스피어 피싱 대응을 위한 관리적 보안대책에 의한 접근

손유승¹ · 남길현² · 고승철^{3*}

On the administrative security approaches against spear phishing attacks

Yu-seung Sohn¹ · Kil-hyun Nam² · Sung-cheol Goh^{3*}

¹Department of Computer Science, Suwon University, Hwaseong 445-743, Korea

²KISTI ReSeat Program, Seoul 130-741, Korea

³Department of Information Security, Suwon University, Hwaseong, 445-743, Korea

요 약

최근 정보보호 기술의 발전으로 사이버 공격의 패러다임이 변화하고 있다. 조직의 시스템이나 네트워크에 대한 보호 대책이 강화되면서 최종 사용자를 대상으로 사회공학적 기법을 이용하는 사이버 공격이 증가하고 있다. 기업이나 정부기관을 대상으로 중요한 기밀 데이터를 절취하거나 중요 서비스를 무력화하는 지능형지속위협(APT, Advanced Persistent Threat) 공격의 약 91%가 스피어 피싱 이메일을 사용하는 것으로 알려졌다. 본 논문에서는 스피어 피싱 공격의 특성과 보안 위협을 자세히 분석하여 기술적인 통제항목만으로 스피어 피싱 공격에 대응하는 것에 한계가 있음을 설명하고 이를 보완할 수 있는 스피어 피싱 공격에 대한 관리적 대응방안을 제안하였다.

ABSTRACT

Recently the paradigm of cyber attacks is changing due to the information security technology improvement. The cyber attack that uses the social engineering and targets the end users has been increasing as the organization's systems and networks security controls have been tightened. The 91% of APT(Advanced Persistent Threat) which targets an enterprise or a government agency to get the important data and disable the critical service starts with the spear phishing email. In this paper, we analysed the security threats and characteristics of the spear phishing in detail and explained why the technical solutions are not enough to prevent spear phishing attacks. Therefore, we proposed the administrative prevention methods for the spear phishing attack.

키워드 : APT 공격, 스피어 피싱, 보안위협, 관리적 대응방안

Key word : APT attack, Spear Phishing, Security threat, Administrative counter measures

접수일자 : 2013. 10. 20 심사완료일자 : 2013. 11. 20 게재확정일자 : 2013. 12. 03

* **Corresponding Author** Sung-cheol Goh(E-mail:goh5703@hanmail.net, Tel:+82-31-229-8219)

Department of Information Security, Suwon University, Hwaseong 445-743, Korea

Open Access <http://dx.doi.org/10.6109/jkice.2013.17.12.2753>

print ISSN: 2234-4772 online ISSN: 2288-4165

©This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright © The Korea Institute of Information and Communication Engineering.

I. 서 론

최근 정보보호 기술의 발전으로 사이버 공격의 패러다임이 변하고 있다. 사이버상의 악의적인 공격자는 보안 대응책이 잘 구현되어 있는 조직의 시스템이나 네트워크를 공격 목표로 설정하는 것 보다 공격 목표 기업이나 기관에서 근무하는 주요 직원, 즉 기밀데이터나 중요 시스템에 접근 권한이 있는 최종 사용자를 공격 목표로 설정한다. 공격 준비 단계에서 대상자에 대해 수집한 정보를 기반으로 철저히 개인화된 이메일, 즉 스피어 피싱 이메일을 보내는 것이다. 이러한 사회공학 적 기법(Social Engineering)¹⁾을 사용하여 주요 직원의 단말기 권한을 획득한 후 장기간의 모니터링을 통해 계정정보(ID, 비밀번호 등) 등을 가로채거나 원격 제어 도구를 이용해 조직의 주요 시스템과 네트워크를 장악한다. 이러한 공격을 목표 지향적 공격, 즉 지능형지속위협(APT, Advanced Persistence Threat) 공격이라 한다.

APT 공격의 목적은 경쟁 우위를 위한 첩보활동과 정보전쟁의 일환으로 기업의 중요정보 또는 정부의 기밀을 획득하거나 주요 시스템에 침투하여 특정 시스템들을 제어하여 정상적인 운용을 방해 또는 마비시키는데 있다. Ponemon 연구소가 IT와 보안 담당자들을 대상으로 실시한 조사에 따르면, 응답자들의 83%가 본인이나 속한 조직이 APT 공격을 받은 것으로 추정하였다[1].

대부분의 APT 공격의 시작은 스피어 피싱 이메일을 보내는 것이다. APT 공격의 약 91%가 스피어 피싱 이메일을 사용하는 것으로 파악되었다[2]. 대표적인 사례로는 2011년 3월에 발행한 RSA사의 시큐어 ID 정보가 유출된 침해사고이다. 공격자는 RSA 직원을 대상으로 “2011 Recruitment Plan” 제목으로 Adobe Flash의 제로데이 취약점(CVE-2011-0609)을 이용한 악성코드를 삽입한 엑셀 파일을 첨부한 이메일을 보내 최종 사용자 단말기에 원격제어 도구를 설치한 후 RSA 회사의 내부망에 침투한 것이다[3]. 공개적으로 확인된 대다수의 다른 APT 공격도 스피어 피싱 이메일을 통해 시작된 것으로 파악되고 있다. 사이버상의 악의적인 공격자들은 스피어 피싱을 비용대비 효과가 높은 침투기법으로 간주하고 있고 최근에 가장 심각한 보안 위협으로 나타나고 있다.

본 논문에서는 스피어 피싱 공격의 보안 위협에 대해 분석하고 스피어 피싱 공격을 예방하는데 기술적인 통제항목만으로 한계가 있음을 설명하고 이에 대한 보완책으로 적용할 수 있는 다양한 관리적 대응방안을 제안한다.

본 논문의 2장에서는 스피어 피싱 공격의 특성과 이에 따른 보안위협에 대해 분석하고, 3장에서는 기존에 제안된 스피어 피싱 대응방안을 살펴본다. 4장에서는 조직의 보안관리자, 최종 사용자 등 다양한 차원에서 조치해야 할 스피어 피싱 공격에 대한 관리적 대응 방안과 스피어 피싱 대응 솔루션을 도입하기 위해 고려해야 할 기술적 요구사항을 제안한다. 마지막으로 5장에서 본 논문의 연구 결과를 정리한다.

II. 스피어 피싱 공격 특성

대규모 이메일 기반의 피싱 공격은 2010년 11억 건에서 2011년에는 5억 건으로 줄었고 스팸 메시지는 하루에 3000억 건에서 400억 건으로 줄었다. 반면에 스피어 피싱 공격은 1년 동안 3배나 늘어 이로 인한 피해 가능성이 높아졌다. 스피어 피싱 공격 대상자의 50% 이상이 첨부파일을 클릭하는 것으로 알려졌다. 또한 스피어 피싱 공격의 경비는 1000명 대상 스피어 피싱 비용이 100만 명 대상 일반 피싱 보다 10배나 많은 비용이 소요됨에도 불구하고 대규모 스팸 메일보다 클릭할 확률이 10배 이상 높다고 조사되었다[4]. 스피어 피싱 공격은 최근 사이버 공격자가 가장 선호하는 공격 기법이고 조직의 보안관리자에게는 보안의 방어 연결 고리중 가장 약한 사람을 대상으로 하는 공격이기에 가장 방어하기 어려운 공격이다. 이 장에서는 이러한 스피어 피싱 공격의 특성에 대해 자세히 살펴본다.

2.1. 공격 단계별 정보 수집

APT 공격의 성공 가능성을 높이기 위해서는 스피어 피싱 이메일을 작성하기 위한 정보수집 단계가 중요하다. 공격자는 먼저 공격 목표 조직의 주요 직원, 즉 기밀데이터나 중요 시스템에 대한 접근 권한이 있는 최종 사용자가 누구인지 파악한다. 스피어 피싱 공격 대상자

1) 사회공학적인 기법은 공격 목표가 되는 사람을 조종 해 특정 행동을 하도록 유도하는 기술임

가 정해지면 대상자에 대한 상세 정보-이름, 가족관계, 생일, 주소, 졸업한 학교, 취미, 친구관계 등-를 수집한다. 스피어 피싱 공격 대상자 관련 정보는 지하 시장(Black market)에서 구입하거나 Facebook, LinkedIn, Twitter와 같은 SNS(Social Network Service) 사이트, 회사 홈페이지, 기업과 학교 출판물, 구글(Google) 검색 등을 통해 쉽게 수집할 수 있다.

특히, 스피어 피싱 공격 대상자의 이메일 주소의 거의 절반은 구글 검색을 통해 얻을 수 있다. 구글 검색을 통해 획득할 수 없는 이메일 주소는 ‘수신자_이름@기업_도메인명’과 같이 공격 대상자의 이름(또는 영어 이니셜)과 기업의 도메인 이름을 조합하여 검색하면 쉽게 찾을 수 있다. 즉, 스피어 피싱 공격 대상자 이메일 주소의 4분의 3은 웹을 통해서 얻을 수 있다[2].

그리고 공격 목표 조직의 위치 정보, 대표자, 관리자, 사용자 정보, 네트워크 환경, IP 주소, 응용프로그램 버전 정보 등도 SNS 사이트나 취업정보 사이트를 통해 쉽게 획득할 수 있다[5]. 이러한 정보는 공격자가 이메일에 첨부할 악성코드 제작시 보안 솔루션을 우회하기 위한 방법을 찾는 데 악용될 수 있다.

목표 조직의 내부망에 위치한 단말기에 침입한 이후의 정보수집 단계에서는 피해자의 컴퓨터에 원격통제 프로그램(RAT, Remote Access Trojan)을 성공적으로 설치한 후 수행된다. 이 단계에서, 공격자는 피해자의 컴퓨터에 어떤 OS와 보안 소프트웨어가 설치되어 있는지 파악하고 로컬 IP 주소, 프락시 서버, 네트워크에 연결되어 있는 다른 컴퓨터에 대한 접근 정보를 획득한다. 이러한 모든 정보는 공격의 지속성을 유지하여 추후 공격을 수행하고 공격 목표 기업에서 데이터를 유출하기 위해 사용된다[2]. 아래 그림1은 이러한 스피어 피싱 공격에서 정보수집 단계를 스피어 피싱 이메일을 보내기 이전과 최종 사용자가 스피어 피싱 이메일의 피해자가 된 후 공격자가 목표 대상 조직의 내부망에 침투한 이후 단계를 구분하여 설명한 것이다.

그림 1. 스피어 피싱 공격 단계별 정보수집
Fig. 1 Information gathering step in spear Phishing attack

2.2. 스피어 피싱 이메일 구성

공격 대상자에 대해 사전 수집한 정보를 기반으로 철저히 개인화된 스피어 피싱 이메일을 작성한다. 스피어 피싱 이메일은 공격 대상자가 악성코드가 있는 URL 링크를 클릭하거나 악성코드가 삽입된 첨부파일 등을 열어보도록 유도하는 본문 내용과 악성코드 URL 링크나 악성코드가 포함된 첨부파일로 구성된다.

그림 2. RSA 해킹에 사용된 스피어 피싱 이메일 샘플
Fig. 2 Spear Phishing email sample used in RSA hacking

공격 목표 대상자가 메일에 첨부된 파일을 열거나 악성코드가 위치한 URL 링크를 클릭하면 사용자가 인지하지 못하는 사이에 단말기에 트로이목마와 같은 악성코드가 설치되고 이 단말기를 통해 공격자는 공격 목표 조직의 주요 시스템과 네트워크를 장악한다.

2.3. 제로데이 취약점 이용

공격자는 스피어 피싱 이메일에 포함된 악성 URL이나 첨부파일을 최종 사용자가 클릭하였을 때 사용자의 단말기를 통제하기 위해 브라우저, 플러그인 등의 응용프로그램의 제로데이 취약점을 이용한 악성코드를 사용한다.

기존에 알려지지 않은 취약점을 이용하여 새로운 악성코드를 작성하는데 불과 몇 시간밖에 걸리지 않는다. 사이버 범죄자의 대부분은 시스템과 응용프로그램의 취약점을 직접 찾지 않고 보안 연구자나 소프트웨어 업체가 취약점 정보를 공개할 때까지 기다렸다 기업이나 기관에서 대응하기 전에 해당 취약점을 이용한 악성코드를 제작해 사용하는 경우가 대부분이다[6].

시그니처(Signature) 기반의 기존 안티바이러스 제품으로는 제로데이 공격을 방어할 수 없는 문제점이 있다.

전 세계적으로 매일 6만개 이상의 새로운 악성코드가 제작되고 있는 것으로 추정하고 있다. 그리고 최고의 안티바이러스 업체가 신규 악성코드에 대한 탐지용 시그니처를 만들어 배포하는데 평균 11.6일이 걸린다[7]. 아래 그림 3은 상위 13개의 안티바이러스 업체가 신규 악성코드에 대한 시그니처를 작성하여 배포하는데 걸린 기간을 비교한 것이다.

그림 3. 안티바이러스 업체별 신규 악성코드 시그니처 작성/배포 기간(단위 :일)[7]

Fig. 3 Average lag time in days between new threat being detected and anti-virus vendors providing protection through new signatures[7]

방화벽, 침입방지시스템(IPS), 안티바이러스(AV), 보안 게이트웨이 같은 기존의 정보보호 시스템으로는 이러한 제로데이 공격을 이용하는 스피어 피싱 공격을 탐지하고 차단하는데 한계가 있다.

2.4. 스피어 피싱 이메일 공격 시점

사회공학적 기법은 사람의 심리 상태를 이용하는 것이므로 사이버 공격자는 사람들의 판단력이 느슨해지는 시점을 찾으려고 노력한다.

스피어 피싱 공격의 성공 확률을 요일별로 분석한 결과(2012년 7월 ~ 8월)는 금요일(38.5%), 월요일(30%), 일요일(10.9%), 목요일(6.5%), 화요일(5.8%), 수요일(5.2%), 토요일(3.2%) 순서였다[4].

금요일은 대부분의 직원들이 주말을 앞두고 한 주간의 근무 피로감 등의 이유로 이메일 공격에 대한 경계심이 약화된 것이 원인인 것으로 추정되고 월요일은 주

말이후 평소보다 많은 메일을 확인하므로 스피어 피싱 이메일 여부를 판단하는데 집중력이 떨어져 스피어 피싱 공격에 취약한 것으로 분석된다.

2.5. 첨부파일 형태

스피어 피싱 이메일 중 94%가 악성코드가 삽입된 첨부파일을 사용하고 나머지가 악의적인 링크를 클릭하여 악성코드를 다운로드하는 방법을 사용하고 있다. 스피어 피싱 이메일에 첨부되는 파일 형태는 다양하다. 가장 많이 사용되는 파일 형태는 .rtf, .xls, .zip, .pdf 등으로 조사되었다[2]. 아래 그림 4는 트렌드마이크로에서 2012년 조사한 스피어 피싱 이메일에 가장 많이 사용된 첨부파일 형태별 통계 자료이다.

그림 4. 스피어 피싱 이메일에 가장 많이 사용되는 첨부파일 형태 [2]

Fig. 4 Top spear Phishing email attachment file types [2]

일반적인 실행파일 형태인 .exe는 기존의 보안솔루션에 의해 탐지 되므로 거의 사용되지 않지만 압축된 형태인 .lzh, .rar, .zip 파일 형태로는 사용되고 있다. 이러한 압축파일에 비밀번호를 걸어 보안 솔루션을 우회한다[2]. 하지만 이러한 실행 파일이 실행될 때 이상하게 보이거나 사용자가 알아챌 수 있으므로 대부분 일반 문서 형태(.xls, .pdf, .doc, .hwp 등)의 파일에 삽입하여 사용자는 일반 문서를 여는 것 같지만 사용자가 인식하지 못하는 사이에 악성코드가 실행되게 된다. 이렇게

실행되는 악성코드는 2.2절에서 언급한 제로데이 취약점을 악용하기 때문에 기존의 보안 솔루션으로는 탐지가 어렵다.

2.6. 다중 요소 위협

스피어 피싱 공격의 일반적인 특성은 기존의 보안대책을 우회하기 위해서 개인별 최적화된 이메일, 송신자 위장, 제로데이 취약점 이용, 동적 URL, 그리고 drive-by 다운로드²⁾ 등의 기술을 혼합하여 사용하는 다중 요소 위협이라는 점이다.

스피어 피싱 이메일을 통해 최종 사용자 단말기를 감염시키고 감염에 성공한 악성코드는 외부와 통신하여 추가 바이너리를 다운받고, 데이터를 유출하는 다중 단계로 구성된다. 이러한 스피어 피싱 이메일 위협은 목표가 지정되어 있고, 철저히 개인에게 최적화된 메일이어서 스팸 필터가 이러한 스피어 피싱 이메일을 탐지할 가능성이 아주 낮은 보안 위협이 존재한다[4].

III. 기존 스피어 피싱 대응 방안

앞 2.2절에서 살펴본 스피어 피싱 이메일의 구성 영역별 대응방안을 정리하면 아래 그림 5와 같다. 스피어 피싱 이메일 본문 부분은 최종 사용자가 스피어 피싱 여부를 판단해야 하는 부분이기 때문에 관리적 대응방안을 적용하고 악성코드 URL 링크나 첨부파일은 기술적인 대응 솔루션을 이용하여 방어하는 것으로 구분하여 기존 대응 방안을 분석하였다.

3.1. 관리적 대응 방안

스피어 피싱 이메일 본문 부분은 사전 정보 수집 단계를 통해 철저히 개인화된 이메일이기 때문에 기존의 자연어 처리 기법과 통계적 기법을 이용한 피싱 메일 탐지 솔루션으로는 탐지하는데 한계가 있다.

지능적인 스피어 피싱 공격을 방어하기 위한 보안 대책으로 가장 기본적인 것은 정기적인 보안 교육을 통해 스피어 피싱 공격 위협에 대한 인식을 제고하는 방법이 가장 좋은 방어 대책인 것으로 조사되었다[8].

그림 5. 스피어 피싱 이메일 영역별 대응 방안

Fig. 5 Counter measures for spear Phishing email parts

두 번째 관리적 대응 방안은 직원을 대상으로 스피어 피싱 모의침투 훈련을 실시하는 것이다. 주기적으로 스피어 피싱 이메일을 보내 직원의 경각심을 일깨워 주기 위함이다. 이러한 모의침투 훈련을 통해 이메일에 첨부된 파일 또는 URL을 클릭하기 전에 보안 위협에 대해 고려해야 하는 이유를 인식시키는 것은 중요하다[9].

3.2. 기술적 대응 솔루션

아래에서 언급하는 상용 보안 솔루션은 스피어 피싱 이메일 영역별 대응 방안 중 기술적 보안 통제 항목으로 적용 가능한 솔루션이다. 2.5절에서 언급한 바와 같이 스피어 피싱 이메일 중 94%가 악성코드가 삽입된 첨부파일을 사용하고 있다. 스피어 피싱 공격을 방어하는 중요한 기술적인 보안 통제 방법은 이러한 첨부파일에 포함된 악성코드를 탐지하고 차단하는 기능이다.

아래 표 1은 주요 스피어 피싱 대응 솔루션 업체와 주요 기능을 정리한 것이다[10-14]. 대부분의 솔루션은 MS 워드, 한글(HWP), PDF 등의 문서 파일에 숨겨진 제로데이 취약점을 이용한 악성코드 탐지 기능을 포함하고 있고 주로 가상 머신 환경에서 행위 기반으로 신규 악성코드를 탐지하고 있다.

하지만 최근에 등장한 악성코드는 가상머신 환경을 인지하면 동작하지 않게 지능적으로 작성되어 탐지가 불가능한 단점이 있고 악성행위에 대한 정의가 완벽하지 않을 경우 탐지가 어려운 문제점이 있다.

2) 공격자가 웹서버에 공격코드를 업로드 해두고 해당 사이트를 방문하는 사용자의 웹브라우저 취약점을 이용한 공격

표 1. 주요 스피어 피싱 솔루션

Table. 1 Top spear Phishing solutions

업체	주요 기능
AhnLab	<ul style="list-style-type: none"> 가상 머신 환경에서 행위분석과 콘텐츠 분석 기반 신종 악성코드를 분석 문서파일 등 비실행(non-PE) 악성코드 탐지 알려진 정상 파일의 사전 분류를 통한 오탐 최소화 네트워크 기반 이상 트래픽 분석 및 추출된 파일 분석 전용 에이전트를 통한 즉각적인 악성코드 제거
Trend Micro	<ul style="list-style-type: none"> PDF, MS 오피스, 한글(HWP) 및 기타 문서 형식 내에 삽입된 알려진 혹은 알려지지 않은 문서 취약점 공격 탐지 샌드박스를 통한 심층 조사 및 분석으로 추가 악성코드 다운로드 탐지 좀비 PC 탐지, 악성 URL 블랙리스트 기반 내부망으로 유입되는 악성코드 사전 탐지
FireEye	<ul style="list-style-type: none"> 가상 실행 엔진 기반으로 알려지지 않은 OS, 브라우저 및 응용프로그램의 취약성을 이용한 악성코드 탐지 일반 파일 및 멀티미디어 콘텐츠 속에 숨어 있는 악성코드 탐지 버퍼오버플로를 악용한 취약성 및 C&C 서버 연결 차단, 데이터 유출에 사용된 콜백 통신 정보 제공 악의적인 URL 실시간 방지 및 공격 목표가 된 조직내 다른 사용자 식별
Websense	<ul style="list-style-type: none"> 제로데이 공격 등 지능형 멀웨어 위협 방어 기능 웹트래픽을 통한 데이터 유출 차단 샌드박스 기반 악성코드 분석 및 포렌식 보고 기능
Symantec	<ul style="list-style-type: none"> 파일 다운로드 및 검색시 평판 통계 알고리즘을 통해 악성 파일뿐만 아니라 모든 실행 파일에 대한 안전 등급을 실시간으로 부여 파일이 단말기에 저장될 때 시그니처 및 휴리스틱 기반의 악성코드 탐지 파일이 실행될 때 행위 기반의 분석을 통한 탐지 및 차단

이와 같은 기술적인 통제 항목으로 지능적인 스피어 피싱 공격을 방어하는데 한계가 있다. 따라서 스피어 피싱 이메일의 본문 영역에서의 최종 사용자 판단력을 향상시키고 조직의 보안관리자 차원에서 수행해야 할 관리적 대책으로 이러한 기술적 대응 방안을 보완할 필요가 있다.

IV. 제안하는 스피어 피싱 대응방안

앞에서 살펴본 바와 같이 기존의 스피어 피싱 대응방안인 기술적인 통제 방안과 사용자 교육과 훈련과 같은 단편적인 관리 방안으로는 스피어 피싱 공격에 대응하기에 제한적인 부분이 있다. 기존의 대응방안의 문제점을 보완하는 사전 예방적인 관리적 대응 방안을 고안할 필요성이 있다.

따라서 이 장에서는 조직의 보안관리자, 웹서버 운영자, 운영체제/응용프로그램 업체, 최종 사용자 차원에서 조치해야 할 스피어 피싱 공격에 대한 관리적 대응 방안을 제안하고 스피어 피싱 대응 솔루션을 도입하기 위해 고려해야 할 기술적 요구사항을 제안한다.

4.1. 보안관리자 차원에서의 대응 방안

스피어 피싱 공격을 예방하기 위해 조직의 보안관리자가 수립해야 할 관리적 대응 방안을 아래와 같이 제안한다.

- 중요한 정보, 지적 재산, 중요 시스템 또는 네트워크에 대해 접근 권한이 있는 주요 직원-CEO, 서버관리자, DB관리자, 보안관리자, 개발자 등-이 누구인지, 즉, 스피어 피싱 공격 대상이 될 가능성이 높은 사람을 파악하고 이들의 개인 정보나 직무와 관련된 상세 정보가 온라인상에 공개되어 있는지 주기적으로 모니터링 할 필요가 있다. 또한, 주요 직원에 대해서는 일반 직원과는 차별성 있는 스피어 피싱 위협에 대한 인식과 대응 교육을 해야 한다.
- 직원 개인별 이메일 수신량을 조사하여 평균보다 많은 양의 이메일을 수신하고 있는 직원을 파악하여 스피어 피싱 예방 교육을 더 집중적으로 받도록 조치해야 한다. 개인별 이메일 수신량이 많으면 각각의 메일에 대해 최종 사용자가 스피어 피싱 여부에 대한 판단에 대한 집중력이 결여될 가능성이 높은 것으로 나타났다[15].
- 2.4절에서 언급한 통계 조사 결과를 기반으로 스피어 피싱 공격이 많은 월요일과 금요일에 최종 사용자에게 스피어 피싱 위협 가능성을 주기적으로 인식시켜줄 방안을 수립해야 한다. 예를 들면, 조직의 인트라넷 게시판에 팝업 공지 창을 띄우는 등 최종 사용자가 스피어 피싱 보안 위협을 재인식 할 수 있는 방

안을 마련하는 것이 요구된다.

- 조직의 정보보호관리체계(ISMS) 수립에 있어서 스피어 피싱 공격에 대한 사용자 인식 제고를 위해 다음과 같은 통제항목을 추가적으로 수립할 필요가 있다.

통제항목: 스피어 피싱 모의 침투 훈련

철저하게 개인화된 스피어 피싱 이메일에 대해 대응하기 위해 분기 1회 이상 스피어 피싱 모의 침투 훈련을 실시하여야 한다. 그리고 이 훈련 결과를 분석하여 스피어 피싱 공격에 취약한 직원에 대해서는 물입형 교육을 실시하여야 한다.

4.2. 웹서버 운영자 차원의 대응 방안

공격자는 스피어 피싱 이메일에 악성코드를 다운로드 받도록 하는 URL 링크를 포함할 수 있다. 사이버 공격자는 보안상 취약한 웹서버를 탐색하여 이를 악성코드 은닉사이트로 악용한다. 이러한 악성코드 은닉사이트는 홈페이지에 악성코드를 숨겨 놓아 방문한 이용자 PC에 악성코드를 유포하거나 홈페이지를 방문한 이용자 모르게 악성코드 유포지로 연결시켜 주는 역할을 한다. 2011년 3월 발생한 3.4 디도스 대란에서도 보안상 취약한 웹서버를 해킹해 악성코드 유포지로 악용한 사례가 있다. 스피어 피싱 이메일 공격자도 이와 유사한 방법을 악용할 수 있기 때문에 웹서버 관리자는 사전 취약점 점검을 통해 웹서버에 삽입된 악성코드 및 악성코드 유포지 URL 탐지, 웹 방화벽 운영 등 웹서버 보안을 위한 대책을 수립하고, 웹셸(Webshell) 차단 및 방어 등 웹 보안을 강화해야 한다[16].

4.3. 응용프로그램 업체 차원에서 대응방안

다양한 형태의 미디어 플레이어, 웹 브라우저 등의 응용프로그램의 취약점을 이용하는 악성코드와 이러한 악성코드가 최종 사용자가 인식하지 못하는 사이에 실행되도록 문서 파일(pdf, hwp, doc, xls 등)의 취약점을 이용해 삽입되는 보안 위협이 있다. 이러한 보안 위협을 제거하기 위해서는 해당 응용프로그램 업체의 시큐어 코딩에 대한 노력과 지속적인 보안 취약점 모니터링 과정을 통해 피해가 최소화되도록 최대한 빨리 보안 패치를 배포해야 한다.

4.4. 운영체제 업체 차원에서 대응방안

운영체제의 취약점을 이용한 악성코드로 인한 피해를 방지하기 위해 운영체제 업체(MicroSoft, HP 등)에서는 지속적인 취약점 모니터링을 통해 운영체제 취약점이 공개되는 즉시 이에 대한 패치를 배포할 수 있도록 시스템을 구축해야 한다.

4.5. 최종 사용자 차원에서의 대응 방안

스피어 피싱 공격의 특성은 기본적인 인간 심리를 이용한다. 은행, 직장 동료, 친구와 같은 알려지고 신뢰된 소스로부터 이메일이 오기 때문에 일부 사람이 공격에 당하는 것은 피할 수 없다. 그러나 문제는 단 한 사람이라도 악의적인 링크를 클릭하거나 악성코드를 감염시키는 첨부파일을 다운로드 받는 경우, 전체 조직에 주요한 명성과 경제적 손실을 입히는 위험에 처하게 만든다. 즉, 단지 한 대의 PC를 감염시킴으로써 전체 네트워크 보안 대책을 우회하는 것이 가능하다[17]. 이러한 사실로 볼 때, 정기적인 보안 교육과 기술적인 대응책만으로 스피어 피싱 공격에 대응할 수 없다. 따라서 이 절에서는 스피어 피싱 공격의 특성을 고려하여 최종 사용자 관점에서 스피어 피싱 위협에 대응하기 위한 가이드라인을 아래와 같이 제안한다[5,18,19].

- 스피어 피싱 공격의 사전 정보 수집단계에 대응하기 위해 최종 사용자는 SNS 사이트 등 인터넷 공간에 개인 정보를 최대한 적게 공개해야 하며 이에 대한 정기적인 자가 모니터링과 지속적인 확인이 요구된다. 왜냐하면 인터넷에서 개인의 정보를 쉽게 얻을 수 있다는 점은 공격자가 APT 공격 효과를 높이기 위해 선정한 목표 대상자에 관련된 정보를 쉽게 획득할 수 있는 취약점이 있기 때문이다.
- 운영체제 및 각종 응용프로그램의 보안 패치를 항상 최신화하고 안티바이러스 백신의 검색엔진 업데이트를 확인하고 실시간 감시기능을 활성화해야 한다.
- 최종 사용자가 이메일의 본문 내용을 기반으로 스피어 피싱 이메일 여부를 판단하기 위한 점검 가이드라인을 아래와 같이 제안한다[20].

1. 송신자의 이메일 주소를 자세히 확인한다.

: 송신자가 사용할 적절한 도메인 주소인지 확인해야 한다. 한 기업의 대표가 업무와 관계된 내용을 회사

메일을 사용하지 않고 무료로 제공하는 웹메일 주소를 사용할 가능성은 낮다.

2. 이메일 본문에 있는 URL 링크를 클릭하지 않는다.
: URL 링크를 클릭하도록 유도하면 먼저 의심하고 인식가능한 주소인지 확인한다. 어떤 웹페이지를 방문하기 위해 이메일 본문에 있는 링크를 사용하지 말고 해당 회사에 전화하거나 웹브라우저에 URL을 직접 입력하고 방문하는 것이 안전하다.
3. 첨부된 파일 형태를 검증한다.
: 첨부된 파일 확장자가 정상적인 .pdf 파일처럼 보이지만 수많은 공백 뒤에 실제 확장자인.exe가 추가되어 사용자는 모니터 화면에서 확인할 수 없는 경우가 있다.
4. 사용자의 최근 근황 정보와 일치하지만 여전히 공포, 긴급성, 호기심 등 감정적인 반응을 유도하는 내용이면 일단 의심한다.
: SNS 사이트에 올린 모임 사진이나 댓글 정보를 이용하여 친구를 가장하여 악성코드가 삽입된 이미지 등과 같은 첨부파일을 열어 보도록 유도하는 경우 메일 내용의 타당성을 확인해야 한다.
5. 공짜 기대 심리를 이용하는 내용인지 확인한다.
: 응모한 적이 없는 이벤트에서 경품에 당첨되었으니 첨부된 양식을 채워 보내라는 등의 내용에 대한 참·거짓 여부를 판단해야 한다.
6. 이메일을 통해 자료를 받을 것으로 기대한 메일을 받았을 경우 SMS 문자 메시지, 다른 이메일 주소, 또는 다른 방법으로 실제 이메일을 보냈는지 재확인해야 한다.
: 사이버 공격자가 친구, 업무 파트너, 커뮤니티에 속한 신뢰할 수 있는 사람의 이메일 계정을 도용하여 반드시 공격 대상자가 열어볼 수밖에 없는 첨부파일을 보낼 위협이 있기 때문이다.
7. 메일 내용에 맞춤법은 잘 준수하고 있는지 확인한다.
: 공식적인 소통에서는 메일을 보내기 전에 맞춤법을 점검하는 반면 스피어 피싱 이메일인 경우 수준 낮은 작문과 맞춤법을 무시하는 경우가 종종 있기 때문이다.

4.6. 스피어 피싱 대응 솔루션 도입시 요구사항

기업이나 기관 등에서 스피어 피싱 공격을 방어하기 위해 적절한 솔루션을 도입하기 위해 고려해야 할 기술

적 요구사항을 아래와 같이 제안한다[4,6,8].

- 행위 기반 악성코드 분석 기능
: 제로데이 공격을 차단하기 위해 시그니처(Signature) 기반이 아닌 가상 환경에서 악성코드를 실행하여 어떤 악의적인 행위를 수행하는지 판단하는 행위 기반으로 악성코드를 탐지하는 능동적 위협 차단 기능이 필요하다.
- 샌드박스(Sandboxing) 기능
: 웹사이트 콘텐츠와 브라우저 코드를 실시간으로 분석하는 기술로 이메일에 첨부된 파일과 URL 링크의 안전성 여부를 점검하는 기능이 요구된다.
- 웹 트래픽 실시간 분석 및 차단 기능
: 실시간 HTTP 프로토콜 검사를 통해 모든Non-HTTP 형태의 원격접속 도구(RAT)의 아웃바운드 콜백(Outbound Callback)을 탐지하고 차단하는 기능이 요구된다.
- 통합로그 분석 기능
: 웹방화벽, 침입탐지시스템, 안티바이러스 등과 같은 정보보호시스템에서 발생하는 모든 로그들을 빅데이터(Big Data) 기반으로 연관성을 분석하여 공격 징후를 사전에 탐지할 수 있는 기능이 요구된다.
- 단말기 상태 변화 감시 기능
: 최종 사용자 단말기의 프로세스, 레지스트리, 파일에 대한 생성·변경 여부를 감시하여 공격 징후를 탐지할 수 있는 기능이 요구된다.

V. 결 론

스피어 피싱 공격은 오늘날 조직을 위협하는 핵심 보안 위협이 되고 있는 반면, 스피어 피싱 공격 목표 대상 기업이나 기관에서는 대부분 기존의 보안 솔루션들에 의존하는 경향이 있다. 따라서 스피어 피싱 공격에 대한 지속적인 관심과 예방 대책이 필요하다.

본 논문에서는 스피어 피싱 공격의 특성에 대해 분석하여 정리함으로써 스피어 피싱 공격의 잠재적인 위협에 대한 인식을 제고하였다. 현재 상용 스피어 피싱 대응 솔루션에 대해 살펴보았고 이를 통해 기술적인 통제 항목만으로 스피어 피싱 공격에 대응하는 것에 한계가 있음을 설명하였다. 따라서 이러한 한계를 보완할 수

있는 스피어 피싱 공격에 대한 다양한 차원에서의 관리적 대응 방안과 조직에서 스피어 피싱 공격에 대응하기 위해 보안 솔루션 도입시 고려해야 할 기술적 요구사항을 제안하였다.

REFERENCES

- [1] Herndon, Va. Ponemon Institute Discovers Majority of Business Leaders Underestimate Risk of Advanced Cyber Threats. <http://www.prnewswire.com/news-releases>
- [2] Trend Micro Inc., "Spear-Phishing Email: Most Favored APT Attack Bait", Trend Micro Incorporated Research Paper, 2012
- [3] Larry Seltzer. How the RSA SecurID Hack Worked. <http://www.pcmag.com/article2/0,2817,2382970,00.asp>
- [4] FireEye, Inc. "Spear Phishing Attacks—Why They are Successful and How to Stop Them", White Paper, 2012
- [5] John H.Sawyer. How Attackers Target and Exploit Social Networking Users. <http://www.darkreading.com/end-user/how-attackers-target-and-exploit-social/240160011>
- [6] IBM Software Thought Leadership, "Proactive response to today's advanced persistent threats", White Paper, 2013
- [7] Cyveillance, (August 2010). Malware Detection Rates for Leading AV Solutions. <http://www.cyveillance.com/web/>
- [8] Patrik Runald. What is Scaring Business the Most? Spear-phishing. <http://community.websense.com/blogs/websense-insights/archive/2012/10/08/what-is-scaring-business-the-most-spear-phishing.aspx>
- [9] Dave Shackelford. Social engineering penetration testing: Four effective techniques. <http://searchsecurity.techtarget.com/tip/Social-engineering-penetration-testing-Four-effective-techniques>
- [10] AhnLab Inc. TrusWatcher Brochure. http://download.ahnlab.com/kr/site/brochure/TrusWatcher_Brochure.pdf
- [11] Trend Micro Inc. Deep Scan Brochure. <http://www.trendmicro.co.kr/cloud-content/kr/pdfs/business/datasheets/deepscan.pdf>
- [12] FireEye Inc. Email Malware Protection System Brochure. <http://www.fireeye.com/ko/resources/pdfs/fireeye-email-malware-protection.pdf>
- [13] Websense Inc. TRITON Web Security Gateway Anywhere. <http://www.websense.com/assets/reports/websense-miercom-report.pdf>
- [14] Micor Plus Co. Symantec Endpoint Protection 12. <http://www.mplsoft.co.kr/entry/>
- [15] Arun Vishwanath, Tejaswini Herath, Rui Chen, Jingguo Wang, H.Raghav Rao, "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model", Decision Support System 51, pp. 576-586, 2011
- [16] Boannews Inc. The shadow of Webshell behind hacking incident. <http://www.boannews.com/media/view.asp?id=37444>
- [17] Bimal Parmar, "Protecting against spear-phishing", Computer Fraud & Security, pp. 8-11, Jan. 2012
- [18] Tracey Caldwell, "Spear-phishing: how to spot and mitigate the menace", Computer Fraud & Security, pp. 11-16, Jan. 2013
- [19] Rebecca Greenfield. How to Avoid Getting Spear Phished by China's Hackers Who Cracked Apple. <http://www.theatlanticwire.com/technology/2013/02/spear-phishing-security-advice/62304/>
- [20] Yu-seung Sohn, Kil-hyun Nam, Seung-chul Goh, "A spear phishing threat and the prevention method for the end user", KIICE Conference in Mokpo, May, 2013.

손유승(Yu-Seung Sohn)

2005년 8월 포항공과대학교 정보통신학 공학석사
 2011년 3월~현재 수원대학교 컴퓨터학과 박사과정
 ※관심분야: 사이버 공격, 암호기술과 정책, 웹 취약점 분석

남길현(Kil-Hyun Nam)

1985년 미 루이지아나대 전산학 박사
 1985-2006 국방대학교 교수(현 명예교수)
 현재 한국과학기술정보연구원 전문연구위원
 ※관심분야: 정보보호, 암호학, 사이버 보안

고승철(Sung-cheol Goh)

1992년 포항공과대학교 전산수학 이학박사

현재 수원대학교 정보보호학과 교수

※관심분야: 정보보호, 알고리즘, Computational complexity