포렌식 관점에서 보는 DarkWeb 보고서

DarkWeb Forensic Tool Production

박성준

목차

1. VPN

*-* VPN개념

*-* VPN을사용하는이유

1. Tor

- Tor개념

*-* 동작원리

1. DarkWeb

*- DarkWeb* 개념

*- DarkWeb* 접근방법

1. VPN

* VPN 개념

VPN(Virtual Private Network)은 흔히 ‘가상사설망’이라고 알고 있는 VPN이라는 기술은 인터넷과 같이 공용으로 사용하는 공중망을 특정 사용자나 조직이 가상의 터널을 만들어 단독으로 사용하는 사설망처럼 동작시키는 것을 말한다. 특수한 목적을 위해 인트라넷을 구축할 때가 있는데 이를 내부망이나 사설망이라고 한다.

특정 인트라넷을 접속해보면 알겠지만 인트라넷을 기존 우리가 사용하는 웹 사이트와는 다른 별도의 주소와 환경을 가지고 있다.

* 사설망 : 특정 소수의 사용자에게 접근이 제한되도록 기업이나 학교 같은 특정 기관에서 구축한 통신망이다.
* 공중망 : 누구든지 제약받지 않고 자유롭게 접근할 수 있는 통신망이다.
* VPN을 사용하는 이유

1. 아이피를 우회하거나 자신의 아이피를 감추기 위해서 사용한다.
2. 방화벽 보안 정책을 우회해서 어떤 서비스를 이용하고자 할때 사용한다.
3. 자신의 VPN 사이의 패킷을 암호화해서 안전한 통신을 위해 사용한다.
4. 해외에서 특정 서비스를 이용하는데 느리면 가상의 네트워크로 묶을 때 사용한다.

VPN을 접속하려면 서버에 접속하는데 이 과정이 전부 암호화가 이루어지며 강력한 수준의 보안성이 확보된다.

그래서 VPN을 사용하면 사용자가 역추적 당할 일이 없고 보안성과 익명성이 보장된 상태로 인터넷을 이용할 수 있다.

2. Tor

* Tor 개념

Tor(The Onion Router)는 DarkWeb 소프트웨어 중 하나로 네트워크 우회와 익명성을 위해 사용된다.

Tor와 VPN을 비교하면 프록시 서버나 로그가 남을 가능성이 있는 VPN보다 Tor가 안전하다. Tor의 트래픽은 출발지에서 각각의 공개 키로 순차적으로 암호화 된다.

일반적인 프록시 우회방식과 다르게 프로그래밍된 DNS 패치 등을 사용해 3중 4중으로 보호해서 Tor 유저만 접속할 수 있는 일종의 인트라넷이 형성되어있는 것이다.

* Tor 동작 원리

일반적으로 인터넷 통신은 사용자의 PC가 ISP를 통해 목적이(서버나 타 PC)에 연결해 데이터를 주고 받는 식으로 이루어진다. 그런데 Tor는 목적지까지 한 번에 통신하지 않고 중간에 같은 Tor 라우터를 실행하고 있는 노드들을 여러 개 거쳐서 보낸다. 즉 쉽게 말해 A → Z 이런 식으로 가지 않고 A → B → C → D → X → Y → Z 이런 식으로 여러 노드를 거쳐서 보낸다. 그래서 Tor가 일반적인 브라우저보다 속도가 느린 이유가 이 때문이다.

패킷을 양파처럼 겹겹이 암호화해서 보내고, 이때 각각의 노드의 공개 키를 통해서 암호화하므로, 패킷의 출발지와 목적지를 알아내려면 세계의 거의 모든 노드를 알아야 한다. 노드는 전 세계에 걸쳐 랜덤하게 흩어져 있으므로, 전 세계 거의 모든 PC를 장악하지 않는 이상 Tor를 이용한 통신은 거의 추적 불가능하다.

3.DarkWeb

* DarkWeb 개념

다크웹은 접속 허가가 필요한 네트워크나 특정 소프트웨어로만 접근할 수 있는 오버레이 네트워크이다. 쉽게 말해 암호화된 네트워크에 존재하며 일반적인 검색 엔진 브라우저를 사용해서는 찾거나 방문할 수 없는 웹 사이트 집합체이다.

이런 다크 웹에 존재하는 거의 모든 사이트는 토르(Tor) 암호화 툴을 사용해 정체를 숨긴다. Tor를 사용하면 위치를 속여 자신의 현재 위치가 아닌 다른 국가에 있는 것처럼 할 수 있다. 그런데 이 다크 웹 사이트를 방문하려면 방문자가 Tor을 사용해야지만 방문할 수 있다.

* DarkWeb 접근 방법

Tor를 설치하고 <http://www.torproject.org> 에서 모든 툴이 포함된 Tor Browser Bundle을 다운로드한다.

다운로드한 파일을 실행하고 압축을 풀고 Start Tor Browser을 하면 접근 할 수 있다.