한국컴퓨터정보학회 하계학술대회 논문집 제28권 제2호 (2020. 7)

북한의 사이버 공격 위협 분석 연구 (공격 기술의 유형 중심으로)

김진광O
OO합동군사대학교
e-mail: whiteseas@naver.comO

North Korea's cyber attack threat analysis research (Based on the type of attack technology)

Jin Gwang KimO
OJoint Forces Military University

● 요 약 ●

북한의 사이버 공격은 매년 증가하고 있으며 공격 수행인력 또한 6,800여 명으로 지속 늘어나고 있어 우리에게 큰 위협이 되고 있다. 그럼에도 불구하고 현재까지 북한의 사이버 공격사례 분석은 각각의 사건에 대한 개별 현황분석밖에 되지 않아 큰 시각에서의 공격 기술 유형이 어떻게 변화하였는지와 관련된 연구가 필요하다. 이에 따라 본 논문에서는 우선 사이버전의 일반사항 및 공격 기술을 확인하고 최근 3년간 발생한 북한의 사이버 공격사례를 조사하여 세부적으로 사용된 주요 공격 기술의 유형을 확인하고자 한다.

키워드: 북한(North Korea), 사이버전(Cyber Warfare), 사이버 공격(Cyber Attack)

I. Introduction

지난 2018년 9월, 美 FBI는 북한 해커 박진혁을 대대적으로 공개수배하였다. FBI의 기소장에 따르면 그는 북한 해커 조직인 라자루스(Lazarus) 그룹에 속해 활동하고 있으며 미국 소니 픽처스, 영국 NHS 등을 해킹한 혐의가 있다. 또한, 당시 미국의 법무차관은 이와 관련하여 "북한 정부의 해커 집단이 중앙은행과 여러 국가의 시민들에게 재산을 강탈하고, 악성코드를 만들어 150여개 국가에 무차별적인 피해자를 양산 및 수십억 달러의 피해를 줬다"고 밝혔다.

한편, 일각에서는 북한이 박진혁을 미국에게 양도하지 않을 것이기에 공개수배의 행위가 큰 영향력은 없다고 주장하나 사실 이러한 수배는 미국이 북한의 무분별한 사이버 공격에 대해 일종의 경고 메시지를 보내는 것으로 해석할 수 있다. 이처럼 북한은 세계 여러 국가를 대상으로 사이버 공격을 하고 있으며 그중 가장 많은 공격이 실시되는 국가가 바로 한국이다. 다음의 <그림 1>처럼 매년 끊이지 않는 사이버 공격의 주요사례만 해도 14건이고, 국가정보원은 지난 2018년 4월 판문점선언 및 9월 평양 정상회담의 남·북간 평화 분위기 속에서도 한국에 대한 북한의 사이버 공격(또는 해킹) 시도가 있었다는 의혹을 제기한 바 있다. [1]

Fig. 1. North Korea Cyber Attack Casea(2009~2018)

이 밖에도 북한의 사이버 공격은 매년 증가하고 있으며 공격 수행인력 또한 2018년 국방백서 상에 6,800여 명으로 지속 늘어나고 있어 우리에게 큰 위협이 되고 있다. 그럼에도 불구하고 현재까지 북한의 사이버 공격사례 분석은 각각의 사건에 대한 개별 현황분석밖에 되지 않아 큰 시각에서의 공격 기술 유형이 어떻게 변화하였는지와 관련된 연구가 필요하다. [2]

이에 따라 본 논문에서는 우선 사이버전의 일반사항 및 공격 기술을 확인하고 최근 3년간 발생한 북한의 사이버 공격사례를 조사하여 세부적으로 사용된 주요 공격 기술의 유형을 확인하고자 한다.

II. Preliminaries

2.1. 사이버전 일반

사이버전에 대해 미국 정부의 보안 전문가인 리처드 클라크(Richard Clarke)는 2010년도 그의 저서 '사이버전(Cyber War)'에서 "특정 국가가 다른 국가의 컴퓨터나 네트워크를 공격하여 피해를 입히거나 파괴할 목적으로 취하는 행동"으로 정의하였다.

한국의 경우 합동참모본부(이하 합참)과 국방부에서 사이버전에 대해 정의하고 있는데, 먼저 합참은 "컴퓨터가 합성한 가상현실의 세계와 가상인간의 영역과 같이 인공지능체계가 운용되는 공간에서 전쟁으로 이는 정보화 사회의 과학기술 발전을 역이용하여 취약점을 공격함으로써 물리적인 군사시스템 파괴보다 훨씬 결정적인 손실을 가용할 수 있는 총체적인 가상공간에서의 정보 마비전을 추구하는 전쟁수행방식을 의미한다"라고 정의하고 있다. 다음으로 국방부는 "사이버 공간에서 일어나는 새로운 형태의 전쟁수단으로서 컴퓨터시스템 및 데이터 통신망 등을 교란, 마비, 무력화함으로써 적의 사이버 체계를 파괴하고 아군의 사이버 체계를 보호하는 것"으로 정의하고 있다. 이러한 사이버전을 대비하여 국방부는 2010년 1월 11일, 국군사이버사령부를 최종 창설하였으며, 2015년 3월 1일부로 사이버전을 본격적인 군사작전으로 인식하여 사이버 작전통제를 국방부에서 합참으로 전환하였다. [3]

Table 1. Cyber Warfare classification

구분	공격적 사이버전	방어적 사이버전	사이버전 지원
내부 사이버전	• 상대의 물적 정보체계 공격 • 상대의 S/W 무력화	• 자신의 물적 정보체계 보호 • 상대의 S/W 공격 방어	• 물적 정보체계 건설, 정비 유지 • S/W 개발 유지관리
외부 사이버전	상대의 물적 정보체계와 정보기반 구조 공격	자신의 물적 정보체계 보호	물적 정보체계와 기반구조의 건설, 정비 유지 고도화

한편, 사이버전은 위의 <표 1>과 같이 분류할 수 있으며 일반적으로 내부 사이버전과 외부 사이버전으로 구분하고 수행방식에 따라서는 방어적 사이버전, 공격적 사이버전, 사이버전 지원으로 나눌 수 있다.

2.2. 사이버전 공격 기술의 유형

사이버전 공격 기술의 유형은 다음의 <표 2>와 같이 다양하며 물리적인 무기체계의 창과 방패의 관계처럼 진화하고 있다. 새로운 사이버 공격 기술이 나타나면 그에 상응하는 방어기술이 개발되어 대응하게 되고 이러한 방어체계를 뚫을 수 있는 새로운 사이버 공격 기술이 다시 개발된다. 이에 따라 초기에는 단순한 기술이 단발적으로 활용되었던 것에 비해 최근에는 좀비 PC 등을 활용한 공격처럼 정교하고 효과가 뛰어난 기술들이 복합적으로 사용되고 있다. [4]

Table 2. Cyber Warfare Cyber attack technology

구분	세부 종류
네트워크 취약점 공격	물리적 공격, 프로토콜 취약점 공격(SYN Flooding, ICMP Flooding DoS, DDoS, IP Spoofing, Sniffing, 세션 하이제킹)
체계 취약점 공격	버퍼 오버플로우, 전자우편 폭탄, 스캔(포트, 서버, 웹 취약점), SQL injection, PHP include, CGI 취약점
바이러스를 이용한 공격	트로이 목마, 트랩도어, 백도어, 쉽핑, 악성코드, 논리폭탄, 웜, 스텍스넷, 스파이웨어
사회공학 기법을 이용한 공격	피싱(Phishing), 스푸핑, 해킹, 해킹 메일, 스미싱(SMS Phishing)
기 타	개체이동 가상무기, 워 드라이빙

2.3. 북한 사이버 부대 일반사항

북한의 사이버 부대 관련 정보는 북한의 폐쇄정책으로 인하여 정확하기 알기 어렵지만 뉴스, 논문 등에 공개된 사항을 통해 확인하면 다음의 <그림 2>고 같이 여러 개의 사이버전 조직을 운용 중이며 그중 정찰총국이 가장 잘 알려져 있다. 북한은 2009년 2월 대남·해외 공작업무를 총괄하기 위해 기존 인민무력부 산하 정찰국과 노동당 산하의 작전부, 35호실 등 3개 기관을 통합, 정찰총국을 만들었고 이때 전자정찰국 사이버전지도국(121국)도 정찰총국 산하에 창설했다. 121국은 다른 나라의 컴퓨터망에 침입해 비밀자료를 해킹하고 바이러스를 유포하는 사이버전 전담부대로 인력만 3천여 명에 이르는 것으로 우리 추정된다. 그리고 이와는 별도로 북한의 총참모부 예하의 지휘자동화국은 바이러스 전문요원과 참모요원으로 구성되어 있으며, 31소와 32소, 56소가 있어 군 관련 프로그램과 함께 해킹 프로그램을 개발하고 있는 것으로 알려졌다. [3]

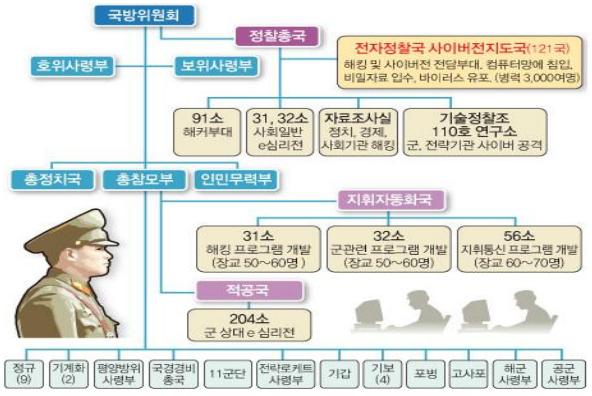

Fig. 2. North Korea Cyber Organization structure

III. North Korea's cyber attack threat analysis

2018년 이후 최근 3년간 북한의 사이버 공격(또는 해킹) 사례 자료는 인터넷 뉴스와 기사를 기반으로 총 1,140건을 조사하였으며 2018년 611건, 2019년 391건, 2020년 138건(5.31. 기준) 분포를 보였다. 유독 2018년에 관련 기사가 많은 이유에 대해 자료 확인결과 서론에 소개된 것과 같이 2018년 9월 美 FBI의 북한 해커 박진혁 기소에 따른 것임을 알 수 있었다.

자료 분석에 앞서 수집한 1,140건의 전처리하여 여러 언론사에서 유사·중복되는 자료는 제외하였으며 공격대상도 한국으로 국한하여 자료를 선별한 결과 총 52건의 공격사례로 정리할 수 있다. 단, 이 자료들은 공식 보안업체 아닌 인터넷 뉴스를 정리한 자료이기에 공격 일자 및 기술 유형 등의 자료 일부가 정확하지 않을 수도 있음을 사전에 밝혀둔다.

3.1. 최근 3년간 사이버 공격 사례 및 키워드 분석

최근 3년간 북한의 사이버 공격 사례 총 52건을 정리하면 다음의 <표 3>과 같으며 연간 발생한 현황을 보면 2018년 21건, 2019년 17건, 2020년 14건으로 평균 매월 1~2건이 발생하고 있음을 알 수 있다. 그리고 2019년에는 공격이 일부 줄어들었으나 올해는 5월까지 벌써 14건으로 다시 증가추세에 있다.

Fig. 3. Keyword analysis of major cyber attacks in North Korea

또한, 사이버 공격 사례에 대한 주요 키워드 분석결과 앞의 <그림 3>과 같이 워드 클라우드로 나타낼 수 있으며 세부적으로 살펴보면 공격 기술은 APT (Advanced Persistent Threat, 지능형지속위협), 스피어피싱 등이 주요 공격 단체로는 김수키, 라자루스, 금성121 등이 관련되어 있으며 주로 가상화폐와 연관된 공격이 많음을 확인할 수 있다.

Table 3. Major cyber attacks in North Korea(2018~2020)

일자	공격 대상	공격 기술 유형	공격 단체
18. 1.10.	가상화폐	악성코드	확인제한
18. 2. 1.	주요 저명인사	피싱	확인제한
18. 2. 6.	가상화폐	APT 공격	확인제한
18. 4.12.	금융 단체	스피어피싱	확인제한
18. 5. 8.	소비자원	DDOS 공격	히든코브라
18. 5.22.	탈북민	악성 앱	확인제한
18. 6. 3.	외교통일부	APT 공격	확인제한
18. 6.11.	가상화폐	스피어피싱, 이메일	라자루스
18. 6.20.	가상화폐	스피어피싱, 이메일	라자루스
18. 6.27.	가상화폐	스피어피싱, 이메일	라자루스
18. 7. 5.	이산가족	APT 공격	금성121
18. 7.18.	공무원	피싱	안다리엘
18. 8. 8.	가상화폐	APT 공격	라자루스
18. 8. 9.	금융 단체	확인제한	김수키
18. 8.31.	금융 단체	랜섬웨어	라자루스
18.10.26.	방사청	스피어피싱	확인제한
18.11.22.	불특정 개인	피싱	확인제한
18.11.29.	주요 저명인사	피싱	확인제한
18.12. 3.	가상화폐	확인제한	확인제한
18.12.13.	국회의원	스피어피싱, 이메일	확인제한
18.12.31.	탈북민	피싱	확인제한
19. 1. 5.	통일업무 기관	APT 공격	확인제한
19. 1.10.	통일부 기자단	스피어피싱	김수키
19. 1.24.	불특정 개인	APT 공격	금성121
19. 2.11.	군업무 관련자	스피어피싱	확인제한
19. 3. 8.	통일업무 기관	스피어피싱	확인제한
19. 3.29.	가상화폐	APT 공격	김수키
19. 5.20.	통일업무 기관	APT 공격	김수키
19. 5.28.	가상화폐	APT 공격	김수키
19. 7.13.	국회의원	APT 공격	금성121
19. 9.27.	금융 단체	스피어피싱, 이메일	코니
19.10.17.	통일업무 기관	스피어피싱, 이메일	김수키
19.10.23.	불특정 개인	APT 공격	라자루스
19.11. 6.	탈북민	APT 공격	금성121
19.11.25.	보안업무 단체	스피어피싱	김수키
19.12. 4.	청와대 관련기관	APT 공격	김수키
19.12.12.	불특정 개인	APT 공격	코니
19.12.20.	민간단체	스피어피싱, 이메일	김수키
20. 1.15.	통일업무 관련자	스피어피싱	김수키
20. 1.29.	올림픽 관련자	APT 공격	코니
20. 2. 5.	가상화폐	APT 공격	라자루스
20. 2.13.	통일부	APT 공격	김수키
20. 2.18.	주요 저명인사	피싱	확인제한
20. 3.20.	주요 저명인사	스피어피싱, 이메일	금성121
20. 3.24.	불특정 개인	스피어피싱, 이메일	김수키
20. 4. 8.	탈북민	스피어피싱, 이메일	라자루스
20. 4.13.	불특정 개인	APT 공격	김수키
20. 4.23.	불특정 개인	APT 공격	코니
20. 4.27.	민간업체	스피어피싱, 이메일	라자루스
20. 4.27.	한수원	APT 공격	라자루스
20. 5. 8.	통일업무 관련자	APT 공격	금성121
20. 5.30.	불특정 개인	피싱, 스미싱	김수키, 코니

3.2. 북한의 사이버 공격 기술 유형 분석

앞서 정리한 <표 3>을 세부적으로 살펴보면 북한의 사이버 공격 대상이 불특정 개인부터 탈북민, 민간단체, 공공업무 관련자들까지 넓게 퍼져 있으며 그 목적 또한 가상화폐 및 주요정보 탈취 등으로

다양함을 확인할 수 있다. 특히, 가상화폐와 관련해서는 2017년 9월 북한의 6차 핵실험 이후 12월에 가해진 대북 경제제재에 따른 자구책으로 볼 수 있다.

다음으로 공격 단체는 김수키가 14회, 라자루스 10회, 금성1216회로 3개의 단체가 한국과 관련된 사이버 공격을 주도하고 있으며 기타사항으로 사이버 공간의 특성상 16회에 대한 공격 배후가 세부적인 확인이 불가하였다.

마지막 사이버 공격 기술의 유형은 APT 공격 21회, 스피어피싱 18회, 이메일 11회, 피싱 7회를 차지하고 있는데 분석 자료를 자세히 확인해보면 북한은 전반적으로 이메일에 첨부된 파일을 통해 악성코드를 유포하고 있음을 알 수 있었다. 또한, 이를 사이버전 공격 기술의 유형 측면에서 보면 4가지의 공격 유형 중 바이러스를 이용한 공격과 사회공학기법을 이용한 공격이 주를 이루고 있다. 즉, 북한은 초기에 DDOS나 랜섬웨어 등을 이용하여 많은 사이버 공격을 시도하였으나 최근에는 발전하는 보안기술 등을 고려하여 직접적인 공격보다는 대응이 제한되도록 사회공학기법의 APT 공격 유형을 주로 활용함을 알 수 있다.

Ⅳ. Conclusions

빠르게 고도화되어가는 ICT기술의 발전은 삶은 윤택하게 해주었지만 반대로 그로 인한 사이버 범죄, 개인정보 침해와 같은 사이버 공격(또는 해킹) 등의 많은 문제점 또한 초래하였다. 더불어 많은 국가에서 사이버 공격으로 인한 피해가 끊이지 않고 있으며 올해 들어 현재까지 보도된 북한의 대남 사이버 공격 사례만 해도 벌써 14건으로 지속 증가추세에 있다. 그리고 공격 기술 역시 진화 중이며 북한이 마음만 먹는다면 한국의 주요 사회 기반시설을 사이버 공격으로 마비시켜 큰 혼란을 초래할 수 있기에 이에 대한 대비가 필요하다. 이에 따라 뉴스 등에 공개된 최근 3년간 발생한 사이버 공격 사례를 정리하고 공격 기술의 유형을 살펴보는 것은 향후 우리의 사이버 대비태세 확립에 활용할 수 있을 것이다. 다만, 향후 연구에서는 공격 사례 기간을 북한이 처음 한국에 사이버 공격을 한 2009년까지 확대하여 공격 기술의 유형이 어떻게 변화하였는지 시계열적 분석 등의 보완이 필요할 것으로 생각한다.

북한의 사이버 공격은 지금까지 그래왔듯 앞으로도 지속 진화하여 더 큰 피해를 발생시킬 것이다. 그리고 최근 1년 연장된 대북재제는 북한의 경제상황을 더욱 힘들게 할 것이기에 더 이상 미사일 발사와 같은 보여주기식 도발보다는 정권유지를 위한 자금 마련을 위해 그들은 더욱 사이버 공격에 집중할 것이다. [5] 따라서 우리는 사이버 공간에서 전쟁을 수행하는 마음가짐으로 강력한 대책을 세워야 할 것이며, '사후약방문'식의 대처가 아닌 필요하다면 우리도 미국처럼 지명수배 등의 적극적인 대응 모습을 보여주어야 할 것이다.

REFERENCES

[1] North Korea invests in cyber wars for 10 years… Can penetrate anywhere in nuclear power plants and subways Source, *https://www.sedaily.com*

[2] Defense White Paper, Ministry of National Defense, p. 21. 2018.

[3] Introduction to Cyber Warfare, Yangseogak, pp. 20 -21, 113-116. 2016.

[4] Strategies for Strengthening Joint Cyber Operations of the Korean Armed Forces, Army Association Ground Forces Research Institute, p. 10. 2015.

[5] Trump extends North Korean sanctions for one year… North Korean nuclear, a special threat to US security, *https://www.donga.com/news*