다크넷과 불법약물거래(1)

저자 최혁재
경희의료원 한약물연구소 부소장
약학정보원 학술자문위원

개요

마약사범은 인터넷을 구입경로로 이용하여 증가추세에 있다. 특히 토르 기술을 바탕으로 한 다크넷에서의 마약거래사이트는 익명성과 추적불가능성을 기반으로 범죄 자체를 은닉화하면서 문제의 온상이 되고 있다. 마약범죄의 증가는 전염병의 유행, 판매수익의 범죄조직으로의 유입 등 파생문제도 심각하다.

키워드

서피스넷, 딥 웹, 다크넷, 다크웹, 토르, 마약사범, 마약사이트

1. 새로운 위협

(1) 서로 다른 네 개의 사건들

그림 1. 워너크라이에 감염된 PC의 화면(출처:B블로터)

첫 번째 사건 - 2015년, 전 세계적으로 랜섬웨어[1]에 의한 해킹 공격이 있었다. 일명 '워너크라이(Wannacry)' 사태였다. 당시 최소 150개국에서 30만대의 컴퓨터가 감염되었고, 해커는 데이터 복구를 조건으로 금전적 대가를 요구했다. 지급방식은 추적이 어려운 비트코인을 요구했는데, 당시 화면에 뜬 옵션은 감염 후 3일 이내에 지급되면 300달러어치의 비트코인을, 3일 이상 7일 이내에는 600달러어치의 비트코인을 요구

1) 인질(Ransome)이라는 뜻대로 감염된 사용자의 PC내 시스템 및 데이터를 암호화 해서 소유주가 접근하는 것을 막는 해킹을 말한다. 파일을 원상복구하기 위해서는 해커가 요구하는 금전적 대가를 치러야 한다.

했다. 물론 7일을 초과하면 다시는 파일을 되살릴 수 없다는 경고도 따라왔다. 울며 겨자 먹기로 해커에게 지급된 돈은 집계된 것만 최소 7만 달러였다. 당시 이전의 랜섬웨어와 달리 워너크라이는 주변에 같은 네트워크로 연결된 컴퓨터에 자동으로 접속해서 감염시키는 특성인 '웜'방식을 이용하면서 피해를 증폭시켰다.

두 번째 사건 - 2010년 12월. 세계 민주주의의 역사에 한 획을 그었다고 할 만한 사건이 아프리카의 튀니지에서 발생했다. 부당한 단속에 항의하며 한 청년이 분신자살한 것을 계기로 대규모 민주화 시위가 일어났다. 아랍 및 아프리카계 국가에서 민중봉기로 독재정권을 무너뜨린 첫 사례가 되었던 이 사건은 튀니지에서 23년간 장기 집권한 벤 알리 대통령이 사우디아라비아로 망명한 뒤에도 그치지 않고, 이집트, 시리아를 비롯한 주변 국가로 독재타도 운동을 전개해 나갔던 '아랍의 봄'의 원동력이 되었다. 그 후, 2015년 튀니지의 국민4자 대화기구는 노벨평화상을 받기도 했지만, 튀니지의 국화였던 재스민의 이름을 따서 '재스민 혁명'이라고 불렸던 민주화 혁명은 그 결실이 지금 모호하다. 그 다음해에 최초로 자유선거를 치렀고, 2016년 12월에는 평화적으로 민선 대통령까지 선출했지만 국가의 부흥을 일으킬 수 있는 경제적, 민주적 기반이 워낙 약했던 탓인지 아직 민주주의의 결실로는 가지 못하고 있다. 되려 테러단체인 IS(이슬람 공화국)에 가장 많은 전사를 제공한 국가가 되었고, 35%에 이르는 높은 청년 실업률도 발목을 잡고 있다. 물론 이것은 무바라크 대통령을 권좌에서 몰아낸 이집트나, 카다피를 몰아낸 리비아에서도 마치 평행이론처럼 되풀이되는 슬픈 역사이다.

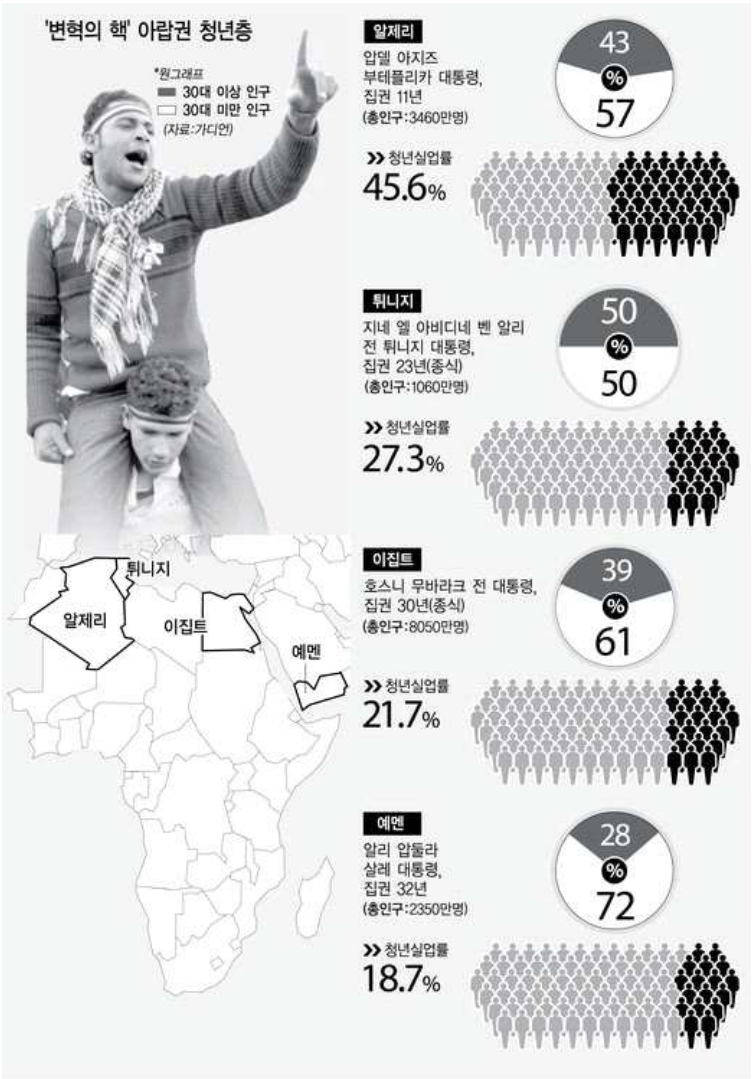

그림 2. 아랍의 봄을 일으켰던 나라들(출처:경향신문)

세 번째 사건 - 2016년 7월 22일 독일 뮌헨의 올림피아 아인카우프스첸트룸에 있던 길가의 맥도날드. 저녁 무렵의 여유로움을 찢고 들려온 소리는 사건을 기억하는 이들에게 결코 잊지 못할 충격이 되고 말았다. 18세의 이란계 독일인은 범행 직후, 스스로 머리를 쏘아 자살했지만, 그가 무차별 난사한 총격으로 인해 평화롭게 하루를 정리해야 할 다른 9명의 사람들은 목숨을 잃었고, 21명의 사람들이 총상을 입었다.

네 번째 사건 - 2015년 8월. 50여 개국에 걸쳐 3천 7백만 명 이상의 수많은 기혼 남녀들을 회원으로 보유하면서 불륜을 조장하며 화제를 뿌려왔던 애슐리 매디슨의 홈페이지가 해킹을 당해 무려 10GB에 달하는 회원정보가 웹상에 업로드되는 사건이 일어났다. 몇몇 회원들은 목숨을 끊기도 했고, 7천억 원 규모의 집단소송 사태가 일어났으며, 해당사는 4억5천만 원에 달하는 현상금을 걸고 해커를 찾기도 했지만, 애슐리 매디슨 해킹 사건의 파장은 일파만파였다. '임팩트팀'이라는 해킹집단이 공개한 정보 덕분에 사용자들은 2,500달러를 비트코인으로 지불하지 않으면 외도사실을 폭로하겠다는 협박편지에 시달리기도 했다.

이 네 가지의 서로 다른 사건은 모종의 공통분모를 가진다. 바로 비공개 비밀 정보를 공유하는 매개체로 연결되어 있던 것이다. 그 정체는 바로 '딥 웹(Deep Web)'이라고도 불리며, '다크넷(Dark Net)', '다크웹(Dark Web)'이라는 별칭으로도 알려진 인터넷 공간이다. 이 익명성으로 가려진 공간에서 해커들이 모의하여 해킹방법을 공유하고, 해킹 프로그램을 서로 간에 거래하며, 또 범죄대상과 시기 등을 마음 놓고 모의하는 통에 워너크라이 뿐만 아니라 그 다음해인 2016년에 미국에서 CNN을 비롯한 85개 업체의 서비스를 중단시킨 디도스(분산서비스거부)공격을 실행한 악성코드 '미라이(Mirai)'가 쉽게 만들어질 수 있었던 것이다. 이들의 활동목적은 초기에는 '과시'가 많았지만, 지금은 금전적 대가 때문이다. 따라서 모든 가전제품까지 네트워크로 연결되는 사물인터넷 시대의 초기인 가까운 미래에는 거꾸로 아직 보안이 약한 사물인터넷의 취약점을 파고들어 사람들의 일상을 위험에 빠트릴 우려가 증폭되고 있는 것이다.

재스민 혁명은 '페이스북 혁명'이라는 별칭으로도 불릴 정도로 소셜 네트워크의 힘을 입었었다. 극도의 언론통제 상황에서도 소셜네트워크를 통해 국민의 여론을 수렴해내고 시위를 조직할 수 있었기 때문에 정치적인 구심점이나 리더가 없는 약점에도 불구하고 혁명을 성공적으로 이끈 것이다. 뿐만 아니라 IP추적이 방지되는 딥 웹의 특수 브라우저를 통해 반정부 시위대원들의 정보 교환 창구가 보호를 받을 수 있었던 것이 큰 원동력이 되었다. 뮌헨총기 난사사건에서 범인 알리 다비트 존볼리가 무기를 구입할 수 있었던 것도 바로 이 다크넷의 무기거래 사이트를 통해서였다는 것이 알려지면서 최근 연이어 벌어지고 있는 무차별 총기 난사사건의 주요 원인으로 지목받고 있다. 총기가 허용된 미국에서도 금지되어 있는, 자동발사를 가능케 하는 장치도 이 사이트에서는 얼마든지 살 수 있다는 것이다. 애슐리 매디슨 사건도 딥 웹이라는 공간에 감추어진 회원정보의 안정성을 굳게 믿던 회사 측의 방심이 해커들에게 일격을 맞은 사건으로 알려지고 있다. 이처럼 이미 딥 웹 또는 다크넷의 세계는 빠르게 세계인들의 일상사와 삶의 안정성 속에 커다란 영향을 미치고 있는 것이다.

(2) 포털 사이트의 한계

국내 마약사범으로 적발되는 건수는 해마다 증가추세에 있다. 물론 한 번 마약중독의 길에 들어서게 되면, 치유되지 않는 중독의 특성상 재범률이 높기 마련이므로 적발건수는 증가할 수밖에 없는 경향을 가진다. 오히려 갑자기 큰 폭의 감소치를 보여준다면, 적발되지 않는 새로운 수법이 등장했다는 적신호가 될 수도 있는 것이다. 하지만, 마약은 어떻게 구입할 것인가? 만약 네이버나 구글, 다음, 야후 및 트위터 등의 소위 포털 사이트에서 마약구입방법을 찾는다면 쉽게 구할 수 있을 것인가? 아마 어느 정도는 가능할 것이다. 하지만, 결국 횟수가 늘어나면서 마약사범으로 입건되는 것은 시간문제일 것이다. 이는 이미 우리나라 검찰청에서 운영하고 있는

'인터넷 마약류 범죄 모니터링 시스템'으로 인해 사이버 상에서 벌어지는 마약류 불법 판매 광고와 밀거래 행위가 수시로 체크되기 때문이다. 접속권한을 가진 사람만 해도 검사 80여명에 수사관 250여명이다. '얼음', '빙두', '아이스' 등 53가지 마약류를 뜻하는 은어들이 자동 검색되고, 이 검색 시스템은 모바일 메신저인 '위커', '텔레그램', '위챗' 등을 통해서 이루어지는 거래들도 모니터링 하고 있다.

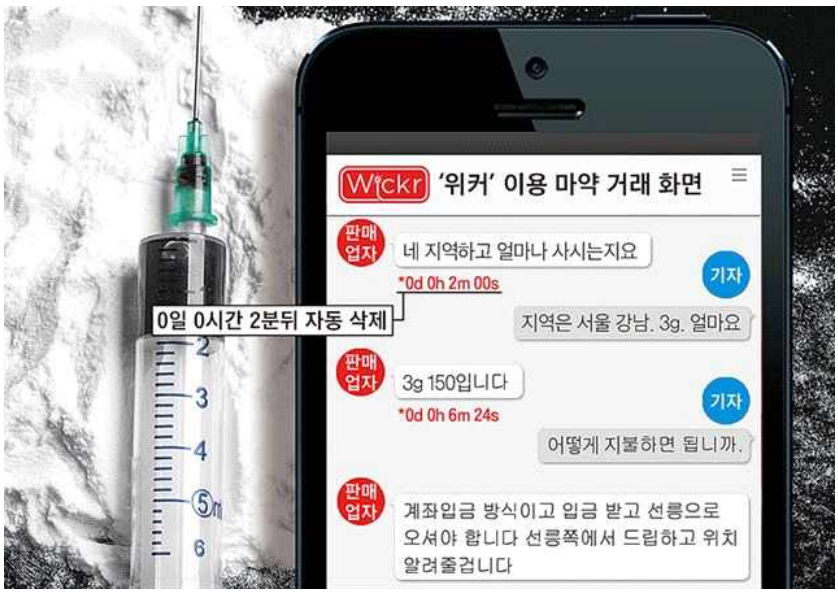

그림 3. 모바일 메신저를 이용한 마약거래 화면(출처:한국일보)

최근에는 스마트폰의 즉석 만남을 위해 이용하는 채팅앱도 마약 담당 수사관들의 주요 관심사가 되었다. 마약 투약자들이 같이 투약을 하면서 성적 욕구를 해소하기 위해 투약 파트너 찾기 창구로 이용하면서부터다. 이 과정에서 함정수사 여부에 대한 논란도 많다. 얼마 전 검거된 모 정치인의 자녀도 이런 방식으로 체포된 것으로 알려졌다. 다시 말해서 포털사이트나 모바일 메신저를 이용한 마약구입은 금방 한계를 드러내게 되어 있다는 것이다. 만약 개인 PC에서 마약거래가 이루어진다면, IP추적을 통해 검거과정은 그리 어렵지 않다. 특정 장소의 공공 PC에서도 잦은 움직임이 감지된다면, 역시 IP추적으로 검거가 가능하다. 특히 포털사이트를 이용하여 관련 단어를 검색할 경우, 클라이언트인 사용자와 포털사이트의 서버사이에 프록시 서버(Proxy server)[2]가 있어서 유사한 검색 결과를 바로 찾아주기 때문에 검색 시간이 단축되기도 하지만, 검색기록이 남아있다는 이유로 거꾸로 수사당국의 입장에서는 마약사범 검거에 유리한 양면성을 가진다.

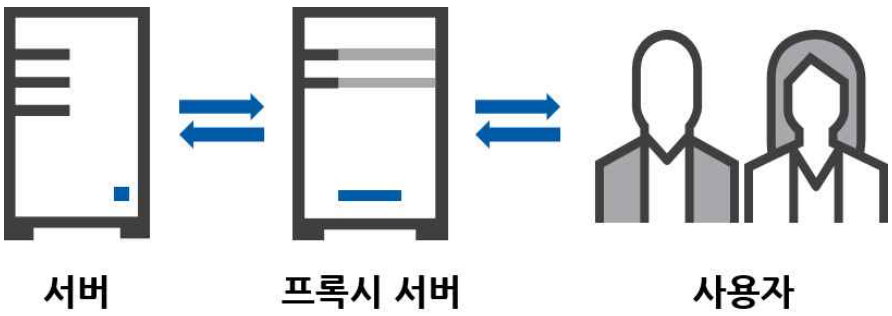

그림 4. 프록시 서버의 개념도(출처:펜타시큐리티 공식 블로그)

2) 네트워크 시스템에 자체 방화벽을 가져야할 필요가 있을 경우, 외부와의 통신 때 직접 통신하지 않고 대리로 통신을 중계하는 기능을 위해 만들어 놓은 서버. 보안상의 목적 이외에도 포털사이트 등에서 검색한 내용 중 최근 사용한 내용들을 일부 저장하는 캐시란 기능을 통해 전송시간을 절약하고 매번 불필요하게 외부와의 연결을 하지 않아도 되는 장점을 줌으로써, 외부 트래픽을 줄이고, 네트워크 병목현상을 방지하는 효과를 줌

(3) 국내외 마약시장의 성장과 사회적 심각성

따라서, 기존의 방식대로 마약을 온라인에서 구입하는 것은 한계가 있음에도 문제는 마약구입자가 점점 늘어난다는 것이다. 2016년까지의 국내 마약사범은 1만 4천명을 돌파하면서 전년 대비 20%나 상승했다.

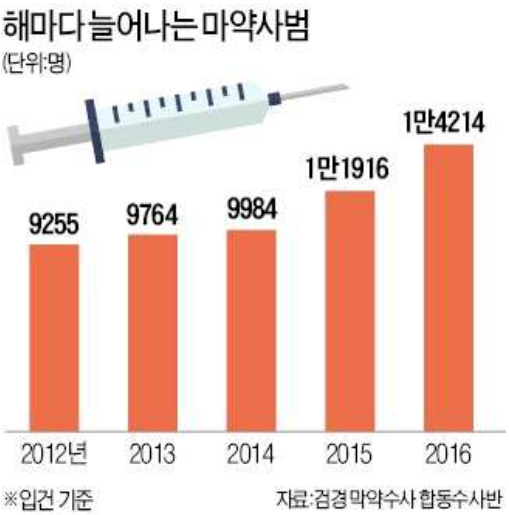

그림 5. 마약사범검거 현황(출처:한국경제)

이 우려는 비단 국내만의 고민은 물론 아니다. 2015년 전 세계 성인인구(15~65세)의 0.6%에 달하는 2천9백5십만 명이 적어도 한 가지 이상의 마약을 사용한 것으로 집계되었다. 물론 통계에 나타나지 않은 숫자는 그 몇 배에 달할 것이라고 추측하고 있다. 이중 마약복용으로 인해 결국 마약중독으로 목숨을 잃은 사망자만 19만 명이나 되었다. 마약 투여자 중 무려 1천 2백만 명이 주사를 통해 마약을 주입했고, 이 과정에서 동일한 주사기를 돌려쓰다가 160만 명이 에이즈에 감염되었다. C형 간염에 걸린 사람만 610만 명이나 되었고, 두 가지 질병에 모두 감염된 사람도 130만 명이나 될 정도로 마약의 부정적 여파는 심각하다. 이 위협은 보건의료 측면에만 존재하지는 않는다. 전 세계 범죄조직 수익 중에서 1/4~1/3이 마약유통에서 발생하는 것이다. 마약중독자들에게 가장 보편적으로 쓰이고 있는 아편만 해도 아프가니스탄에서 재배되는 아편 수입의 85%가 탈레반의 수입원으로 사용되고 있음을 볼 때, 범죄조직과 테러조직의 유지, 확장에 마약판매수익이 사용되고 있다는 것은 결코 간과할 사항이 아닌 것이다.

더군다나 국내외를 막론하고 이들 중 다수가 앞에서 얘기한 다크넷을 통한, 수사의 한계선을 지난 경로를 이용해서 마약을 구입하고 있다는 것이다.

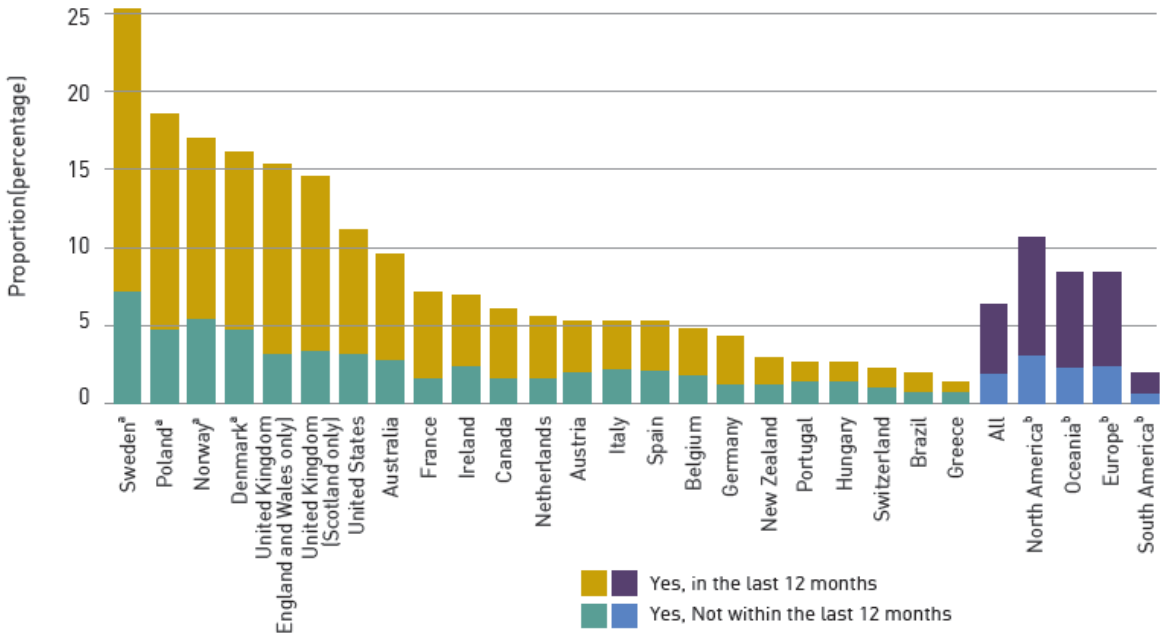

그림 6. 다크넷을 통해 마약을 구입한 국가 및 지역별 응답자(출처:대검찰청 마약류범죄백서, 2015)

위 그래프에서는 2014년에 스웨덴과 폴란드, 노르웨이 등이 다크넷을 통해 마약을 구입한 비율이 가장 높은 것으로 드러났다. 하지만, 2016년에는 핀란드 마약 사용자의 41%가 다크넷을 통해 마약을 구입했고, 이어 덴마크(27.2%), 영국(25.3%), 웨일즈(25%), 스웨덴(24.5%), 스코틀랜드와 스페인(22.5%)이 그 뒤를 따를

정도로 변화가 있었다. 앞으로도 이 비율은 위 그래프처럼, 현재 마약중독자수가 많은 북미, 유럽, 오세아니아를 중심으로 상위권을 형성할 것으로 보인다. 국내에서도 이런 다크넷을 이용한 마약거래는 이미 홈쇼핑처럼 쉽게 이루어지고 있다는 것이 일선의 평이다. 마약의 수령방법은 감시체계가 가장 소홀하기 마련인 국제특급우편이 애용되는데, 2017년 상반기만 해도 국제특급우편을 통해 들여오다 적발된 마약류만 총 197건이나 되었다. 전년대비 무려 160%가 늘어난 규모인 것이다. 이 외에도 속칭 '던지기'라는 수법으로 지하철 사물함이나 심지어는 길거리의 휴지통에 마약을 던져놓고 가면서 검거를 피하는 방법, 국외 여행지에서 직접 만나는 방법 등도 쓰이고 있는 것으로 알려졌다. 현재 50개 이상의 마약판매 사이트가 다크넷에서 성업 중이지만, 향후 다크넷의 효용도가 올라가면 이 숫자는 기하급수적으로 증가할 가능성이 농후하다고 할 수 있다.

국내에서의 다크넷 관련 마약범죄는 완성된 제품의 판매확산에만 있지 않았다. 재배방법까지 상세히 소개된 다크넷을 통해 대마를 직접 재배하고 흡연용 파이프로 위장해 파는 일들이 생기는 것이다. 한마디로 정상적인 루트를 통해서 접하기 어려운 범죄정보가 그대로 노출되는 셈이다.

2. 다크넷의 실체

(1) 다크넷의 개념과 토르(Tor)의 등장

그림 7. 인터넷의 개념도(출처:대검찰청 다크웹과 가상화폐를 이용한 범죄동향)

인터넷은 등장 초기부터 '정보의 바다'라고 불려왔다. 직접 오프라인으로 찾기 어려운 정보들을 한눈에 볼 수 있는 인터넷이야말로 정보화 시대에 꼭 필요한 도구로 선택되어왔다. 그런데 우리가 네이버, 구글, 다음, 야후 등을 통해 사이트와 정보를 직접 검색할 수 있는 통상적인 의미의 인터넷은 서피스웹(Surface Web)이라 불리며, 이와 달리 검색엔진을 통해 검색되지 않는 종류의 모든 웹페이지를 통칭하여 딥 웹(Deep Web)이라 부른다. 딥 웹의 가장 쉬운 예로는 외부 네트워크와 연결되지 않는 전자도서관의 데이터베이스, 기업의 직원 전용 홈페이지, 미국 기상청의 데이터베이스, 검찰청의 직원전용 수사정보페이지인 E-pros 등이라고 할 수 있다.

즉, 외부에 공개하기 어려운 정보에 대해 접근권한을 설정한 것이다. 최근에는 아예 외부에서는 아무리 아이디와 패스워드를 알아도 접근할 수 없도록 원천적 차단이 된 기업의 직원전용 홈페이지도 많다. 보안을 강화하기 위해서 정보보호 인증 자체가 강화된 탓이다. 따라서 이 정도의 딥 웹만 하더라도 수사에 필요할 경우, 압수영장을 청구해야 하는 것이다. 참고로 북한의 인터넷은 전체가 딥 웹화가 되어 있다. 통신 시스템 광명망은 극소수를 빼면 외부의 IP와 서버에서 접속이 불가능하기 때문이다.

그런데 실제로 마약이나 기타 범죄와 관련된 사이트를 찾기 위해서는 그 딥 웹 중에서도 한정된 방법으로 들어가는 쉐도우넷, 다크넷 또는 다크웹의 세계로 들어가야 한다. 물론 클린넷(Clean Net)이라고도 불리는 검색엔진으로는 안되고, 직접 IP를 찾아서 들어가야 한다. 그러나 다크넷으로 입장하는 목적 자체가 불법거래 등의 분명하지 않은 부분이 많으므로 자신의 IP에서 직접 사이트로 들어가는 것은 의미가 없다. 따라서 역추적이 불가능한 방법을 써야 한다. 이 때, 전문적인 기술 없이도 IP 역추적을 불가능하게 하면서 감춰진 다크넷의 사이트를 방문하게 해주는 전용 브라우저가 등장한다. 늘 익스플로러나 크롬에만 익숙해져 있던 각국의 인터넷 이용자들에게는 다소 생소한 감도 없지 않으나, 새로운 브라우저인 토르의 개발은 역설적으로 정부기관에 의해서 이루어졌다. 1990년경 범죄 수사 등을 위해 미국 해군연구소에서 익명으로 인터넷 접속이 가능한 기술을 개발해낸 것이다. 하지만, 이 기술을 정부 관계자만 사용한다면, 이 정체불명의 IP로 접속할 때마다 새로운 존재가 자신을 들여다본다는 것을 범죄용의자, 해커들이 알 우려가 있기 때문에 아예 오픈 소스로 하여 일반에 공개해버린 것이다. 그 결과, 이 '은닉의 기술'은 주로 불법거래에 악용되기 시작한 것이다.

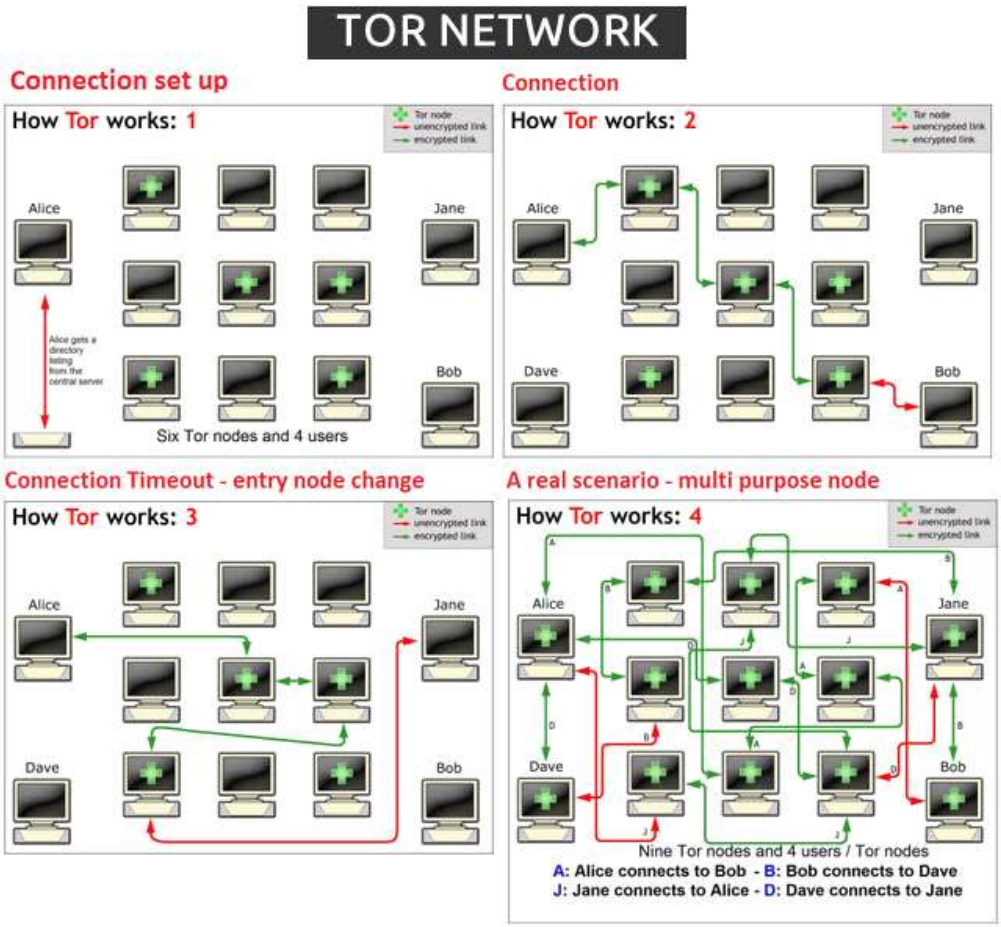

그림 8. 토르를 이용한 접속방식(출처:네이버 블로그)

토르의 접속방식은 위 그림과 같이 사용자의 PC에서 최종 정보를 담고 있는 서버까지 최소 3, 4번씩 프록시 서버를 우회해서 사이트에 접속한다. 직접 프록시로 접속해서 기록을 남기지 않기 위함이다. 세계 각국의 수많은 서버를 거쳐 국적불명의 IP를 생성해내는 것이다. 5분 만에 갈 수 있는 지름길을 놔두고 1시간 동안 길을 빙빙 돌아 찾아가는 것과 같다. 이 경우, 원래 사용자의 IP를 찾아내려면 그 IP가 거쳐 온 서버 기록을 전부 뒤져야 한다. 그런데 서버 1대에는 실시간으로 수많은 IP가 드나든다. 그 잠깐 머무르는 IP를 경유하기도 하니까 그 기록을 전부 역으로 추적한다는 것은 불가능에 가까운 일이다. 물론 수많은 PC를 드나드는 동안 암호화가 이루어진다. 토르의 가장 큰 약점이라면 이런 장치들 때문에 접속 속도가 무척 느리다는 것이다.

그림 9. 토르 브라우저로의 접속화면(출처:다크웹과 가상화폐를 이용한 범죄동향)

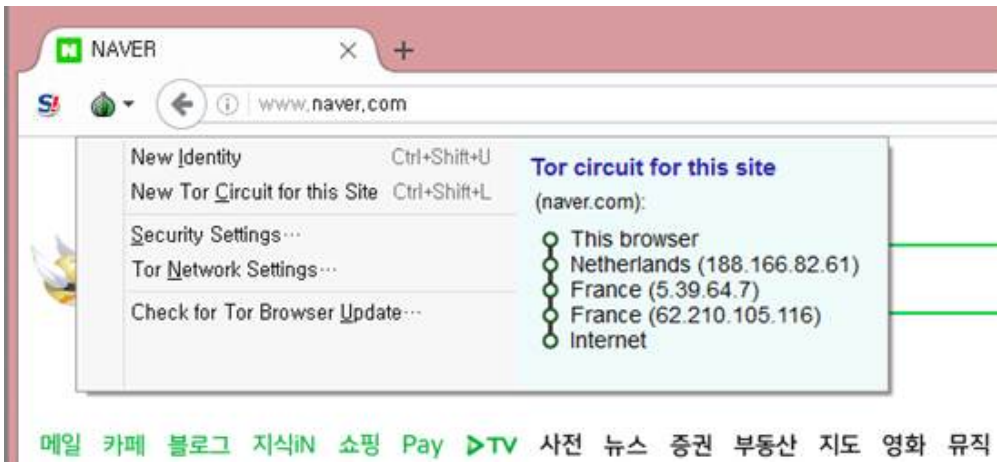

그림 10. 토르 브라우저에서 네이버 접속시 화면(출처:네이버 블로그)

토르가 일반인에게 공개되기 시작한 뒤, 최근 5, 6년간 본격적으로 이용자가 증가하면서 토르를 기반으로 하는 불법사이트도 급격히 증가하기 시작했다. 이 중 마약거래 사이트가 압도적으로 많다. 국내에서도 자생적으로 생겨난 사이트 중 대마초 유통을 목적으로 하는 한 사이트는 동시 접속자만 평균 20~30여명에 이를 정도이다. 사실 다크넷의 상위 20대 판매 상품 대부분은 마약과 불법 포르노물이 차지하고 있다. 전 세계 누구라도 주문을 하면 그 나라로 직접 배송하는 유통망을 가지고 있을 정도이다.

약사 Point

1. 마약범죄의 증가는 예기치 못한 전염병의 유행, 마약판매수익의 범죄조직으로의 유입으로 인한 범죄의 확장 등 여러문제를 일으킬 수 있음에 주목해야 한다.

2. 최근 익명성을 기반으로 한 다크넷을 통해 마약거래가 통제 불능의 영역으로 진입하고 있음에 대해 경각심을 가져야 한다.

■ 참고문헌 ■

1) 네이버 지식백과

2) 다크웹과 가상화폐를 이용한 범죄 동향, 대검찰청, 2017년

3) 정보화 시대의 자금세탁과 규제, 대구지검, 2017년

4) 인터넷과 마약시장, Drug Focus, 여름호, 한국마약퇴치운동본부, 2016년

5) B블로터,
http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=293&aid=0000019839

6) 중앙일보, http://news.joins.com/article/21613805

7) 경향신문,
http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=104&oid=032&aid=0002112657

8) 머니투데이,
http://news.mt.co.kr/mtview.php?no=2016072507301980931&outlink=1&ref=http%3A%2F%2Fsearch.naver.com

9) IT world, http://www.itworld.co.kr/news/105740

10) 맥심 데일리뉴스, http://maxim.wowtv.co.kr/cms/contents_view.php?contents_uid=6008

11) 연합뉴스,
http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=101&oid=422&aid=0000051446

12) 중앙일보, http://news.joins.com/article/21978730

13) 한국경제, http://news.hankyung.com/article/2017071802321

14) 한국일보, http://www.hankookilbo.com/v/06a91812d758466697f346d47b72f2f5

15) 펜타시큐리티 공식블로그, http://blog.naver.com/pentamkt/221034907968

16) 연합뉴스,
http://www.yonhapnews.co.kr/bulletin/2017/06/22/0200000000AKR20170622192651088.HTML

17) 글로벌 이코노믹,
http://news.g-enews.com/view.php?ud=20170617000200921 09bdce8ae77_1&md=20170723170101_I

18) 한국일보, http://www.hankookilbo.com/v/2be38b627d474f5f8c715aeb447c7403

19) 네이버 블로그, http://blog.naver.com/nms200299/220739398798

20) 네이버 블로그, http://blog.naver.com/barencom/220980446185