The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 20, No. 3, pp.189-194, Jun. 30, 2020. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2020.20.3.189
JIIBC 2020-3-26

지능형 악성코드의 이메일 전파에 대한 효과적인 대응 방안에 관한 연구

A Study on Effective Countermeasures against E-mail Propagation of Intelligent Malware

이은섭*, 김영곤**

Eun-Sub Lee*, Young-Kon Kim**

요 약 대부분의 사이버 침해사고는 악성코드를 이용한 APT 공격들에 의해 발생하고 있다. 해커들은 공격 대상에 침투하기 위해 이메일 시스템에 메계체로 한다. 내부로 접근하기 위한 방법으로 이메일을 이용하고, 장기간에 걸쳐 수집된 취약점을 이용해 데이터베이스를 파괴하고, 시스템 운영방해 및 랜섬웨어(Ransomware)를 통해서 개인정보를 불법으로 취득하고 있다. 이처럼 이메일시스템은 가장 친근하고 편리하지만 동시에 보안의 사각지대에서 운영되고 있는 게 현실이다. 이로 인해 개인정보 유출사고가 발생한다면 기업 및 사회 전체에 큰 피해를 줄 수 있다. 이번 연구는 기업내에서 운영 중인 이메일 시스템에 대한 보안 구성을 강화하여 APT 공격으로부터 안전하게 관리하기 위한 효과적인 방법론을 제시하고자 하였다.

Abstract Most cyber breaches are caused by APT attacks using malware. Hackers use the email system as a medium to penetrate the target. It uses e-mail as a method to access internally, destroys databases using long-term collected vulnerabilities, and illegally acquires personal information through system operation and ransomware. As such, the e-mail system is the most friendly and convenient, but at the same time operates in a blind spot of security. As a result, personal information leakage accidents can cause great damage to the company and society as a whole. This study intends to suggest an effective methodology to securely manage the APT attack by strengthening the security configuration of the e-mail system operating in the enterprise.

Key Words : E-mail, Intelligent Malware, APT attacks, Privacy

Ⅰ. 서 론

대부분의 APT공격이 문서를 통한 악성코드 공격으로 발생하고 있으며 실행파일을 실행하여 이상행위를 분석하는 기존 행위기반 APT 방어시스템으로는 최근 문서를 이용한 악성코드를 탐지하는데 한계가 있다. 최근 등장한 리버스 엔지니어링 기술은 '국정원 지침: 해킹메일차단시스템, 망연계 자료전송 악성코드차단시스템 연동'등의 정

*정회원, 한국산업기술대학교 컴퓨터공학과
**정회원, 한국산업기술대학교 컴퓨터공학과(교신저자)
접수일자 2020년 5월 6일, 수정완료 2020년 6월 3일
게재확정일자 2020년 6월 5일

Received: 6 May, 2020 / Revised: 3 June, 2020 /
Accepted: 5 June, 2020
**Corresponding Author: ykkim@kpu.ac.kr
Dept. of Computer Engineering, Korea Polytechnic University, korea

책과 함께 악성코드 보안강화의 대책으로 추진하고 있다.

최근 금융감독원 사칭 '유사수신행위위반' 이메일 피싱 사고 발생('18.08.09), 랜섬웨어 한국유포('19.11.29), '윤건영 청 국정상황실장 사칭 이메일 발송'('18.11.29) 등 이메일 악성 코드를 통한 해킹 및 피해 사례가 지속적으로 증가하고 있다.

랜섬웨어, 악성코드 공격 및 감염경로는 그림2와 같이 이메일, 망연계, 웹서비스를 통해 이루어진다.

그림 1. '18 한국인터넷진흥원 갠드크랩 피해신고 건수
Fig. 1. Number of damages reported by Korea Internet Security Agency

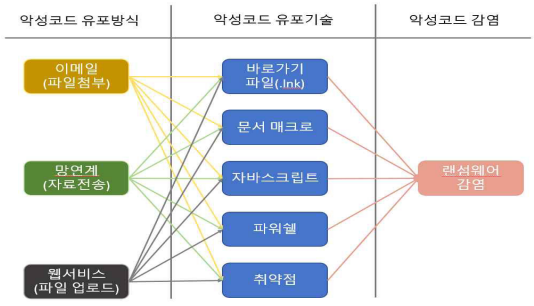

그림 2. 랜섬웨어 악성코드 공격 및 감염경로
Fig. 2. Ransomwe malware attack and infection path

II. 이메일 지능형 위협(APT) 공격

1. 이메일 주요 보안 위협 유형과 공격사례

해커들이 기업 내부로 침투해 정보를 탈취하는 주요 수단으로 가장 많이 활용되는 수단은 이메일이다. 최근의 치명적인 위협들이 기술적인 공격이 아닌 사회공학(SocialEngineering) 해킹 기법이 주를 이뤄 사람의 취약점을 공략해 원하는 정보를 탈취해간다. 이메일은 사회공학적 해킹을 이용하기 가장 손쉬우며 공격 성공률 또한 높다.[1]

이번에는 사업 이메일 침해(Business Email Compromise)의 공격 유형에 대표적인 내용을 알아보고자 한다.

가. 이메일 주소 사칭 공격

사용자의 계정을 탈취, 동일한 메일 주소를 사용하여 상대방에게 악성메일 발송 평소 메일을 주고받던 계정에서 온 메일이기 때문에 아무런 의심 없이 메일을 확인하여 피해 발생

나. 유사 도메인 주소 공격

사용자가 눈으로 확인하기 불가능 하도록 정상 계정과 유사하게 계정을 생성하여 악성메일 발송 평소 메일을 주고받던 계정에서 온 메일이기 때문에 아무런 의심 없이 메일을 확인하여 피해 발생

다. 헤더 위/변조 공격

사용자와 실제 수/발신을 하고 있는 도메인을 사용하여 악성 파일을 첨부하여 메일발송 회사의 도메인으로 들어온 메일이기에 의심 없이 메일 열람 및 첨부파일 다운로드하여 피해 발생

다. 헤더 위/변조 공격

사용자와 실제 수/발신을 하고 있는 도메인을 사용하여 악성 파일을 첨부하여 메일발송 회사의 도메인으로 들어온 메일이기에 의심 없이 메일 열람 및 첨부파일 다운로드하여 피해 발생

라. 본문 악성 URL 공격

세금보고 소프트웨어 회사로 위장하여 세금보고 대행자에게 악성코드가 심어진 웹사이트

링크 첨부하여 메일 발송 세금보고용 소프트웨어 회사라고 생각하여 본문에 담겨진 링크를 클릭하여 PC에 악성코드가 심어진 개인정보 유출

2. 이메일 공격경로

메일을 통한 악성코드 공격경로는 아래와 같이 5가지로 구분할 수 있다.

가. Facebook에서 발송한 메일로 위장

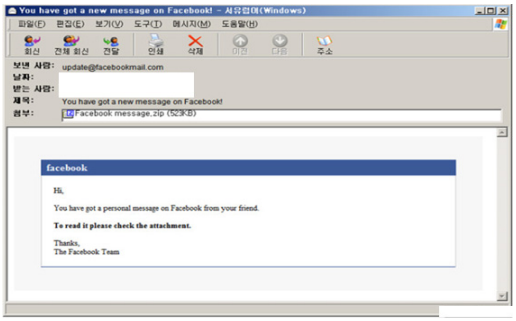

그림 3. Facebook에서 발송한 메일로 위장
Fig. 3. Disguise as an email from Facebook

나. 구글에서 발송한 메일로 위장

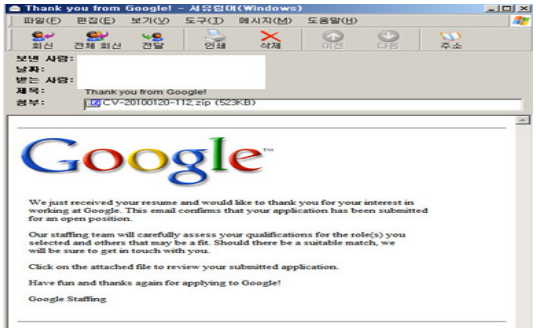

그림 4. Google에서 발송한 메일로 위장
Fig. 4. Disguise as an email from Google

다. 초대 E-Card로 위장한 경우

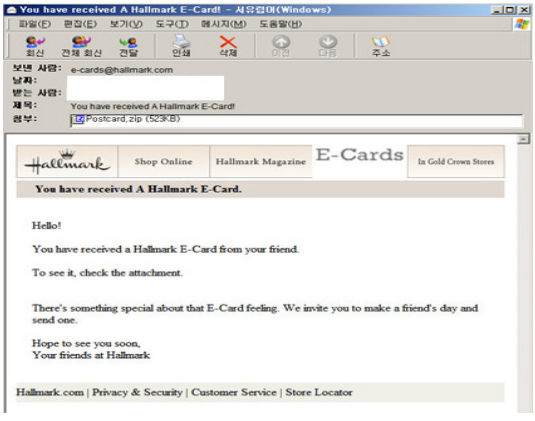

그림 5. 초대 E-Card로 위장한 경우
Fig. 5. Disguised as an invitation E-Card

라. hi5 사이트에서 발송한 메일로 사칭한 경우

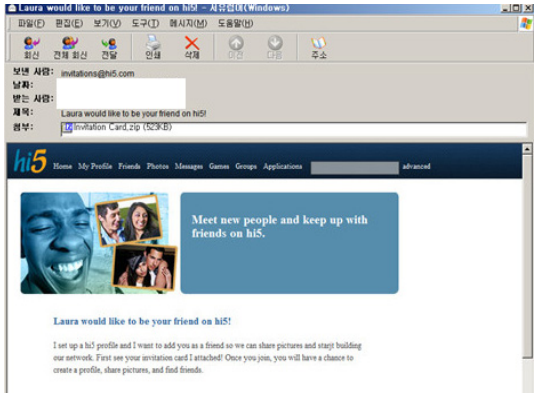

그림 6. hi5 사이트에서 발송한 메일로 사칭한 경우
Fig. 6. impersonating an email sent by hi5 site

마. 아마존 사이트에서 발송한 메일로 사칭한 경우

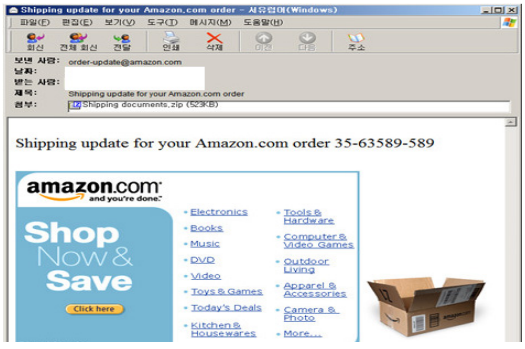

그림 7. 아마존 사이트에서 발송한 메일로 사칭한 경우
Fig. 7. impersonating an email sent amazon site

Ⅲ. 지능형 지속 공격(APT) 이메일 보안시스템

기존 구축된 보안 솔루션으로는 신종 악성코드 방어에 한계가 있으므로, 사이버 위협대비 대응체계에 강화방화를 제시하고, 많은 APT 보안 솔루션들이 네트워크 및 엔드포인트인 PC에 관점을 두고 예방을 위한 방어체계를 제시한다. 본 장에서 이메일 보안시스템구축을 통해 악성 첨부파일과 열람을 유도하는 악성 URL이 얼마나 통과되고 차단되는지 알아보고, 해커들의 공격 방식을 다변화할 경우 대응 방안에 대해서 제시한다.[2]

1. 이메일 APT 시스템 구성

APT 시스템 구성은 메일 관문에서 스팸메일을 1차로 차단하고 악성코드를 2차로 차단하도록 그림 8과 같이 구성하였다.

이메일 APT 시스템 구성으로 공격용 악성코드를 검출하고, 검출되는 악성메일의 상세내용을 확인하고 악성코드를 분석하여 이메일의 보안을 강화 방안을 제시한다. 이메일 분석 구간은 스팸 필터링(스팸장비) 후 실제 사용자에게 전달되는(이메일 서버) 구간을 대상으로 지정했으며 기능은 아래와 같다.

○ 정상적인 메일로 위장한 악성메일의 분석/차단을 수행

○ 일반 문서파일과 같은 비실행파일로 작성된 악성파일 및 감염된 사이트로의 접속을 유도하는 URL링크 등에 대하여 직접적인 분석을 통해 악성여부 확인

○ 기존 스팸차단 솔루션 필터링 이후 분석을 통해 효율성 확보

- 스팸메일 장비와 이메일 서버 사이에 구성하여 분석/격리/전달의 기능 수행

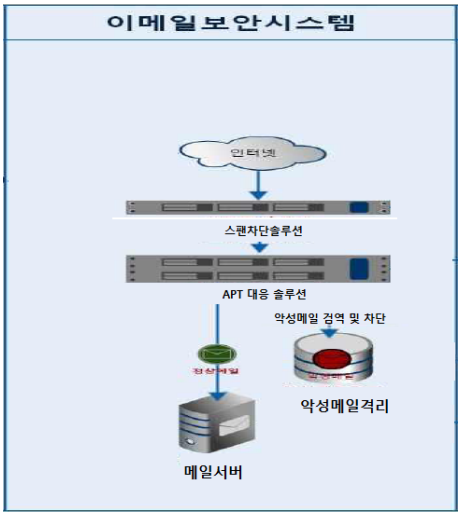

그림 8. 이메일 APT 시스템 구성도
Fig. 8. email APT System diagram

2. 공격용 악성 코드 검출 내용

이메일 APT 시스템 구성에 의해 검출되는 이메일 지능형 APT공격 이메일을 아래와 같이 세분화 내용을 제시한다.[3]

○ 업무형태로 메일서버 규약을 지키지 않은 메일

○ 광고형태로 메일서버 규약을 지키지 않은 메일

○ 악성코드 및 피싱 사이트가 삽입된 URL이 본문에 있는 메일

○ 패턴 악성코드 (백신에서 검출이 가능한 바이러스, 본문 및 문서 내부의 첨부된 악성 URL)

○ 신종 악성코드 (백신에서 검출이 불가능한 새로운 형태의 악성코드)

○ 행위 검출 (악성코드와 같은 행위를 시도하는 파일, 신종 랜섬웨어 등 포함 될 수 있음)

○ 헤더 위변조(보낸 주소와 답장 받는 주소가 다른 메일)

○ 발송 경로 변경(메일 작성지/경유지/메일서버 등 기존 IP와 변경)

○ 유사 도메인(문자의 유사성 및 배열이 기존 계정과 유사)

3. 검출되는 악성메일 상세 내역

제시하는 검출된 악성 코드 상세 내역은 아래 와 같다.

가. 악성코드 및 피싱 사이트가 삽입된 URL이 본문에 있는 메일

유명 포털 메일을 이용한 케이스로, 포털메일에서 제공하는 저장소를 이용하여 악성코드 파일을 업로드 하였다.

나. 패턴 악성코드의 분류는 ①백신에서 검출이 가능한 바이러스 첨부 ②첨부된 문서 내부에 악성코드가 삽입된 메일

사회 공학적 해킹수법을 이용한 케이스로, 악성코드를 첨부파일로 업로드 하여 발송하였다.

다. 행위 검출

해외 유명 배송기업 메일계정을 해킹해 발송한 케이스로, 첨부파일을 직접 실행하는 형태(Behavior Detection Technique)로 행위를 검출하였다. 불특정 다수에게 메일을 발송하는 형태로 스팸 필터링을 우회하는 방법을 사용하였다[4]

라. 발송 경로 변경

특정 일자에 집중적으로 수신하였던 메일로, 발송지 및 계정을 지속적으로 바꾸며 보내는 복합 공격을 검출

하였다.

마. 유사도메인

도메인 유사성을 불일치 문자 개수에 따라 상중하로 나누어 검출하고 상위도메인(Top Level Domain)은 별도 검출하였다.

4. 검출되는 악성코드 분석

가. 발신패턴

조사기간 동안 악성(의심) 메일을 보내는 발신계정의 패턴이 다양했지만, 스팸 및 방화벽 차단정책(동일계정/제목으로 지정한 카운트 이상 발신한 경우 차단)을 우회할 수 있도록 프로그램을 사용하여 계정 및 IP를 계속 변경해서 발송하는 패턴이 주를 이뤘다. 또한 이러한 경우 불특정 다수에게 악성메일을 배포하는 방식을 많이 채택하며 이번 조사 기간에도 악성코드가 첨부된 메일의 경우 다수 발견되었다.[5]

나. 위변조패턴

보낸 주소에서 답장을 하면 답장 받는 주소가 변경되는 헤더위변조를 사용한 메일이 다수 검출되었고 본문 내용은 혹스(Hoax) 메일과 같은 스팸메일이 다수 검출되었다. 스팸 솔루션 필터링 패턴에 등록되지 않고 새롭게 수신된 스팸 메일은 사용자에게 수신된다는 취약점이 발견된 것이고, 이 부분에 대응할 수 있도록 조치를 취해 리스크를 최소화하는 방안을 마련해야한다. 메일 작성지, 경유지, 서버의 IP 정보(국가단위)가 변경된 건이 검출되었지만 주로 정상의 메일이었다. 하지만, 나이지리아 스캠 사건의 원인이 될 수 있는 요소를 검출할 수 있는 환경구축이 필요하다. 유사 도메인 수신 건은 케이스가 많지 않았지만, TLD(Top Level Domain) 부분만 다른 계정에서의 스팸성 메일이 수신되었다.

다. 악성코드 패턴

조사기간 동안 22건의 악성파일 및 40건의 악성 URL이 수신되었다. 2019년 TrendMicro의 2019년 보고서(MAPPING THE FUTURE)에 조사된 것과 같이 직접적인 악성코드 공격보다 피싱 URL을 이용한 사회공학 공격이 더 많이 수신된 것으로 조사되었다. 이는 현재 대부분의 악성 URL 검출이 패턴에 의존하고 있는 점을 이용한 것으로 새로운 주소로 공격을 시도하면 대응할 수 없는 취약점을 노린 공격이다.[6]

V. 결 론

대부분의 사이버 침해사고는 악성코드를 이용한 APT 공격들에 의해 발생하고 있다. 해커들은 공격 대상에 침투하기 위해 이메일 시스템을 메계체로 한다. 내부로 접근하기 위한 방법으로 이메일을 이용하고, 장기간에 걸쳐 수집된 취약점을 이용해 데이터베이스를 파괴하고, 시스템 운영방해 및 랜섬웨어(Ransomware)를 통해서 개인정보를 불법으로 취득하고 있다.

이처럼 이메일시스템은 가장 친근하고 편리하지만 동시에 보안의 사각지대에서 운영되고 있는 게 현실이다. 이로 인해 개인정보 유출사고가 발생한다면 기업 및 사회 전체에 큰 피해를 줄 수 있다.

더 이상 사용자에게 의심 메일을 열지 말 것을 교육하는 것은 무의미 해졌다. 이보다는 경로 탐지, 콘텐츠 분석, 유사 도메인 탐지, 행위 기반을 통한 악성코드 탐지 및 수신자 관련성과 결합하여 위협 메일을 탐지하는 적극적인 방어책이 필요한 시점이다. 이를 위해 이메일 보안 프로세스를 재정비하고 체계화하여 개인정보 유출 및 침해사고예방을 위한 노력이 필요하다.

이에, 본 논문은 지능형 지속 위협(APT) 공격에 대한 이해를 돕고, 사이버 공격 전망과 악성코드 은닉사이트 동향에 대해서 살펴보았다. 또한 이메일 지능형 보안 위협 공격 및 이메일 보안시스템 구축을 통해서 악성 이메일 유입 유형에 대해서 기술하였다.

또한 기업내에서 운영 중인 이메일 시스템에 대한 보안 구성을 강화하여 APT 공격으로부터 안전하게 관리하기 위한 효과적인 방법론을 제시하고자 하였다.

References

[1] Yong-Gyu Jung, Bum-Joon Lee, 'Features Reduction using Logistic Regression for Spam Filtering', The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 10, No. 2, pp. 13-18. 2010

[2] Chun-sik , Kim, 'E-Mail Clustering for the filtering Spam E-mail', The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 5, No. 1, pp. 47-51. 2005

[3] MiSug Gu, YongZhen Li 'A Study of Countermeasures for Advanced Persistent Threats attacks by malicious code', Journal of Convergence for Information Technology, 5(4), pp. 37-42. 2015

[4] Chun-sik Kim, 'E-Mail Clustering for the filtering Spam E-mai', The Journal of The Institute of Internet,

Broadcasting and Communication, Vol. 5, No. 1, pp. 47-51. 2005

[5] Hye Won Kim, Ho Jun Yoo, Jae Woo Lee, 'Technical Threat Research of Email Cloud Security Service', Korea Institute Of Information Security And Cryptology, 27(6), pp. 57-64, 2017

[6] Se Heon Lim, 'An Investigation of the Psychology of Password Replacement by Email Users', Korea Institute Of Information Security And Cryptology, 26(5), pp. 1251-1258, 2016

저 자 소 개

이 은 섭(준회원)

- 2003년 2월 : 한국산업기술대학교 컴퓨터공학과(공학사)
- 2017년 2월 : 한국산업기술대학교 컴퓨터공학과(공학석 사)
- 2020년 2월 : 한국산업기술대학교 컴퓨터공학과(공학박사)

- 관심분야 : 보안, 정보보호, DB, 네트워크, 서버

김 영 곤(정회원)

- 1983.2:경북대학교 전자공학과(공학사)
- 1985.2:연세대학교 본대학원 전자공학과(공학석사)
- 2000.2:한국과학기술원 전산학과(공학박사)
- 1985~2007:KT 수석연구원

- 2007 ~ : 한국산업기술대학교 컴퓨터공학과 교수
- 전문분야 : 소프트웨어공학, 정보통신시스템 통합, 보안