https://doi.org/10.33778/kcsa.2020.20.3.061

스피어피싱 메일 필터링 보안 기능 분석 : 기업메일 호스팅 서비스 중심으로★

신 동 천*, 염 다 연**

요 약

스피어피싱 메일 공격은 특정 대상의 정보를 지속적으로 수집하여 이용하므로 지능적이고 새로운 공격 유형인 APT 공격이나 사회공학적 공격의 일환으로 공격 대상에 미치는 영향이 매우 크다. 스피어피싱 메일은 공격 대상, 목적, 수단 등이 스팸메일과 다르므로 보편적인 스팸메일 필터링 서비스 기능으로는 대응에 한계가 있다. 본 논문에서는 상대적으로 보안성이 취약한 중소기업을 대상으로 호스팅 메일 서비스를 제공하는 기업의 메일 보안 기능이 스피어피싱 메일 공격에 대응할 수 있는지를 분석한다. 분석 결과에 따르면, 스피어피싱 메일 공격 방식이 다양해짐에도 불구하고 제공하고 있는 메일 보안 서비스는 스팸메일을 포함한 메일 관리 수준에 머물러 있다고 판단할 수 있다. 분석 결과는 스피어피싱 메일 공격에 대한 체계적이고 효과적인 대응방안 도출을 위한 기초로 활용될 수 있다.

Spear-phishing Mail Filtering Security Analysis : Focusing on Corporate Mail Hosting Services

Dongcheon Shin*, Dayun Yum**

Abstract

Since spear-phishing mail attacks focus on a particular target persistently to collect and take advantage of information, it can incur severe damage to the target as a part of the intelligent and new attacks such as APT attacks and social engineering attacks. The usual spam filtering services can have limits in countering spear-phishing mail attacks because of different targets, goals, and methods. In this paper, we analyze mail security services of several enterprises hosted by midium and small-sized enterprises with relatively security vulnerabilities in order to see whether their services can effectively respond spear-phishing mail attacks. According to the analysis result, we can say that most of mail security hosting services lack in responding spear-phishing mail attacks by providing functions for mainly managing mails including spam mail. The analysis result can be used as basic data to extract the effective and systematic countermeasure.

Key-words: Spear-phishing, Mail Filtering, Mail Hosting Services, Bayesian Intelligent,

접수일(2020년 08월 31일), 수정일(2020년 09월 14일), 게재확정일(2020년 09월 29일)

★ 이 논문은 2019년도 중앙대학교 연구장학기금 지원에 의한 것임

* 중앙대학교 산업보안학과

** 중앙대학교 대학원 융합보안학과

1. 서론

피싱은 '전화, 문자, 전자메일 등의 전기통신 수단을 이용하여 피해자를 기만, 공갈함으로써 이용자의 개인정보나 금융정보를 빼낸 후 금품을 갈취하는 수법'이다[9]. 피싱 수법 중 하나인 스피어피싱 메일 공격은 일반적으로 불특정 다수가 아닌 특정 개인이나 집단을 대상으로 한다. 스피어피싱 메일은 사회공학적 방법을 사용하여 범죄 대상의 정보를 수집하여 공격 메일을 보낸다. 그리고 메일에 첨부한 URL을 누르게 유도하여 악의적인 웹사이트에 방문하게 한다거나, 악성파일을 내려받게 하는 등의 수법을 사용한다.

스팸메일 필터링 기술은 스피어피싱 메일의 효과적인 필터링에 한계가 있다. 스팸메일의 목적은 이메일을 이용한 광고가 주목적이므로 자신이 누구인지, 어디서 이메일을 보내는지 등을 숨기지 않는다. 스팸메일의 송신 방식은 스팸메일 차단 시스템에 적용된 SPF, DKIM, DMARC 기술이 왜 쓰였는지를 알 수 있게 한다. 이메일 주소, 전송 경로 등을 위조하여 보내는 것을 찾아내고 필터링하는 것이 스팸메일 차단 시스템의 핵심이라 할 수 있다.

스피어피싱 메일은 공격자의 의도가 이메일에 나타나지 않는다. 송신자의 의도와 목적을 뚜렷하게 나타내는 스팸메일과는 달리 스피어피싱 메일은 공격자의 의도와 목적을 숨기고, 공격 대상의 지인 혹은 거래업체로 가장하여 스피어피싱 메일을 보낸다. 메일의 주소, 메일의 내용이 스팸메일처럼 불법 정보를 광고하지 않기 때문에 스팸메일로 분류되지 않으며, 특정 개인만을 대상으로 하므로 피해자의 신고를 바탕으로 수집되는 데이터 또한 절대적으로 부족하다. 즉, 공격자에 대한 정보수집이 불가능하므로 스팸메일처럼 이메일 주소, 전송 경로를 찾아내는 필터링 시스템으로는 스피어피싱 메일에 효과적으로 대응하기 어렵다.

본 논문에서는 스피어피싱 메일 공격에 효과적이고 체계적으로 대응할 수 있는 방안 도출을 위한 기초자료로 활용할 수 있도록 중소기업을 주요 대상으로 하는 기업메일 호스팅 서비스들의 스피어피싱 메일 필터링 기능을 분석한다. 중소기업을 대상으로 하는 것은 중소기업의 매출액 대비 보안 투자 규모가 대기업의 매출액 대비 보안 투자 규모보다 적기 때문이다[6]. 피싱 메일 중 기업 내부의 정보탈취와 같은 목표로 특정 인물을 공격하는 스피어피싱 메일 공격은 공격 대상이 기업이라는 점에서 피해의 규모가 개인의 개인정보 유출 사고보다 크다고 할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 스피어피싱 메일 공격을 기술한다. 3장에서는 중소기업이 사용하는 기업 메일 호스팅 서비스들의 메일 보안 기술에 대해 분석한다. 4장에서는 스피어피싱 공격 대응 기능을 제시하고 기업 메일 호스팅 서비스의 보안 기술을 제시한 기능 관점에서 비교 분석한다. 5장에서는 결론을 맺는다.

2. 스피어피싱 메일 공격

스피어피싱 메일 공격은 APT(Advanced Persistent Threats) 공격의 종류이다. APT 공격은 지능형 지속위협으로 지능적인 방법을 사용해서 지속적으로 특정 대상을 공격한다[17]. APT 공격은 내부로 침입 성공할 때까지 다양한 정보기술과 공격방식을 이용하여 여러 위협을 만들어내고, 공격을 멈추지 않는다.

스피어피싱 메일 공격은 공격의 대상이 되는 인물을 속이고 금전적인 이득을 취할 목적으로 공격의 대상을 물색하고, 그 대상의 수집 가능한 모든 정보를 수집하며, 기회를 포착하기 위해 정보를 수집에 많은 시간이 필요하다. 예로, 공격 대상의 지인 혹은 거래업체로 가장하여 메일 주소와 제목을 위장한 형태로 공격 대상에게 메일을 송신한다. 메일 내용 또한 스팸메일과는 다르게 거래업체와의 일반적인 내용으로 작성한다. 이렇게 작성된 메일을 받은 공격 대상은 의심 없이 메일을 열게 되므로 공격이 성립하게 된다.

스피어피싱 메일의 공격은 정보수집단계, 목표물 접근단계, 그리고 회사 내부의 정보시스템에 침투하여 원하는 정보를 얻는 공격 성공단계로 구분할 수 있다[8]. 스피어피싱 메일 공격은 공격하고자 하는 대상을 정하면서 시작된다. 특정 기업의 관계자인 임직원을 물색하여 대상을 정한다. 기업의 정보시스템에 접근권한이 있거나, 회사 내의 보안에 취약한 대상으로 정해진다. 그 이후 물리적인 해킹과 같은 공격이 아닌 사회공학적 방법을 사용하여 공격 대상이 되는 인물의 온라인상의 정보들을 다양한 방법으로 광범위하게 수

집한다[16][18]. 수집된 정보를 활용하여 공격자는 다음 단계인 목표 대상에 접근을 시도한다. 수집된 정보들을 조합하여 공격자는 목표 대상의 거래업체 혹은 지인으로 가장한다. 마지막으로 공격 대상의 회사 내부 네트워크로 침입하는 것에 성공하면 공격자는 원하는 정보를 수집하고 관리자 권한을 획득하거나 중요 안건을 탈취하는 등의 수법으로 공격을 마친다.

스피어피싱 메일을 보내 공격 대상을 유인하는 방법은 크게 공격자가 이메일 파일에 악성코드를 첨부하는 방법, 메일 내용에 URL을 첨부하는 방법, 그리고 최근에 나타난 방법으로 클라우드에 악성코드가 담긴 파일을 첨부하여 클라우드를 메일에 연결하는 방법 등이 있다. 메일 내용에 URL을 첨부하는 방법은 공격자가 만든 가상의 페이지에 접속하도록 유도하는 방법으로 지원이 종료된 브라우저 버전을 이용하여 취약점을 공격하는 방법이 있다. 클라우드를 이용한 방법은 악성코드를 탐지하는 솔루션을 피하는 방법으로 발전한 공격 형태이다. 클라우드에 파일을 첨부하여 클라우드를 메일로 타인과 공유하는 방법은 단순히 메일 내에 한글, 워드, 엑셀, 실행 파일과 같은 파일을 첨부하는 방법을 넘어선 공격으로 기존의 악성코드 탐지 방법을 피하고 있다.

3. 호스팅 메일 보안 기능 분석

기업 메일 호스팅 서비스를 제공하는 업체는 그룹웨어라는 이름으로 서비스를 제공한다. 이 장에서는 그룹웨어의 서비스 중에서 이메일 서비스를 중심으로 각 기업 메일 호스팅 서비스의 메일 보안 기능을 분석한다. 분석하게 될 기업 메일 호스팅 서비스 업체는 점유율을 기준으로 선정했다[12].

3.1 메일 보안 기술 분석

기업 메일 호스팅 서비스 업체가 제공하는 메일 보안 기능은 차이가 있다[1][2][3][4][5][7][10][11][13]. 본 논문에서는 메일 보안 기능을 크게 사내 메일을 통제하는 기능, 스팸메일 필터링 기능, 메일 내에 첨부된 문서 파일의 필터링 기능, 메일 송수신 암호화 기능으로 분류하여 분석한다.

3.1.1 메일 서비스 통제

메일 서비스 통제를 위한 기능은 메일 모니터링, 승인 메일, POP3/SMTP 설정으로 분류할 수 있다. 메일 서비스를 통제하면, 보안에 취약한 임직원이라 할지라도 관리자의 통제 아래에서 비교적 안전하게 외부와 메일을 송수신할 수 있기 때문이다. 메일 모니터링 기능을 통해 접속 허용 IP를 제한하거나 메일의 송수신 수치를 통계적으로 분석하여 과도하게 수신되는 메일을 모니터링 할 수 있다. 또한 메일의 중요도에 따라 관리자의 승인을 거쳐 메일을 송수신하는 방법으로 메일 서비스를 통제할 수 있으며, 메일을 아웃룩과 같은 메일 계정을 통해 사내 메일이 아닌 계정으로 연동하는 것을 제한할 수 있다.

메일 서비스 통제를 위해 기업이 제공하는 기능으로는 메일 모니터링, 삭제 경로 확인 및 복원(관리자 권한), 접속 내역 관리, 접속 IP 통제, 메일 이용 통계, 중복 로그인 차단, 로그인 2차 인증, 이메일 열람 횟수 제한, 타사 액세스 제한, 승인 메일 기능, 보안 메일 기능, 기밀 메일 시각화, POP3/SMTP 설정 기능이 해당한다. 타사 액세스 제한은 F가 제공하는 기능으로 메일과 캘린더, 주소록 연동에 타사의 어플리케이션을 제한하는 것을 뜻한다. 기밀 메일 시각화란 기밀 문서와 같은 내용의 이메일을 송수신할 때 보안 등급 부여를 의미한다.

3.1.2 스팸메일 차단

스팸메일 차단 시스템은 이메일 발송자 정보를 위/변조하는 스팸메일을 차단하기 위한 기술로 한국인터넷진흥원과 국내 포탈업체가 함께 추진한 기술이다. 메일서버 등록제를 통해 스팸메일을 차단할 경우, 메일을 발송할 때 발송서버 정보가 특정한 형태(SPF, DKIM, DMARC 레코드)로 메일에 포함되어 함께 전송되는데, 이를 통해 수신자 측에서는 해당 메일이 발송자 정보가 위/변조되지 않았음을 확인할 수 있게 된다. 이러한 기술을 도입하여 발송자 정보가 위/변조 된 스팸메일을 차단할 수 있다. 해외에서 보내는 메일의 경우 해외 IP 차단 기능을 통해 스팸메일을 차단할 수 있으며, 발송자와 발송 도메인이 일치하는지 확인하여 도메인의 신뢰 여부를 확인할 수 있다[14].

스팸메일 차단을 위해 기업이 제공하는 기술들로 SPF, DKIM, DMARC 설정, 수,발신 게이트웨이 필터

링, 의심 메일 신고, Bayesian Intelligent 스팸 필터 시스템, 발신자 IP 및 국가 정보 표시 및 접근제어, 실제 발송주소 및 발송 도메인이 다른 경우 주의 표시 기능이 있다. 이 중 Bayesian Intelligent 스팸 필터 시스템은 AI 알고리즘으로 스팸메일의 유형을 학습하여 자동으로 분류하는 알고리즘이다[15].

3.1.3 첨부파일 필터링

첨부파일 필터링 기능으로 첨부파일 Preview, 다운

<Table 1> Technologies of mail security

메일 보안 기능	세부 기능	기업이 제공하는 기능	기업								
			A	B	C	D	E	F	G	H	I
메일 서비스 통제	메일 모니터링	메일 모니터링	○	○	-	○	-	-	-	-	-
		삭제 경로 확인 및 복원(관리자 권한)	○	-	-	-	-	-	-	-	-
		접속 내역 관리	○	○	-	-	-	-	-	-	-
		접속 IP 통제	○	○	-	○	-	-	○	○	○
		메일 이용 통계	○	-	-	○	-	-	○	-	-
		중복 로그인 차단	-	○	-	-	-	-	-	-	-
		로그인 2차 인증	-	-	○	-	-	○	-	-	-
		이메일 열람 횟수 제한	○	-	○	-	-	-	-	-	-
		타사 액세스 제한	-	-	-	-	-	○	-	-	-
	승인 메일 기능	승인 메일 기능	○	-	○	-	-	-	○	-	○
		보안 메일 기능	-	-	○	-	-	○	○	○	○
		기밀 메일 시각화	-	-	-	-	-	-	○	-	-
	POP3/SMTP 설정	POP3/SMTP 설정	○	○	○	○	○	○	○	○	○
스팸메일 차단	스팸메일 차단 시스템	SPF, DKIM, DMARC 설정	○	○	○	○	○	○	○	○	○
		수,발신 게이트웨이 필터링	-	○	-	-	-	-	-	-	-
		의심 메일 신고	○	○	○	○	○	○	○	○	○
		Bayesian Intelligent 스팸 필터 시스템	-	-	-	-	-	○	○	-	-
	해외 IP 차단	발신자 IP 및 국가 정보 표시 및 접근제어	○	-	○	○	-	-	○	-	○
	발송자와 발송 도메인 일치 확인	실제 발송주소 및 발송 도메인이 다른 경우 주의 표시	○	○	○	○	-	○	-	-	-
첨부파일 필터링	첨부파일 Preview	첨부파일 미리보기	○	○	○	○	○	○	○	○	○
	다운로드 시 바이러스 필터링	다운로드 전 바이러스 필터링	-	○	-	○	○	○	-	-	-
	첨부파일 제한	첨부파일 확장자 제한	-	○	-	-	-	○	-	-	-
	첨부파일 실행환경 제공	-	-	-	-	-	-	-	-	-	-
암호화	암호화	TSL/SSL	-	-	○	○	○	○	-	-	-

로드 시 바이러스 필터링, 첨부파일 제한, 첨부파일 실행환경 제공이 있다. 첨부파일 Preview 기능을 통해 먼저 첨부된 파일이 정상적으로 작성된 문서인지 확인하는 방법이 있으며, 미리 살펴봄으로써 악성코드와 해킹 의심 메일을 사전에 차단할 수 있는 기능이다. 첨부파일을 다운로드 할 때 문서 파일이 안전한 파일인지 필터링 하는 기능을 포함하며, 파일이 안전한지 확인할 수 없을 경우 경고 메시지가 표시된다. 이메일에 파일을 첨부할 때 확장자에 제한을 두어 안전한 파일을 주고 받을 수 있도록 범위를 제한하며, 첨부파일을 다운로드 받을 시에도 사용자의 컴퓨터가 안전할 수 있게 첨부파일을 다운로드 하여 실행할 수 있는 환경을 제공 할 수 있다. 첨부파일 필터링을 위해 기업들이 제공하는 기술들로 첨부파일 미리보기, 다운로드 전 바이러스 필터링, 첨부파일 확장자 제한이 있다.

3.1.4 암호화

메일을 송수신할 때 메일 송수신 간의 암호화 기능으로 메일 송수신 서버 간 전송구간에 데이터를 암호화 하여 전송(TLS)하는 기능이 있으며, 클라이언트와 메일 서버 간에 통신할 때 암호화 하여 전송(SSL)하는 기능이 존재한다. 또한, 이렇게 수신된 메일들은 데이터 압축, 메일 암호화, 무결성 검토 등을 거쳐 사내 시스템에 보존된다. 암호화를 위해 기업들이 제공하는 기술들로 TLS/SSL 기능이 있다.

유형별 메일 보안 기능에 각 유형을 위한 기능들을 도출하고 기업이 제공하는 기능 별로 각 기업 별 메일 보안 기술을 정리하면 <Table 1>과 같다.

4. 스피어피싱 메일 필터링 기능 분석

이 장에서는 스피어피싱 메일 공격 유형별로 각 유형에 대응할 수 있는 기능을 제시하고 제시한 대응 기능 관점에서 호스팅 서비스 업체의 메일 보안 기능을 분석한다.

4.1 스피어피싱 메일 공격 유형

4.1.1 메일 주소의 도메인 위조

스피어피싱 메일 공격자는 공격 대상의 거래처 혹은 지인을 가장하여 도메인의 주소를 거래업체 혹은 지인의 메일과 비슷한 주소로 변경하여 메일을 발송한다. 예를 들어, '@naver.com'이라는 도메인을 '@never.com'으로 바꾼다. 공격 대상은 메일 주소에 적혀있는 도메인보다는 메일의 제목과 보낸 이의 이름을 중심으로 신뢰 여부를 정하기 때문에 위험하다고 할 수 있다. 따라서 스피어피싱 메일 공격의 필터링 요건으로 도메인 주소의 정확성 여부를 판단할 필요가 있다.

4.1.2 메일 내 악성코드 첨부

메일 내용에 악성코드가 담긴 파일을 첨부하여 공격 대상이 열어보도록 유도한다. 스피어피싱 메일 공격의 주된 방법인 첨부파일을 이용한 공격은 워드, 엑셀, 한글 문서 파일이 전체 파일 형식의 70%에 달했으며, 실행 파일(.exe)은 1% 정도 수준으로 거의 사용되지 않았다[18]. 워드, 엑셀, 한글 문서를 이용한 악성코드 공격은 계속 사용되고 있으며 실행 파일은 보안 솔루션에 의해 필터링 및 차단되므로, 공격자들은 실행파일 대신 워드, 엑셀, 한글 문서파일이 담긴 압축 파일을 사용한다. 따라서 첨부파일을 이용한 악성코드 공격 필터링을 위해서는 메일 수신 시 첨부파일을 검사하고 문서 파일과 같은 워드, 엑셀, 한글 파일의 외의 확장자를 필터링할 필요가 있다. 또한 압축된 첨부파일일지라도 압축된 문서의 내용을 필터링 할 필요가 있다. 아울러 첨부파일을 다운로드 하지 않고 서전에 미리 열어 볼 수 있는 Preview 기능을 통해 파일의 악성코드 여부를 판단할 필요가 있다.

4.1.3 메일 내용 내 악성 링크 삽입

메일 내용에 URL을 삽입하여 악성코드를 유포하는 방법이라 할 수 있다. 공격 대상은 링크의 안전 여부와 상관없이 링크를 클릭하여 공격자가 만들어 유도하고자 하는 가상의 웹페이지, 혹은 악성코드를 첨부한 웹페이지로 유도한다. 웹페이지 방문만으로도 사내 정보시스템에 공격자가 침입할 수 있게 만드는 악성코드가 사용자의 PC 내에 설치되기도 한다. 따라서 메일 내용에 포함된 단순한 URL 주소를 메일 수신 시 검사하여, 신뢰할 수 있는 URL 주소 여부를 판단하고 필터

링하는 방안이 필요하다.

4.1.4 메일 내 클라우드 링크 공유

클라우드를 통한 스피어피싱 메일 공격은 이메일에 악성코드를 첨부하는 방식에 대한 첨부파일 필터링 기능이 강화되어, 악성코드를 필터링 하는 기능을 우회하고자 나타난 공격 형태이다. 클라우드에 악성코드가 첨부된 파일을 업로드 후, 이메일에 클라우드 링크를 공유하는 방식이다. 이 공격은 스팸메일을 필터링 하는 기능, 첨부파일을 필터링 하는 기능들을 피해 메일을 수신하기 때문에 클라우드 내의 파일에 대해 안전 여부를 확인할 수 없다. 따라서 클라우드를 이용한 스피어피싱 메일 공격에 대한 기존의 대응 방안 외의 새로운 방안이 필요하다.

4.2 스피어피싱 메일 공격 유형별 필터링 기능

4.2.1 메일 주소 확인

스피어피싱 메일 공격 중 이메일 주소의 도메인을 위조하는 것에 대한 방안으로 이메일을 수신할 때 이메일 주소의 도메인을 확인하여 스피어피싱 메일 공격에 대응할 수 있다. 이메일을 송수신 할 때 도메인을 신뢰할 수 있는지 여부를 판단하여 자주 사용하거나 거래 업체의 도메인 주소를 사내 정보 시스템에 등록을 할 수 있다. 안전성을 확인하고 등록한 도메인 주소의 경우 위조된 도메인 주소에서 보내진 이메일과 비교하여 차단을 하거나 다시 확인을 할 수 있다.

4.2.2 파일 preview 기능

이메일을 주고 받을 때, 첨부파일을 첨부할 수 있다. 그러나 첨부파일의 신뢰성은 첨부파일을 다운 받아야만 첨부파일 신뢰 여부를 확인할 수 있다. 공격자는 이러한 방법을 악용하여 악성코드를 첨부한 파일을 이메일에 첨부한다. 이를 막을 수 있는 방안으로 첨부파일을 미리 열어 볼 수 있다. 문서 형식의 첨부파일을 보안 샌드박스(Sandbox)에서 미리 검토하여 이메일에 첨부된 파일 내용에 대한 신뢰 여부의 확인이 가능하다.

4.2.3 첨부파일 다운로드 전 파일 검토

이메일을 수신한 뒤 공격 대상은 이메일에 첨부된 파일을 다운받는다. 첨부된 파일을 다운받기 전 첨부파일의 악성코드 감염 여부를 확인하고 악성코드가 첨부된 파일이면 경고 메세지를 띄우거나 파일을 다운받는 것을 제한할 수 있다.

4.2.4 불확실한 확장자 제한

이메일에 파일을 첨부할 때, 상대방과 주고받을 수 있는 모든 종류의 파일을 첨부하고자 한다. 그러나 손상된 파일, 신뢰할 수 없는 파일, 기업에서 제한하고자 하는 파일과 같은 파일의 경우 확장자를 제한하여 이메일 상에 첨부할 수 없게 할 수 있다. 특히 공격 대상이 알 수 없는 확장자의 첨부파일을 의심 없이 다운받게 되었을 때 공격 대상의 PC에 악성코드가 퍼질 수 있기 때문에 기업에서 제한하고자 하는 첨부파일의 확장자는 제한하고 필터링 할 수 있다.

4.2.5 다운로드 파일 실행환경 별도 제공

안전한 환경에서 이메일에 첨부된 파일을 다운받을 수 있다. 공격 대상이 사용하고 있는 개인 PC에 바로 첨부파일을 다운받는 방법보다, 샌드박스와 같은 환경을 제공하여 첨부된 모든 파일을 다운로드 하여 거치는 것이 사내 정보 시스템을 외부의 침입으로부터 안전하게 보호할 수 있다. 이메일에 첨부된 파일을 미리 보는 방법과 비슷하다고 할 수 있지만 첨부파일을 파일의 내용으로 구분할 수 없는 공격에 대응하는 방안이다.

4.2.6 본문 내 삽입 URL 검토

이메일을 수신할 때 이메일 본문에 적힌 링크를 검토하고 신뢰할 수 있는지 여부를 미리 확인한다. 하이퍼링크로 연결된 URL 뿐만 아니라 텍스트만으로 적힌 URL과 도메인의 주소를 확인할 수 없게 단축된 URL까지 검토하여 신뢰여부를 미리 검토하여 필터링 한다.

4.2.7 클라우드 URL 검토

이메일에 파일을 첨부하는 방법으로 클라우드에 업

로드 되어 있는 파일을 첨부하기 위해 클라우드 링크를 첨부하는 방법이 있다. 상대방의 클라우드에 악성코드가 첨부된 파일이 있는지 필터링 하거나, 외부에서 제공된 클라우드 링크를 필터링 할 수 있다.

<Table 2>는 주요 스피어피싱 메일 공격유형에 대한 대응 기능을 보여주고 있다.

<Table 2> Responses for spear-phishing mail attacks

공격 \ 대응	이메일 주소 확인	파일 preview 기능	첨부파일 다운로드 전 검토	불확실한 확장자 제한	다운로드 파일 실행환경 별도 제공	본문 내 삽입 URL 검토	클라우드 URL 검토
메일 주소의 도메인 위조	○	-	-	-	-	-	-
메일 내 악성코드 첨부	-	○	○	○	○	-	-
메일 내용 내 악성 링크 삽입	-	-	-	-	-	○	○
메일 내 클라우드 링크 공유	-	-	-	-	-	-	○

4.3 기업별 스피어피싱 메일 필터링 기능 분석

A, B, C, D, F의 경우 메일 주소의 도메인 위조에 대한 대응 기술이 존재한다. 실제 이메일 발송주소 및 도메인이 다른 경우, 메일 열람 시 주의 팝업창을 띄우거나, 주의하도록 안내하여 사용자가 주의를 기울일 수 있게 한다. 메일 내 악성코드 첨부 공격에 대한 대응 방안으로 기업들은 첨부파일 미리보기, 다운로드 전 바이러스 필터링, 첨부파일 확장자 제한의 기능을 제공하고 있다. 첨부파일 미리보기 기술의 경우 모든 기업들이 제공하고 있으나, 다운로드 전 바이러스 필터링의 경우 B, D, E, F의 경우만 제공하고 있다. 또한 첨부파일 확장자 제한 기술의 경우 B와 F만 제공하고 있다. 메일 내 악성코드 첨부 공격 대응 방안으로 제안한 다운로드 파일 실행환경 별도 제공의 경우 어떠한 기업도 제공하지 않고 있다. 마찬가지로 본문 내 삽입된 URL 검토, 클라우드 URL 검토에 대한 스피어피싱 메일 공격에 대한 대응 방안 기술 또한 제공하지 않고 있다. <Table 3>은 기업별 메일 보안 기능이 스피어피싱 메일 공격에 대응할 수 있는지를 보여주고 있다.

스피어피싱 메일 공격에 대한 대응 기능을 분석한 결과 기업별로 제공하는 메일 보안 기술은 다양하지만 스피어피싱 메일 공격에 대응할 수 있는 기능은 전반적으로 부족하다고 할 수 있다. 즉, 분석 대상 업체 전체적으로는 4개의 기능이 해당되었으나 2개 업체만이 4개의 기능을 제공한다. 현재 기업들이 제공하는 메일 보안 기능은 다양하다고 할 수 있으나 스팸메일을 필터링하고 계정에 대한 권한을 외부로부터 막는 기능이 중심이라고 판단할 수 있다.

5. 결론

본 논문에서는 중소기업을 주요 대상으로 하는 호스팅 메일 보안 서비스가 스피어피싱 메일 공격에 대응할 수 있는 기능에 대해 분석하였다. 이를 위해 서비스 업체가 제공하는 보안 메일 기능을 비교 분석하였다. 다음으로 스피어피싱 공격유형을 기초로 스피어피싱 공격에 대응할 수 있는 7가지 기능을 제시하였다. 마지막으로 제시된 기능을 호스팅 서비스 기업들이 지원할 수 있는 기능을 제공하는지 분석하였다.

분석 결과에 따르면, 스피어피싱 메일 공격에 대응하는 것을 목표로 보안 기술을 제공하는 기업은 상대적으로 2개 기업에 불과했다. 기업메일 호스팅 서비스를 제공하는 기업들이 스팸메일 차단 시스템의 연속으로 스피어피싱 메일 공격에 대응하고 있다고 판단할 수 있다. 즉, 스피어피싱 메일 공격이 점차 고도화되고

<Table 3> 기업별 메일 보안 기술과 스피어피싱 메일 공격 대응 비교

스피어피싱 메일 공격		기업별 메일 보안 기술	기업								
공격 유형	대응 기능		A	B	C	D	E	F	G	H	I
메일 주소의 도메인 위조	이메일 주소 확인	실제 발송주소 및 발송 도메인이 다른 경우 주의 표시	○	○	○	○	-	○	-	-	-
메일 내 악성코드 첨부	파일 preview 기능	첨부파일 미리보기	○	○	○	○	○	○	○	○	○
	첨부파일 다운로드 전 검토	다운로드 전 바이러스 필터링	-	○	-	○	○	○	-	-	-
	불확실한 확장자 제한	첨부파일 확장자 제한	-	○	-	-	-	○	-	-	-
	다운로드 파일 실행환경 별도 제공	-	-	-	-	-	-	-	-	-	-
메일 내용 내 악성 링크 삽입	본문 내 삽입 URL 검토	-	-	-	-	-	-	-	-	-	-
메일 내 클라우드 링크 공유	클라우드 URL 검토	-	-	-	-	-	-	-	-	-	-

다양해지고 있으나 기업별 메일 보안 기술은 메일을 관리하고 스팸메일만을 관리하는 현실로 판단할 수 있다. 따라서 산업 기술의 보안에 대한 중요성이 커지는 만큼 스피어피싱 메일 대응 방안에 대한 관심과 연구가 필요하며 본 결과는 효과적인 대응방안 도출에 기초 연구로 활용될 수 있다. 끝으로, 본 논문에서 분석한 기업들의 기능들은 공개된 자료들만을 기초로 분석되어 한계성이 존재할 수 있다.

참고문헌

[1] https://daouoffice.com/intro/security.jsp
[2] https://help.worksmobile.com/kr/mail/spam-mail/
[3] https://mailnara.co.kr/index.php/business/functional
[4] https://www.mailplug.com/mailplug/why_mailplug/security
[5] https://www.bizmeka.com/store/main/storesubView.doproductId=PRO_000563&categoryId=collabor
[6] 중소벤처기업부, “중소기업 기술보호역량수준 실태조사”, 2019.
[7] https://www.hiworks.com/manual#/hiworks/103
[8] 한국인터넷진흥원(KISA), “국내 스피어피싱 유형 분석”, 2014.
[9] 한국인터넷진흥원(KISA), “피싱 예방 가이드”
[10] http://www.duzongroupware.com/
[11]https://support.google.com/a/topic/7556597?hl=ko&ref_topic=7556782
[12] The research company, “그룹웨어 시장점유율 조사 보고서”, 2019.
[13] https://bizmarket.uplus.co.kr/intro/introMain?sltnId=BPZ0000004&sltnId1=BPZ0000004
[14] H. Hu, P. Peng and G. Wang, "Towards Understanding the Adoption of Anti-Spoofing Protocols in Email Systems," 2018 IEEE Cybersecurity Development (SecDev), Cambridge, MA, pp. 94-101, 2018.
[15] J. Wu and T. Deng, "Research in Anti-Spam Method Based on Bayesian Filtering," 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Wuhan, pp. 887-891, 2008.
[16] Mario Silic, Andrea Back "The dark side of social networking sites: Understanding phishing risks", Computers in Human Behavior, pp. 35-43, 2016.
[17] P Chen, L Desmet, C Huygens, “A study on advanced persistent threats”, IFIP International Conference on Communications and Multimedia Security, pp. 63-72, 2014.
[18] Trend Micro, “Spear-Phishing Email: Most Favored APT Attack Bait”, Trend Micro Incorporated Research Paper, 2012.

[저자소개]

신동천 (Dongcheon Shin)
1985년 2월 학사
1987년 2월 석사
1991년 2월 박사
email : dcshin@cau.ac.kr

염다연 (Dayun Yum)
2019년 2월 학사
2019년 3월~현재 석사과정
email : dyum@cau.ac.kr