J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

피싱 메일 공격조직에 대한 프로파일링 사례 연구

A Profiling Case Study to Phishing Mail Attack Group

이 재 일[1] 이 용 준[2*] 권 혁 진[3]
Jae-il Lee Yong-joon Lee Hyuk-jin Kwon

요 약

최근 국방, 안보, 외교 분야 관련자를 대상으로 하는 피싱 공격이 급증하고 있다. 특히 해킹 공격조직 Kimsuky는 2013년 이후 피싱 공격을 통해 공공기관의 주요 정보 수집을 위한 활동을 하고 있다. 본 논문에서는 피싱 메일 공격조직에 대한 프로파일링 분석을 수행하였다. 이를 위해 피싱 메일 공격의 유형을 분류하고 해킹 공격조직의 공격방식에 대한 분석을 하였다. 상세한 프로파일링 분석을 통해 공격조직의 목적을 추정하고 대응방안을 제시하였다.

☞ 주제어 : 피싱 메일, 해킹, 사이버 공격 그룹, 프로파일링,

ABSTRACT

Recently, phishing attacks targeting those involved in defense, security and unification have been on the rise. In particular, hacking attack organization Kimsuky has been engaged in activities to collect important information from public organizations through phishing attacks since 2013. In this paper, profiling analysis of phishing mail attack organization was performed. Through this process, we estimated the purpose of the attack group and suggested countermeasures.

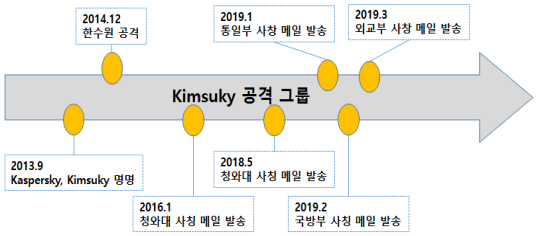
☞ keyword : Phishing mail, Hacking, Cyber Attack Group, Profiling

1. 서 론

2013년 발표된 해외 백신 기업 Kaspersky의 보고서에서 특정 사이버 공격에 사용된 메일계정이 Kimsukyang으로 등록된 것이 확인된 후 Kimsuky로 공격조직을 명명했다. Kimsuky 공격조직은 이메일을 이용하여 사이버 공격을 수행하여 국방, 안보, 외교 분야 관계자로 부터 중요정보를 수집하는 것으로 알려졌다. 공격기법은 정상메일로 위장한 피싱 메일에 악성코드를 은닉하여 보안이 취약한 한글파일을 유포하거나 사회공학적 공격기법으로 관심을 유도하여 계정정보를 수집하는 것이 주요 특징이다[1].

2014년 한국수력원자력에 대한 사이버공격 이후 관련 자료를 공개하며 협박으로 이어진 내부정보 유출사고에 대해 정부합동수사단은 사용된 악성코드의 구성이나 동작 방식이 기존 Kimsuky 공격조직이 사용하는 쉘코드와 유사하고, 사용된 IP가 이전 공격에 사용된 중국 IP대역과 부분적으로 일치한다는 사실을 근거로 공격조직을 Kimsuky으로 잠정 결론을 내렸다.

그림 1과 같이 Kimsuky 공격조직은 지속적으로 국방, 안보, 외교 분야 관계자를 대상으로 지속적으로 사이버 공격을 감행하고 있는 것으로 추정되고 있다.



(그림 1) Kimsuky 공격조직에 의한 사이버공격 사례
(Figure 1) Cases of cyber attacks by Kimsuky attack group

본 논문에서는 2018년 이후 Kimsuky 공격조직이 발송한 피싱 메일, 메일 발송지, 악성코드 유포지의 연관성을 분석

1 KrCERT/CC, Korea Internet & Security Agency, Seoul, 05717, Korea.
2 Department of Cyber Security, Far East University, Chungbuk, 27601, Korea.
3 Research Planning Department, Korea Institute for Defense Analyses, Seoul, 02455, Korea.
* Corresponding author (yjlee4279@gmail.com)
[Received 19 November 2019, Reviewed 21 November 2019(R2 12 January 2020, R3 14 February 2020), Accepted 26 Febuary 2020]

하여 공격조직의 주요 특징과 대응 방법에 대해 제안한다.

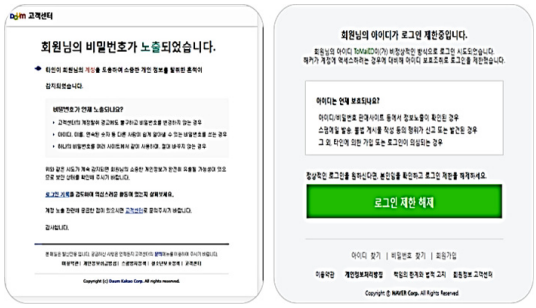
2. 피싱 메일 공격 유형

피싱(Phising)은 개인정보(Private Data)와 낚는다(Fishing)의 의미를 포함하는 이메일을 이용하는 공격기법을 말한다[2]. 공격자가 인터넷 사용자의 정보(기밀, 중요, 개인 등)를 탈취하기 위해 이메일 또는 메신저에 악성코드를 은닉하고 정상적인 내용으로 위장하여 발송하는 방식이다. Kimsuky 공격조직은 피싱 메일을 주요 공격경로로 활용하여 계정정보 탈취, 악성코드 유포 등 사이버공격을 지속적으로 수행하고 있다. 이에 Kimsuky 조직이 활용한 피싱 메일에 대한 연관성을 분석하여 다음과 같이 제시한다.

2.1 위장 이메일

2.1.1 포털사이트 안내메일 피싱 공격

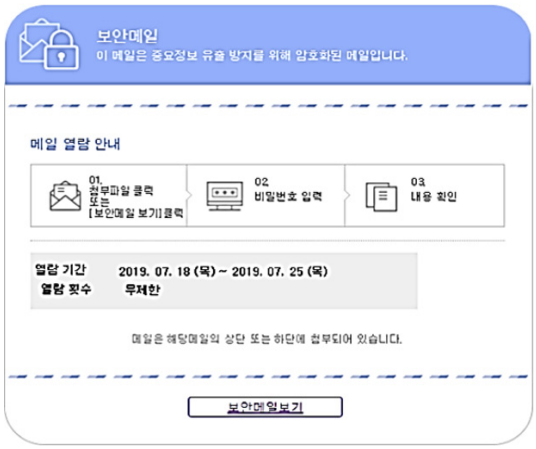
최근 개인정보가 탈취되는 사고가 지속적으로 발생하고 있으며 유출된 개인정보로 계정 도용, 판매 등이 발생하고 있다[3]. 그림 2와 같이 포털사이트에서는 계정에 대한 접속 기록, 비밀번호 변경 기록 등을 사용자에게 안내 메일을 제공하고 있다. 공격자는 이러한 안내메일을 악용하여 포털 사이트 고객센터에서 발송된 메일로 위장하여 계정정보 입력을 유도하는 공격기법을 사용하고 있다. 이는 포털 사이트의 고객센터라는 신뢰할 수 있는 발송자를 사칭한 것으로 전형적인 사회공학적인 공격기법을 사용하고 있다.



(그림 2) 포털사이트 안내메일로 위장한 피싱 공격
(Figure 2) Phishing attack as counterfeit portal reminder mail

2.1.2 보안메일 피싱 공격

최근 피싱 메일을 통한 사이버공격이 증가함에 따라서 메일 본문의 보안강화를 위해 보안메일을 사용하는 기업이 증가하고 있다[4]. 보안메일은 정부, 금융기관 등에서도 많이 사용하고 있는데 공격자는 그림 3과 같이, 보안메일로 위장한 피싱 메일을 발송하고 있다. 보안메일은 특정 비밀번호 입력 후 일치하는 경우에만 메일 본문을 열람할 수 있는데, 피싱 메일의 경우 메일보기 버튼을 누르면 비밀번호 입력 없이 피싱 사이트로 연결하여 계정을 입력하도록 유도하여 계정정보를 획득한 후 첨부파일을 제공한다.



(그림 3) 보안메일로 위장한 피싱 공격
(Figure 3) Phishing attack as counterfeit secure mail

2.2 메일 본문 취약점

공격자는 메일 본문에 취약점을 삽입시켜 열람만 해도 피싱 사이트로 연결될 수 있다. 기존의 방법은 메일 사용자가 링크를 클릭하거나 첨부파일을 열람하는 등의 행위가 필요한데, 메일 본문 취약점을 이용하는 경우 메일 열람 시 숨겨진 악성 스크립트가 바로 실행되어 피싱 사이트로 연결시킨다[5].

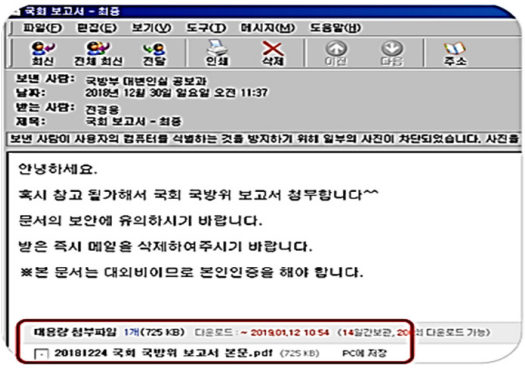
(그림 4) 웹취약점 스크립트가 은닉된 피싱 메일
(Figure 4) Phishing mails using hidden web vulnerability scripts

그림 4와 같이, 메일 열람 시 바로 피싱사이트로 자동 연결되고 공격자는 사용자가 계정정보를 입력하도록 유도한다. 메일 본문 웹취약점으로 공격하는 경우 HTML을 지원하는 웹 메일 또는 메일 프로그램을 이용한다.

2.3 첨부파일 위장

2.3.1 첨부파일 위장을 통한 피싱사이트 연결

공격자는 첨부파일이 있는 것처럼 위장하여 피싱 메일을 발송하기도 한다[6]. 그림 5와 같이, 첨부파일 링크를 클릭하는 경우 공격자가 개설한 피싱 사이트로 연결되어, 사용자에게 계정정보 입력을 유도하는 화면이 표시된다. 일반적으로 첨부파일은 메일 본문에서 바로 다운되지만 대용량 첨부파일의 경우, 별도 사이트에서 다운로드되기 때문에 사용자의 의심을 줄일 수 있다는 점을 악용한 것으로 추정할 수 있다.

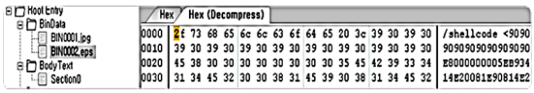


(그림 5) 첨부파일을 위장한 피싱 메일
(Figure 5) Phishing mails using counterfeit attached files

2.3.2 악성코드 은닉 이메일

공격자는 제목과 본문, 첨부 파일명으로 관심을 유도하거나 수신자와 관련된 내용으로 위장하여 악성코드가 숨겨진 압축파일, 한글문서, MS워드 등을 발송한다. 메일 본문에 '첨부파일을 확인 바란다'는 내용을 작성하여 메일을 받은 수신자가 첨부파일을 읽도록 유도한다[7].

그림 6과 같이, 최근 악성코드가 은닉된 한글파일의 대부분이 2017년에 패치가 된 고스트 스크립트 취약점(CVE-2017-8291)을 이용하여 악성코드를 실행시킨다. 2017년 2월 이전 버전의 한글 프로그램 사용자는 첨부된 악성 한글파일 열람 시 취약점으로 인해 악성코드에 감염되며 원격제어, 키로깅, 정보유출 등의 악성 행위에 노출된다[8].



(그림 6) 악성코드가 은닉된 한글파일
(Figure 6) PHWP files containing malicious codes

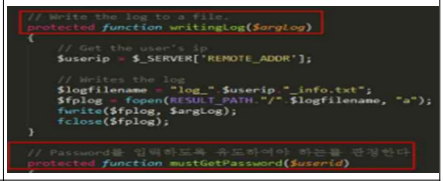
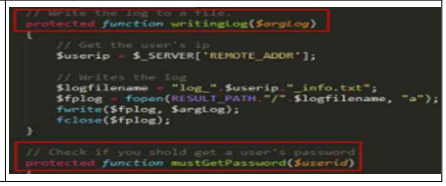
3. 피싱 메일 공격조직(Kimsuky) 프로파일링 사례 분석

3.1 피싱 메일 공격의 공통점

Kimsuky 공격 조직이 악용한 서버를 분석하여 연관성을 분석하였다. 공격자는 동일한 IP로 다수의 웹사이트의 FTP 계정에 접속하여 메일 발송지로 위장하여 피싱 메일을 전송하였다. 또한 특정 계정을 이용해서 메일 발신을 테스트를 하고 유사한 도메인 주소를 사용하였다. 피싱 메일 공격으로 인한 연관성은 다음과 같다.

3.1.1 피싱 사이트 소스코드

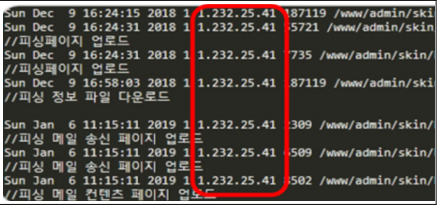
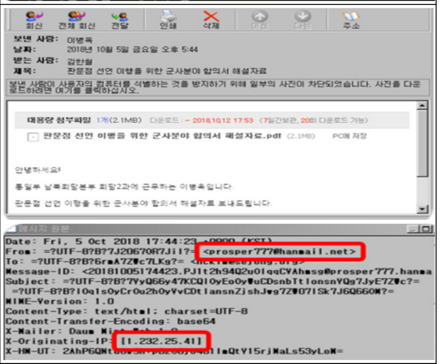
그림 7과 같이, 공격자는 제작한 피싱 사이트에 사용자가 입력한 계정정보를 파일형태로 저장하는데 계정정보 저장 소스코드가 Kimsuky 공격조직이 2014년 한수원, 2019년 포털 사칭 메일에 사용한 소스코드와 유사점이 확인되었다.

분석사례	피싱 페이지 소스코드 비교
2016년 피싱메일 (한수원)	
2019년 피싱메일 (포털)	

(그림 7) 피싱 페이지 소스코드의 유사점 비교분석
(Figure 7) Comparative analysis of similarities in phishing page's source codes

3.1.2 FTP 접속 및 메일 발신지 주소

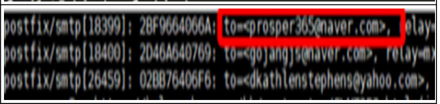
그림 8에서 보듯이, 공격자는 특정 IP를 통해 해킹한 다수의 웹사이트 FTP 계정에 접속하여 피싱 메일을 발신하였다. 이는 공격자가 특정 서버를 경유하여 FTP 접속 및 발송을 선호하기 때문이다.

<table>
<tr><th>주소지</th><th>공격자 경유지 분석</th></tr>
<tr><td>FTP
해킹접속
IP</td><td> 
</td></tr>
<tr><td>피싱메일
발송지
IP</td><td> 
</td></tr>
</table>

(그림 8) FTP 접속 및 메일 발송지 주소의 유사점 분석
(Figure 8) Comparative analysis of similarities in FTP's addresses and Mail's addresses

3.1.3 공격자 메일 계정

공격자는 피싱 메일을 보낼 때 prosper777@○○○.net 메일 계정을 사용하였다. 그림 9와 같이, 이 계정은 피싱 사이트로 악용된 공격자 메일 계정과 동일하였다.

<table>
<tr><th>분석사례</th><th>피싱 페이지 소스코드 비교</th></tr>
<tr><td>피싱메일
발송계정</td><td> 
</td></tr>
<tr><td>피싱사이트
접속계정</td><td> 
</td></tr>
</table>

(그림 9) 피싱사이트 서버 및 피싱메일 발송 계정 분석
(Figure 9) Analyze to connection accounts of phishing servers and phishing mails

또한 피싱 사이트로 악용된 피해 서버는 다른 공격자 계정인 papanda@○○○.net이 확인되었다. papanda 계정은 공격자로부터 발송된 피싱 메일 발송 서버 maillog에서 수신 이력이 있는 것을 확인하였다. 공격자는 실제 피싱 메일 공격을 수행하기 전에 메일이 원활하게 발송되는지 테스트하기 위해 공격자 계정으로 발신 테스트를 한 것으로 추정된다.

공격자는 다수의 메일 발송 서버에서 mail함수를 이용하여 피싱 메일을 발송하는데 공격자 계정으로 테스트를 시도하는 발송 페이지에 PHPMailer 오픈소스 메일 라이브러리를 이용였다. 해당 라이브러리를 사용하면 해당 서버의 SMTP 서비스를 이용하지 않고 외부의 SMTP 서버를 이용하기 때문에 maillog에 남기지 않기 위해 사용한 것으로 추정된다.

3.1.4 피싱 메일 서버 재사용

공격자가 피싱 메일 서버로 해킹하여 악용한 서버는 기존에 악성코드 유포를 위해 해킹한 서버가 재사용 하였다. 공격자는 이전에 악성코드 유포지로 악용되었던 웹사이트 이력을 활용하였다. 이는 해당 피해 서버는 보안이 취약하여 지속적으로 공격자에게 악용되는 것으로 추정된다.

3.1.5 경유지 주소 대역

Kimsuky 공격 조직은 사이버공격을 시도할 때 지속적으로 175.167.x.x IP대역을 사용해왔다. 이 IP 대역은 중국 선양 지역에서 사용되는 대역이며, 한수원, 청와대 사칭 해킹 메일 공격에서도 해당 IP 대역이 사용되었다. 악용된 서버의 FTP 로그, 웹 로그를 분석한 해당 IP 대역의 공격자 IP는 그림 10과 같다.

악용서버	접속IP	수집처	최초 접속시간	Whois
종교 사이트	175.167.146.24	웹로그	2017-10-03	선양
	175.167.130.5	웹로그	2019-02-10	선양
	175.167.154.230	웹로그	2019-02-11	선양
학회 사이트	175.167.138.154	웹 에러로그	2018-08-19	선양
	175.167.130.129	웹 에러로그	2018-08-22	선양
독도 관련 사이트	175.167.128.140	웹로그	2019-03-17	선양
	175.167.128.219	웹로그	2019-03-18	선양
	175.167.136.115	웹로그	2019-03-20	선양
	175.167.136.22	웹로그	2019-03-20	선양
	175.167.144.238	웹로그	2019-03-20	선양
	175.167.144.226	웹로그	2019-03-21	선양

(그림 10) 피해 서버에서 확인한 공격 IP대역
(Figure 10) Attack IP bands on the damaged servers

3.1.6 경유지 호스팅 서비스

공격자가 사용하는 피싱 사이트에 특정 호스팅 서비스가

주로 이용되었다. 해외 호스팅 서비스인 hostinger가 사용되었는데 한국에서 해킹사고 조사를 위한 요청 및 분석이 어렵다. 또한 익명성이 보장되며, 차단되어도 다른 도메인을 개설하여 사용할 수 있기 때문에 주된 경로로 이용한 것으로 추정된다. 그림 11에서 보듯이, 공격자는 hostinger의 무료 도메인 7개를 개설하여 공격에 사용했는데 해당 도메인 목록과 정상사이트와 유사한 주소를 조합하여 도메인을 생성하고 피싱 공격에 사용하였다.

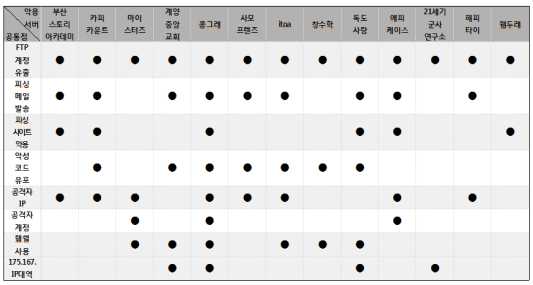
hostinger 무료 도메인 목록			
.esy.es	96.lt	pe.hu	hol.es
16mb.com	000webhostapp.com	890m.com	

(그림 11) 해외 호스팅(hostinger)를 통해 개설한 도메인 목록
(Figure 11) Lists of domain opened through overseas hosting company(hostinger)

3.2 피싱 메일 공격 특징 분석

3.2.1 피싱 메일 피해 서버 연관성 분석

Kimsuky 공격조직이 악용한 서버 분석을 통해 공통점을 확인하였다. 그림 12에서 보듯이, 공격자는 동일한 IP로 다수의 웹사이트의 FTP계정에 접속했을 뿐만 아니라 메일 발송기로 피싱 메일을 전송하였다. 또한 특정 계정을 이용해서 메일 발신 테스트를 하고, 비슷한 형태의 도메인 주소를 사용하였다.



(그림 12) 피해 서버의 연관성 분석
(Figure 12) Comparative analysis of similarities in the damaged servers

3.2.2 공격 조직의 주요 특징

국내·외 전문보안기업은 위와 같은 피싱 사이트, 악성코드 등을 분석하여 국방, 안보, 외교 등의 민감하고 중요한 정보를 수집하고자 하는 공격조직으로 Kimsuky로 판단하고 있으며 피싱 메일 공격 분석을 통한 특징은 다음과 같다.

첫째, 대부분의 악용된 서버에 대해 FTP계정으로 실패 없이 로그인에 성공한 것으로 보아, 유출된 FTP계정을 통해 서버 접근을 시도하는 것으로 추정된다.

둘째, 메일 발송기, 피싱 사이트, 악성코드 등을 FTP를 통해 업로드 하며, 입수한 계정정보는 동일한 FTP를 통해 다운로드 하였다.

셋째, 피싱 메일 발송지 및 피싱 사이트로 악용된 서버 중 일부에 추가로 악성코드를 업로드하여 유포한다.

넷째, 악성코드의 대부분이 원격제어 보다는 정보수집, 키로깅에 집중되어 공격자는 금전적인 목적 보다 특정한 중요 정보 수집이 목적인 것으로 추정된다.

다섯째, 지속적으로 새로운 피싱 페이지를 생성하고 제로데이 등을 이용한 피싱 페이지 연결과 같은 다양한 방식을 사용하고 있다.

4. 피싱 메일 공격의 목적 및 대응 방안

4.1 피싱 메일 공격의 목적

최근의 피싱 사이트는 고객센터, 대용량 첨부파일 위장, 취약점을 이용한 피싱 페이지 유도와 같은 다각화하여 이용자의 계정이 지속적으로 유출하고 있다.

공격자가 피싱 메일을 발송한 목적은 악성코드 유포 및 계정정보 탈취였다. 인터넷상에 공개된 메일 주소로 피싱 메일을 발송하여 개인정보와 계정정보 탈취를 목적으로 하고 있다.

피싱 메일의 발송지 위조는 포털 사이트 고객센터 위장과 공격대상에 관련 있는 공공기관, 기업으로 위장하는 두 가지 방식이다. 포털 사이트 위장은 메일 주소 수집이 쉽고 즉시 발송할 수 있으나 메일 이용자가 의심할 수 있어 성공률이 낮다. 공공기관, 기업으로 발신지를 위장할 경우 공격대상과 관련된 내용으로 메일을 위조하기 위해 추가적인 정보 수집을 해야 하지만 높은 공격 성공률을 보이고 있다.

4.2 피싱 메일 공격 대응 방안

4.2.1 이메일 서비스 제공자

이메일 서비스 제공자는 우선적으로 피싱 메일 공격자로부터 해킹되지 않도록 보안강화가 필요하다. 분석을 통해 피싱 공격조직이 주로 FTP 계정 정보를 수집하여 해킹하기 때문에 FTP 계정에 대한 강화된 인증이 요구된다. 추가적으로 원격으로 FTP에 접속하지 않도록 망분리를 하며 지속적

으로 FTP 이력에 대한 관리가 필요하다. 또한 메일 서버에 외부로부터 접속을 차단하기 위해 방화벽을 구축하여 인증되지 않은 외부로 부터의 접속을 차단해야 한다. 특히 공격조직이 외부 호스팅업체 도메인을 사용하고 있어 방화벽에서 중국, 해외 호스팅 도메인에 대한 차단 정책이 필요하다.

공격자는 FTP 계정 이외에도 보안이 취약한 웹사이트를 해킹하여 악용하였다. 따라서 웹 서비스 제공자는 웹 메일 접속을 통한 공격자의 해킹을 차단하기 위해 웹방화벽을 구축하여 악성스크립트 삽입 등의 외부 공격으로부터 차단이 필요하다. 해킹조직이 유사한 악성스크립트를 재사용하는 특성을 고려하여 웹방화벽에 해당 탐지패턴을 등록하여야 한다.

피싱 메일 공격자는 메일 본문에 웹취약점을 이용한 스크립트를 사용하였다. 따라서 메일 서비스 운영자는 메일 서비스가 해킹되어 공격자에 의한 피싱 메일 발송을 대비하여 메일 열람 페이지에 XSS(Cross Site Scripting Vulnerability) 취약점 발생을 방지하기 위한 시큐어 코딩으로 검증한 이후에 메일 서비스를 제공해야 한다.

4.2.2 이메일 서비스 이용자

이메일 이용자에게는 피싱 메일을 방지하기 위해 사회공학적 방법에 대한 인식제고가 필요하다. 우선적으로 계정관리를 철저히 해야하며 이메일 비밀번호는 '영문 대·소문자 + 숫자 + 특수문자'를 포함하는 9자리 이상으로 3개월에 1회 변경을 하며 필요시 SMS, OTP 등을 이용한 2단계 인증 로그인 설정을 한다. 계정 유출 예방을 위해 해외 로그인 차단 기능을 설정하고 로그인 이력을 수시로 점검한다.

메일에 파일이 첨부되어 있거나 외부 링크가 있는 경우 이메일 열람전에 메일 발송 주소가 정상적인 주소인지 확인하고 기존에 메일 발신자와 이력이 있었는지 재확인한다.

이메일에 첨부한 파일은 다운로드 되기 전에 이용자의 계정 입력 등을 요구할 경우 차단하며 악성코드로 악용되는 한글, 오피스, PDF문서는 최신 버전으로 패치하여 관리한다.

메일 본문에 외부 사이트로 링크가 있는 메일은 링크를 클릭하지 않고 새로운 창으로 정상 사이트 여부를 확인하고 접속한다.

5. 결 론

본 논문에서는 최근 급증하는 국방, 안보, 통일 분야 관련자를 대상으로 하는 피싱 공격조직을 분석하였다. 해킹공격조직 Kimsuky는 2013년 이후 피싱 공격을 통해 공공기관의 주요 정보 수집을 위한 활동을 하고 있다.

2018년 이후에는 포털사이트의 고객센터로 위조하거나 국방, 정부 조직을 사칭하는 이메일로 위조하는 전형적인 사회 공학적인 공격기법을 사용하고 있다.

본 논문에서는 피싱 메일 공격조직에 대한 프로파일링 사례 분석을 통해서 피싱 메일 공격의 유형을 분석하고 공격조직의 목적에 대해 분석하였다. 피싱 공격조직은 금전적 목적이 아닌 피싱 사이트, 악성코드 등을 유포하여 국방, 안보, 외교 등의 중요한 정보를 수집하고자 하는 공격으로 추정한다.

추가적으로 사회적 공격방식은 피싱 메일을 대응하기 위한 메일 서비스 제공자, 메일 이용자에 대한 대응방안을 제시하였다.

참고문헌(Reference)

[1] V. Suganya, "A review on phishing attacks and various anti-phishing techniques", Int. Journal of Computer Applications, vol. 139, pp. 20-23, 2016. https://doi.org/10.5120/ijca2016909084

[2] K. L. Chiew, K. S. C. yong and C. Tan, "A survey of phishing attacks: their types, vectors and technical approaches", Expert Systems with Applications, vol 106, pp. 1-20, 2018. https://doi.org/10.1016/j.eswa.2018.03.050

[3] I. Qabajeh, F. Thabtah and F. Chiclana, "A recent review of conventional vs. automated cybersecurity anti-phishig techniques", Computer Science Review, vol. 29, pp. 44-55, 2018. https://doi.org/10.1016/j.cosrev.2018.05.003

[4] Y. J. Lee, C. B. Lee, "An Fingerprint Authentication Model of ERM System using Private Key Escros Management Server", Journal of The Korea Academia Industrial cooperation Society, 20.6, 1-8, 2019. https://doi.org/10.5762/KAIS.2019.20.6.1

[5] J. Y. Kim, S. J. Bu and S. B. Cho, "Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders", Information Sciences, vol. 460, pp. 83-102, 2018. https://doi.org/10.1016/j.ins.2018.04.092

[6] J. Ma, L. K. Saul, S. Savage and G. M. Voelker, "Beyond blacklists: learning to detect malicious web sites from suspicious URLs", In Proc. of the 15th ACM SIGKDD Int, Conf. on knowledge Discovery and Data Mining, pp. 1245-1245, 2009.
https://doi.org/10.1145/1557019.1557153

[7] Y. J. Lee, T. Y. Jeon, "A Malware Detection Method using Analysis of Malicious Script Patterns", Journal of The Korea Academia Industrial cooperation Society, 20.7, 613-621. 2019.
https://doi.org/10.5762/KAIS.2019.20.7.613

[8] R. Verma and K. Dyer, "On the character of phishing URLs: Accurate and robust statistical learning classifiers", In Proc. of the 5th ACM Conf. on Data and Application Security and Privacy, pp. 111-122, 2015.
https://doi.org/10.1145/2699026.2699115

◐ 저 자 소 개 ◑

이 재 일(Jae-il Lee)
1986년 서울대학교 계산통계학과(이학사)
1988년 서울대학교 자연과학대학원 계산통계학과(이학석사)
2006년 연세대학교 공학대학원 컴퓨터과학과(공학박사)
1996년~현재 한국인터넷진흥원 사이버침해대응본부장
관심분야 : 정보보호, 융합보안
E-mail : leeji@kisa.or.kr

이 용 준(Yong-joon Lee)
2005년 숭실대학교 컴퓨터학과(공학박사)
2006년~2009년 LG CNS 기술연구부문 부책임연구원
2010년~2015년 한국인터넷진흥원 사이버침해대응본부 수석연구위원
2016년~2019년 국방보안연구소 정보보호실 디지털포렌식연구관
2020년~현재 극동대학교 사이버보안학과 조교수
관심분야 : 산업보안, 사이버보안, 내부정보유출차단
E-mail : yjlee4279@gmail.com

권 혁 진(Hyuk-jin Kwon)
1989년 성균관대학교 산업공학과(공학사)
1991년 성균관대학교 대학원 산업공학과(공학석사)
2000년 성균관대학교 대학원 산업공학과(공학박사)
1991년 3월~2017년 12월 한국국방연구원
2017년 12월~현재 국방부 정보화기획관실
관심분야 : 정보보호, 정보보안경영체계, 정보화평가
E-mail : k1253@mnd.go.kr