원격근무 환경에 대한 악성코드 보안 기술 동향

홍승표*, 이훈재**

*동서대학교 (대학원생)

**동서대학교 (교수)

Malware security technology trends in remote work environments

Seoung-Pyo Hong*, Hoon Jae Lee**

*DongSeo University(Graduate student)

**DongSeo University(Professor)

요 약

최근 코로나 19를 통한 우리 생활의 패턴은 많은 변화를 주었다. 기업 근무환경은 원격근무가 표준으로 잡힐 만큼 많은 변화가 있었다. 코로나 19 확산에 따라 사이버 공간은 관련된 위협이 더 증가할 것으로 보인다. 공격자들은 이러한 코로나 19 확산을 이용하여 피싱, 스미싱 등 사회공학적 기법으로 악성코드 및 악성 앱 유포, 개인정보 유출 등 다양한 공격을 수행한다. 본 논문에서는 이에 따른 보안 기술 동향을 분석하고, 보안 위협에 대응하는 해결방안을 알아보려고 한다.

I. 서론

2019년 12월을 기점으로 코로나 19가 퍼진 이래 2021년 현재도 아직 큰 피해를 보고 있다. 기업 근무환경도 국내·외 기업에서는 원격근무가 표준으로 잡힐 만큼 많은 변화가 있었다. 비대면을 일컫는 '언택트(Untact)'가 급격히 증가했기 때문이다. 코로나 19 이전에는 원격 진료, 온라인 쇼핑, 재택근무 등 스마트폰 앱을 이용하여 비대면 일들이 부분적으로 이루어졌지만, 앞으로는 온라인 일 처리가 더욱 심화하고 일상화되는 세상이 되었다. 이런 상황에서 사이버 공간은 관련된 위협이 지속되고 있다. 공격자들은 코로나 19 관련 피싱, 스미싱 등 사회공학적 기법으로 악성코드 및 악성 앱 유포, 개인정보 유출 등 다양한 형태의 공격을 수행하고 있다. 많은 기업은 이러한 사이버 보안 위협 속에서 대응할 수 있는 보안 솔루션이 취약해 있다. 이에 따른 보안 기술 동향을 분석하고, 보안 위협에 대응하는 해결방안을 알아보려고 한다.

II. 관련 연구

2.1 원격근무

원격근무 개념은 1973년 미국 캘리포니아대학 미래연구센터의 'Jack Nilles'가 보험회사의 원격근무 시범프로젝트를 수행하면서 최초로 사용되었다. [1] 개인용 컴퓨터나 통신기기를 이용해서 사무실 이외의 장소에서 작업을 수행하는 근무를 이야기한다.

2.2 원격근무에 대한 위협

많은 국내·외 기업들은 코로나 19 확산에 따라 비대면 근무를 하고 있다. 변화된 근무형태에 따라 새로운 보안 위협이 발생할 수 있다. 원격근무에 대한 보안 위협을 [시스템 OS, 네트워크, 애플리케이션, 정보보호 일반/사회공학]의 4가지의 기준으로 [표 1]과 같이 분류 및 분

석한다. [2]

시스템 / OS	네트워크
Mac 사용자 대상 공격	안전하지 않은 네트워크로의 접속
엔드포인트 장비 및 관련기기에 대한 위협	다수의 원격 접속 지점으로 인한 취약점
취약한 접근제어기술에 대한 위협	종단(Edge, Endpoint) 보안에 대한 취약점
애플리케이션	정보보호일반
취약한 FTP 서비스의 사용, 그에 대한 위협	근무자의 보안 부주의
취약한 이메일 서비스의 사용	임직원 계정을 노리는 크리덴셜 스터핑/피싱
웹캠 관련 해킹	중요 데이터 유출
웹, DNS에 대한 위협	원격접속 로그 기록위협

표 1 원격근무에 대한 보안 위협

III. 사이버 보안 위협 동향

3.1 사회공학적 기법

사회공학적 기법 공격은 크게 2가지로 인간 기반과 컴퓨터 기반으로 나누어지는데, 사이버 공간에서는 컴퓨터 기반 방법으로 피해를 본다. 컴퓨터 기반은 공격 대상에게 악성코드, 컴퓨터 프로그램 혹은 웹 사이트 등의 수단을 이용하여 접근하는 경우이다. [3] [그림 1]은 사회공학적 공격 분류를 나타내는 그림이다.

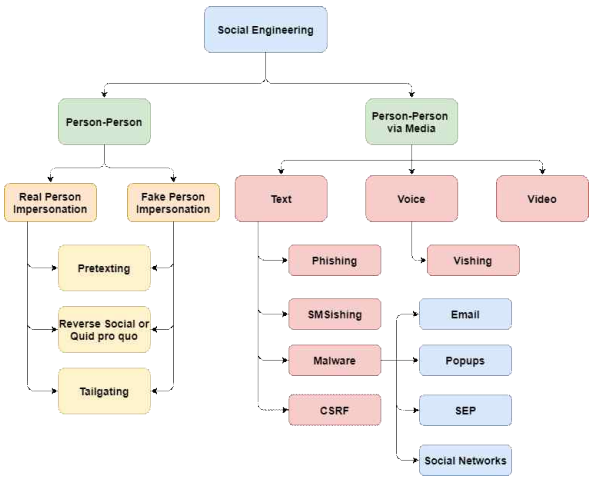

그림 1 사회공학적 공격 분류

3.2 사회공학적 공격 피해사례

현재 국내에서는 코로나 19 확산에 따른 재난지원금이 지급된다. 1차 재난지원금 같은 경우 전 지역에서 지원이 되었다. 최근에는 2차 재난지원금을 경기도에서 지원하게 되는데, 일부 포털사이트에서 재난지원금 관련 검색을 하면 공식 홈페이지가 아닌 광고·유사·가짜사이트로 위장한 피싱범죄가 일어나고 있다. 악성코드가 설치된 해당 사이트는 지급을 위해 접속을 하게 되면 소액결제를 하여 돈을 빼가는 사이트로 확인이 되었다.

3.3 사회공학적 공격 대응방안

정보기기의 종류와 새로운 정보기술서비스의 증가로 인해 사회공학적 공격을 할 수 있는 통로가 증가하고 있다. 미리 그 통로를 예측하고, 사용자들에게 미리 위험성을 경고해야 한다. 일반 사용자 측면에서 보았을 때 사회공학적 공격에 대한 대응은 어떻게 대응할 것인지에 초점이 맞춰질 수 있다. 사회공학적 공격에 대한 대응방안은 여러 논문에서 제시가 되었지만 큰 효과를 볼 수가 없었다. 정보보안의 가장 큰 위협은 '사람'이다. 보안의 위협 '사람'을 막기 위해서는 기업 내부를 통제하기 위한 정보보호 매뉴얼이 필요하다. 기초적인 매뉴얼은 아래와 같다.

1) 인터넷 브라우저의 차단 기능

2) 광고 홍보, 스팸 메일 차단 기능

3) 피싱, 스미싱 사례 및 통계 제공

4) 일반적인 보안 준수 사항 고지

3.4 첨부파일 악성코드 유포

대부분의 피싱 공격은 SMS, 메일을 통해 진행된다. SMS 같은 경우 코로나 19 관련 내용을 통해 사용자의 클릭을 유도해 개인정보를 탈취해 간다. 메일 같은 경우 사회공학적 기법을 통해 사용자가 클릭하게끔 유도하여 첨부파일을 실행하게끔 한다. 첨부파일의 내용은 기업 업무 관련 문서파일, 재난 본부 등으로 속여 파일첨부를 하게 된다. 첨부한 실행 파일은 RAT 계열 및 개인정보 유출형 악성코드로 확인이 된다. 업무 관련 문서파일의 경우 MS 오피스의 취약점을 악용하여 추가 악성 파일을 다운로드 하게 한다. 추가 악성 파일은 사용자의 시스템

을 장악하고, 다양한 악성 행위를 할 수 있다.

IV. 결론

코로나 19 이슈로 인해 현재 사이버 공간에서는 많은 보안 위협들이 존재한다. 그중에서도 이를 악용하는 사회공학적 기법 공격은 인간의 심리를 이용하여 많은 사람의 개인정보를 탈취해 간다. 기업들의 가장 치명적인 위협은 사회공학 해킹 기법이 주를 이룬다. 사회공학 기법은 보안 담당자를 포함해서 모든 직원이 인지하고 대비해야 사전 예방, 피해를 최소화할 수 있다.

[참고문헌]

[1] “Recommended Guide to Information Protection for Smart Work Activation” KISA, pp. 40-107, December 2011.

[2] 김소연, 하영민, 김성율, 최상용, 이종락 (2020). 원격근무 환경에서의 사이버 보안 위협 분석. 한국컴퓨터정보학회 학술발표논문집, 28(2), 97-98.

[3] “사회공학적 해킹의 변화양상”, KISA, 2008.