# 2022. 11. 09

**# 아이디어 1**

모든 사이트 이용자의 정보를 저장하는 데이터베이스 및 저장소를 마련하여, 개인정보 불법 유통 등의 문제 발생 시 데이터베이스 서버가 임의로 그 정보의 모든 효력을 상실시킬 수 있게 함으로써 정보 유출로 인한 2차,3차 피해 최소화

**아이디어 제안 목적**

유출된 개인정보에 보다 원활한 접근을 가능하게 하여 사후 처리를 원활하게 진행할 수 있게 하고, 추가적으로 정보 유출로 인한 2,3차 피해 최소화하기 위함이다.

**개인정보 불법 유통 여부 인식 방법**

사용자의 각 정보(계정 등)가 일정 기간마다 서버에게 정상적으로 정보가 보호되고 있다는 증거 제출(신호 전송).

특정 기간동안 신호가 오지 않으면 정보가 유출되었다고 판단, 그 후 정보를 원격 파기

**# 아이디어 2**

사진이나 불법 영상이 올라오면 그 영상 속의 사람들을 대상으로 안면 인식 후 사진, 영상 속 주인에게 영상 삭제 여부 전송. 그 후 사진 속 인물의 선택에 따라 영상이나 사진을 삭제 및 파기

**아이디어 제안 목적**

사회적으로 큰 문제가 되는 몰레카메라 및 불법촬영물과 관련하여 2,3차 피해 예방을 위함이다.

**사진이나 불법 영상의 범위 및 탐색 방법**

사람이 아닌 컴퓨터 등의 기계는 영상물의 채도, 명도에 따라 명확한 불법 촬영 여부를 식별하기 어려울 것으로 예측. 따라서 별도로 불법 촬영 영상 및 사진 등을 추려내는 알고리즘을 적용하지 않고, 모든 업로드된 영상물에 대해 안면 인식 등의 기술을 사용할 계획임

---

개인정보 위험대응 공모전 자료조사&아이디어

- 딥웹은 검색에 걸리지 않는 사이트. 이중 네트워크가 암호화되고 특수경로로만 접근 가능한 웹사이트가 다크웹

1. 안랩은 자사 위협 인텔리전스 플랫폼 ‘AnLab TIP’를 통해 딥웹과 다크웹의 최신 동향 정보 제공, DDW 스크랩퍼를 통해 다크웹 상의 데이터를 자체 수집,처리,분석해 연계 정보를 제공

=> 안랩에서 제공되는 정보를 통해 현존하는 다크웹 사이트들에서 주기적으로 사용자의 정보를 조회해보고 유출 여부(됐는지 안됐는지)를 알려주는 서비스 제공하는 앱을 개발

다음(밑의 url)과 같은 서비스가 존재하지만, 수동으로 입력해야 하고 하루에 5개밖에 입력하지 못함.

즉, 자신의 아이디를 모두 입력하여 주기적으로 유출 여부를 검사하고, 사용자에게 알려주는 앱을 개발하면? (하지만 보안상 문제가 걱정됨)

1. KB국민은행의 ‘히든채널 모니터링 체계 구축’. 즉, 은행에서 딥웹이나 다크웹에서 자사 중요정보가 유출됐는지를 모니터링함.

=> 여러 분야에서 다크웹을 지속적으로 모니터링 하는 것으로 보아 다크웹 모니터링 관련 아이디어는 제외시키거나 기술적으로 더 자세하고 깊이 파고들어서 하는 것이 좋을 것으로 보임

1. S2W가 사이버 위협을 분석하는 인텔리전스(CTI) 플랫폼 '퀘이사'를 출시. 퀘이사는 다크웹 및 딥웹 등에서 수집한 정보를 분석, 공격 패턴 등 핵심 정보를 제공하는 플랫폼임. 다크웹과 딥웹에서부터 시작되는 공격을 비롯해 랜섬웨어나 피싱, APT 공격 등 까다로운 신종 사이버 위협에 대응하기 위한 효과적이고 즉각적인 예방책으로 쓰일 수 있음
2. 다크웹의 주요 사고 사례는 DB 권한 유출, DB의 정보 유출, DB 무단 접속임.

↑다크웹 사고를 막기 위한 보안 점검 및 강화 방안

4-1. DB 서버 보안

: DB의 취약점은 모의 해킹과 내부 보안 감사를 통해 검출이 가능함.

데이터베이스의 보안 솔루션은 암호화 솔루션 및 접근제어 솔루션으로 나뉨. 암호화는 유출 시 해독이 불가하여 뛰어난 보안성을 제공하며 법규를 충족함. 접근 제어는 DB 전체에 대해 접근제어 및 감사를 제공하지만 암호화 기능이 없어 단독 적용 시 법규 충족이 되지 않음.

=> 정보의 유출을 막기 위해서는 그 정보가 저장되어 있는 ‘데이터베이스’의 보안이 가장 중요하다고 생각함. 데이터베이스의 보안을 위해서는 데이터베이스가 있는 서버의 보안이 필요함. DB 서버 보안 관련해 간단히 공부해보고 DB 서버의 취약점에 대한 간단한 기술적 아이디어를 낸다면 정보 유출 자체를 막는 아이디어가 나올 것이라고 생각함.

1. 다크웹 사이버범죄의 수사방법

- 네트워크 패킷 감청

: 네트워크 패킷 감청은 다크웹 사이버범죄의 수사방법의 핵심으로, 범죄가 의심되는 사용자의 Tor 네트워크 상의 패킷을 수집하고 분석 후 범죄혐의를 입증 할 수 있는 디지털 증거를

찾아내어 추적한다. Wireshark 등의 도구를 활용하여 tcpdump/windump를 사용한다.

- 온라인 수색

: 수사기관이 범죄 혐의자가 알지 못하게 그 범죄 혐의자 가 이용하였거나 이용하고 있는 컴퓨터 등에서 사건과 관련된 정보를 전 자적인 방식으로 수색하여 범죄의 혐의를 밝히는 수사 방법. 온라인 수색은 대개 일시적으로 타인의 컴퓨터 시스템에 저장된 데이터에 비밀리에 일시적으 로 접근함. 실제 다크웹 상의 웹 서버가 아닌 미리 설정해놓은 수사기관의 웹서버로의 접속을 유도하여 온라인 수색 프로그램인 스파이웨어 프로그램이 대상자가 인지 하지 못한 상태에서 설치되도록 유도하는 것

=> 네트워크 패킷/온라인 수색 관련하여 아이디어 내는 것도 괜찮을 것 같음. 특히 네트워크 패킷 부분은 네트워크 수업에서 배운 내용들이 많아서 아이디어를 낸다면 기술적으로 접근이 가능하지 않을까 생각함.

---

- 다크웹에서의 개인정보 보호라 하면 피해자들의 것이라고 생각되므로 이에 중점을 두고 생각해보면, 보호할 개인정보는 크게 두 가지로 나뉨
  - 다크웹 상의 개인정보
  - 다크웹에서 표면웹으로 유출된 개인정보

- 개인정보 보호를 위한 방안을 생각 해 보면
  - 유출된 개인정보를 빠르게 삭제
  - 유출된 개인정보를 당사자에게 통지
- 포상금 제도
  - 다크웹 내 사용자들을 대상으로 포상금 지급을 유인책으로 개인정보를 판매하는 인물을 제보
  - 단점: 현실적으로 너무 많은 비용이 듦
  - 제보자도 다크웹 상에 접속했음으로 의미하므로 처벌이 두려워 임하지 않을 수 있지만 이에 대해서는 대안을 주어 정보 제공에 어려움이 없도록 하는 방법 도입

> 흔적이 남지 않는 다크웹
> 한 번 올라간 정보는 사실상 삭제가 불가능함(서버를 압수수색해 폐쇄하지 않는 한)
> 국가정보 유출도 심각한 상황

---

기술적인 방법으로는 솔직히 모르겠음 이게 가능한건가 싶음

아니면 생각한게 기술로 안된다면 인적 자원을 이용해보고자 함

(해킹 기법에서 사회공학적 방법이 있듯이)

경찰에 보안전문가로 구성된 다크웹 전담팀을 만들어 다크웹에 숨겨놓는 방법이 가장 최선인 것 같다(잠복수사)

- 이때의 문제? 익명성 때문에 상대를 알 지 못함 → 어떻게 하지 수사관한테 특별한 기술을 주어 해독? 개인의 고유 키 값이라도 추적?
- 현재의 인력으로는 부족하다고 들음→앞으로 인재 양성 필요
- 기술이 필요하다 하면: 수사관이 다크웹 내에서 모니터링→개인정보 유출 정황 및 거래 발견 시 잠입하여 해당 거래자의 인터넷 정보 수집해 검거 후 처벌 및 네트워크 끊기??

## 크리덴셜 스터핑: 무차별 대입 공격

- 공격자들의 개인정보 대입 수법

## 다크웹 수사 관련 법령 및 제한

- 사이버범죄 수사에 효율적인 방법인 온라인수색과 **역외 압수수색, 감청 등의 수단은 현재 우리나라에서는 개인정보보호법 및 통신비밀보호법 등에서 허용하지 않거나** 엄격히 제한되고 있다.
  - 현재 다크웹 정보는 정보통신망에서 유통되는 정보라는 점에서 **‘정보통신망이용촉진 및 정보보호 등에 관한 법률’ 제44조의7 제2항과 제3항에 근거하여 방송통신심의위원회의 심의**를 거쳐 다크웹에 유통되는 불법 정보의 **삭제및접속차단을 명령**할 수 있다.
  - 그러나 방송통신위원회의 경우 주로 표면웹에 대한 불법정보 차단에 집중하고 있으며, **다크웹에 유통되는 불법정보에대해서는 다크웹의 정보가 표면웹에 노출되는 경우에만 해당 정보를 표면웹에서 차단하고 있다.**

## 다크웹 수사의 현실

- 다크웹 범죄 수사를 위해선 수사 인력의 전문성 외에도 대용량 파일및추적경로 분석을 위한 고성능 장비와 수사시스템의 지원이 필수적임.
  - 그러나 경찰청의 경우 사이버안전국 사이버수사과 내 1개 수사팀(6명 이내)에서만 다크웹 수사를 전담하고 있고, 대용량 파일을 분석하기 위한 기본 장비만 있는 실정이다.

- 수사지원을 위한 시스템도 개발하고는 있으나, 예산 및 기술의 한계로충분한 기능을 갖추기에는 많은 시간이 소요될 것으로 보임

## 개인 식별 단서 PGP

- 다크웹 게시물을 보면 거래내용과 장소, 비트코인 지갑주소 노출을 피하기 위해 암호화하고 복호화하는 프로그램인 PGP(Pretty GoodPrivacy)를 이용하는 경우가 대부분이다.
  - 이 경우 한 사람이 여러 다크웹사이트에서 여러 아이디(ID)를 사용하여 게시하는 경우 동일한 PGP 키를사용하는 아이디들이 동일한 사람에게 속하는 것을 보여주는 결정적인 증거가될 수 있음
- 향후 다크웹 수사 시 PGP 공개키를 기반으로 상호 연관성을 분석한다면 범죄자가 신분을 은닉하며저지른 범행 간의 관계를 밝혀낼 수 있을 것이라고 이 논문은 말함.

---

모니터링, 탐지체계 마련, 유·노출된 개인정보에 대한 안전조치 방안
다크웹의 최신 동향을 면밀하게 살피고, 기업 정보가 다크웹에서 거래되는지 여부를 모니터링하는 방법
다크웹 모니터링 사업

> 사이트 가입할 때 아이디와 비번에 꼬리표를 달아 다른 사이트에 같은 아이디로 로그인 시도가 일어나면 알리는 방법?
> 내 아이디 비번을 등록해두면 주기적으로 유출 여부와 어디 사이트에서 유출되었는지를 자동으로 검사해주는 서비스?
> 개인정보를 등록해두면 유명 포럼에서 내 정보가 돌아다니는지 모니터링하는…