이, 워싱턴주는 생체인식 정보 수집 시 사전 안내 및 동의 획득을 의무화하는 내용의 법을 이미 도입했고, 뉴욕, 오클라호마, 켄터키 등 여타 주에서도 유사한 성격의 입법이 추진되고 있음
- 생체인식 분야의 여러 기술 중에서도 특히 안면인식은 당사자의 동의를 구하지 않은 채 일반적인 인물사진까지 식별 자료로 활용 가능하다는 점에서 주요 규제 대상으로 지목되고 있으며 이와 관련된 집단소송 사례도 이미 존재
- 단적으로 Facebook의 경우, 얼굴인식 기능을 이용해 일리노이 사용자들의 개인정보를 무단 수집한 혐의로 집단 소송*을 당해 총 6억 5,000만 달러의 합의금을 지불기로 합의
- * 해당 소송은 사진이나 동영상 속의 사용자 얼굴을 자동으로 인식해 태그를 제안하는 기능에 관한 것인데, 일리노이주 생체정보보호법에 따르면 기업이 얼굴이미지, 지문, 홍채 등 생체정보를 수집할 경우 사용 목적과 보관 기간 등을 소비자에게 구체적으로 설명하고 사전 동의를 구해야 하지만 Facebook 측은 문제의 기능을 '기본 활성화' 상태로 출시
- 개별 도시 차원에서도 안면인식에 대한 규제 움직임이 나타나고 있는데, 포틀랜드시의 경우는 대중 이용 시설에서 해당 장비의 사용을 전면 금지하는 조례를 이미 시행 중이고, 뉴욕시는 안면인식 장비의 사용 자체는 허용하되 그에 대한 공지를 시설 입구 근처에 눈에 잘 띄도록 배치할 것을 의무화

▶ 또한 기업들 입장에서는 안면인식 정보 무단 수집 시 지역별 법규와 별개로 미국 연방 차원의 제재를 받을 수 있다는 점 또한 유의할 필요가 있음

- 지난 1월, 미국 연방거래위원회(Federal Trade Commission)는 인물 사진을 당사자 동의 없이 안면인식 AI 훈련에 활용한 Everalbum에 대해 '이용자들이 업로드 한 사진이나 동영상으로부터 (무단으로) 입수한 모든 데이터(face embedding)와 이를 일부라도 활용해 개발한 일체의 알고리즘 및 모델을 삭제'할 것을 명령
- 아울러 FTC는 ▲생체인식 정보의 수집 및 활용에 관한 안내를 프라이버시 정책 및 이용약관과 별개의 문서로 작성해 소비자들에게 공지하고 ▲해당 정보의 수집에 앞서 소비자로부터 명시적인 사전 동의를 얻을 것을 동 업체에 의무화

[출처]

- JDSUPRA, "Biometric And Facial Recognition Technology In The U.S.: What's In Store For 2021?", 2021.4.5.
- The Guardian, "Judge approves \$650m settlement of privacy lawsuit against Facebook", 2021.2.27.

개인정보보호

개인정보정책단 개인정보정책기획팀

프랑스 CNIL, 쿠키 등 트래커에 대한 새 지침 발표

- ▶ 프랑스 개인정보 감독기구 CNIL*은 모바일사이트와 애플리케이션의 추적 기능에 관한 기존의 규칙이 '21년 3월로 종료되면서 쿠키 및 기타 추적 도구(tracker)에 대한 새로운 지침**을 발표('21.4.2)

* Commission nationale de l'informatique et des libertés

** Nouvelles règles pour les cookies et autres traceurs : bilan de l'accompagnement de la CNIL et actions à venir

- 새로운 규칙에 따라, 사업자는 추적 프로그램의 활용과 관련된 모든 목적을 이용자에게 명확히 안내하고 추적 프로그램을 이용자 스스로 손쉽게 거부할 수 있도록 지원해야 함
- CNIL은 이번 규칙의 핵심 내용을 요약한 자료와 더불어 웹사이트 방문 시 제3의 도메인에서 가져온 쿠키를 확인할 수 있게끔 지원하는 쿠키비즈(CookieViz) 소프트웨어 및 규칙 변경사항을 설명하는 교육용 비디오 등 실용적 조안과 도구들을 제공

[출처]

- IAPP, "CNIL publishes ad tracker guidelines", 2021.4.2.

개인정보보호

개인정보정책단 개인정보정책기획팀

이탈리아 국무원, Facebook의 불법광고 과징금 관련 상고 기각

- ▶ 이탈리아 국무원(Consiglio di Stato)*은 불법광고 혐의로 각각 5백만 유로 과징금을 부과 받은 Facebook 및 Facebook Ireland의 상고를 기각('21.3.29)

* 이탈리아 공공행정 부문의 법적 사건을 판단하는 사법-행정 협의체로서 이탈리아 내 모든 행정 당국의 행위에 대한 관할권을 보유

- 국무원은 Facebook이 상업적 목적으로 이용자 개인정보를 수집·처리하고 제3자와 공유하면서도 해당 사실을 계정 생성 시점에 이용자에게 충분히 안내하지 않았고 제3자와의 개인정보 공유에 대해 유효한 사전 동의를 확보하지도 못했다고 지적
- 또한 Facebook처럼 개인정보의 상업적 처리를 기반으로 수익을 내는 업체가 스스로를 '무료 서비스'로 지칭하는 행위는 이용자를 오도할 여지가 있음

[출처]

- DataGuidance, "Italy: Council of State issues judgment on Facebook deceptive commercial practices rejecting Facebook's appeal", 2021.3.31.

개인정보보호

개인정보정책단 개인정보정책기획팀

유럽 인터넷광고협회, '정당한 이익(legitimate interests)' 관련 지침 발행

- ▶ 유럽 인터넷광고협회(IAB Europe)*가 GDPR 개인정보 처리의 법적 근거 중 하나인 '정당한 이익(legitimate interests)'에 관한 지침 발행('21.3.25)

* Interactive Advertising Bureau Europe

- IAB Europe은 영국인터넷광고협회(IAB UK)와 공동으로 GDPR의 개인정보영향평가(DPIA)를 보완할 수 있는 디지털 광고 분야의 정당한 이익 평가(LIA: legitimate interests assessments)에 관한 실용 지침을 개발
- 동 지침은 EU에서 디지털 광고에 종사하는 회사를 대상으로 LIA를 수행하는 표준화된 접근 방식을 제공하고, 개인정보 처리의 특수성과 업계의 관련 위험을 다룸
- 지침은 ▲GDPR 하에서 LIA 정의와 목적, ▲LIA를 수행해야하는 경우, ▲LIA 진행방법, 법에 규정된 절차 및 관련자, ▲일반적 디지털 광고 데이터 유형 및 처리 활동에서 균형 있는 테스트를 위한 방법 등을 포함

[출처]

- DataGuidance, "EU: IAB Europe issues guidance on GDPR legitimate interests assessments", 2021.3.31.

개인정보보호

개인정보정책단 개인정보정책기획팀

AI 이루다 개인정보 유출 피해자, 개발사 상대로 손해배상 청구 소송 제기

- ▶ 인공지능(AI) 챗봇 '이루다'의 개발 과정에 개인정보를 유출 당했다고 주장하는 이용자들이 개발사 '스캐터랩'을 상대로 2억원대 손해배상 청구 소송을 제기
- 법무법인 태림은 이루다 관련 피해자 254명을 대리해 서울동부지법에 손해배상 청구 소송을 제기
 - 총 소송 가액은 약 2억원으로 피해자 1인당 배상액을 80만원으로 산정
 - 이용자들은 스캐터랩이 카카오톡 대화를 AI 챗봇 학습에 쓴다고 구체적으로 고지·설명하지 않았고, 회사 안팎에 개인정보·민감정보를 유출한 정황도 있다고 주장
 - 법무법인 태림은 스캐터랩이 이용자 동의 없이 개인정보를 무단 이용하고 개인정보 보관 이유·목적 등을 고지하지 않은 점, 대화 내용에 포함된 민감정보·고유식별정보를 동의 없이 보관한 점 등을 고려했을 때 개인정보보호법을 위반했다고 주장

[출처]

- 조선비즈, "개인정보 유출 논란 '이루다' 개발사, 2억 원대 손배소 당해", 2021.4.1.

사이버침해

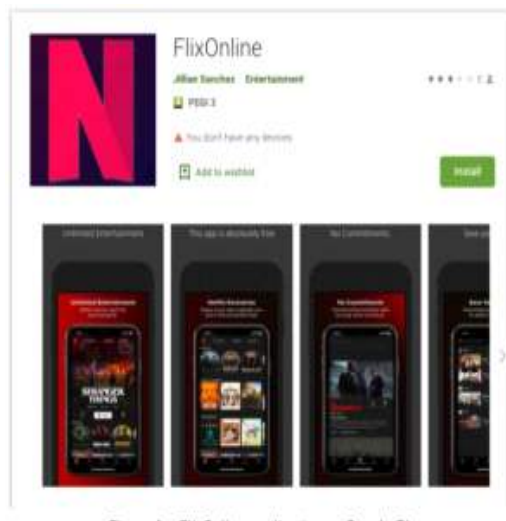
사이버보안빅데이터센터 AI빅데이터보안팀

Google Play의 가짜 Netflix 앱이 WhatsApp을 통해 악성코드 전파

▶ 주요 내용

- 구글 플레이 스토어에 숨어있는 넷플릭스 앱으로 위장한 악성 코드가 WhatsApp 메시지를 통해 퍼져 나가고 있다는 사실을 연구원들이 발견함(체크포인트 분석 보고서)
- 악성 코드는 "FlixOnline"이라는 앱으로 위장하여 WhatsApp 메시지를 통해 "넷플릭스 2개월 무료 이용"으로 홍보하며 설치를 유도하며 설치 후에는 데이터와 자격증명을 도난
- 공식 안드로이드 앱 스토어에서 지속적으로 데이터를 훔치거나 악성코드 드롭퍼가 내장된 앱들이 퍼지고 있으므로 주의해야 함

< 넷플릭스 위장 가짜 앱 예시 >



▶ 악성코드의 동작

- FlixOnline은 설치 후 오버레이, 배터리 최적화 무시 및 알림 리스너 등의 특정 권한을 요청
- 오버레이를 통해 다른 애플리케이션 위에 새 창을 만들어서 다른 앱에 대한 가짜 로그인 화면을 생성
- 배터리 최적화 무시를 통해 악성코드의 실행 종료를 방지하며 백그라운드에서 가짜 메시지를 보냄
- 권한 부여 후 명령 및 제어서버(C&C)에 연결하여 주기적으로 구성 요소를 업데이트함
- On Notification Posted 등의 함수를 사용하여 이용자의 수신 메시지를 구문 분석하고 조작함

시사점

- 이용자는 메시징 앱을 통해 받은 다운로드 링크 또는 첨부 파일에 대해 주의해야 하며 설치된 가짜 앱을 발견하면 즉시 제거 및 모든 비밀번호 변경을 진행해야 함

[출처]

- Threatpost, "Fake Netflix App on Google Play Spreads Malware Via WhatsApp", 2021.4.7.
- Techworm, "Fake Netflix App on Google Play Spreads Malware Via WhatsApp", 2021.4.8.

GitHub 서버에서 암호화폐 채굴을 위해 악용되는 GitHub Actions

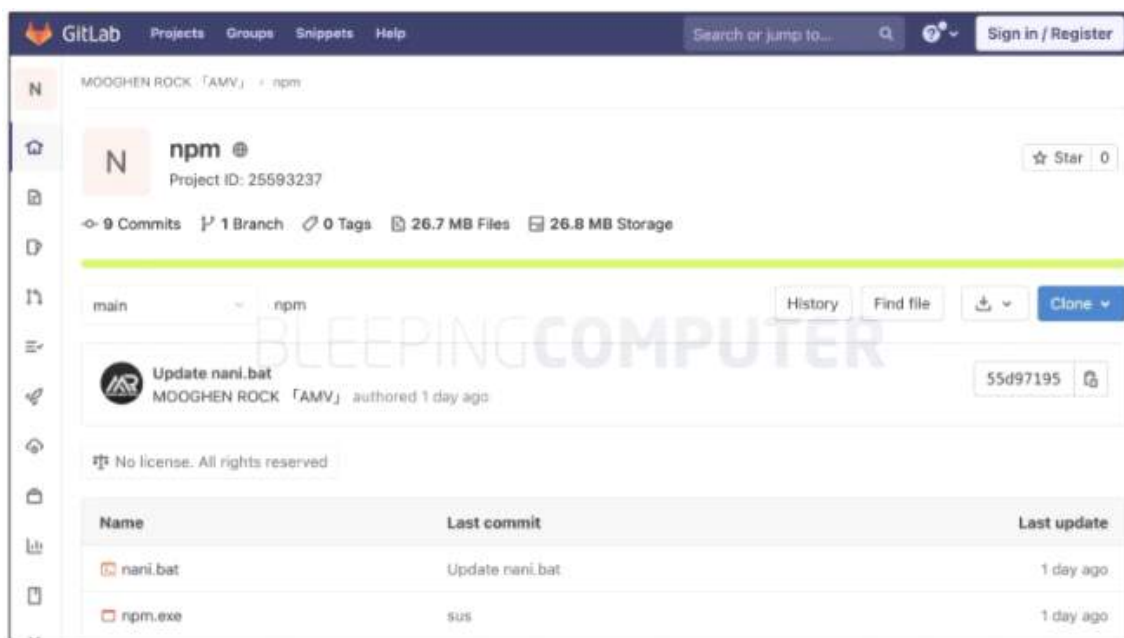
GitHub Actions이 자동화된 공격으로 GitHub 서버에서 암호화폐를 채굴하도록 악용

- ▶ 공격자는 암호화폐 채굴을 위해 GitHub Actions를 사용하는 GitHub repository를 악용했으며 최소 95개의 repository가 공격자에 의해 타겟팅 되었음

주요 내용

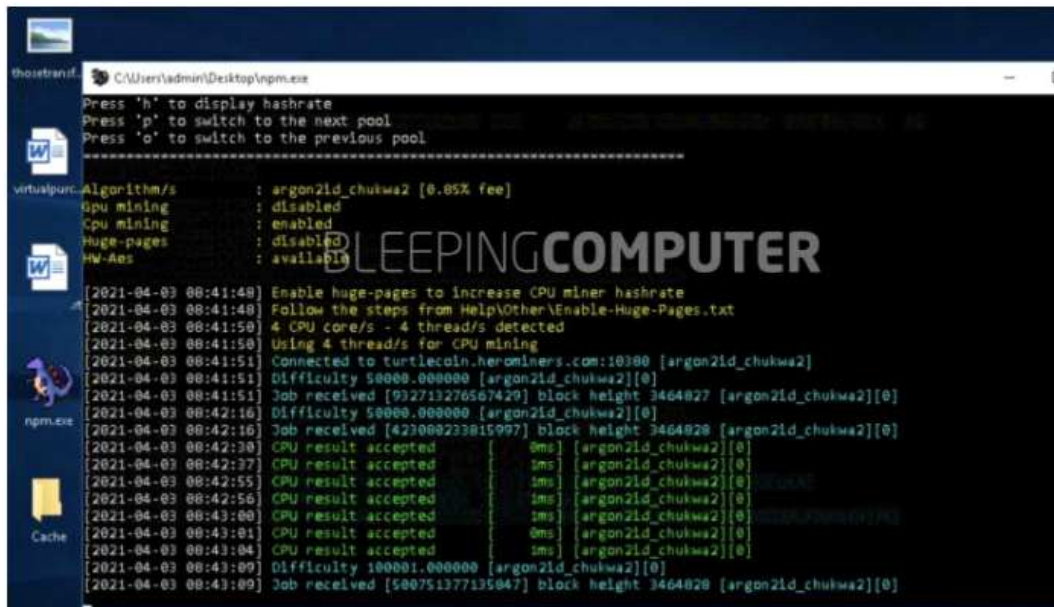
- ▶ 공격자는 GitHub Actions를 악용하여 악성코드를 전파하고 GitHub서버에서 암호화폐를 채굴함
※ GitHub Actions : Github repository를 기반으로 소프트웨어 개발 workflow 자동화를 위한 작업을 쉽게 설정할 수 있는 CI/CD 솔루션
- ▶ 공격자는 정상 repository를 fork하여 악성 코드를 삽입하고 정상 repository 코드와 다시 병합하도록 Pull Request를 보냄
- 악성 Pull Request에 의해 호출된 자동화된 코드는 GitLab으로부터 npm.exe라는 변조된 이름의 암호화폐 채굴 프로그램을 GitHub 서버에 로드
- 암호화폐 채굴 프로그램(npm.exe)이 로드되면 공격자는 자신의 지갑 주소를 인수로 전달하여 채굴을 시작

< GitLab에서 호스팅된 암호화폐 채굴 악성코드 "nnpm.exe" >



- ▶ 해당 공격에서 정상 프로젝트 관리자의 승인 없이 Pull Request를 제출하는 것만으로도 공격을 유발할 수 있음
- Pull Request의 유효성을 검사하기 위해 자동화된 workflow 설정이 있는 GitHub 프로젝트의 경우 기존 프로젝트 관리자의 승인 없이 악의적인 Pull Request를 실행하여 공격자의 코드를 실행

< 암호화폐 채굴 활동을 수행하는 npm.exe 악성코드 >



- ▶ GitHub Actions를 사용하는 프로젝트를 대상으로 하는 의심스러운 Pull Request가 접수되고 있는 현재 더 많은 모방 공격을 발견
- 모방 공격 중 하나는 XMRig의 공식 GitHub repository에서 오픈 소스 XMRig 암호화폐 채굴 프로그램을 가져옴

시사점

- ▶ 자동화된 workflow를 통해서 Pull Request의 유효성을 테스트하는 Github 프로젝트 소유자들이 주요 공격 대상이므로 필요한 경우에만 자동화 workflow를 사용할 수 있게 설정하도록 권고
- ▶ 암호화폐 채굴의 경우 피해가 쉽게 드러나지 않기 때문에 탐지가 더욱 어려우며, 시스템의 자원을 활용하여 속도 등 측면에서 악영향을 미칠 수 있고 추가적인 위험에도 노출 될 수 있으므로 주기적인 모니터링 필요

[출처]

- Bleepingcomputer, "GitHub Actions being actively abused to mine crypto-currency on GitHub servers", 2021.4.3.
- Securityaffairs, "The popular code repository hosting service GitHub is investigating a crypto-mining campaign abusing its infrastructure.", 2021.4.3.

유럽이사회, 신규 EU사이버보안 전략 채택

▶ 개요

- 유럽이사회*가 '20년 12월에 발표된 '디지털 10년을 위한 유럽연합의 사이버보안 전략(이하 '신규 EU사이버보안 전략')**을 최종적으로 채택('21.3.22)

* European Council: 유럽연합(EU) 회원국 정부 정상들의 모임으로써 EU의 최고의사결정기구

** The EU's Cybersecurity Strategy for the Digital Decade: EU집행위와 외교안보정책고위대표(HR/VP)가 '20년 12월 16일에 발표한 사이버보안 전략

▶ 주요 내용

- '신규 EU사이버보안 전략'은 향후 7년('21~'27년)동안 3가지 목표를 달성하기 위하여 3가지 도구(규제, 투자, 정책 기구)를 활용할 예정
 - 3가지 목표는 다음과 같음 ▲사이버보안 회복력·기술 주권·리더십 강화 ▲주요 사이버위협 대응 역량 강화 ▲사이버공간 보안 및 안전성을 보장하기 위해 전 세계 파트너국과 협력

< 디지털 10년을 위한 유럽연합의 사이버보안 전략 >

구분	주요 내용
사이버보안 회복력, 기술주권·리더십 강화	• 네트워크정보시스템 보안지침(NIS Directive) 개정 - EU집행위는 주요분야(에너지, 교통, 건강, 선거 등)별 구체적인 사이버보안, 네트워크 규칙(network code)을 마련할 계획 • 유럽사이버방패(European Cyber Shield) - EU 전역에 보안운영센터(Security Operations Centre)를 설립하여 네트워크를 구성 - 보안운영센터는 인공지능 기술(머신러닝)을 활용하여 사이버공격 징후를 감지, 선제적인 조치를 통해 피해를 최소화하는 역할을 수행 • 안전이 보장된 통신 인프라 구축 - 강력한 암호화기술로 기밀 정보를 안전하게 전송하는 차세대 양자통신기반시설(QCI) 개발을 위해 회원국이 공동협력 - EU 우주 프로그램과 협력하여 EU와 회원국이 보안과 안정성이 보장된 우주 기반 통신을 제공 • 5G 및 차세대 광대역 모바일 네트워크의 안전 확보 • 안전한 사물인터넷(Internet of Secure Things, IoST) • 글로벌 인터넷 보안 강화 - EU 시민, 기업, 행정부가 안전하게 접속할 수 있는 EU DNS 리졸버 서비스*를 개발 * DNS resolver service: 사용자가 입력한 아이디와 비밀번호를 훔쳐가는 'DNS 가로채기'를 비롯한 취약점 공격으로부터 사용자를 보호할 수 있는 서비스 • 기술 공급망 강화 - 사이버보안 역량강화 및 국가협력센터(Cybersecurity Competence Centre and Network of National Coordination Centre) 설립을 통해 EU 사이버보안 기술 주권 개발 및 5G와 같은 민감한 기반시설의 안전을 확보할 수 있는 역량을 강화 - EU 차원의 연구개발 프로그램을 통해 '21-'27년 기간 동안 최대 45억 유로 규모의 공공·민간 투자가 진행될 예정

구분	주요 내용
	- EU 사이버 전문인력 확보 - 최고의 사이버보안 인재를 교육, 업스킬, 유치 - 세계적인 수준의 사이버보안 연구 및 혁신 투자를 진행 - 개정된 디지털 교육 실행 계획(Revised Digital Education Action Plan)을 통해 개인, 청소년, 조직, 중소기업에 사이버보안 인식 제고 - 소외계층 및 여성의 STEM 교육, 리스킬링·업스킬링을 통한 ICT 업계의 참여를 장려
주요 사이버위협을 방지·억제·대응할 수 있는 운영 역량 강화	- 통합사이버 부서(Joint Cyber Unit) 설립 - 유럽 사이버보안 위기관리 프레임워크를 작성 - 통합사이버 부서 설립을 위한 프로세스, 이정표, 일정 등을 결정 - 보안연합전략*에 포함된 사이버 범죄 의제를 지속적으로 최신화 * Security Union Strategy 2020-2025: EU집행위에서 '20년 7월에 공개한 전략으로, 유럽의 물질적 공간·디지털 공간의 안전을 보장하기 위한 행동계획, 도구, 조치 등으로 구성되어있으며, 주로 조직범죄·테러·주요기반시설 및 공공장소 안전·사이버범죄·법집행 기관 간 협력 및 정보 공유 등에 대한 내용을 수록 - 사이버 정보수집 실무그룹 설립 장려 및 촉진 - 유럽 대외정보기관인 INTCEN 산하 '사이버정보 워킹그룹'을 설치하여 사이버 공격에 신속 대응 - EU 사이버 억제 태세 개선 - 사이버공격 발생시 기존에 활용중인 EU 사이버외교툴박스(cyber diplomacy toolbox)를 EU 위기대응 메커니즘과 통합하여 악의적인 사이버 활동을 효과적으로 방지, 억제 및 대응 - 사이버방어 정책프레임워크(Cyber Defence Policy Framework) 검토 - EU 공동안보방위정책(CSDP)* 차원, '작전영역으로서의 사이버 공간에 대한 군사적 비전 및 전략' 개발을 추진 * Common Security and Defence Policy: 안보방위 문제를 유럽연합 차원에서 공동대응을 모색하는 정책으로 국제적 위협 대처, 위기 및 분쟁지역의 안보·재건지원 등을 수행 - 우주 기반시설 사이버보안 강화 - EU 차원의 우주 프로그램을 통하여 민간·국방·우주산업 간의 시너지 효과를 지원하고 우주기반 통신장비의 사이버보안 강화
사이버공간의 보안 및 안전성을 보장하기 위해 전 세계 파트너국과 협력	- 디지털 기술에 대한 국제 표준화 과정에 적극적으로 참여 - 차세대 주요 기술(인공지능, 클라우드, 양자 컴퓨팅, 양자통신 등) 표준화에 EU 차원으로 적극적으로 참여하여 사이버보안 체계를 확립 - 유엔 사이버공간 국제안보 및 안정성 향상 프로그램 참여 및 기여 - 사이버공간에서의 인권, 기본적 자유를 적용하는 방안을 담은 실용적인 지침을 제공 - 부다페스트 협약(Budapest Convention)*의 강화 및 홍보 * 인터넷 상에서 벌어지는 사이버범죄(DoS 공격, 해킹, 피싱, 아동포르노물, 저작권 침해물 유통 등) 수사의 국제공조를 위하여 '01년 유럽평의회를 통해 채택된 협약으로, 전 세계62개국이 가입 - 부다페스트 협약의 추가적인 프로토콜 개발을 위해 협력 - 사이버보안 관련하여 민간·학계·시민사회와의 정기적이고 체계적인 교류 진행 - EU 외부 사이버역량강화 어젠다(EU external cyber capacity buliding agenda) 제안 - EU 사이버 역량 강화 위원회 설치 및 EU사이버넷(EU CyberNet) 구현 등을 통해 전 세계적으로 사이버 복원력 및 보안 역량 강화

[출처]

- Consilium, "Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy", 2021.3.22.

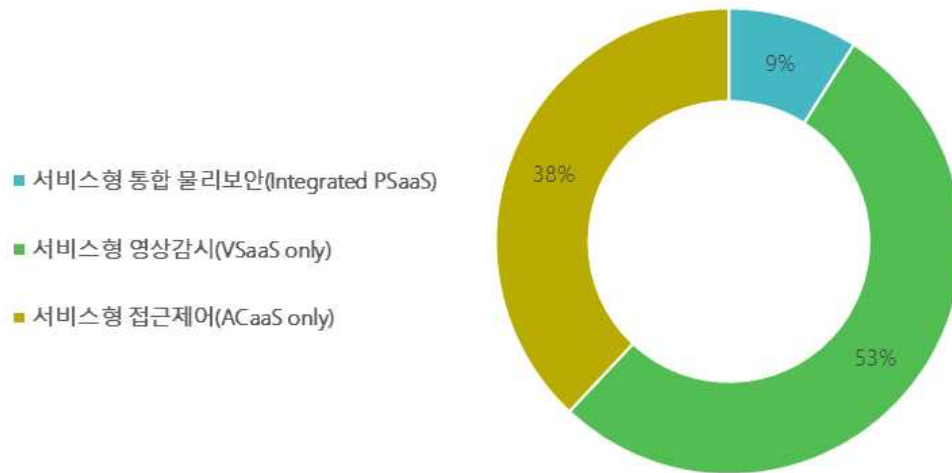
옴디아, 서비스형 통합 물리보안 시장 전망

- 시장조사기관 옴디아(Omdia)가 출입통제와 영상감시 기능을 결합한 서비스형 통합 물리보안(Integrated Physical Security as a Service, PSaaS) 시장 현황과 전망을 개괄('21.3.15)

최근 물리보안 시장에서 빅데이터 분석과 같은 새로운 기능과 유연한 확장성을 제공하는 클라우드 기반의 서비스형 영상감시 및 출입통제 솔루션의 도입이 증가 추세

- ▶ **(개념)** 서비스형 통합 물리보안 시스템은 상호연결형 데이터베이스를 통해 출입통제와 영상감시 기능을 동시 관리하는 서버에 대해 고객이 주간·월간·분기 단위로 비용을 지불하는 종합 보안 솔루션을 의미
- ▶ **(주요 이점)** 출입통제와 영상감시를 결합한 서비스형 통합 물리보안 시스템을 통해 최종 사용자, 보안 담당자, 시스템 통합업체 등은 다양한 이점을 누릴 수 있음
 - 최종 사용자는 서비스형 출입통제 솔루션과 영상감시 솔루션에 각각 투자하는 대신 통합 시스템을 선택함으로써 투자비용을 절감할 수 있으며, 특히 중소 규모 시설에서 최대 비용 절감이 가능
 - 보안 담당자는 단일 소프트웨어를 통해 출입통제와 영상감시 시스템을 관리할 수 있으며, 출입통제와 영상감시 데이터를 결합해 다양한 빅데이터 분석을 실시하는 한편, 시스템 시험과 유지관리 추적 등 자동화 보안 절차의 간소화가 가능해질 것
 - 시설주는 서비스형 통합 물리보안 시스템을 활용한 빅데이터 분석을 통해 건물의 점유 수준을 보다 정확하게 평가하고 접근 시도나 보안 침해 등을 실시간으로 확인 가능
 - 출입통제와 영상감시 시스템의 유지관리를 담당하는 시스템 통합업체는 각 영역의 유지관리 루틴과 보고 절차를 간소화 할 수 있음
- ▶ **(시장 규모와 전망)** '20년 전세계 서비스형 물리보안 시장은 약 15억 달러 규모이며, 이중 서비스형 통합 물리보안 시장 비중은 9% 이하로, '24년에는 13%로 증가 예상
 - 통합 물리보안 시스템의 다양한 장점에도 불구하고 대부분 제품은 개별 출입통제 및 영상감시 솔루션 간 공통 사용자 인터페이스와 데이터 전송 등의 제한적인 결합만을 지원
 - 서비스형 통합 물리보안 시스템은 향후 5년간 CAGR 24.6%의 성장이 예상되나, 기존 서비스형 출입통제 및 영상감시 솔루션 시장 수요를 대체하지는 않을 것

< '20년 전 세계 서비스형 물리보안 시스템 유형별 시장 점유율 >



- 지역별로는 미주 지역의 서비스형 통합 물리보안 시장 매출이 7,440만 달러 규모로 가장 높지만, 성장세는 아시아 지역이 가장 높게 나타남

< 주요 지역별 서비스형 통합 물리보안 시장 현황 >

지역	매출규모('20년)	서비스형 물리보안 시장 내 비중	CAGR('19~'24)
유럽·중동·아프리카(EMEA)	1,790만 달러	9.1%	19.0%
미주	7,440만 달러	11.0%	23.4%
아시아	3,660만 달러	6.5%	29.7%

- ▶ **(시장 저해요인)** 출입통제와 영상감시 판매모델 결합의 어려움, 최종 사용자의 인식 부족, 지역 간 수요의 불균형 등이 시장 발전을 저해

- 개별 출입통제 및 영상감시 솔루션은 통상 건물에 설치되는 도어나 보안 카메라의 개수에 따라 월별 사용료를 계산하며, 두 솔루션을 결합해 표준화된 사용료를 책정하는 방식은 유연성의 부족 또는 지나치게 복잡함을 이유로 최종 사용자에게 외면 받는 경향
- 다수의 최종 사용자들은 서비스형 물리보안 솔루션의 분석 기능을 제대로 활용하지 않고 인공지능 기반의 자동화 절차 대신 기존 보안 절차를 고수하여 통합 시스템의 장점을 인식하지 못함
- '20년 출입통제 시장 수요의 70% 이상이 북미에서 나온 반면, 영상 감시 시장에서는 중국을 중심으로 아시아 지역이 3분의 2가량을 차지해 지역 간 수요의 불균형도 통합 시스템의 발전을 저해

- ▶ **(시장 기회)** 보안업계 외부의 이해관계자 포섭과 빅데이터 분석 기능의 장점 홍보, 혁신적인 판매 모델 등을 통해 서비스형 통합 물리보안 시장의 기회를 모색 가능

- 최근 보안 운영 업무에 인사팀, IT 전문가, 자산관리팀 등 외부 이해관계자의 참여가 늘어나고 있으며 이들은 기존 보안 관계자 대비 빅데이터 분석 등의 새로운 기능에 호의적인 경향
- 벤더들은 리셀러와 최종 사용자에게 운영비용 절감, 침해사고 조사 및 보안 절차 간소화 등과 같은 빅데이터 분석의 장점을 홍보 필요
- 또한 다양한 수직시장(vertical market)의 최종 사용자에게 탄력적이고 개별화된 접근방식을 제공할 수 있도록 판매 모델의 혁신을 지속해야 함

[출처]

- Omdia, "Integrated Physical Security as a Service platforms offer "great opportunities for innovative vendors", 2021.3.15.



| 발 행 | 한국인터넷진흥원
| 기획 및 편집 | 한국인터넷진흥원 미래정책연구실 미래정책팀
| 발 행 처 | 전라남도 나주시 진흥길 9