

Host 파일 변조를 이용한 파밍

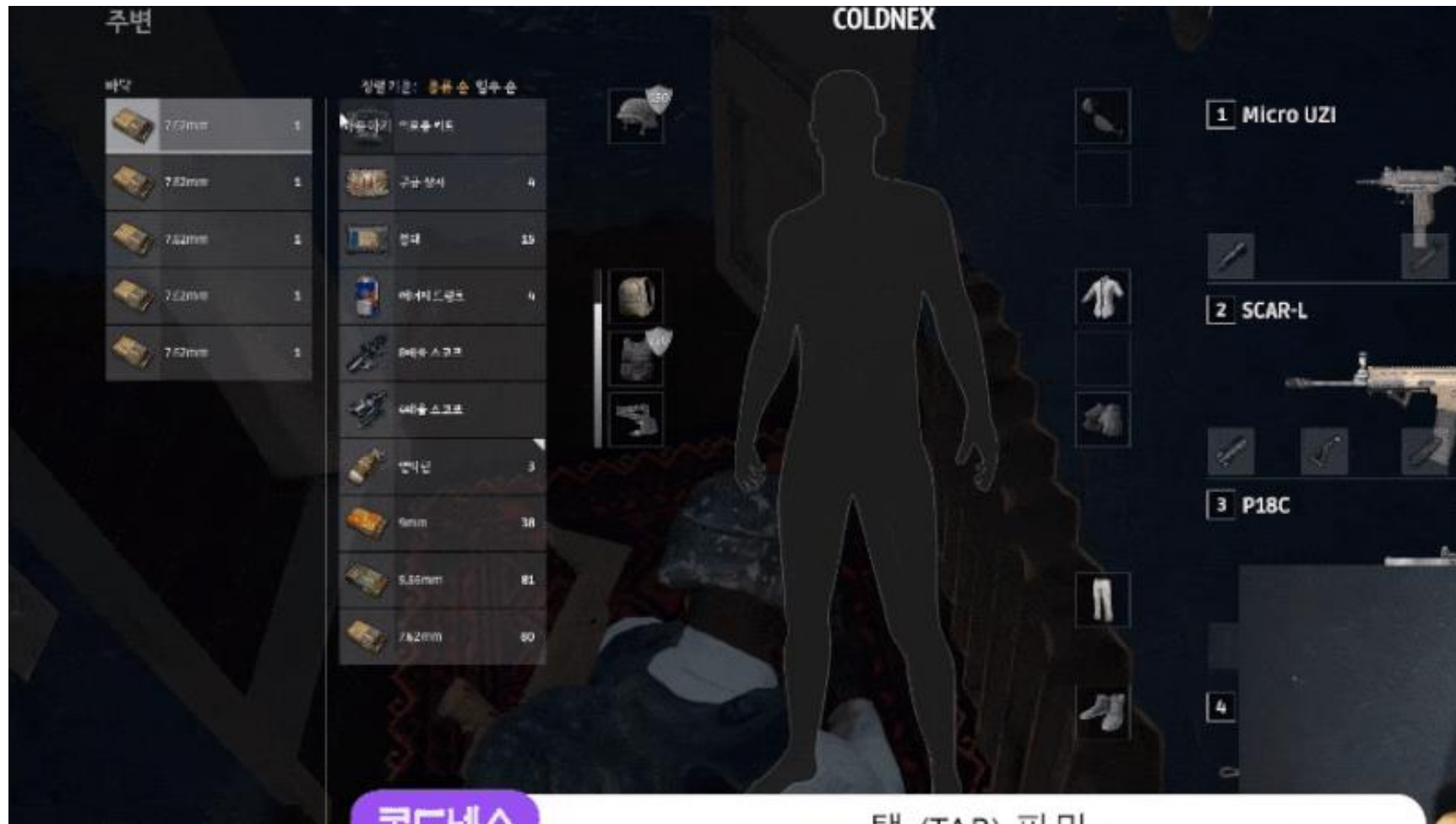
중부대 SCP 정보보안 동아리
92113566 1학년 부원 노무승

목차

1. 파밍이란?
2. Host 파일이란?
3. 실습
4. 대비 방안

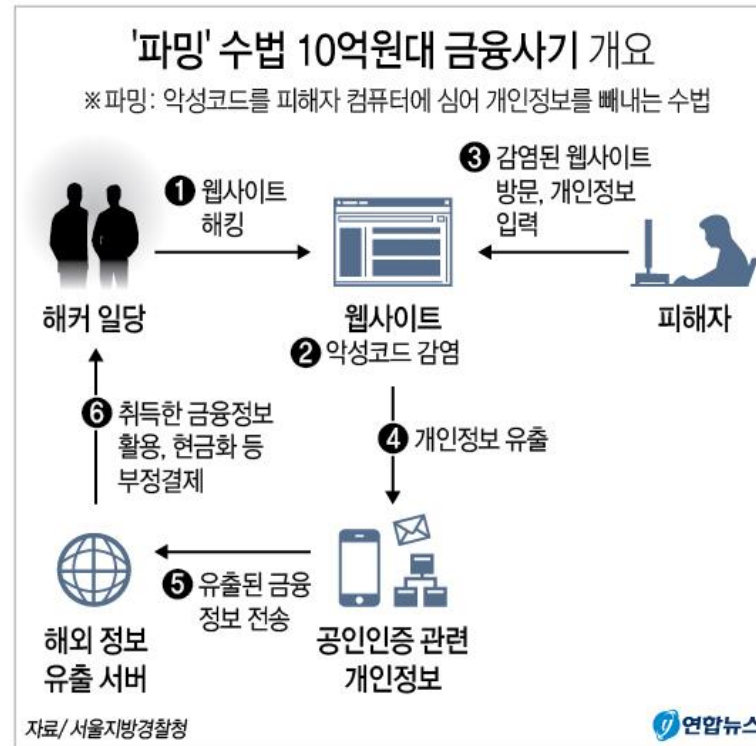
1. 파밍이란?

1-1. 파밍이란?



파밍(Farming)?

1-1. 파밍이란?



이재윤 기자 / 20171101 트위터 @yonhap_graphics 페이스북 tune.kr/LeYN1

파밍 (Pharming) :
 사용자를 속여 사용자가 가짜 사이트에 접속하도록 유도하는 사기 수법.

1-2. 피싱이란 다른 점

피싱 (Phishing):

비정상적인 사이트를 정상적인 사이트인 것 처럼 보여줌.

<https://www.g00gle.com>

파밍 (Pharming) :

정상적인 사이트를 비 정상적인 사이트로 보여줌.

<https://www.google.com>



<https://www.g00gle.com>

1-3. 다양한 파밍 공격..

호스트 파일 변조 뿐만 아니라..

DNS 스푸핑 :

DNS 요청에 변조된 DNS 응답 패킷을 전송

공유기 DNS 변경 :

공유기 설정 페이지에 관여하여 악성 DNS로 변경

DHCP 스푸핑 :

DHCP 서버에서 자동으로 IP와 DNS를 할당 받을 때,
해커가 이를 변조하여 악성 DNS로 변경

2. Host 파일이란?

2-1. Host 파일?

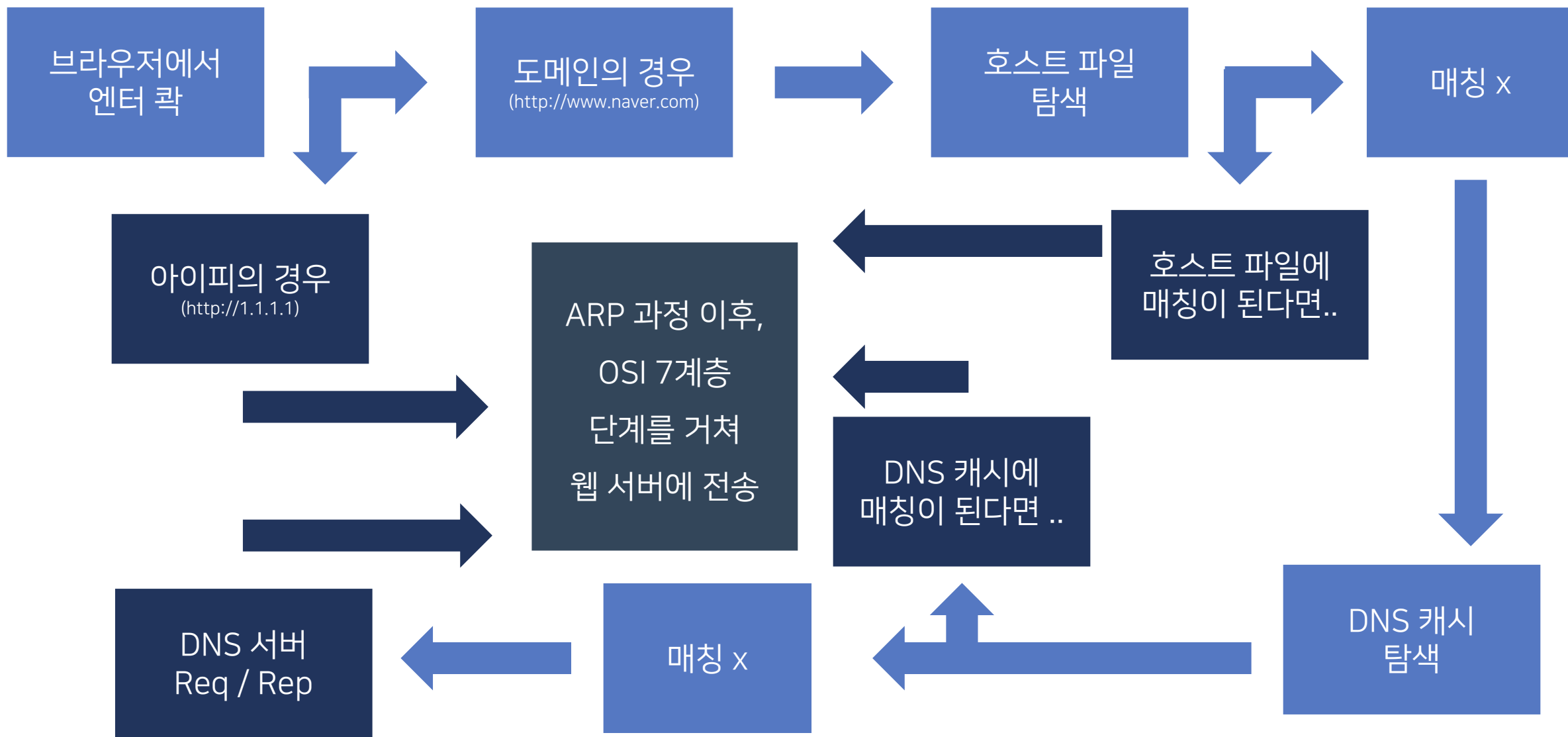
호스트 파일 (Hosts File):

운영체제가 호스트 네임을 특정 IP에 매핑하기 위한 파일

운영 체제	버전	위치
유닉스, 유닉스 계열, POSIX		/etc/hosts ^[1]
마이크로소프트 윈도우	3.1	%WinDir%\hosts
	95, 98, ME	%WinDir%\winhosts ^[2]
	NT, 2000, XP, ^[3] 2003, 비스타, 2008, 7, 2012, 8, 10	%SystemRoot%\System32\drivers\etc\hosts ^[4]

(출처: <https://ko.wikipedia.org/wiki/Hosts>)

2-2. 컴퓨터가 웹 서버에 접속할 때..



2-3. 검은색 박스의 공통점

(호스트 네임(www.naver.com)에 해당하는)

IP 주소를 알아내는 과정

```
▼ Ethernet II, Src: IntelCor_d4:8d:de (0c:dd:24:d4:8d:de), Dst: EFMNetwo_de:51:5a (88:36:6c:de:51:5a)
  > Destination: EFMNetwo_de:51:5a (88:36:6c:de:51:5a)
  > Source: IntelCor_d4:8d:de (0c:dd:24:d4:8d:de)
  Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.0.11, Dst: 223.130.195.95
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 41
    Identification: 0x1cd0 (7376)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.11
    Destination Address: 223.130.195.95
  > Transmission Control Protocol, Src Port: 3582, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

3. 실습

3-1. 실습전..



변조 대상 호스트는 네이버임.
현재 www.naver.com 접속시, 네이버로 연결이 잘 됨.

3-2. 변조 할 아이피 획득

```
C:\Users\#2N>nslookup www.joongbu.ac.kr
서버:      kns.kornet.net
Address:    168.126.63.1

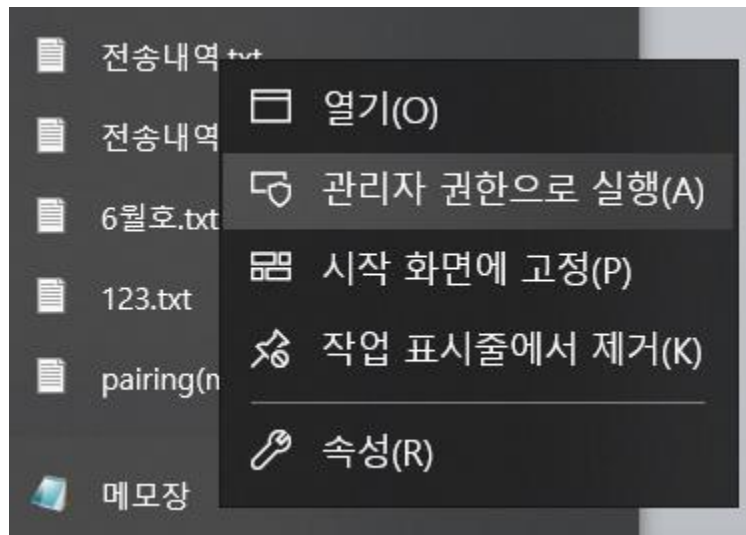
권한 없는 응답:
이름:      www.joongbu.ac.kr
Address:    210.125.239.51
```

cmd에서 nslookup 명령어로
중부대 홈페이지의 아이피를 알아냄

3-3. Hosts 파일 변조 (1)

로컬 디스크 (C:) > Windows > System32 > drivers > etc				
이름	수정한 날짜	유형	크기	
hosts	2021-08-05 오전 3:18	파일	1KB	
lmhosts.sam	2019-12-07 오후 6:12	SAM 파일	4KB	
networks	2019-03-19 오후 1:49	파일	1KB	
protocol	2019-03-19 오후 1:49	파일	2KB	
services	2019-03-19 오후 1:49	파일	18KB	

C:\Windows\System32\drivers\etc\hosts



3-4. Hosts 파일 변조 (2)

hosts - Windows 메모장

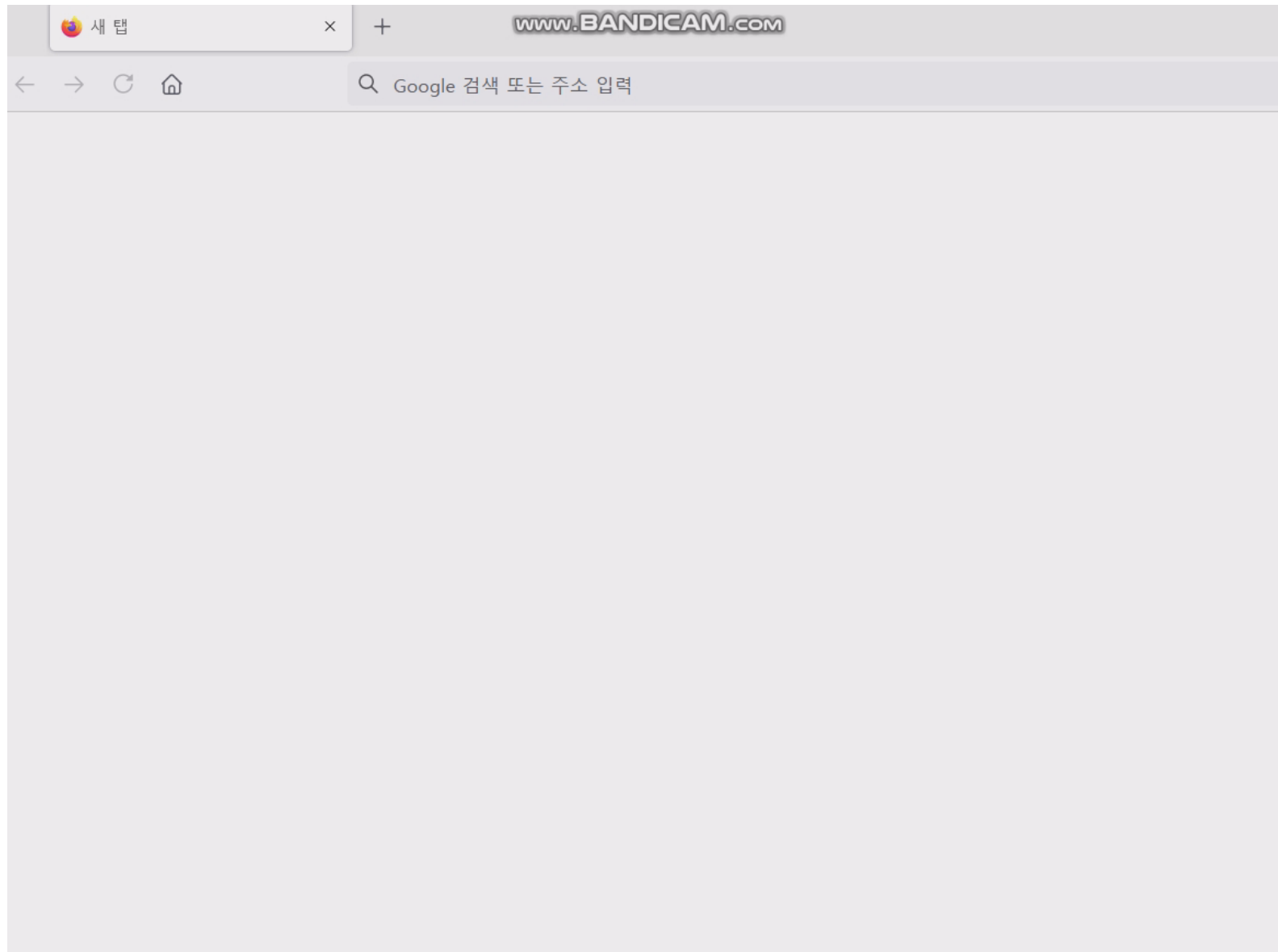
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
# Copyright (c) 1993-2006 Microsoft Corp. # = 주석
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
210.125.239.51 www.naver.com
```

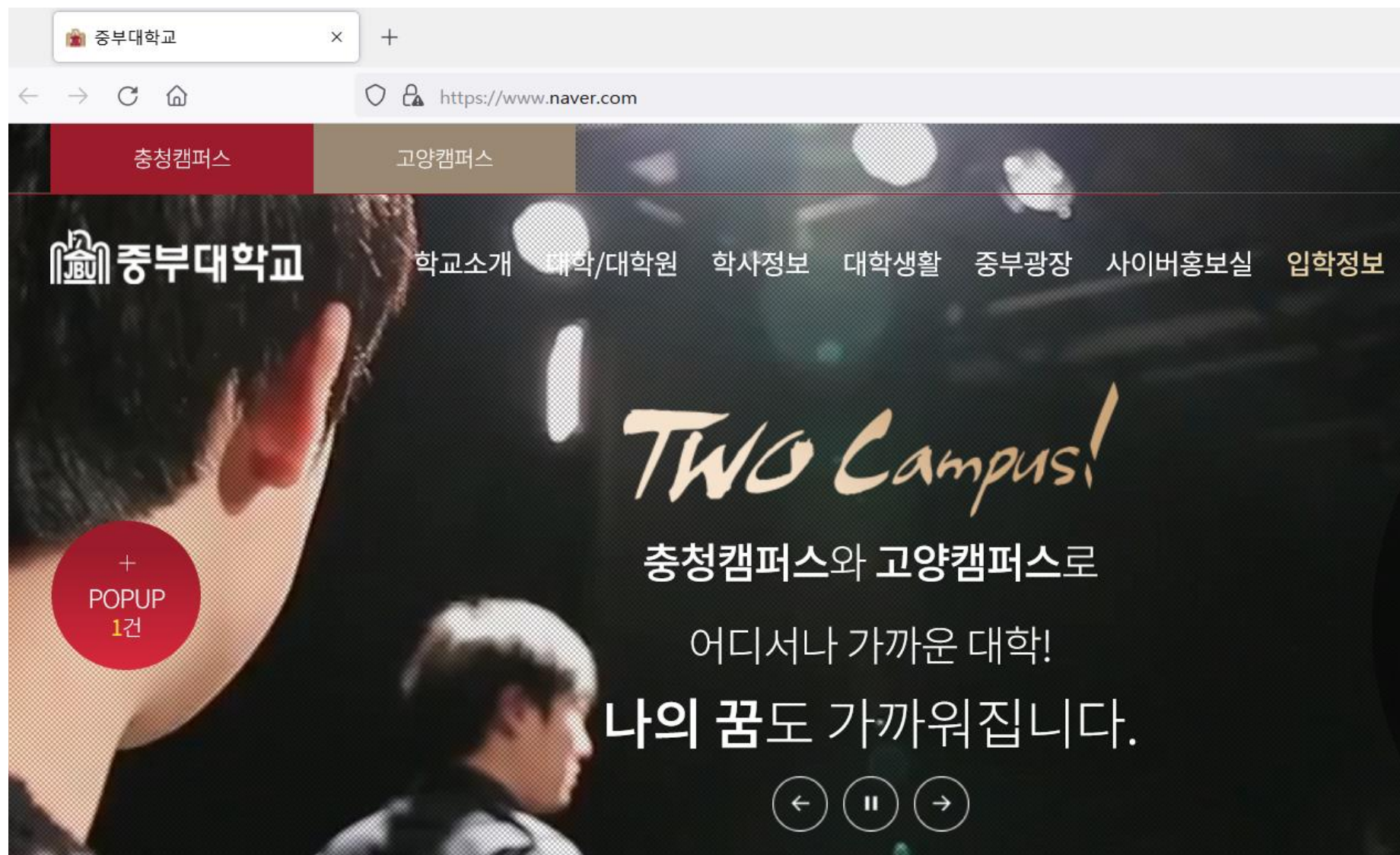
[아이피] [호스트 이름]

= 우변의 호스트 이름은 좌변의 아이피를 나타낸다.

3-5. PoC(Proof of Concept) 영상



3-6. Pwned!



3-7. 실제 사례..

보안뉴스

전체기사


SECURITY

IT

SAFETY

Security World

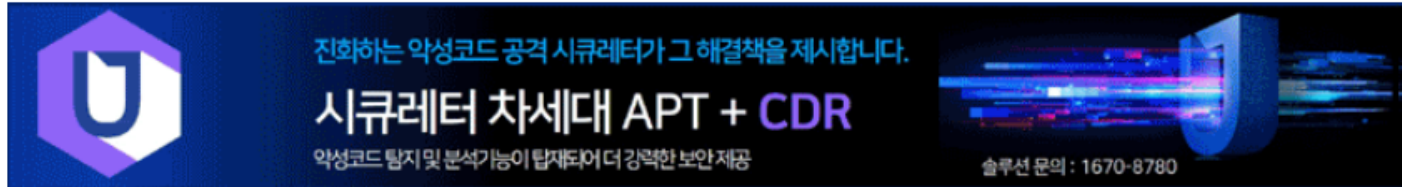
변경된 네이버 메인에 금감원 사칭 파밍! 점점 지능·신속화

 좋아요 103개

| 입력: 2017-04-03 01:30



가장



#파밍

#네이버

#피싱

#금융감독원

#금융정보

신규 네이버 메인 페이지에 금감원 사칭 팝업 띄워
국내 공유기 DNS 변조해 네이버 접속시 QR 코드 띄우기도
미래부와 KISA 사칭하기도...공격기법 더욱 기발해져

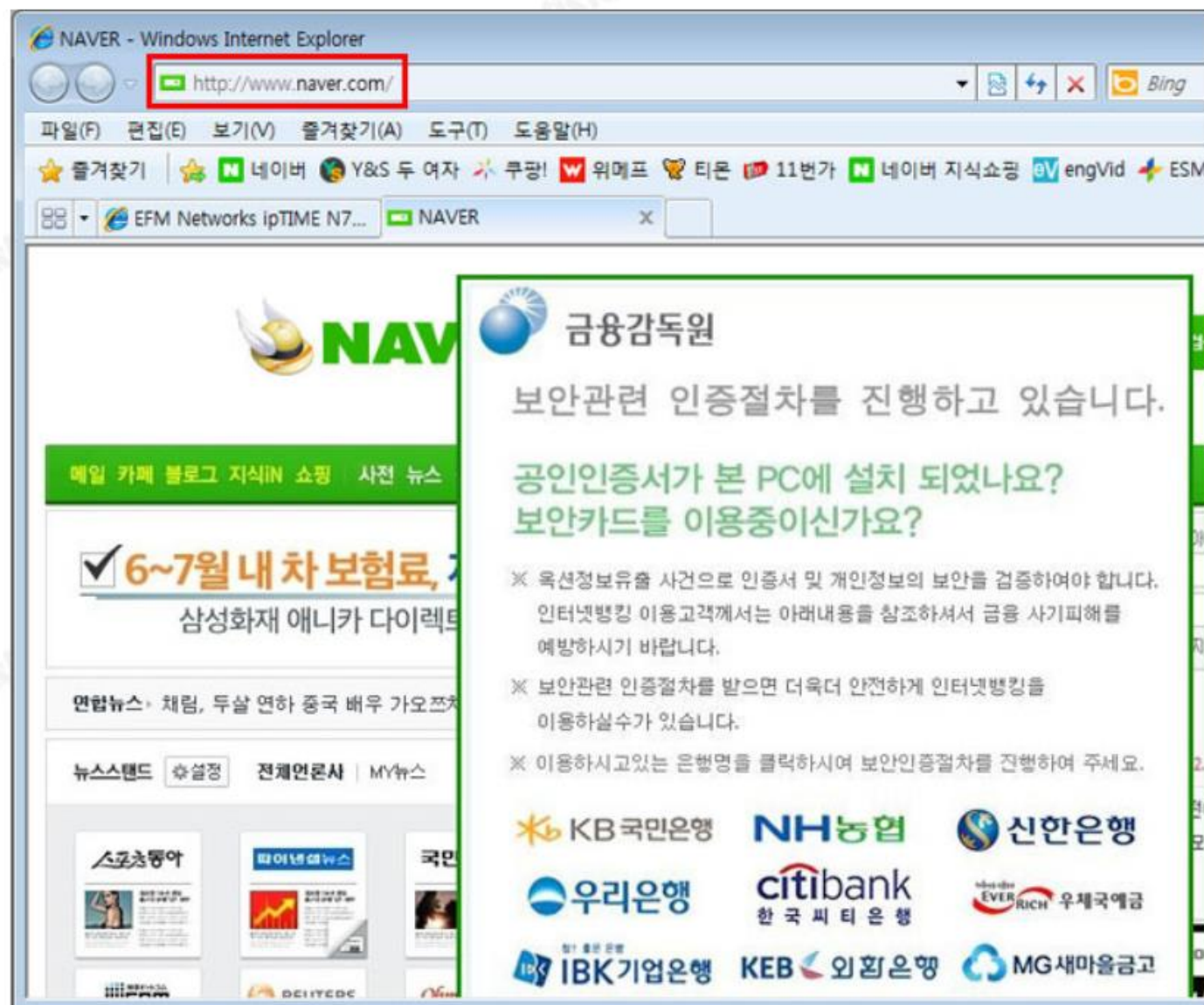
[보안뉴스 성기노 객원기자] ‘파밍’ 사기 수법이 더욱 교묘해지고 빈도도 잦아지고 있다. 파밍 해커조직들이 지난 3월말부터 변경된 네이버 메인 페이지에 대한 적응을 끝내고 새로운 네이버 메인 페이지에 금융감독원 사칭 팝업을 띄워 사용자들을 속이는 파밍 기법이 새롭게 등장했다. 또한, 얼마 전에는 국내 공유기 DNS를 변조해 네이버 접속시 QR 코드를 띄우는 피싱 사이트가 나오게 하는 파밍 기법도 출현했다는 게 한 보안전문가의 설명이다.

- 1 [
- 2 운
- 3 린
- 4 □
- 5 산
- 6 [
- 7 人
- 8 을
- 9 각
- 10 린

주요

W

3-8. 실제 사례..



4. 대비 방안

4-1. 사용자측 대비방안(1)



알약 호스트 파일 보호 알림

4-2. 사용자측 대비방안(2)

1. 호스트 파일은 주기적으로 체크해주면 좋음
2. 백신에 '호스트 파일 보호 기능'이 있으면 활용하자.
3. 인터넷에서 무분별하게 받은 실행 파일은 항상 확인하자.
(컴퓨터 내부 백신 or 바이러스 토탈)
4. 문서형 악성코드, 확장자 취약점(U+202E) 악성코드,
페이크 파일(아이콘만 정상)도 항상 조심하자.

4-3. 개발자(시큐어코딩)측 대비방안

1. MITM 공격에 취약하지 않게끔 프로그래밍 하자.

(AES+RSA 암호화 통신 등..)

2. 호스트 파일이나 DNS 캐시 등을 검증하는 루틴을 추가하자.

```
Public Function HFCheck(url As String)
'[제목: HostFileCheck]
'[함수이름: HFCheck]
'[제작자: 2N(nms200299)]
'[제작날짜: 2015-11-30]
'[수정날짜: 2015-12-02]
Dim File As Integer
Dim i As String, data As String
' 필요한 변수 선언
File = FreeFile
Open "C:\Windows\System32\drivers\etc\hosts" For Input As #File
'Host File 파일을 읽기모드로 연다.
Do Until EOF(File)
'파일의 끝까지 반복한다.
Line Input #File, i
'특정 줄의 파일의 내용을 읽는다.
data = data + i + vbNewLine
'data에 읽어들인 파일의 내용을 저장한다.
Loop
'반복한다.
data = UCase(data): url = UCase(url)
'[수정내용] data 랑 url을 대문자로 변환한다.
'해주는 이유는 host파일안 내용중 특정 문자가 대문자일 경우를 대비해
'Host파일로 부터 읽은 내용과 감지할URL을 똑같이 대문자로 바꾼 다음 비교한다.
Close #File
'읽기모드로 연 파일의 읽기를 종료한다.
If InStr(data, url) Then
'data변수에 url이 들어있으면
HFCheck = True
'HFCheck에 True를 반환하고,
Exit Function
'함수를 나간다.
Else 'data변수에 url이 들어있지않다면
HFCheck = False
'HFCheck에 False를 반환한다.
End If
End Function
```

사용법(폼 소스코드)

```
If HFCheck([감지할 URL]) = True Then
MsgBox "Host파일 변조가 감지되었습니다. 프로그램을 종료합니다.", 16, "Host파일 변조 감지"
End
End If
```

[감지할 URL] 에는 하드인증을 할때 사용하는 웹사이트를 넣으시면 됩니다.
단, 꼭 http:// 는 빼주셔야 합니다.

```
예):
If HFCheck("nms200299.dothome.co.kr") = True Then
MsgBox "Host파일 변조가 감지되었습니다. 프로그램을 종료합니다.", 16, "Host파일 변조 감지"
End
```

```
End If
```

음.. 하지만 위 방법이 만능은 아니예요...
위 방법은 그냥 단순한 스크립트 키드들을 막기위한 방법이죠.

Q & A

「
감사합니다
」