한국컴퓨터정보학회 하계학술대회 논문집 제31권 제2호 (2023. 7)

다크웹 상의 범죄 사례 및 포렌식 기법 동향

박소희[O], 도은정[*], 이훈재[**]
[O]동서대학교 정보보안학과,
[*]동서대학교 일반대학원 디지털포렌식학과,
[**]동서대학교 정보보안학과
e-mail: sohui7793@naver.com[O], thedo_1230[*], hjlee@dongseo.ac.kr[**]

Criminal Cases and Trends in Forensic Techniques on the Dark Web

So-Hee Park[O], Eun-Jeong Do[*], Hoon-Jae Lee[**]
[O]Dept. of Information Security, Dongseo University,
[*]Dept. of Digital Forensic, Dongseo University,
[**]Dept. of Information Security, Dongseo University

● 요 약 ●

오늘날 전 세계적으로 연결되어 있는 인터넷을 통해 사용자들은 아무런 제약 없이 의사소통 및 거래 등 다양한 활동을 할 수 있게 되었다. 그러나 이러한 인터넷상의 자유를 범죄의 수단으로 한 인터넷상의 사이버 범죄가 급속하게 증가하고 있다. 특히 인터넷 중 하나로 분류되는 다크웹에서는 심각한 중대 범죄들이 많이 발생하고 있는데, 다크웹은 일반 네트워크와 달리 암호화 기술을 사용하는 특정 네트워크를 통해서만 접속이 가능하기 때문에 사용자에게 익명성과 비밀성을 제공할 수 웹 사이트이다. 이러한 다크웹의 특성으로 인해 마약 거래, 아동 포르노 유포, 개인정보 유출 등 다양한 사이버 범죄가 발생하고 있다. 본 논문에서는 이러한 다크웹 상에서 발생하는 주요 범죄 사례를 알아보고 이에 대한 포렌식 수사 기법의 동향을 살펴보고자 한다.

키워드: 다크웹(Dark Web) 사이버 보안(Cyber Security), 디지털 포렌식(Digital Forensic)

I. Introduction

다크웹이란 인터넷의 한 부분으로서 일반적인 웹브라우저로 접근이 불가능한 비공개 네트워크를 말한다. 다크웹은 토르(Tor)나 프리넷(Freenet)과 같은 익명화 네트워크를 통해서만 접속할 수 있다. 일반적인 인터넷의 사용자들은 IP 주소나 개인정보를 통해 식별되어질 수 있지만, 토르 네트워크와 같은 특정 암호화 네트워크는 사용자의 인터넷 트래픽을 여러 개의 노드로 암호화하여 전송되도록 하여 사용자의 실제 IP 주소를 추적하는데 어려움이 있다. 따라서 다크웹은 사용자의 신원과 정보를 보호해주기 때문에 추적하기가 쉽지 않은 상황이다. 이와 같은 다크웹의 특성을 악용하는 중대 범죄 발생률이 급격하게 증가하고 있다.

KDB 미래전략연구소 산업기술리서치센터의 한 보고서에 따르면, 다크웹의 사이트 중 51%가 범죄 관련 사이트로 분석되었고, 마약 거래 등 불법 상품 거래와 성 착취물 유통, 그리고 개인정보 탈취와 같은 사이버 범죄가 그것의 대표적인 사례로 나타났다[1].

익명의 사용자들의 정보 교환 및 소통을 위해 사용되기 시작한 다크 웹이 결국 사이버 범죄의 배경과 수단으로서 전락되고 있는 상황이다.

본 논문에서는 다크웹에서 발생하였던 중대 범죄 사례들을 살펴보며, 수사에 사용되었던 포렌식 기법들을 분석해보며 그것의 한계점에 대해 알아보고자 한다.

II. Preliminaries

1. 다크웹 상에서의 중대범죄 사례

1) 마약거래

다크웹 상에서 마약 거래는 매우 큰 규모로 이루어지고 있다.

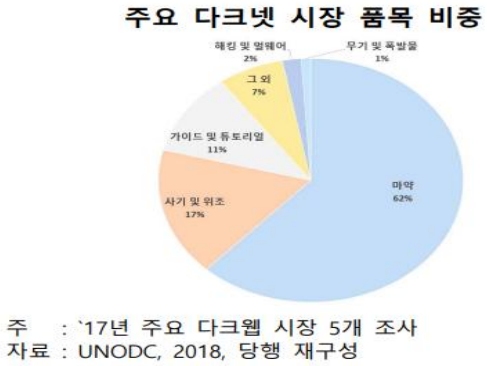

Fig 1. Share of major darknet market items

UNODC에 따르면, 2017년 기준 마약 거래가 다크웹 시장에서 발생되는 범죄에서 전체의 62%를 차지했음을 알 수 있다[1]. 다크웹이 제공하는 익명성과 그것의 거래 수단인 암호 화폐의 비밀성을 통해 마약 거래를 수월하게 진행되도록 하는데, 이는 국제적으로 거래가 이루어지기도 하여 사용자들의 흔적을 찾는데 어려움을 주는 상황이다. 대표적으로 'silk road 사건'이 있다.

Silk Road는 2011년 한 개인에 의해 개설된 다크웹 상의 사이트로 대규모 마약 거래 사이트로 유명한 사이트이다. Silk Road는 마약뿐만 아니라 다양한 불법 상품도 판매하였고, 비트코인을 통하여 익명 거래로 이루어졌다. Silk Road는 앞서 설명하였던 토르 네트워크를 통해 접근할 수 있는 웹 사이트였기에 판매자 구매자 모두 익명성을 보장받으며 활동할 수 있었다.

2) 아동 포르노그래피

아동 포르노그래피는 아동을 대상으로 한 성 착취와 같은 성적학대 형태로 이루어진 불법 콘텐츠이다. 다크웹에서는 이러한 아동 포르노그래피가 제작되어 유통 및 판매가 활발히 이루어지고 있다. 그것의 대표적인 사례로 'Playpen 사건'이 있다.

'Playpen'은 아동 포르노 사이트로 다크웹에서 운영되었던 유명 사이트이다. 해당 사이트의 회원들은 서로 아동 포르노를 공유하고 거래하는 활동을 활발히 했다. 'Playpen' 또한 암호화된 통신으로 운영되었다.

3) 개인정보 유출

해커들은 피해자의 신용 카드 정보, 소셜 보안 번호, 은행 계좌 정보 등 다양한 피해자들의 개인정보를 수집하여 다크웹 상에 유출 및 판매하여 큰 수익을 얻는다. 이러한 개인 정보 유출은 신용 카드 사기 범죄로도 이어질 수 있기 때문에 큰 위험성을 가지고 있다.

NordVPN의 최고기술책임자 '마리유스 브리디스'의 발표에 따르면 12,500 여개의 대한민국 카드가 다크웹상에 판매되었고, 대한민국 카드의 평균 가격이 8,630원이다. 또한, 지난 2020년 랜섬웨어 조직 '클롭'이 랜섬웨어 공격으로 대한민국 기업 이랜드 그룹의 200만 건의 신용카드 정보를 탈취하여 다크웹에 공개하여 약 100만개의 신용카드 정보가 다크웹 상에 무방비하게 노출된 사례도 있다.

2. 다크웹 상의 중대범죄를 분석시 사용되는 주요 포렌식 기법

이러한 다크웹 상의 범죄를 수사할 때 사용된 포렌식 기법은 크게 트래픽 분석, 비트코인 거래 분석, 암호해독, 스니핑, 디지털 포렌식으로 이루어진다.

1) 트래픽 분석 : 다크웹 상의 범죄자를 식별하기 위해 다크웹 상의 트래픽 패턴을 분석한다. 이를 통해 네트워크 흐름과 통신 프로토콜 등을 파악하여 다크웹 상의 의심스러운 사이트 접속 기록을 추적한다.

2) 비트코인 거래 분석 : 다크웹 상의 범죄에서 거래가 이루어질 시 대부분 암호화폐를 사용한다.

Fig. 2. Transactions on the dark web through cryptocurrencies

이처럼 암호화폐의 등장으로 인해 다크웹 상의 범죄가 기승을 부리고 있는데, 블록체인 상의 데이터 분석을 통해 관련 비트코인 주소와 트랜잭션 등 비트코인 거래 기록을 추적한다. 이를 위해 블록체인 탐색기를 사용하고, 데이터베이스에 접근하며, 또한 주소 클러스터링 기법을 활용하기도 한다. 이 기법은 비트코인 주소들 사이의 관계 분석을 통해 특정 소유주에 의해 여러 주소들이 제어되고 있는지 파악할 수 있도록 한다. 이러한 방법으로 해당 사건의 운영자가 사용한 비트코인 주소를 추적하고, 이 주소를 통해 다른 사용자들의 주소를 연결하여 판매자 및 구매자를 식별하고 그들의 패턴을 분석한다.

3) 암호해독 : 암호화된 통신을 추적하기 위해 암호화를 직접 해독하거나 우회하여 암호문을 해독하여야한다. 이를 위해 아래와 같은 방법이 주로 사용된다.

- 키로깅 : 키로깅이란 사용자의 키보드 입력 행위를 가로채어 기록하는 기술로, 이를 분석하여 암호를 추측하여 해독하는 방법이다. 악성 소프트웨어나 하드웨어 장치를 사용해 실행되며, 사용자가 암호화된 통신을 사용하더라도 사용자의 입력을 가로챌 수 있다. 이러한 키로깅을 통해 사용자의 로그인 정보, 금융정보 등을 탈취할 수 있기 때문에 개인정보침해의 문제가 있는 불법적인 방법에 속한다.

- 암호 해독 알고리즘 : 암호화된 데이터를 해독하기 위한 알고리즘으로 대칭키·비대칭키 암호화가 있다. 대칭키 암호화의 대표적인 알고리즘으로 AES(Advanced Encryption Standard)가 있으며, 암

호화와 복호화에 동일한 키가 사용된다. 비대칭키 암호화의 대표적인 알고리즘으로는 RSA가 있으며 공개키와 개인키가 쌍으로 사용된다. 이처럼 암호 해독 알고리즘을 통해 암호화된 데이터를 복원하기 위해 관련 키를 추측하거나 계산한다.

- 브루트 포스 공격 : 브루트 포스 공격 '무차별 암호 대입 공격'으로, 가능한 모든 조합을 시도하여 암호를 해독하는 공격 기법이다. 이는 간단한 암호에 대해서는 효과적일 수 있지만, 암호가 복잡한 경우 탐색하는 데에 시간이 오래 걸릴 수 있기 때문에 실현 가능성이 낮을 수 있다.

- 사회공학기법 : 사회공학기법은 사람들의 신뢰를 바탕으로 정보를 추출하여 암호를 해독하는 기법으로 사람들을 속이거나 유인하여 정보를 획득한다. 전화, 메세지, 이메일 등 다양한 수단을 통해 위협, 협박, 유인 등의 위협적인 방법으로 이루어진다.

4) 스니핑 : 네트워크상에서 데이터가 전송될 때, 스니퍼같은 도구를 사용하여 데이터 패킷을 가로채어 정보를 분석하는 기법이다. 또한 스니핑은 토르 네트워크와 같이 암호화된 통신에서도 메타데이터나 패턴 등을 분석하여 정보를 파악하는데 사용할 수 있다.

5) 디지털 포렌식 (Digital Forensics): 다크웹 상에서 사용된 컴퓨터나 서버, 저장 매체 등의 디지털 자산을 분석하여 범죄 혐의자의 행위나 데이터를 추적하고 수집하기 위해 디지털 데이터 복구, 메모리 분석, 파일 시그니처 분석 등의 기법이 활용될 수 있다. 또한 통신이나 파일에 대한 정보를 담고 있는 메타데이터 분석을 통해 사용자의 활동 패턴이나 통신 상대방을 파악한다.

III. Conclusions

수많은 노드로 이루어진 토르 네트워크상에서 운용되고 있는 다크웹 자체를 포렌식 하는 행위는 여전히 어려운 실정이다. 하지만 이러한 암호화 네트워크의 등장은 애초에 범죄의 목적이 아니었기에, 본 네트워크가 제공하는 익명성과 비밀성이 강제적으로 해제시키는 것은 다크웹의 본질을 잃어버리도록 할 것이다.

그러나 다크웹 상의 범죄들은 날이 갈수록 악질적으로 발전하고 있기 때문에 다크웹 사용자를 포함한 모든 인터넷 사용자가 스스로 이러한 위험을 사전 차단 및 예방하기 위해 위험방지수칙 등 취할 수 있는 다양한 예방법이 필요할 것으로 보인다.

REFERENCES

[1] Park Kyung-min(2021), KDB Future Strategy Institute Industrial Technology Research Center. Current status and implications of the dark web