특집 02

사이버 공격자 인프라 추적을 통한 선제적 대응방법

김혁준 (㈜나루씨큐리티)

목 차

1. 서 론

사이버보안의 수준은 연결된 체계의 가장 낮은 수준으로 수렴하며 이는 국방 무기체계의 사이버 보안에도 동일하게 적용된다. 국내 방위사업의 22년 수주액은 약 95조원에 이르고 있으나 최근 발생하고 있는 방산기술 해킹사고는 대한민국의 사이버안보를 위협하고 있다. 최근 서울경찰청은 북한의 공격그룹 “안다리엘”이 국내 방산 업체 등을 상대로 해킹공격을 가해 레이저 대공 무기 등 관련 파일을 탈취하고, 방산 업체, 기술원, 연구소, 대학 제약회사, 금융기관 등을 공격하여 1.2테라바이트에 이르는 분량의 자료를 탈취 하였다는 수사결과를 발표하였고[1], 이는 21년 대우조선해양 및 한국우주산업주식회사를 등 대한민국 주요 방산업체를 대상으로 하는 조직적이고, 지속적인 사이버공격행위의 연속선 상에 있다. 이런 현실을 국방연구기관, 민간업체 및 소요군을 연결하는 국방무기체계 사이버보안 공급망 관점에서 본다면, 적성국의 사이버 공격에 대한 대한민국 무기체계 사이버보안 수준은 매우 취약한 것으로 판단된다.

2. 현 사이버방어 체계의 문제점

사이버보안체계의 문제점은 비단 대한민국에 한정된 것은 아니다. 세계 최고의 사이버보안 수준을 갖춘 것으로 알려진 미국의 사이버사령부 사령관이자, NSA 수장인 키스 알렉산더 장군은 미국 기업은 2012년 기준 매년 2천 5백억 달러의 지적재산권에 가치에 달하는 해킹사고가 발생하고 있으며 약 1,104억 달러에 달하는 사이버범죄 피해가 발생하며 이는 사이버공격으로 역사상 인류 최대의 부의 이동이 발생한 것이라고 말하였으며.[3] 이러한 현실은 결국 21년 5월 미국 백악관은 대통령 행정명령을 통해 위협정보 공유를 저해하는 요소를 제거하고, 연방정부와 클라우드 서비스 공급업체에 대한 제로트러스트 아키텍처 도입을 의무화 하였다. 2003년 미국 보안 엔지니어 클리프 리그 (Cliff Riggs)의 "Network Perimeter Security - Building Defense in-depth"의 출간 이후 지난 20년간 업계의 표준 여겨오던 경계선기반 방어는 진화하는 사이버공격에 대응하기에 적합하지 않다는 것으로 암묵적으로 선언하며 이의 대

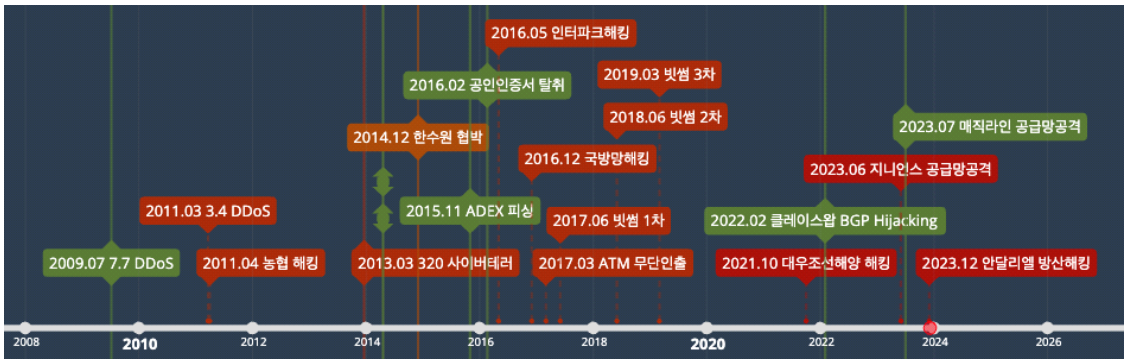
안으로 제로트러스트에게 그 자리를 넘겨주었다. 이는 국내에서도 9방어 5분석이라는 이름으로 공공분야 방어체계의 표준으로 여겨지는 경계선기반 다단계 방어의 개선이 시급하다는 것을 말하고 있다.

3. 공격자와 방어자의 상호작용

방어체계의 변경의 당위는 공격자와 방어자의 끊임없는 상호작용에서 찾을 수 있다. 그림 1은 2009년 이후 대한민국에서 발생한 주요 침해사고 사례를 나타낸다. 2009년은 사이버침해사고 역사상 첫 국가기반공격자의 공격이 발생한 시점으로 대한민국 정부, 금융 및 민간 등 21개 사이트를 대상으로 하는 서비스거부공격이 발생한 시기이다. 당시 공격자는 대한민국의 사이버방어 체계를 우회하기 위해 시간적, 공간적 전술공간의 확장을 통해 공격의 효과를 극대화 하고, 탐지를 우회하였다. 당시 경찰청 사이버테러대응센터의 발표자료에서는 공격자는 전세계 6개국에 9대의 좀비PC 관리서버, 59개국에 416대의 파일정보수집서버 등 일회성 공격을 위해 전세계 500여대 이상의 공격자원을 활용 하였으며 웹하드 프로그램의 업데이트 파일을 변조하는 사이버공격 역사상 첫 소프트웨어 공급망 공격 기법을 활용하여 경계선 내부에 50만대 이상의 봇넷을 구성하였다. 공격자는 이를 통해 대한민국의 인터넷 관문 중심의 경계선기반 방어체계를 무력화 하여 모든 공격 대상 서버를 서비스거부상태에 빠지도록 하였다.

당시 공격자는 소프트웨어 공급망 공격을 통한 내부 자원 감염 전술로 관문중심의 경계선기반 방어체계를 무력화 하였고, 세션기반 공격전술을 차용하여 대역폭소진 방식의 서비스거부공격을 대응체계를 우회하였다. 7.7 DDoS 공격 발생 후 대한민국 정부는 공격에 대한 맞대응으로 국토해양, 국세, 국방, 외교, 경찰 등 5개 분야에 범정부 DDoS 대응체계 사업을 추진하여 HTTP 기반 서비스거부공격에 대한 국가적 방어체계를 수립 하였고 이는 2년후 다시 발생한 3.4 DDoS 공격을 성공적으로 방어하여 관련 공격에 대한 공격표면을 축소 하였고 국가정보보호백서에 따르면 7.7 DDoS 공격 후 만들어진 한국인터넷진흥원의 DDoS 대피소는 이후 발생한 800건 이상의 HTTP 세션기반 공격을 성공적으로 방어하고 있는 것으로 나타났다.

그림 1에서 초록색으로 표시된 공격은 새로운 공격 전술이 처음 사용된 침해사고로, 7.7 DDoS 공격은 소프트웨어기반 공급망 공격 및 공격자원 인프라의 구조적 사용이 처음 확인된 공격으로 이러한 전술은 웹하드 기반의 소프트웨어 공급망 공



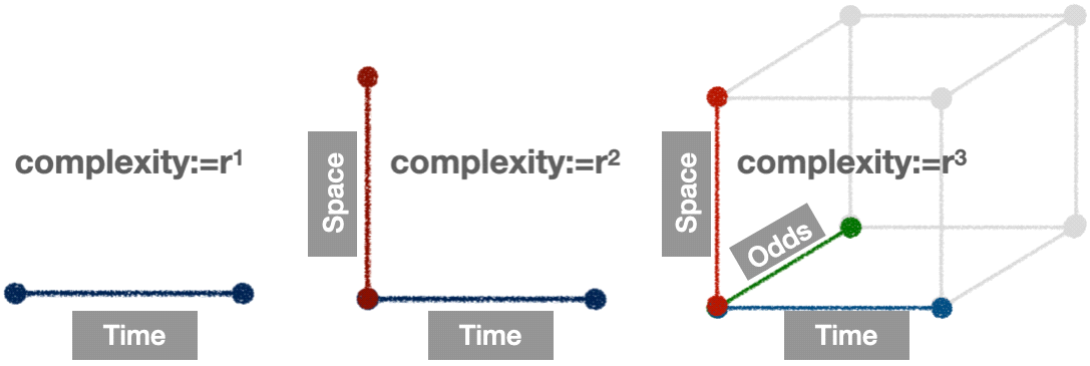
(그림 1) 대한민국에서 발생한 주요 침해사고

격 기법을 재 활용한 2011년 3.4 DDoS 공격, 정보보호 소프트웨어에 대한 공급망 공격으로 방송, 금융 등 6개사 4만여대의 컴퓨터에 장애를 유발하였고, 이는 2016년 다시 백신 소프트웨어에 대한 공급망 공격으로 발생한 국방망 해킹, 암호화폐 거래소 빗썸에 대한 공급망 공격, 및 최근 발생한 매직라인 취약점을 이용한 공급망 공격까지 동일한 전술이 반복적으로 사용 되고 있다.

2015년 11월 ADEX(서울 국제 항공우주 및 방위산업 전시회) 운영본부를 사칭한 스피어피싱은 기존의 기술적 취약점 기반의 사이버공격 침투전술을 넘은 사회공학적 해킹기법을 사용한 사례이다. 이는 3.20 사이버테러이후 강화된 국내 사이버 방어체계를 우회하기 위한 것으로 기존의 공격이 경계선 기반 다단계 방어체계를 관통하는 형태를 가지고 있다면, 이메일은 이용한 공격은 당시 운영되는 모든 방어체계를 우회하여 사용자에게 직접 전달 되는 특징이 있으며, 기술적 방법으로 개선될 수 없는 사회공학적 접근 방법을 사용하였다. 이때 사용된 피싱 공격은 8년간의 시간 동안 구조적인 인프라를 갖추고 사용자의 인증정보를 탈취하기 위해 지속적, 조직적으로 이루어지고 있다.

2022년 2월 발생한 카카오 클레이스왑 BGP Hijacking 공격은, 지역기반 방어체계로는 탐지가 불가능한 인터넷 라우팅 경로에 대한 공격으로 현존하는 모든 사이버방어체계에서 탐지가 불가능한 공격을 수행하여 사이버공격에 새 지평을 열었으며 23년 7월 발생한 매직라인 공급망 공격은 공격목표에 대한 선택적 동작방식을 차용하여 원인규명 방식의 방어체계를 무력화하며 시간적, 공간적 방어공간의 확대에 확률 공간을 더하여 방어자의 대응공간을 기하급수적으로 증가시키는 효과를 발생시켰다.

그림 2는 사이버공격 전술의 변화에 따른 방어공간의 확대를 나타내고 있다. 90년대 낮은 전송속도 및 연구망 중심의 인터넷 환경에서는 발생하는 모든 이벤트를 프린트로 출력하여 이를 육안으로 확인하는 방식의 사이버공격을 탐지가 가능하였으나[쿠크의 에그] 이후 연구망을 넘어 상업적, 개인적 컴퓨터 사용이 일반화 된 환경에서는 폭발적으로 증가한 네트워크 및 컴퓨터 자원의 영향으로 공격표면이 크게 증가 하였으며, 판데믹 이후 일반화된 글로벌 클라우드 서비스의 일반화, 재택근무등의 변화로 기존의 방어체계의 선형적 확장으로는 효과적 대응이 불가능게 되었다.이렇게 확대된 공격 표면은 목표, 시기, 방법 선택에 이니셔티브를 장악하고 있는 공격자에게는 다양한 선택권을 주었으나 인터넷 기반 업무 환경의 확장과 더불어 시간적, 공간적 그리고 확률적 대응 공간의 확대는 국가적 사이버방어전략의 수정을 요구



(그림 2) 공격전술 변화에 따른 방어 공간의 확대

하게 되었다

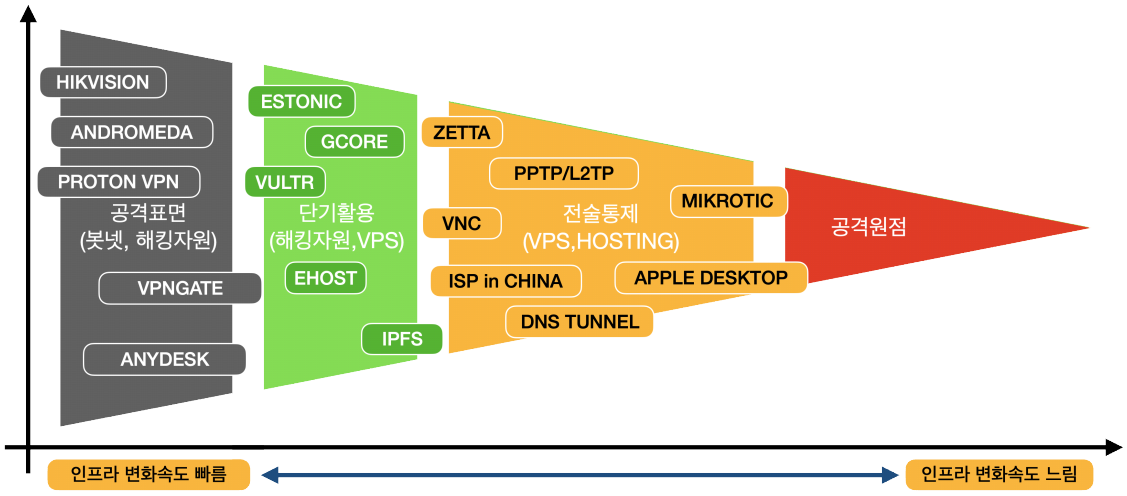
4. 사이버 공격자 인프라 추적

국가기반 사이버 공격그룹은 공격목표에 대한 지속적인 사이버작전 수행을 위해 인터넷 공간에 구조화된 공격 인프라를 구축하고 운영하고 있다. 사이버 작전운영을 위한 공격자원 배치는 원점, 전술통제, 단기활용 및 공격표면으로 구성된다. 이 그림에서 가장 왼쪽에 위치한 공격표면은 가장 휘발성이 높은 자원으로 개별 개체에 대한 추적이 어려우나 관리 체계를 갖추고 있어 관리 단위의 추적이 가능하다. 공격표면은 소유자와 이를 활용하는 그룹이 시점에 따라 상이하여 민감한 정보의 유통 보다는 IAB(Initial Access Broker)와 같이 정보수집, 권한확보 등의 초기 단계에 활용된다.

그림에서 녹색으로 표현된 단기활용자원은 해킹을 통해 확보한 국내 IT자원 및 특정 VPS 사업자 거점 및 국내에 위치한 해외 호스팅 사업자 자원을 활용하여 국내 수사기관의 및 방호체계의 탐지를 회피한다. 피싱 페이지, 악성코드 유포 혹은 최종 정보유출 경유지 구성 등 탐지 및 추적을 회피하기 위한 목적의 작업에 활용된다. 마지막으로 전술통제 지점은 공격자 직접 운영하는 자원으로 국내 수사기관의 국가간 정보공유가 어려운 해외 지역 VPS 호스팅 사업자를 사용하거나 인터넷에 운용되는 특정 제품을 활용한 오버레이 통신망 구성/통제 등에 활용된다. 열거된 3개의 자원 중 휘발성이 가장 낮은 특성을 보인다.

국가기반 공격그룹은 알려지지 않은 공격기법을 활용하여 공격대상 네트워크에 침투하여 정보탈취, 시스템파괴 등의 작업을 수행하지만 전통적 정보보호 방어체계로 이를 탐지하기 위해서는 지속적인 데이터 수집, 분석 등의 작업이 소요되며 또한 방어환경에 따라 지속적으로 변화하는 공격자의 전술(TTPs)로 대부분의 공격은 공격자의 침투목적이 발생한 이후 탐지되어 왔다.

국가기반 사이버 공격은 조직적 협업을 통해 이루어 지기에 이를 위해 인터넷 구간에 사이버공격 인프라를 구축하고 빠르게 변화하는 공격표면 정보만을 노출시키는 방법으로 방어체계의 탐지를 회피해 왔다. 그러나 수년간의 작업을 통해 구축된 공격 인프라는 공격원점에 가까워 질수록 그 변화 속도가 느려지는 특성이 있으며, 공격 원점



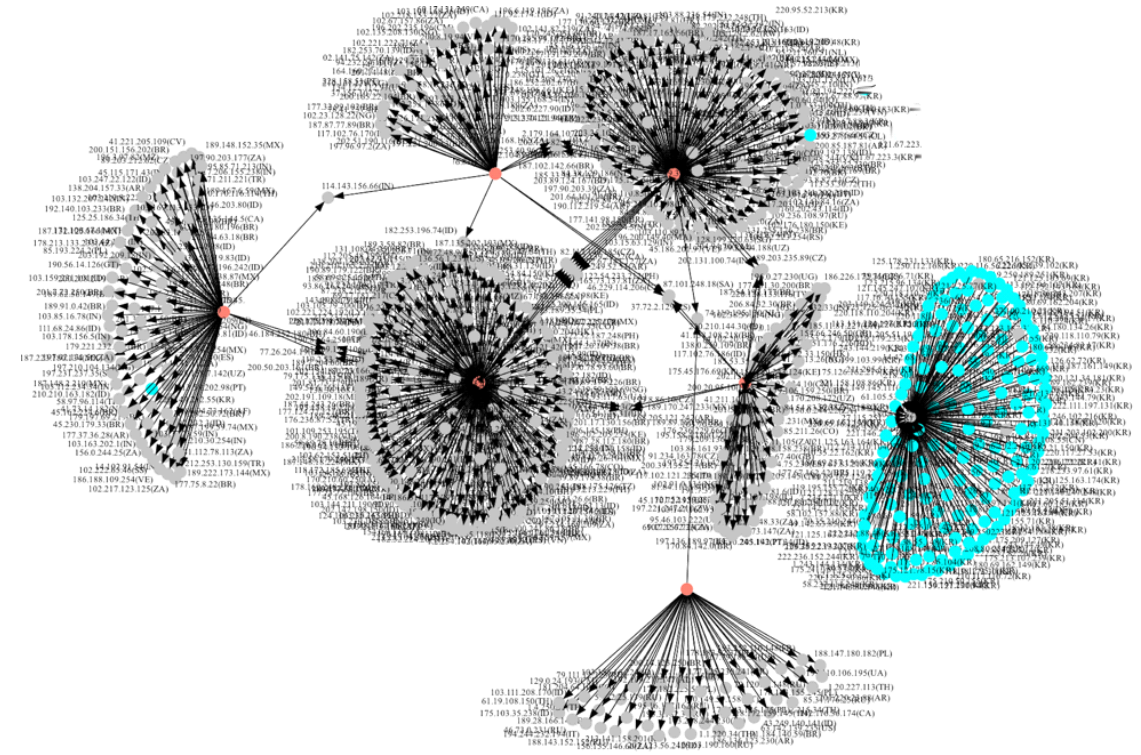
(그림 3) 공격자 인프라 구조도

에 가까운 공격 인프라의 모니터링을 통해 공격자가 목적을 달성하기 전 이를 탐지하고 대응할 수 있다.

그림 4는 인터넷서비스제공자(ISP) 수준에서 수집된 네트워크 플로우 데이터 분석을 통해 공격 원점(그림에서 적색으로 표시)에서 타깃 네트워크(그림에서 청색으로 표현) 까지의 연결도를 구성한 것으로 그림에 표시된 각각의 점은 연결지점의 공개 IP를 나타내며, 각 노드를 연결하는 선은 두 점 사이에 통신사실이 발생한 것을 나타낸다.

통신 플로우 기반의 연결도는 특정 공격 그룹이 인터넷 공간에 분산되어 있는 취약한 라우터에 불법적으로 획득된 권한을 이용해 구축한 오버레이 네트워크로 공격 원점에서 타깃 네트워크까지 구성된 경로를 보여주고 있다. 국가 기반 공격자는 임의의 시점에 공격 목적을 달성하기 위해 다수의 국내 기업/기관 네트워크를 점유하고 특정 시점 발생한 필요에 따라 실질적인 공격을 수행하는 것으로 분석된다. 따라서 이러한 공격 그룹의 사이버 공격 인프라를 모니터링하는 것으로 실질적인 피해가 발생하기 전 선제적인 대응이 가능할 것이다.

이러한 접근방법을 통해 현장에서 실질적인 대응이 가능하도록 하기 위해서는 먼저 인터넷구간에서 발생하는 통신사실에 대한 지속적인 수집, 사고분석을 통해 획득된 기초자료를 통해 구성된 공격자 인프라를 식별하기 위한 분석작업, 분석된 결과의 처리 및 시각화 과정이 지속적으로 이루어져야 하며 이를 통해 축적된 데이터를 기반으로 공격자 인프라 정보를 기반으로 하는 공격그룹 프로파일링 작업이 이루어 진다면 현재 운영되는 사이버 방어체계의 한계를 넘어 대한민국을 목표로



(그림 4) 통신 플로우 분석을 통한 공격자 인프라 추적

하는 국가기반 공격자의 인프라에 대한 선제적 대응이 이루어 질 수 있을 것이다.

5. 결 론

대한민국의 사이버 전쟁의 시작은 2009년 7월 7일 북한이 수행한 대규모 분산서비스거부공격에서 시작되었다고 볼 수 있으며 지난 13년 동안 국가기반 사이버 공격자는 대한민국에 대한 사이버 공격을 수행하기 위해 대한민국 내부는 물론 전 세계 각지에 매우 조직적으로 구성된 사이버 공격 인프라를 운영하고 있는 것으로 나타났다. 공격의 수준이 변화하면 이에 대응하는 방어 체계의 수준 역시 변화하여야 한다. 공격자는 방어 시야 밖에서 긴 준비 기간을 거쳐 침투 준비를 한 후 모든 것이 준비된 후 추적 가능한 모든 증거자료를 삭제한 후 공격의 마지막 단계인 목적 수행을 실행하기에 공격 라이프사이클 전 과정에 대한 대응 시야를 확보한다면 방어자는 비로소 공격자에 대한 대응 우위를 확보할 수 있게 된다.

빠르게 변화하는 공격 표면의 효과적 관리를 위해 인터넷 공간에 사이버 공격자들의 협업 도구로 구축된 사이버 공격 인프라는 공격 원점에 가까울수록 쉽게 변화할 수 없게 된다. 이러한 접근 방법을 통해 공격자 움직임과 공격 의도를 예측하고, 구축된 사이버 공격 인프라를 관측하는 것으로 기존의 수동적 대응방식에서 벗어나 선제적 사이버 공격 대응으로의 획기적인 전환이 이루어 질 수 있다

참 고 문 헌

[1] 2023 국가정보보호백서, 2023-06-02, 4283
[2] Riggs, Cliff. Network perimeter security: building defense in-depth. CRC Press, 2003.
[3] Stafford, V. A. "Zero trust architecture." NIST special publication 800 (2020): 207.
[4] https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/
[5] https://www.sedaily.com/NewsView/29YE4DM2W1
[6] https://m.boannews.com/html/detail.html?idx=102043
[7] https://www.donga.com/news/Politics/article/all/20210709/107867900/1

저 자 약 력

김 혁 준

이메일 : joonkim@narusec.com

- 2003년 캐나다 알버타 주립대학교 컴퓨터공학과(학사)
- 2003~2004년 캐나다 알버타 주립대학교 PINTS 센터 연구원
- 2004~2005년 RandomKnowloedg Inc. 연구원
- 2005~2009년 한국인터넷진흥원 침해사고대응센터 연구원
- 2014~현재 정보통신망 침해사고 민관합동조사단 전문가
- 2017~현재 경찰청 사이버범죄 전문가 그룹 위원
- 2020~현재 성균관대학교 법과대학 과학수사과 겸임교수
- 2010~현재 (주)나루씨큐리티 대표이사
- 관심분야 : 사이버 보안, 침해사고대응, 위협 모델링, 인공지능, 빅데이터