악성코드 상세 분석 보고서

네이버로 위장한 피싱 공격

(Document No : DT-20240528-001)

HAURI

www.hauri.co.kr

ㅇ 분석 개요

최근 국내 포털 사이트 네이버 로그인 계정을 탈취하기 위해 피싱 사이트를 만들어 국내 사용자들에게 메일을 통해 유포되고 있는 것이 발견됐다.

이들은 피해자가 입력한 계정 정보를 네이버(naver.com)에 전송하여 올바른 계정 정보를 입력하였는지 검증하였으며, 로그인 성공 시 패스워드 변경도 요청하여 피해자가 피싱 사이트로 인지 못 하게 여러 기능들을 구현해놓는 치밀함을 보이고 있다.

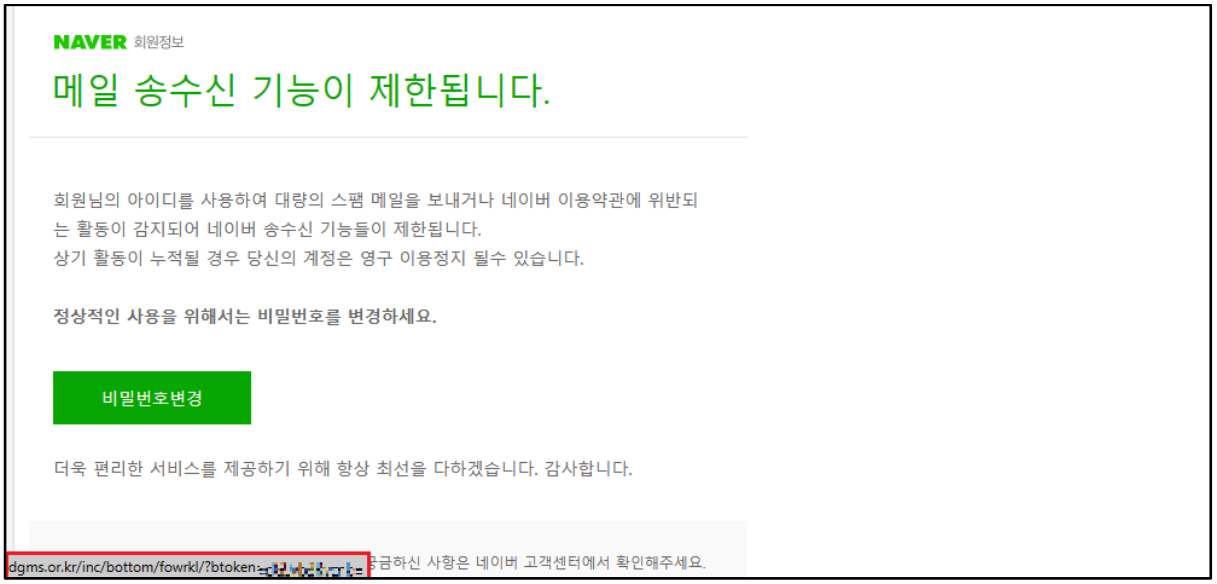
해당 피싱 공격의 배후로는 북한 해킹 그룹 **김수키(Kimsuky)**로 추정되고 있으며, 김수키 그룹은 이전부터 카카오 및 네이버 등을 사칭하여 피싱 공격을 진행한 기록이 있다.

ㅇ 피싱 메일

상세분석 :

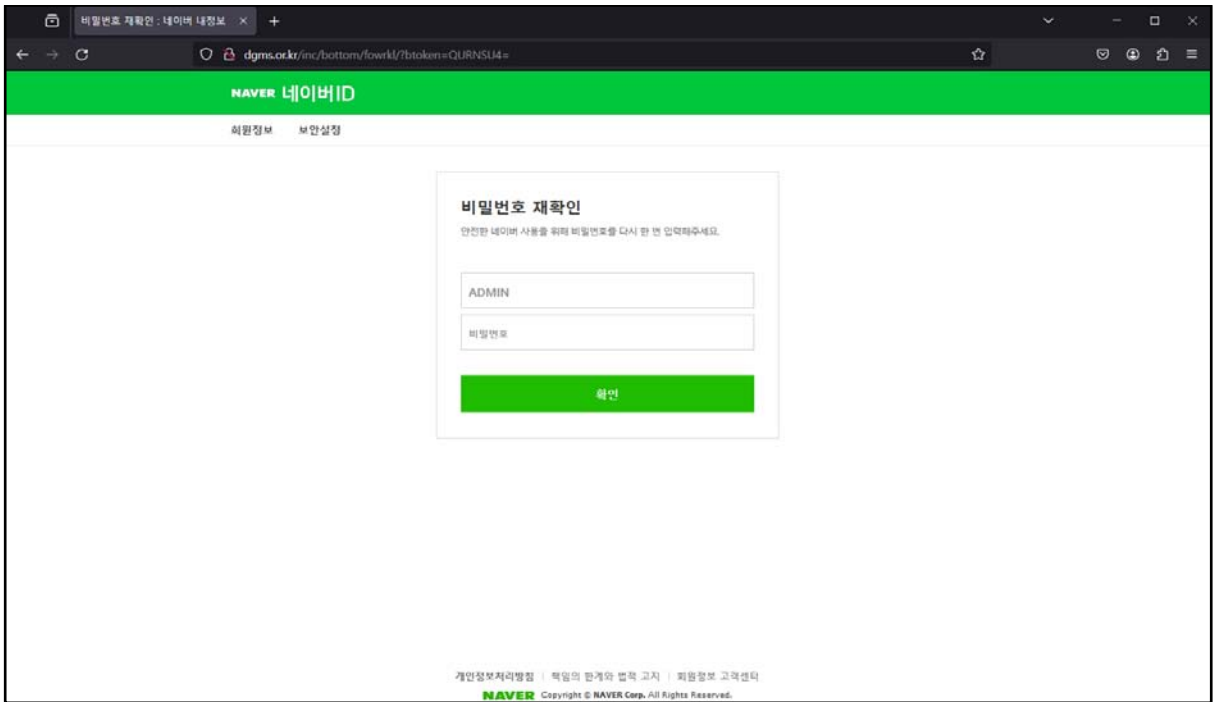
(1) 국내 포털 사이트 "네이버" 고객센터를 사칭하여 보안상의 문제로 비밀번호 변경을 미끼로 피싱 사이트 접속을 유도하고 있으며, **"비밀번호 변경"** 버튼에 하이퍼링크를 설정됨

※ **피싱 사이트 주소 : hxxp://dgms.or.kr/inc/bottom/fowrkl/?btoken={BASE64 인코딩된 ID}**



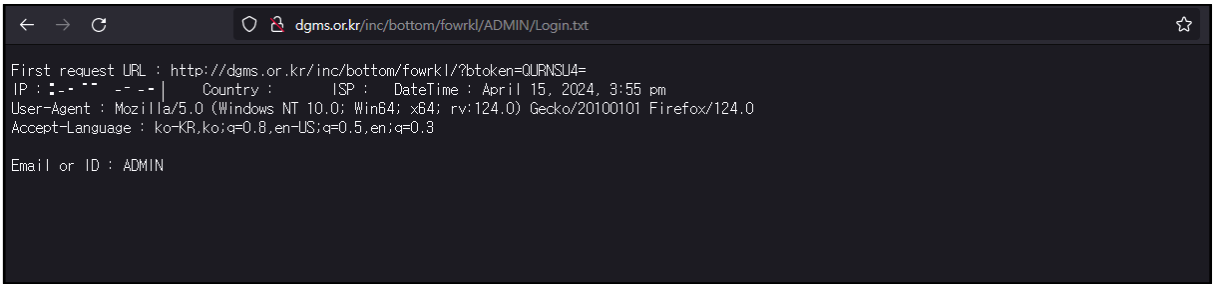
[그림 1] 하이퍼링크

(2) 피싱 사이트 접속 시 네이버 비밀번호 확인 화면이 나오며, "btoken" 값에 설정된 값을 BASE64 디코딩하여 네이버 계정을 설정한다.



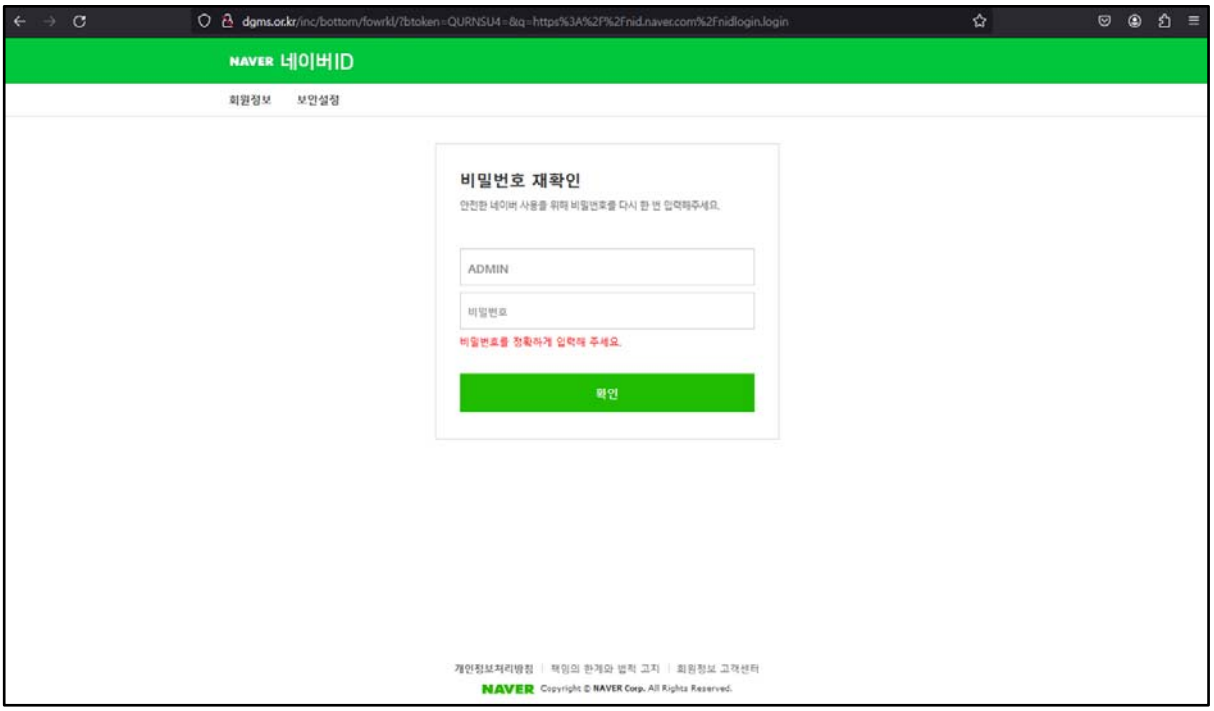
[그림 2] 피싱 사이트

(3) 피싱 서버에는 접속한 네이버 ID 로 폴더가 생성되며, IP 주소 및 User-Agent 를 **"/네이버 ID/Login.txt"**에 파일을 생성하여 기록한다.



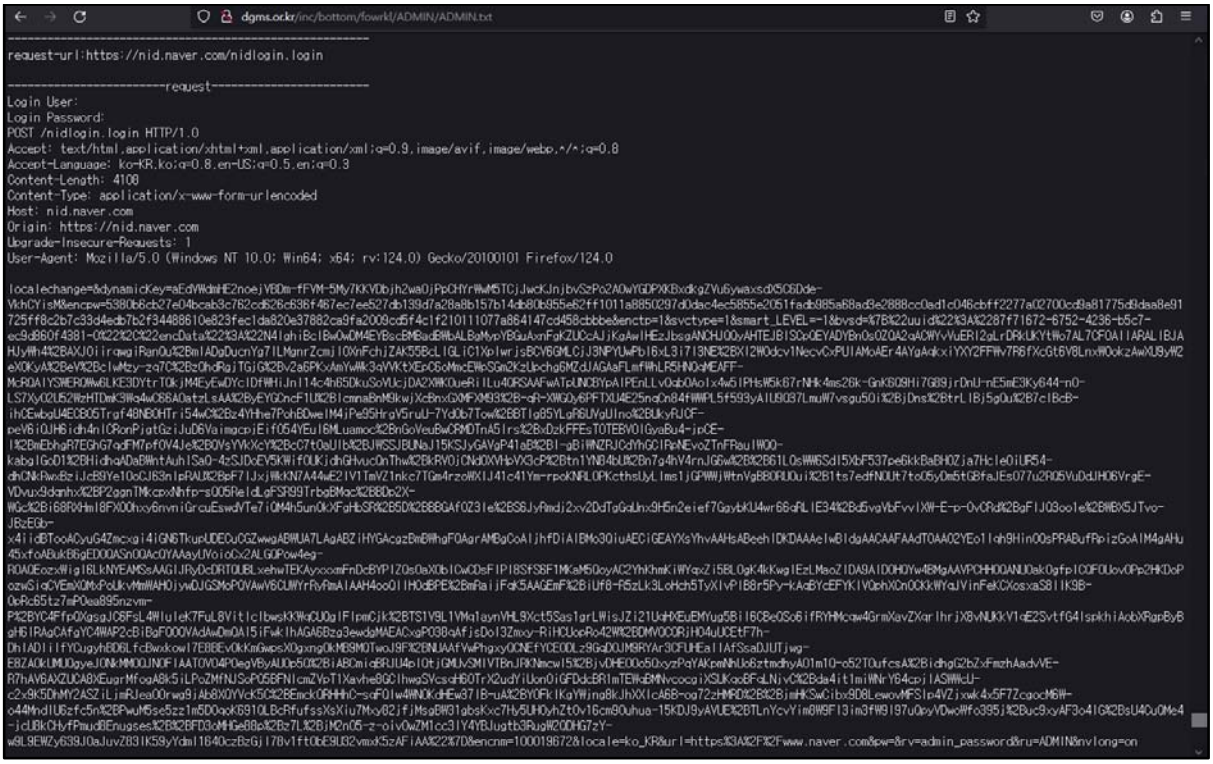
[그림 3] /네이버 ID/Login.txt

(4) 패스워드를 입력 시 실제 네이버 사이트에 로그인을 시도하여 올바른 패스워드인지 검증한다.



[그림 4] 틀린 패스워드 입력 시 화면

(5) 피싱 서버는 네이버와 HTTP 통신을 기록을 **"/네이버 ID/네이버 ID.txt"** 로그 파일에 기록하고 있다.



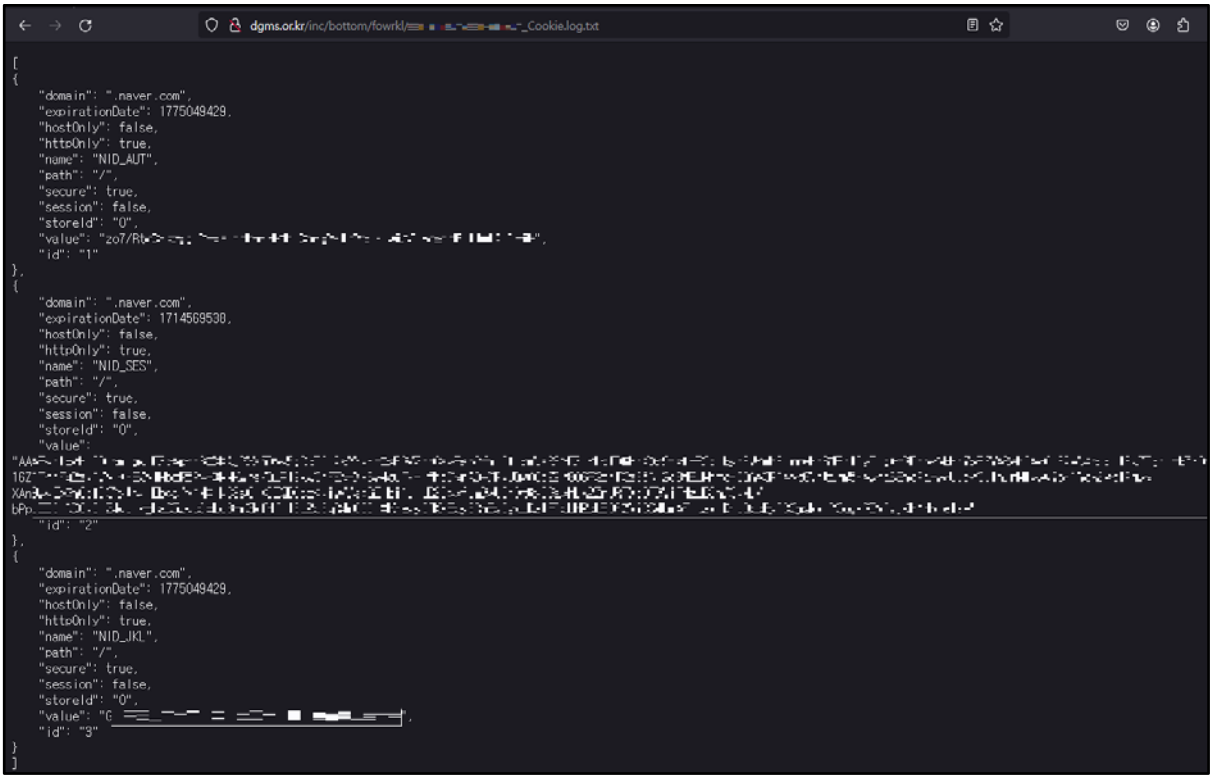
[그림 5] 네이버 통신 로그

(6) 만약 올바른 계정 정보를 입력할 경우 피싱 서버에서 네이버에 로그인 후 네이버 계정 접속에 필요한 Cookie 들을 **"/네이버 ID/네이버 ID_Cookie.log.txt"** 파일에 저장한다.

※ **수집되는 Cookie : NID_SES, NID_AUT, NID_JKL, NID_SAUTO**

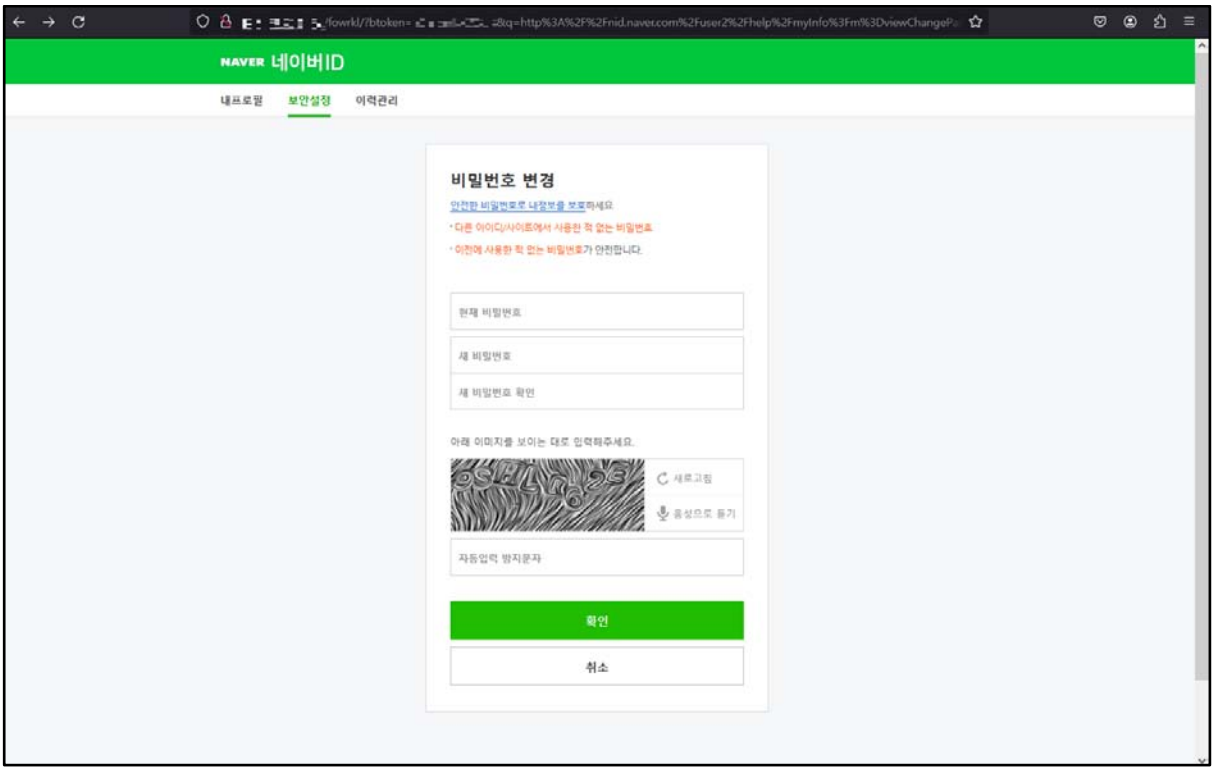
```
555   do {
799       if (isset($_response_headers['set-cookie']) && $_flags['accept_cookies']) {
800           foreach ($_response_headers['set-cookie'] as $cookie) {
805               $_set_cookie[] = $cookie;
806               /*********************************************************/
807               if ($_http_mode_proxy) {
808                   $name = $value = '';
809                   preg_match('#^\s*([^=;,\s]*)\s*=?\s*([^;]*)#',$cookie, $match) && list(, $name, $value) = $match;
810                   preg_match('#;\s*expires\s*=\s*([^;]*)#i',      $cookie, $match) && list(, $expires)      = $match;
811                   preg_match('#;\s*path\s*=\s*([^;,\s]*)#i',      $cookie, $match) && list(, $path)         = $match;
812                   preg_match('#;\s*domain\s*=\s*([^;,\s]*)#i',    $cookie, $match) && list(, $domain)       = $match;
813                   //preg_match('#;\s*(secure\b)#i',                 $cookie, $match) && list(, $secure)       = $match;
814                   $expires_time = empty($expires) ? 0 : intval(@strtotime($expires));
815                   if ($value == '')
816                       continue;
817                   //NID_AUT,NID_SES,NID_JKL,NID_SAUTO인 경우만 기록
818                   if($name == "NID_AUT" || $name == "NID_SES" || $name == "NID_JKL" || $name == "NID_SAUTO"){
819                     Add_Plugin_Cookie("Cookie.log","$name","$value","naver.com",'false',$expires_time);
820                   }
```

[그림 6] Cookie 를 수집하는 피싱 페이지 코드(index.php)



[그림 7] 수집된 Cookie 들

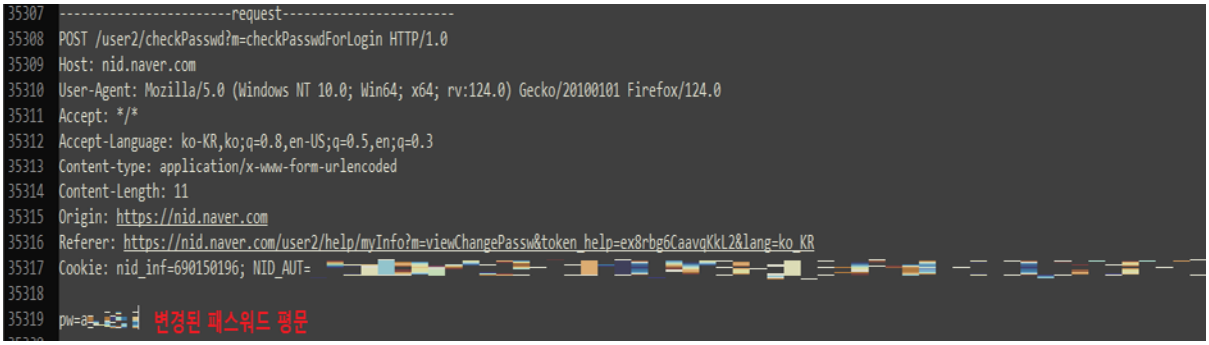
(7) Cookie 들을 저장 후 비밀번호 변경 페이지를 출력한다.



[그림 8] 비밀번호 변경 페이지

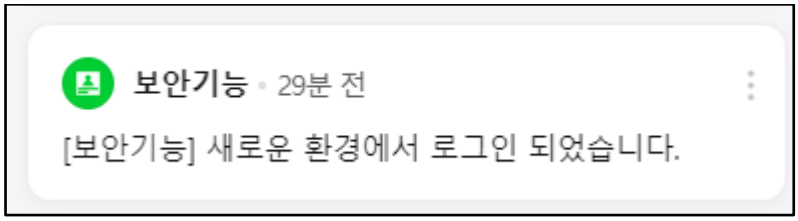
(8) 비밀번호 변경 시 실제 계정 패스워드도 변경되며, 네이버와의 통신 로그에 변경된 패스워드도 기록된다.

[그림 9] 실제 변경된 패스워드



[그림 10] 네이버 통신 로그에 기록된 패스워드

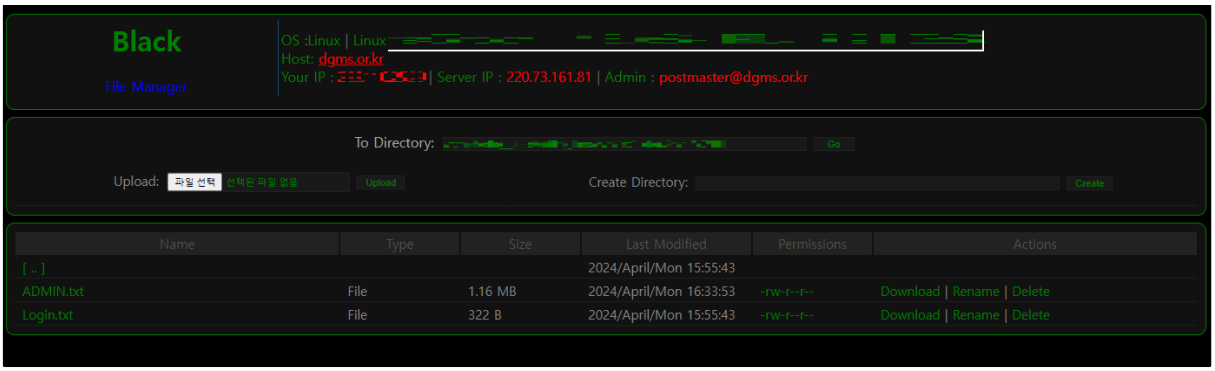
(9) 이후 공격자가 수집된 Cookie 들을 사용해 계정에 접속할 경우 네이버 계정 접속 기록 및 보안 기능에 걸리지 않는다.



[그림 11] 네이버 보안 기능

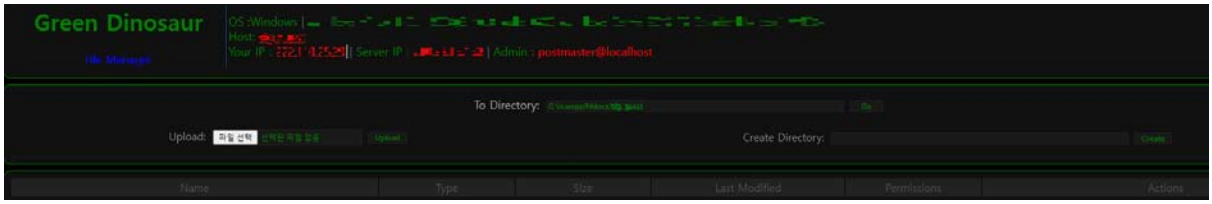
(10) 피싱 서버에서 웹쉘이 발견됐으며, 취약한 사이트에 웹쉘을 업로드하여 사용 중인 것으로 추정된다.

※ 웹쉘 발견 주소 : hxxp://dgms.or.kr/inc/bottom/myid.php



[그림 12] 피싱 서버에서 발견된 웹쉘

(11) 발견된 웹쉘은 북한 해킹 그룹 **김수키(Kimsuky)**가 사용하는 것으로 알려진 **"Green Dinosaur"** 웹쉘과 인터페이스 및 코드가 동일한 것으로 확인됐으며, 이번 피싱 공격도 김수키의 소행일 것으로 추정된다.



[그림 13] Green Dinosaur 웹쉘

[그림 14] Green Dinosaur, Black 코드 비교

IOC

Index.php

- C456E2E0C015A4D3FEE7E17B7229B9AA

myid.php

- 5BFA4D6D14C5BAF5AD3DB44BC58CFEE4

hxxp://dgms.or.kr/inc/bottom/fowrkl

hxxp://dgms.or.kr/inc/bottom/myid.php

hxxp://www.lkh.co.kr/eng/data/ncdos

hxxp://www.lkh.co.kr/eng/data/myid.php