사회적 이슈를 악용한 사이버 공격 동향 분석

김휘수, 김경백
전남대학교 정보보안협동과정

Analysis of Cyber Attack Trends Exploiting Social Issues

Hwisoo Kim, Kyungbaek Kim
Interdisciplinary Program of Information Security,
Chonnam National University

요 약

사회의 혼란 뒤에는 그것을 이용해 이득을 취하려는 자들이 있기 마련이다. 지금의 코로나19에 의한 혼란속에서 사이버 공격자들은 이 상황에서 갖가지 공격들을 통해 이득을 취하고 있다. 특정 기업이나 개인을 목표로 하는 공격뿐만 아니라 대상이 정해지지 않은 무차별성 공격도 이루어진다. 이를 사회적공격기법이라고 하는데 이는 현재뿐만 아니라 오래 전부터 존재 했던 공격 방식이다. 이 논문에서는 사회적 이슈를 악용한 공격기법의 유형들을 알아보고 분석한다.

I. 서론

최근 전 세계적으로 코로나19에 의한 팬데믹 상황에서 각종 사이버 공격이 자행되고 있다. 공격자들은 각종 기법을 이용하여 기업, 또는 정부기관 등의 특정 대상 또는 일반인들을 목표로 삼아 기업비밀과 개인정보 탈취를 통한 금전적 이득을 취하거나 국가기밀을 유출하여 사회적, 정치적 이득을 보거나 사회혼란을 조장하려는 시도가 많다. 특히 현대인은 인터넷에 대한 의존도가 높아져가는데 스마트폰을 통해 위치에 구애받지 않고 온라인 접속이 가능하며 메신저, SNS등을 통한 정보공유가 쉽고 팬데믹으로 인해 이전 대비 재택근무가 활발하게 늘어나는 추세이기에 공격자들에게는 최상의 공격여건이 마련된 셈이다. 게다가 코로나19는 전 세계의 이목을 집중시키는 아주 큰 사건이었기에 코로나19를 향한 관심은 해커들에게 좋은 먹잇감이었다.

사회적 이슈를 악용한 사이버 공격이 어떠한 형태로 일어났었고, 현재 일어나고 있는지에 대해 사례를 중심으로 알아보고 대비 방안을 알아보고자 한다.

II. 본론

사이버 공격이란 사전적 의미를 보면 컴퓨터 네트워크상에서 악의적인 목적을 가진 공격자가 습득한 사이버 정보(cyber intelligence)를 기반으로 다양한 공격 수단과 공격 기법으로 시스템이나 데이터 자산을 파괴하는 일체의 모든 행위이며 컴퓨터 네트워크 및 공격 대상 시스템에 허가되지 않은 접근을 하거나, 웹 게시판이나 메일을 통해 유포한 악성 파일로 공격 대상 시스템의 정상 동작을 방해하거나 데이터를 탈취, 변조, 파괴하는 것을 말한다. [2] 사이버 공격에는 다양한 기법을 사용하는데 가장 대표적인 것은 악성코드를 이용한 공격이다. 랜섬웨어(ransomware), 바이러스(virus), 웜(warm)등을 유포하여 시스템을 감염시키며 특히 랜섬웨

어는 감염된 컴퓨터의 데이터를 암호화시켜 사용 불가한 상태로 만들고 복호화를 위한 대가로 금전을 요구한다. 2020년 랜섬웨어 피해자들이 지불한 금액이 전년대비 311%증가하였고 올해는 더욱 늘어날 것으로 보인다.[7]

(그림1) 랜섬웨어 공격으로 지급된 암호화폐 증가량 추이

이외에도 이메일 등을 조작해 목표대상을 속여서 유해한 행동을 취하는 피싱(Phishing)등이 있다. 이 중 몇가지 사례를 알아보겠다. 2015년 MERS(메르스)전염이 이슈였던 2015년에 이를 이용한 악성코드가 있었다. 당시 발견된 공격에 사용된 악성파일은 윈도우 바로가기 파일 형식을 하고 있었다. 이를 실행하면 정상적인 DOC 파일과 악성 JPG파일을 특정사이트로부터 다운로드 후 실행하도록 되어있었다. 사용자는 이 둘이 정상적인 파일로 인식하여 넘어갈 수 있으며 파일이 실행되며 악성코드가 실행되어 공격자의 악의적인 행위가 수행되었다.[5] 또 다른 예로 2019년 보잉737 맥스8 추락사고 이슈가 한참 대두되던 때 "위험 항공사 리스트가 있다"는 내용의 메일을 통한 피싱이 있었다. 당시 발견된 메일에는 해당기종 여객기의 추락사고에 대한 요약과 함께 해당 기종을 이용하는 항공사의 목록을 첨부했으니 주위에 전하라는 내용이었다. 사용자가 해당 파일을 실행하면 악성코드가 설치되고 해당 pc정보를 수집해 공격자 서버와 통신하며 pc원격 조종, 추가 악성코드 다운로드 등을 수행했다. [6] 물론 항공사 리스트는 없었다. 이러한 피싱 스미싱 피해를 막기 위해선 출처가 불분명한 메일의 첨부파일 실행 금지, 의심스러운 웹사이트 접속, 메일,SNS,커뮤니티의 접근 자제, 운영체제와 인터넷 브라우저, 응용프로그램, 오피스 프로그램 등의 최신 버전 유지와 보안 패치, 백신 프로그램 설치와 최신 업데이트 등의 필수 보안 수칙 실천이 필요하다. 최근의 가장 큰 이슈는 단언컨대 코로나19다. 해외에서의 경우 중국에 근거를 둔 공격 그룹이 SOGU 공격 및 코발트 스트라이크 페이로드를 배포하며 코로나 이슈를 악용하였다. 코로나19에 관련된 성명서 및 생활안전수칙을 악용해 피싱메시지를 구성하였다.[8] 백신 접종이 본격화 되고 있는 가운데, 질병관리청 예방접종 증명서를 사칭해 개인정보 및 금융정보를 요구하는 스미싱, 피싱 문자 사기가 계속되고 있다. 또한 '(코로나)확진자 동선', '재난지원금', '소상공인 지원 종합안내'등 코로나19 상황과 관련한 키워드 사용 공격이 다수 발견됐다.

(그림2)코로나19상황을 이용한 스미싱문자

정부기관등에서 개인정보를 온라인 상으로 요구하지 않는다는 건 대부분의 사람들이 알고 있는 상식이나 고지능화되는 피싱 형태의 악성코드가 내재된 메일 또는 메시지는 상당히 그럴 듯 하게 보이기 때문에 사용자들이 당하기 쉬울 수 밖에 없다. 사용자들이 이에 당하지 않기 위해서는 함부로 URL에 접속하지 않고 의

심이되는 메일, 문자 메시지를 차단하는등의 기본적인 수칙만 지킨다면 피해를 크게 줄일 수 있을 것이다. 기업에 대한 공격도 증가하였다. 2021년 가장 많이 발견된 악성코드는 폼북(Formbook), 에이전트테슬라(AgentTesla)등의 정보유출형 악성코드이다. 대부분 기업 운영을 위한 서류를 사칭하는 형태의 메일등에 악성 URL을 넣어 이를 접속하게 하는 형식이다. 미국연방수사국(FBI)은 코로나19 방역을 위한 개인 보호 장비 또는 기타 공급품을 구매하는 지자체를 대상으로 하는 악성 이메일을 통한 사기가 증가했다고 지적했다. 코로나19 이후 많은 기업에서 재택근무가 활성화되고 비율이 늘어나면서 공격자들이 이를 노린 공격을 행하기도 했다. FBI는 재택근무 환경이 증가함에 따라 화상 회의 및 원격 회의를 하이재킹하는 형태의 공격에 대해서도 경고했다.[12] 또한, 재택근무 시에 보안을 위해 많이 쓰이는 가상시설망(VPN)의 취약점을 노린 공격도 행해졌다. 기업에선 외부 공격에는 민감하게 대응하는 것이 일반적이지만 기존의 프로그램이나 시스템에 대해선 경계를 낮추는 경향이 있어 이에 대한 대비 및 보완이 필요하다.

III. 결론

코로나19사태가 사이버 공격 증가에 직접,간접적으로 영향을 미쳤다고 볼 수 있는데 국내의 경우 2020년 국내에서 본격적인 확진자 증가 양상을 보이던 2월부터 4월사이에 공격 건수가 가파르게 증가했었다.[3] 코로나19 관련 정보나 긴급 재난 지원금 지급을 사칭한 스미싱 공격과 코로나19관련 공격용url이 무려 9만여 개로 집계되었다.[4] 이러한 공격방식은 시스템의 취약점이 아닌 사람들간의 기본적인 신뢰를 바탕으로 사람을 속이는 공격기법을 통칭하는 것으로, 시스템의 취약점이 아닌 불안과 흥미에 취약한 사람의 마음을 이용한 공격이다. 특히 메르스, 코로나19처럼 널리 알려진 커다란 이슈에 의한 불안 심리를 이용하는 경우가 많아 이런 형태의 공격에 의한 피해의 최소화를 위해 무엇보다도 사용자들의 각별한 주의가 필요하다. 이외에도 정교하고 고지능화되어가는 공격으로부터의 피해를 최소화하기 위해 각 정부부처와 기업들의 긴밀한 협력을 통해 대응 및 보안 정책 수립, 그리고 이를 준수하도록 노력해야 할 것이다.

ACKNOWLEGEMENTS

"이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임"(IITP-2019-0-01343)

[참고문헌]

[1] 최희식, 김현규 "사회적 이슈 관점에서 바라본 사이버 테러 유형에 대한 위험 대응방안", 디지털산업정보학회 논문지 제13권 제1호-2017년3월

[2] https://terms.naver.com/entry.naver?docId=6210355&cid=42346&categoryId=42346

[3] 사회적 이슈를 이용한 악성코드 https://www.ahnlab.com/kr/site/securityinfo/asec/asecView.do?groupCode=VNI001&seq=14713

[4] 코로나 19로 인한 사이버 위협 증가! SK 인포섹, 상반기 공격 통계 발표 https://blog.naver.com/skinfosec2000/222003373866

[5] 6월 주요 보안 이슈 https://www.ahnlab.com/kr/site/securityinfo/asec/asecView.do?groupCode=VNI001&seq=23904

[6] 보잉737 추락사고 이슈 악용한 악성코드 주의보 https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=1&seq=28172

[7] 진화하는 랜섬웨어, 본격화되는 디지털 팬데믹 https://post.naver.com/viewer/postView.naver?volumeNo=32139708&memberNo=48110825&vType=VERTICAL

[8] 코로나19 악용한 사이버 공격 전 세계에 '기승' https://www.segye.com/newsView/20200313511661

[9] 지난해 4분기 차단된 랜섬웨어 공격 17만건...사회적 이슈 악용한 피싱으로 접근 https://blog.naver.com/widgetnuri4/222204641301

[10] 코로나19 이후 사이버공격 유형 및 대응방안 https://scienceon.kisti.re.kr/srch/selectPORSrchReport.do?cn=KOSEN000000000001690

[11] 코로나19 닮은 '사이버 팬데믹' 시대 온다 https://scienceon.kisti.re.kr/srch/selectPORSrchTrend.do?cn=SCTM00208118

[12] Cyberattacks on the rise during the Covid-19 pandemic https://www.bizjournals.com/cincinnati/news/2020/06/01/cyberattacks-on-the-rise-during-covid-19.html

[13] Roundup: COVID-19 pandemic delivers extraordinary array of cybersecurity challenges https://www.zdnet.com/article/roundup-the-coronavirus-pandemic-delivers-an-array-of-cyber-security-challenges/