정 보 보 호 학 회 지
제 31 권 제5호, 2021. 10

안보 관점에서의 OSINT와 SOCMINT 조사 분석업무의 한계와 극복 방안을 위한 요구사항 연구

나 가 진*, 이 하 늘**

요 약

인터넷이 발달되고 소셜미디어의 사용이 증가함에 따라 공개정보와 소셜네트워크를 통해 국제 범죄조직, 테러리스트 그룹, 주변 국제 안보환경, 사이버 범죄에 대한 정보 분석의 요구가 늘어나고 있다. 하지만 아직 국내에서 OSINT와 SOCMINT 활동에 대한 공개된 정보가 많지 않아 이에 대한 연구가 많지 않다. 저자는 OSINT와 SOCMINT 조사 분석을 실제 수행하면서 알게 된 문제점과 이를 극복하는 방안을 제시하고자 한다. 다만 Intelligence 업무의 특성상 정보 보안이 매우 중요하여 구체적인 내용에 대해서 제시하기 보다는 업무에서 발생되는 문제를 보편화하여 작성하였다.

Ⅰ. 서 론

최근 디지털 수단의 다양화로 인해 오프라인보다 온라인에서의 데이터가 급격하게 증가하고 있다. 또한 오프라인 활동의 대부분이 다양한 형태의 온라인 데이터로 변환되고 있다. 1980년대까지 군대나 정보기관에서 정·첩보 활동의 주요 활동은 적의 메일을 읽거나 휴대전화, 컴퓨터를 획득하여 분석을 수행하는 것이었다. 하지만 흥미롭고 유용한 정보가 신문이나 공개적인 데이터베이스와 같은 형태로 존재하고 이를 통해 의미 있는 정보를 획득할 수 있음을 알게 되면서 OSINT가 본격적으로 시작되었다.

OSINT(Open Source Intelligence)는 공개된 정보를 사용하여 의사 결정에 필요한 데이터를 획득하고 정보를 처리하는 일련의 활동을 말한다. 전 세계의 모든 활동이 온라인을 기반으로 일어나고 있고 거의 모든 오프라인 활동 또한 온라인의 다양한 매체를 통해 기록된다. 관련 데이터의 증가 및 빅 데이터, 머신러닝, 데이터 과학의 발달로 OSINT를 통해 획득할 수 있는 정보의 양과 질은 빠르게 증가하고 있다.

그러나 데이터 수집과 관련된 다양한 활동에 제약을 줄 수 있는 개인정보 보호 및 데이터 수집 관련 법규가 새롭게 만들어지거나 증가하고 있는 추세이고, 다양한 지정학적 이해관계로 인해 정보를 수집하는 활동이 국가 간의 문제로 커질 수 있다. OSINT를 수행하면서 접근하게 되는 다크웹이나 불법적인 정보 또한 OSINT를 효과적으로 수행하는 데 있어서 많은 어려움을 주고 있다.

이에 OSINT의 효과적인 수행을 위해 현재 OSINT 수행과 관련된 문제점에 대해 알아보고 이를 해결하기 위한 방안에 대해 살펴보기로 한다.

Ⅱ. OSINT 주요 업무

OSINT를 수행하는 데에는 다양한 활동이 포함될 수 있고, 이 활동을 지원하기 위한 많은 OSINT 도구가 개발되었다. 대부분의 도구가 한 가지 이상의 기능을 지원하지만, 주로 하나의 기능에 특화되어 있는 경우가 많다. OSINT 도구의 주요 기능들은 세 가지 정도로 분류할 수 있으며, 이는 곧 해당 기능들이 OSINT 활동의 주요 업무를 나타낸다고 할 수 있다. 세 가지 주요 업무는 다음과 같다.

첫째, 공개되어 있는 자산을 발견하는 작업이다. OSINT의 최종 목표가 정·첩보 활동이든 공격에 대한 방어이든지 가장 먼저 수행해야 하는 업무는 정해진 주제에 대한 공개정보를 찾는 것이다. 악의적인 공격자들이 보안 취약점을 수집할 때 수행하는 첫 번째 단

* 쿤텍 주식회사 (수석연구원, gajin@coontec.com)
** 쿤텍 주식회사 (주임연구원, skylife910@coontec.com)

계처럼, 공개되어 있는 관련 자산을 수집하여 잠재적인 공격 표면을 발견하는 것이다. 바로 해당 자산의 취약점이나 침투 테스트를 수행하지 않고, 공격 표면이 될 수 있는 수집중인 자산의 특성을 파악하는 것이다. 이를 패시브(passive) 자산 수집이라고 칭한다. 많은 OSINT 도구들이 다크웹에 접근하여 정보를 수집 및 분석 할 수 있는 기능을 지원함으로써 서피스(surface) 웹 뿐만 아니라 다크웹에서 유통되고 있는 정보에 접근할 수 있도록 한다.

둘째는 소셜 미디어 게시물 또는 밀접하게 연관된 네트워크 정보 등을 통해 특정 조직이나 자산과 관련된 정보를 수집하는 것이다. 소셜 미디어의 급격한 성장과 인기를 감안할 때, 조직 외부에서 조직과 관련된 정보를 찾는 것은 OSINT 활동에서 매우 중요한 부분이다. 실제로 대부분의 마약이나 밀수품과 관련된 정보는 대부분 소셜 미디어를 통해 거래되며, 이 거래를 위한 데이터가 소셜 미디어 상에서 급격하게 증가하고 있다. 또한, 자신의 신분과 IP 주소 등을 은닉해 익명성을 보장해주는 소셜 미디어도 증가하여 불법적인 거래는 큰 폭으로 상승하고 있다. 이는 소셜 미디어의 각 특성을 파악하고 다양한 소셜 미디어의 데이터를 연계하여 거래자 정보나 위치를 파악하고 수사하는 것이 그 어떤 방법보다 더 빠르고 정확할 수 있음을 의미한다.

셋째는 수집한 정보를 실행 가능한 형태로 만드는 것이다. OSINT 업무를 위해 사용하는 일부 도구는 발견된 모든 정보를 유용하고 실행 가능한 인텔리전스로 조합하고 그룹화하는데 도움을 준다. 온라인상의 데이터의 증가로 OSINT를 통해 대량의 데이터를 수집할 수 있으며, 이 모든 데이터를 결합하고 분석하여 가장 심각한 문제나 취약점을 가장 먼저 처리할 수 있도록 우선순위를 정하는 것 또한 OSINT 업무의 가장 중요한 부분 중 하나이다. 공격을 위한 OSINT 수행의 경우, 가장 침입이 쉽고 유용한 정보를 빼낼 수 있는 시스템이나 사람에 대한 정보가 생성되고, 다양한 접근 방안도 제공할 수 있다. 방어를 위한 경우에는 조직 내 가장 취약한 인물이나 시스템을 선별하여 적절한 조치를 취할 수 있다.

Ⅲ. OSINT 수행의 어려움

급격히 증가하는 온라인 데이터와 관련된 기술의 발전으로 OSINT에 대한 관심과 적용 사례가 늘어나고 있다. 하지만 실제로 OSINT 업무를 효과적으로 수행하는 데에는 몇 가지 어려움이 있다.

3.1. 데이터 보안 관련 법규

개인정보 수집 및 관리에 대한 관심이 증가하고, GDPR(일반 개인정보 보호법)과 같은 엄격한 데이터 보안 법률이 등장함에 따라, 데이터 보안에 대한 우려가 증가하고 있다. 이러한 데이터 보안 법률은 데이터 과학자가 결론을 도출하기 위해 데이터를 수집, 처리 및 분석하는 데 사용했던 기존의 방식이 변경되어야 할 수도 있음을 의미한다. 이제 데이터를 수집하고 분석하는 조직과 개인은 수집된 정보의 분석을 수행하기 전에 데이터 주체의 명시적 동의를 고려해야 할 수 있으며, 이점은 다양한 조직에서 주의해야 하는 주요 OSINT 과제 중 하나이다.

3.2. 콘텐츠 필터링 기술

다양한 디지털 수단의 증가로 인해 전 세계의 사용자는 비용을 들이지 않고 자유롭게 자신의 의견이나 관련 정보를 온라인에 올릴 수 있다. 그러나 이는 데이터의 양도 급격하게 증가했음을 의미한다. OSINT에서 가장 가치 있는 인텔리전스 결과를 얻기 위해서는 고품질의 데이터가 필요하며, 이는 조직이 고품질의 데이터를 얻기 위해 다양한 콘텐츠에 대한 효과적인 필터를 적용해야 함을 의미한다. 많은 조직이 데이터 과학자의 여러 기술과 알고리즘을 통해 대량의 데이터에서 유용한 정보를 필터링하기 위해 노력하고 있다. 이는 빅 데이터, 머신러닝 및 인공 지능 등과 같이 최신의 기술과 결합하여 발전하고 있는 추세지만 일차적인 필터링 기준이나 알고리즘이 매우 중요한 영향을 미칠 수 있기 때문에 수행하고 있는 OSINT의 주제나 목적에 맞는 필터링 기술이 매우 중요하다.

3.3. 다른 인텔리전스와의 구별 및 연계

OSINT는 지정학적 인텔리전스(GEOINT), 측정 및 서명 인텔리전스(MASINT), 휴먼 인텔리전스(HUMINT), 소셜 인텔리전스(SOCMINT), 신호 인텔리전스(SIGINT)와 같은 다양한 인텔리전스 기술의 조

합이다. OSINT를 구성하는 인텔리전스의 공통된 특성으로 인해 OSINT의 작업 유형을 분류하기가 쉽지 않다. 예를 들어, 소셜 미디어 분석에서 수집한 정보는 기본적으로 HUMINT에 속해야 하지만 인터넷에서 공개적으로 사용 가능하기 때문에 SOCMINT에도 속한다. 이러한 중복적인 특성 때문에 카테고리를 분류하여 작업을 하는 경우에 데이터의 중복 및 투입해야 하는 리소스에 대한 효율적인 관리가 쉽지 않다.

다양한 OSINT 도구가 관련 데이터를 자동으로 수집하거나 분석해주는 것과는 별개로, 인력에 의한 데이터 분석과 특정 데이터에 대한 추가적인 검색 작업이 필수적이다. 따라서 어떤 카테고리로 얼마만큼의 인력을 투입하느냐는 OSINT 전체의 효율적인 수행에 있어 매우 중요한 요소가 될 수 있다.

또한 소셜 인텔리전스(SOCMINT)와 지정학적 인텔리전스(GEOINT)를 통해 수집한 데이터를 연계하고 분석해야 의미 있는 정보를 생성할 수 있다. 소셜 미디어에서의 모니터링 대상의 특정 행동이 지정학적 위치나 이해관계에 따라 다양하게 해석될 수 있으며, 이는 OSINT 만이 할 수 있는 매우 중요한 기능이다. 따라서 여러 인텔리전스와의 효과적인 구분 및 연계는 OSINT 수행 조직이 해결해야 하는 중요한 과제 중 하나이다.

3.4. 지정학적 갈등

OSINT는 국가의 방위 활동과 관련되어 사용되는 경우, 전 세계에 걸친 데이터 모니터링이 수반되어야 하므로 몇 가지 정치적인 문제를 일으킬 수 있다. 예를 들어, CIA, 인터폴과 같은 정부 기관이 잠재적인 테러 위협을 추적하고 중지하는데 있어서 데이터 모니터링은 매우 유용하다. 그러나 동시에 이러한 방첩 활동은 국경을 초월한 데이터 모니터링을 포함하기 때문에 지정학적 관심의 대상이 될 수밖에 없다. 실제로 국방과 관련된 조직에서는 OSINT에 대한 업무 수행 시, 이러한 잠재적인 갈등 상황의 가능성 때문에 상당히 많은 제약사항이 있고, 이는 OSINT 수행의 결과에 한계가 있을 수밖에 없음을 의미한다. 민간 기관과의 협력을 통해 이 부분을 해결한다 하더라도, 보안 준수 사항 점검 및 국가 기밀사항에 대한 접근이 제한될 수밖에 없다는 점에서 이 또한 한계가 있을 수밖에 없다.

이러한 부분은 OSINT 기술에서 방위 활동에 관한 한 극복하기 어려운 부분이며, 정부 기관은 이러한 문제를 해결하기 위해 국가 간 관계 개선이나 부분적인 협력 방안을 모색해야 한다.

3.5. 합법과 불법

OSINT 기술은 특정 시스템이나 자산에 대해 종종 악의적인 해커가 불법적인 공격을 시작하기 전에 정찰 방법의 하나로 사용하지만, 대부분의 경우 OSINT 업무와 관련된 도구와 기술 자체는 완벽하게 합법이다. 정부 기관조차 OSINT 기술을 사용하여 자체 사이버 보안 방어의 결점을 찾아내는 것이 좋다.

그러나 이러한 OSINT 수행 활동 중 수집하게 되는 정보나 주체를 따라가게 되면, 합법과 불법의 경계에 매우 쉽고 자주 접근이 가능하다. 예를 들어, 다크웹의 공개된 영역에 접근하는 것은 불법이 아니며, 조직의 데이터가 침해되거나 도난당해 다크웹 상에서 불법적으로 거래되고 있는지 확인하려는 경우, 다크웹으로의 접근은 매우 중요하다. 하지만 연구나 확인 활동의 일부여도, 도난당한 데이터를 구매하거나 특정 기관을 사칭하여 도난당한 정보를 빼내려고 해서는 안 된다. 그것은 명백하게 불법으로 간주될 수 있다.

일반적으로 이러한 수집 활동에서 어떻게 행동해야 하는지 OSINT 활동을 하는 주체에게 지침을 제시하고 관련 법률을 위반하지 않도록 하는 것은 조직에게 매우 중요하다. OSINT 수행 중 불법 활동을 하지 않았음을 입증하기 위해 수행하는 모든 작업을 문서화할 수 있도록 절차를 마련하고, 불법 활동에 포함되는 행동을 하지 않도록 사전에 행동 지침 등을 개발하여 배포하는 것이 매우 중요하다.

또한 OSINT 수행을 위한 프레임워크를 개발하여 해당 프레임워크 내에서만 업무를 수행하도록 시스템 차원에서 불법적인 활동을 제한할 수 있다. 이는 개인별로 다르게 이해하고 적용할 수 있는 행동 지침들을 프레임워크나 프로세스에 반영하여 불법적인 행동의 원천을 차단할 수 있는 효과적인 방법이 될 것이다.

Ⅳ. OSINT &SOCMIN 체계 구축 프레임워크

OSINT는 급격하게 증가하는 디지털 데이터를 기반으로 활발하게 연구되고 있는 여러 기술과 함께 작동할 수 있는 유연성으로 인해 지금까지의 그 어떤 기술

보다 더 정교한 기술로 간주되고 있다.

조직은 데이터를 쉽게 분석하고 보다 정확한 결론을 도출할 수 있도록 관련된 데이터를 수집하여 데이터베이스를 생성할 수 있다. 인공지능, 머신 러닝 및 빅 데이터 분석과 같은 기술의 급속한 발전은 생성된 데이터베이스에 대해 여러 알고리즘을 적용하여 매우 정확한 정보와 결론을 도출할 수 있다. 이렇게 여러 기술의 발달은 이전의 HUMINT 위주의 OSINT 기술을 몇 단계 위로 끌어올렸다.

하지만 3장에서 살펴본 것처럼 현재 OSINT를 수행하는 데에는 몇 가지 어려움이 있다. 이는 단순히 데이터 수집과 관련된 법률이 증가하여 데이터를 수집하는 방법을 변경시켜야 한다는 것뿐만 아니라, 다양한 인텔리전스와의 연계, 콘텐츠를 수집하고 다루는 기술, 합법적으로 OSINT를 수행하기 위한 다양한 지침들을 준비해야 함을 나타낸다.

이렇게 OSINT 수행 시 다양한 문제점이 발생할 수 있고, 이에 효과적으로 대응하고 OSINT 자체의 활동도 효율적으로 수행하려면 전체 OSINT 활동을 관통하는 업무 체계와 가이드라인이 필요하다.

4.1. 국제 연계 필요

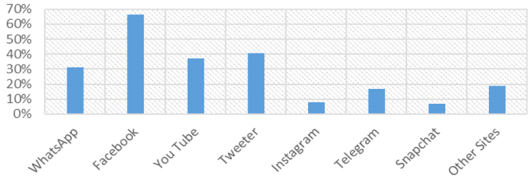
4.1.1. 정보 동맹의 필요성

글로벌 공개 정보를 기반으로 하는 또는 소셜 네트워스를 기반으로 하는 인텔리전스 활동은 매우 포괄적이고 넓다. 언어와 지역, 문화적 특성이 넘나들기 때문에 사회정보를 기반으로 분석할 수 있는 역량이 필요로 하다. 이것은 매우 포괄적인 역량 개발을 요구하기 때문에 한 국가와 사회가 모든 것을 하기에는 많은 어려움이 있다.

Five Eyes는 영국, 미국, 캐나다, 호주 및 뉴질랜드가 연합하는 세계에서 가장 완전하고 포괄적인 정보 동맹중 하나이다. Five Eyes(FVEY)는 세계에서 가장 중요한 정보 동맹으로 알려져 있고, 그것의 기원은 2차 세계 대전의 영국과 미국 사이에 중요한 정보를 공유하여 양국이 긴밀한 전쟁 노력을 강화할 수 있도록 해야 할 필요성으로 거슬러 올라간다.

그 시작은 2차 세계 대전 이후 1946년 3월 5일 UKUSA 협정으로 알려진 신호 정보 협력을 위한 다자간 협정(SIGINT)을 통해 공식적으로 설립되었다. 처음에는 영국과 미국만 협력했지만, 1948년에는 캐나다와 1956년에는 호주와 뉴질랜드도 포함하도록 확장되었다. 일반인이 접근할 수 있는 문서는 거의 없지만 공식적으로 1946년 비밀 해제된 조약의 내용에 따르면 트래픽 수집 및 분석, 통신 문서 및 장비 획득, 암호 분석, 암호 해독 및 번역, 통신 조직, 관행, 절차 및 장비에 관한 정보 등의 작업에 대하여 포함 된 것으로 나타난다. 정보동맹의 범위가 매우 넓은 것을 알 수 있다. 또한 동맹의 각 구성원은 세계의 특정 지역에 대한 정보 수집 및 분석을 담당하는 것으로 알려져 있다. 영국은 유럽, 러시아 서부, 중동 및 홍콩을 수집한다. 미국은 중동과 중국, 러시아, 아프리카 및 카리브해 지역도 수집한다. 호주는 남아시아와 동아시아를 담당하고 뉴질랜드는 남태평양과 동남아시아를 담당한다. 캐나다는 러시아와 중국의 내부와 라틴 아메리카의 일부를 담당한다. 이러한 구분에도 불구하고 FVEY는 주로 공동 작업하며 최종 결과물은 일반적으로 둘 이상의 구성원의 결과이다. 정보 분석의 결과로서 신뢰성과 효율성을 높이기 위해 서로 간 협력하는 것은 필수적인 부분이다. 2001년 9.11 테러 이후 테러리스트 조직은 Five Eyes의 정보 분석 범위에 속한다. 테러단체와 범죄 집단은 웹에서 페이스북, 트위터 등으로 빠르게 전화하여 적극적으로 활용하고 있다.

테러리스트 그룹은 주로 선전(Propaganda)과 모집에 소셜미디어를 활용한다. SNS에 테러단체의 목적과



〔그림 1〕 테러시스트 그룹의 활동 분표 이미지

〔표 1〕 테러리스트 그룹이 활동하는 소셜 미디어 분포

Item	Value
왓츠앱	31%
페이스북	66.4%
유튜브	37.2%
트위터	40.7%
인스타그램	8%
전보	16.8%
스냅챗	7.1%

사상을 설명하는 글, 이미지, 영상 등의 형태로 선전하고 소셜 네트워킹 사이트를 사용하여 관계를 구축하고 동정적인 청중의 지원을 구하고 비공개 채팅을 통해 모집한다.

우리는 공개 정보에서 특히 언어적인 특성과 글로벌 정보력을 확보하는 데 어려움이 있다. 정보 동맹과 연계를 통한 협력이 필요한 이유이다. 또한 국내 사이버 범죄도 해외 조직과 연계 그리고 비트코인 등으로 국경의 경계선을 넘어서고 있어서 해외 인터폴 등과 협력이 필요로 하다. 공격자와 사이버 범죄자, 테러리스트 등은 국가의 경계선이 없이 활동한다. 정보동맹을 통해서만이 이러한 한계를 극복하여 대응이 가능할 것이다.

4.2. 추적 보호 시스템

오픈 소스 정보를 수집하는데 있어서 익명성을 유지하는 것은 매우 중요하다. 하지만 다양한 정보 수집자를 위한 추적 기술과, 보안 시스템 등으로 완전한 온라인에서의 익명성 개념을 달성하는 것은 매우 어려운 과제이다.

완전한 온라인 익명이 되려면 일련의 도구와 기술, 전술적인 방법을 사용하여 가짜 디지털 신원을 생성하고, 인터넷 액세스에 사용하는 하드웨어 및 연결 유형을 익명성을 유지할 수 있는 VPN, 보안 브라우저, 추적기 또는 역추적기로 부터 보호되는 보안 네트워크, 내부 네트워크와 완전히 분리되어 있는(물리적, 논리적, 지리적) 네트워크를 통해 추적으로부터 숨겨야 한다. 이것은 별도의 네트워크와 깊이 있는 기만 기술이 병행 되어야 한다.

국가 안보 또는 해외 스파이와 관련된 사건은 이러한 수준의 익명성이 요구되며 일반적으로 수집 활동을 은폐하는 방법을 잘 알고 있어야 하며, 적절한 수준까지 익명을 유지해야 우리가 그들에 대한 정보를 찾으려고 한다는 사실 자체를 알 수 없거나 최소한 논쟁을 일으킬 증거로서의 식별이 불가능 하다.

사용되는 온라인 추적기술은 다양한 웹사이트에서 인터넷 사용자의 인터넷 검색 기록, 온라인에서 행동(클릭, SNS에서의 행위)를 기록하는 프로세스로 정의될 수 있다. 검색 기록을 대상 사용자에게 연결하기 위해 식별자를 사용하여 각 온라인 사용자를 추적할 수 있다. 이 식별자는 연결된 수백만 명의 사용자 중에서 특정 사용자 시스템을 구별할 수 있다는 점에서 사람의 지문과 유사하다.

대표적인 것은 IP 주소 추적이다. 모바일이든 컴퓨터든 IP 주소 없이는 인터넷에 액세스할 수 없다. IP 주소는 인터넷 연결 시 장치를 식별하는 고유 식별자이므로 온라인 추적기의 첫 번째 대상이 된다. 고정 IP 주소는 ISP(인터넷 서비스 공급자)가 할당한 주소이며 시간이 지나도 변경되지 않는다. 동적 IP 주소는 인터넷에 연결할 때마다 ISP에서 동적으로 할당한다. VPN 및 TOR 네트워크와 같은 익명 네트워크와 같은 다양한 기술을 사용하여 온라인에 접속할 때 IP 주소가 스푸핑될 수 있다.

두 번째로 쿠키 추적이다. 쿠키는 온라인 사용자를 추적하는 가장 일반적인 기술이며, 쿠키는 사용자가 특정 웹사이트를 방문할 때 생성되는 작은 텍스트 파일이며, 그 안에 포함된 표준 정보에는 클라이언트 장치를 식별하는 고유 ID, 만료 날짜 및 쿠키 웹 사이트 이름이 포함된다. 쿠키는 동일한 웹 사이트로 다시 돌아올 때 클라이언트 장치를 구별하는 데 사용된다. 웹사이트는 로그인 자격 증명을 저장하고 사용자 온라인 행동을 추적하는 두 가지 목적으로 주로 쿠키를 사용한다.

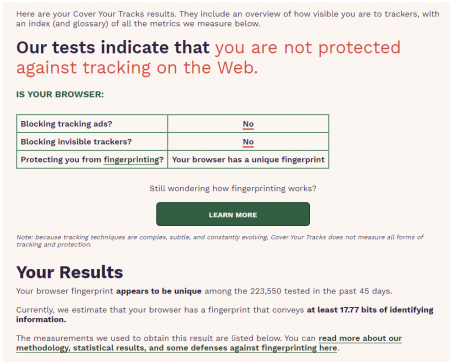
세 번째로 ETag 또는 엔티티 태그는 웹 캐시 유효성 검사를 제공하는 HTTP (Hypertext Transfer Protocol) 메커니즘의 일부이며 클라이언트 측에서 특정 파일이 캐시되는 기간을 제어하기 위한 것이다. 예를들면 ETag는 사용자가 백그라운드에서 음악을 재생하는 웹 사이트를 방문할 때 동일한 웹 리소스를 두 번 로드하지 않도록 웹 브라우저의 성능을 개선 한다. 처음 방문할 때 웹 서버는 오디오 파일과 함께 ETag를 클라이언트 브라우저로 보내고 클라이언트 브라우저는 오디오 파일을 다운로드하고 캐시한다. 사용자가 동일한 웹 사이트를 다시 방문하면 웹 서버는 클라이언트 브라우저에 오디오 파일이 변경되지 않았음을 알린다. 결과적으로 브라우저는 캐시의 로컬 복사본을 사용하여 대역폭을 절약하고 로드 시간을 단축한다.

4.2.1. 디지털 지문

브라우저 지문은 사용자의 시스템을 온라인으로 식별할 수 있는 사용자 시스템 및 브라우저에 대한 기술 정보 집합이다. 이 정보에는 브라우저 유형, 운영 체제

(OS) 버전, 설치된 애드온, 사용자 에이전트, 설치된 글꼴, 언어 설정, 시간대, 화면 크기 등이 포함된다. 디지털 지문에서 수집된 정보는 개별 컴퓨터를 온라인으로 식별하기에 충분하지 않을 수 있다. 그러나 이 정보가 결합되면 각 사용자 컴퓨터에 대한 포괄적인 고유의 식별이 추정 도리 수 있으며 다른 PII(개인 식별 정보)와 결합되면 실제 ID와 연결될 수 있다. 사이버 추적자들은 브라우저의 취약점을 이용하여 시스템의 정보를 탐지하고 추적하는 Exploit을 개발 한다. 이런 경우 추적되고 있는 것을 인지하지 못하는 경우도 있다.

살펴본 바와 같이 매우 중요한, 고부가가치 정보를 수집하기 정보 인텔리전스 활동에서 추적당하지 않는 것은 매우 어려운 일이다. 그렇기 때문에 지속적으로 최신 추적 기법을 탐지하고 회피할 수 있는 기술과 방법을 정보수집체계 시스템에 내장하고 기만 기술 등을 활용하여 추적자들을 역추적 가능하도록 해야 한다.



〔그림 2〕 Panopticlick 사이트 트랙킹

4.3. 지속성

사실 사이버상의 정보를 기반으로 범죄나 테러를 식별하고 분석하여 유효하고 고부가가치의 정보를 생산하는 것은 매우 어려운 일이다. 현재의 OSINT와 SOCMINT를 기반으로 하는 대부분의 프로젝트는 아직 단기적인 형태로 보인다. 물론 이러한 부분의 정보 접근은 매우 제한적인 한계가 있다.

고급 인력으로 구축된 인텔리전스 팀이라고 해도 하나의 타겟을 지속적으로 Tracking할 수 없다면 정보의 파편화와 방향성을 정확하게 알 수 없다. 해외의 SOCMINT와 공개정보는 일회성으로 나타는 경우도 많고 데이터가 보존되지 않는 경우도 많다. 그렇기 때문에 특정한 타겟을 오랫동안 지속적으로 누적하여 식별하고 상대의 기만정보에 속지 않는 지속력이 필요로 하다.

Ⅴ. 결 론

앞서 살펴본 사이버위협에 대한 효율 적인 인텔리전스 활동을 위해서는 OSINT와 SOCMINT와 같은 인터넷 정보 인텔리전스 체계 구축이 필요로 하다. 체계를 구축하기 위해서 대외적으로는 글로벌 정보 동맹 또는 연계, 협력이 필요로 하며, 두 번째로는 추적자로부터 보호하기 위한 보안 시스템, 정교한 역추적 방지 시스템, 공격적으로는 추적자를 속이고 역추적하기 위한 기만 시스템이 필요로 하다. 세번째로는 인터넷의 공개된 정보가 변동성이 있기 때문에 이를 지속적으로 모니터링하고 분석할 수 있는 운영적인 환경이 필요로 하다.

Cyber War의 저자이자, 미 정부의 (전)사이버보안 대통령 특별 고문은 이미 사이버 전쟁이 이미 시작되었고 국가들이 사이버 전쟁터를 준비하고 있다고 이야기 한다. 실제 Colonial Pipeline, 이란 핵시설 사이버 공격, 머스크 운송 시스템 사이버 공격 등은 그것이 결코 과장되지 않았음을 이야기 한다.

우리의 안보적인 주변 환경은 사이버 정보세계에서는 이미 작전 중이다. 그러한 증거는 수도 없이 언론에 노출 되고 있다. 우리는 그에 맞는 체계와 프레임워크를 기반으로 사이버 OSINT, SOCMINT 인텔리전스 체계를 구축하고 운영해야 한다.

참 고 문 헌

[1] 마이클 바젤 저, 최윤석 역 , “공개 정보 수집 기법”,2017.

[2] Clive Best, “Challenges in Open Source Intelligence,” 2011 European Intelligence and Security Informatics Conference, Sep 2011.

[3] UK Defense Journal, “The Five Eyes The Intelligence Alliance of the Anglosphere”, Apr 2020.

[4] International Journal of Research, “USING SOCIAL MEDIA WEBSITES TO PROMOTE TERRORISM ISSUES- A STUDY OF SITE USERS’ SAMPLE, May 2020.

〈저 자 소 개〉

나 가 진 (Gajin Na)

2002년 2월 : 이화여자대학교 컴퓨터학과 석사 졸업
2004년 2월 : 이화여자대학교 컴퓨터학과 석사 졸업
2020년 12월~현재 : 쿤텍(주) 수석연구원
<관심분야> 정보보호, 사이버 인텔리전스, 빅데이터

이 하 늘 (Neul Lee)

2019년 2월 : 세명대학교 IoT융합시스템학과 학사 졸업
2019년 4월~현재 : 쿤텍(주) 주임연구원
<관심분야> 정보보호, 사이버 인텔리전스