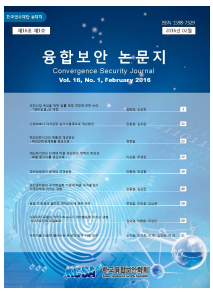


융합보안논문지
제16권 제1호

ISSN : 1598-7329(Print)

이미지를 이용한 웹사이트 위·변조 탐지 기법 연구

신지용, 조지호, 이한, 김정민, 이극

To cite this article : 신지용, 조지호, 이한, 김정민, 이극 (2016) 이미지를 이용한 웹사이트 위·변조 탐지 기법 연구, 융합보안논문지, 16:1, 81-87

이미지를 이용한 웹사이트 위·변조 탐지 기법 연구

신지용* · 조지호* · 이 한* · 김정민* · 이 극**

요 약

본 논문에서는 이미지를 이용한 웹사이트 위·변조 탐지 기법을 제안한다. 제안하는 시스템은 사용자가 웹사이트 위·변조를 통한 금융정보 탈취 목적을 가진 악성코드에 감염된 후 특정 금융 웹사이트에 접속 시 사용자가 접속한 웹사이트의 캡처 이미지와 정상 웹사이트의 캡처 이미지의 유사도를 비교분석하여 웹사이트 위·변조 여부를 탐지하고 정상인 경우 분석을 종료하지만 비정상으로 판단될 경우 이를 사용자에게 메시지를 통해 현재의 피해 상태를 알려줌으로써 위·변조된 웹사이트를 통해서 추가적인 금융정보 유출 사고가 발생하지 않도록 사전에 방지한다.

A Study on Website Forgery/Falsification Detection Technique using Images

JiYong Shin*·Jiho Cho*·Han Lee*·JeongMin Kim*·Geuk Lee**

ABSTRACT

In this paper, we propose a forgery/falsification detection technique of web site using the images. The proposed system captures images of the web site when a user accesses to the forgery/falsification web site that has the financial information deodorizing purpose. The captured images are compared with those of normal web site images to detect forgery/falsification. The proposed system calculates similarity factor of normal site image with captured one to detect whether the site is normal or not. If it is determined as normal, analysis procedure is finished. But if it is determined as abnormal, a message informs the user to prevent additional financial information spill and further accidents from the forgery web site

Key words : Website Forgery/Falsificatin Detection, Pharming, Images Analysis

접수일(2016년 1월 21일), 게재확정일(2016년 2월 25일)

★ 본 연구는 산업통상부 지역혁신연구센터사업인 민군겸용 보안공학 연구센터의 지원으로 수행되었음.

* 한남대학교 컴퓨터공학과

** 한남대학교 컴퓨터공학과 (교신저자)

1. 서 론

온라인을 이용한 금융서비스의 편리함으로 인해 사용자는 계속 늘어 2015년 3월말을 기준으로 인터넷뱅킹서비스(모바일뱅킹 포함) 등록고객 수는 1억 861만 명으로 전분기말대기 5.3% 증가하였다. 일평균 인터넷뱅킹(모바일뱅킹 포함) 이용건수는 7,694만 건으로 전분기 대비 8.6% 증가하였다[1].

인터넷뱅킹 사용자의 증가는 해커들로부터의 위협에 쉽게 노출되는 결과 또한 초래하게 되었다. 실제의 은행 사이트와 유사한 파밍사이트를 이용하여 이용자로부터 금융거래가 가능한 개인정보를 입력하도록 유도하여 피해가 발생하는 방법이다. 이와 같은 방법은 실제 사이트와 유사하기 때문에 사용자가 사이트의 위·변조 여부를 직접 판단하기 어려움이 있다. 국내에서는 사이버 위협에 대응하기 위해 '국가 사이버 안전센터(NCSC)'를 중심으로 분야별 사이버 보안을 담당하는 부문 보안관제 센터를 구축·운영하고 있으나, 보안관제 센터의 대상기관 수가 증가함에 따라 실시간으로 위·변조를 탐지하고 대응하는데 있어서 한계가 있다.

앞으로 다양한 패턴의 웹사이트 위·변조 공격 유형이 나타날 것으로 예상되며, 본 논문에서는 이러한 웹사이트 위·변조 공격의 유형을 분석하여 효율 적으로 탐지하고 예방할 수 있는 시스템을 제안한다. 제안된 시스템은 사용자가 웹사이트 위·변조를 통한 금융정보 탈취 목적을 가진 악성코드에 감염된 후 특정 금융 웹사이트(제1금융권 인터넷 뱅킹 웹사이트)에 접속 시 사용자가 접속한 웹사이트의 캡처 이미지와 정상 웹사이트의 캡처 이미지의 유사도를 비교분석하여 웹사이트 위·변조 여부를 탐지한다. 탐지 결과가 정상인 경우 분석을 종료하지만 비정상으로 판단될 경우 이를 사용자에게 메시지를 통해 현재의 탐지 결과를 알려줌으로써 위·변조된 웹사이트를 통해서 추가적인 금융정보 유출 사고가 발생하지 않도록 사전에 방지한다.

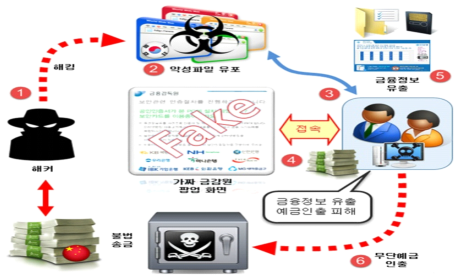
2. 관련연구

2.1 웹사이트 위·변조 공격의 종류

2.1.1 피싱(Phishing)과 파밍(Pharming)공격

피싱(Phishing)이란 개인정보(Private data)와 낚시(Fishing)의 합성어로 개인으로부터 금융기관이나 공공기관으로 가장해 전화나 이메일로 웹페이지에서 금융거래 가능한 정보를 요구하는 수법이다.

파밍(Pharming)이란 피싱(Phishing)과 조작(Farming)의 합성어로 악성프로그램에 감염된 PC를 조작하여 피해자가 정상 사이트로 접속하더라도 가짜 은행사이트로 접속을 유도하여 금융거래정보를 빼낸 후 금전적인 피해를 입히는 수법을 말한다.



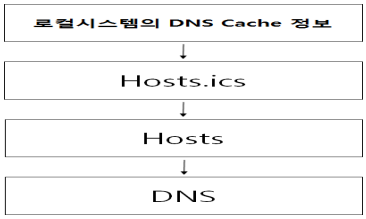
(그림 1)금융감독원 사칭 파밍악성코드 유포과정

공격자는 다수의 웹사이트를 해킹해보며 보안이 취약한 웹사이트에 파밍 악성코드를 감염시키고 보안에 약한 이용자가 해당 웹사이트를 접근 시 악성코드가 설치된다. 최근에는 대표적으로 금융감독원을 사칭한 플로팅 배너기법을 사용하여 공격을 시도하는데, 배너에 포함된 파밍 사이트는 위·변조된 파밍 국내 금융사이트이며, 이를 통해 공격자는 이용자들의 개인정보(공인인증서, 보안카드 번호, 아이디 및 패스워드 등)를 탈취하는데 목적이 있다.

2.1.2 hosts파일 및 hosts.ics파일 변조 공격

hosts 파일은 파일 내에 URL 주소와 대응하는 IP 주소를 기록하며, DNS 서버 접근 이전에 확인하여 해당 URL이 hosts 파일 목록에 존재 한다면 그 URL에 해당하는 IP 주소로 연결시킨다. hosts.ics 파일은 인터

넷 연결 공유 (ICS: Internet Connection Sharing) 시 해당 시스템의 네트워크 주소를 강제로 지정하는 기능을 하는 것이다. 이 파일은 일반 hosts 파일보다 우선순위가 높기 때문에 hosts 파일과 hosts.ics 파일이 같이 존재 할 경우 hosts.ics 파일을 먼저 참조하게 되며, hosts.ics 파일이 존재 하지 않을 경우 hosts파일을 바로 참조한다[2].



(그림 2)웹사이트 접속 시 참조되는 우선순위

2.1.3 플로팅 배너 기법을 이용한 파밍 공격

플로팅 배너 기법은 광고배너에 파밍 광고를 넣어 이를 클릭하면 파밍 사이트로 연결하는 악성코드이다.

(그림 3)홈페이지 유포 파밍형 악성코드 감염 사례

공격자는 다수의 웹사이트를 해킹해보며 보안이 취약한 웹사이트에 파밍 악성코드를 감염시키고 보안에 약한 이용자가 해당 웹사이트를 접근 시 악성코드가 설치된다. 최근에는 대표적으로 금융감독원을 사칭한 플로팅 배너기법을 사용하여 공격을 시도하는데, 배너에 포함된 파밍사이트 또한 위·변조된 파밍 국내 금융사이트이며, 이를 통해 공격자는 이용자들의 개인정보(공인인증서, 보안카드 번호, 아이디 및 패스워드 등)를 탈취하려는데 목적이 있다[3].

2.2 기존 웹사이트 위·변조 탐지 및 대응 기술

2.2.1 페이져스(Pagers)

페이져스는 PhantomJS를 이용해서 웹사이트를 지정한 해상도 별로 스크린 샷을 찍어 주는 node.js 커맨드라인 도구이며, 반응형 웹을 개발할 때 많이 사용되는 프로그램이다.

(그림 4) 페이져스 해상도 별 스크린샷 결과

2.2.2 단일/인접 픽셀방식

O단일 픽셀 비교 방식은 이미지 1개의 픽셀의 RGB(Red, Green, Blue)값이 모두 같을 때 동일한 픽셀로 판단한다.

인접 픽셀 비교방식은 이미지 1개의 픽셀에 인접한 픽셀들의 RGB(Red, Green, Blue)값까지 동일해야 동일한 이미지로 판단한다.

인접픽셀방식은 단일픽셀 방식과는 달리 인접한 픽셀들의 값까지 비교하기 때문에 정확도는 높지만, 신속성이 떨어진다[4].

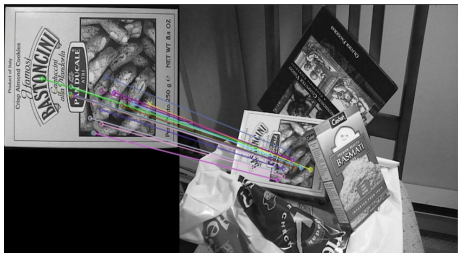
2.2.3 OpenCV(Open Computer Vision)

OpenCV(Open Computer Vision)은 오픈 소스 컴퓨터 비전 C 라이브러리이지만 2015년 06월 04일 최신 OpenCV3.0버전은 java 라이브러리도 지원한다. 원래는 인텔이 개발하였으며, 윈도우, 리눅스 등의 여러 플랫폼에서 사용할 수 있다. OpenCV는 실시간 이미지 프로세싱에 중점을 둔 라이브러리이며, 응용 기술의 예로는 인간과 컴퓨터 상호 작용(HCI), 물체 인식, 안면인식, 모바일 로보틱스, 제스처 인식 등이 있다[5].

OpenCV는 세가지 이미지 비교방식(Comparing Histograms, Template Matching, Feature Matching)

이 있다.

피처 매칭은 이미지 유사성을 비교할 때 가장 효과적인 방식이다. 이미지로부터 수많은 피처(Feature)를 추출하며, 피처 부분이 회전, 확대/축서, 찌그러짐이 발생하더라도 동일한 피처로 인식하도록 보장한다. 추출된 피처들을 다른 이미지의 피처셋과 비교하면서 유사성을 검사하게 된다. (그림 5)은 두 개의 이미지에서 추출한 피처셋이 높은 비율로 일치한다면, 동일하거나 유사한 이미지로 볼 수 있다. 본 논문에서는 피처 매칭 기법을 이용하여 이미지의 유사성을 비교한다.[6].



(그림 5) 피처 매칭 방식의 예

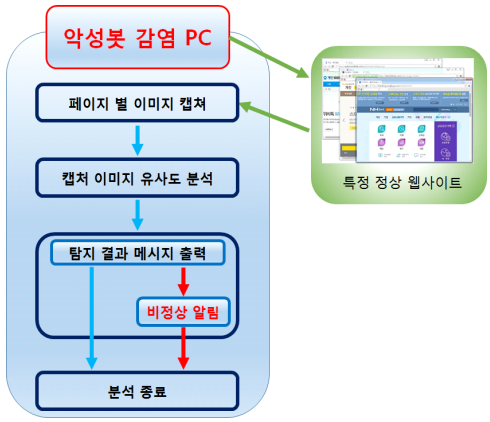
3. 이미지를 이용한 웹사이트 위변조 탐지 기법

3.1 이미지를 이용한 웹사이트 위변조 탐지 시스템 제안

본 논문에서는 이미지를 이용한 웹사이트 위·변조 탐지 시스템을 제안한다. 제안된 시스템은 사용자가 웹사이트 위·변조를 통한 금융정보 탈취 목적을 가진 악성코드에 감염된 후 특정 금융 웹사이트에 접속할 경우, 사용자가 접속한 웹사이트와 정상 웹사이트를 비교분석하여 웹사이트 위·변조 여부를 탐지하고 이를 사용자에게 알려줌으로써 금융정보 유출 사고를 사전에 방지한다.

3.1.1 시스템 구성 및 동작순서

제안된 시스템은 총 5개로 구성되며, 페이지 별 이미지 캡처와 캡처이미지 유사도 분석, 탐지결과 메시지 출력, 비정상 알림으로 구성된다.



(그림 6) 이미지를 이용한 웹사이트 위·변조 탐지 시스템 구성도

분석을 수행하기 전에 해커로부터 악성코드에 감염된 사용자 PC가 금융 웹사이트에 접근 할 경우 사용자가 접속한 웹페이지의 URL을 크롤링하여 정상 금융웹페이지의 URL과 비교하게 되며, 비교된 결과를 토대로 분석을 수행 할지 아니면 분석을 종료할지를 판단하게 된다.

이때 사용자가 접속하여 분석 대상이 되는 특정 금융 웹사이트는 농협 인터넷뱅킹, KB국민은행 인터넷뱅킹, 우리은행 인터넷뱅킹, 신한은행 인터넷뱅킹, 신협은행 인터넷뱅킹 등의 제1금융권 인터넷 뱅킹 웹사이트로 한다.

사용자가 특정 금융 웹사이트에 접속하였다면 이미지의 비교분석을 위해 웹페이지 별로 이미지를 캡처하게 된다.

페이지 별 이미지 캡처는 사용자가 접속한 특정 금융 웹사이트의 MAIN 페이지, 로그인 페이지, 보안카드 번호 입력 페이지를 이동할 때마다 웹페이지를 캡처하게 되며, 사용자 마다 해상도가 다를 수 있기 때문에 pageres를 이용하여 정상 웹사이트로부터 업데이트된 이미지와 동일한 해상도로 웹페이지를 캡처한다.

pageres로 부터 수집된 이미지를 사전에 업데이트 해놓은 정상 웹사이트 이미지와 비교하게 된다. 비교는 OpenCV '피처 매칭'을 사용하였으며, 각각의 이미지 분석결과는 다음과 같이 나타낸다.

이미지가 같은 경우 정상을 의미하는 '1', 이미지가 다른 경우 '0'의 값을 담지결과 알림 단계로 보내게 된다.

탐지 결과 통보는 이미지 분석을 통해 얻어진 결과를 토대로 정상인 경우 분석을 종료하고, 비정상인 경우 사용자 본인이 접속한 페이지가 비정상임을 확실히 알고 추가적인 개인정보 입력하지 않도록 메시지를 출력해준다.

3.2 웹사이트 위·변조 탐지 시스템 실험 결과

3.2.1 실험환경

실험 대상은 이용고객수가 가장 높은 실제의 농협인터넷뱅킹, 국민은행인터넷뱅킹의 웹사이트로 하였으며, WINDOWS 7 운영체제를 사용하였다. 또한 이미지 분석을 위한 OpenCV3.0 라이브러이와 개발언어는 JAVA를 사용하였다.

3.2.2 페이지 별 이미지 캡처 실험 결과

페이지별 이미지를 캡처하기 위해서 pageres를 사용하였으며, 캡처한 이미지는 농협인터넷뱅킹의 MAIN 페이지 와 로그인 페이지, 계좌 이체 페이지 부분이다.

(그림 7)과 같이 캡처된 이미지를 통해 이미지 유사도 분석을 진행한다.

(그림 7) 페이지 별 캡처 이미지
(좌측은 정상 웹사이트,우측은 탐지대상 웹사이트)

3.2.3 캡처 이미지 유사도 비교

(그림 8)은 OpenCV를 이용한 피쳐매칭(feature matching) 결과를 나타내며, 분석결과를 자세히 확인하기 위해 '매칭 수'의 값과 '매칭 시간' 값을 출력하였다. '매칭 수'는 피쳐매칭(feature matching)을 통해서 매칭(Matching)된 요소(feature)의 수를 나타낸다. '매칭 시간'은 이미지를 매칭(Matching)하는데 걸리는 시간을 나타낸다.

```
run:
▶이미지1 비교 결과
매칭시간 = 345ms / 매칭 수 = 500(feature)
이미지가 동일합니다.

▶이미지2 비교 결과
매칭시간 = 128ms / 매칭 수 = 500(feature)
이미지가 동일합니다.

▶이미지3 비교 결과
매칭시간 = 91ms / 매칭 수 = 0(feature)
이미지가 다릅니다.
```

(그림 8) 이미지 유사도 비교 결과

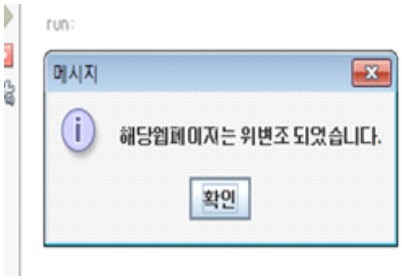
이미지는 총 세가지 페이지를 캡처한 이미지를 비교하였으며, 이미지 1과 이미지 2의 분석결과는 매칭 시간에는 다소 차이가 있었지만 매칭 수는 동일하게 비교되었다. 하지만 이미지 3번과 같은 경우, 두 웹페이지의 이미지가 다르다고 판단되었다. 확인한 결과 비교되어진 두 이미지는 보안카드 번호입력을 요구하는 페이지이지만, 사용자가 접속한 페이지는 위·변조된 사이트의 보안카드번호 입력을 요구하는 페이지이며, 정상웹사이트와는 전혀 다른 웹페이지 구조와 보안카드번호 전체를 입력하도록 유도하는 부분이 포함되어 있음을 확인하였다.

3.2.4 탐지결과 통보 실험 결과

(표 1)는 캡처된 이미지의 유사도 비교 결과를 보여주고 있으며, 이미지 1과 2는 정상, 이미지 3은 비정상으로 분석되었으며, 비정상으로 판단된 경우 (그림 9)와 같이 사용자에게 메시지를 출력해준다.

[표 1] 웹사이트 위·변조 탐지결과

	정상	비정상	결과	결과에 따른 처리
이미지 1	1	0	정상	분석 종료
이미지 2	1	0	정상	
이미지 3	0	1	비정상	사용자 통보 후 분석 종료



(그림 9) 탐지결과에 따른 메시지 출력 화면

4. 결 론

온라인을 이용한 금융 서비스의 편리함으로 인하여 사용자가 지속적으로 증가하고 있으며, 이러한 인터넷 뱅킹 사용자의 증가는 해커들로부터의 위협에 쉽게 노출되는 결과 또한 초래하게 된다.

본 논문에서는 현존하는 공격 탐지 방법들을 응용 및 적용하고 웹사이트의 위·변조 여부를 탐지하기 위하여 이미지를 이용한 웹사이트 위변조 탐지 기법을 제안하였다. 제안된 기법은 사용자가 웹사이트 위·변조를 통한 금융정보 탈취 목적을 가진 악성코드에 감염된 후 특정 금융 웹사이트(제1금융권 인터넷 뱅킹 웹사이트)에 접속 시, 사용자가 접속한 웹사이트의 캡처 이미지와 정상 웹사이트의 캡처 이미지의 유사도를 비교분석하여 웹사이트 위·변조 여부를 탐지한다. 분석 결과가 정상인 경우 분석을 종료하지만 비정상으로 판단될 경우 이를 사용자에게 메시지를 통해 현재의 피해 상태를 알려줌으로써 위·변조된 웹사이트를 통해서 추가적인 금융정보 유출 사고가 발생하지 않도록 사전에 방지한다.

향후 연구 과제로서는 이미지의 유사도를 분석하는데 있어서 빠른 분석 속도와 정확성 더욱 강화해야 할 것이며, 관제요원의 모니터링을 함께 진행한다면 빠른 대응이 이루질 수 있다. 또한 이미지와 금융 웹사이트가 가지고 있는 추가적인 요소들을 함께 분석하여 보다 신속하고 정확하게 탐지할 수 있도록 기술을 보완해야 할 것이다.

참고문헌

[1] http://www.bok.or.kr, 한국은행 보도자료, '2015년 1/4분기 국내 인터넷 뱅킹 서비스 이용현황', 공보 2015-5-29호 , 2015.5

[2] http ://www.hauri.co.kr/ information/ issue_view.html? intSeq=243&page=1, ㈜하우리, 보안이슈 분석 "2014년에 등장한 파밍의 기술", 2015.

[3] http://blog.alyac.co.kr/285, 알약블로그, "더욱 교묘해지고 있는 금융감독원 사칭 파밍 수법", 2015.03.

[4] 김규일, 최상수, 박학수, 고상준, 송중석, '이미지 및 코드분석을 활용한 보안관제 지향적 웹사이트 위·변조 탐지 시스템', 정보보호학회논문지, 제24권 25호, pp.871-883, 2014.10

[5] https://ko.wikipedia.org/wiki/OpenCV, "OpenCV",

[6] http://blog.acronym.co.kr/archive/20150922, "OpenCV를 활용한 이미지 유사도 비교 방법", 2015.08.

[저자소개]

신 지 용 (Jiyong Shin)

2014년 한남대학교
컴퓨터공학과 학사 졸업
현 재 한남대학교 대학원
컴퓨터공학과 석사과정
재학 중

email : shinpar90@naver.com

조 지 호 (Jiho Cho)

2012년 한남대학교
컴퓨터공학과 학사 졸업
2014년 한남대학교 대학원
컴퓨터공학과 석사 졸업
현 재 한남대학교 대학원
컴퓨터공학과 박사과정
재학 중

email : charismaup@nate.com

이 한 (Han Lee)

2015년 한남대학교
컴퓨터공학과 학사 졸업
현 재 한남대학교 대학원
컴퓨터공학과 석사과정
재학 중

email : history1989@naver.com

김 정 민 (Jeong-Min Kim)

2015년 한남대학교
수학과 학사 졸업
현 재 한남대학교 대학원
컴퓨터공학과 석사과정
재학 중

email : kjm9366@naver.com

이 극 (Geuk Lee)

1983년 경북대학교
전자계산공학과 졸업
1986년 서울대학교
컴퓨터 공학과 석사 졸업
1993년 서울대학교
컴퓨터 공학과 박사 졸업
2003년~2012년 지경부지정RIC 민군
겸용보안공학 연구센터(SERC)
소장
1988년~현재 한남대학교
컴퓨터공학과 교수

email : leegeuk@hnu.kr