국가전략연구위원회 이슈브리핑 10호 (발간일: 2023.09.25.)

중국 사이버 공격 양상 변화와 사이버 안보에의 함의[1)]

김상규 (경기연구원)

1. 문제 제기

2023년 1월 22일, 중국 해킹 조직 '샤오치잉(曉騎營, Cyber Security Team)'은 한국의 교육 관련 사이트 70여 곳을 해킹했다. 곧이어 1월 24일, 텔레그램에 공개 성명을 올려 자신들이 한국 기관의 홈페이지를 공격했다고 밝혔다. 이들은 "우리는 중국 정부를 위해 일하지 않으며 우리 팀은 자유 그룹"이라며 "한국을 훈련장으로 삼아 각 멤버가 한국 공격에 참여하겠다."라고 천명했다. 해킹을 한 이유는 "한국의 일부 스트리밍 스타가 나를 화나게 했다."라는 이유 때문이었다. 이 같은 이슈가 한국 사회에 얼마나 큰 영향을 끼쳤는지 확인하기 이전, 더 중요한 것은 우리가 사건을 인식했는지와 상관없이 사이버 공격이 이제는 일상과 떼려야 뗄 수 없는 일 중의 하나가 되었다는 사실이다. 우리는 현재 사이버 공간에서 해킹 등 사이버 공격을 통한 수많은 정보의 유출과 악영향에 노출되어 있다. SNS 등 개인의 공간을 넘어 기업의 정보 국가 안보 차원에서 직간접적인 피해를 보는 중이다.

그렇다면 사이버 공격은 왜 일어나는 것이며, 그 주체와 대상, 방법은 무엇일까? 상술한 것처럼 공격 대상이 자신을 드러내는 경우를 제외하고 공격자를 정확하게 특정하거나 사전에 예상하기는 힘들다. 하지만, 사이버 공격이 어디에서, 누가 시작했는지, 어떤 방식으로

1) 이 글은 2023년 9월 20일 제4차 국가전략포럼에서 발표된 발표문을 수정보완한 것이다. 미완의 발제문이므로 인용을 불허하오니 양해 바랍니다.

시행했는지 파악할 수 있는 기술적 범위 안에는 있다. 이 때문에 선진 기술력을 가진 국가와 후발 주자로 추격하는 국가, 블랙 해커와 화이트 해커 사이에서 창과 방패의 자웅을 겨루는 수단으로써 사이버 공방전이 벌어지기도 한다. 특히, 현재 미국은 동맹국과의 규합을 통해 민주주의 가치, 규범을 강조하며 중국을 압박하고 있다. 미·중 양국의 갈등이 신냉전으로 명명되기도 하며 진영 간 대결이 사이버 공간에서 무시로 일어난다. 현실 공간에서만큼 국가 간 갈등 상황이 치열하게 이루어진다는 점에서 미·중 양국이 사이버 공간에서 벌이는 행위의 의도와 목적을 정확하게 파악하는 것은 상당히 중요한 국제정치학적 함의가 있다.

한편, 중국은 러시아, 북한과 더불어 가장 많은 사이버 공격을 시행하는 국가로 알려져 있다. 하지만 중국이 어떤 나라를 대상으로, 얼마만큼의 사이버 공격을 시행하는지 정확히 확인하기란 쉽지 않다. 공격의 주체가 중국이라는 명확한 객관적 증거를 확보하기도 어려울 뿐더러 확인하더라도 우회하는 방식으로 이루어진 경우라면 중국 정부가 부정하고 있기에 더욱 그렇다. 다만, 여러 가지 해킹 사례와 해킹 예고 등 드러난 사실에 근거해 추론해야 한다. 기술적으로 추적해 확인한 결과를 분석하면 사이버 공격 주체와 양상, 패턴과 내용을 찾아볼 수 있다. 본 발제문은 미국과의 경쟁 구도 속, 사이버 공간에서 강력한 행위자로 행동하는 중국에 대해 주목한다. 중국이 사이버 공간에서 대외적으로 공격을 수행하는 주요 주체, 방식, 그 양상은 무엇이고 어떻게 변할 것인지에 초점을 둔다. 이를 통해 사이버 안보에 주는 함의를 분석하고 그 시사점을 도출하고자 한다.

2. 사이버 공격의 정의와 형태

사이버 공간에서 다양한 목표를 달성하기 위한 사이버 공격 및 방어 기술들을 통합한 체계를 사이버 무기체계라고 하며 이는 다시 소프트웨어 및 하드웨어 무기체계로 구분할 수 있다.[2] 소프트웨어 무기체계와 사이버 공격기법은 상호 연관되어 있지만, 두 개념에는 차이점이 존재하는데 사이버 공격기법은 사이버 공간에서 시스템, 네트워크, 데이터에 대한 공격이나 침투를 실행하는 데 사용되는 특정한 방법이나 기술로서, WannaCry, NotPetya, Bad Rabbit 등의 랜섬웨어, SQL Injection, Zero-day, APT, DDoS 등이 여기에 해당한다. 이러한 기법들은 사이버 공격을 수행하는 동안 취약점을 이용하거나 시스템 조작에 사용한다.[3] 소프트웨어 무기체계는 다양한 사이버 공격기법뿐만 아니라 공격자의 전략, 인프라, 자원, 지식 등의 개념을 포함한다. 즉, 사이버 공격기법은 소프트웨어 무기체계 내에서 사용되는 도구 또는 기술로, 이러한 기법을 효과적으로 전개하기 위한 전체적 구조와 전략을 의미한다. 구체적인 내용으로는 악성 소프트웨어인 악성코드, 웜, 트로이 목마와 다른 악성 소프트웨어

2) 유도진. "중국 해킹그룹 샤오치잉 사이버 무기체계 대응방안 연구: SQL Injection 및 OSINT 기반 Known Vulnerability 공격." 한국산학기술학회논문지 24.6 (2023).
3) 상동

를 개발 및 배포하여 타깃 시스템에 침투하고 제어하는 데 사용한다. 또한, 감시, 스파이 활동 및 정보수집을 위한 고급 스파이웨어를 개발하여 외부 조직이나 국가의 정보를 획득하는 방법을 활용한다. 더 나아가 중요한 데이터나 시스템을 파괴하거나 변조하는 목적으로 사용할 수 있으며, 대상 시스템의 기능과 사이버 공간의 무력화를 통해 사용 불가능하게 만드는 공격을 수행한다. 특히 기술적인 발전을 이루면서 군사적 차원에서 충돌을 불러일으키는 데 활용이 가능하며 온라인 사이버 전투 플랫폼을 통해 사이버 공격 기술을 관리하고 조정할 수 있다.

하드웨어 무기체계는 하드웨어를 기반으로 전력 인프라 공격인 전자파(Electromagnetic Pulse, EMP), 드론을 이용한 무선 네트워크 공격 등 특정 인프라, 통신 등을 무력화하기 위해 사용하지만, 사전 징후나 식별이 비교적 뚜렷하다.[4] 반면에 소프트웨어 무기체계는 국제적 해킹그룹의 주요 공격수단으로 사용하며, 주요 방식은 하드웨어 무기체계를 이루는 컴퓨터 시스템, 네트워크 인프라, 통신 장비 등 물리적인 하드웨어를 공격하거나 하드웨어 침입을 통해 타깃 시스템 파괴와 제어를 통해 전투 상황에서 상대방의 하드웨어를 무력화하는 데 활용한다. 이처럼 사이버 무기체계는 공격과 방어의 목적으로 사용할 수 있으며, 군사적 충돌, 국가 간 갈등, 정보수집, 경제 스파이 등 영역을 넘나들며 사이버 공간에서 국가 간 경쟁과 안보의 위협을 증대시키고 있다.

3. 중국 사이버 공격의 주요 주체와 방식, 내용의 변화

중국 사이버 공격의 주요 주체와 해킹 조직은 구체적인 특성이나 규모, 임무 등을 정확하게 확인하기는 사실상 어렵다. 하지만 기본적인 방첩 업무를 수행하는 국가기관을 비롯해 국내외 정보기관이 해킹 결과를 분석하거나 사이버 공격 행위에 대한 선전 포고 등을 통해 드러난 사실을 토대로 확인할 수 있다. 중국이 사이버 공격은 물론 스파이 활동을 수행하는 조직 중 하나는 중국 인민해방군 (PLA, People's Liberation Army)이다. 해당 조직은 국가 차원에서의 중요 정보 수집, 군사 기밀 획득, 정치적 영향력 확장, 경제적 이익 추구 등 다양한 목적에 기반해 사이버 공격을 수행한다. 사이버 공격을 통해 중요 정보와 기술을 탈취하고, 미국을 비롯한 기타 국가와의 군사 및 경제적 경쟁에서 이점을 취하려는 데 주안점을 두고 있다. 중국 국가안전부 (MSS, Ministry of State Security) 역시 정보수집과 사이버 활동을 주도하는 주체 중 하나로 외국 정부 기관 기업의 정보를 수집하고 기밀 정보를 획득하기 위해 활동한다. 이외에 중국 정부나 군사 기관과 직접 연관되지 않은 독립적인 해커그룹들도 많이 존재한다. 이들 해커그룹은 자체적인 활동, 해킹 업무 계약에 따른 특정 임무의 수행, 금전적 이득을 얻기 위한 목적에 기초하고 있다.

4) 유도진. "중국 해킹그룹 샤오치잉 사이버 무기체계 대응 방안 연구: SQL Injection 및 OSINT 기반 Known Vulnerability 공격." 한국산학기술학회논문지 24.6 (2023).

그중에서도 APT1 또는 Comment Crew라 불리는 그룹은 중국과 관련이 있는 것으로 알려져 있다. 중국이 주로 행하는 해킹의 방식은 APT라 불리는 지능형지속위협(Advanced Persistent Threat, APT)인데 특정한 피싱 공격을 통해 전자 우편 주소로 악성코드를 발송하고 컴퓨터 점유가 끝나면 수 시간 내에 기업 전체를 불능화시킬 수 있다. APT1(Advanced Persistent Threat는 PLA Unit 61398의 일부로 활동 시기는 2006년부터로 알려져 있다. 이는 중국이 인터넷 및 사이버 과학 기술 분야에서 급속한 성장이 시작하는 시기와 맞물려 있는데 주로 에너지, IT, 통신, 항공 우주, 국방 등의 분야를 공격 대상으로 삼고 기업 비밀 정보, 지적 재산, 정치적 정보 등의 중요 데이터를 탈취하고 정보수집을 한다. 주요 공격 방식은 spear-phishing(표적형 피싱)과 악성코드를 배포하는데 자체 개발한 악성코드와 도구를 사용하여 정보를 수집하되 흔적을 숨긴다. 공격 대상과 지역은 주로 영어권 국가들이며 미국에서 가장 큰 피해를 준 것으로 보고되었다.[5)]

이외에도 메뉴패스팀으로도 불리는 APT10 역시 2006년부터 관리형 IT 서비스 제공업체를 활용해 미국, 유럽과 일본 등 전 세계의 항공 우주 및 통신 기업과 건설과 엔지니어링 기업, 정부 기관을 노리고 공격 활동을 벌였다. 실제로 미국 법무부는 미국, 브라질, 프랑스를 비롯한 12개국에서 안보 기밀, 영업비밀, 지식재산권 등을 유출하기 위해 해킹을 저지른 혐의로 APT10 소속 중국인 해커 2명이 기소했는데, 이들은 IBM, HP 등 민간 기업들을 비롯하여 미국의 해군과 항공우주국(NASA) 제트추진연구소, 미국 에너지부 등의 정부 기관 전산망을 공격했다.[6)]

APT 20은 중국 정부의 정책인 중국제조 2025 나 '일대일로'와 같은 국가대전략의 성공적인 수행을 위해 필요한 산업 기밀 해킹을 통해 정보를 수집하는 데 주요 방식은 오픈소스인 제이보스(JBoss)의 취약한 특정 버전으로 운영하는 네트워크에 침입하거나 스피어 피싱 메일, 휴대용 미디어 장비의 감염, 소프트 웨어 공급망 공격 등의 방식을 사용하고 있다. 중국 해커그룹 Barium(APT41, Winnti)은 중국 정부와 연계된 곳으로 주로 산업 스파이 활동 및 금융 범죄에 관여한 것으로 알려져 있다. 주 공격 수단과 방법은 스피어 피싱, 제로데이 취약점, 무선 툴을 사용하며 주로 게임 회사, 기술 기업, 통신 업체, 정부 기관 등을 대상으로 산업 스파이 활동과 금융 이익 추구를 병행한다.

이외에도 '틱'(Tick)은 주로 한국과 일본의 방위와 관련한 기밀 정보를 탈취할 목적으로 임무를 수행하는 해커집단이다. 주요 사이버 공격 방식은 표적형 공격(TTP)을 사용하여 스피어피싱 이메일을 전송하고, 악성코드를 사용하여 시스템 방비가 허술한 대상을 노려 바이러스를 침투시키는 방법을 활용한다. 2016~2017년 우주항공연구개발기구(JAXA)를 비롯한 연구기관과 대학, 방위·항공기업 등 약 200곳의 정보 탈취를 시도했는데, 일본 경찰은 '틱'이 중국군 61419 부대의 지시를 받으며 2018년 이후 미국과 유럽을 대상으로 활발한 활동으로

5) Mandiant, APT1: Exposing One of China's Cyber Espionage Units, https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf
6) 美, 중국인 해커 2명 기소... 최소 12개국서 해킹 혐의, https://www.munhwa.com/news/view.html?no=2018122101070830129001

벌이는 조직으로 판단했다.[7] 또한, 무스탕 판다(Mustang Panda), 딥 판다(Deep Panda) 같은 조직은 중국 정부의 전략적 목표에 맞춰 미국, 아시아뿐 아니라 러시아 조직을 비롯한 유럽 단체들까지 다양한 분야의 주요 기업을 대상으로 하며 지적 재산 및 민감 데이터 탈취를 주로 하는데, 딥 판다는 정부, 군대, 공공시설, 금융 기관을 대상으로 하는 별도의 국가 후원 사이버 스파이 그룹으로 로그4j 취약점을 악용해 의료 기관에 피해를 주고, 이후 공격 지속성을 유지하기 위해 맞춤형 백도어를 배포하는 형태로 활동한다.[8]

서두에 거론했던 샤오치잉은 한국 내 기관 2천여 개 웹사이트를 대상으로 사이버 공격을 예고하고 개인정보 유출 및 공격 등을 감행한 뒤 해킹포럼 등을 통해 공개한 바 있다. 해킹 대상은 주로 소규모 기관과 기업, 학회 등을 표적으로 선택하는데 그 이유는 중소기업 등 소규모 조직의 경우 보안에 대한 경각심이 부족하고 취약해 공격 성공 확률이 높기 때문이라고 할 수 있다. 또한, 공격에 성공한 후 획득한 관련 정보를 공개하는 것은 피해 기관과 기업에 추가적 부담과 더불어 자신들의 공격이 사회적으로 영향력을 행사한다는 이미지를 심어주기 위한 것으로 보인다. 사이버 공격을 통해 경제적 이익, 정치적 목적, 경제적 이익, 사회적 영향력을 확보하고자 한 것이다.[9] 주로 사용하는 공격 방식은 SQL Injection과 공개 정보를 활용해 취약점을 공략한다.

앞서 살펴본 것처럼 중국의 사이버 공격 주체나 기술적인 것 이외에 내용적인 차원에서 분석해 보면 그 형태가 어느 정도 분류가 가능하다. 초기에는 기술적인 차원에서 여러 가지 방법을 시도 했다면, 기술 축적을 이루고 난 후 자국에 유리한 정보를 수집하기 위한 좀 더 적극적인 형태로 전환했다. 특히, 2018년 이후부터 중국의 사이버 공격 대상과 내용이 아주 명확해진 시기로 볼 수 있다. 미·중 관계가 악화한 이후 중국의 사이버 공격 대상국은 미국의 동맹을 비롯한 우호 관계를 맺는 국가, 그리고 중국에 부정적 태도를 보이는 국가를 대상으로 이루어진 사례가 많이 나타났기 때문이다.

구체적인 사례로는 2020년 호주의 스콧 모리슨 총리가 코로나19 바이러스의 중국 우한 기원설에 대한 조사를 공식적으로 제안하자 양국 관계는 급속도로 악화했는데, 양국이 무역 보복을 하는 과정에서 중국발 해킹 봇이 호주 정부의 인터넷 네트워크를 동시다발적으로 공격하는 사건이 발생했다. 이외에도 양안 관계가 악화하면서 대만에 대한 중국의 사이버 공격은 더욱 강화했는데, 특히 대만은 2024년 선거를 앞두고 중국이 친중 정권 수립을 위해 대만 내부의 혼란을 도모하고 중국의 의도를 이식하고자 사이버 심리전을 벌이고 있는 것으로 보인다. 2023년 5월 30일, 대만 정보기관인 국가안전국(NSB)을 담당하는 국가안전회의(NSC)가 발표한 내용에 따르면, 대만은 매일 500만 회에 달하는 인터넷 공격을 받고 있고

7) "日 연구기관 등 200곳 사이버 공격 연루 혐의 중국인 입건", https://www.yna.co.kr/view/AKR20210420131100073
8) 이란·중국·북한 배후 사이버공격 기승..."보안사고엔 '만약' 없다", https://zdnet.co.kr/view/?no=20230421112257
9) 유도진, 중국 해킹그룹 샤오치잉 사이버 무기체계 대응방안 연구: SQL Injection 및 OSINT 기반 Known Vulnerability 공격, 한국산학기술학회 논문지, 2023, vol. 24, no.6,

대부분은 중국발 사이버 공격이 이루어졌다.[10)]

가장 최근에는 중국 정부가 조직한 '912 특별 프로젝트팀'이 가짜 SNS 계정을 이용해 코로나19 발원지가 중국이라는 주장 등 중국에 불리하거나 남중국해에서 중국의 군비 확장 위험성 경고, 중국의 인권 문제의 심각성 등 중국이 민감해하는 내용과 관련한 의사를 표명한 인사들에게 사이버 공격을 가한 사실이 밝혀졌다. 미국 연방 검사가 중국 공안부 소속 요원 34명을 궐석 기소하면서 제출한 89페이지 분량의 고소장과 진술서에 관련 활동을 상세히 기술했는데 트위터·유튜브 등에 개설한 가짜 계정을 통해 중국 공산당과 정부를 옹호하는 메시지를 적극적으로 전파했는가 하면 이른바 '중국의 적'들을 겨냥해 강도 높게 공격했다는 내용이다.[11)]

이렇듯 중국은 이전보다 더 적극적이고 공세적으로 중국에 반하는 정보에 대해 민감하게 반응하여 공격적인 행태를 보인다. 이 같은 행위는 중국이 자국 내에서 행하는 언론 통제와 내용상의 검열을 국제사회에도 적용하고자 하는 의도를 엿볼 수 있다. 이 같은 상황에서 미국은 '2023 국방부 사이버 전략'을 발표했는데, 주요 내용은 중국의 사이버 위협 사례가 어떤 형태로 일어나고 있는지, 향후 어떤 방향성을 가지게 될 것인지 등을 포함하고 있다. 즉, 미국 기업과 정부 기관 해킹, 기술 탈취를 위한 사이버 스파이 활동, 미국 내정 간섭 시도 등을 대규모로 진행하고 있으며 중국이 미국과 동맹을 상대로 악의적인 사이버 활동을 하는 행위가 광범위하게 만연된 사이버 위협이라고 규정한 것이다.[12)]

미국의 이 같은 위협 인식의 발로는 중국의 사이버 공격이 기술적인 차원에서 이전보다 더 고도화하고 전문화한 그룹들이 주도하며 확장성을 갖기 때문이다. 특히 APT(Advanced Persistent Threat) 그룹은 목표 기관에 대한 정교한 표적 공격을 수행하고 지속해서 침투하는데 이는 다양한 벡터를 결합하여 공격 효과를 높이는 경향이 있다. 다중 벡터 공격은 소셜 엔지니어링, 제로데이 취약점 활용, DDoS(분산 서비스 거부) 공격, 악성코드 배포 등 공격 형태를 조합하는 방식으로 나타난다. 또한, 중국은 자체 해킹 도구와 악성 소프트웨어를 개발하고 있는데, 이는 중국의 사이버 공격을 효과적으로 수행하는 데 유리하며 자국의 능력을 강화하고 외부 의존도를 줄이는데 유효하기 때문이라고 할 수 있다.

이외에도 사회 공학적(Social Engineering) 차원에서 소셜 엔지니어링과 피싱 공격을 통해 개인과 기업의 정보를 획득하려 한다. 이러한 시도는 주로 악성 이메일을 통해 실행하는데 정보수집 및 사이버 스파이 활동의 주요한 방식을 설정하여 외국 기업과 정부 기관의 중요 정보와 경제, 군사, 기술을 빼내려는 것이다. 2018년에는 중국인으로 추정되는 해커가 러시아·이탈리아 삼성전자 서비스 센터에 스피어피싱을 통해 해킹한 후 국내 삼성전자 본사

10) 대만 정부 "대만, 사이버 공격 매일 500만 번 받아...대부분 중국발", https://www.yna.co.kr/view/AKR20230530070000009
11) 중국 욕하면 사이버 공격...미국서 암약한 중국 비밀조직 또 적발, https://www.hankookilbo.com/News/Read/A2023042616320003429?did=NA
12) Fact Sheet: 2023 DoD Cyber Strategy, https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF

에 접근하려는 시도를 발견하였고, LG전자 미국 앨라배마 지사, LG생활건강 베트남 지사 등 국내 기업의 해외 지사를 대상으로 한 사이버 공격으로 내부 정보가 유출하는 사건이 지속해서 발생했는데, 이는 상대적으로 공격이 쉬운 해외 지사를 통해 국내 본사에 접근, 추가 내부 기술을 유출하려는 시도로 분석할 수 있다.[13] 이처럼 중국의 사이버 공격은 확인할 수 있는 사실이 있음에도 해킹그룹이 다른 국가의 서버를 경유하거나 외국의 서버를 통해 공격하는 경우가 많아 추적과 방어가 쉽지 않다.

표 1. 중국의 시기별 사이버 공격 양상

시기/ 내용	주요 주체	목표	수단과 방식	
1990년대 중반	해킹그룹 정부 연관성 미확인	정보탈취, 도용, 경제 스파이	기본적인 해킹 기술, 스파이웨어 사용	초기 단계 사이버 공격으로부터 경험 축적
2000년대 초반			향상된 악성 코드와 표적형 공격 사용	기술확보, 국가안보와 사이버 제도 수립
2010년대 초반	PLA	군사, 과학 기술, 기업, 경제적 목적 포괄	고급 표적형 공격,APT 활동 확대	사이버 전략 고도와, 사이버 부대 확대, 공격 강화
2010년대 중반	MSS		다국적 기업, 정부 기관 대상 스파이 활동	사이버 국가전략 중요성 부각, 기술 발전 주력, 사이버 공격 활동 강화
2020년대	정부 기구, 해킹 그룹	이념, 선전 활동, 내부 정치 영향	APT, 렌섬웨어, 스피어싱 공격 확대 소프트 웨어 공급망 공격	5G,AI 기술 적용 사이버 공격, 방어 능력 다각화

4. 사이버 안보에 주는 함의

사이버 공격은 전통적인 공격 수법에 그치지 않고 다중 인증(MFA: Multi-Factor Authentication) 우회, TOAD 등과 같은 복잡한 사이버 공격 기법의 출현으로 진화하고 있다. 특히, 중국과 러시아의 공격 그룹이 기업의 소프트웨어 공급망을 표적화하는 사례가 늘어나고 있는데 이는 소프트 웨어 공급망의 무기화 가능성이 커지고 있음을 보여준다. 소프트웨어 공급망에서는 오픈 소스 및 상용 소프트웨어를 조합하여 사용하는 경우가 많다. 특히, 클라우드 컴퓨팅, 오픈 소스 생태계, 소프트웨어 배포 및 자동화 도구 등의 발전으로 인해 소프트웨어 개발 및 배포가 더 빠르고 광범위하게 이루어지고 있다. 그러나 그만큼 보안 및 관리가 제대로 이루어지지 않아 사이버 공격과 취약점 등의 위험성 역시 높아지고 있다. 한 번의 공격으로 수십만 대, 수백만 대의 컴퓨터를 악성코드로 감염시키는 파급력이 있기

13) 최원석 외, 경제 안보 이슈의 부상과 대외 협력 방향, KIEP 연구보고서 22-28, 2022, p189.

때문이다. 러시아가 벌인 2017년 악성코드 NotPetya(2017) 사건과 중국 해커 그룹 Barium[14]도 소프트 웨어 공급망을 주로 활용하는 것으로 알려져 있다. 이들은 1단계 공격 시 향후 추가로 이용할 가능성이 있는 피해자에게 2단계 스파이웨어를 남겨두어 단순히 현재의 이익에만 치중하는 공격이 아닌 장기적 관점에서 지속해 공격하려는 치밀함으로 보인다. 이렇게 되면 시스템의 무결성은 손상되고, 소프트 웨어를 신뢰하는 기본 메커니즘은 더욱 약화하게 된다.

중국의 사이버 공격 양상은 한 번의 성공적인 공격으로 장기적인 접근 권한을 확보하려는 전략을 보여준다. 또한, 보안, 네트워킹, 가상화 소프트웨어, 라우터 표적화에서 조직의 네트워크 내외부로 공격자 트래픽을 중계하고 감추기 위해 제로데이 취약점을 악용하고 있다. 2021년과 2022년 중국 사이버 스파이 제로데이 취약점 공격은 보안, 네트워킹 및 가상화 기술에 집중하고 있는데, 이러한 장치를 목표 대상으로 삼으면 피해자 네트워크에 대한 은밀한 액세스를 확보하고 유지하는 데 몇 가지 전술적 이점이 있기 때문이다. 일부 탈취 공격에서는 탐지를 피하려고 로그 및 보안 제어 우회, 로그 삭제 및 수정, 시작 시 파일 시스템 확인 비활성화에 우선순위를 둔 맞춤형 멀웨어를 사용한다.[15]

중국은 향후 국제사회에서 새로운 형태와 주체를 활용해 사이버 공격의 양상을 이끌어 갈 가능성이 크다. 왜냐하면, 공격의 다양성은 사이버 공격 능력을 향상했다는 것을 전제로 하기 때문이다. 이는 사이버 공간에서의 권력 균형을 무너뜨리고 국제사회에서 중국의 영향력을 강화하는 데 유리하게 작용할 수 있다. 즉, 중국이 향후 사이버 공격과 방어에 관한 선진 기술을 공간에 투영한다면 그만큼 중국이 장악력과 발언권을 가지게 될 것이며, 이는 국제사회가 사이버 공간의 표준과 규범을 만드는 과정에서 중국의 전략적 협상 능력을 확대하는 데 유리하게 작용할 가능성이 크다. 따라서 중국은 사이버 공간에 대한 국가적 이익을 확보하고자 사이버 기술에 기초한 공격 능력을 적극적으로 활용할 것이다. 결국 중국의 고도화된 사이버 공격 기술에 대한 방어와 대응 능력을 마련하는 것은 필수적이며 투자와 연구를 지속해서 확대하고 사이버 공간 전략에 대한 재평가와 더불어 국제사회와 협력을 강화해 나가야 할 방법을 고민해야 할 것이다.

14)분석 그룹의 명명에 따라 Barium 또는 ShadowHammer, ShadowPad 또는 Wicked Panda로도 알려져 있으며, NetSarang(2017),CCleaner(2017) 및 ASUS(2019) 공격의 유사성으로 중국 배후 해킹 그룹으로 분류됨 (WIRED, 2019) 2023년 상반기 사이버 위협 동향 보고서,p.49. 재인용

15) 중국 사이버 공격 그룹의 최신 동향,
https://www.mandiant.com/resources/blog/chinese-espionage-tactics