스피어 피싱 위협과 최종 사용자 관점에서 대응방안 제안

손유승* · 남길현** · 고승철*

*수원대학교 · **한국과학기술정보연구원

A spear phishing threat and the prevention method for the end user

Yu-seung Sohn* · Kil-hyun Nam** · Seung-chul Goh

*The University of Suwon · **KISTI ReSeat Program

E-mail : useung@hanmail.net, khnamk@gmail.com, goh5703@hanmail.net

요 약

최근 기업과 정부기관을 대상으로 한 목표지향적 공격이 증가하는 추세이다. 목표 지향적 공격이라 불리는 지능형 지속 위협(Advanced Persistent Threat) 공격의 시작은 공격 목표 조직에 근무하는 특정 대상자에게 사전 수집된 정보를 기반으로 철저히 개인화된 이메일, 즉 스피어 피싱 이메일을 보내는 것이다. 목표지향적 공격의 약 91%가 스피어 피싱 이메일을 사용하는 것으로 알려졌다. 본 논문에서는 최근 스피어 피싱 개요와 특징에 대해 설명하고 기존에 제안된 스피어 피싱 대응방안을 분석하였다. 이러한 분석과 이해를 바탕으로 최종 사용자 관점에서 효과적인 스피어 피싱 대응방안을 제안하였다.

ABSTRACT

Recently target oriented attacks which target an enterprise and a government agency are increasing. The starting point of APT(Advanced Persistent Threat), called as target oriented attacks, is the spear phishing email that is personalized based on the information collected via Internet of the target personnel. It is known that 94% of target oriented attacks use spear phishing emails. Therefore, in this paper, we analysed spear phishing methods in detail and the characteristics and recent trends of spear phishing threats and proposed the effective prevention method of spear phishing for the end user.

키워드

목표 지향적 공격, 스피어 피싱, 대응 방안

Ⅰ. 서 론

최근 들어 사이버 공격의 패러다임이 변하고 있다. 악의적인 공격자는 보안 대응책이 잘 구현되어 있는 서버나 네트워크를 공격 목표로 설정하는 것이 아니라 공격 목표 기업이나 기관에서 근무하는 핵심 직원을 대상으로 사회공학적 기법(Social Engineering)을 사용하여 해당 단말기를 점령한 후 조직의 주요 네트워크와 시스템을 장악하는 방법을 사용하고 있다. 이러한 공격 방법을 목표 지향적 공격, 즉 지능형 지속가능 위협(APT, Advanced Persistence Threat) 공격이라 한다.

최근 급증하고 있는 APT 공격의 시작은 공격 목표 조직에 근무하는 특정 대상자에 대한 민감한 정보-사는 곳, 직업, 생일, 취미와 같은 개인정보-를 Facebook, LinkedIn, Twitter와 같은 SNS(Social Network Service) 사이트, 회사 홈페이지, 구글(Google) 검색을 통해 수집한 후, 이 정보를 기반으로 철저히 개인화된 이메일, 즉 스피어 피싱 이메일을 보내는 것이다. 목표 지향적 공격의 약 91%가 스피어 피싱 이메일을 사용하는 것으로 알려졌다[1]. 즉, 공격 목표 대상자가 메일에 첨부된 파일을 열거나 악성코드 링크 URL을 클릭하면 사용자가 모르는 사이 단말기에 악성코드가 설치되고 이 단말기를 통해 공격 목표 조직의 서버와 네트워크를 장악한 후 중요 정보를 유출하는 것이다.

2011년 농협 전산망 해킹사건, 네이트 개인정보 유출사건, 2012년 KT 개인정보 유출 사건 등이 APT 공격의 피해 사례로 파악되고 있다. 사이버 공격자들은 스피어 피싱을 효율성이 높은 침투기법으로 간주하고 있고 이를 이용한 목표 지향적 공격이 급증하고 있다.

본 논문에서는 스피어 피싱 공격의 기본 개념과 특성에 대해 알아보고 최근 스피어 피싱 기법의 동향에 대해 살펴본다. 그리고 스피어 피싱 공격을 예방하기 위해 기존에 제시된 보안 대책을 분석하여 이를 바탕으로 최종 사용자 관점에서 효과적인 스피어 피싱 대응방안을 제안한다.

II. 목표 지향적 공격

APT 공격은 2000년대 중반부터 발생되었으며, 최근에는 공격 횟수가 늘어나고 있으며 이로 인한 피해가 증가하고 있다. APT 공격과 같은 목표 지향적 공격의 대상이 전 세계적으로 활동하는 NGO 단체나 정부기관들의 유력 인사 대상으로 공격이 증가하고 있다. Ponemon 연구소가 IT와 보안 담당자들을 대상으로 실시한 조사에 따르면, 응답자들의 83%가 본인이 속한 조직이 APT 공격을 받은 것으로 추정하였다[2].

APT 공격자는 우수한 은폐 능력과 지속 가능한 공격기법으로 장기간에 걸쳐 특정 기업과 정부의 시스템 구성요소로 침투하여 목적을 달성한다. APT 공격 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. 그리고 핵티비스트(hacktivist)인 경우에는 DDoS 공격 또는 데이터 불법 획득을 통해 정치적 여론 형성 등의 공격 목적이 있다. 아래 그림1은 APT 공격의 4단계를 개념적으로 설명한 것이다.

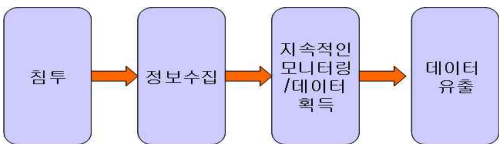

그림 1. APT 공격 4단계

이러한 APT 공격은 통상적으로 사용자가 첨부파일이나 악성코드 URL을 클릭하도록 유인하는 스피어 피싱으로부터 시작된다. 고스트넷, 나이트드래곤, 오퍼레이션 오로라, RSA 침해, 그리고 공개적으로 확인된 대다수의 다른 APT 공격도 스피어 피싱 이메일을 통해 시작되었다.

III. 스피어 피싱 특성

스피어 피싱은 공격자가 소수의 특정 개인 또는 조직을 공격 목표로 설정하고 공격의 성공 확률을 높이기 위해, 사전에 공격 대상의 개인정보 또는 조직에 대한 정보를 Facebook, LinkedIn, Twitter와 같은 SNS 사이트 등을 통해 수집한다.

대규모 이메일 기반의 피싱 공격은 2010년 11억 건에서 2011년에는 5억건으로 줄었다. 그리고 스팸 메시지는 하루에 3000억건에서 400억건으로 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 공격은 대규모 스팸 메일보다 클릭할 확률이 10배 이상 높다는 통계가 나왔다. 그러나 스피어 피싱 공격의 경비는 1000명 대상 스피어 피싱 비용이 100만 명 대상 일반 피싱 보다 10배나 더 많이 드는 것으로 나타났다[3].

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. 금요일은 대부분의 근무자들이 정신이 해이해져서 피싱에 대한 경계심이 약화된 것이 원인이었다. 그리고 월요일은 주말이후 평소보다 많은 메일을 확인하므로 집중력이 떨어져 스피어 피싱 공격에 취약하다고 판단된다[4].

방화벽, 침입 차단 시스템(IPS), 안티바이러스(AV), 보안 게이트웨이 같은 전통적인 방어 시스템을 효과적으로 우회하는 지능형 악성코드의 파일명으로 사용되는 단어의 특성을 살펴보면 다음과 같다. 배송 서비스는 광범위하게 제공되고, 본질적으로 중요하고 긴급한 경우가 많기 때문에, 사용자는 배송 관련 단어가 들어있는 악성 파일을 대부분 열어 볼 수밖에 없다. 확인, 주의, 통지와 같은 긴급성과 관련된 단어들이 두 번째로 많이 사용된 단어였고, 금융 기관 및 이와 관련된 거래 및 커뮤니케이션에 대한 단어들도 많이 사용되었다[5].

스피어 피싱 공격의 일반적인 특성은 기존의 보안대책을 우회하기 위해서 이메일 스푸핑, 제로데이 취약점 이용, 동적 URL, 그리고 drive-by 다운로드 등의 기술을 혼합하여 사용하는 다중 요소 위협이라는 점이다. 둘째, 사용자 시스템을 통제하기 위해 브라우저, 플러그인, 그리고 응용프로그램의 제로데이 취약점을 이용하여 악성코드를 감염시킨다. 셋째, 공격의 첫 단계는 시스템 감염이고 시스템 감염에 성공한 악성코드는 외부와 통신하여 추가 바이너리를 다운받고, 데이터를 유출하는 다중 단계로 구성된다. 넷째, 스피어 피싱 이메일 위협은 목표가 지정되어 있고, 종종 개인에게 최적화된 메일이어서 스팸 필터가 이러한 스피어 피싱 메일을 탐지할 가능성이 낮다는 점이다[3].

Ⅳ. 기존 스피어 피싱 대응방안

스피어 지능적인 스피어 피싱 공격을 방어하기 위한 보안 대책으로 가장 기본적인 것은 정기적인 보안 교육을 통해 스피어 피싱 공격에 대한 인식을 제고하는 방법이 가장 좋은 방어 대책인 것으로 조사되었다[4]. 두 번째 대응 방안은 직원을 대상으로 스피어 피싱 모의침투 훈련을 실시하는 것이다. 스피어 피싱 메일을 보내 직원의 경각심을 일깨워 주기 위함이다. 이러한 모의침투 훈련을 통해 이메일에 첨부된 파일 또는 URL을 클릭하기 전에 보안 위험에 대해 고려해야 하는 이유를 인식시켜 주어야 한다[6]. 스피어 피싱 공격을 방어하는 가장 중요한 기술적인 보안 통제 방법은 이메일 속에 포함된 URL 링크의 안전성 여부를 점검하는 솔루션을 설치하는 것이다. 인바운드(Inbound) 이메일 샌드박싱(sandboxing) 기술은 웹사이트 컨텐츠와 브라우저 코드를 실시간으로 분석하는 URL 샌드박싱 기술이다[4]. 또 다른 기술적인 대책은 웹 트랙픽의 실시간 분석 및 검사이다. 일부 사용자는 Gmail과 같은 개인 이메일 계정을 통해 악성 링크를 클릭할 가능성이 있다. 이러한 경우에는 스피어 피싱 방어 수단이 웹 트래픽을 모니터링 할 수 없다. 따라서 실시간으로 웹컨텐츠를 분석하여 악의적인 URL을 차단할 필요가 있다. 이러한 기능을 수행하는 웹 보안 게이트웨이의 조건은 지능형이고 실시간 컨텐츠 분석이 가능해야 하며 악성코드 감시 기능과 아웃바운드 콜백(Outbound Callback)을 차단 기능을 포함해야 한다[4]. 또다른 기술적인 대응책은 기존의 보안 장비로 탐지할 수 없는 제로데이 공격을 차단하기 위해 시그니처(signature) 기반이 아닌 능동적 위협차단 솔루션 설치가 필요하다[3].

Ⅴ. 최종 사용자 관점에서 스피어 피싱 대응방안

앞 절에서 언급한 기존의 방어대책으로는 스피어 피싱 이메일을 100% 차단할 수는 없다. 기존의 대응방안의 문제점을 보완하는 좀 더 효과적인 방법을 고려할 필요성이 있다. 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[7]. 이러한 사실로 볼 때, 정기적인 보안 교육과 기술적인 대응책만으로 스피어 피싱 공격에 대응할 수 없다. 스피어 피싱 공격의 특성을 고려하여 최종 사용자 관점에서 스피어 피싱 위협에 대응하기 위한 방안이 필요하다. 먼저, 스피어 피싱 공격의 사전 정보 수집단계에 대응하기 위해 최종 사용자는 SNS 사이트 등 인터넷 공간에 개인 정보를 최대한 적게 공개해야 하며 이에 대한 정기적인 자체 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.

최종 사용자가 스피어 피싱 이메일 여부를 판단하기 위한 점검 가이드라인을 아래와 같이 제안한다[8].

- 자신의 최근 근황 정보와 일치하지만 메일 내용이 타당한지 확인한다. 예를 들면, SNS 사이트에 올린 모임 사진이나 댓글 정보를 바탕으로 친한 친구를 가장하여 안부를 묻는 경우 메일 내용의 타당성을 확인해야 한다.
- 메일을 통해 자료를 받을 것으로 기대한 메일을 받았을 경우 SMS 문자 메시지와 같은 다른 통신수단을 통해 진위 여부를 확인한다. 왜냐하면 공격자가 사용자의 메일 내용을 모니터링하고 있으면서 반드시 열어볼 수밖에 없는 첨부파일을 보내는 경우에 대비할 필요가 있다.
- URL 링크를 클릭하도록 유도하면 먼저 의심하고 인식가능한 주소인지 확인한다.
- 공짜 기대 심리를 이용하는지 확인한다. 즉 이벤트 경품에 당첨되었다는 등의 메일은 열지 않는다.
- 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.

Ⅵ. 결 론

스피어 피싱 공격은 오늘날 보안 관리자를 압박하는 핵심 보안 위협이 되고 있는 반면 스피어 피싱 공격 목표 기관은 대부분 기존의 보안 장치들을 맹신하는 경향이 있다. 따라서 스피어 피싱 공격에 대한 지속적인 관심과 예방 대책이 필요하다. 본 논문에서는 스피어 피싱의 개념, 최신 동향과 특성에 대해 살펴보았다. 그리고 기존의 스피어 피싱 대응 방안에 대해 조사하고 분석한 후, 이를 바탕으로 목표 지향적 공격에 대비하기 위한 최종 사용자 관점에서 효과적인 스피어 피싱 대응방안을 제안하였다.

참고문헌

[1] “Spear-Phishing Email: Most Favored APT Attack Bait”, 「Trend Micro Incorporated Research Paper 2012」
[2] "Ponemon Institute Discovers Majority of Business Leaders Underestimate Risk of Advanced Cyber Threats", http://www.prnewswire.com/news-releases/
[3] FireEye, Inc. White Paper, "Spear Phishing Attacks－Why They are Successful and How to Stop Them"
[4] 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
[5] FireEye, Inc. “FireEye 보고서 : 스피어 피싱 공격에 가장 흔히 사용되는 단어들”
[6] Dave Shackleford , “Social engineering penetration testing: Four effective techniques“, http://searchsecurity.techtarget.com/tip/Social-engineering-penetration-testing-Four-effective-techniques
[7] Bimal Parmar, “Protecting against spear-phishing“, Computer Fraud & Security(January 2012), pp. 8-11
[8] Tracey Caldwell, "Spear-phishing: how to spot and mitigate the menace", Computer Fraud & Security(January 2013), pp. 11-16