Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.2, Apr. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.2.313

내부 네트워크에서 알려지지 않은 피싱사이트 탐지방안

박 정 욱,[1†] 조 기 환[2‡]
[1]전라북도교육청, [2]전북대학교

A Unknown Phishing Site Detection Method in the Interior Network Environment

Jeonguk Park,[1†] Gihwan Cho[2‡]
[1]Jeollabukdo Office of Education, [2]Chonbuk National University

요 약

피싱 공격이 지속적이고 다양하게 증가하고 있지만 대응방안은 아직도 공격을 식별한 이후에 방어하는 형태에 머무르고 있다. 공격 이전에 HTTP의 Referer 헤더필드를 이용한 피싱사이트 탐지방안이 제안 되었으나, 피싱의 표적이 될 사이트 마다 개별적인 트래픽 수집 시스템을 설치해야하는 한계점이 존재한다. 본 논문은 내부 네트워크에서 기존에 알려져 있지 않은 피싱사이트에 접속하는 것을 탐지하는 방안을 제안한다. 사용자가 피싱사이트에 접속할 때 발생하는 트래픽을 HTTP 프로토콜의 특성과 피싱사이트 특성을 바탕으로 전처리를 수행한다. 피싱으로 의심되는 사이트는 컨텐츠를 분석하는 피싱사이트 판단단계를 통해 탐지된다. 제안된 탐지방안은 100개의 피싱 URL과 100개의 정상 URL을 대상으로 두 가지 형태의 실험으로 검증하였다. 실험결과 피싱 URL의 탐지율은 66%, 정상 URL에 대한 오탐율 0%로 나타났으며, 이는 기존에 제안된 탐지방안에 비해 알려지지 않은 피싱사이트를 탐지하는데 높은 탐지율을 보인다.

ABSTRACT

While various phishing attacks are getting to be increased in constant, their response methods still stay on the stage of responding after identifying an attack. To detect a phishing site ahead of an attack, a method has been suggested with utilizing the Referer header field of HTTP. However, it has a limitation to implement a traffic gathering system for each of prospective target hosts. This paper presents a unknown phishing site detection method in the Interior network environment. Whenever a user try to connect a phishing site, its traffic is pre-processed with considering of the characteristics of HTTP protocol and phishing site. The phishing site detection phase detects a suspicious site under phishing with analysing HTTP content. To validate the proposed method, some evaluations were conducted with 100 phishing URLs along with 100 normal URLs. The experimental results show that our method achieves higher phishing site detection rate than that of existing detection methods, as 66% detection rate for the phishing URLs, and 0% false negative rate for the normal URLs.

Keywords: Phishing Site Detection, HTTP, White List, Interior Network

I. 서 론

피싱 공격은 사용자의 개인정보 중 민감정보를 탈취하기에 손쉽고 효과적인 방법으로 알려져 있다. 피싱은 일반적으로 신뢰할 수 있는 웹 사이트를 사칭하여 사용자의 개인정보(특히, 금융정보)를 탈취하는 형

접수일(2015년 1월 6일), 수정일(2015년 3월 12일),
게재확정일(2015년 3월 13일)

† 주저자, zsvei@jbnu.ac.kr
‡ 교신저자, ghcho@chonbuk.ac.kr(Corresponding author)

태로 구성 된다. 전 세계적으로 피싱사이트는 2014년 2분기에만 128,378개가 발견되었으며, 이는 APWG(Anti-Phishing Working Group)가 피싱에 대해 통계를 작성한 2004년 이후로 2번째로 많은 수치이다[1].

국내의 경우, 경찰청과 KISA에서 발표하는 피싱사이트 차단건수를 살펴보면, 2013년에는 총 7,999개였으나, 2014년에는 상반기에만 6,263개로 급증하는 추세에 있다[2]. 피싱사이트는 증가와 더불어 그 목표도 다양해지고 있다. 2013년에는 피싱사이트 대부분이 금융권사이트를 사칭 하였으나, 2014년 상반기에는 정부·공공기관의 웹사이트를 사칭하는 비율이 약 35%로 증가하였다. 이는 피싱사이트 공격대상이 금융 및 결제영역에서 다양한 영역으로 확대 되는 것을 보여준다.

공격유형은 Table 1.과 같이 DNS 변조를 기반으로한 파밍(pharming), 문자메시지(SMS)를 이용한 스미싱(smishing), 특정 타겟을 대상으로 이루어지는 스피어 피싱(spear phishing) 등으로 다양해지고 있다. 각각의 공격은 분리되거나 서로 연계하여 피싱을 유도하며 각종 범죄에 악용되고 있다.

이처럼 피싱사이트 공격이 공격 범위를 넓혀가며 다수의 사용자에게 정신적, 금전적 피해를 일으키고 있다. 특히 정부·공공기관의 내부 사용자가 피싱사이트 등의 공격을 받았을 때의 피해는 그 규모를 산정하기 어렵다.

기존 피싱사이트 대응은 공격이 발생되고 난 사후에 방어하는 형태(블랙리스트 추가)로 이루어지고 있다. 이는 알려져 있지 않은 피싱사이트에 내부 사용자가 접속을 시도할 때 탐지할 수 있는 방안이 없으며, 피싱사이트의 생명주기(2~3일)를 고려했을 때 효과성이 미비하다.

본 논문에서는 정부·공공기관 내부에서 외부인터넷과 물리적인 분리 없이, 라우터와 보안스위치, 침입차단시스템, 침입탐지(방지)시스템 등을 통하여 접근통제하여 운용하고 있는 업무용 내부네트워크(행정전산망 등)에서 활용할 수 있는 피싱사이트 탐지 방안을 제안한다.

Table 1. Type of phishing attacks

	attack induction method	type of attack
1	e-mail	spear phishing
2	website	phishing Site
3	SMS	smishing
4	DNS spoofing	pharming
5	voice	voice phishing
6	instant messenger	messenger phishing
7	QR code	qshing

효과적인 탐지를 위해, 내부 사용자가 웹 사이트에 접속할 때 발생하는 트래픽(traffic)을 수집한다. 수집된 트래픽의 HTTP Referer와 Host 정보를 추출하고 화이트리스트와 비교하여 피싱으로 의심되는 사이트를 분류하는 전처리단계를 수행한다. 분류된 사이트는 TF-IDF[3]기반으로 컨텐츠를 분석하고, 검색엔진을 통해 검색한 결과로 피싱사이트 여부를 최종 판단한다.

2장에서는 피싱사이트 탐지를 위한 관련 연구동향을 살펴보고, 3장에서는 최근 발생하는 피싱사이트의 특성을 바탕으로 HTTP 프로토콜의 특성을 이용한 피싱사이트 탐지 방안을 제안한다. 4장에서는 제안된 탐지방안을 두 가지 형태의 실험을 통해 알려지지 않은 피싱사이트를 탐지의 효과성 분석하고, 5장에서는 결론을 맺는다.

II. 관련 연구

피싱 사이트를 탐지하는 방법은 일반적으로 블랙리스트(blacklist)와 휴리스틱(heuristics)으로 나눌 수 있다. 블랙리스트 탐지기술은 피싱 사이트로 알려진 서버의 주소를 블랙리스트에 등록하여 탐지하는 방법으로 구현이 간편하여 보편적으로 사용하고 있다. 하지만 블랙리스트 탐지 방법은 업데이트 정도에 따라 성능이나 안정성이 떨어질 수 있다[4].

블랙리스트 기술을 사용하는 솔루션은 인터넷진흥원(KISA)의 웹체크[5]가 있으며, 네이버툴바, 알툴바 등도 안티피싱 기능을 제공하고 있다[6, 7]. 해외의 경우는 마이크로소프트의 인터넷 익스플로러(internet explorer) 9에서 제공되는 스마트스크린 필터(smart screen filter)[8], 구글의 세이프브라우징(safe browsing)[9] 등이 있다.

휴리스틱 기술을 기반으로한 피싱 사이트 탐지 방법은 피싱사이트에서 발견할 수 있는 특징을 바탕으로 한 다양한 분야의 연구가 진행되었다. 참고문헌[10]는 SpoofGuard라는 휴리스틱을 기반으로한 Plug-in을 제안하였다. SpoofGuard는 비연결형 페이지(Stateless page), 연결형 페이지(Stateful page), post data 평가(evaluate)를 대상으로

Spoof Score를 산출하여 피싱사이트를 탐지한다.

참고문헌[11]은 플러그인 형태의 피싱탐지 솔루션 9종에 대해 비교 평가를 진행하였다. 휴리스틱을 기반으로 한 6종은 60% ~ 90%의 높은 탐지율을 나타냈다. 반면 블랙리스트 기반의 솔루션은 50%이하의 낮은 탐지율을 나타냈다.

참고문헌[12]는 피싱사이트의 URL 구조를 분석하여 피싱사이트를 탐지하는 방법을 제안하였다. 하지만 공격자가 URL 패턴을 변경하면 탐지율이 저하될 수 있는 단점이 존재 한다.

참고문헌[3]은 텍스트 마이닝(text mining)에서 주로 활용하는 TF-IDF(Term Frequency - Inverse Document Frequency)를 기반으로 하여 용어의 빈도와 로버스트 하이퍼링크(robust hyperlinks)를 이용하여 피싱사이트를 탐지한다.

기존 연구방법은 웹브라우저 플러그인 형태의 피싱 탐지 솔루션[3, 10, 11, 12]으로, 네트워크 기반에 비해 피싱 사이트 탐지율이 높은 반면에 플러그인 설치에 따른 리소스 사용과 추가적 관리가 필요하여, 정부·공공기관의 내부네트워크 관리자에게 효과적인 해결책이 아니다.

참고문헌[13]은 피싱사이트가 원시 사이트의 이미지나 컨텐츠 등을 링크하여 사용하는 특성을 기반으로 하여 원시사이트로 유입되는 HTTP Referer를 수집하여 실시간으로 탐지하는 방안을 제안하였다. 특정 사이트를 대상으로 하여 6일간 40개의 피싱사이트를 탐지 하여, HTTP Referer를 기반으로 한 피싱사이트 탐지의 효과성을 증명하였다.

하지만 피싱의 표적이 되는 사이트 마다 개별적인 트래픽 수집 시스템을 설치해야하는 한계점이 존재한다. 이는 설치대상을 국내로 한정을 한다 하더라도, 수백 사이트 이상 될 것으로 판단되며, 이는 현실적으로 실현가능성이 없다. 또한 어느 사이트가 피싱사이트의 표적이 될지 예측하는 것이 불가능하기 때문에 선별적인 설치가 불가능하고, 해당 시스템이 설치가 되지 않은 사이트를 표적으로 한 피싱사이트는 탐지가 불가능하게 된다.

본 논문에서는 트래픽 수집 위치를 원시사이트에서 사용자 단으로 변경하여 이러한 단점을 보완 한다. 사용자가 인터넷 사이트 접속 시 발생하는 트래픽의 헤더정보의 HTTP Referer와 Host를 화이트리스트 기반으로 분석한다. 오탐을 방지하기 위해 화이트리스트, TF-IDF를 통해 컨텐츠를 분석하고 피싱사이트로 판단한다.

III. 피싱사이트 탐지 방안

3.1 피싱사이트의 탐지 전략

다양한 연구를 통해 피싱사이트 탐지 기법이 발전함에 따라, 피싱사이트의 생명주기(lifecycle)가 이전에 비해 짧아지고 있다. 반면에 탐지를 피하기 위해 피싱사이트의 완성도는 더욱 높아지고 있다. 이런 이유로 해커들은 사이트 제작소요시간을 줄이고, 사용자의 의심을 피하기 위해 피싱사이트 제작 시 원시사이트의 이미지를 참조하여 그대로 이용하거나, 원시사이트로 연결되는 하이퍼링크를 다수 생성하고 있다.

Fig.1.은 원시사이트의 이미지를 직접 참조해서 제작된 피싱사이트를 사용자가 접속하는 시나리오를 통해 HTTP Referer와 Host의 정보를 설명하고 있다. 원시사이트를 참조하는 방식으로 제작된 피싱사이트를 사용자가 접속(Fig.1.의 ①)하게 되면 사용자의 브라우저는 피싱사이트에서 전송해주는 HTML을 해석하게 되고 Fig.1.의 ②와 같이 원시사이트의 이미지를 참조하게 된다. 요청(Fig.1.의 ③) 을 받은 원시 사이트의 웹서버는 해당 이미지 정보를 전송하면서, RFC2616(HTTP/1.1)[14]에 정의된 HTTP Referer, Host 등의 필드를 함께 전송한다.

HTTP Referer 정보를 통해 해당 요청이 어떠한 소스 URL에서 참조되었는지 확인이 가능하며, HTTP Host를 통해 이미지를 제공하고 있는 서버의 정보를 확인할 수 있다. 이러한 특성을 바탕으로 원시사이트에서 이미지 전송 시 발생하는 트래픽을

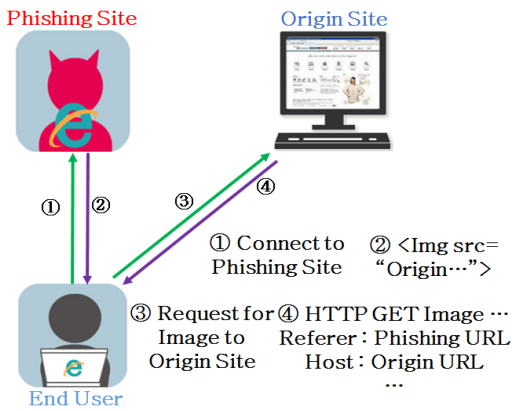

Fig. 1. The concept of HTTP Referer and Host in HTTP 1.1

분석함으로써 피싱사이트 접속을 탐지할 수 있다.

3.2 피싱사이트 탐지를 위한 환경 구성

3.2.1 내부 네트워크

내부 네트워크는 정부·공공기관에서 구성하여 운영하고 있는 네트워크로 외부 인터넷과 물리적인 분리 없이, 보안스위치, 침입차단시스템, 침입탐지(방지)시스템 등을 통하여 접근통제하여 운영하고 있는 네트워크이다.

내부 네트워크는 기관내부의 보안정책에 따라서 특정 웹사이트 접속을 제한하거나 외부의 악의적인 트래픽이 내부네트워크로 접속하는 행위의 제어가 가능하다.

3.2.2 트래픽 수집

피싱사이트 탐지를 위해서 내부 사용자가 외부사이트 접속 시 발생하는 HTTP Header 정보의 수집이 필요하다. 특히 원시사이트를 참조하여 생성된 피싱사이트를 접속할 때 원시사이트에서 사용자에게 전송하는 정보 인 HTTP Referer와 Host 정보의 포함 유무를 확인하여야 한다.

본 논문에서는 피싱사이트 탐지를 위해 필요한 트래픽 수집 시스템을 Fig.2.와 같이 구성하여, 사용자가 외부의 인터넷에 접속할 때 경유하는 내부 네트워크의 스위치 포트를 미러링(mirroring)한다. 이는 내부 사용자의 정보를 수집하기에 적합하면서 네트워크에 발생하는 부하를 최소화 할 수 있다.

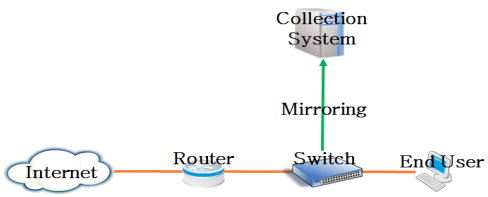

Fig.2. The configuration of traffic collection system

3.3 탐지정보의 구성

3.3.1 수집정보 구성

수집정보는 트래픽을 기반으로 피싱사이트를 탐지하기 위해, 접속 요청자인 Src IP와 목적지 정보인 Dst IP, 접속 시점인 시간(time)으로 구성한다. 또한 HTTP 프로토콜의 링크 요청주소와 제공주소인 Referer와 호스트 정보를 포함한다. 수집정보 구성은 Table 2.에 제시하였다. 이는 내부 네트워크의 부하가 없는 탐지를 위한 최소한의 정보이다.

Table 2. The collected information

field name	role
src ip	user ip
dst ip	phishing or origin site ip
time	access time
referer	request site URL
host	origin site URL

3.3.2 화이트리스트 구성

기존 연구방법들이 블랙리스트를 기반으로 하여 탐지하는 것과는 다르게 제안한 방안은 화이트리스트(whitelist)를 기반으로 피싱사이트를 탐지한다.

화이트리스트는 피싱사이트 탐지와 오탐율 개선을 위한 두 가지 용도로 이용한다. 첫째는 사용자에게 전송되는 HTTP Host 정보의 피싱사이트 공격대상 포함 유무를 화이트리스트를 기반으로 판단한다. 이는 피싱사이트 탐지의 기반을 제공한다. 두 번째는 HTTP Referer 정보의 정상사이트 여부를 화이트리스트로 판단한다. 화이트리스트에 포함되어있다면, 이는 정상사이트로 분류하여 오탐을 예방할 수 있다.

화이트리스트는 별도로 추출한 Referer 및 Host와 비교를 위해 유효도메인[15]만을 이용하여 구성한다. 화이트리스트에 등록되는 사이트는 국가기관 및 공공기관, 금융기관, 포털사이트 등 신뢰할 수 있고, 피싱의 대상이 될 수 있는 모든 사이트를 포함한다.

3.4 피싱사이트의 탐지

3.4.1 수집데이터의 전처리

수집정보는 HTTP POST와 GET인 형태의 정보만 필터링 하여, 클래스배열 Dx에 저장한다. 클래스 배열인 D는 각각의 HTTP Referer 정보인 referer와 호스트(host) 정보인 host, 피싱사이트 구분자인 flag를 변수로 포함한다. flag 값은 1, 0으로 구성하며, 1은 피싱사이트 의심, 0의 값은 정

상사이트로 구분한다. 수집정보의 전처리를 위해 화이트리스트는 배열 W에 구성한다.

$$D = (d_1, d_2, \cdots, d_n)$$

Variable {
referer : String
host : String
flag : int (1, 0)
}

Referer와 Host가 동일한 경우 대형사이트의 내부 참조로 판단하여, flag를 0으로 처리 한다. flag 정보가 0인 정보는 피싱사이트 판단단계를 처리하지 않고 종료한다.

Referer 필드가 W에 포함되어있는 경우 역시 flag를 0으로 처리하며, Referer 필드가 W에 포함되어있지 않으면서, Host 필드가 W에 포함되어있는 경우 flag를 1로 처리 한다. 전처리 절차는 Fig.3.에 제시하였다.

이는 피싱사이트는 화이트리스트에 포함되어있지 않으며, 공격의 대상이 정부기관이나 은행, 포털사이트 등 신뢰된 사이트라는 것에 기반을 둔 접근법이다. Fig.3.의 전처리 단계를 통해 flag가 1인 피싱의심 사이트는 3.4.2의 피싱사이트 판단 절차를 수행한다. 이 절차를 통해 정상사이트를 피싱사이트로 오인하는 오인 탐지를 감소시킨다.

```
1: input: Dx, x∈{1,2,⋯, n}
2: if (Dx.referer == Dx.host) then
3:   Dx.flag = 0
4: else
5:   if (Dx.referer in W) then
6:     Dx.flag = 0
7:   else
8:     if (!Dx.host in W) then
9:       Dx.flag = 0
10:    else
11:      Dx.flag = 1
12:    end if
13:  end if
14: end if
```

Fig.3. The preprocess of collected information

3.4.2 피싱사이트 판단

전처리 단계를 통해 피싱 의심사이트(*D*x.flag == 1)는 피싱사이트 판단 절차를 수행한다. *D*x.referer의 값을 국내의 검색엔진을 이용하여 검색한다. 결과가 존재할 경우 정상사이트로 판단하여, *D*x.flag 값을 0으로 변경 한다. 검색결과가 존재하지 않을 경우 피싱사이트 최종 판단을 위해, *D*x.referer의 값을 통해 해당 사이트에 접속하여 컨텐츠를 파싱한다.

파싱한 컨텐츠는 CANTINA[3]에서 제안한 탐지 방법을 활용하여 처리한다. CANTINA는 구문 분석을 통해 TF-IDF점수가 높은 5개의 단어를 어휘서명(lexical signature)으로 선택하여, 검색엔진의 검색결과의 유무로 피싱사이트를 판단하는 기법이다. 검색 결과가 없을 경우 피싱사이트로 판단하고 블랙리스트에 추가하며, 검색결과가 존재할 경우

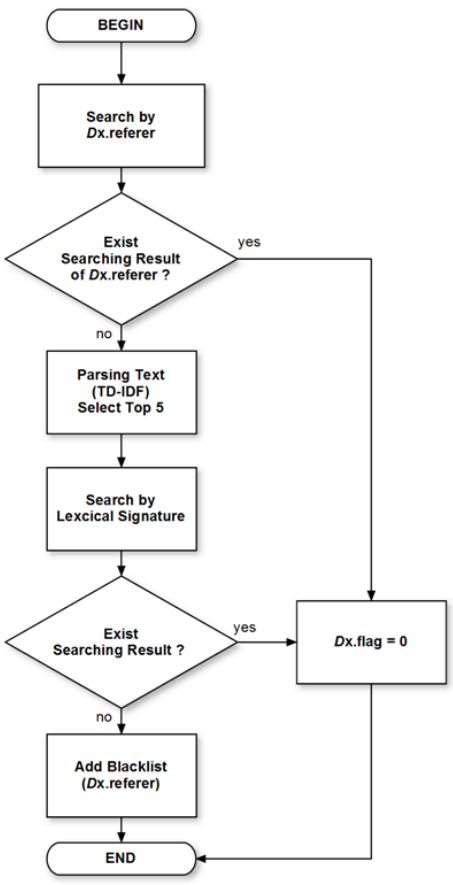

Fig.4. The phishing site detection procedure

*D*x.flag를 0으로 변경한다.

IV. 실 험

4.1 실험 구성

본 논문에서는 제안한 탐지방안의 효과 검증을 위해 피싱URL 100개와 정상URL 100개를 이용하여 실험을 진행한다. 피싱URL은 2014년 11월 6일 ~ 11월 7일 사이에 OpenDNS[16]의 PhishTank를 통해 보고된 피싱URL 목록에서 무작위로 선택하였다. 피싱사이트의 수명을 고려하여 모든 피싱URL은 6시간 이내에 보고된 사이트로 구성한다.

정상URL은 Mediachannel[17]의 Rankey의 2014년 11월 4일 기준의 인터넷, 쇼핑, 뉴스, 금융 등 영역의 중소형 사이트 중 임의적으로 선택한 100개의 사이트를 사용한다. 정상URL은 본 논문에서 화이트리스트로 사용되지만, 탐지 방안의 검증을 위해 실험은 화이트리스트에 등록한 경우와 등록하지 않은 경우로 나뉘어 진행한다.

4.2 실험 결과

실험은 두 가지 형태로 진행하였다. 첫 번째 실험은 3.4.1의 전처리 단계와 3.4.2의 피싱사이트 판단단계의 효과성을 비교 검증하기 위해 진행하였다. 피싱URL을 대상으로 기존 연구에서 제안된 툴바 형태의 피싱사이트 탐지 방법인 네이버툴바, 알툴바, 스마트스크린필터[6, 7, 8]와 비교하는 방법으로 진행하였다. 각각을 정탐율과 오탐율로 나뉘어 비교하였다.

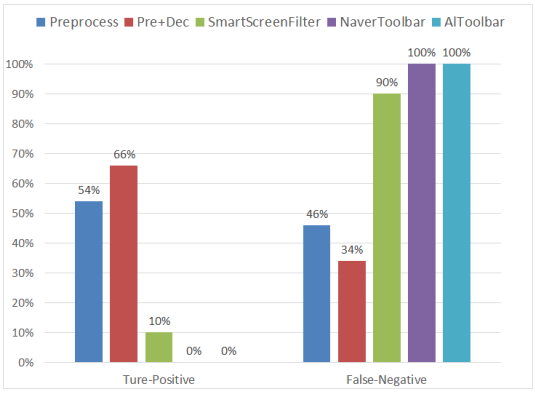

Fig.5. Detection rate of phsihing URL in comparison of preprocess, pre+dec, SmartScreenFilter, NaverToolbar, Altoolbar

전처리 단계만을 적용하였을 때 피싱사이트의 탐지율은 54%로 나타났다. 피싱사이트 판단단계를 함께 적용할 경우 탐지율은 66%로 나타났다. 이는 기존의 탐지방법인 스마트 스크린 필터[9]와 네이버툴바, 알툴바[7, 8]의 탐지율과 대조되는 결과이다. 기존 탐지방법은 블랙리스트를 기반으로 하고 있어, 알려져 있지 않은 피싱사이트를 탐지하는데 어려움이 있다. 반면 본 논문에서 제안된 방안은 알려지지 않은 피싱사이트의 접속을 탐지하는데 효과가 있는 것을 보여준다.

두 번째 실험은 본 논문에서 제안한 탐지방안의 경우 오탐이 발생하지 않지만, 피싱사이트 판단단계와 화이트리스트 사용의 필요성을 검증하기 위해 진행하였다.

전처리 단계만을 적용하였을 경우 정상URL을 피싱URL로 인식하는 비율은 78%로 나타났으며, 정상적인 URL로 인식하는 비율은 21%로 낮게 나타났다. 피싱사이트 판단단계만을 적용하면 정상탐지율은 69%로 나타났으며, 전처리단계와 판단단계를 함께 적용하면 78%의 정탐율을 보였다.

화이트 리스트에 정상URL을 추가할 경우 100%의 정탐율을 보였으며, 오탐은 나타나지 않았다. 이는 기존에 알려져 있는 정상사이트의 경우 제안된 방안으로 탐지하는 것에 문제가 없으며, 알려져 있지 않은 정상 사이트의 경우도 정상적으로 식별할 수 있음을 보여준다.

두 종류의 실험을 통해 제안된 방안이 내부 네트워크 내부의 사용자가 기존에 알려지지 않은 피싱사이트의 접속을 탐지하는데 좋은 방안이 될 수 있음을 보여준다. 그러나 이미지 등을 다운로드하여 직접 제

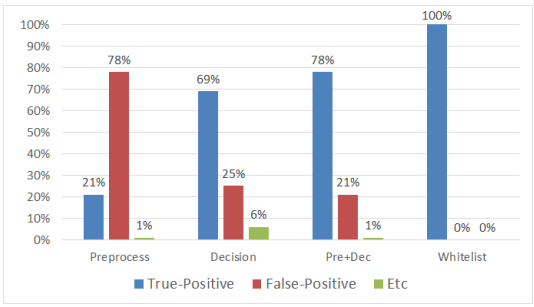

Fig.6. False positive rate of normal URL in comparison of preprocess, decision, whitelist)

작된 피싱사이트나 SSL(Secure Socket Layer) 기반의 사이트를 링크하여 제작된 피싱사이트의 탐지에는 한계를 보인다.

V. 결 론

본 논문에서는 내부 네트워크 환경에서 외부 인터넷에 접속하는 사용자의 트래픽을 미러링하고 이를 분석하여, 내부사용자가 기존에 알려지지 않은 피싱사이트의 접속을 탐지하는 방안을 제안하였다.

내부네트워크 환경의 사용자는 다양한 보안장비를 통하여 통제받은 인터넷 환경을 이용하고 있다. 하지만 알려져 있는 악성코드나 피싱사이트 공격보다, 알려져 있지 않은 형태의 악성코드나 피싱에 의한 피해가 발생하고 있으며, 내부직원의 피해를 탐지할 수 있는 방법이 없다.

제안된 탐지방안은 알려지지 않은 피싱사이트를 대상으로 66%의 탐지율과 34%의 미탐율을 보였다. 이는 기존에 제안된 블랙리스트 방식의 탐지 방법이 알려져 있지 않은 피싱사이트는 탐지하지 못하는 것과 비교할 때 매우 의미있는 탐지율이다. 하지만, 제안된 탐지방안은 이미지 등을 다운로드하여 직접 제작된 피싱사이트나 SSL기반의 사이트를 링크하여 제작된 피싱사이트의 탐지에는 한계를 보였다. 탐지율을 높이기 위해 휴리스틱, 블랙리스트 등과 결합한 추가적인 연구가 필요하다.

정상사이트를 대상으로 한 실험에서는 화이트리스트와 결합하여 0%의 오탐율을 나타냈다. 이는 제안된 방안이 내부네트워크를 운용하는데 문제를 발생시키지 않음을 보여준다. 따라서 침입차단시스템, 침입방지(탐지)시스템, 등의 기존 보안장비와 결합하여 사용할 때 효과적으로 피싱사이트 접속을 탐지 할 수 있을 것이다.

References

〔1〕 R. Manning, “Phishing Activity Trends Report 2Q 2014,” AntiPhishing Working Group(APWG), Aug. 2014.

〔2〕 KISA, “Computer Emergency Response Statics,” Internet & Security Focus, pp. 155-158, Aug. 2014

〔3〕 Y. Zhang, J. Hong, and L. Cranor, “CANTINA:A Content-Based Approach to Detecting Phishing Web Sites,” WWW ‘07 Proceedings of the 16th international conference on World Wide Web, pp. 639-648, May. 2007.

〔4〕 J.S. Shin, “Study on Anti-Phishing Solutions Related Researches and Future Directions,” Journal of The Korea Institute of Information Security & Cryptology, 23(6), pp. 1037 - 1047, Dec. 2013

〔5〕 KISA, “WebCheck System,” http://webcheck.kisa.or.kr

〔6〕 Naver, “Naver Toolbar Anti-Phishing,” http://tools.naver.com/service/toolbar

〔7〕 Estsoft, “Altoolbar Anti-Phishing,” http://www.altools.co.kr/Product /ALToolbar_Intro.aspx

〔8〕 Microsoft Corp, “Internet Explorer 9 Smart Screen Filter,” http://windows.microsoft.com/k o-kr/internet-explorer/products/ie-9/features/smartscreen-filter

〔9〕 Google, “Google Safe Browsing,” https://www.google.com /transparencyreport/safebrowsing/

〔10〕 N. Chou, R. Ledesma, Y. Teraguchi and J.C. Mitchell, “Client-Side Defense Against Web-Based Identity Theft,” Network and Distributed System Security Symposium, 2004.

〔11〕 Y. Zhang, S. Egelman, L. Cranor, and J. Hong, ″Phinding Phish: Evaluating Anti-Phishing Tools,″ Human Computer Interaction Institute, pp 76, http://repository.cmu.edu/hcii/76, 2006.

〔12〕 S. Garera, N. Provos, M. Chew, and Rubin, “A Framework for Detection and Measurement of Phishing Attacks,“ WORM ′07, pp. 1-8, Nov. 2007.

〔13〕 J.H. Sa and S. Lee, “Real-time Phishing Site Detection Method,” Journal of The Korea Institute of Information Security & Cryptology, 22(4), pp. 819-825, Aug. 2012

〔14〕 R. Fielding, J. Gettys, J. Mogul, H.

Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, "Hypertext Transfer Protocol – HTTP/1.1." RFC 2616, Jun 1999.
〔15〕 M. Still, "Python effective TLD library," http://www.stillhq.com /python/etld/000001.html
〔16〕 OpenDNS, "PhishTank," http://www.phishtank.com
〔17〕 Mediachannel Inc, "Rankey," http://www.rankey.com

〈저자소개〉

박 정 욱 (Jeong-Uk Park) 정회원
2003년 2월: 원광대학교 컴퓨터·정보통신공학부 학사
2006년 8월: 전북대학교 컴퓨터정보학과 석사
2013년 2월: 전북대학교 정보보호공학과 박사 수료
2007년 1월~현재: 전라북도교육청 주무관
〈관심분야〉 정보보호, 이동컴퓨팅, 만물인터넷, SDN

조 기 환 (Gi-Hwan Cho) 종신회원
1985년 2월: 전남대학교 계산통계학과 학사
1987년 2월: 서울대학교 계산통계학과 석사
1996년 5월: 영국 Newcastle 대학교 전산학과 박사
1987년 9월~1997년 8월: 한국전자통신연구원 선임연구원
1997년 9월~1999년 2월: 목포대학교 컴퓨터과학과 교수
1999년 3월~현재: 전북대학교 컴퓨터공학부 교수
〈관심분야〉 이동컴퓨팅, 컴퓨터통신, 분산처리시스템, 정보보호, 무선네트워크