보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

해킹의 진원지 '다크웹과 딥웹', 무슨 일이?

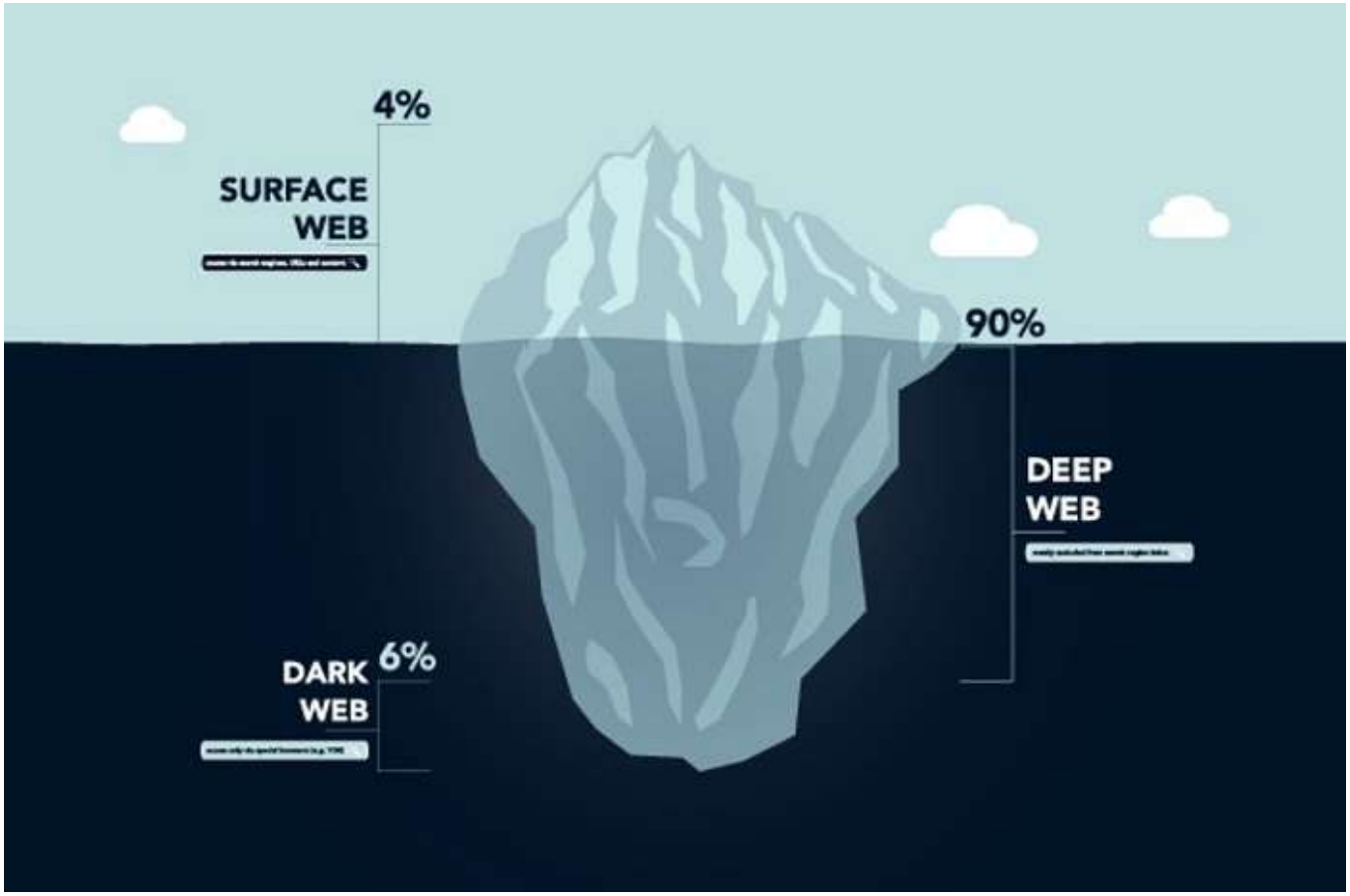
AhnLab 2022-06-03

2022년 1분기에는 미국과 러시아의 신냉전 사태와 러시아의 우크라이나 침공으로 인해 사이버 세계에도 크나큰 일들이 있었다. 가장 활발히 활동했던 콘티 랜섬웨어 그룹의 실체가 밝혀졌고 소스코드도 유출되었다. 또한 악명 높은 레빌 랜섬웨어 그룹 조직원들이 대거 체포되었으며 다수의 언더그라운드 포럼들도 폐쇄되었다. 그럼에도 불구하고 다크웹과 딥웹을 이용한 범죄는 계속되고 있다. 이런 시장이 어떻게 일반 비즈니스와 같은 생태계를 유지할 수 있었을까? 그 이유는 바로 끊임없는 수요와 마켓 사용의 용이성 때문이다.

이번 글에서는 랜섬웨어, 포럼 및 블랙마켓, 그리고 해킹 그룹을 중점으로 다크웹 및 딥웹 동향을 면밀히 알아본다.

다크웹(Dark Web)은 과거 일부 범죄자, 해커 등만 이용하는 공간으로 치부되었다. 그러나 KISA(한국인터넷진흥원)에 따르면 다크웹 접속자만 하루 평균 1만 5천 명에 달하고 있는 것으로 나타났다.

우선, 다크웹의 의미는 정확히 무엇일까?



[그림 1] 인터넷 세계의 구조: 표면웹, 딥웹, 그리고 다크웹

다크웹은 딥웹(Deep Web)이라는 용어와 혼용되기도 하지만 의미가 같지는 않다. 딥웹은 검색 엔진이 찾을 수 없는 모든 웹페이지를 의미하며, 전체 인터넷의 96~99%로 추정된다. 다크웹은 의도적으로 숨겨진 딥웹의 하위 집합으로 특정 브라우저를 통해 접속이 가능하다. 다크웹은 전체 웹페이지의 5%에 해당된다.

다크웹은 모두 불법적인 목적으로 사용되는 것은 아니나 주로 랜섬웨어와 해킹 그룹이 악의적인 의도로 이용하곤 한다.

다크웹 & 딥웹 주요이슈 1: 랜섬웨어

랜섬웨어 그룹들은 꾸준히 리브랜딩을 통해 각종 제재를 피하고 있다. 가장 대표적인 예로 ALPHV 랜섬웨어를 들 수 있다. ALPHV 또는 블랙캣(BlackCat)이라고 불리는 랜섬웨어 제작자는 동일인으로 추정된다. 해당 제작자는 레빌(REvil), 다크사이드(DarkSide), 블랙매터(BlackMatter), 메이즈(Maze) 등 여러 랜섬웨어 조직에서 활동한 사람들을 적극적으로 모집해 리브랜딩을 감행했다.

- 리브랜딩 순서: DarkSide → BlackMatter → BlackCat (ALPHV)

[그림 2] ALPHV 랜섬웨어 그룹의 운영 페이지

최근 여러 랜섬웨어 그룹들이 리브랜딩을 시도하고 있는데, 이름이 계속해서 바뀌는 것을 볼 때 이들의 생태계가 보이는 것보다 크지 않다는 견해도 있다.

또 다른 예로 콘티 랜섬웨어가 있다. 콘티 랜섬웨어는 류크(Ryuk) 랜섬웨어의 리브랜드로 알려져 있으며, 지금까지 800개가 넘는 조직이 콘티 랜섬웨어의 공격을 받았을 만큼 매우 활발히 활동하고 있다.

[그림 3] 콘티 랜섬웨어 그룸의 운영 페이지

최근 이들의 대화 내용과 랜섬웨어 암·복호화 소스코드 및 도구들이 유출되기 시작했다. 하지만 콘티 랜섬웨어 그룹은 아직도 활발히 활동하고 있다. RaaS(Ransomware as a Service)가 일반 비즈니스와 비슷한 생태계를 가지고 있어 내부 자료 유출은 운영에 큰 영향을 미치지 않는 것으로 알려졌다.

랜섬웨어 협상을 위한 웹사이트를 별도로 운영하는 랜섬웨어 그룹도 증가하고 있다. 일례로 하이브(Hive) 랜섬웨어 그룹은 피해자 목록이 있는 PR 웹사이트와 협상용 웹사이트를 운영하고 있다.

[그림 4] 하이브 랜섬웨어 그룹의 운영 페이지(좌), 협상 페이지(우)

하이브 랜섬웨어 그룹과 몸값(ransom) 지불에 대한 협상을 위해서는 랜섬노트에 언급된 어니언(onion) 주소와 로그인 계정 정보가 필요하다. 최근 하이브 랜섬웨어는 기본 몸값을 120만 달러에서 200만 달러로 증가시켰으며, 랜섬노트도 일부 변경했다.

별도의 협상 페이지를 운영하는 랜섬웨어 그룹이 있는가 하면, 리눅스와 같은 새로운 환경에서 동작할 수 있도록 변형을 준 랜섬웨어 그룹도 있다. 록빗(LockBit) 랜섬웨어 그룹은 윈도우 환경 외에도 리눅스와 ESXi 환경에서 동작하는 변형을 갖추고 있다.

MD5	V3 진단명
3c9e550d41f3de930e678776a6e018ed	Ransomware/Linux.Generic.260872
9661c01af31a41caef2ccd3b6be06e60	Ransomware/Linux.Generic.259496
18a352d33c8c01b6a196adce176c5a96	Ransomware/Linux.Generic.252680

[표 1] 록빗 랜섬웨어의 리눅스 변형

록빗 랜섬웨어는 콘티 랜섬웨어만큼 활발히 활동했고, 거의 비슷한 수준의 피해자 리스트를 가지고 있다. 2022년 1월 기준 500 곳이 넘었으며 2월 중순경에는 한 번에 14곳, 3월 중순에는 2일 만에 22곳의 새로운 피해자 리스트를 게시하기도 했다.

활발히 활동을 이어온 랜섬웨어 그룹들과는 사뭇 다른 행보를 보인 랜섬웨어 그룹도 있었다. 갑작스럽게 은퇴를 선언하거나 체포된 그룹들이다. 메이즈 랜섬웨어 제작자로 추정되는 인물이 블리핑컴퓨터닷컴 포럼에 메이즈(Maze), 에그레고르(Egregor), 세크멧(Sekhmet)의 마스터 키를 공개했고, 이를 기반으로 보안 업체인 엠시소프트(Emsisoft)사에서 복호화 도구를 제작했다.
- 링크: https://www.emsisoft.com/ransomware-decryption-tools/maze-sekhmet-egregor?__c=1

[그림 5] 엠시소프트의 메이즈/세크멧/에그레고르 복호화 툴

메이즈 랜섬웨어 제작자 또는 블랙마켓 운영자가 은퇴를 하는 이유는 체포나 체포될지 모른다는 두려움 또는 리브랜딩, 재정적인 목표 달성, 건강 문제와 같은 개인적인 이유가 있을 것으로 추정된다.

은퇴를 선언하기 전에 체포된 랜섬웨어 그룹도 있었다. 갠드크랩(GanbCrab) 랜섬웨어로 알려졌으며 레빌(REvil), 소디노키비(Sodinokibi) 등으로 리브랜딩한 랜섬웨어 그룹의 조직원들은 지난 1월에 체포되었다.

그런데 놀랍게도 이들 그룹은 여전히 활동을 이어 나가고 있는 것으로 알려졌다. 이에 체포된 인물들은 펜 테스터(pentesters) 또는 제휴사이며, 핵심 인력이 체포된 이후에도 이들 그룹은 새로운 브랜드로 활동 중이라는 소문이 돌고 있다.

2021년에 체포된 레빌(REvil) 랜섬웨어 협력자에 관한 타임라인은 [표 2]와 같다.

2021년	국가 및 체포 인원
2월, 4월, 10월	한국에서 3명의 REvil 및 GandCrab 협력자 체포
11월	루마니아 콘스탄차에서 2명의 REvil 협력자 체포
11월	쿠웨이트에서 1명의 GandCrab 협력자 체포

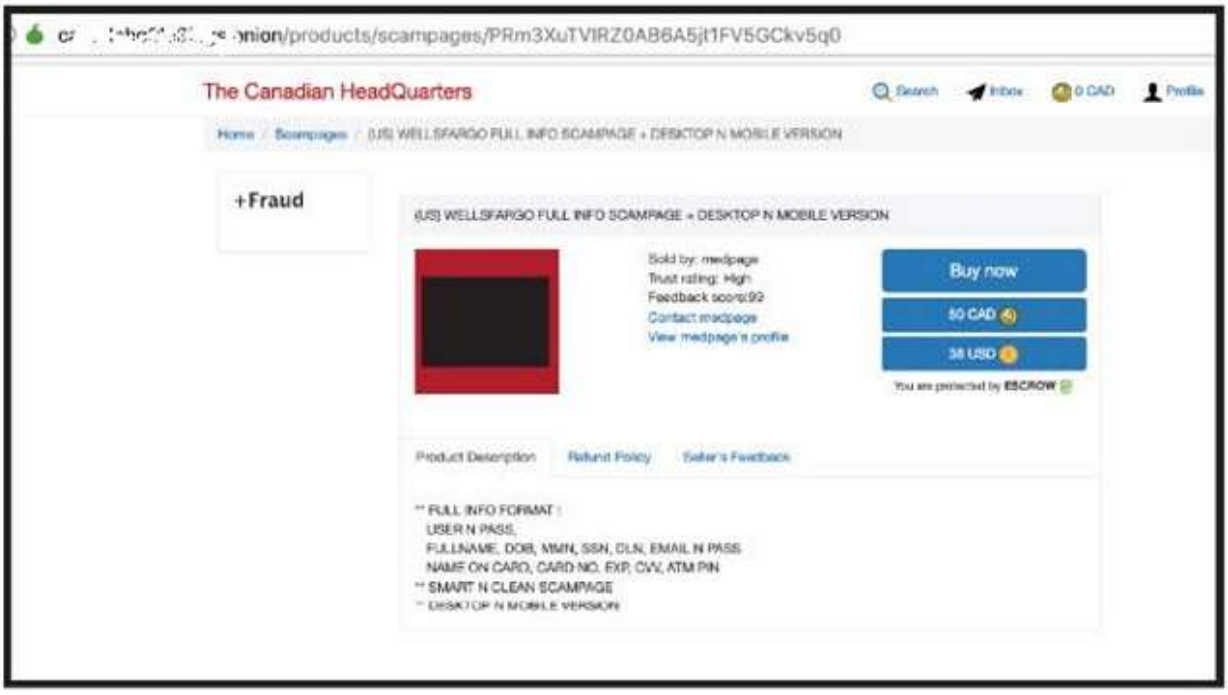
[표 2] 2021년 체포된 레빌 랜섬웨어 협력자 타임라인

다크웹 & 딥웹 주요이슈 2: 포럼과 블랙마켓

정부기관들이 활발하게 나서며 포럼과 블랙마켓도 많은 변화를 겪었다. 정부기관 또는 법 집행기관에 의해 폐쇄된 곳도 있었으며, 자발적 은퇴 또는 출구 사기(Exit Scamming)를 감행한 곳도 있었다.

1. CanadianHQ, Monopoly Market 등 블랙마켓 폐쇄

2018년부터 운영되었던 Canadian HeadQuarters(CanadianHQ)가 캐나다 정부에 의해서 폐쇄되었다. CanadianHQ이라고도 불리는 Canadian HeadQuarters는 제법 알려진 다크웹 마켓플레이스 중 하나로 사기, 마약, 스팸 서비스, 피싱 키트, 훔친 자격 증명과 봇넷에 감염된 컴퓨터에 관한 액세스 정보가 거래되었다. 캐나다 정부는 블랙마켓 운영자 4명의 이름과 닉네임을 공개하고 벌금을 부과했다.



Screen shot of a stolen Wells Fargo customer's credit card advertised on the Canadian HeadQuarters site. Image from a Terbium Labs report in 2020

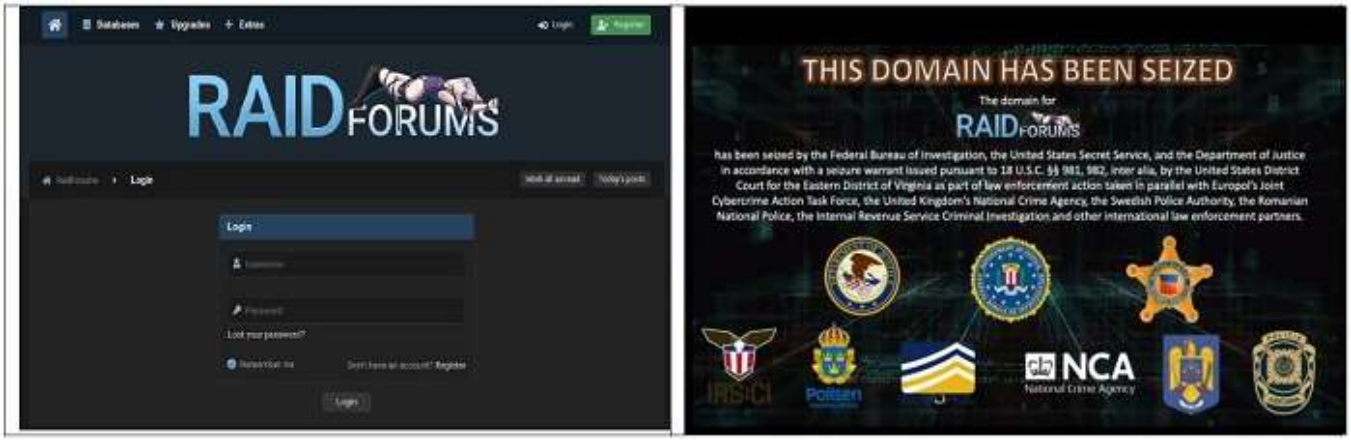
[그림 6] CandianHQ (출처: Terbium Labs Report in 2020)

모노폴리 마켓(Monopoly Market)은 2019년부터 운영되었던 가장 오래된 다크웹 마켓플레이스다. 판매되는 상품은 마약류였으며 폐쇄된 이유는 정확히 알려지지 않았으나 앞서 언급한대로 법 집행기관에 체포될지 모른다는 두려움, 금전적인 목표 도달 등의 이유로 자발적 은퇴를 한 것으로 추정된다.

[그림 7] Monopoly Market

2. 레이드 포럼(Raid Forums) 접속 불가

데이터베이스(DB) 유출 경로로 잘 알려진 레이드 포럼(Raid Forums)이 지난 2월 중순경부터 접속이 되지 않고 있다. 레이드 포럼(Raid Forums)는 세계에서 가장 큰 해킹 포럼 중 하나로 알려졌으며, 500,000명 이상의 사용자를 보유하고 있다.

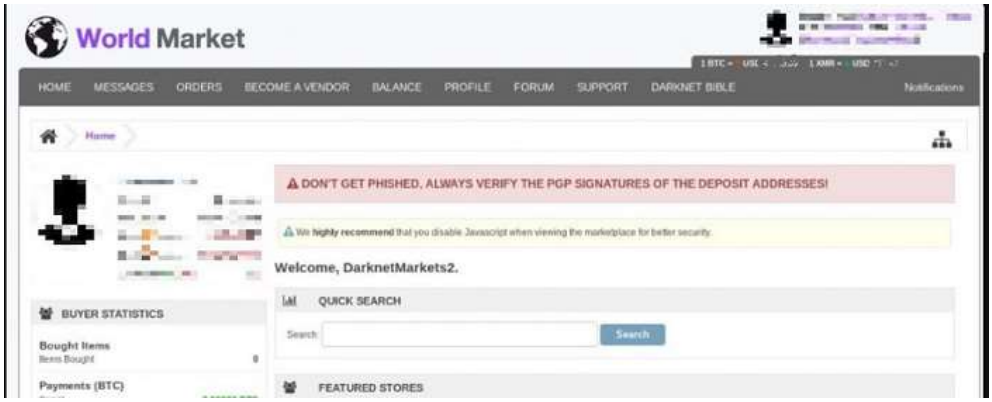


[그림 8] 폐쇄 전 레이드 포럼 로그인 페이지 (좌), 현재 법 집행기관에 의해 도메인이 압류된 모습 (우)

[그림 8]과 같이 미국 법무부가 영국, 스웨덴, 포르투갈, 루마니아의 법 집행 당국이 협력해 포럼을 폐쇄한 것으로 알려졌다. 2022년 4월 12일에 포럼의 설립자이면서 운영자로 확인된 인물을 영국에서 체포됐다. 현재 도메인은 미국 법무부에 의해서 압수된 것으로 보도됐다.

3. 월드 마켓(World Market)의 출구 사기

2020년 11월부터 운영된 월드 마켓(World Market)은 최근 출구 사기(Exit Scamming) 문제가 불거지고 있다. 월드 마켓은 다크웹에 있는 마켓플레이스로, 주문이 이행될 때까지 자금을 보유하는 에스크로(escrow) 서비스를 제공한다. 그런데 최근 이런 서비스에 문제가 생긴 것으로 알려졌다.



[그림 9] 월드 마켓 로그인 후 화면

사용자들이 맡긴 암호화폐가 사라지거나 출금 지연 또는 소액만 인출하는 문제가 발생하고 있는 것으로 알려졌다.

4. SkyFraud 및 Ferum 포럼 폐쇄

비교적 규모가 큰 포럼으로 도난 된 신용 카드 정보를 판매하는(일명 Carding Forum) Sky Fraud와 Ferum 포럼이 폐쇄되었다.

[그림 10] 러시아 연방 내무부 BSTM-K 조직에 의해서 압류된 SkyFraud 메인 페이지

러시아 연방 내무부의 BSTM-K 조직이 수행한 것으로 추정되는 작전으로 해당 포럼 외에도 두 곳이 더 폐쇄됐다. 이들은 SkyFraud 메인 페이지에 러시아어로 '다음은 누가 될 것인가?' 라는 메시지를 남겨 러시아 내에서 사이버 범죄자들에 대한 후속 체포 작전을 암시했다.

다크웹 & 딥웹 주요이슈 3: 해킹 그룹

포럼과 함께 해킹 그룹에 관한 폐쇄 소식도 이어졌다. 2022년 1월에는 미국과 불가리아 정부 당국의 노력으로 넷워크(NetWalker) 랜섬웨어 그룹이 폐쇄되었다. 또한 제휴사로 알려진 캐나다 남성에게는 80개월 징역이 선고됐고, 그가 소유한 719.99 BTC, 15.72 XMR도 압수됐다.

콘티 랜섬웨어 그룹은 우크라이나에 거주하는 보안 연구원에 의해서 유출된 메시지 대화 내용을 통해 그룹과 인물을 특정한 내용이 알려졌다. 알려진 바에 따르면, GOLD BLACKBURN, GOLD ULRICK 두 그룹이 랜섬웨어 그룹의 주축을 이루고 있다.

GOLD BLACKBURN은 재정적 동기가 있는 사이버 범죄 그룹으로 2014년 6월부터 활동하고 있다. 2016년 말부터 2022년 3월까지 트릭봇(TrickBot) 악성코드를 작성 및 운영했으며 BazarLoader, Anchor, ZIoader 및 Buer Loader와 같은 악성코드도 배포하였다.

GOLD ULRICK은 랜섬웨어 공격에만 집중하고 있으며 2018년 중반부터 활동하고 있다. 2018년 8월부터 2021년 초까지 류크 랜섬웨어를 유포했으며 2020년 초부터 리브랜딩을 거쳐 콘티 랜섬웨어를 유포 중에 있다.

전 세계적으로 많은 기업들을 해킹한 랩서스(LAPSUS$) 그룹이 옥타(Okta)를 해킹해 일부 고객 정보가 유출되는 사건도 있었다. 이번 유출 사건은 고객 지원 서드파티 업체인 사익스 엔터프라이즈(Sykes Enterprise)로부터 시작되었다고 밝혀졌다. 고객 지원 회사는 고객 요청을 이행하기 위해 광범위한 액세스 권한을 보유하고 있어 해킹 그룹의 표적이 되는 경우가 많다.

결론

딥웹과 다크웹에서 활동하는 사이버 범죄 조직은 일반 비즈니스와 같은 생태계를 가지고 있다. 이러한 비지니스가 지속되는 두 가지 이유는 바로 수요의 요구와 마켓 사용의 용이성 때문이다.

다크웹 마켓은 구매자와 판매자가 물리적으로 떨어져도 비즈니스가 가능하다. 랜섬웨어는 RaaS (Ransomware as a Service) 그리고 악성코드는 MaaS(Malware as a Service)를 통해서 말이다. 구매자와 판매자를 연결하는 중앙 집중식 서비스를 제공하며, 사용자 등급 제도, 주문이 이행 때까지 자금을 보유하는 에스크로(escrow) 서비스도 갖추고 있다. 사용의 용이성 외에도 높은 수익성 때문에 딥웹과 다크웹을 악의적인 의도로 사용하는 사이버 범죄자들이 계속해서 증가하고 있다.

다크웹과 딥웹 그리고 거기서 활동하는 사이버 범죄자들을 집중 단속하기 위한 글로벌 협력이 계속되고 있는 가운데, 이들의 움직임과 변화를 전 세계적으로 모두 예의주시하고 있다.

AhnLab TI개발팀 정진성 수석